Уильям Р. Станек

Windows® 7

Справочник администратора

- Подробный справочник по администрированию Windows 7
- Таблицы, пошаговые инструкции, описание параметров

IT Professional

РУССКАЯ РЕДАКЦИЯ Microsoft bhv®

William R. Stanek

Windows® 7

Administrator's Pocket Consultant

Microsoft® Press

Уильям Р. Станек

Windows® 7

Справочник администратора

РУССКАЯ РЕДАКЦИЯ

bhv®

2010

УДК 681.3.06
ББК 32.973.26–018.2
С76

Станек Уильям Р.

С76 Windows 7. Справочник администратора / Пер. с англ. — М. : Издательство «Русская редакция» ; СПб. : БХВ-Петербург, 2010. — 720 стр. : ил.

ISBN 978-5-7502-0399-4 («Русская редакция»)
ISBN 978-5-9775-0587-1 («БХВ-Петербург»)

Эта книга — подробный справочник по администрированию новейшей клиентской операционной системы от Microsoft Windows 7. В ней содержатся сведения об архитектуре системы, описание ее установки и развертывания, а также работы в средах Windows PE и Windows RE. Детально рассказывается об управлении Windows 7, об использовании групповой политики, об автоматической и ручной настройке системы, о настройке рабочего стола и панели задач. Приводятся сведения о настройке и контроле учетных записей пользователей и групп, об организации входа в систему и о работе в компьютерных сетях. Отдельные главы посвящены вопросам установки оборудования и программного обеспечения, управлению дисками и другими накопителями, а также использованию новых технологий — TPM и шифрованию BitLocker. Особое внимание уделено вопросам производительности системы, безопасности данных, а также их архивации и восстановлению. Кроме того, специально рассматривается использование Window 7 на мобильных компьютерах.

Книга состоит из 17 глав и богато иллюстрирована. Она предназначена, главным образом, для администраторов и ИТ-специалистов общего профиля, но будет также полезна всем желающим изучить возможности новейшей операционной системы от Майкрософт.

УДК 681.3.06
ББК 32.973.26–018.2

Оглавление

Введение

Писать эту книгу было очень интересно, но и нелегко. Когда я приступал к работе над ней, то предполагал, что опишу отличия Windows 7 от Windows Vista и Windows XP и подчеркну новые возможности администрирования. Для адекватного знакомства с любой новой операционной системой (ОС), особенно с Windows 7, приходится детально исследовать ее работу и глубоко погружаться в ее внутреннее устройство.

Отличия Windows 7 от предыдущих версий Windows бросаются в глаза, как только вы начинаете работать с этой ОС. Однако это первое впечатление не покажет, насколько сильно Windows 7 отличается от своих предшественниц: наиболее значительные изменения скрыты под внешней оболочкой. Они затрагивают не только интерфейс, но саму архитектуру системы, и именно об этих изменениях писать было сложнее всего.

Любой справочник администратора должен быть компактным и ясным, чтобы с его помощью можно было разобраться в проблеме, где бы она вас ни застала. Поэтому мне пришлось тщательно проанализировать итоги своих исследований и приложить усилия, чтобы сосредоточиться исключительно на основных аспектах администрирования Windows 7. Результатом стала книга, которую вы держите в руках. Я надеюсь, что вы согласитесь со мной и признаете эту книгу самым практичным и компактным руководством по Windows 7. В книге рассмотрены все вопросы, ответы на которые понадобятся вам для решения типичных административных задач на компьютерах, работающих под управлением Windows 7.

Поскольку я поставил перед собой задачу вложить максимум содержания в минимальный объем, вам не придется продираться через сотни страниц лишних подробностей, чтобы разыскать нужные сведения. Вы найдете в точности то, что нужно для устранения конкретной проблемы и решения конкретной задачи. Говоря коротко, эта книга должна стать единым ресурсом, к которому вы будете обращаться всякий раз, когда у вас возникнут вопросы по администрированию Windows 7. В ней подробно описаны повседневные действия администратора, объяснены типичные задачи, приведены примеры и списки параметров, представительные, хотя и необязательно исчерпывающие.

Эту книгу хотелось с одной стороны сделать лаконичной, чтобы не дать ей разбухнуть и чтобы в ней было просто ориентироваться, а с другой сторо-

ны максимально заполнить ее информацией, чтобы она была действительно полезным ресурсом. И вот к вашим услугам не тяжеленный тысячестраничный том и не стостраничная брошюра, а удобное издание, которое поможет вам быстро справиться со всеми типичными проблемами.

Кому адресована книга

В этой книге рассматриваются все издания Windows 7. Основная аудитория книги такова:

- администраторы систем Windows;
- опытные пользователи, частично выполняющие обязанности администраторов;
- администраторы, переходящие на Windows 7 с предыдущих версий;
- администраторы, переходящие на Windows 7 с других платформ.

Чтобы сэкономить место для более важной информации, я буду предполагать, что у вас имеются навыки по работе в сети и общее знакомство с семейством ОС Windows. Поэтому в книге нет глав с описанием работы в Windows, архитектуры и сетей Windows. С другой стороны, я уделил внимание настройке рабочего стола, особенностям работы с портативными компьютерами, конфигурированию TCP/IP, профилям пользователей и оптимизации системы.

В книге также подробно рассматривается устранение неполадок: я постарался включить соответствующие разделы в каждую главу. Советы по диагностике проблем вплетены в основной текст книги, чтобы вы всегда читали их без отрыва от контекста, поэтому я не написал о неполадках самостоятельную главу. Надеюсь, прочитав эту книгу, вы станете работать эффективнее и обеспечите более удобную рабочую среду для своих пользователей.

Структура книги

Предполагается, что вы будете использовать этот справочник в повседневном администрировании, и потому за основу в структуре книги взяты не компоненты Windows 7, а решаемые администратором задачи. Как и прочие книги этой серии, она предназначена для использования в «боевых условиях».

Существенным элементом такого справочника является простота поиска нужной информации. В этом вам поможет развернутое оглавление, а также многочисленные перекрестные ссылки в тексте. В книге много подробных инструкций и справочных таблиц.

Соглашения, принятые в книге

Чтобы текстом было проще пользоваться, я включил в него некоторые специфические элементы оформления. Примеры команд даны моноширинным шрифтом. Строки и команды, которые вы должны вводить с клавиатуры, отмечены **полужирным** шрифтом. Новые термины выделяются *курсивом*.

В книге использованы следующие виды примечаний:

Примечание	Дополнительные сведения по конкретной теме, которые необходимо особо подчеркнуть
Совет	Полезная рекомендация или дополнительные сведения
Внимание!	Предупреждение о возможной проблеме
Ближе к реальности	Примеры реального приложения обсуждаемых вопросов и методик

Я искренне надеюсь, что в *Справочнике администратора Windows 7* вы оперативно и эффективно найдете все необходимое для выполнения основных административных функций на компьютерах под управлением этой ОС. Жду ваших комментариев по адресу *williamstanek@aol.com*. Спасибо.

Другие ресурсы

Дополнительные материалы к этой книге будут публиковаться на веб-сайте Microsoft Press Online Windows Server and Client. Там вы найдете обновления, статьи, ссылки на дополнительное содержимое, замеченные ошибки, примеры глав и др. Для доступа к этому сайту используйте адрес *http://microsoftpresssrv.libredigital.com/serverclient*. Эта книга также обсуждается по адресу *www.williamstanek.com*. Ищите меня на Twitter — WilliamStanek.

Поддержка

Мы приложили значительные усилия, чтобы сделать содержание этой книги максимально точным. Список поправок (если таковой имеется) вы найдете по адресу:
http:/www.microsoft.com/mspress/support
Если у вас возникнут вопросы или комментарии по поводу этой книги, обращайтесь в Microsoft Press по следующим адресам:

Обычная почта:
Microsoft Press
Attn: *Windows 7 Administrator's Pocket Consultant* Editor
One Microsoft Way
Redmond, WA 98052-6399

Электронная почта:
mspinput@microsoft.com
Имейте в виду, что эти адреса *не предназначены* для поддержки программных продуктов. За информацией о поддержке обращайтесь на веб-узел Майкрософт по адресу *http://www.microsoft.com/support*.

Глава 1

Администрирование Windows 7: первые шаги

Операционная система Windows 7, как и Windows Vista, существенно отличается от Windows XP и более ранних версий Windows. ОС Windows 7 не только более гибка, чем Windows XP, но и построена на революционной архитектуре, впервые использованной в Windows Vista. Наиболее значительные изменения в архитектуре таковы:

- управление учетными записями и повышение полномочий;
- модульность и образы дисков;
- предустановочная среда и предзагрузочная среда.

В этой главе рассматриваются основы Windows 7. Вы узнаете, насколько сильно повлияли на работу в ОС и на управление ею изменения в управляющих инструментах и полномочиях. Из главы 2 вы узнаете, как благодаря другим изменениям в архитектуре упростилось развертывание Windows 7. Во всех главах книги вы найдете подробное обсуждение изменений в управляемости, благодаря которым усовершенствованы все аспекты администрирования компьютера. Хотя эта книга посвящена именно администрированию Windows 7, описанные в ней методики будут полезны и тем, кто поддерживает эту ОС, работает в ней или разрабатывает для нее программы.

Предполагается, что наряду с этой книгой вы будете пользоваться книгой *Windows Server 2008 Administrator's Pocket Consultant*, Second Edition (Microsoft Press, 2010). Первое издание этого справочника переведено на русский язык: *Windows Server 2008 Справочник администратора* (Русская Редакция, БХВ-Петербург, 2009). В книгах серии «Справочник администратора», посвященных серверам, рассматриваются не только общие вопросы администрирования, но и администрирование службы каталогов, данных и сети. В этой книге, напротив, больше внимания уделяется администрированию системы и работы пользователей. Подробно рассматриваются следующие вопросы:

- настройка ОС и рабочей среды Windows;
- настройка оборудования и сетевых устройств;
- управление доступом пользователей и глобальными параметрами;

- настройка портативных компьютеров и мобильных устройств;
- удаленное управление и удаленная помощь;
- диагностика системных проблем.

Важно отметить, что практически всеми параметрами настройки ОС Windows можно управлять при помощи групповой политики. Я не буду в каждом разделе напоминать, что компонент А можно настраивать, только если это разрешено групповой политикой. Надеюсь, вы и сами разберетесь во влиянии групповой политики на настройку системы и управление ею. Я также буду считать, что вы знакомы с командной строкой и с Windows PowerShell. Это позволит мне сосредоточиться на главных административных задачах.

Знакомство с Windows 7

Windows 7 — последняя версия ОС Windows для клиентских компьютеров. Она доступна в следующих изданиях:

- **Windows 7 Starter** Экономичная версия Windows 7 для нетребовательных пользователей и развивающихся рынков. Она совместима с новейшими приложениями и устройствами, а также более надежна и защищена, чем прежние версии Windows. Однако возможности ее по сравнению с другими изданиями существенно ограничены.
- **Windows 7 Home Basic** Экономичная версия Windows 7 для домашних пользователей. Включает в себя основной набор развлекательных компонентов, но не предоставляет возможности присоединиться к домену.
- **Windows 7 Home Premium** Усовершенствованная версия Windows 7, включающая расширенный набор развлекательных компонентов, но не предоставляющая возможности присоединиться к домену.
- **Windows 7 Professional** Базовая версия Windows 7 для коммерческих пользователей. Включает базовый набор инструментов управления и допускает подключение к домену.
- **Windows 7 Enterprise** Усовершенствованная версия Windows 7 для коммерческих пользователей. Включает расширенный набор инструментов управления и допускает подключение к домену.
- **Windows 7 Ultimate** Усовершенствованная версия Windows 7, включающая все компоненты для домашних и коммерческих изданий, а также допускающая подключение к домену.

В Windows 7 поддерживаются установка и развертывание с использованием образов. Благодаря новой аппаратно-независимой архитектуре Windows 7, о которой мы поговорим чуть позже, все издания Windows 7, за исключением Windows 7 Starter, поддерживают как 32-разрядное, так и 64-разрядное оборудование. Иными словами, все версии этой ОС, кроме Starter, можно устанавливать и на 32-разрядные, и на 64-разрядные компьютеры. На компьютерах с 32-разрядной архитектурой x86 допускается использовать до 4 гигабайт (Гб) оперативной памяти. На компьютерах с 64-разрядной ар-

хитектурой допускается использовать до 8 Гб памяти в версии Home Basic, до 16 Гб памяти в Home Premium и более 128 Гб в версиях Professional, Enterprise и Ultimate. В трех последних версиях имеется также поддержка многопроцессорных систем.

Обзор различий между изданиями Windows 7 приводится в табл. 1-1. Подробный список отличий вы найдете также по адресу *www.williamstanek.com/windows7/*.

Табл. 1-1. Версии Windows 7

Компонент	Home Basic	Home Premium	Professional	Enterprise	Ultimate
Интерфейс Aero		X	X	X	X
Шифрование диска BitLocker				X	X
Полная архивная копия ПК			X	X	X
Средства развертывания			X	X	X
Поддержка многопроцессорности (не считая многоядерных процессоров)			X	X	X
Шифрующая файловая система			X	X	X
Общее использование файлов и принтеров	10	20	20	20	20
Клиент NAP			X	X	X
Центр сетевых подключений и общего доступа	X	X	X	X	X
Родительский контроль	X	X			X
Качество обслуживания для сетей на основе политики			X	X	X
Охвачена Premier Support			X	X	
Архивирование по расписанию	Ограничено	X	X	X	X

Табл. 1-1. (*окончание*)

Компонент	Home Basic	Home Premium	Professional	Enterprise	Ultimate
Входит в программу Microsoft Software Assurance			X	X	X
Подсистема для приложений UNIX				X	X
Планшетные ПК		X	X	X	X
Многоязычный пользовательский интерфейс				X	X
Ключи для корпоративного лицензирования			X	X	
Лицензии виртуальных машин (4)				X	X
Факс и сканирование Windows (Windows Fax and Scan)			X	X	X
Windows Media Center	X	X	X	X	X
Готовность к работе с беспроводными сетями			X	X	X

Windows XP и другие прежние версии ОС Windows нельзя было обновлять от одной версии до другой. В Windows 7 такое обновление допускается — с использованием Windows Anytime Upgrade или Deployment Image Servicing and Management. Возможные варианты обновления описаны в табл. 1-2. Как видите, в каждой версии есть несколько вариантов перехода от более простого издания к более сложному. Чтобы определить, какая версия Windows 7 установлена на вашем компьютере, щелкните кнопку **Пуск (Start)**, правой кнопкой щелкните элемент **Компьютер (Computer)** и выберите команду **Свойства (Properties)**. Издание Windows 7 будет указано в открывшемся окне.

Табл. 1-2. Варианты обновления изданий Windows 7

Версия Windows	Обновляется до	Обновляется до
Для домашних пользователей	Windows 7 Home Premium	Windows 7 Ultimate
Windows 7 Home Basic	Да	Да
Windows 7 Home Premium		Да

Табл. 1-2. (*окончание*)

Версия Windows	Обновляется до	Обновляется до
Для коммерческих пользователей	Windows 7 Enterprise	Windows 7 Ultimate
Windows 7 Professional	Да	Да
Windows 7 Enterprise		Да

Программа Windows Anytime Upgrade позволяет купить диск с обновлением в магазине, использовать для обновления встроенный компонент, введя соответствующий ключ продукта, или приобрести обновление через Интернет. Чтобы воспользоваться встроенным компонентом Windows Anytime Upgrade, щелкните кнопку **Пуск (Start)** и выберите команду **Панель управления (Control Panel)**. В окне панели управления щелкните категорию **Система и безопасность (System and Security)**, затем щелкните значок **Windows Anytime Upgrade** и следуйте инструкциям. Вам понадобится установочный носитель Windows 7. Он содержит двоичные файлы для всех версий Windows 7. Разблокирование и установка компонентов для конкретной версии определяется введенным ключом продукта.

Примечание 32-разрядные и 64-разрядные версии Windows 7 поставляются на разных носителях. Чтобы установить 32-разрядную версию Windows 7 на компьютере x86, используйте 32-разрядный дистрибутив. Чтобы установить 64-разрядную версию Windows 7 на компьютере x64, используйте 64-разрядный дистрибутив. Как правило, если вы работаете в 32-разрядной ОС и хотите установить 64-разрядную ОС (при условии, что оборудование компьютера это позволяет), вам нужно перезапустить компьютер и загрузиться с установочного диска. Примерно так же нужно действовать, если вы хотите установить 32-разрядную ОС на компьютер, работающий под управлением 64-разрядной ОС. Учтите, что для компьютеров с процессорами IA64 в Майкрософт разработана специальная версия Windows 7 — Windows 7 for Itanium-Based Systems.

С коммерческими версиями Windows 7 поставляется инструмент Deployment Image Servicing and Management (DISM). Он позволяет управлять оперативными и автономными образами ОС Windows, включая образы для развертывания и для виртуальных машин. Для развертывания Windows 7 применяются файлы Windows Image (.wim), для виртуальных машин — файлы виртуальных жестких дисков (.vhd). Для работы как с WIM-файлами, так и с VHD-файлами применяются одни и те же команды.

Как вы узнаете из главы 2, DISM применяется для решения следующих задач:

- добавление и удаление пакетов (языковых пакетов, исправлений, утилит и пр.);
- включение и выключение компонентов Windows;
- установка и удаление драйверов устройств от независимых разработчиков.

Чтобы запустить DISM в административной командной строке, выполните следующие действия:

1. Щелкните кнопку **Пуск (Start)**, раскройте меню **Все программы (All Programs)** и щелкните команду **Стандартные (Accessories)**.
2. Щелкните правой кнопкой команду **Командная строка (Command Prompt)** и выберите в контекстном меню **Запуск от имени администратора (Run As Administrator)**.

   Если на экране появится окно **Контроль учетных записей пользователей (User Account Control)**, действуйте так же, как при запуске любой программы с административными полномочиями.
3. В командной строке введите **dism /?**, чтобы просмотреть параметры DISM.
4. Чтобы просмотреть команды для работы с оперативными образами, введите **dism /online /?**.

Хотя утилита DISM предназначена в основном для работы с автономными образами и образами, к которым вы подключились, с ее помощью можно также получить много полезной информации о действующей ОС компьютера. Обзор подкоманд DISM Online для работы с действующей ОС приводится в табл. 1-3. Допустим, чтобы отобразить список версий Windows, до которых можно обновить ОС компьютера, введите команду:

```
dism /online /get-targeteditions
```

Табл. 1-3. Подкоманды DISM Online для работы с действующей ОС

Подкоманда	Описание
/Disable-Feature /featurename:*ИмяКомпонента*	Отключение заданного компонента. Имя компонента вводится с учетом регистра
/Enable-Feature /featurename:*ИмяКомпонента*	Включение заданного компонента. Имя компонента вводится с учетом регистра
/Get-CurrentEdition	Отображение установленной версии Windows
/Get-DriverInfo /driver: *ИмяДрайвера.inf*	Отображение информации о заданном драйвере независимого разработчика, установленном в хранилище драйверов. Имя драйвера вводится без учета регистра
/Get-Drivers	Отображение информации обо всех драйверах независимых разработчиков, установленных в хранилище драйверов
/Get-FeatureInfo /featurename:*ИмяКомпонента*	Отображение информации о заданном компоненте. Имя компонента вводится с учетом регистра
/Get-Features	Отображение информации об установленных компонентах Windows
/Get-Intl	Отображение информации о языке интерфейса системы по умолчанию, региональных данных, часовом поясе по умолчанию, раскладке клавиатуры и установленных языках

Табл. 1-3. (*окончание*)

Подкоманда	Описание
/Get-PackageInfo /packagename:*ИмяПакета*	Отображение информации о заданном пакете. Имя пакета вводится с учетом регистра
/Get-Packages	Отображение информации об установленных пакетах Windows
/Get-TargetEditions	Вывод списка изданий Windows, до которых можно обновить текущую ОС

В комплект поставки Windows 7 входит Windows PowerShell 2.0. Если вы настроили PowerShell на удаленную работу, в вашем распоряжении несколько способов выполнить команды на удаленном компьютере. Один из способов заключается в создании удаленного сеанса с нужным компьютером. Далее показан пример того, как можно выяснить, какая версия Windows установлена на удаленной системе:

```
$s = new-pssession -computername engpc15, hrpc32, cserpc28
invoke-command -session $s {dism.exe /online /get-currentedition}

Система DISM
Версия: 6.1.7350.0
Версия образа: 6.1.7350.0
Текущий выпуск : Ultimate
Операция успешно завершена.
```

Примечание В параметре –ComputerName команды New-PSSession указывается DNS-имя, NetBIOS-имя или IP-адрес удаленного компьютера, с которым вы собираетесь работать. Если вы предполагаете работать с несколькими компьютерами, вводите их имена или адреса через запятую. Подробнее о работе с Windows PowerShell 2.0, в том числе, в удаленном режиме, читайте в главе 4 книги *Windows PowerShell 2.0 Administrator's Pocket Consultant* (Microsoft Press, 2009) [*Windows PowerShell 2.0 Справочник администратора* (Русская Редакция, БХВ-Петербург, 2010)].

Знакомство с 64-разрядными системами

С момента первого появления в семействе ОС Windows 64-разрядные системы значительно изменились. Компьютеры под управлением 64-разрядных версий Windows не только работают быстрее и производительнее своих 32-разрядных собратьев. Они еще и более масштабируемы, поскольку способны обрабатывать больше данных за один тактовый цикл, адресовать больше памяти и быстрее справляться с численными расчетами. В Windows 7 поддерживаются две различных 64-разрядных архитектуры:

- **x64** Основана на 64-разрядном расширении набора инструкций x86, реализованном в процессорах AMD Opteron (AMD64), Intel Xeon с 64-разрядным расширением и др. В этой архитектуре поддерживается исходная 32-разрядная обработка и 64-разрядная расширенная обработ-

ка, что позволяет одновременно проводить как 32-разрядные, так и 64-разрядные расчеты.

- **IA64** Основана на архитектуре процессоров EPIC (Explicitly Parallel Instruction Computing), реализованной в процессорах Intel Itanium (IA64) и др. Эта архитектура является изначально 64-разрядной, что позволяет 64-разрядным приложениям работать с максимальной производительностью.

Работа с 64-разрядными архитектурами выгодна в тех случаях, когда для расчетов требуется много памяти, да и сами расчеты весьма ресурсоемки. В этом случае приложение может загрузить большой объем данных в физическую память (то есть в ОЗУ), что сокращает интенсивность страничного обмена и существенно повышает производительность. Набор инструкций EPIC позволяет процессорам на базе Itanium выполнять одновременно до 20 операций.

В настоящее время распространены следующие микропрограммные (firmware) интерфейсы:

- BIOS (Basic input/output system);
- EFI (Extensible Firmware Interface);
- UEFI (Unified Extensible Firmware Interface).

Компьютеры на базе Itanium фундаментально отличаются от компьютеров на базе x86 и x64. На компьютерах Itanium применяется интерфейс EFI и диски GPT (GUID partition table), тогда как на компьютерах x86 применяются BIOS и диски MBR (Master Boot Record). На компьютерах x64 применяется UEFI поверх BIOS или EFI (подробнее — в главе 10). Это означает, что управление компьютерами на этих архитектурах осуществляется по-разному, особенно в отношении настройки и конфигурирования дисков. Однако благодаря растущей популярности UEFI и способности Windows 7 работать как с MBR, так и с GPT-дисками независимо от типа микропрограммного интерфейса, использование на компьютере конкретного интерфейса и типа дисков уже необязательно определяется архитектурой процессора. Решение должен принимать производитель оборудования.

Примечание Работа с дисками MBR и GPT подробно описана в главе 12. Пока заметим кратко, что на компьютерах с BIOS диски MBR используются и для загрузки, и для хранения данных, а диски GPT — только для хранения данных. На компьютерах EFI могут применяться как GPT, так и MBR-диски, но вам необходим будет по крайней мере один GPT-диск для хранения системного раздела ESP (EFI system partition) и основной раздел или простой том для хранения загружаемой ОС.

В большинстве случаев 64-разрядное оборудование совместимо с 32-разрядными приложениями. Однако производительность 32-разрядных приложений выше на 32-разрядном оборудовании. В 64-разрядных версиях Windows благодаря уровню эмуляции Windows on Windows 64 (WOW64) x86 поддерживаются как 64-разрядные, так и 32-разрядные приложения. В подсистеме WOW64 происходит изоляция 32-разрядных приложений от

64-разрядных приложений. Это позволяет избежать проблем с файловой системой и реестром. Операционная система обеспечивает интероперабельность для модели объектов COM (Component Object Model) и для базовых операций с буфером обмена (вырезания, копирования и вставки). Однако 32-разрядные процессы неспособны загружать 64-разрядные библиотеки DLL, а 64-разрядные процессы не могут загружать 32-разрядные DLL.

В эпоху общего перехода на 64-разрядные системы полезно выяснить, какие компьютеры предприятия поддерживают использование 64-разрядных ОС, на каких компьютерах уже работают 64-разрядные ОС или и то, и другое. Windows PowerShell позволяет сделать следующее:

- Выяснить, установлена ли на компьютере 64-разрядная ОС, при помощи свойства OSArchitecture объекта Win32_OperatingSystem. Далее приведен пример:

```
get-wmiobject -class win32_operatingsystem | format-list osarchitecture

osarchitecture : 32-bit
```

- Выяснить, поддерживает ли компьютер 64-разрядные ОС, при помощи свойств Name и Description объекта Win32_Processor:

```
get-wmiobject -class win32_processor | format-list name, description

name        : Intel(R) Core(TM)2 Quad CPU           @ 2.66GHz
description : x64 Family 6 Model 15 Stepping 7
```

В результате работы программы в первом примере говорится, что компьютер работает под управлением 32-разрядной версии Windows. Из второго примера вы узнаете, что на компьютере работает процессор x64. Поэтому компьютер можно обновить до 64-разрядной версии Windows 7.

Чтобы не проверять каждый компьютер в отдельности, напишите сценарий, который выполнит эту проверку. Примеры сценариев вы найдете в главе 9 книги *Windows PowerShell 2.0 Administrator's Pocket Consultant (Windows PowerShell 2.0 Справочник администратора)*.

Установка Windows 7

В доменах Active Directory можно использовать только издания Windows 7 Professional, Enterprise и Ultimate. При установке Windows 7 на компьютер с существующей ОС вы вольны выбрать между чистой установкой и обновлением. Основные отличия между ними таковы:

- **Чистая установка** Программа установки Windows полностью заменяет ОС на компьютере. Все параметры пользователей и приложений теряются. Чистую установку следует использовать лишь в тех случаях, когда ОС нельзя обновить, когда на компьютере устанавливается несколько ОС, когда необходима установка в стандартизованной конфигурации или когда на компьютере не установлена никакая ОС.

- **Обновление** В ходе обновления сохраняются параметры пользователя, установленные приложения и их параметры, а также основные параметры системы. Установку с обновлением следует осуществлять, когда у вас есть компьютеры с версиями ОС Windows, допускающими обновление до Windows 7, и вы хотите свести к минимуму потери существующей конфигурации.

Конкретная процедура обновления зависит от того, какую именно ОС вы обновляете. Если вы обновляете Windows Vista, программа установки Windows ставит новую систему поверх старой. Имеется также возможность обновления с Windows XP, но здесь ставить одну ОС поверх другой уже не получится. При обновлении Windows XP вам нужно сначала при помощи Windows Easy Transfer перенести нужные файлы и параметры, а затем запустить Windows Setup. Программа установки Windows выполнит чистую установку ОС. Затем вам придется переустановить все приложения.

Подготовка к установке Windows 7

Чтобы установить Windows 7, загрузите компьютер с установочного носителя Windows, запустите программу Setup из текущей версии ОС Windows, выполните установку из командной строки или воспользуйтесь одним из вариантов автоматической установки.

Существует два основных подхода к установке Windows 7 — интерактивный и автоматический. Интерактивная установка — это та самая привычная установка Windows, к которой привыкло большинство пользователей, когда вы проходите процесс шаг за шагом, вводя много всяческой информации. Ее можно запускать с установочного носителя (загрузившись с него или запустив программу установки из командной строки). При загрузке с купленного DVD-диска Windows 7 по умолчанию запускается интерактивный процесс с заполнением полей во множестве диалоговых окон.

Автоматическая установка бывает нескольких видов. Объем информации, вводимой пользователем, задается администратором. При базовой автоматической установке взаимодействие с пользователем вообще не требуется; вся информация считывается из файлов ответов. Файл ответов (answer file) полностью или частично содержит информацию, которую вы при интерактивной установке вводили бы вручную. Чтобы создать файл ответов, воспользуйтесь диспетчером Windows System Image Manager, входящим в комплект Windows Deployment Toolkit (доступен по адресу *www.download.microsoft.com*). Чтобы несколько усложнить процесс автоматической установки, примените службы развертывания Windows (Windows Deployment Services), описанные в главе 2.

Стандартная программа установки Windows 7 называется Setup.exe. Ее можно запустить из текущей версии Windows, чтобы обновить ее или установить Windows 7 в другой раздел. На компьютерах с BIOS (x86) для начала процесса установки достаточно загрузиться с установочного носителя. На компьютерах с процессорами Itanium (IA64) программа Setup запускается

в оболочке EFI. Запустите с DVD-диска \IA64\Setupldr.efi Setup. Если не считать особенностей работы с разделами, программа Setup на системах IA64, на 32-разрядных системах x86 и на 64-разрядных системах x64 работает одинаково.

Работая с Windows 7 на системах x86, помните о том, что ОС использует несколько специальных дисковых разделов:

- **Активный (active)** Активный раздел, или том, применяется для хранения системного кеша и загрузочной информации. Активный раздел может размещаться на съемных носителях.
- **Загрузочный (boot)** На загрузочном разделе, или томе, содержатся операционная система и ее файлы. Может совпадать с системным разделом.
- **Системный (system)** На системном разделе, или томе, содержатся аппаратно-зависимые файлы, необходимые для загрузки ОС. Будучи одним из хранилищ конфигурации системы, системный раздел не может размещаться на томе с чередованием или на расширенном томе.

Раздел и том — по сути, одно и тоже, тем не менее, иногда между этими терминами все-таки проводят различие, поскольку разделы создаются на простых дисках, а тома — на динамических. Чтобы сделать диск активным на компьютере x86, воспользуйтесь оснасткой Управление дисками (Disk Management).

Хотя активный, системный и загрузочный тома (или разделы) могут совпадать, нужен, тем не менее, каждый из них. Когда вы устанавливаете Windows 7, программа Setup осуществляет доступ ко всем доступным дисковым ресурсам. Как правило, Windows 7 помещает загрузочные и системные файлы на одном и том же диске и на одном и том же разделе и помечает этот раздел как активный. Преимущество такой конфигурации состоит в том, что для установки ОС вам достаточно одного диска, поэтому остальные диски компьютера вы вольны использовать для хранения собственной информации или в качестве зеркала разделов ОС.

Установка ОС на платформу IA64 осуществляется с некоторыми важными отличиями. Интерфейс EFI в начале работы отображает микропрограммное загрузочное меню. Структуру разделов на дисках IA64 определяет таблица GPT, основанная на глобально-уникальных идентификаторах (globally unique identifier, GUID). Эта структура существенно отличается от структуры разделов на 32-разрядных платформах на базе MBR.

На дисках GPT есть два обязательных раздела и один или несколько необязательных (OEM или разделы данных) разделов (полным числом до 128):

- системный раздел EFI (ESP);
- раздел, зарезервированный Майкрософт (Microsoft reserved partition, MSR);
- по крайней мере, один раздел с данными.

В загрузочном меню IA64 имеется команда для вызова оболочки EFI. Эта оболочка предоставляет возможности для работы с файловыми системами FAT и FAT32, а также для управления файлами. Чтобы просмотреть список разделов на компьютере IA64, используйте команду Map. В ее выводе символами *blk* обозначены блоки разделов, а символами *fs#* — читаемые файловые системы. Чтобы перейти в конкретный раздел, введите соответствующий номер блока и запятую. Введите **dir**, чтобы просмотреть список файлов в разделе. В EFI имеется также диспетчер обслуживания загрузки (boot maintenance manager), позволяющий настроить загрузочное меню.

Как вы узнаете из главы 2, при установке Windows 7 программа Setup автоматически создает раздел среды восстановления Windows (Windows Recovery Environment, Windows RE) и устанавливает в этот раздел дополнительные компоненты для восстановления и диагностики. В результате в Windows 7 всегда доступны следующие инструменты:

- **Startup Repair** Устранение проблем, препятствующих загрузке Windows. Если загрузка не происходит из-за сбоя в диспетчере загрузки или в системном файле, инструмент запускается автоматически и инициирует восстановление компьютера.
- **System Restore** Восстановление Windows к состоянию в некоторый предшествующий момент времени. При наличии точек восстановления вы можете воспользоваться этим инструментом для устранения последствий неудачного изменения конфигурации или установки приложения.
- **System Image Recovery** Полное восстановление компьютера на основе ранее созданного образа системы. Этот инструмент применяется, если систему не удалось восстановить инструментами Startup Repair, System Restore и др., конечно, только при наличии образа системы.
- **Windows Memory Diagnostics** Диагностика памяти компьютера. Этот инструмент поможет вам найти причину неисправности, если компьютер не загружается или работает со сбоями из-за проблем с памятью.

Вы как администратор вольны использовать эти инструменты самостоятельно или проинструктировать об их использовании удаленного пользователя. Объясните ему, как запустить Windows RE и начать процесс восстановления. Для этого пользователю нужно открыть доступ к меню с дополнительными параметрами загрузки. Подробнее — в главе 17.

Выполнение установки Windows 7

Прежде чем приступать к установке Windows 7, выясните, отвечает ли его оборудование требованиям к памяти, мощности процессора и графическим возможностям. Как обычно, Майкрософт разделяет аппаратные требования на минимальные и рекомендуемые. Итак, для работы Windows 7 требуется, как минимум, следующее:

- процессор — 32-разрядный (x86) или 64-разрядный (x64) с тактовой частотой не менее 1 ГГц;

- оперативная память — не менее 1 Гб на 32-разрядном компьютере и не менее 2 Гб на 64-разрядном компьютере;
- графический процессор — не хуже DirectX 9 с драйвером WDDM 1.0 или лучшим.

Примечание Согласно рекомендациям Майкрософт, на компьютере необходимо предусмотреть свободное дисковое пространство не менее 16 Гб в 32-разрядной версии и 20 Гб в 64-разрядной версии. Требования к объему свободного пространства существенно возрастают при работе различных компонентов Windows 7, например точек защиты (protection point), в которые включаются предыдущие версии измененных файлов и папок. Чтобы обеспечить оптимальную производительность жесткого диска, следите за тем, чтобы на нем оставались свободными как минимум 15% его объема, а также имелось достаточно места для файла подкачки (как правило, в два раза больше объема оперативной памяти системы). Кроме того, если вы устанавливаете Windows 7 поверх старой версии, помните, что на диске в папке Windows.old будут сохранены файлы и папки этой версии.

ОС Windows 7 можно установить на любой компьютер, параметры которого соответствуют перечисленным требованиям или превосходят их. Для интерактивной установки Windows 7 необходимо выполнить следующие действия:

1. Запустите программу Windows 7 Setup одним из указанных ниже способов:
   - В случае новой установки включите компьютер и вставьте в DVD-ROM-дисковод установочный диск Windows 7. Когда появится приглашение, нажмите клавишу, чтобы запустить установку с DVD-диска.
   - В случае обновления запустите компьютер и войдите в систему, используя учетную запись с административными полномочиями. Вставьте установочный диск Windows 7 в DVD-ROM-дисковод. Программа Windows 7 Setup запустится автоматически. Если этого не произошло, перейдите на диск с помощью Проводника Windows (Windows Explorer) и дважды щелкните файл Setup.exe.
2. Щелкните кнопку **Установить (Install Now)**, чтобы запустить установку. Программа Setup скопирует временные файлы и начнет работу. Если вы запустили установку из действующей ОС и подключены к сети или Интернету, укажите, нужно ли в ходе установки загружать обновления: щелкните **Выполнить подключение к Интернету для получения последних обновлений программы установки (Go Online to Get the Latest Updates for Installation)** или **Не загружать последние обновления программы установки (Do not Get the Latest Updates for Installation)**.

Совет Загружать обновления во время установки необязательно. Это можно сделать позже, при помощи компонента Обновление Windows (Windows Update).

3. Прочитайте лицензионное соглашение. Если вы согласны с ним, щелкните **Я принимаю условия лицензии (I Accept the License Terms)** и **Далее (Next)**.

4. Укажите тип установки — **Обновление (Upgrade)** или **Полная установка (Дополнительные параметры) (Custom (Advanced))**. Первый вариант соответствует случаю, когда вы обновляете до Windows 7 существующую ОС. Чтобы установить Windows 7 «с нуля», выберите второй вариант.

Примечание При чистой установке Windows 7 на компьютер, где уже установлена одна из прежних версий Windows, программа Setup перемещает файлы и папки старой версии в папку Windows.old. Запустить прежнюю версию будет нельзя.

5. Когда вам будет предложено указать место для установки, выберите диск, на который нужно установить ОС, и щелкните **Далее (Next)**.

Совет На странице **Выберите раздел для установки Windows (Where Do You Want to Install Windows)** программы установки можно вызвать окно командной строки, нажав Shift+F10. После этого вы попадете в среду MinWinPC, которой программа Setup пользуется для установки ОС. В ней доступны многие стандартные инструменты командной строки Windows 7.

6. Если на выбранном вами диске установлена одна из предыдущих версий Windows, на экран будет выведена информация о том, что существующие параметры пользователей и приложений будут перемещены в папку Windows.old и что вам придется скопировать эти параметры в новую установку Windows. Щелкните **OK**.

   Программа Setup начнет установку. В ходе этого процесса она копирует образ Windows 7 на выбранный вами диск и распаковывает его. Затем на основе конфигурации компьютера и обнаруженных устройств производится установка компонентов, для чего требуется несколько перезагрузок. По окончании работы программы Setup загружается ОС, и ее нужно настроить для первого использования.
7. Выберите страну или регион, укажите формат времени и денежных сумм, а также раскладку клавиатуры. Щелкните **Далее (Next)**.
8. Создайте локальную учетную запись, которая будет использоваться в качестве учетной записи администратора компьютера. Введите имя пользователя.
9. Введите имя компьютера и щелкните **Далее (Next)**.
10. Введите и подтвердите пароль. Введите подсказку для напоминания пароля. Щелкните **Далее (Next)**.

Совет Старайтесь делать пароли учетных записей достаточно сложными. Используйте сочетание всех доступных типов символов, включая буквы верхнего и нижнего регистров, цифры и знаки.

11. Если вы приобрели розничную версию Windows 7, вам нужно будет ввести ключ продукта. По умолчанию ОС Windows будет автоматически активирована при очередном подключении к Интернету. Щелкните **Далее (Next)**.
12. Задайте параметры обновления Windows. Как правило, следует сохранить рекомендуемый вариант, при котором Windows 7 автоматически устанавливает все доступные обновления и инструменты безопасности

по мере их появления. Если вы выберете вариант **Отложить решение (Ask Me Later)**, обновление Windows будет отключено.

13. Просмотрите параметры даты и времени и при необходимости измените их. Щелкните **Далее (Next)**.
14. Если в процессе установки была обнаружена сетевая плата, будут автоматически установлены сетевые компоненты. Выберите вариант **Домашняя сеть (Home)**, **Сеть предприятия (Work)** или **Общественная сеть (Public Network)**. Windows 7 настроит сеть для выбранного варианта. Затем Windows 7 подготовит рабочий стол.

Есть несколько причин, по которым установка Windows 7 может застопориться. Далее описаны варианты решения нескольких типичных проблем.

- **Не удается загрузиться с установочного диска Windows 7** Хотя у большинства компьютеров есть возможность загрузки с DVD-диска, иногда она бывает отключена. Задайте в BIOS нужный порядок загрузки, чтобы DVD стоял в списке загрузки перед жестким диском и другими загрузочными устройствами. Подробнее — в главе 10.
- **Во время установки не удается выбрать жесткий диск** Хотя на установочном диске Windows 7 есть драйверы для большинства дисковых контроллеров, не исключено, что для вашего контроллера драйвера в этом комплекте не окажется. Вставьте диск с нужными драйверами и щелкните **Загрузка (Load Drivers)** на странице **Выберите раздел для установки Windows (Where Do You Want To Install Windows)**. Если драйвер находится на внешнем жестком диске, нажмите Shift+F10, чтобы открыть командную строку, и воспользуйтесь командой Xcopy, чтобы скопировать файлы драйвера на USB-накопитель или другой съемный носитель. Затем щелкните **Загрузка (Load Drivers)**, чтобы загрузить драйверы с этого носителя.
- **Вы забыли изменить конфигурацию жесткого диска перед началом установки** На странице **Выберите раздел для установки Windows (Where Do You Want To Install Windows)** щелкните вариант **Настройка диска (Drive Options (Advanced)**). Затем воспользуйтесь командами для создания, удаления и форматирования разделов. Если вам нужно сжать или расширить раздел (даже при установке-обновлении), нажмите Shift+F10, чтобы открыть командную строку, а затем используйте команду Disk Part для работы с разделами. Расширить или сжать раздел можно, не удаляя его. Кроме того, командой Disk Part можно воспользоваться для изменения типа диска и раздела. Подробнее — в главах 10, 11 и 12 книги «*Windows Command-Line Administrator's Pocket Consultant*» (Microsoft Press, 2008) [*Командная строка Windows Vista и Windows Server 2008 Справочник администратора* (Русская Редакция, БХВ-Петербург, 2009)].

Работа в Windows 7

Когда ОС установлена, вы можете входить в систему и работать с рабочим столом. По умолчанию Windows 7 хранит данные профиля пользователя

в папке %SystemDrive%\Users\%UserName%. В персональной папке пользователя имеются следующие подпапки, по умолчанию применяемые в качестве места для хранения данных и файлов определенных типов:

- **AppData** Настройки приложений для конкретного пользователя (в скрытой папке).
- **Контакты (Contacts)** Контакты и группы контактов.
- **Рабочий стол (Desktop)** Рабочий стол пользователя.
- **Загрузки (Downloads)** Программы и данные, загруженные из Интернета.
- **Избранное (Favorites)** Избранные ссылки Интернета.
- **Ссылки (Links)** Наиболее нужные пользователю ссылки.
- **Мои документы (My Documents)** Файлы документов пользователя.
- **Моя музыка (My Music)** Музыкальные файлы пользователя.
- **Изображения (My Pictures)** Пользовательские файлы с изображениями.
- **Мои видеозаписи (My Videos)** Пользовательские видеофайлы.
- **Сохраненные игры (Saved Games)** Сохраненные данные игр.
- **Поиски (Searches)** Сохраненные данные поиска.

Примечание Символами %SystemDrive% и %UserName% обозначены переменные среды *SystemDrive* и *UserName*, соответственно. В ОС Windows имеется множество переменных среды, которые применяются для хранения значений параметров, специфических для данного пользователя и системы. Я буду часто указывать переменные среды, используя такой синтаксис — %VariableName%. Если вы произвели обновление прежней версии Windows до Windows 7, в личной папке пользователя будут также содержаться символические ссылки (они выглядят как ярлыки) на папки и параметры, применявшиеся в прежней версии. Символическая ссылка (symbolic link) — это указатель на файл или папку, который часто создается для обеспечения обратной совместимости с приложениями на случай, если они будут искать в конкретном расположении папку или файл, которые были перемещены. Для создания символических ссылок применяется утилита командной строки Mklink. Введите в командной строке **mklink /?**, чтобы узнать о ней подробнее.

Помимо персональных папок в Windows 7 используются персональные библиотеки. Библиотека (library) — это просто собрание папок и файлов, которые сгруппированы друг с другом и отображаются в общем представлении. К стандартным библиотекам относятся:

- **Документы (Documents)** Данные из папки Мои документы (My Documents) пользователя и папки Общие документы (Public Documents).
- **Музыка (Music)** Данные из папки Моя музыка (My Music) пользователя и папки Общая музыка (Public Music).
- **Изображения (Pictures)** Данные из папки Изображения (My Pictures) пользователя и папки Общие изображения (Public Pictures).
- **Видео (Videos)** Данные из папки Мои видеозаписи (My Videos) пользователя и папки Общие видео (Public Videos).

Чтобы создать новую библиотеку, в проводнике Windows щелкните правой кнопкой узел **Библиотеки (Libraries)**, раскройте подменю **Создать (New)** и выберите команду **Библиотека (Library)**.

Внимание! При работе с библиотеками важно понимать, что это лишь представления для собранных в них данных. Сами по себе библиотеки никаких данных не содержат, и любое действие, которое вы применяете к элементу библиотеки, в реальности будет применено к исходному файлу или папке.

Для настройки внешнего вида меню, окон и рабочего стола в Windows 7 применяются темы (theme). Чтобы выбрать тему, щелкните кнопку **Пуск (Start)** и выберите команду **Панель управления (Control Panel)**. В панели управления щелкните ссылку **Изменение темы (Change The Theme)** из раздела **Оформление и персонализация (Appearance and Personalization)** и выберите нужную тему. Тема Windows Aero улучшит визуальное отображение интерфейса и сделает его более динамичным. Если вас устроит более скромный дизайн, выберите тему Классическая (Windows Classic) или Windows 7 — упрощенный стиль (Windows 7 Basic).

Важно помнить, что усовершенствования интерфейса, доступные на данном компьютере, зависят от установленного издания Windows 7 и от оборудования компьютера.

Работа с Центром поддержки (Action Center) и активация Windows

Рабочий стол Windows 7 переработан и наделен новыми возможностями настройки. По умолчанию при первом входе в систему в области уведомлений отображается значок **Центр поддержки (Action Center)**. Центр поддержки (Action Center) — это консоль, контролирующая состояние важных аспектов безопасности и обслуживания. Когда состояние одной из областей мониторинга изменяется, Центр поддержки (Action Center) меняет значок в области уведомлений соответственно серьезности проблемы. Чтобы просмотреть все оповещения, поместите указатель мыши над значком. Если вы щелкнете его, Windows отобразит диалоговое окно со списком всех оповещений и действий, которые требуют вашего внимания. Щелкните соответствующую ссылку, чтобы отобразить возможное решение проблемы в веббраузере по умолчанию. Щелкнув ссылку **Открыть центр поддержки (Open Action Center)**, вы запустите консоль.

Если вы отключили отображение уведомлений Центра поддержки (Action Center) на панели задач, для его запуска выполните следующие действия:

1. Щелкните кнопку **Пуск (Start)** и выберите команду **Панель управления (Control Panel)**.
2. В окне панели управления щелкните заголовок категории **Система и безопасность (System And Security)**.
3. Щелкните **Центр поддержки (Action Center)**.

В окне **Центр поддержки (Action Center)**, показанном на рис. 1-1, приводится обзор состояния компьютера, а также сообщается о любых проблемах, ко-

торые ждут своего разрешения. Допустим, на компьютере настроены не вполне безопасные параметры обновления. Щелкните кнопку **Изменить параметры (Change Settings)**, чтобы отобразить окно с командами настройки (рис. 1-2). Сообщения о некоторых проблемах можно сохранить в архиве. Установите флажок **Архивировать это сообщение (Archive This Message)**, прежде чем щелкнете **OK**, чтобы закрыть страницу с информацией о проблеме.

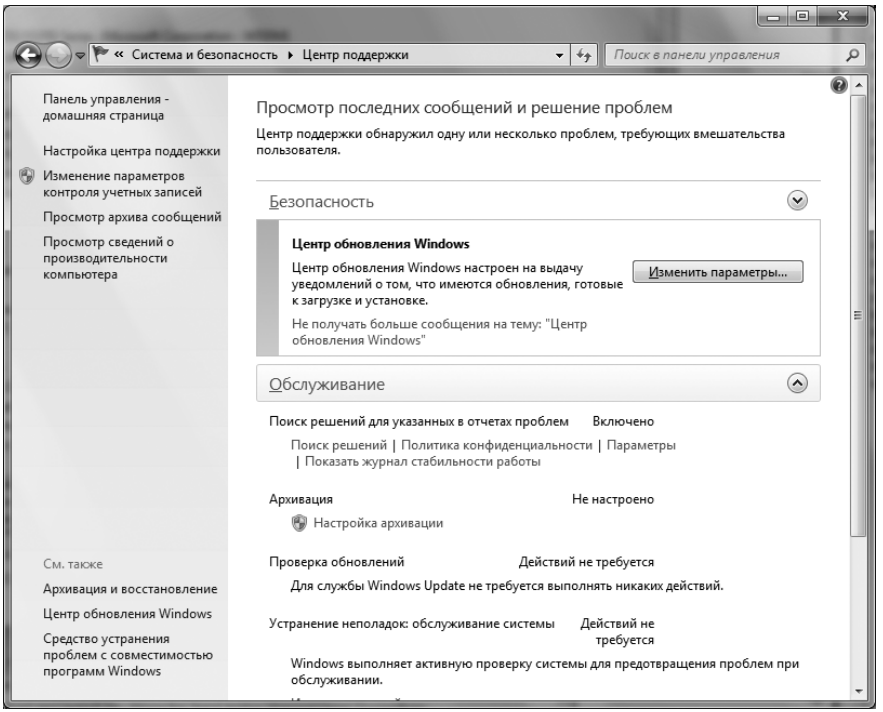

Рис. 1-1. Окно Центра поддержки (Action Center)

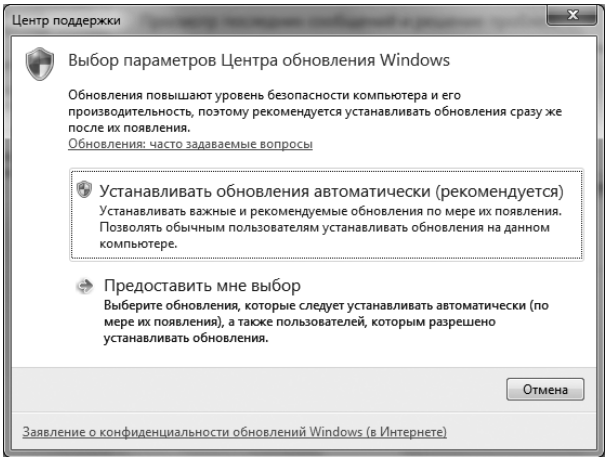

Рис. 1-2. Измените параметры системы, чтобы устранить сбой

Левая панель Центра поддержки (Action Center) позволяет выполнить следующие действия:

- **Настройка центра поддержки (Change Action Center Settings)** Щелкнув эту команду, вы сможете включить или отключить сообщения (alert message). Они делятся на две категории: сообщения о безопасности и сообщения о обслуживания. Сообщения о безопасности относятся к системе обновления Windows, параметрам безопасности Интернета, брандмауэру, управлению учетными записями (User Account Control, UAC), антишпионским, антивирусным и другим подобным программам. Сообщения об обслуживания относятся к системе резервного копирования, проверке обновлений и диагностике Windows. Также вы получите доступ к ссылкам для настройки параметров программы Customer Experience Improvement Program, отправки отчетов и обновления Windows.
- **Изменения параметров контроля учетных записей (Change User Account Control Settings)** Щелкнув эту команду, вы сможете настроить параметры управления учетными записями (User Account Control). Установите бегунок в положение **Всегда уведомлять (Always Notify)**, чтобы текущий пользователь получал уведомления обо всех устанавливаемых программах и попытках изменения параметров компьютера и Windows. Если вы установите переключатель в положение **По умолчанию (Default)**, система будет сообщать текущему пользователю только о попытках программ изменить что-либо на компьютере. Уведомления о редактировании параметров Windows пользователем отображаться не будут. Положение **Уведомлять только … (не затемнять рабочий стол) (Notify Me Only When … (Do Not Dim My Desktop))** аналогично положению **По умолчанию (Default)**, но не дает системе управления учетными записями переключиться на безопасный рабочий стол. Установите переключатель в положение **Никогда не уведомлять (Never Notify)**, чтобы полностью отключить уведомления системы управления учетными записями. Подробнее — в главе 5.
- **Просмотр архива сообщений (View Archived Messages)** Отображает архивированные сообщения Центра поддержки (Action Center) о проблемах на компьютере.
- **Просмотр сведений о производительности компьютера (View Performance Information)** Щелкнув эту команду, вы узнаете показатель производительности компьютера и определите, имеются ли у вас какие-либо проблемы, связанные с производительностью. Базовый показатель компьютера определяется по наименее производительному компоненту. Допустим, на компьютере установлен основной жесткий диск с низкой скоростью передачи данных. Показатель компьютера в этой области будет невысок, что отразится и на базовом показателе. Чтобы повысить производительность, вы должны будете заменить основной жесткий диск. Если вам кажется, что показатель производительности неточен, щелкни-

те ссылку **Повторить оценку (Re-Run the Assessment)**, чтобы Windows повторно оценила работу компьютера.

В изданиях Windows 7 Professional и Windows 7 Enterprise поддерживается корпоративное лицензирование. В отличие от корпоративных версий Windows 7, в розничной версии вам понадобятся как ключ продукта, так и активация. Чтобы выяснить, активирована ли уже Windows 7, щелкните кнопку **Пуск (Start)** и выберите команду **Панель управления (Control Panel)**. В панели управления выберите категорию **Система и безопасность (System And Security)** и щелкните ссылку **Система (System)**. На странице **Система (System)** просмотрите содержимое раздела **Активация Windows (Windows Activation)**: в нем как раз и написано, была ли уже проведена активация. Если Windows 7 не активирована и вы подключены к Интернету, щелкните параметр **Активировать Windows (Activate Windows Now)** в разделе **Активация Windows (Windows Activation)**, чтобы запустить мастер активации Windows.

В отличие от Windows XP и более старых версий Windows, ключ продукта, введенный при установке Windows 7, затем можно изменить согласно требованиям вашего плана лицензирования. Чтобы изменить ключ продукта, выполните следующие действия:

1. Щелкните кнопку **Пуск (Start)** и выберите команду **Панель управления (Control Panel)**. Перейдите в категорию **Система и безопасность (System And Security)** и щелкните **Система (System)**.
2. В разделе **Активация Windows (Windows Activation)** окна **Система (System)** щелкните **Изменить ключ продукта (Change Product Key)**.
3. В окне **Активация Windows (Windows Activation)** введите ключ продукта и щелкните **Далее (Next)**.
4. Если ключ продукта принят системой, вам придется повторно активировать Windows, щелкнув **Активировать Windows (Activate Windows Online Now)**. Если ключ не принят системой или предназначен для другого издания Windows 7, прежде чем активировать Windows, вам нужно будет ввести правильный ключ.

Работа с Windows 7 в группах и доменах

Компьютеры, работающие под управлением Windows 7, могут быть членами домашней группы (homegroup), рабочей группы (workgroup) или домена (domain). Домашняя группа — это объединение слабо связанных компьютеров домашней сети. Совместное использование данных в домашней группе обеспечивается при помощи пароля, общего для всех пользователей группы. Пароль домашней группы задается в момент ее создания и при необходимости позже может быть изменен.

Рабочая группа — это объединение слабо связанных компьютеров, каждый из которых управляется отдельно. Домен — это объединение компьютеров, которые управляются коллективно при помощи контроллеров домена,

серверов под управлением Windows, которые организуют доступ к сетевым ресурсам и базе данных каталога.

Домашняя группа доступна лишь при условии, что компьютер Windows 7 подключен к домашней сети. Доступ к рабочим группам и доменам открывается только при подключении компьютера к сети на рабочем месте. Подробнее об управлении сетями и сетевыми подключениями написано в главе 15. Чтобы изменить тип сети, к которой компьютер подключен в данный момент, выполните следующие действия:

1. Щелкните значок **Сеть (Network)** в области уведомлений, а затем щелкните ссылку **Центр управления сетями и общим доступом (Open Network And Sharing Center)**. Если значок сети не отображается, щелкните кнопку **Пуск (Start)** и выберите команду **Панель управления (Control Panel)**. В панели управления перейдите в категорию **Сеть и Интернет (Network And Internet)** и щелкните **Центр управления сетями и общим доступом (Network And Sharing Center)**.
2. В разделе **Просмотр активных сетей (View Your Active Networks)** щелкните ссылку **Сеть предприятия (Work Network)**, **Домашняя сеть (Home Network)** или **Общественная сеть (Public Network)**.
3. В диалоговом окне **Настройка сетевого размещения (Set Network Location)** выберите вариант **Сеть предприятия (Work Network)**, **Домашняя сеть (Home Network)** или **Общественная сеть (Public Network)** и щелкните **Закрыть (Close)**.

От того, в какой сети находится компьютер (домашней группе, рабочей группе или домене) зависят некоторые аспекты работы Windows 7. Далее подробно обсуждаются различия, связанные с управлением учетными записями, входом в систему, быстрой сменой пользователей и управлением паролями.

Управление учетными записями в Windows 7

В домашней или рабочей группе на компьютере Windows 7 имеются только локальные учетные записи. В домене на компьютере Windows 7 есть как локальные, так и доменные учетные записи. Локальные учетные записи в Windows 7 бывают двух основных типов:

- **Стандартная (standard)** Пользователю со стандартной учетной записью разрешено запускать большинство программ и изменять параметры системы, которые не затрагивают других пользователей или безопасность компьютера.
- **Административная (Administrator)** Администратор имеет полный доступ к компьютеру и может вносить в его конфигурацию любые изменения.

Управление учетными записями в Windows 7 преследует цель подлинного разделения полномочий между учетными записями администратора и обычного пользователя, что существенно повышает безопасность ком-

пьютера. Действие функции UAC в Windows 7 выражается в том, что все приложения выполняются либо от имени обычного пользователя, либо от имени администратора. Когда вы запустите приложение, требующее административных полномочий, система безопасности выдаст запрос, даже если вы вошли в систему в качестве администратора. Действия, доступные в окне запроса, зависят от настроек групповой политики (подробнее — в главе 5) и от полномочий учетной записи, с которой вы вошли в систему.

Если вы зарегистрировались как обычный пользователь, вам будет предложено ввести пароль администратора (рис. 1-3). В домашней или рабочей группе в окне будут перечислены имена всех локальных администраторов. Чтобы продолжить работу, выберите учетную запись, введите ее пароль и щелкните **Передать (Submit)**.

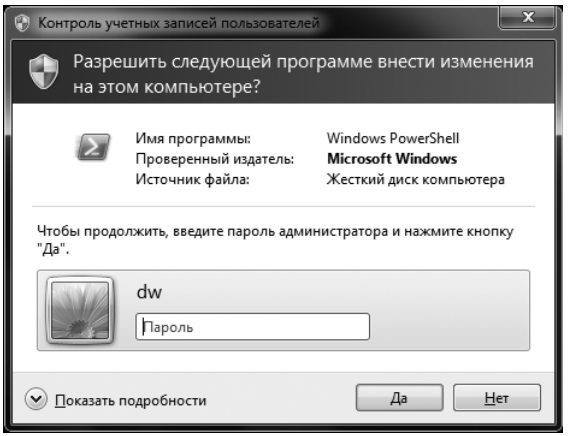

Рис. 1-3. Запрос административных полномочий

В домене окно **Контроль учетных записей пользователей (User Account Control)** не содержит списка административных учетных записей. Чтобы продолжить работу, вы должны знать не только пароль, но и имя учетной записи администратора домена по умолчанию (в котором вы зарегистрировались) или доверенного домена. Введите имя учетной записи и пароль, а затем щелкните **OK**. Если учетная запись относится к домену по умолчанию, указывать его имя не нужно. Если же учетная запись принадлежит другому домену, вы должны будете указать его в учетной записи, используя формат *домен\имя_пользователя*, например crandl\williams.

Если вы зашли в систему в качестве администратора, система предложит вам подтвердить продолжение выполнения (рис. 1-4). Щелкните **Да (Yes)**, чтобы выполнить действие, или **Нет (No)**, чтобы остановить его выполнение. Щелкните команду **Показать подробности (Show Details)**, чтобы отобразить полный путь выполняемой программы.

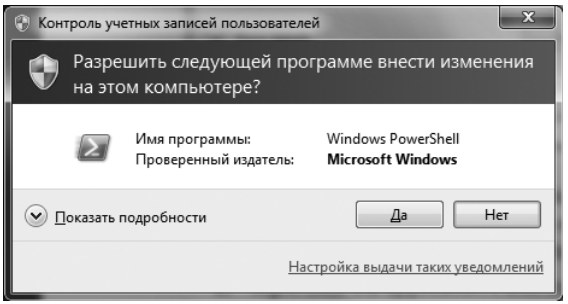

Рис. 1-4. Запрос на продолжение действия

В этом же контексте важно еще одно изменение, связанное с повышением полномочий (elevation of privileges). Оно позволяет наделить административными правами обычное пользовательское приложение. Чтобы запустить приложение с повышенными полномочиями, выполните следующие действия:

1. Щелкните правой кнопкой ярлык приложения в меню или на рабочем столе и выберите команду **Запуск от имени администратора (Run As Administrator)**.
2. В окне **Контроль учетных записей пользователей (User Account Control)** выполните обычные действия, необходимые для работы от имени администратора.

Примечание Чтобы запускать административные утилиты из командной строки, вы должны запустить окно командной строки с повышенными полномочиями. Если этого не сделать, попытка выполнения команды, требующей административных полномочий, приведет к ошибке.

Вход в Windows 7

В рабочей группе при запуске Windows 7 отображает экран входа в систему. На нем перечислены все стандартные и административные учетные записи, созданные на компьютере. Чтобы войти в систему, щелкните имя нужной учетной записи. Если запись защищена паролем, щелкните ее имя, введите пароль и щелкните значок со стрелкой.

В домене после инициализации системы Windows 7 отображает пустой экран. Чтобы отобразить экран входа в систему, вы должны нажать Ctrl+Alt+Del. По умолчанию в окне указана последняя учетная запись, которая была использована для входа на компьютер — в формате *компьютер\имя_пользователя* или *домен\имя_пользователя*. Чтобы войти в систему от имени этой же учетной записи, достаточно ввести ее пароль и щелкнуть кнопку со стрелкой. Чтобы войти от имени другой учетной записи, щелкните кнопку **Сменить пользователя (Switch User)**, нажмите Ctrl+Alt+Del и щелкните **Другой пользователь (Other User)**. Информация, которую вы должны ввести для входа в систему, зависит от типа используемой учетной записи.

- Если учетная запись принадлежит домену по умолчанию, введите имя пользователя и пароль, а затем щелкните кнопку со стрелкой.
- Если учетная запись принадлежит другому домену, вы должны указать имя учетной записи в формате *домен\имя_пользователя*, например cpandl\williams.
- Если вы хотите войти на локальный компьютер, введите ***.\имя_пользователя***, где *имя_пользователя* — имя локальной учетной записи, например .\williams.

Быстрая смена пользователей в Windows 7

В Windows 7 быстрая смена пользователей поддерживается и в домене, и в домашней группе, и в рабочей группе. После того как один пользователь зарегистрировался в Windows 7, в систему может войти и другой пользователь; первому пользователю при этом выходить из системы не нужно.

Чтобы сменить пользователя, нажмите Ctrl+Alt+Del и щелкните кнопку **Сменить пользователя (Switch User)**. На компьютере из состава рабочей группы отобразится экран входа в систему. В домене на экране появится диалоговое окно с сообщением **Нажмите Ctrl+Alt+Del, чтобы войти в систему (Press Ctrl+Alt+Del To Log On)**, после чего вам нужно будет снова нажать Ctrl+Alt+Del.

Управление паролями учетных записей в Windows 7

В отличие от Windows XP и прежних версий Windows, в Windows 7 предусмотрено простое и быстрое управление паролями учетных записей. Доступны следующие действия:

- изменение пароля текущего пользователя;
- изменения пароля локальной учетной записи для локального компьютера или другого домена;
- создание диска сброса пароля;
- сброс пароля пользователя.

Эти действия подробно описаны далее.

Изменение пароля текущего пользователя

Чтобы изменить пароль текущего пользователя, выполните следующие действия:

1. Нажмите Ctrl+Alt+Del и щелкните **Сменить пароль (Change A Password)**.

Примечание В домене имя текущего пользователя указывается в формате *домен\имя_пользователя*. В домашней или рабочей группе указывается только имя учетной записи текущего пользователя.

2. Введите в поле **Старый пароль (Old Password)** действующий пароль учетной записи.

3. Введите новый пароль учетной записи в поле **Новый пароль (New Password)** и еще раз введите его в поле **Подтверждение (Confirm Password)**.
4. Щелкните кнопку со стрелкой, чтобы подтвердить изменение.

Изменение пароля другой учетной записи

Чтобы изменить пароль доменной или локальной учетной записи другого пользователя (не текущего), выполните следующие действия:

1. Нажмите Ctrl+Alt+Del и щелкните **Сменить пароль (Change A Password)**.
2. Щелкните поле **Имя пользователя (User Name)** и введите имя учетной записи.

Примечание В домене имя пользователя указывается в формате *домен\имя_пользователя*, например cpandl\williams. Чтобы указать локальную учетную запись, введите ***.\имя_пользователя***, где *имя_пользователя* — имя локальной учетной записи, например .\williams.

3. Введите в поле **Старый пароль (Old Password)** действующий пароль учетной записи.
4. Введите новый пароль учетной записи в поле **Новый пароль (New Password)** и еще раз введите его в поле **Подтверждение (Confirm Password)**.
5. Щелкните кнопку со стрелкой, чтобы подтвердить изменение.

Создание и применение диска сброса пароля

Управление паролями доменных и локальных учетных записей осуществляется по-разному. В доменах паролями учетных записей ведают администраторы. В этом случае сброс пароля выполняется при помощи консоли Active Directory — пользователи и компьютеры (Active Directory Users and Computers).

В домашней или рабочей группе пароли локальных учетных записей можно сохранить в защищенном зашифрованном файле на диске сброса пароля (password reset disk), в качестве которого может применяться либо дискета, либо «флешка». Чтобы создать диск сброса пароля текущего пользователя, выполните следующие действия:

1. Нажмите Ctrl+Alt+Del, а затем щелкните **Сменить пароль (Change A Password)**.
2. Щелкните **Создать дискету для восстановления пароля (Create A Password Reset Disk)**, чтобы запустить Мастер забытых паролей (Forgotten Password Wizard).
3. Прочитайте сообщение на вводной странице и щелкните **Далее (Next)**. В качестве диска сброса пароля можно использовать дискету или USB-накопитель. В первом случае вставьте в дисковод A: пустую отформатированную дискету и выберите в списке дисков вариант **Дисковод (A:)**

(Floppy Disk Drive (A:)). Во втором случае выберите в списке нужный съемный диск. Щелкните **Далее (Next)**.

4. Введите в соответствующее поле действующий пароль текущего пользователя и щелкните **Далее (Next)**.
5. Когда мастер закончит создание диска, щелкните **Далее (Next)**, извлеките диск и щелкните **Готово (Finish)**.

Если пользователь забыл пароль и не может войти в систему, дискета сброса пароля позволит задать для него новый пароль. Надежно спрячьте дискету сброса пароля, поскольку любой ее обладатель получит беспрепятственный доступ к данным пользователя.

Ближе к реальности Для защиты и шифрования флеш-накопителей и других съемных накопителей можно использовать технологию BitLocker To Go. Когда пользователь вошел в систему, для разблокирования защищенного носителя применяется пароль или смарт-карта с PIN-кодом. Однако если пользователю не удается войти в систему, доступа к защищенному диску он не получит. Поэтому не применяйте защиту BitLocker To Go к дискам сброса пароля. Подробнее — в главе 11.

Сброс пароля пользователя

Чтобы сбросить пароль, выполните следующие действия:

1. На экране входа в систему, не вводя пароль, щелкните кнопку со стрелкой и затем **ОК**. На экране должна появиться команда **Восстановить пароль (Reset Password)**. Она также отображается при вводе неправильного пароля.
2. Вставьте дискету или USB-накопитель с файлом восстановления пароля и щелкните **Восстановить пароль (Reset Password)**, чтобы запустить Мастер сброса пароля (Reset Password).
3. Прочитайте вводное окно мастера и щелкните **Далее (Next)**.
4. Выберите в списке нужное устройство и щелкните **Далее (Next)**.
5. Введите и подтвердите новый пароль пользователя.
6. Введите подсказку пароля и щелкните **Далее (Next)**. Щелкните **Готово (Finish)**.

Планы энергосбережения, «спящие» режимы и выключение

В Windows 7 изменены параметры управления электропитанием. По умолчанию на компьютерах Windows 7 используется план Сбалансированный (Balanced), в котором при отсутствии действий пользователя в течение заданного периода времени отключается дисплей, а компьютер переводится в «спящий» режим.

При переходе в «спящее» состояние ОС автоматически сохраняет всю работу, отключает дисплей и переводит компьютер в «спящий» режим, то есть в режим с пониженным энергопотреблением. Информация о состоянии хранится в памяти компьютера, вентиляторы и жесткие диски выключаются. Поскольку Windows 7 перед переходом в «спящий» режим сохраняет состояние компьютера, вам не нужно выходить из программ.

Совет В мобильных компьютерах «спящий» режим работает с некоторыми особенностями. Часто компьютер настроен так, что он переходит в «спящий» режим при закрытии крышки и «просыпается», когда вы открываете крышку. Если заряд батареи заканчивается, пока ноутбук находится в «спящем» режиме, состояние компьютера сохраняется на жестком диске, после чего он полностью выключается. Это финальное состояние похоже на гибернацию, применяемую в Windows XP.

Чтобы просмотреть или изменить параметры питания по умолчанию, щелкните кнопку **Пуск (Start)** и выберите команду **Панель управления (Control Panel)**. В панели управления перейдите в категорию **Система и безопасность (System And Security)**. В разделе **Электропитание (Power Options)** щелкните вариант **Настройка перехода в спящий режим (Change When The Computer Sleeps)**. Задайте время, по истечении которого при использовании данного плана энергосбережения должен отключаться монитор, а компьютер должен переходить в «спящее» состояние (рис. 1-5). Затем щелкните **Сохранить изменения (Save Changes)**.

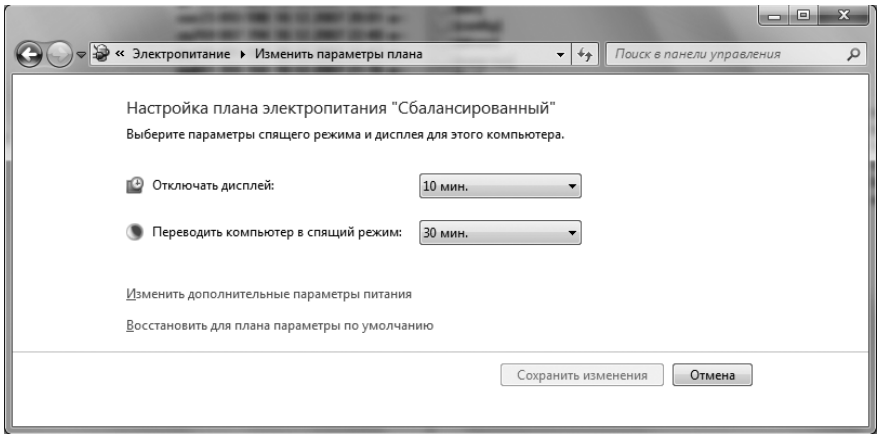

Рис. 1-5. Настройка параметров энергосбережения

На большинстве компьютеров для входа в спящее состояние нужно щелкнуть кнопку **Пуск (Start)**, затем щелкнуть переключатель **Завершение работы (Shutdown)** и выбрать **Сон (Sleep)**. Чтобы вывести компьютер из спящего состояния, передвиньте мышку или нажмите любую клавишу на клавиатуре. Обратите внимания, что у некоторых компьютеров на корпусе имеются отдельные кнопки для выключения и для перехода в спящее состояние. Способ работы этих кнопок можно задать при помощи параметров плана энергосбережения.

На некоторых компьютерах использовать спящее состояние нельзя. Иногда такое состояние не поддерживается оборудованием. Переход в спящее состояние также невозможен, если вы установили программы или обновления, требующие перезагрузки компьютера. Кроме того, помните, что администратор мог перенастроить кнопки включения и перехода в спящий режим так, чтобы при их нажатии выполнялись другие действия.

Внимание! Помните, что и в спящем состоянии компьютеру все равно требуется питание. При этом в компьютер нельзя устанавливать новое оборудование или подключать к нему новые устройства. Чтобы избежать путаницы, перед установкой нового оборудования на компьютер с Windows 7 обязательно физически отключайте его от электричества. Исключением являются внешние устройства, подключаемые через порты USB, IEEE 1394 (FireWire) или eSATA. Для их подключения выключать компьютер необязательно.

Чтобы изменить действие кнопки включения питания, щелкните кнопку **Пуск (Start)** и откройте панель управления. Раскройте категорию **Система и безопасность (System And Security)** и щелкните ссылку **Настройка функций кнопок питания (Choose What The Power Buttons Do)** в группе **Электропитание (Power Options)**. Как показано на рис. 1-6, далее вы сможете задать действие, выполняемое при нажатии кнопки включения питания и кнопки перехода в спящий режим. При необходимости щелкните ссылку **Изменение недоступных в данный момент параметров (Change Settings that are Currently Unavailable)** и установите переключатель **Запрашивать пароль (Require A Password)**, чтобы при пробуждении компьютера нужно было вводить пароль. Щелкните **Сохранить изменения (Save Changes)**.

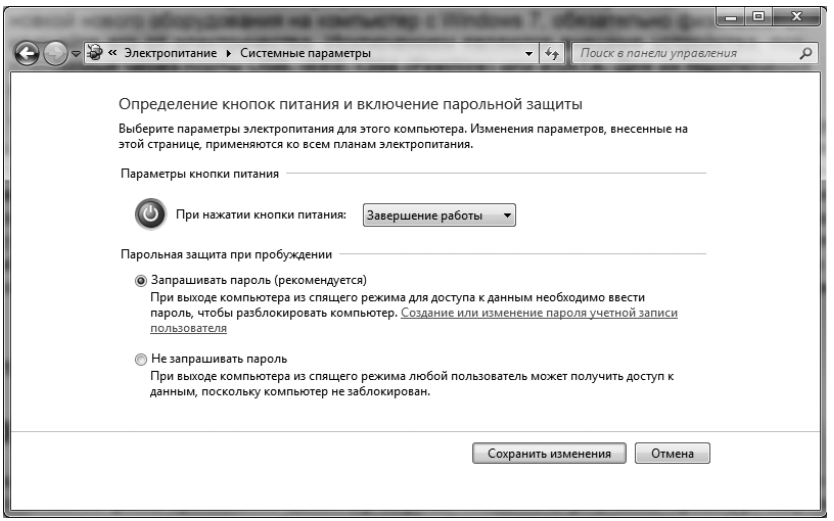

Рис. 1-6. Настройка параметров кнопок

Архитектура Windows 7

Теперь мы немного поговорим о внутреннем устройстве Windows 7. Для загрузки этой ОС вместо инициализационного файла применяется диспетчер загрузки Windows. В результате процедура запуска ОС претерпела значительные изменения. Загрузочная среда (boot environment) была создана Майкрософт для решения некоторых болезненных проблем с целостностью загрузки, целостностью ОС и абстрагированием микропрограммного кода (firmware). Загрузочная среда запускается перед ОС и может применяться

для проверки целостности процесса запуска и самой ОС, прежде чем ОС действительно начинает работу.

Загрузочная среда — это расширяемый уровень абстрагирования, который позволяет ОС работать с несколькими типами микропрограммных интерфейсов без необходимости переписывания кода ОС для каждого из этих интерфейсов. В результате при появлении нового микропрограммного интерфейса модернизировать ОС уже не нужно, при условии что разработчик интерфейса следует правилам программного интерфейса загрузочной среды.

Абстрагирование микропрограммного интерфейса — первый ингредиент, позволяющий Windows 7 абсолютно одинаково работать как с компьютерами на базе BIOS, так и с компьютерами на базе EFI. Это же одна из основных причин независимости Windows 7 от оборудования. Подробнее вы прочитаете об этом в главах 2 и 10.

Следующий ингредиент независимости Windows 7 от оборудования — формат образов Windows (Windows Imaging Format, WIM). Майкрософт распространяет Windows 7 на носителях в формате образов WIM. В них применятся сжатие и хранение в одном экземпляре, благодаря чему существенно сокращается объем файлов. Хранение в одном экземпляре (single-instance storage) означает, что в образе диска для каждого файла сохраняется лишь одна физическая копия.

Поскольку формат WIM не зависит от оборудования, появилась возможность использовать один двоичный файл для каждой поддерживаемой архитектуры:

- один двоичный файл для 32-разрядных архитектур;
- один двоичный файл для 64-разрядных архитектур;
- один двоичный файл для архитектур Itanium.

Наконец, последний ингредиент аппаратной независимости Windows 7 — модульная структура. Каждый компонент ОС определен в виде самостоятельного модуля. Поскольку модули могут содержать в своем составе другие модули, основные компоненты ОС можно группировать друг с другом и описывать независимо от других основных компонентов. Независимость модулей друг от друга позволяет выборочно устанавливать и удалять их для тонкой настройки рабочей среды.

В Windows 7 включена обширная архитектура поддержки. В основе этой архитектуры лежат встроенные системы диагностики и поиска неисправностей. Предполагается, что большую часть ошибок эти системы найдут и исправят самостоятельно, а если это не получится, выдадут необходимую диагностическую информацию.

В Windows 7 имеются также службы отслеживания сети (network awareness) и обнаружения сети (network discovery). Служба отслеживания сети следит за изменениями в сетевой конфигурации и сетевых подключениях. Служба обнаружения сети управляет способностью компьютера обнаруживать в сети другие компьютеры и устройства.

Служба отслеживания сети позволяет Windows 7 определять текущую сетевую конфигурацию и состояние подключения. Это важно, поскольку многие сетевые параметры и параметры безопасности зависят от того, к сети какого вида подключен сейчас компьютер Windows 7. В Windows 7 предусмотрены отдельные конфигурации для доменных сетей, частных сетей и сетей общего доступа. ОС способна зафиксировать:

- изменение сетевого подключения;
- появление подключения к Интернету;
- подключение к корпоративной сети через Интернет.

В отличие от прежних версий Windows, в Windows 7 брандмауэр поддерживает одновременное подключение к нескольким сетям и одновременное использование нескольких профилей. В результате профиль брандмауэра, активный в данный момент, зависит от типа соединения.

Если вы отключите компьютер от одного концентратора и подключите к другому концентратору, компьютер может ошибочно решить, что его подключили к другой сети. При некоторых настройках групповой политики это может привести компьютер в состояние блокировки, в котором применяются дополнительные параметры сетевой безопасности. Как показано на рис. 1-7, для просмотра информации о состоянии сетевого подключения используется Центр управления сетями и общим доступом (Network And Sharing Center). Чтобы открыть его, щелкните ссылку **Центр управления сетями и общим доступом (Network And Sharing Center)** в категории **Сеть и Интернет (Network And Internet)** панели управления.

Совет Благодаря компоненту DirectAccess, компьютеры Windows 7 способны теперь непосредственно обращаться к корпоративной сети, где бы они ни находились, при условии наличия подключения к Интернету. При этом инициализация VPNподключения не требуется. В корпоративной сети должен быть настроен сервер DirectAccess. Кроме того, необходимо разрешить DirectAccess в групповой политике. Подробнее — в главе 16.

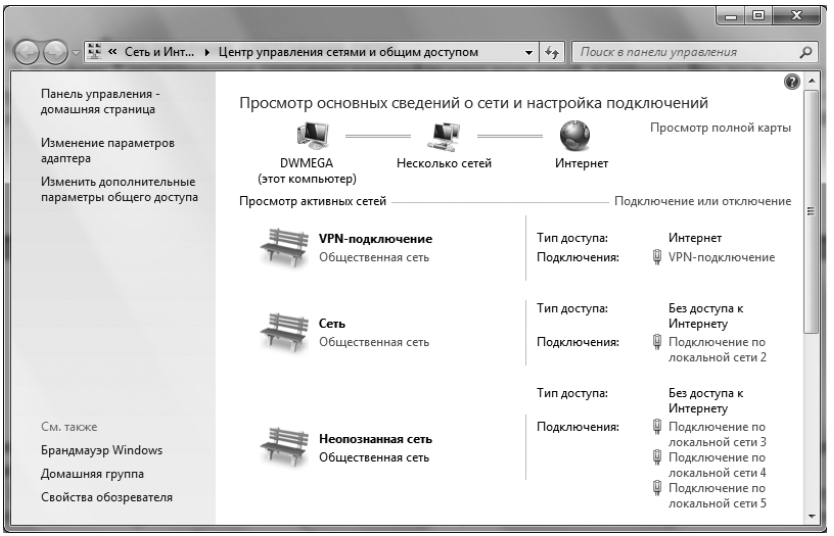

Рис. 1-7. Просмотр состояния сетей

В Windows 7 отслеживается состояние идентификации всех сетей, к которым был подключен компьютер. Когда Windows 7 находится в процессе идентификации сети, в консоли Центр управления сетями и общим доступом (Network and Sharing Center) отображается временное состояние **Идентификация сети (Identifying Networks)**. Когда сеть идентифицирована, она включатся в список сетей со своим сетевым или доменным именем.

Если идентифицировать сеть не удается, в консоли Центр управления сетями и общим доступом (Network And Sharing Center) сеть отображается как Неопознанная сеть (Unidentified Network). Для каждого состояния сети, а также для всех сетей в групповой политике можно задать расположение по умолчанию и разрешения пользователей. Соответствующие разрешения находятся в подузле **Конфигурация Windows\Параметры безопасности\Политики диспетчера списка сетей (Windows Settings\Security Settings\Network List Manager Policies)** узла **Конфигурация компьютера (Computer Configuration)**.

При работе с консолью Центр управления сетями и общим доступом (Network And Sharing Center) для выяснения смысла предупреждения вы можете воспользоваться компонентом системы диагностики и поиска неисправностей в сети. Чтобы запустить это средство, щелкните значок предупреждения на карте сети или команду **Устранение неполадок (Troubleshoot Problems)**, а затем щелкните **Подключения к Интернету (Internet Connections)**. Инструмент диагностики Windows попытается определить причину сбоя в сети и предложит возможные пути его устранения.

Инфраструктура диагностики и поиска неисправностей Windows включает в себя усовершенствованные рекомендации, дополнительные данные об ошибках, развернутое ведение журналов и обширные политики восстановления. Хотя некоторые справочные и диагностические функции включались уже в Windows XP и в более ранние версии Windows, они не включали в себя возможности самодиагностики и самоисправления. Windows 7, напротив, способна не только обнаруживать разнообразные сбои в оборудовании, памяти и производительности, но и автоматически устранять их или выдавать пользователю рекомендации по устранению вручную.

Диагностические компоненты Windows разделены на 15 категорий, перечисленных в табл. 1-4. В групповой политике для настройки этих компонентов применяются политики из подузла **Административные шаблоны\Система\Диагностика (Administrative Templates\System\Troubleshooting and Diagnostics)** узла **Конфигурация компьютера (Computer Configuration)**.

Табл. 1-4. Основные области диагностики Windows 7

Область диагностики	Описание	Необходимые службы
Диагностика совместимости приложений (Application compatibility)	Поддерживает работу Помощника по совместимости программ (Program Compatibility Assistant, PCA) по выявлению драйверов, заблокированных из-за проблем с совместимостью. PCA способен обнаруживать сбои, вызванные приложениями, которые попытались вызвать DLL для старых версий Windows или создать COM-объекты, удаленные Майкрософт. Также PCA умеет выявлять несколько типов сбоев при установке приложений, в частности сбоев, связанных с отсутствием необходимых разрешений для установки или запуска дочерних процессов. В подобных случаях PCA предложит вам перезапустить установщик или процесс обновления от имени администратора	Служба политики диагностики (Diagnostic Policy Service), Служба помощника по совместимости программ (Program Compatibility Assistant Service)
Диагностика быстродействия загрузки Windows (Boot performance)	Поддерживает автоматическое выявление и диагностику неполадок, затрагивающих производительность загрузки. Основные причины неполадок, снижающих производительность загрузки, записываются в журналы событий. Также эта область поможет устранить причины неполадки	Служба политики диагностики (Diagnostic Policy Service)
Восстановление поврежденного файла (Corrupted file recovery)	Поддерживает автоматическое обнаружение и восстановление поврежденных файлов. Если поврежден важный системный файл, ОС генерирует уведомление и пытается исправить файл, что в большинстве случаев требует перезагрузки системы	Служба политики диагностики (Diagnostic Policy Service)
Средство диагностики службы технической поддержки Майкрософт (External support)	Поддерживает работу диагностического инструмента MSDT (Microsoft Support Diagnostic Tool) по сбору диагностических данных и их отправке профессионалам службы поддержки. Программа Msdt.exe хранится в папке %SystemRoot%\System32. Параметры политики позволяют настроить ее на использование локальной и удаленной поддержки или только удаленной поддержки	Служба политики диагностики (Diagnostic Policy Service)
Отказоустойчивая куча (Fault-tolerant heap)	Поддерживает автоматическое выявление и исправление типичных проблем с управлением памятью, связанных с кучей	Служба политики диагностики (Diagnostic Policy Service)

Табл. 1-4. (*продолжение*)

Область диагностики	Описание	Необходимые службы
Диагностика утечки памяти Windows (Memory leak)	Поддерживает автоматическое выявление и исправление типичных проблем с утечкой памяти. Утечка происходит, когда приложение или системный компонент не полностью освобождают области памяти, закончив работу с ними	Служба политики диагностики (Diagnostic Policy Service)
Восстановление поврежденного файла MSI (MSI corrupted file recovery)	Поддерживает автоматическое выявление и исправление поврежденных приложений MSI. Если Windows обнаруживает поврежденные файлы приложений, то генерирует уведомление и пытается исправить файлы	Служба политики диагностики (Diagnostic Policy Service)
Быстродействие Windows Perf-Track (Performance Perf Track)	Поддерживает автоматическое отслеживание событий реагирования (responsiveness event) и передачу информации о них в команду Майкрософт Software Quality Management (SQM)	
Обнаружение и устранение нехватки ресурсов Windows (Resource exhaustion)	Поддерживает автоматическое выявление и устранение проблем, связанных с исчерпанием виртуальной памяти. Также уведомляет пользователя об исчерпании виртуальной памяти и указывает процессы, потребляющие максимальный объем памяти, предоставляя команды для завершения некоторых или всех таких процессов. Уведомление записывается в журнал событий	Служба политики диагностики (Diagnostic Policy Service)
Запланированное обслуживание (Scheduled maintenance)	Поддерживает периодический запуск диагностической проверки при помощи Планировщика заданий (Task Scheduler)	Планировщик заданий (Task Scheduler Service)
Диагностика со сценариями (Scripted diagnostics)	Поддерживает работу Центра поддержки (Action Center) и определяет, может ли пользователь получить доступ к информации о диагностике и диагностическим инструментам	
Диагностика быстродействия завершения работы Windows (Shutdown performance)	Поддерживает автоматическое выявление и диагностику проблем, снижающих быстродействие завершения работы Windows. Основные причины неполадок, снижающих производительность завершения работы, записываются в журналы событий. Также эта область поможет устранить причины неполадки	Служба политики диагностики (Diagnostic Policy Service)

Табл. 1-4. (*окончание*)

Область диагностики	Описание	Необходимые службы
Диагностика производительности ждущего режима и возобновления работы Windows (Standby/resume performance)	Поддерживает автоматическое выявление и диагностику проблем, снижающих быстродействие входа в спящий режим и выхода из него на настольных компьютерах. Основные причины неполадок, снижающих производительность входа в спящий режим и выхода из него, записываются в журналы событий. Также эта область поможет устранить причины неполадки	Служба политики диагностики (Diagnostic Policy Service)
Диагностика скорости отклика системы Windows (System responsiveness)	Поддерживает автоматическое выявление и диагностику проблем, связанных с общими характеристиками отклика ОС. Основные причины неполадок записываются в журналы событий. Также эта область поможет устранить причины неполадки	Служба политики диагностики (Diagnostic Policy Service)

Другие диагностические средства Windows 7 таковы:

- Диспетчер перезапуска (Restart Manager).
- Центр поддержки (Action Center) и средства устранения неполадок (troubleshooter).
- Инструмент Восстановление при загрузке (Startup Repair).
- Инструменты для мониторинга производительности.
- Средство проверки памяти Windows (Windows Memory Diagnostics).

В Windows XP и других предыдущих версиях Windows о зависании приложения свидетельствовали слова Не отвечает (Not Responding). Пользователю предлагалось самому решить, хочет ли он перезапустить приложение. Система Windows 7 пытается устранить проблемы, связанные с неотвечающими приложениями, при помощи Диспетчера перезапуска (Restart Manager), который способен самостоятельно завершать работу зависших приложений и перезапускать их. Во многих случаях это означает, что разрешение проблем с зависшими приложениями вообще не потребует вашего вмешательства.

Неполадки при установке приложений и зависания приложений и драйверов отслеживаются также в Центре поддержки (Action Center). Когда случается что-то подобное, на значке Центра поддержки (Action Center) появляется красный кружок с буквой «X». Щелкните этот значок, чтобы отобразить отчет о текущих проблемах. Для каждой проблемы приводится ссылка, щелкнув которую, вы узнаете, как устранить сбой, или, по крайней мере, получите более подробную информацию о нем. Если эти действия не привели к успеху, откройте главное окно Центра поддержки (Action Center) и пролистайте его вниз до ссылок **Устранение неполадок (Troubleshooting)** и **Восстановление (Recovery)**.

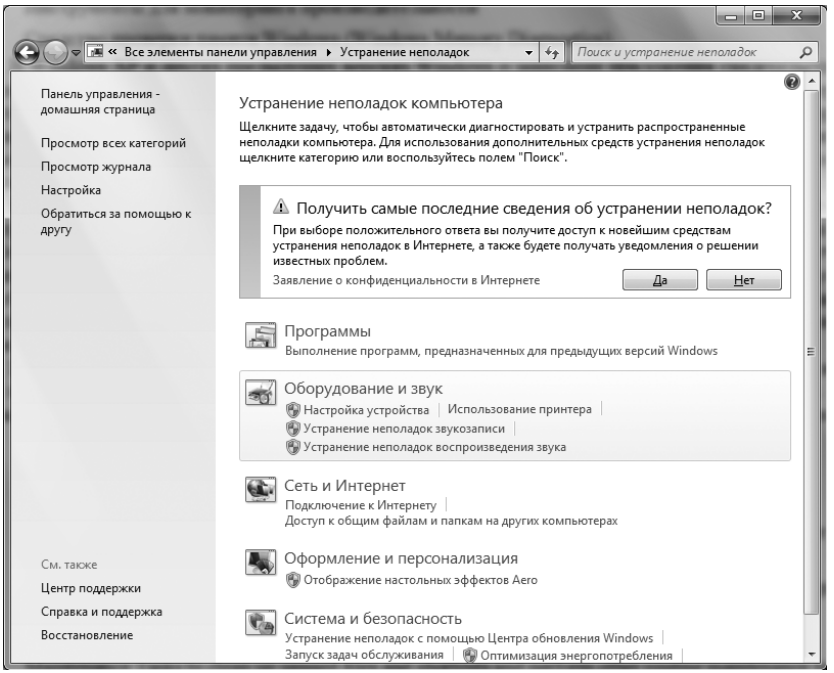

Рис. 1-8. Средства для устранения типичных неполадок

Щелкните ссылку **Устранение неполадок (Troubleshooting)**, чтобы открыть окно **Устранение неполадок компьютера (Troubleshooting)**. В нем имеется несколько средств устранения неполадок (рис. 1-8), которые помогут вам оперативно устранить типичные сбои, не требующие вмешательства администратора:

- **Программы (Programs)** Проблемы совместимости приложений, написанных для прежних версий Windows.
- **Оборудование и звук (Hardware and Sound)** Проблемы с оборудованием, записью и воспроизведением аудио.
- **Сеть и Интернет (Network and Internet)** Проблемы с сетевыми подключениями и с доступом к общим папкам на других компьютерах.
- **Оформление и персонализация (Appearance and Personalization)** Проблемы с внешним видом дисплея и персональными параметрами. Чтобы быстро устранить сбои в работе Aero, щелкните ссылку **Отображение настольных эффектов Aero (Display Aero Desktop Effects)**.
- **Система и безопасность (System and Security)** Проблемы с обновлением Windows Update, электропитанием и производительностью. Щелкните ссылку **Запуск задач обслуживания (Run Maintenance Tasks)**, чтобы удалить неиспользуемые файлы и ярлыки, а также выполнить другие действия по повседневному обслуживанию.

Для разрешения проблем с запуском в Windows 7 используется инструмент Восстановление при запуске (Startup Repair, StR), который автоматически устанавливается и запускается, если вам не удалось загрузить систему.

После запуска инструмент StR пытается определить причину сбоя запуска, анализируя журналы запуска и отчеты об ошибках. Затем он пытается автоматически исправить проблему. Если сделать это не удается, StR восстанавливает систему до последнего работоспособного состояния и сохраняет информацию для последующей диагностики.

Проводя диагностику, инструмент Восстановление при запуске (Startup Repair) выполняет множество проверок, занимающих от 5 до 30 минут и даже более, в зависимости от настроек оборудования. В частности, выполняются следующие проверки:

- **Проверка установки обновлений** На процесс запуска могут отрицательно влиять недавно установленные обновления.
- **Проверка системного диска** Возможно, запустить ОС не удается из-за сбоя на системном диске. Если это действительно так, StR пытается восстановить отсутствующие или испорченные файлы.
- **Диагностика дисковых сбоев** Проверка всех настроенных дисков.
- **Проверка метаданных диска** Возможно, запустить ОС не удается из-за проблем с метаданными доступных дисков, то есть с данными о разделах и файловых системах.
- **Проверка целевой ОС** Возможно, запуск не удается осуществить из-за сбоя в ОС, которую вы пытаетесь загрузить.
- **Проверка содержимого тома** Проверка доступности содержимого томов.
- **Диагностика диспетчера загрузки** Проверяется, не связан ли сбой с диспетчером загрузки или с его элементами.
- **Проверка журнала системной загрузки** Проверяются записи в журнале системной загрузки, относящиеся к предыдущим запускам. Возможно, информация о причинах сбоя обнаружится в них.
- **Проверка журнала событий** В журнале событий ищутся записи с информацией об ошибках, которые могут иметь отношение к сбою запуска.
- **Проверка внутреннего состояния** Проверяется внутреннее состояние предзагрузочной среды.
- **Проверка состояния загрузки** Проверяется текущее состояние загрузки в предзагрузочной среде.
- **Проверка состояния установки** Проверяется, не находится ли компьютер в состоянии установки.
- **Проверка разделов реестра** Проверяется реестр на компьютере.
- **Проверка журнала загрузки Windows** Записи журнала загрузки Windows просматриваются на предмет наличия конкретных ошибок, которые могут быть связаны со сбоем при запуске.
- **Анализ ошибок** Выполняется базовая проверка ошибок ОС.
- **Проверка управления доступом** Выясняется, не являются ли причиной сбоя при запуске ОС параметры управления доступом.
- **Проверка файловой системы (chkdsk)** Средствами Chkdsk выполняется базовая проверка файловой системы.

- **Проверка журнала установки приложений** Записи журнала установки приложений просматриваются на предмет наличия конкретных ошибок, которые могут быть связаны со сбоем при запуске.
- **Диагностика отката** Проверяется, установлены ли какие-либо флаги, указывающие, что для устранения сбоя при запуске компьютер необходимо откатить до предыдущего состояния. Если это так, StR пытается восстановить предыдущее состояние.

Автоматизировано также обнаружение ошибок устройств и сбоев на жестких дисках. Если устройство столкнулось с проблемами, диагностические инструменты определяют причину возникновения ошибки и либо исправляют ее автоматически, либо выдают пользователю необходимые инструкции по исправлению. В случае проблем на жестком диске диагностические инструменты при помощи отчетов, созданных дисками, выявляют потенциальные сбои и заблаговременно предупреждают вас о возможных неполадках, а также предлагают провести резервное копирование данных.

ОС Windows 7 способна автоматически обнаруживать проблемы с производительностью, включая медленный запуск приложений, медленную загрузку, медленный вход в спящий режим и выход из него, медленное завершение работы. Если производительность компьютера падает, диагностические средства Windows обнаружат причину и предложат меры по ее устранению. Чтобы провести детальный анализ производительности, воспользуйтесь Монитором производительности (Performance Monitor), доступ к которому открывает меню **Администрирование (Administrative Tools)**.

Также автоматически выявляются проблемы со сбоями в памяти и с утечкой памяти. Если вы заподозрили неполадки в памяти, но автоматически они не обнаруживаются, запустите Средство проверки памяти Windows (Windows Memory Diagnostics) вручную, выполнив следующие действия:

1. Щелкните кнопку **Пуск (Start)**, введите **mdsched.exe** в поле поиска и нажмите Enter.
2. Укажите, нужно ли немедленно перезапустить компьютер и начать проверку или запустить средство при следующем перезапуске.
3. Средство проверки памяти Windows (Windows Memory Diagnostics) автоматически запускается при перезапуске компьютера и выполняет стандартную проверку памяти. Если вы хотите сократить или расширить число выполняемых проверок, нажмите F1, а затем при помощи клавиш-стрелок выберите в группе **Набор тестов (Test Mix)** вариант **Базовый (Basic)**, **Обычный (Standard)** или **Широкий (Extended)**. Затем нажмите F10, чтобы применить параметры и продолжить проверку.
4. По завершении проверки компьютер перезапускается. После входа в систему просмотрите результаты проверки.

Если компьютер зависает из-за нарастающих проблем с памятью, и эти проблемы удалось выявить, вам будет предложено назначить проверку памяти при следующем запуске компьютера.

Глава 2

Развертывание Windows 7

Настраиваемые образы Windows 7 можно развертывать как вручную, так и автоматически. Чтобы развернуть Windows вручную, необходимо создать загрузочный и установочный образы, а также образы восстановления. Для автоматизации развертывания установите службы развертывания Windows. Каким бы способом вы ни пользовались (развертывание вручную, автоматически или при помощи комбинации обоих способов), вам придется решать одни и те же административные задачи. Предполагается, что у вас есть навыки работы со следующими компонентами:

- предустановочной средой Windows (Windows PE);
- средой восстановления Windows (Windows RE);
- инструментами Windows для создания образов;
- службами развертывания Windows.

В этой главе мы обсудим эти технологии и продемонстрируем, как пользоваться ими при развертывании Windows 7.

Предустановочная среда (Windows PE)

Предустановочная среда Windows (Windows pre-installation environment, Windows PE) пришла на смену MS-DOS в качестве среды для подготовки к установке ОС Windows. Установка Windows Vista и Windows 7 осуществляется только при помощи Windows PE и образов дисков. Также Window PE можно использовать для запуска компьютеров и их подготовки к установке.

Подробнее о Windows PE

В Windows 7 и Windows Server 2008 Release 2 применяется загружаемая среда предустановки Windows PE 3.0, предоставляющая ОС инструментарий для решения следующих задач:

- **Установка** В среде Windows PE работают графические инструменты, собирающие информацию о системе при установке Windows 7.
- **Развертывание** Когда новый компьютер загружается из сети, встроенный клиент предзагрузочной среды выполнения (PXE) способен подключиться к серверу развертывания Windows, загрузить образ среды

Windows PE по сети и затем запустить из этой среды сценарии развертывания.

- **Восстановление** Если Windows 7 не запускается из-за сбойного системного файла, Windows PE позволяет получить доступ к пакету восстановления и запустить его.
- **Устранение неполадок** Если при работе Windows 7 возникли проблемы, диагностику которых обычным способом провести не удается, для устранения неполадок или диагностики можно запустить Windows PE вручную.

Windows PE имеет модульную расширяемую архитектуру. Она предоставляет полный доступ к разделам диска как с файловой системой FAT, так и с файловой системой NTFS. Поскольку среда Windows PE основана на компонентах Windows, в ней можно запускать многие приложения Windows, работать с оборудованием и подключаться к сетям IP. В среде Windows PE доступны некоторые инструменты командной строки, в том числе:

- **BCDBoot** Создает хранилище данных конфигурации загрузки (BCD) и позволяет копировать файлы загрузочной среды в системный раздел.
- **Bootsect** Инструмент для создания на жестких дисках и флеш-накопителях загрузочных секторов и работы с ними.
- **DiskPart** Инструмент для создания дисков, разделов и томов и работы с ними.
- **DISM** Инструмент для обслуживания образов и управления ими.
- **Drvload** Позволяет добавлять драйверы устройств и динамически загружать драйвер после загрузки Windows PE.
- **ImageX** Инструмент для записи и загрузки образов Windows.
- **Net** Набор вспомогательных команд для управления локальными пользователями, запуска и остановки служб и подключения к общим папкам.
- **Netcfg** Инструмент для настройки сетевого доступа.
- **Oscdimg** Инструмент для создания ISO-образов CD-дисков и DVD-дисков.
- **Wpeinit** Инициирует Windows PE при каждом ее запуске.

Для выполнения основных конфигурационных процедур во время развертывания ОС перечисленные выше средства можно запускать из сценариев конфигурации. Например, можно выполнить следующие действия:

- настроить доступ к сети при помощи Netcfg;
- установить драйвер и подключить оборудование без перезагрузки компьютера при помощи Drvload;
- отформатировать жесткий диск и разбить его на разделы при помощи DiskPart;
- подключиться к общей папке с установочными файлами Windows 7 при помощи Net Share;
- запустить программу установки Windows 7.

Среда Windows PE включена в пакеты Windows OEM Preinstallation Kit (Windows OPK), Windows Automated Installation Kit (Windows AIK) и Windows PE Kit. Чтобы можно было создавать при помощи Windows PE загрузочную и установочную среду Windows 7, перечисленные пакеты должны предназначаться именно для Windows 7.Поскольку они часто обновляются, проверьте, нужным ли пакетом обновления вы пользуетесь.

В пакеты отдельно включены 32-разрядная и 64-разрядная версия Windows PE. Для 32-разрядной версии Windows 7 нужно использовать 32-разрядную версию Windows PE, для 64-разрядной версии Windows 7 — 64-разрядную.

Windows PE, как и сама Windows 7, может содержаться в образе диска. Если в образе хранится Windows 7, единственный способ запустить ее — полностью скопировать образ на жесткий диск компьютера. Если в образе хранится Windows PE, ее можно запустить прямо из образа, не копируя его на жесткий диск. Это позволяет хранить образы Windows PE на загрузочных носителях, например DVD-дисках или USB-накопителях, а затем запускать Windows PE напрямую с носителя. В установочном комплекте Windows 7 эта возможность используется для загрузки Windows PE в оперативную память во время установки ОС.

Загрузка Windows PE в оперативную память может также потребоваться при устранении неполадок. В этом случае загрузчик Windows PE создает в памяти виртуальный диск и копирует на него сжатую версию Windows PE. Затем загрузчик подключает виртуальный диск как один из дисков компьютера и запускает Windows PE. Запуск Windows PE с виртуального диска позволяет записать на этот диск временные файлы, что невозможно, если запуск произведен с накопителя, допускающего только чтение, например с CD-диска. Также вы вольны после запуска предустановочной среды извлечь накопитель Windows PE и вставить другой дистрибутив на CD-диске, DVD-диске или USB- накопителе.

При работе с Windows PE необходимо иметь в виду следующее:

- Для работы Windows PE требуется VESA-совместимый графический адаптер и объем оперативной памяти не менее 256 Мб. Если во время запуска Windows PE не может определить поддерживаемые режимы экрана, устанавливается разрешение 640×480 точек. В противном случае устанавливается самое высокое разрешение.
- Среда Windows PE поддерживает устройства Plug and Play и способна в процессе работы находить и устанавливать оборудование. Это означает, что вы сможете установить любое устройство Plug and Play, включая съемные накопители и жесткие диски, для которого в хранилище драйверов есть драйвер.
- Среда Windows PE поддерживает подключение как к сетям IPv4, так и к сетям IPv6. С компьютера, на котором запущена Windows PE, можно получить доступ к общим разделам на других компьютерах. К папкам и файлам на самом компьютере доступа не будет.

- Windows PE всегда запускается со стандартным порядком букв для дисков. Измененные назначения букв при перезапуске не сохраняются.
- Windows PE не сохраняет изменения в реестре. Это означает, что изменения в реестре будут отсутствовать при следующем запуске. Чтобы сохранить изменения в реестре, необходимо подключить образ Windows PE и внести изменения в редакторе реестра.
- Windows PE не поддерживает платформу Microsoft .NET Framework и подсистему Windows в Windows 64 (WOW64). Это означает, что ни в одной версии Windows PE не удастся запустить приложения .NET. Также в 32-разрядной версии Windows PE не будут работать 16-разрядные приложения, а в 64-разрядной версии не будут работать 32-разрядные приложения.
- Windows PE автоматически перезагружается каждые 72 часа. Это защита от использования Windows PE в качестве обычной ОС.

Среду Windows PE можно загрузить из файла Boot.wim на установочном диске Windows. После инициализации Windows PE вызывается команда Wpeinit, которая инициализирует устройства Plug and Play и подключается к сети.

Настройка Windows PE

В Windows PE поддерживается несколько файлов конфигурации, управляющих ее запуском и последующей работой:

- **Хранилище данных конфигурации загрузки (Boot Configuration Data, BCD)** Содержит параметры загрузки Windows PE.
- **Startnet.cmd** Сценарий, настраивающий запуск сети. В него можно добавить собственные команды.
- **Unattend.xml** Файл, позволяющий автоматизировать установку Windows PE.
- **Winpeshl.ini** Файл инициализации оболочки Windows PE. Содержит интерфейс Windows PE по умолчанию. Изменяя этот файл, можно настроить среду оболочки.

Во время запуска компьютера с Windows 7 перед загрузкой ОС осуществляется вход в предзагрузочную среду, которая при помощи диспетчера загрузки Windows управляет загрузкой и определяет, какие загрузочные приложения должны выполняться. Стандартное загрузочное приложение Windows 7 — загрузчик Windows (Windows Boot Loader). Он отвечает за доступ к записям в хранилище данных BCD, которые содержат параметры конфигурации загрузки и управляют запуском ОС.

Хранилище BCD позволяет абстрагироваться от конкретной микропрограммы, облегчая работу Windows 7 с их новыми версиями, например с интерфейсом EFI. Также хранилище BCD лежит в основе ряда новых возможностей Windows 7, включая восстановление при загрузке и ярлыки многопользовательской установки, которые можно запустить в предзагрузочной среде.

Хранилище BCD находится в файле реестра BCD, который на BIOS-компьютерах хранится в папке \Boot\Bcd активного раздела, а на EFI-компьютерах — в системном разделе EFI. На большинстве компьютеров в хранилище данных конфигурации загрузки содержатся несколько записей:

- запись для диспетчера загрузки Windows (поскольку имеется только один диспетчер загрузки, в хранилище BCD такая запись только одна);
- по одной записи загрузчика Windows для каждой копии ОС Windows 7, установленной на компьютере;
- одна запись для устаревших ОС.

Последняя запись не предназначена для загрузочных приложений. В ней для запуска версий Windows, выпущенных до Windows Vista, используются Ntldr и Boot.ini. Эта запись применяется для загрузки Windows Server 2003, Windows XP и более ранних версий, если они установлены на компьютере. Подробно о микропрограммах и хранилище данных конфигурации загрузки написано в главе 10.

Выполнение Windows PE приходится на проход настройки Windows PE процесса установки Windows. На этом этапе Windows PE ищет файл Unattend.xml. Если он существует, Windows PE считывает разделы файла, которые используются для автоматизации ее установки. Для создания и изменения файлов Unattend.xml применяется диспетчер системных образов Windows (Window SIM), включенный в пакет Windows AIK. Файл Unattend.xml можно также создать вручную в текстовом редакторе.

После создания файла Unattend.xml скопируйте его в корневую папку загрузочного устройства, поскольку по умолчанию Windows PE ищет его именно там. Расположение файла Unattend.xml можно также указать при помощи команды Wpeutil или сценария StartNet.

Инициализация Windows PE осуществляется при помощи файла Winpeshl.ini из папки %SystemRoot%\System32 образа Windows PE. В этом файле можно указать путь и имя исполняемого файла пользовательского приложения, которое должно быть запущено при запуске Windows PE. В частности, среда восстановления Windows, включенная в Windows 7, — это просто образ Windows PE, запускающий пользовательское приложение.

Подготовка среды сборки

При установке пакета Windows OPK, Windows AIK или Windows PE устанавливаются среда сборки и средства для работы с образами, необходимые для создания образов Windows PE. Загрузить Windows AIK можно со страницы Центра загрузки Майкрософт (http://download.microsoft.com/). Затем запишите пакет на DVD-диск или подключите его при помощи виртуального DVD-дисковода. Если установка не начинается автоматически, откройте DVD в проводнике и щелкните дважды команду StartCD.exe.

После установки пакета вы увидите следующие папки (где *Версия* — Windows OPK, Windows AIK или Windows PE):

- **%SystemRoot%\Program Files*Версия*\Tools** Файлы программ для данной версии.
- **%SystemRoot%\Program Files*Версия*\Tools\amd64** Исходные файлы ImageX для 64-разрядных компьютеров на базе amd64.
- **%SystemRoot%\Program Files*Версия*\Tools\x86** Исходные файлы ImageX для 32-разрядных компьютеров на базе x86.
- **%SystemRoot%\Program Files*Версия*\Tools\ia64** Исходные файлы ImageX для компьютеров на базе Itanium.
- **%SystemRoot%\Program Files*Версия*\Tools\Image Manager** Диспетчер системных образов Windows и связанные файлы.
- **%SystemRoot%\Program Files*Версия*\Tools\PETools** Исходные файлы и дополнительные компоненты Windows PE.
- **%SystemRoot%\Program Files*Версия*\Tools\Servicing** Файлы служб.
- **%SystemRoot%\Program Files*Версия*\Tools\USMT** Инструмент переноса данных пользователей и связанных файлов для компьютеров на базе x86 и x64.

Чтобы создать образ, необходимо установить среду сборки. Для создания среды сборки Windows PE применяется сценарий Copype.cmd из папки Tools. Среда сборки содержит сценарии сборки и исходные файлы, которые можно настроить и затем использовать для создания новых образов Windows PE.

При работе с инструментами пакета пользуйтесь командной строкой средств развертывания. Она настроена для работы с установленным пакетом и запускается после выполнения следующих действий:

1. Щелкните кнопку **Пуск (Start)**, выберите **Все программы (All Programs)**, а затем щелкните **Microsoft Windows OPK**, **Microsoft Windows AIK** или **Microsoft Windows PE**.
2. Правой кнопкой мыши щелкните команду **Утилиты командной строки Windows PE (Deployment Tools Command Prompt)** и выберите команду **Запуск от имени администратора (Run As Administrator)**.

Чтобы настроить среду сборки для 32-разрядных компьютеров на базе x86, введите команду:

```
copype x86 c:\winpe_x86
```

Чтобы настроить среду построения для 64-разрядных компьютеров на базе x64, введите команду:

```
copype amd64 c:\winpe_x64
```

Чтобы настроить среду построения для компьютеров на базе Itanium, введите команду:

```
copype ia64 c:\winpe_ia64
```

Эти команды создают среду сборки в папках C:\Winpe_x86, C:\Winpe_x64 и C:\Winpe_ia64, соответственно. Можно указать для установки и другие папки, однако использование стандартных имен облегчит работу другим администраторам организации.

В папке среды сборки находятся подпапки ISO и Mount. Папка ISO содержит все необходимые файлы для создания ISO-файла при помощи утилиты Oscdimg. Она разделена на подпапки Boot, EFI и Sources. Папка Mount пуста. Ее можно использовать для размещения образов Windows PE при помощи утилиты ImageX.

При работе с файлами образов Windows применяются следующие аргументы утилиты ImageX:

- **imagex /append** Добавляет образ тома к существующему файлу образа Windows. В приведенном ниже примере *ПутьОбраза* — путь к образу добавляемого тома, *WIMФайл* — путь к существующему WIM-файлу, *ИмяОбраза* — уникальное имя образа, *Описание* — пояснительный текст. Параметр */Boot* помечает образ тома как загружаемый (только для образов Windows PE). Параметр */Check* позволяет проводить проверку целостности WIM-файла, а */Config Config.ini* указывает на файл конфигурации, при помощи которого вы исключаете файлы и задаете параметры сжатия. Параметр */Norpfix* блокирует активность маркеров повторной обработки. Благодаря параметру */Scroll* осуществляется прокрутка выходных данных для перенаправления. Параметр */Temp* указывает путь к хранилищу временных файлов, а параметр */Verify* позволяет осуществить проверку файловых ресурсов.

```
imagex {Параметры} /append ПутьОбраза WIMФайл «ИмяОбраза» [«Описание»]

{Параметры}
[/boot] [/check] [/config config.ini] [/norpfix] [/scroll] [/temp] [/verify]

imagex /append c: d:\images\windows.wim «Drive C»
```

- **imagex /apply** Применяет образ тома к указанному назначению. *WIMФайл* — путь к WIM файлу, содержащему образ тома, *НомерОбраза* — идентификатор (номер) образа в WIM-файле, *ИмяОбраза* — имя, определяющее образ в WIM-файле, *ПутьОбраза* — путь, по которому будет применяться образ. Параметр */Ref Splitwim.swm* позволяет разделять WIM-файлы:

```
imagex {Параметры} /apply WIMФайл {НомерОбраза | ИмяОбраза} ПутьОбраза

{Параметры}
[/check] [/norpfix] [/ref splitwim.swm] [/scroll] [/temp] [/verify]

imagex /apply d:\images\windows.wim 1 c:\
```

- **imagex /capture** Записывает образ тома с диска в файл образа Windows. *ПутьОбраза* — путь к образу тома, который следует записать, *WIMФайл* — путь к новому WIM-файлу, *ИмяОбраза* — уникальное имя образа, который требуется записать, *Описание* — текст с дополнительной информацией. Параметр */Compress Maximum* указывает на максимально высокий уровень сжатия, а */Compress Fast* позволяет провести быстрое сжатие.

```
imagex {Параметры} /capture ПутьОбраза WIMFайл «ИмяОбраза» [«Описание»]

{Параметры}
[/boot] [/check] [/compress {maximum | fast | none}]
[/config] [/norpfix] [/scroll] [/temp] [/verify]

imagex /capture c: d:\images\windows.wim «Drive C»
```

- **imagex /cleanup** Удаляет все ресурсы, связанные с подключенным образом, который более не используется. Эта команда не отключает подключенные образы и не удаляет образы, которые можно восстановить при помощи команды imagex /remount.
- **imagex /commit** Сохраняет изменения в подключенном образе без его отключения. *ПутьПодключения* — путь к подключенному образу, *ИмяОбраза* — имя образа. Параметр */Append* приводит к созданию нового образа с включением в него произведенных изменений. Если используется параметр */Append*, необходимо указать уникальное имя образа.

```
imagex [/append] /commit ПутьПодключения [«ИмяОбраза»]

imagex /commit c:\mount
imagex /commit /append c:\mount «New Image»
```

- **imagex /delete** Удаляет указанный образ тома из файла образа Windows, содержащего несколько образов томов. *WIMФайл* — путь к WIM-файлу, содержащему нужный образ. *НомерОбраза* — номер образа в WIM-файле, *ИмяОбраза* — имя образа в WIM-файле.

```
imagex [/check] [/temp] /delete WIMФайл {НомерОбраза | ИмяОбраза}

imagex /delete d:\images\windows.wim 1
```

- **imagex /dir** Отображает список файлов и папок в указанном образе тома. *WIMФайл* — путь к WIM-файлу, содержащему нужный образ. *НомерОбраза* — номер образа в WIM-файле, *ИмяОбраза* — имя образа в WIM-файле.

```
imagex /dir WIMFile {НомерОбраза | ИмяОбраза}

imagex /dir d:\images\windows.wim 1
```

- **imagex /export** Экспортирует копию образа в другой файл образа Windows. *Источник* — путь к WIM-файлу, содержащему образ, который нужно экспортировать, *НомерИсточника* — номер образа в исходном WIM-файле, *ИмяИсточника* — имя образа в исходном WIM-файле, *Назначение* — путь к WIM-файлу, в который будет скопирован образ, *ИмяНазначения* — уникальное имя для образа в WIM-файле назначения. Если вместо имени источника задан символ «*», в файл назначения экспортируются все образы.

```
imagex {Параметры} /export Источник {НомерИсточника | ИмяИсточника}
Назначение ИмяНазначения

{Параметры}
[/boot] [/check] [/compress {maximum | fast | none}]
[/ref splitwim.swm] [/temp]

imagex /export d:\images\windows.wim 1 d:\images\win_copy.wim «Exported Image»
```

- **imagex /info** Возвращает описания для файла образа Windows или образа тома. *WIMФайл* — путь к WIM-файлу для запроса, *НомерОбраза* — номер образа в WIM-файле, *ИмяОбраза* — имя образа в WIM-файле, *НовоеИмя* — новое уникальное имя указанного образа, *НовоеОписание* — новое описание указанного образа. Параметр */XML* возвращает данные в формате XML.

```
imagex {Параметры} /info WIMФайл {НомерОбраза | ИмяОбраза} [НовоеИмя]
[НовоеОписание]

{Параметры}
[/boot] [/check] [/temp] [/xml]

imagex /info d:\images\windows.wim
```

- **imagex /mount** Подключает образ Windows только для чтения в указанную папку. *WIMФайл* — путь к WIM-файлу, содержащему нужный образ, *НомерОбраза* — номер образа в WIM-файле, *ИмяОбраза* — имя образа в WIM-файле, *ПутьОбраза* — путь, по которому будет применяться образ. Если параметры не заданы, команда создает список всех подключенных образов.

```
imagex [/check] /mount [WIMФайл {НомерОбраза | ИмяОбраза} ПутьОбраза]

imagex /mount d:\images\windows.wim 2 c:\mount
```

- **imagex /mountrw** Подключает образ Windows с правами для чтения и записи в указанную папку. *WIMФайл* — путь к WIM-файлу, содержащему нужный образ, *НомерОбраза* — номер образа в WIM-файле, *ИмяОбраза* — имя образа в WIM-файле, *ПутьОбраза* — путь, по которому будет при-

меняться образ. Если параметры не заданы, команда создает список всех подключенных образов.

```
imagex [/check] /mountrw [WIMФайл {НомерОбраза | ИмяОбраза} ПутьОбраза]

imagex /mountrw d:\images\data.wim 2 c:\mount
```

- **imagex /remount** Восстанавливает путь к образу. *ImagePath* — путь, который следует переподключить. Если параметры не заданы, команда создает список всех подключенных образов.

```
imagex /remount [ПутьОбраза]

imagex /remount c:\mount
```

- **imagex /split** Разделяет существующий файл образа Windows на несколько разделенных WIM-файлов (SWIM), доступных только для чтения. *WIMФайл* — путь к WIM-файлу, который требуется разделить, *Назначение* — путь к разделенному файлу или файлам, *Размер* — максимальный размер в мегабайтах для каждого создаваемого файла.

```
imagex [/check] /split WIMФайл Назначение Размер

imagex /split d:\images\windows.wim d:\images\splitdata.swm 600
```

- **imagex /unmount** Отключает файл образа Windows из указанной папки. *ПутьОбраза* — путь к папке, образ из которой нужно отключить. Параметр */Commit* сохраняет изменения перед отключением образа. Если существуют несохраненные изменения, в этой команде нужно использовать параметры */Commit* или */Discard*. Если параметры не заданы, команда создает список всех подключенных образов.

```
imagex /unmount [[/commit | /discard] ПутьОбраза]

imagex /unmount /commit c:\mount
```

Если вы хотите работать с образами Windows на компьютере, на котором не установлен соответствующий пакет, необходимо скопировать на этот компьютер файлы Dism.exe, Imagex.exe, Oscdimg.exe, Wimmount.sys, Wimmount.inf и Wimserv.exe, а затем установить драйвер подключения. Щелкните правой кнопкой файл Wimmount.inf и выберите **Установить (Install).** Для удобства скопируйте файлы Dism.exe, Imagex.exe, Oscdimg.exe и Wimserv.exe в папку %SystemRoot%\System32.

Основы создания среды сборки

Создание среды сборки для Windows PE заключается в создании базовых образов Windows PE. Ранее для настройки Windows PE применялась утилита PeImg, а теперь ей на смену пришла более надежная система обслужи-

вания образов развертывания DISM. Для создания пользовательской среды сборки при помощи DISM необходимо выполнить следующие действия:

1. Подключите образ.
2. Настройте образ.
3. Отключите образ.
4. Запишите образ в WIM-файл.
5. Создайте загрузочный ISO-образ.

Далее мы обсудим эти этапы подробнее. При работе с инструментами пакета пользуйтесь командной строкой средств развертывания. Чтобы запустить ее, выполните следующие действия:

1. Щелкните кнопку **Пуск (Start)**, выберите **Все программы (All Programs)**, а затем разверните подменю **Microsoft Windows OPK**, **Microsoft Windows AIK** или **Microsoft Windows PE**.
2. Правой кнопкой мыши щелкните команду **Утилиты командной строки Windows PE (Deployment Tools Command Prompt)** и выберите команду **Запуск от имени администратора (Run As Administrator)**.

Подключение образа Windows PE

После установки среды сборки необходимо подключить базовый образ. Это позволит настроить образы Windows PE.

- Чтобы подготовить к настройке 32-разрядную Windows PE, подключите базовый образ в папку сборки, введя команду **imagex /apply c:\winpe_x86\iso\sources\boot.wim *n* c:\winpe_x86\mount**, где *n* — номер образа в файле Boot.wim, который нужно применить, а указанный после него путь — место, куда нужно скопировать содержимое образа.
- Чтобы подготовить к настройке 64-разрядную Windows PE, подключите базовый образ в папку сборки, введя команду **imagex /apply c:\winpe_x64\iso\sources\boot.wim n c:\winpe_x64\mount**, где *n* — номер образа в файле Boot.wim, который нужно применить, а указанный после него путь — место, куда нужно скопировать содержимое образа.
- Чтобы подготовить к настройке Windows PE на базе Itanium, подключите базовый образ в папку сборки, введя команду **imagex /apply c:\winpe_ia64\iso\sources\boot.wim n c:\winpe_ia64\mount**, где *n* — номер образа в файле Boot.wim, который нужно применить, а указанный после него путь — место, куда нужно скопировать содержимое образа.

Примечание Есть еще несколько способов подключить образы для настройки. Например, для подключения образов можно использовать команду ImageX /MountRW. Синтаксис будет таким же, что и в команде ImageX /Apply. DISM также позволяет использовать параметры /Mount-wim и /Unmount-wim. Подробнее — в разделе «Настройка образов Windows» этой главы.

Если подключить образ при помощи ImageX не удается, убедитесь, что у вас запущена именно командная строка средств развертывания и вы работаете от имени администратора. Если эти условия выполнены, проверьте свойства файла образа и правильность настройки параметров безопасности.

Подключив образ, просмотрите его содержимое. Для доступа к папке, к которой подключен образ, можно воспользоваться проводником Windows. При работе с Windows PE необходимо помнить, что образы среды предустановки включают минимальный комплект компонентов Windows — а именно, только компоненты, которые необходимы для запуска компьютера и его подготовки к установке. Среда восстановления (Windows RE) отличается от стандартной конфигурации Windows PE только тем, что включает в себя дополнительные компоненты, используемые для восстановления и запуска процесса устранения неполадок.

Настройка образа Windows PE

При помощи DISM можно настроить подключенный загрузочный или установочный образ. Работа с подключенным образом осуществляется при помощи команд DISM/image. В табл. 2-1 перечислены параметры DISM, используемые для обслуживания образов Windows PE. Также при работе с Windows PE можно использовать и другие параметры, указанные в табл. 2-4 и 2-5.

Табл. 2-1. Основные параметры DISM, применяемые при работе с образами Windows PE

Параметр	Описание	Пример
/Get-PESettings	Отображает список настроек Windows PE в подключенном образе. В список включаются текущее состояние профилирования, параметры рабочей области и целевого пути	Dism /image:C:\winpe_x86\mount /Get-PESettings
/Get-Profiling	Отображает состояние профилирования	Dism /image:C:\winpe_x86\mount /Get-Profiling
/Get-ScratchSpace	Отображает настроенную рабочую область системного тома Windows PE, то есть доступное для записи пространство на системном томе Windows PE при загрузке с виртуального диска	Dism /image:C:\winpe_x86\mount /Get-ScratchSpace
/Get-TargetPath	Отображает целевой путь к образу Windows PE, то есть путь к корню образа Windows PE во время загрузки	Dism /image:C:\winpe_x86\mount /Get-TargetPath
/Set-ScratchSpace:Size	Задает объем рабочей области в мегабайтах. Допустимые значения — 32, 64, 128, 256 и 512	Dism /image:C:\winpe_x86\mount /Set-ScratchSpace:256

Табл. 2-1. (*окончание*)

Параметр	Описание	Пример
/Set-TargetPath:Path	При загрузке на жесткий диск этот параметр указывает местоположение образа Windows PE на диске. Путь должен начинаться с буквы (от C до Z); после буквы должно быть указано сочетание символов :\	Dism /image:C:\winpe_x86\mount /Set-TargetPath:X:\
/Enable-Profiling	Включает профилирование для создания собственных профилей. По умолчанию профилирование отключено	Dism /image:C:\winpe_x86\mount /Enable-Profiling
/Disable-Profiling	Отключает профилирование	Dism /image:C:\winpe_x86\mount /Disable-Profiling
/Apply-Profiles:Path	Применяет профиль и удаляет файлы, которые не используются в пользовательском профиле. Важные для загрузки файлы не удаляются. Образ Windows PE, измененный при помощи любого профиля, не обслуживается	Dism /image:C:\winpe_x86\mount /Apply-Profiles:C:\profiles\prof.txt

Если вы подключаете образ при помощи команды:

```
imagex /apply c:\winpe_x86\iso\sources\boot.wim 1 c:\winpe_x86\mount\
```

то будете работать с ним через точку подключения:

```
c:\winpe_x86\mount\
```

У всех образов Windows PE имеются следующие настройки:

- **Состояние профилирования** Указывает, включено или выключено профилирование.
- **Пространство рабочей области** Указывает объем рабочей области Windows PE, например 32 Мб.
- **Целевой путь** Указывает конечный путь при загрузке образа Windows PE, например, X:\.

Для просмотра настроек подключенного образа введите команду:

```
dism /image:ПутьОбраза /Get-PESettings
```

где *ImagePath* — путь к подключенному образу, например:

```
dism /image:c:\winpe_x86\mount\ /get-pesettings
```

По умолчанию Windows PE выделяет в качестве рабочей области 32 Мб памяти. Объем рабочей области можно увеличить до 512 Мб, введя в командной строке:

```
dism /image:ПутьОбраза /Set-ScratchSpace:Размер
```

где *ПутьОбраза* — путь к подключенному образу, а *Размер* — объем рабочей области в мегабайтах. Допустимые значения параметра *Размер* — 32, 64, 128, 256 и 512. Ниже приводится пример, в котором устанавливается размер рабочей области 128 Мб:

```
dism /image:c:\winpe_x86\mount\ /Set-ScratchSpace:128
```

Если вы планируете использовать профилирование или запускать в среде предустановки нестандартные приложения, объем рабочей области рекомендуется увеличить. Если Windows PE будет недостаточно памяти, приложения могут перестать отвечать на запросы.

Работая с образами Windows PE, вы можете воспользоваться и другими возможностями. Например, чтобы получить информацию обо всех установленных драйверах, введите следующую команду:

```
dism /image:c:\winpe_x86\mount\ /get-drivers /all
```

Примечание Если параметру DISM требуется значение, введите после имени параметра двоеточие и затем укажите требуемое значение. Между двоеточием и значением пробел не ставится.

Чтобы добавить драйвер к образам Windows PE, используйте команду /Add-Driver. Ее базовый синтаксис таков:

```
dism /image:ТочкаПодключения /add-driver /Driver:ПутьInf
```

где *ТочкаПодключения* — путь к месту подключения образа, а *ПутьInf* — путь к файлу .inf драйвера, например:

```
dism /image:c:\winpe_x86\mount\ /add-driver /driver:c:\drivers\remmedia\rem.inf
```

Если в общей папке есть вложенные папки с драйверами, которые нужно добавить, рекурсивный поиск в базовой папке можно задать, используя следующий синтаксис:

```
dism /image:ТочкаПодключения /add-driver /driver:БазоваяПапка /recurse
```

где *ТочкаПодключения* — путь к месту подключения образа, а *БазоваяПапка* — папка, где проводится поиск драйверов, например:

```
dism /image:c:\winpe_x86\mount\ /add-driver /driver:c:\drivers /recurse
```

Совет На компьютерах x64 и Itanium по умолчанию необходимо использовать подписанные драйверы. Чтобы DISM принял неподписанные драйверы, добавьте параметр /ForceUnsigned.

Чтобы добавить приложения в образ Windows PE, воспользуйтесь командой Copy или Xcopy, чтобы скопировать необходимые файлы в соответствующую папку. Например, файл Imagex.exe можно скопировать в корневую папку образа при помощи команды:

```
xcopy «C:\Program Files\Windows AIK\Tools\x86\Imagex.exe» c:\winpe_x86\mount\
```

Информацию о пакетах, установленных в образе Windows PE, вы получите при помощи параметра /Get-Packages. Его базовый синтаксис таков:

```
dism /image:ТочкаПодключения /get-packages
```

Например:

```
dism /image:c:\winpe_x86\mount\ /get-packages
```

Чтобы добавить пакеты, используйте параметр /Add-Package. Пакеты, доступные для установки, перечислены в табл. 2-2. Базовый синтаксис при добавлении пакетов таков:

```
dism /image:MountPoint /add-package /PackagePath:PathtoCab
```

Например:

```
dism /image:C:\winpe_x86\mount /Add-Package /PackagePath:"C:\Program Files\
Windows AIK\Tools\PETools\x86\WinPE_OCs\winpe-wmi.cab"
```

Табл. 2-2. Основные пакеты Windows PE

Имя пакета	Описание
WinPE-FONTSupport-*Язык*.cab	Устанавливает шрифты для указанного языка: ja-jp, ko-kr, zh-cn, zh-hk или zh-tw
WinPE-HTA.cab	Устанавливает поддержку HTML-приложений
WinPE-LegacySetup.cab	Устанавливает пакет установки прежних версий
WinPE-MDAC.cab	Устанавливает поддержку компонентов доступа к данным Майкрософт
WinPE-Scripting.cab	Устанавливает поддержку сервера сценариев Windows
WinPE-Setup-Client.cab	Устанавливает пакет установки клиента (после установки основного пакета установки)
WinPE-Setup.cab	Устанавливает основной пакет установки
WinPE-Setup-Server.cab	Устанавливает пакет установки сервера (после установки основного пакета установки)
WinPE-SRT.cab	Устанавливает компонент среды восстановления Windows (только для Windows OPK)
WinPE-WDS-Tools.cab	Устанавливает пакет инструментов служб развертывания Windows
WinPE-WMI.cab	Устанавливает поддержку инструментария управления Windows (WMI)

В базовом образе Windows PE есть не все пакеты, перечисленные в таблице. Для установки дополнительных пакетов воспользуйтесь инструментом DISM. Пакеты находятся в папке \Windows OPK\Tools\PETools*ПроцТип* или в папке \Windows AIK\Tools\PETools*ПроцТип*, где *ПроцТип* — тип процессора (amd64, ia64 или x86). При установке поддержки дополнительных языков убедитесь, что нужный язык установлен на клиентском компьютере. Языковые ресурсы для конкретного языка находятся в подпапке папки \Windows OPK\Tools\PETools*ПроцТип* или \Windows AIK\Tools\PETools*ПроцТип* .

После установки языковой поддержки при помощи параметра /Set UILang можно указать язык интерфейса пользователя. Например, если вы хотите пользоваться английским языком, введите команду:

```
dism /image:c:\winpe_x86\mount /Set-UILang:en-US
```

Проверить настройки языка можно при помощи параметра /Get-Intl, например:

```
dism /image:c:\winpe_x86\mount /Get-Intl
```

После внесения всех изменений отключите образ и сохраните изменения. Базовый синтаксис таков:

```
imagex /unmount MountPath /commit
```

Например:

```
imagex /unmount c:\winpe_x86\mount /commit
```

Примечание Если вы отключите образ без параметра /commit, изменения будут утеряны.

Теперь у вас есть настроенный образ Windows PE. Чтобы заменить образ Windows PE по умолчанию в папке ISO новым пользовательским образом, введите следующую команду:

```
copy c:\winpe_x86\boot.wim c:\winpe_x86\ISO\sources\boot.wim
```

Запись образа

Когда пользовательский образ Windows PE готов, его нужно записать в WIM-файл при помощи следующей команды:

```
imagex /boot /capture c:\winpe_x86\mount c:\winpe_x86\iso\sources\boot.wim
«Primary WinPE Build»
```

В данном примере параметр /Boot указывает, что образ загрузочный, а параметр /Capture задает запись содержимого папки C:\Winpe_x86\Mount и создает файл образа в папке C:\Winpe_x86\ISO\Sources. Строка «Primary WinPE Build» представляет собой описание загрузочного файла образа.

Примечание WIM-файлы могут быть загрузочными и установочными. Обычно загрузочные образы, используемые с Windows PE, хранятся в файлах Boot.wim, а установочные образы, применяемые для развертывания Windows, хранятся в файлах Install.wim. Файлы Install.wim могут содержать различные версии Windows. Стандартные дистрибутивы Windows 7 содержат и файл Boot.wim, и файл Install.wim. Файл Boot.wim загружает Windows PE для запуска компьютера и подготовки к установке. Файл Install.wim содержит образ Windows, необходимый для установки Windows 7.

Папка ISO/Sources — стандартная папка среды сборки для хранения образов Windows PE. В каталоге ISO есть вложенные папки Boot и EFI, которые требуются для создания загрузочного носителя. Создав загрузочный образ, вы можете создать загрузочный носитель или импортировать образ в службы развертывания Windows.

Оптимизация образа

Функция профилирования отслеживает необходимые компоненты образа и позволяет оптимизировать его. Чтобы воспользоваться профилированием, установите пакет WinPE-WMI и включите функцию профилирования в образе Windows PE при помощи параметра /Enable-Profiling. При включенном профилировании ведется запись всех файлов и компонентов, используемых вами при загрузке образа Windows PE.

После загрузки образа Windows PE протестируйте все компоненты, которые будете использовать. Соответствующие файлы будут занесены в журнал профиля, как используемые. Сохранить профиль перед завершением сессии Windows PE можно при помощи команды Wpeutil SaveProfile. Ее базовый синтаксис таков:

```
wpeutil saveprofile Путь «Описание»
```

где *Путь* — путь к папке, где будет храниться профиль, а *Описание* — его описание, например:

```
wpeutil saveprofile x:\st-profile.txt «Optimization Profile»
```

Затем следует подключить образ и применить профиль. Базовый синтаксис для применения профиля таков:

```
dism /image:ПутьОбраза /apply-profiles:ПутьПрофиля
```

где *ПутьОбраза* — путь к подключенному образу, а *ПутьПрофиля* — путь к профилю, который вы хотите применить для оптимизации образа, например:

```
dism /image:c:\winpe_x86\mount\ /apply-profiles:c:\st-profile.txt
```

После оптимизации отключите образ и сохраните изменения. Обратите внимание, что применение профиля отключает компоненты профилирования и отмечает образ, поэтому он больше не обслуживается.

Создание загрузочного образа ISO и загрузочных носителей

Для создания ISO-образа, который можно записать на DVD, воспользуйтесь утилитой Oscdimg. Для образов с одной загрузочной записью используются следующие параметры:

- *–bФайлЗагрузки*, где *ФайлЗагрузки* — файл, который будет записан в загрузочных секторах диска.
- *–pIDПлатформы*, где *IDПлатформы* имеет значение 0 для платформ BIOS, и значение EF для платформ EFI. По умолчанию принимается значение 0.
- *–e* отключает эмуляцию гибких дисков. Это обычно нужно, если используется параметр *–p*.

Следующая команда создает ISO-образ для созданного ранее образа:

```
oscdimg -n -bc:\winpe_x86\etfsboot.com c:\winpe_x86\iso c:\winpe_x86\winpe.iso
```

Здесь C:\Winpe_x86\Etfsboot.com — путь к загрузочному файлу, который будет записан в загрузочном секторе, C:\Winpe_x86\ISO — путь к папкам ISO-образа, а C:\Winpe_x86\Winpe.iso — путь к папке, где будет создан ISO-образ. После создания ISO-образа его можно записать на DVD при помощи программы записи на CD/DVD, например Roxio Media Creator или Nero Media Burner.

Для создания мультизагрузочных образов, которые требуются для систем на базе EFI, воспользуйтесь параметром –bootdata. Базовый синтаксис таков:

```
-bootdata:ЧислоЗаписей#Записьпоумолчанию#Запись2#...#ЗаписьN
```

где *ЧислоЗаписей* указывает на количество загрузочных записей, записи отделены друг от друга символом #, а параметры загрузочной записи разделены запятыми. Параметры загрузочной записи в порядке использования таковы:

- p*IDПлатформы*, где *IDПлатформы* имеет значение 0 для платформ на базе BIOS, и значение EF для платформ на базе EFI$;
- e — отключить эмуляцию гибких дисков;
- b*ФайлЗагрузки*, где *ФайлЗагрузки* — файл, который будет записан в загрузочных секторах диска.

Чтобы создать ISO-образ Windows PE x64, поддерживающий системы на базе EFI и BIOS, введите следующую команду:

```
oscdimg "-bootdata:2#p0,e,betfsboot.com#pEF,e,befisys.bin -u2 -udfver102
-o c:\winpe_x64\ISO c:\winpe_x64\winpe_2X.iso"
```

Здесь –bootdata задает загрузочную информацию для EFI и BIOS, а –UDFVer указывает требуемую версию UDF. В качестве пути к папкам для создания ISO-образа указывается путь C:\Winpe_x64\ISO, а сам ISO-образ будет создан в папке C:\Winpe_x64\Winpe_2X.iso. Создав ISO-образ, запишите его на DVD при помощи программы записи.

Примечание По умолчанию используется версия UDF 1.5. Параметр –udfver102 обозначает формат UDF 1.02, поддерживаемый Windows 98 и более поздними системами; параметр –udfver150 соответствует формату UDF 1.50, поддерживаемому Windows 2000 и более поздними системами, а параметр –udfver200 указывает на формат UDF 2.00, поддерживаемый Windows XP и более поздними системами.

Создание загрузочного флеш-накопителя

Загрузочные образы Windows PE можно создать на флеш-накопителе, если его объем позволяет сохранить образ целиком. Возможно, вам придется разрешить загрузку с USB-устройства в микропрограммном коде. Более подробная информация о настройках микропрограмм — в главе 10.

Для создания загрузочного USB-накопителя вставьте устройство в USB-порт, затем подготовьте его при помощи инструмента DiskPart, выполнив следующие команды:

1. В административной командной строке введите diskpart, а затем list disk. Обратите внимание на номер диска и размер USB-накопителя.
2. Введите **select disk *n***, где *n* — устройство, которое вы подготавливаете.
3. Введите **clean** для удаления всей информации на устройстве.
4. Введите **create partition primary size=*размер***, где *размер* — объем в мегабайтах указанного USB- устройства.
5. Введите **select partition 1** для выбора раздела диска, который вы только что создали, затем введите **active**, чтобы сделать новый раздел активным.
6. Введите **format fs=fat32**, чтобы отформатировать раздел в системе FAT32.
7. Введите **assign**, чтобы назначить USB-устройству следующую доступную букву диска. Затем введите **exit**, чтобы выйти из DiskPart. Не выходите из командной строки.
8. Запишите новый загрузочный сектор на USB-накопитель, введя команду **bootsect /nt60 e: /force**, где *e:* — буква накопителя.

Примечание Утилита Bootsect находится в папках образа PeTools\x86 и PeTools\amd64. Используйте версию Bootsect, которая поддерживает создаваемый вами образ Windows PE.

9. Скопируйте содержимое папки ISO на USB-накопитель, введя **xcopy /echry c:\winpe_x86\iso*.* e:**.

Завершив копирование, извлеките USB-устройство. Теперь оно является загрузочным носителем Windows.

Примечание На некоторых USB-накопителях описанный выше процесс подготовки провести нельзя. Такое устройство нельзя будет сделать загрузочным. Подобные устройства обычно опознаются системой как съемные носители, а не как USB-диски. Попробуйте найти информацию о форматировании в документации на веб-сайте производителя.

Загрузка из образа на жестком диске

Загружая Windows PE в ОЗУ с жесткого диска, вы можете обновить установку Windows 7: заново создать дисковые разделы и установить новый образ Windows. Также можно использовать Windows PE в качестве среды восстановления Windows.

Для загрузки Windows PE с жесткого диска выполните следующие действия:

1. Загрузите компьютер при помощи подготовленного дистрибутива Windows PE.
2. В командной строке введите **diskpart**, а затем **list disk**. Запомните номер основного диска. Обычно ему присваивается номер 0.
3. Введите **select disk *n***, где *n* — номер основного диска.
4. Введите **clean** для удаления всей информации на диске.
5. Введите **create partition primary size=*размер***, где *размер* (в мегабайтах) — объем раздела, достаточный для хранения исходных файлов Windows PE.
6. Введите **select partition 1**, чтобы выбрать только что созданный раздел диска, и введите **active**, чтобы сделать новый раздел активным.
7. **Введите format fs=fat32**, чтобы отформатировать раздел в системе FAT32.
8. Введите **exit** для выхода из DiskPart. Не выходите из командной строки.
9. Запишите на диск новый загрузочный сектор, введя команду **bootsect /nt60 c:**, где *c:* — буква основного диска, который вы форматировали.

Примечание Утилита Bootsect находится в папках образа PeTools\x86 и PeTools\amd64. Используйте версию Bootsect, которая поддерживает создаваемый вами образ Windows PE.

10. Скопируйте содержимое папки ISO на диск, введя **xcopy /echry x:*.* c:**.

Включение образа Windows PE в службы развертывания Windows

После установки служб развертывания Windows в сети, в них можно добавить образ Windows PE, чтобы облегчить его установку. Выполните следующие действия:

1. На сервере или компьютере, где запущены службы развертывания Windows, запустите консоль служб развертывания. Щелкните кнопку **Пуск (Start)**, выберите **Все программы (All Programs)**, **Администрирование (Administrative Tools)** и щелкните команду **Службы развертывания Windows (Windows Deployment Tools)**.
2. В консоли служб развертывания раскройте узел **Серверы (Servers)** и выберите сервер, с которым хотите работать. Правой кнопкой мыши щелкните папку **Образы загрузки (Boot Images)** и выберите команду **Добавить образ загрузки (Add Boot Image)**.
3. На странице **Файл образа (Image File)** введите путь к образу Windows PE и щелкните **Открыть (Open)**.
4. На странице **Метаданные образа (Image Metadata)** введите имя и описание образа и щелкните **Далее (Next)**.
5. На странице **Отчет (Summary)** щелкните **Далее (Next)**, чтобы добавить образ к службам развертывания Windows. После завершения операции импорта щелкните **Готово (Finish)**.

Среда восстановления Windows

Среда восстановления Windows (Windows RE) — это образ предустановочной среды Windows PE с установленными дополнениями, предназначенными для восстановления системы. После создания и настройки образа Windows RE его можно развернуть, создав загрузочный носитель или импортировав образ в службы развертывания Windows.

Чтобы обеспечить максимально быстрое восстановление, Windows RE автоматически устанавливается вместе с Windows 7. Обычно Windows RE настраивается в отдельном разделе жесткого диска, отличном от раздела, где устанавливается Windows. Благодаря этому Windows RE отделена от ОС.

Создание собственного образа Windows RE

В Windows 7 пользователи могут инициировать восстановление при помощи образа, не запуская Windows RE вручную. Панель управления среды восстановления позволяет пользователям создать резервную копию личных данных и затем перезагружает систему в среде восстановления Windows, где автоматически запускается приложение восстановления образа.

Чтобы создать собственный образ Windows RE, выполните следующие действия:

1. Щелкните **Пуск (Start)**, выберите **Все программы (All Programs)** и **Microsoft Windows OPK**, **Microsoft Windows AIK** или **Microsoft Windows PE**.
2. Запустите командную строку средств развертывания от имени администратора.
3. Чтобы создать папки для подключения образа, последовательно введите следующие команды:
   а) Введите **c:**, затем **mkdir c:\win7**.
   б) Введите **cd win7**, затем **mkdir mount**. Папка mount используется для подключения образа Windows 7.
   в) Введите **mkdir mountre**. Эта папка используется для подключения среды восстановления Windows.
4. Вставьте дистрибутив Windows 7 в дисковод DVD-ROM и скопируйте образ установки Windows на жесткий диск, введя **copy e:\sources\install.wim c:\win7**, где e: — буква, обозначающая дисковод DVD-ROM.
5. Подключите образ Windows 7 при помощи команды **imagex /mountrw e:\sources\install.wim c:\win7\mount**.
6. Скопируйте исходный образ Windows RE из подключенного образа при помощи команды **copy c:\sources\mount\windows\system32\recovery\winre.wim c:\win7**.
7. Отключите образ Windows 7, введя **imagex /unmount c:\win7\mount**.
8. Подключите образ Windows RE, введя **imagex /mountrw c:\win7\winre.wim c:\win7\mountre**.

9. Настройте образ Windows RE, как описано выше в разделе «Настройка образа Windows PE». Обязательно добавьте в образ пакет WinPE-SRT-Package.
10. Отключите настроенный образ Windows RE с сохранением изменений при помощи команды **imagex /unmount /commit c:\win7\mountre**.
11. Подключите образ Windows 7, скопированный ранее в папку C:\Win7, при помощи команды **imagex /mountrw c:\win7\install.wim c:\win7\mount**.
12. Сохраните настроенный образ Windows RE поверх исходного образа Windows RE при помощи **copy c:\win7\winre.wim c:\win7\mount\Windows\System32\recovery**.
13. Сохраните изменения в образе Windows 7, введя **imagex /unmount c:\win7\mount /commit**.

Теперь у вас имеется загрузочный образ Windows RE в файле C:\Win7\Winre.wim и дистрибутив Windows 7, в котором содержится образ Windows RE. При помощи файла C:\Win7\Winre.wim можно создать носитель среды восстановления Windows, как описано в следующем разделе.

Создание носителя Windows RE для восстановления системы

Настроив пользовательский образ Windows RE, создайте загрузочные образы Windows RE на CD-ROM, DVD-ROM или USB-накопителе. Если компьютер не запускается, его можно запустить при помощи носителя для восстановления системы, а затем устранить неполадки. Процедура создания носителя для восстановления системы не отличается от процедуры создания образов Windows PE. Основное отличие — ISO-образ создается из образа Windows RE , а не Windows PE.

Чтобы создать среду сборки Windows RE на 32-разрядном компьютере, выполните следующие действия:

1. Щелкните **Пуск (Start)**, выберите **Все программы (All Programs)** и **Microsoft Windows OPK**, **Microsoft Windows AIK** или **Microsoft Windows PE**.
2. Запустите командную строку средств развертывания от имени администратора.
3. В командной строке введите **copype x86 c:\winrec_x86**.

Так создается среда сборки для WIndows RE на 32-разрядных компьютерах. При необходимости можно также создать среду сборки для компьютеров на базе x-64 и Itanium.

Создав среду сборки, создайте среду Windows RE, как описано выше в разделе «Создание собственного образа Windows RE». Затем скопируйте образ Windows RE в среду сборки, введя следующую команду:

```
copy c:\win7\winre.wim c:\winrec_x86\ISO\sources\boot.wim
```

Файл образа Windows RE необходимо назвать Boot.wim. Это гарантирует возможность загрузки компьютеров при помощи этого образа.

Для создания ISO-образа, который можно записать на DVD, воспользуйтесь утилитой Oscdimg. Следующая команда создает ISO-образ для созданного ранее образа Windows RE:

```
oscdimg -n -bc:\winrec_x86\etfsboot.com c:\winrec_x86\iso c:\winrec_x86\
winrec.iso
```

Здесь C:\Winrec_x86\Etfsboot.com — путь к сценарию Etfsboot.com, который нужен для создания ISO-образа, C:\Winrec_x86\ISO — путь к папкам для ISO-образа, а C:\Winrec_x86\Winrec.iso — путь и имя файла создаваемого ISO-образа. Создав ISO-образ, запишите его на DVD при помощи программы записи на CD/DVD, например Roxio Media Creator или Nero Media Burner.

Чтобы создать ISO-образ Windows RE с поддержкой EFI и BIOS для 64-разрядного компьютера, введите команду:

```
oscdimg "-bootdata:2#p0,e,betfsboot.com#pEF,e,befisys.bin -u2 -udfver102 -o
c:\winrec_x64\ISO c:\winrec_x86\winrec_2X.iso"
```

Здесь параметр –bootdata задает использование загрузочной информации как для EFI, так и для BIOS, а параметр –UDFVer указывает требуемую версию UDF. В качестве пути к папкам для создания ISO-образа указывается путь C:\Winrec_x64\ISO, а сам ISO-образ будет создан в папке C:\Winrec_x64\Winrec_2X.iso.

Загрузочные образы Windows RE можно также создавать и на USB-накопителе. Процедура та же, что описана выше в разделе «Создание загрузочного флеш-накопителя», только вместо копирования образа Windows PE необходимо будет скопировать образ Windows RE.

Включение образа Windows RE в службы развертывания Windows

После установки служб развертывания Windows в сети, в них можно добавить образ Windows RE, чтобы облегчить его установку. Выполните следующие действия:

1. На сервере или компьютере, где запущены службы развертывания Windows, запустите консоль служб развертывания. Щелкните кнопку **Пуск (Start)**, выберите **Все программы (All Programs)**, **Администрирование (Administrative Tools)** и щелкните команду **Службы развертывания Windows (Windows Deployment Tools)**.
2. В консоли служб развертывания раскройте узел **Серверы (Servers)** и выберите сервер, с которым хотите работать. Правой кнопкой мыши щелкните папку **Образы загрузки (Boot Images)** и выберите команду **Добавить образ загрузки (Add Boot Image)**.
3. На странице **Файл образа (Image File)** введите путь к образу Windows RE и щелкните **Открыть (Open)**.
4. На странице **Метаданные образа (Image Metadata)** введите имя и описание образа и щелкните **Далее (Next)**.

5. На странице **Отчет (Summary)** щелкните **Далее (Next)**, чтобы добавить образ к службам развертывания Windows. После завершения операции импорта щелкните **Готово (Finish)**.

Развертывание Windows с пользовательской средой восстановления

Среда Windows RE включена в Windows 7. При развертывании компьютера Windows можно настроить образ восстановления, создав на диске раздел восстановления, скопировав образ восстановления в этот раздел и затем создав связь между образом восстановления и установкой Windows 7.

Образ Windows RE можно установить на GPT-диски (диски с GUID-таблицей разделов) с атрибутом PARTITION_MSFT_RECOVERY_GUID и на MBR-диски (диски с основной загрузочной записью) типа 0x7 или 0x27. На дисках 0x27 раздел восстановления должен находиться в начале диска. Раздел для Windows RE должен быть основным разделом в формате NTFS на том же диске, что и раздел с установкой Windows.

Раздел восстановления может совпадать с системным разделом, но лучше иметь два отдельных раздела. Объем раздела восстановления должен быть достаточным для образа восстановления. Чтобы определиться с объемом, посмотрите на размер настроенного образа установки Windows 7. При полноценном образе для раздела восстановления обычно требуется от 9 до 10 Гб.

Чтобы создать раздел восстановления на компьютере с MBR-дисками, выполните следующие действия:

1. Запустите компьютер при помощи загрузочного носителя Windows PE. Среда предустановки, которую вы загружаете, должна содержать пакет WinPE-SRT. Обычно этот пакет доступен только в версии Windows OPK.
2. В командной строке Windows PE введите **diskpart**, а затем **list disk**. Посмотрите, какие диски доступны, и отметьте их размер. На диске 0 должно быть достаточно места для раздела восстановления и раздела установки Windows.
3. Введите **select disk 0**. Затем введите **clean**, чтобы удалить всю информацию на диске.
4. Создайте системный раздел при помощи команды **create partition primary size=*размер***, где *размер* — объем системного раздела в мегабайтах, например size=250.
5. Отформатируйте системный раздел при помощи команды **format=fat32 label=«System» quick**. Сделайте системный раздел активным, введя **active**, затем присвойте ему букву S, введя **assign letter=s**.
6. Создайте раздел восстановления при помощи команды **create partition primary size=*размер* id=27**, где *размер* — объем раздела восстановления в мегабайтах, например size=1000, а значение id=27 означает, что создаваемый раздел восстановления является скрытым.

7. Для форматирования раздела в файловой системе NTFS введите **format=ntfs label=«Recovery» quick**.
8. Чтобы присвоить букву R разделу восстановления, введите **assign letter=r**.
9. Создайте раздел установки Windows при помощи команды **create partition primary size=*размер***, где *размер* — объем раздела установки в мегабайтах, например size=2000.
10. Отформатируйте раздел Windows при помощи команды **format=ntfs label=«Windows» quick**, затем присвойте разделу букву C: командой **assign letter=c**.
11. Введите **exit**, чтобы выйти из DiskPart. Не выходите из командной строки.

Чтобы создать раздел восстановления на компьютере с GPT-дисками, выполните следующие действия:

1. Запустите компьютер при помощи загрузочного носителя Windows PE. Среда предустановки, которую вы загружаете, должна содержать пакет WinPE-SRT. Обычно этот пакет доступен только в Windows OPK. Для компьютеров на базе UEFI запускать Windows PE нужно в режиме загрузки EFI в оболочке EFI.
2. В командной строке введите **diskpart**, а затем **list disk**. Посмотрите, какие диски доступны, и отметьте их размер. На диске 0 должно быть достаточно места для раздела восстановления и раздела установки Windows.
3. Введите **select disk 0**. Затем введите **clean**, чтобы удалить всю информацию на диске. На компьютере с UEFI потребуется ввести команду **convert gpt**.
4. Создайте системный раздел EFI при помощи команды **create partition efi size=*размер***, где *размер* — объем системного раздела EFI в мегабайтах, например size=200.
5. Отформатируйте системный раздел EFI, введя **format=fat32 label=«System» quick**. Затем присвойте разделу букву S: командой **assign letter=s**.
6. Создайте раздел MSR при помощи команды **create partition msr size=*размер***, где *размер* — объем раздела MSR в мегабайтах, например size=128.
7. Создайте раздел восстановления при помощи команды **create partition primary size=*размер***, где *размер* — объем раздела восстановления в мегабайтах, например size=1000.
8. Пометьте раздел как раздел восстановления при помощи команды **set id=«de94bba4-06d1-4d40-a16a-bfd50179d6ac»**.
9. Отформатируйте раздел восстановления, введя **format=ntfs label=«Recovery» quick**, затем присвойте разделу букву R: командой **assign letter=r**.
10. При помощи команды **create partition primary** создайте раздел установки Windows. Поскольку вы не указали размер раздела, он займет все оставшееся место на диске.

11. Для форматирования раздела в файловой системе NTFS введите **format=ntfs label=«Windows» quick**.
12. Чтобы присвоить разделу Windows букву C, введите **assign letter=c**.
13. Введите **exit** для выхода из DiskPart. Не выходите из командной строки.

Теперь, когда вы сконфигурировали жесткие диски компьютера, можно начать развертывание Windows. Один из способов развертывания Windows представлен ниже:

1. Вставьте носитель с образом или подключитесь по сети к ресурсу, содержащему образ Windows 7.
2. Воспользуйтесь командой ImageX, чтобы применить образ Windows 7. Например, если образ установки записан на диске E, введите **imagex /apply e:\images\install.wim 1 c:**.
3. Для копирования системных файлов в системный раздел и обновления хранилища данных конфигурации используйте команду BCDBoot. Введите **cd c:\windows\system32**, а затем **bcdboot c:\windows /l en-us /s s:**. Параметр /l указывает на регион. Параметр /s указывает букву системного раздела.
4. Скопируйте образ Windows RE в раздел 1. Например, если образ записан на диске E, введите **copy e:\images\winre.wim r:**.
5. Создайте связь между образом Windows RE и установкой Windows 7 при помощи утилиты Reagentc.exe. Например, введите **reagentc.exe /setreimage /path r:**.

Совет Вы вольны настроить клавишу или кнопку так, чтобы при ее нажатии во время загрузки системы запускалась Windows RE. Чтобы запрограммировать клавишу или кнопку, включите в командную строку утилиты Reagentc.exe параметр /Bootkey, например **reagentc.exe /setreimage /path r: /bootkey *КодКнопки***, где *КодКнопки* — четырехзначный шестнадцатеричный код клавиши или кнопки.

Примечание Обычно установка Windows RE завершается, когда ее завершает пользователь. Если перед завершением установки вам необходимо запустить компьютер в режиме аудита и вы не подготавливаете установку заново при помощи средства Sysprep, вы можете завершить установку Windows RE в режиме аудита. В командной строке введите **reagentc.exe /enable /auditmode**.

Другой способ развертывания Windows — использование отдельных образов для каждого раздела. Допустим, вы записали отдельные образы, выполнив следующие действия:

1. Запустите компьютер при помощи загрузочного носителя Windows PE. Для компьютеров на базе UEFI запускать Windows PE нужно в режиме загрузки EFI в оболочке EFI.
2. В командной строке Windows PE введите **diskpart**, затем **list disk 0**, затем **list volume**. Проверьте информацию о разделе. Если одному из разделов, которые вы хотите записать, не присвоена буква, выберите том и назначьте букву. Например, если раздел восстановления является томом 0 и не имеет буквы, введите **select volume 0** и **assign letter=r**.

3. Чтобы попасть в папку с утилитой ImageX, введите **cd c:\windows\system32**.
4. Запишите образы для каждого настроенного раздела. Например, если у вас имеются отдельные раздел Windows, системный раздел и раздел восстановления, воспользуйтесь следующими командами:

```
imagex /capture c:\ c:\win-partition.wim «Windows partition»

imagex /capture s:\ c:\sys-partition.wim «System partition»

imagex /capture r:\ c:\rec-partition.wim «Recovery partition»
```

5. Подключитесь к общему ресурсу с дистрибутивом при помощи команды Net Use, например **net use Z: \\ImageShare\Images**. Скопируйте WIM-файлы на общий ресурс при помощи команд:

```
copy c:\win-partition.wim Z:\

copy c:\sys-partition.wim Z:\

copy c:\rec-partition.wim Z:\
```

Чтобы применить отдельные образы, выполните следующие действия:

1. Запустите компьютер при помощи загрузочного носителя Windows PE. Для компьютеров на базе UEFI запускать Windows PE нужно в режиме загрузки EFI в оболочке EFI.
2. Вставьте носитель с образом или подключитесь к сетевому ресурсу, содержащему образы, которые вы будете развертывать. К сетевому ресурсу можно подключиться при помощи команды Net Use, например **net use Z: \\ImageShare\Images**.
3. В командной строке Windows PE введите **diskpart**, затем **select disk 0**, затем **list volume**. Просмотрите информацию о разделе. Если одному из разделов, к которым вы хотите применить образ, не присвоена буква, выберите соответствующий том и назначьте букву. Например, если раздел восстановления является томом 0 и не имеет сопоставленной буквы, введите **select volume 0** и **assign letter=r**.
4. Чтобы попасть в папку с утилитой ImageX, введите **cd c:\windows\system32**.
5. При помощи ImageX примените образ Windows к разделу. Например, если образ установки записан на диске Z, введите **imagex /apply z:\win-partition.wim 1 c:**.
6. При помощи ImageX примените образ системного раздела. Например, если образ системного раздела записан на диске Z, введите **imagex /apply z:\sys-partition.wim 1 s:**.
7. При помощи ImageX примените образ раздела восстановления. Например, если образ раздела восстановления записан на диске Z, введите **imagex /apply z:\rec-partition.wim 1 r:**.

Создание образов Windows для развертывания

ОС Windows 7 основана на архитектуре Windows Vista, не зависящей от языковой среды и оборудования. В Windows 7 независимость от языка достигается при помощи модульной структуры компонентов, а независимость от оборудования достигается благодаря формату образов. В модульной структуре каждый компонент представляет собой небольшой независимый модуль, выполняющий определенную задачу или функцию. Благодаря этому компоненты ОС, от драйверов устройств до языковых пакетов и пакетов обновлений, могут создаваться отдельно друг от друга. Их можно подключить или отключить, настраивая «под себя» среду ОС.

Подробнее об образах Windows

Когда вы обновляете Windows 7, добавляя или удаляя компоненты, устанавливая исправления или пакеты обновлений, вы просто изменяете набор доступных модулей. Поскольку эти модули независимы друг от друга, производить изменения можно без воздействия на систему в целом. Благодаря тому что пакеты языков также являются отдельными модулями, вы легко примените различные конфигурации языков без необходимости отдельной установки Windows для каждого языка.

Корпорация Майкрософт распространяет Windows 7 на носителях с образами диска в формате WIM. В этом формате для уменьшения объема файлов используются сжатие и хранение единственной копии. Последнее означает, что для каждого файла в образе диска хранится только одна физическая копия. Поскольку WIM-файл независим от оборудования, Майкрософт достаточно было предоставить один двоичный файл для 32-разрядной архитектуры и один для 64-разрядной архитектуры. Для компьютеров на базе Itanium доступен собственный двоичный файл.

ОС Windows 7 можно установить как автоматически, так и интерактивно. Существует несколько способов автоматизировать установку Windows:

- **Создать файл ответов** В Windows 7 применяется стандартизированный файл ответов. Этот файл — Unattend.xml — создается в формате XML, что облегчает его обработку стандартными средствами. Создав пользовательский файл ответов и запустив затем программу Setup с этим файлом, вы автоматически установите Windows 7. Программа Setup способна устанавливать ОС с дистрибутива на общем ресурсе или с носителя.
- **Использовать установку из образа при помощи Sysprep** В этом случае требуется запустить утилиту командной строки SysPrep на компьютере, который используется в качестве образца для развертывания, а затем создать образ диска с конфигурацией этого компьютера. Утилита Sysprep находится в папке %SystemRoot%\System32\Sysprep. Чтобы облегчить применение Sysprep для развертывания, в пакет автоматической установки Windows (Windows AIK) включены диспетчер системных образов Windows и утилита ImageX. Диспетчер системных образов используется

для создания файла ответов, а ImageX — для создания образов дисков и управления ими.

Благодаря формату WIM и модульной структуре Windows 7, удается значительно сократить количество образов дисков, которые требуется поддерживать. Вам более не нужны образы для каждого набора оборудования или для каждого языка. Достаточно одного образа для каждого типа архитектуры, использующегося в вашей компании. Для настройки установки ОС можно, при необходимости, использовать различные сценарии установки.

Формат WIM имеет и другие преимущества по сравнению с другими форматами образов дисков. Он, например, позволяет обслуживать образы дисков автономно. То есть, можно добавить или удалить дополнительные компоненты или драйверы или произвести обновления без создания нового образа. Достаточно подключить образ диска как папку и затем при помощи проводника Windows или других программ обновлять, изменять или удалять файлы.

Диспетчер системных образов Windows, ImageX и Sysprep предоставляют несколько способов автоматизации развертывания. Ниже приведен список основных шагов:

1. Установите и настройте Windows 7 на компьютере, не используемом для повседневной работы. Затем установите и настройте необходимые компоненты и приложения.
2. Запустите Sysprep для подготовки компьютера к записи. Sysprep удаляет уникальные идентификаторы и назначает компьютер образцом для развертывания. После окончания процесса подготовки на компьютере не остается идентификаторов, которые позволяют входить в систему и работать в рамках домена или рабочей группы.
3. Чтобы захватить образ диска и сохранить на носителе или на общем ресурсе, воспользуйтесь командой ImageX /Capture. Образ можно обслуживать автономно: при помощи команды ImageX /Mountrw подключите образ с возможностью чтения и записи и внесите необходимые изменения. Для отключения образа после внесения изменений воспользуйтесь командой ImageX /Unmount.

   Можно также подключать образы при помощи команды DISM /Mount-WIM, а отключать их — при помощи команды DISM /Unmount-WIM. У DISM имеется также функциональность для управления образами. С ее помощью вы вольны задавать ключи продукта, выполнять обновления, добавлять или удалять драйверы, устанавливать язык и региональные параметры, добавлять или удалять пакеты и компоненты, а также очищать образы.
4. Для создания файла ответов воспользуйтесь диспетчером системных образов Windows. Затем можно создать сценарии развертывания, при помощи которых будет настраиваться компьютер, выполнить Setup с использованием файла ответов и применить ранее созданный образ диска.

5. Выполните сценарий развертывания для настройки компьютера и установки операционной системы.

Создание образа установки Windows

Основной инструмент для подготовки образов установки Windows — утилита Sysprep. Готовясь использовать Sysprep на любом компьютере, помните, что Sysprep удаляет уникальные идентификаторы с компьютера и назначает его образцом для развертывания. После окончания данного процесса на компьютере не остается идентификаторов, которые позволяют войти в систему и использовать компьютер в рамках домена или рабочей группы. После создания образа установки вам придется переустановить Windows и лишь потом опять пользоваться этим компьютером.

Во всех версиях Windows 7 утилита Sysprep находится в каталоге %SystemRoot%\System32\Sysprep. В табл. 2-3 приводится обзор ее основных параметров.

Примечание Все версии Windows 7 необходимо активировать в течение определенного периода времени, даже в случае многопользовательской активации при использовании серверов службы управления ключами. При первом использовании команды /Generalize утилита Sysprep запускает льготный период работы без активации, предоставляя 30 дней для активации системы после развертывания. После окончания льготного периода можно опять запустить Sysprep /Generalize, чтобы льготный период начался заново, что даст вам еще 30 дней для активации системы. Это можно сделать не более 3 раз. Однако применение команды /Generalize удаляет уникальные идентификаторы, точки восстановления и журналы событий.

Совет Если вы пользуетесь службой управления ключами (KMS), вернуть компьютер в исходное состояние активации можно при помощи сценария Slmgr.vbs и параметра –Rearm. Этот параметр заново запускает льготный период и инициализирует некоторые параметры активации, включая уникальный идентификационный код компьютера. Количество подобных перезапусков льготного периода зависит от того, сколько раз вы перед этим воспользовались Sysprep /Generalize. Больше трех раз запускать льготный период активации нельзя.

Табл. 2-3. Основные параметры утилиты Sysprep

Параметр	Описание
/Audit	Задает запуск компьютера в режиме аудита. В режиме аудита вы можете добавлять к ОС драйверы и приложения. Также в режиме аудита можно протестировать установку перед развертыванием
/Generalize	Подготавливает установку Windows перед созданием образа, удаляя уникальные системные идентификаторы. При этом идентификатор безопасности (SID) обнуляется, точки восстановления системы сбрасываются, журналы событий удаляются. Во время следующего запуска компьютера создается новый идентификатор безопасности (SID)

Табл. 2-3. (*окончание*)

Параметр	Описание
/Oobe	Задает запуск компьютера в режиме приветствия, который видят конечные пользователи после развертывания системы
/Reboot	Перезагружает компьютер
/Shutdown	Завершает работу компьютера после завершения работы программы Sysprep
/Quiet	Отключает отображение запросов на подтверждение во время работы программы Sysprep. Используйте этот параметр при автоматической работе Sysprep
/Quit	Закрывает Sysprep после выполнения указанных программ
/Unattend: *AnswerFile.xml*	Применяет во время автоматической установки настройки файла ответов. Здесь *AnswerFile.xml* — имя файла ответов

Для подготовки компьютера зайдите в систему, которую хотите настроить в качестве пользовательского образа, и используйте ее как основу для других образов. Настройте компьютер, изменяя параметры, устанавливая приложения и производя другие нужные изменения. После настройки компонентов компьютера используйте Sysprep для подготовки системы к использованию в качестве образа.

Утилиту Sysprep можно использовать как в режиме командной строки, так и в режиме графического интерфейса. При каждом использовании Sysprep утилита производит следующие действия:

- **Действие по очистке системы** Задает работу системы при следующей перезагрузке в режиме приветствия (OOBE) или в режиме аудита. Возможно также задать подготовку системы к использованию (параметр /generalize).
- **Параметры завершения работы** Вариант завершения работы после выполнения команды Sysprep: выход, перегрузка или завершение работы.

Чтобы запустить Sysprep, откройте окно командной строки от имени администратора и введите **cd %systemroot%\system32\sysprep**.

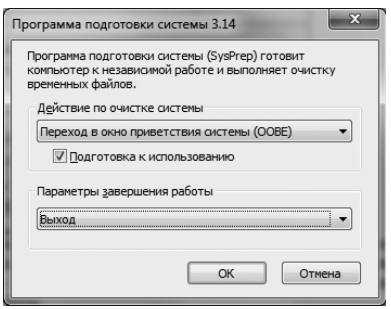

Рис. 2-1. Подготовка компьютера и установка режима приветствия системы

Чтобы подготовить систему к использованию в качестве образца и задать запуск в режиме приветствия при следующей загрузке, задайте параметры, показанные на рис. 2-1, или введите:

```
sysprep /oobe /generalize /quit
```

Если после подготовки компьютера при помощи параметра /generalize вы хотите установить дополнительные приложения и изменить параметры, настройте компьютер на запуск в режиме аудита, задав параметры, показанные на рис. 2-2, или введя команду:

```
sysprep /audit /generalize /reboot
```

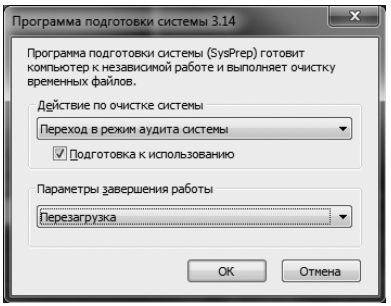

Рис. 2-2. Подготовка компьютера и установка режима аудита

Тогда можно произвести все необходимые изменения. Эти изменения будут записаны и применены при развертывании системы. После внесения всех изменений, завершите настройку операционной системы, задав выключение компьютера и запуск в режиме приветствия системы при следующей загрузке, задав параметры, показанные на рис. 2-3, или введя команду:

```
sysprep /oobe /shutdown
```

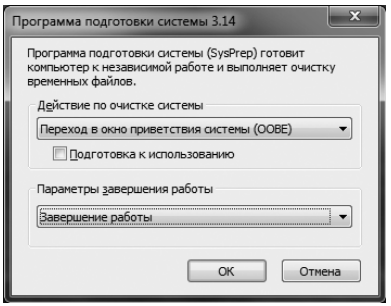

Рис. 2-3. После работы в режиме аудита установите следующий запуск в режиме приветствия системы и завершите работу

Теперь система готова к созданию образа. Вы можете импортировать образ в службы развертывания Windows или записать его и развернуть вручную. На службах развертывания Windows мы подробнее остановимся далее в этой главе. Для записи образа вручную выполните следующие действия:

1. Запустите компьютер при помощи загрузочного носителя Windows PE. Для компьютеров на базе UEFI запускать Windows PE нужно в режиме загрузки EFI в оболочке EFI.
2. В командной строке, запущенной от имени администратора, введите **diskpart** и **list disk**. Запомните номер диска, который будете использовать. Введите **select disk *n***, где *n* — номер этого диска.
3. Введите **list volume**. Просмотрите информацию о разделе. Если одному из разделов, которые вы хотите записать, не присвоена буква, выберите соответствующий том и присвойте ему букву. Например, если системный раздел является томом 1 и не имеет буквы, введите **select volume 1**, а затем введите **assign letter=s**.
4. Чтобы попасть в папку с утилитой ImageX, введите **cd c:\windows\system32**.
5. Запишите образы для каждого настроенного раздела. Если у вас имеются отдельно раздел Windows и системный раздел, введите следующие команды:

```
imagex /capture c:\ c:\win-partition.wim «Windows partition»

imagex /capture s:\ c:\sys-partition.wim «System partition»
```

6. Подключитесь к общему ресурсу с дистрибутивом при помощи команды Net Use, например **net use Z: \\ImageShare\Images**. Скопируйте WIM-файлы на общий ресурс при помощи команд:

```
copy c:\win-partition.wim Z:\

copy c:\sys-partition.wim Z:\
```

Теперь примените отдельные образы, выполнив следующие действия:

1. Запустите компьютер при помощи загрузочного носителя Windows PE. Для компьютеров на базе UEFI запускать Windows PE нужно в режиме загрузки EFI в оболочке EFI.
2. Вставьте носитель с образом или подключитесь к сетевому ресурсу, содержащему образы, которые вы будете развертывать. К сетевому ресурсу можно подключиться при помощи Net Use, например **net use Z: \\ImageShare\Images**.
3. В командной строке Windows PE введите **diskpart**, затем **select disk 0**, затем **list volume**. Просмотрите информацию о разделе. Если одному из разделов, которые вы хотите записать, не присвоена буква, выберите соответствующий том и присвойте ему букву. Например, если раздел восстановления является томом 0 и не имеет буквы, введите **select volume 0**, а затем введите **assign letter=r**.
4. Чтобы попасть в папку с утилитой ImageX, введите **cd c:\windows\system32**.

5. При помощи ImageX примените образ Windows к разделу. Например, если образ установки записан на диске Z, введите **imagex /apply z:\win-partition.wim 1 c:**.
6. При помощи ImageX примените образ системного раздела. Например, если образ системного раздела записан на диске Z, введите **imagex /apply z:\sys-partition.wim 1 s:**.
7. Перегрузите компьютер и войдите в систему.

Настройка и использование служб развертывания Windows

Службы развертывания Windows (Windows Deployment Services) применяются для развертывания Windows 7 по сети при помощи среды предзагрузочного выполнения (PXE). После настройки служб развертывания Windows вы можете установить Windows 7 на любой клиентский компьютер, поддерживающий PXE и загрузку по сети. Достаточно включить его в то время, когда он подключен к сети. Для клиентских компьютеров, не поддерживающих PXE, придется создать загрузочные диски при помощи утилиты Oscdimg, как описано выше.

Настройка служб развертывания Windows

Службы развертывания Windows выполняются в Windows Server 2008 и более поздних версиях в основном режиме, в котором поддерживаются только загрузочная среда Windows PE и файлы образов Windows. Сервер служб развертывания Windows должен быть контроллером или рядовым сервером домена Active Directory. Также в сети должны иметься работающие DHCP-сервер и DNS-сервер.

Для установки служб развертывания Windows на компьютер с Windows Server 2008 или более поздней версией выполните следующие действия:

1. Запустите Диспетчер сервера (Server Manager), щелкнув мышью соответствующую кнопку на панели быстрого запуска. В диспетчере сервера выберите узел **Роли (Roles)**, затем щелкните ссылку **Добавить роли (Add Roles)**, чтобы запустить мастер добавления ролей.
2. В первой странице мастера добавления ролей щелкните **Далее (Next)**. На странице **Выбор ролей сервера (Select Server Roles)** выберите **Службы развертывания Windows (Windows Deployment Services)** и щелкните **Далее (Next)**. Прочтите описание служб и опять щелкните **Далее (Next)**.
3. На странице **Выбрать службы роли (Select Role Services)** автоматически установлены флажки **Сервер развертывания (Deployment Server)** и **Транспортный сервер (Transport server)**. Вам потребуются обе роли. Щелкните **Далее (Next)** и затем **Установить (Install)**.

После установки служб развертывания Windows необходимо зарегистрировать сервер развертывания и настроить его, выполнив следующие действия:

1. Запустите консоль служб развертывания Windows, щелкнув кнопку **Пуск (Start)** и выбрав **Все программы (All Programs)**, **Администрирование (Administrative Tools)**, **Службы развертывания Windows (Windows Deployment Services)**.
2. В дереве консоли раскройте узел **Серверы (Servers)**. Если вы подключены к серверу развертывания, он должен быть автоматически указан в списке. Если сервера нет в списке, щелкните правой кнопкой узел **Серверы (Servers)** в дереве консоли и затем выберите **Добавить сервер (Add Server)**. В диалоговом окне **Добавить сервер (Add Server)** выберите сервер, который нужно добавить к консоли, и щелкните **ОК**.
3. В дереве консоли щелкните сервер правой кнопкой мыши и выберите **Настроить сервер (Configure Server)**. Когда запустится мастер настройки, просмотрите все задачи в начальном разделе и убедитесь, что сеть подготовлена должным образом. Вам необходим DHCP-сервер с активной областью и работающий DNS-сервер. Также необходимо, чтобы на сервере имелся раздел в формате NTFS.
4. На странице **Местонахождение папки удаленной установки (Remote Installation Folder Location)** введите путь к хранилищу образов и щелкните **Далее (Next)**. Указанный каталог должен быть разделом на диске в формате NTFS. В большинстве случаев, этот раздел должен быть отличен от системного. Если вы выберете каталог в системном разделе, щелкните **Да (Yes)** для подтверждения действия.
5. На странице настроек PXE-сервера задайте один из следующих параметров, чтобы определить, на запросы каких клиентов будет отвечать сервер:
   - **Не отвечать никаким клиентским компьютерам (Do not Respond to Any Client Computers)** Выберите этот вариант, если не хотите, чтобы сервер отвечал на запросы клиентских компьютеров.
   - **Отвечать только известным клиентским компьютерам (Respond Only to Known Client Computers)** Выберите этот вариант, если хотите, чтобы сервер отвечал на запросы только известных клиентских компьютеров (подготавливаются предварительно). Администратору перед загрузкой клиентского компьютера необходимо создать в Active Directory учетную запись, чтобы провести установку по сети.
   - **Отвечать всем (известным и неизвестным) клиентским компьютерам (Respond to All Client Computers)** Выберите этот вариант, если хотите, чтобы сервер отвечал на запросы как известных, так и неизвестных клиентов. Неизвестный клиент — это клиент, для которого не была создана учетная запись. По умолчанию, если вы разрешаете отвечать на запросы неизвестных клиентов, список учетных записей, которым разрешено устанавливать ОС, определяется параметрами

безопасности файла образа Windows. Права одобрения установки можно дать только администраторам, установив флажок **Если клиент неизвестен, уведомлять администратора и отвечать после утверждения (Require Administrator Approval For Unknown Clients)**.

6. Щелкните **Далее (Next)**, чтобы мастер начал настройку сервера. Когда вы щелкнете **Готово (Finish)**, укажите, хотите ли вы сразу же устанавливать образы. Чтобы загрузить клиентский компьютер с использованием протокола PXE и установить ОС, необходимо иметь на сервере как минимум один образ установки и один образ загрузки.
   - Если вы хотите сразу настроить образы, вставьте установочный носитель Windows 7 в DVD-ROM-дисковод и щелкните **Готово (Fi-nish).** Продолжите выполнение процедуры.
   - Если вы хотите настроить образы позднее, сбросьте флажок **Добавить образы (Add Image Files)**, затем щелкните **Готово (Finish)**. Дальнейшие шаги не выполняйте.
7. Запустится мастер добавления образов. На странице файла образа введите путь к корню установочного DVD-диска, содержащего образы, которые нужно добавить, например **E:**. Также путь можно задать при помощи кнопки **Обзор (Browse)**. Щелкните **Далее (Next)**.
8. Группа образов — это собрание образов с общим файловым ресурсом и параметрами безопасности. На странице **Группа образов (Image Group)** укажите имя первой группы образов, затем щелкните **Далее (Next)**. Мастер добавит с носителя загрузочный и установочный образ.

Совет Чтобы изменить способ реагирования сервера на запросы, в консоли служб развертывания Windows щелкните сервер правой кнопкой мыши и выберите команду **Свойства (Properties)**. В диалоговом окне **Свойства (Properties)** выберите способ ответа на запросы и щелкните **OK**.

Импорт образов

После настройки служб развертывания Windows вы можете импортировать любой доступный загрузочный или установочный образ, а затем использовать его для развертывания на клиентских компьютерах.

Загружаемые образы импортируются напрямую из исходных файлов Windows или из пользовательских загрузочных образов. Чтобы добавить загрузочный образ, выполните следующие действия:

1. На сервере или компьютере, где запущены службы развертывания Windows, откройте консоль служб развертывания, щелкнув кнопку **Пуск (Start)**, и выбрав команды **Все программы (All Programs)**, **Администрирование (Administrative Tools)** и **Службы развертывания Windows (Windows Deployment Tools)**.
2. Вставьте дистрибутивный диск Windows 7 или загрузочный образ в DVD-ROM-дисковод или откройте установочные файлы на сервере по сети.
3. В консоли служб развертывания Windows раскройте узел **Серверы (Ser-**

vers) и выберите сервер, с которым хотите работать. Правой кнопкой мыши щелкните папку **Образы загрузки (Boot Images)** и выберите команду **Добавить образ загрузки (Add Boot Image)**.

4. На странице **Файл образов (Image file)** введите путь к корневому каталогу установочного DVD-диска или щелкните кнопку **Обзор (Browse)**, чтобы выбрать образ загрузки. Затем щелкните **Открыть (Open)**. Например, если дистрибутив Windows находится на диске E:, укажите загрузочный образ по умолчанию — E:\Source\Boot.wim. Щелкните **Далее (Next)**.
5. На странице **Метаданные образа (Image Metadata)** введите имя и описание образа, затем щелкните **Далее (Next)**.
6. На странице **Сводка (Summary)** щелкните **Далее (Next)**, чтобы добавить образ к службам развертывания Windows. После завершения операции импорта щелкните **Готово (Finish)**.

Установочные образы можно импортировать напрямую из исходных файлов Windows. Выполните следующие действия:

1. На сервере или компьютере, где запущены службы развертывания Windows, запустите консоль служб развертывания, щелкнув кнопку **Пуск (Start)** и выбрав команды **Все программы (All Programs)**, **Администрирование (Administrative Tools)** и **Службы развертывания Windows (Windows Deployment Tools)**.
2. Вставьте дистрибутив Windows 7 в DVD-ROM-дисковод или откройте установочные файлы на сервере по сети.
3. В консоли служб развертывания Windows раскройте узел **Серверы (Servers)** и выберите сервер, с которым хотите работать. Правой кнопкой мыши щелкните папку **Образы установки (Install Images)** и выберите команду **Добавить группу образов (Add Image Group)**.
4. Введите имя группы образов и щелкните **ОК**. Будет создано хранилище групп образов.
5. Правой кнопкой мыши щелкните папку **Образы установки (Install Images)** и выберите команду **Добавить образ установки (Add Install Image)**. Выберите созданную ранее группу образов и щелкните **Далее (Next)**.
6. На странице **Файл образов (Image File)** щелкните **Обзор (Browse)**, выберите образ установки, затем щелкните **Открыть (Open)**. Например, если дистрибутив Windows находится на диске E, введите **E:\Source\Install.wim**. Затем щелкните **Далее (Next)**.
7. На странице **Список доступных образов (List of Available Images)** выберите образ для импорта и щелкните **Далее (Next)**.
8. На странице **Сводка (Summary)** щелкните **Далее (Next)**, чтобы добавить образ к службам развертывания Windows. После завершения операции импорта щелкните **Готово (Finish)**.

Установка Windows из образа

Для установки Windows при помощи служб развертывания выполните следующие действия:

1. Настройте микропрограмму компьютера на загрузку из сети и перегрузите компьютер.
2. При запуске компьютера и выводе на экран окна загрузчика нажмите F12, чтобы загрузить и запустить клиент служб развертывания Windows.
3. На странице служб развертывания Windows выберите языковой стандарт и раскладку клавиатуры. Затем щелкните **Далее (Next)**.
4. При появлении запроса на соединение с сервером служб развертывания Windows введите имя учетной записи и пароль. Затем щелкните **ОК**.
5. На странице **Выбор операционной системы для установки (Select The Operating System You Want To Install)** выберите образ для установки и щелкните **Далее (Next)**.
6. На странице **Выбор раздела для установки Windows (Where Do You Want To Install Windows)** выберите раздел для установки Windows и щелкните **Далее (Next)**. Если вы хотите заново разбить диск на разделы, прежде чем щелкнуть **Далее (Next)**, выберите **Настройка диска (дополнительно) (Drive Options (Advanced))**. Затем настройте разделы диска.
7. Программа Windows Setup установит Windows. Необходимые настройки, не указанные в файле ответов, будут запрашиваться в процессе установки.

Запись образов

Службы развертывания Windows используются как при развертывании пользовательских образов, так и при развертывании исходных образов из дистрибутивов Windows. При создании пользовательских загрузочных и установочных образов их можно импортировать, как описано выше, или записать.

Сначала необходимо записать образ загрузки, выполнив следующие действия:

1. В консоли служб развертывания Windows раскройте узел **Серверы (Servers)** и выберите сервер, с которым хотите работать. Затем, щелкните папку **Образы загрузки (Boot Images)**, чтобы вывести доступные образы загрузки.
2. Правой кнопкой мыши щелкните образ загрузки, который будет использоваться в качестве образа записи. Выберите команду **Создать образ загрузки записи (Create Capture Boot Image)**.
3. На странице **Метаданные образа записи (Capture Image Metadata)** введите имя и описание образа записи, затем местоположение и имя файла создаваемого образа, например C:\Images\Win_capture.wim.
4. Щелкните **Готово (Finish)**.

Для записи образа необходимо выполнить следующие действия:

1. При помощи служб развертывания Windows установите существующий образ на компьютер, как описано в разделе «Установка Windows из образа».
2. Настройте образ.
3. В командной строке введите **cd %systemroot%\system32\sysprep**, а затем **sysprep /oobe /generalize /reboot**.
4. При запуске компьютера и выводе на экран окна загрузчика нажмите F12 для загрузки и запуска клиента служб развертывания Windows.
5. В диспетчере загрузки Windows выберите образ загрузки для записи.
6. Когда запустится мастер записи образов служб развертывания Windows, щелкните **Далее (Next)**.
7. На странице **Исходный образ для записи (Image Capture Source)** выберите том или тома для записи в списке **Том для записи (Volume to Capture)**. Введите имя и описание файла. Щелкните **Далее (Next)**.
8. На странице **Назначение захвата образа (Image Capture Destination)** щелкните кнопку **Обзор (Browse)** и выберите местоположение для хранения образа записи. В поле **Имя файла (File Name)** введите имя файла с расширением .wim. Щелкните **Сохранить (Save)**.
9. Щелкните **Загрузить образ на сервер WDS (Upload Image To WDS Server)**. Введите имя сервера и щелкните **Подключиться (Connect)**. Введите имя пользователя и пароль учетной записи, у которой есть доступ к серверу.
10. В списке групп образов выберите группу, где должен храниться образ, и щелкните **Готово (Finish)**.

Управление доступом и предварительная настройка компьютеров

Управлять образами можно при помощи системы DISM, а также описанных выше инструментов. Чтобы предотвратить несанкционированную установку образов:

- Предварительно настройте компьютеры и разрешите развертывание только на известных компьютерах.
- Изменить параметры безопасности файлов образов так, чтобы к ним имели доступ только авторизованные сотрудники.
- Задайте требование утверждения администратором для клиентской установки.

Предварительная настройка компьютеров

Предварительная настройка компьютеров предполагает создание учетных записей компьютеров в Active Directory перед их использованием. При помощи предварительной настройки вы определяете, какие клиенты и серверы связываются друг с другом. Прежде чем провести предварительную настройку компьютеров, убедитесь, что службы развертывания Windows

настроены на прием запросов только от известных компьютеров. Для этого необходимо выполнить следующие действия:

1. В консоли служб развертывания Windows раскройте узел **Серверы (Servers)**. Правой кнопкой мыши щелкните сервер, с которым хотите работать, и выберите команду **Свойства (Properties)**.
2. На вкладке **Параметры PXE-ответа (PXE Response Settings)** установите переключатель **Отвечать только известным клиентским компьютерам (Respond Only To Known Client Computers)** и щелкните **ОК**.

Для предварительной настройки компьютера необходимо знать его глобальный уникальный идентификатор (GUID). Идентификатор GUID выдается адаптером активной сети и должен вводиться в формате {*dddddddd-dddd-dddd-dddd-dddddddddddd*}, где *d* — шестнадцатеричная цифра, например {AEFED345-BC13-22CD-ABCD-11BB11342112}.

Требуемый идентификатор можно узнать несколькими способами. В некоторых случаях производитель печатает GUID на наклейке, прикрепленной к корпусу компьютера. Помните, что этот GUID соответствует сетевому адаптеру, который поставляется вместе с компьютером. Если вы замените адаптер, у нового адаптера будет новый идентификатор.

Чтобы узнать GUID установленного сетевого адаптера, загляните в микропрограммные настройки. Если вы работаете на удаленном компьютере, введите в окне Windows PowerShell команду:

```
get-wmiobject win32_networkadapter | format-list guid
```

Запишите или скопируйте GUID сетевого адаптера, подключенного к локальной сети.

Для предварительной настройки компьютера выполните следующие действия:

1. В оснастке Active Directory — Пользователи и компьютеры (Active Directory — Users And Computers) правой кнопкой щелкните подразделение или контейнер, к которому будет привязан клиент, затем щелкните **Создать (New)** и **Компьютер (Computer)**.
2. Введите имя компьютера. Если вы хотите указать пользователя или группу, которым разрешено добавление этого компьютера в домен, щелкните **Изменить (Change)**. Затем щелкните **Далее (Next)**.
3. На странице **Управляемый (Managed)** установите флажок **Это управляемый компьютер (This is a Managed Computer)**, введите GUID компьютера и щелкните **Далее (Next)**.
4. На странице **Сервер (Host Server)** выберите сервер служб развертывания Windows, который будет обслуживать этот клиентский компьютер. Щелкните **Далее (Next)** и **Готово (Finish)**.

Изменение параметров безопасности файлов образов

Чтобы изменить параметры безопасности файла образа, откройте Проводник Windows (Windows Explorer). Правой кнопкой щелкните файл образа и

выберите команду **Свойства (Properties).** В диалоговом окне **Свойства (Properties)** задайте необходимые параметры безопасности на вкладке **Безопасность (Security)**. Можно также настроить параметры безопасности для папки **Группа образов (Image Group),** в которой хранится файл образа. Они наследуются образами, хранящимися в этой папке.

Запрос утверждения администратора

Вместо предварительной настройки компьютеров или настройки параметров безопасности файла образа можно также задать обязательное подтверждение администратором установки системы при помощи образа. Выполните следующие действия:

1. В консоли служб развертывания Windows раскройте узел **Серверы (Servers)**. Правой кнопкой щелкните сервер, с которым хотите работать, и выберите команду **Свойства (Properties)**.
2. На вкладке **Параметры PXE-ответа (PXE Response Settings)** установите переключатель **Отвечать всем (известным и неизвестным) клиентским компьютерам (Respond to All Client Computers)**.
3. Установите флажок **Если клиент неизвестен, уведомлять администратора и отвечать после утверждения (Notify Administrator And Respond After Approval)**. Затем щелкните **ОК**.

После этого компьютеры, загружаемые по сети, будут входить в режим ожидания. Установка продолжится только после того, как ее подтвердит администратор.

Чтобы утвердить запрос, выполните следующие действия:

1. В консоли служб развертывания Windows выберите сервер, с которым будете работать. Затем щелкните узел **Ожидающие устройства (Pending Devices)**, чтобы раскрыть список компьютеров, ожидающих утверждения.
2. Правой кнопкой щелкните нужный компьютер и выберите команду **Утвердить (Approve)**.

Чтобы отклонить запрос, выполните следующие действия:

1. В консоли служб развертывания Windows выберите сервер, с которым будете работать. Затем щелкните узел **Ожидающие устройства (Pending Devices)**, чтобы раскрыть список компьютеров, ожидающих утверждения.
2. Правой кнопкой щелкните нужный компьютер и выберите команду **Отклонить (Reject)**.

Настройка образов Windows

Для настройки подключенного загрузочного или установочного образа применяется утилита DISM. Параметры DISM указаны в табл. 2-4. Компоненты внутри образа управляются при помощи хранилища компонентов.

Табл. 2-4. Основные параметры DISM

Команда	Описание
Общие команды	
/Cleanup-Wim	Удаляет ресурсы, связанные с поврежденными подключенными образами Windows
/Commit-Wim	Сохраняет изменения подключенного образа Windows
/Get-MountedWimInfo	Отображает сведения о подключенных образах Windows
/Get-WimInfo	Отображает сведения об образах в wim-файле
/Image	Задает путь к корневой папке автономного образа Windows
/Mount-Wim	Подключает образ из wim-файла
/Online	Указывает, что действие выполняется с работающей в данный момент ОС
/Remount-Wim	Снова подключает ставшую недоступной папку подключения WIM
/Unmount-Wim	Отключает подключенный образ Windows
Дополнительные параметры	
/English	Отображает вывод команды на английском языке
/Format	Задает формат отчета
/LogLevel	Задает уровень детализации отображения журнала (1-4)
/LogPath	Задает путь к файлу журнала
/NoRestart	Предотвращает автоматическую перезагрузку и запросы на перезагрузку
/Quiet	Отключает отображение сведений о ходе выполнения, кроме сообщений об ошибках
/ScratchDir	Задает путь к папке временных файлов
/SysDriveDir	Задает путь к файлу системного загрузчика BootMgr
/WinDir	Задает путь к папке Windows

После подключения образа с ним можно работать при помощи подкоманд DISM /Image, перечисленных в табл. 2-5. С их помощью вы обновите образ до более полного выпуска, добавите или удалите драйверы устройств, укажете часовой пояс и региональные параметры, отобразите установленные обновления и MSI-приложения, добавите или удалите пакеты и др.

Табл. 2-5. Подкоманды для подключенных и автономных образов

Параметры	Описание
/Add-Driver	Добавляет пакеты драйверов в автономный образ
/Add-Package	Добавляет пакеты в образ

Табл. 2-5. (*продолжение*)

Параметры	Описание
/Apply-Unattend	Применяет к образу файл ответов AnswerFile.xml
/Check-AppPatch	Отображает, применимы ли к подключенному образу исправления MSP
/Cleanup-Image	Производит все действия по очистке и восстановлению образа
/Disable-Feature	Отключает указанный компонент образа
/Enable-Feature	Подключает указанный компонент образа
/Gen-LangIni	Создает новый файл Lang.ini
/Get-AppInfo	Отображает информацию о конкретном установленном MSI-приложении
/Get-AppPatches	Отображает информацию обо всех примененных исправлениях MSP для всех приложений
/Get-AppPatchInfo	Отображает информацию об установленных исправлениях MSP
/Get-Apps	Отображает сведения обо всех установленных MSI-приложениях
/Get-CurrentEdition	Отображает издания конкретного образа
/Get-DriverInfo	Отображает информацию о конкретном драйвере для автономного образа или для работающей в данный момент ОС
/Get-Drivers	Выводит сведения обо всех драйверах для автономного образа или для работающей в данный момент ОС
/Get-FeatureInfo	Отображает информацию о конкретном компоненте
/Get-Features	Выводит сведения обо всех компонентах пакета
/Get-Intl	Отображает информацию о региональных параметрах и языках
/Get-PackageInfo	Отображает информацию об отдельном пакете
/Get-Packages	Выводит сведения обо всех пакетах образа
/Get-TargetEditions	Выводит список изданий Windows, до которых можно обновить образ
/Remove-Driver	Удаляет пакеты драйверов из автономного образа
/Remove-Package	Удаляет пакеты из образа
/Set-AllIntl	Устанавливает все региональные параметры в автономном образе
/Set-Edition	Обновляет образ Windows до более поздней редакции
/Set-InputLocale	Задает язык ввода и раскладку клавиатуры для использования в подключенном автономном образе

Табл. 2-5. (*окончание*)

Параметры	Описание
/Set-LayeredDriver	Определяет драйвер клавиатуры для японской или корейской клавиатуры
/Set-ProductKey	Вводит ключ продукта в автономный образ
/Set-SetupUILang	Определяет язык по умолчанию, который будет использоваться при установке
/Set-SKUIntlDefaults	Приводит в подключенном автономном образе все региональные параметры к значениям по умолчанию для конкретного языка
/Set-SysLocale	Задает язык для программ, не поддерживающих Юникод, а также параметры шрифта в автономном образе
/Set-TimeZone	Задает часовой пояс по умолчанию в автономном образе
/Set-UILang	Задает язык пользовательского интерфейса системы по умолчанию, используемый в автономном образе
/Set-UILangFallback	Устанавливает базовый язык пользовательского интерфейса системы по умолчанию, используемый в автономном образе
/Set-UserLocale	Устанавливает пользовательские региональные параметры в автономном образе

Система обслуживания образов содержит команды для работы с образами в WIM-файлах. Синтаксис подключения образов таков:

```
dism /mount-wim /wimfile:Путь /index:Номер /mountdir:ПутьПодключения
```

где *Путь* — полный путь к WIM-файлу, *Номер* — номер образа в WIM-файле, а *ПутьПодключения* — папка, где будет подключен образ. Например:

```
dism /mount-wim /wimfile:c:\winpe_x86\iso\sources\boot.wim /index:1
/mountdir:c:\win7
```

Затем вы можете изменить образ в соответствии со своими требованиями. Для сохранения изменений воспользуйтесь командой Dism /Commit-Wim, например:

```
dism /commit-wim /mountdir:c:\win7
```

В данном случае изменения сохраняются в WIM-файлах, подключенных к папке C:\Win7.

Для отключения WIM-файла используйте следующую команду:

```
dism /unmount-wim /mountdir:c:\win7
```

Здесь отключается образ в WIM-файле, подключенном к папке C:\Win7. Если были произведены изменения, при отключении образа их надо сохранить или отклонить. Используйте параметр Add /Commit для сохранения изменений или /Discard для отказа от них. Это касается только тех изменений, которые вы еще не сохраняли.

Глава 3

Настройка политик пользователей и компьютеров

Групповая политика это набор правил, применяемый для управления пользователями и компьютерами. В Windows 7 в групповые политики включаются как управляемые параметры, называемые *параметрами* (setting) политик, так и неуправляемые параметры, называемые *предпочтениями* (preference). Параметры политик позволяют управлять настройками ОС и ее компонентов. Предпочтения позволяют настраивать и разворачивать ОС, а также управлять ею и параметрами приложений. Ключевое отличие между параметрами и предпочтениями политик — обязательность исполнения. Групповые политики требуют обязательного соответствия системы параметрам, тогда как предпочтения проводятся не столь жестко.

В этой главе мы рассмотрим, как пользоваться параметрами политик, а в следующей поговорим о предпочтениях.

Основные сведения о групповых политиках

Групповые политики используются для управления параметрами ОС, а также для отключения некоторых возможностей пользовательского интерфейса. Большинство параметров политик хранится в относящихся к ним ветвях реестра. ОС и некоторые приложения проверяют эти ветви, чтобы определить, управляются ли в них различные аспекты ОС.

Имеются групповые политики двух типов: локальные и основанные на Active Directory. Локальные политики позволяют управлять параметрами локального компьютера, а политики Active Directory используются для управления компьютерами сайтов, доменов и подразделений. Групповые политики упрощают администрирование, предоставляя возможность централизованного управления полномочиями, разрешениями и возможностями пользователей и компьютеров. Вдумчивое применение политик является ключом к эффективной эксплуатации администрируемых систем. Параметры политик разделяются на две обширные категории: применяемые к компьютерам и применяемые к пользователям. Политики компьютеров обычно применяются при запуске системы, политики пользователей — при входе пользователя в систему.

Разбираясь со сбоями в системе, помните, что в процессе запуска и входа в систему политики применяются в четком порядке. При наличии нескольких политик порядок их применения таков:

1. Локальные политики.
2. Политики сайта.
3. Политики домена.
4. Политики подразделений.
5. Политики дочерних подразделений.

При конфликте политик по умолчанию последующая политика перекрывает предыдущие. Например, политики подразделений перезаписывают политики домена. Легко догадаться, что у этого правила есть исключения, позволяющие администратору блокировать, контролировать и отключать политики.

Клиентская служба групповых политик получает сообщения независимо от процесса регистрации Windows, что сокращает издержки на фоновую обработку политики, увеличивает общую производительность и позволяет проводить доставку и применение новых файлов политик в ходе процесса обновления, без перезапуска компьютера.

В отличие от Windows XP, в Windows 7 для отслеживания событий не используется Userenv.dll. Вместо этого сообщения о событиях записываются в системный журнал. Кроме того, рабочий журнал групповых политик заменяет ведение журнала Userenv. Решая проблемы с групповыми политиками, используйте подробные сообщения о событиях в рабочем журнале, а не журнал Userenv. Журнал групповых политик называется \Microsoft\Windows\GroupPolicy\Operational и в консоли просмотра событий находится в категории Журналы приложений и служб (Applications And Services Logs).

Вместо протокола ICMP (ping) в Windows 7 применяется служба Network Location Awareness. С ее помощью компьютер узнает тип сети, к которой он присоединен, а также может реагировать на изменения состояния системы или настроек сети. С помощью Network Location Awareness клиент групповых политик определит состояние компьютера, состояние сети и доступную полосу пропускания для медленных соединений. В результате клиент имеет более четкое представление о рабочей среде и способен применять соответствующие политики.

Применение локальных групповых политик

Локальная групповая политика применяется при локальном входе к любому пользователю или администратору, заходящему на компьютер рабочей группы или на компьютер домена.

Компьютер под управлением Windows 7 можно ассоциировать с одним или несколькими объектами локальной политики. Локальная групповая политика управляется через локальный объект групповой политики (Group Policy Object, GPO). Локальный GPO хранится на каждом компьютере

в папке %SystemRoot%\System32\GroupPolicy. Дополнительные GPO, связанные с пользователями или группами, хранятся в папке %SystemRoot%\System32\GroupPolicyUsers.

Несколько локальных GPO удобны в случае изолированного компьютера, не входящего в домен. Можно создать один локальный GPO для администраторов и другой для остальных пользователей, что избавит от необходимости явным образом изменять настройки, препятствующие управлению компьютером, при каждом выполнении административных задач. Однако в случае домена использовать несколько локальных GPO следует далеко не всегда, поскольку, как правило, к большинству компьютеров и пользователей и так применено несколько GPO. В этом случае добавление еще и нескольких локальных GPO способно резко затруднить управление групповыми политиками.

В Windows 7 имеется три слоя локальных GPO:

- **Локальная групповая политика** Единственный локальный GPO, позволяющий применять ко всем пользователям компьютера как параметры компьютера, так и параметры пользователя.
- **Локальная групповая политика администраторов и не-администраторов** Содержит только параметры пользователя и применяется на основании принадлежности пользователя к локальной группе администраторов.
- **Пользовательская локальная групповая политика** Содержит только параметры пользователя и применяется к пользователям и группам.

Слои GPO обрабатываются в следующем порядке: локальная групповая политика, локальная групповая политика администраторов, пользовательская локальная групповая политика.

Поскольку набор параметров пользователя во всех локальных GPO совпадает, между ними возможны конфликты. Во избежание этих конфликтов в Windows 7 предусмотрена перезапись любого предыдущего параметра последующим. Поэтому используется итоговое значение параметра. При разрешении конфликтов учитываются только включенные и выключенные параметры; параметры, которые не были заданы, не учитываются. Чтобы упростить администрирование в домене, отключите обработку локальных GPO. В Windows 7 для этого нужно задать политику Выключение обработки локальных объектов групповой политики (Turn Off Local Group Policy Objects Processing) в доменном GPO. Эта политика расположена в категории **Административные шаблоны (Administrative Templates)** параметров компьютера в узле **Система\Групповая политика (System\Group Policy)**.

Примечание Если локальные GPO включены, они всегда обрабатываются, но с наименьшим приоритетом. Это означает, что их параметры перекрываются параметрами сайта, домена и подразделения.

По умолчанию на компьютере имеется только один локальный GPO. Создавать другие локальные объекты политики и управлять ими можно посредством редактора объектов групповой политики. Поскольку локальная

групповая политика входит в групповую политику домена, локально многие действия по ее настройке недоступны. Во-первых, невозможно управлять предпочтениями политик. Во-вторых, доступна только часть параметров политик. В остальном локальная групповая политика и групповая политика Active Directory управляются одинаково.

Для работы с локальными GPO нужно использовать учетную запись администратора. Самый быстрый способ добраться до самого высокоуровневого GPO локального компьютера — ввести команду:

```
gpedit.msc /gpcomputer: "%ComputerName%"
```

Эта команда откроет в консоли MMC оснастку Редактор объектов групповой политики (Group Policy Management Editor), указав в качестве целевого локальный компьютер.

Есть и другой способ управления локальным GPO верхнего уровня. Выполните следующие действия:

1. Щелкните кнопку **Пуск (Start)**, введите **mmc** в поле поиска и нажмите Enter.
2. В открывшейся консоли MMC выберите в меню **Файл (File)** команду **Добавить или удалить оснастку (Add/Remove Snap-In)**.
3. В диалоговом окне **Добавление и удаление оснасток (Add Or Remove Snap-Ins)** выделите элемент списка **Редактор объектов групповой политики (Group Policy Object Editor)** и щелкните **Добавить (Add)**.
4. В диалоговом окне **Выбор объекта групповой политики (Select Group Policy Object)** щелкните **Готово (Finish)**, поскольку нас интересует объект по умолчанию — локальный компьютер. Щелкните **OK**.

Теперь при помощи редактора вы вольны управлять параметрами локальных групповых политик (рис. 3-1). Поскольку локальная групповая политика не содержит предпочтений, вы не найдете в узлах **Конфигурация компьютера (Computer Configuration)** и **Конфигурация пользователя (User Configuration)** отдельных подузлов для политик и предпочтений.

При необходимости можно создать и настроить другие объекты локальной политики. Выполните следующие действия:

1. Щелкните кнопку **Пуск (Start)**, введите **mmc** в поле поиска и нажмите Enter. В открывшейся консоли MMC выберите в меню **Файл (File)** команду **Добавить или удалить оснастку (Add/Remove Snap-In)**.
2. В диалоговом окне **Добавление и удаление оснасток (Add Or Remove Snap-Ins)** выделите элемент списка **Редактор объектов групповой политики (Group Policy Object Editor)** и щелкните **Добавить (Add)**.
3. В диалоговом окне **Выбор объекта групповой политики (Select Group Policy Object)** щелкните кнопку **Обзор (Browse)**. В диалоговом окне **Поиск объекта групповой политики (Browse For A Group Policy Object)** перейдите на вкладку **Пользователи (Users)**.

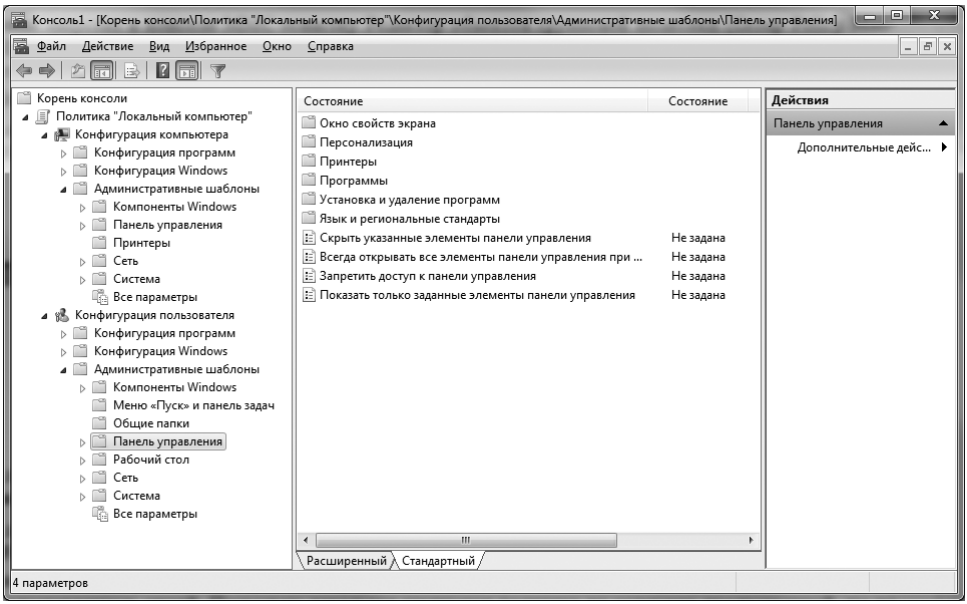

Рис. 3-1. Доступ к локальному GPO верхнего уровня

4. На вкладке **Пользователи (Users)**, показанной на рис. 3-2, записи в столбце **Объект групповой политики существует (Group Policy Object Exists)** указывают, создан ли конкретный объект локальной политики. Выполните одно из перечисленных действий:
   - Выберите вариант **Администраторы (Administrators)**, чтобы создать локальный GPO для администраторов. Выбирайте именно группу Администраторы (Administrators), а не пользователя Администратор (Administrator), чтобы применить политику ко всем локальным администраторам.
   - Выберите вариант **Не администраторы (Non-Administrators)**, чтобы создать или изменить локальный GPO для обычных пользователей.
   - Выберите конкретного локального пользователя, чей личный локальный GPO хотите создать или модифицировать.

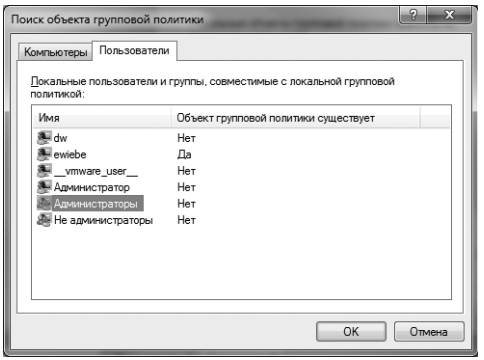

Рис. 3-2. Доступ к дополнительным локальным GPO

5. Щелкните **OK**. Если выбранного объекта не существует, он будет создан. В противном случае он будет открыт для просмотра и редактирования.

Работа с политиками сайта, домена и подразделения

Благодаря Active Directory каждый сайт, домен и подразделение могут иметь одну или несколько групповых политик. При использовании групповых политик Active Directory для работы с GPO применяется консоль Управление групповой политикой (Group Policy Management, GPMC). При этом необходимы полномочия администратора.

Консоль GPMC входит в стандартный установочный пакет серверной версии Windows. При работе с пользовательской версией Windows для работы с GPMC необходимо установить пакет средств удаленного администрирования сервера (Remote Server Administration Tools, RSAT). Вы найдете его в центре загрузки Майкрософт.

Установив консоль GPMC из комплекта RSAT, для ее открытия воспользуйтесь меню **Администрирование (Administrative Tools)**: щелкните кнопку **Пуск (Start)**, раскройте подменю **Все программы (All Programs)** и **Администрирование (Administrative Tools)**, а затем щелкните команду **Управление групповой политикой (Group Policy Management Console)**.

Левая панель GPMC по умолчанию содержит два узла высшего уровня (рис. 3-3): корень консоли и узел леса, с которым вы соединены. Развернув узел леса, вы увидите следующие подузлы:

- **Домены (Domains)** Предоставляет доступ к параметрам политик для доменов в администрируемом лесу. По умолчанию вы соединены с доменом, из которого зашли. Можно добавить соединения с другими доменами. Если развернуть узел домена, появятся узлы объекта GPO домена по умолчанию, подразделения контроллеров доменов (и соответствующие политики по умолчанию) и объектов GPO, определенных в домене.
- **Сайты (Sites)** Предоставляет доступ к параметрам политик сайтов в соответствующем лесу. По умолчанию сайты скрыты.
- **Моделирование групповой политики (Group Policy Modeling)** Предоставляет доступ к Мастеру моделирования групповой политики (Group Policy Modeling Wizard), помогающему планировать внедрение политик и имитировать параметры политик для их тестирования. Также здесь доступны сохраненные модели политик.
- **Результаты групповой политики (Group Policy Results)** Предоставляет доступ к Мастеру результатов групповой политики (Group Policy Results Wizard).

Объекты GPO, расположенные в контейнерах домена, сайта и подразделения на самом деле являются ссылками. Собственно GPO расположены в контейнере **Объекты групповой политики (Group Policy Objects)** выбранного домена. Обратите внимание на маленькие стрелки в нижнем левом углу значков GPO; эти стрелки аналогичны стрелкам на значках ярлыков.

Чтобы открыть GPO для редактирования, щелкните его правой кнопкой и выберите команду **Изменить (Edit)**.

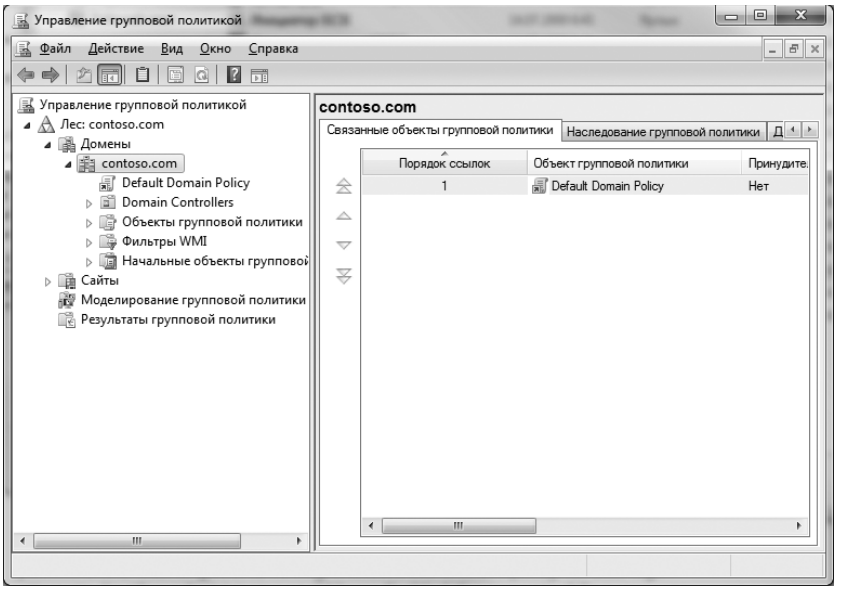

Рис. 3-3. Доступ к объектам GPO доменов, сайтов и подразделений

Выбрав или создав политику, используйте для работы с GPO Редактор управления групповыми политиками (Group Policy Management Editor). В его окне есть два главных узла (рис. 3-4):

- **Конфигурация компьютера (Computer Configuration)** Позволяет задавать политики, применяемые к компьютерам, вне зависимости от того, кто использует компьютер.
- **Конфигурация пользователя (User Configuration)** Позволяет задавать политики, применяемые к пользователям, вне зависимости от того, с какого компьютера осуществлен вход.

Примечание Помните, что настройки пользователя, произведенные при помощи объектов локальных политик, применяются только на тех компьютерах, на которых они были заданы. Если вы хотите, чтобы эти параметры применялись на всех компьютерах, на которых работает пользователь, используйте политики доменов сайтов или подразделений.

В узлах конфигурации компьютера и пользователя вы найдете отдельные подузлы **Политики (Policies)** и **Настройка (Preferences)**. При работе с параметрами политик используйте первый подузел. Элементы узла **Политики (Policies)** зависят от установленных дополнений и типа создаваемой политики. В большинстве случаев в обоих узлах будут следующие подузлы:

- **Конфигурация программ (Software Settings)** Настройка политик параметров приложений и установки приложений. При наличии установленных приложений, здесь могут появиться подузлы.

- **Конфигурация Windows (Windows Settings)** Настройка политик перенаправления папок, сценариев и безопасности.
- **Административные шаблоны (Administrative Templates)** Настройка политик ОС, компонентов Windows и программ. Эти политики, рассмотренные далее в этой главе, применяются к компьютерам и пользователям.

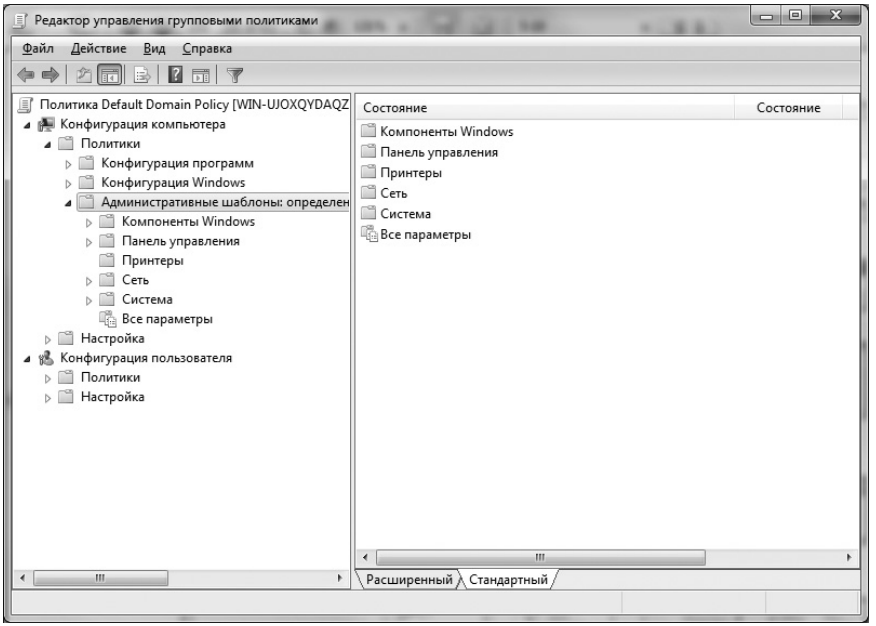

Рис. 3-4. Параметры групповой политики зависят от типа создаваемой политики и установленных дополнительных компонентов

Настройка политик

Для управления пользователями и компьютерами нужно настроить политики административных шаблонов. Они предоставляют легкий доступ к расположенным в реестре параметрам политик, управляющим ОС, компонентами Windows и программами. В предыдущих версиях Windows с поддержкой групповых политик для хранения параметров политик из реестра применялись файлы собственного формата ADM. В Windows 7 используется формат ADMX, основанный на стандарте XML. В отличие от ADM, хранившихся в соответствующем GPO, файлы ADMX находятся в централизованном хранилище, что облегчает работу с этими файлами в случае управления доменом.

Просмотр политик и шаблонов

Как показано на рис. 3-5, текущие шаблоны можно просмотреть в узле **Административные шаблоны (Administrative Templates)** консоли Редактор управления групповыми политиками (Group Policy Management Editor). В этом узле содержатся политики локальных систем, подразделений, доменов

и сайтов. В подузлах **Конфигурация компьютера (Computer Configuration)** и **Конфигурация пользователя (User Configuration)** расположены разные наборы шаблонов. Шаблоны, содержащие новые политики, добавляются при установке новых компонентов Windows, а также вручную при помощи редактора управления групповыми политиками.

Все изменения политик, производимые через административные шаблоны, сохраняются в реестре. Настройки компьютера сохраняются в разделе HKEY_LOCAL_MACHINE, настройки пользователя — в разделе HKEY_USER. Чтобы познакомиться с административными шаблонами, просмотрите содержимое узла **Административные шаблоны (Administrative Templates)** редактора управления групповыми политиками. Политики находятся в одном из трех состояний:

- **Не задана (Not Configured)** Политика не используется, и ее параметры не влияют на существующую конфигурацию компьютера.
- **Включена (Enabled)** Политика активна, ее параметры сохранены в реестре.
- **Отключена (Disabled)** Действия, заданные политикой, не производятся, но могут производиться другие действия. Например, действие отключенной политики может быть противоположно действию при ее включении. Соответствующие параметры хранятся в реестре.

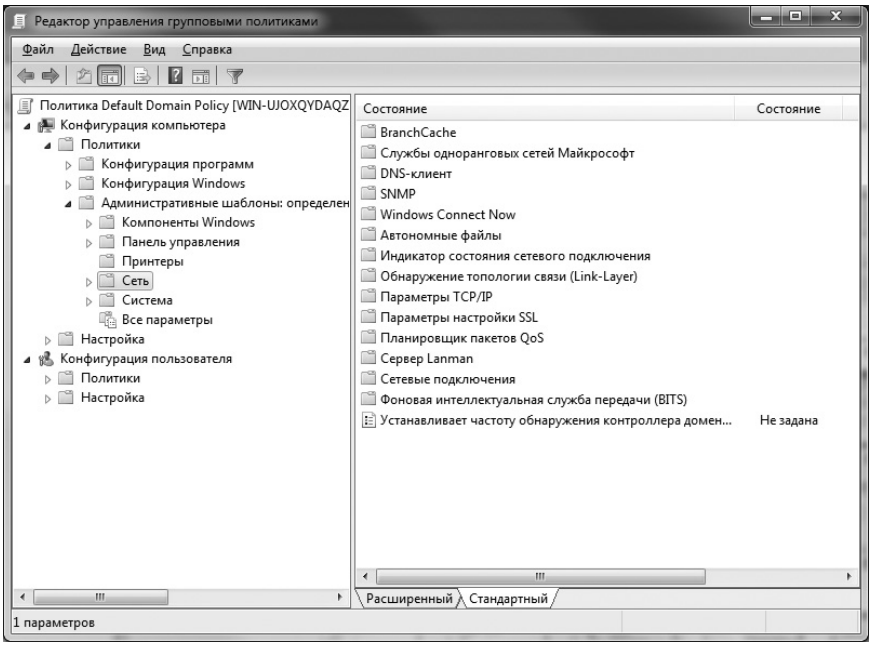

Рис. 3-5. Настраивайте политики пользователей и компьютеров при помощи шаблонов администрирования

Включение, выключение и настройка политик

Административные шаблоны содержатся в двух узлах редактора управления групповыми политиками: **Конфигурация компьютера (Computer Configuration)** и **Конфигурация пользователя (User Configuration)**. В большинстве случаев политики этих областей не перекрываются и не конфликтуют. Однако в случае возникновения конфликта приоритет отдается компьютерным политикам. Далее подробно описано использование основных политик.

Перед началом работы с политиками войдите в редактор управления групповыми политиками соответствующего сайта, домена или подразделения. Для доступа к GPO домена или подразделения выполните следующие действия:

1. В консоли GPMC разверните узел леса, с которым собираетесь работать. Затем разверните соответствующий узел Домены **(Domains)**.
2. Разверните узел соответствующего леса, затем разверните соответствующий узел **Объекты групповой политики (Group Policy Objects)**.
3. Щелкните правой кнопкой GPO, с которым собираетесь работать, и выберите команду **Изменить (Edit)**. GPO будет открыт для редактирования.

Открыв GPO в редакторе управления групповыми политиками, вы сможете включить, отключить или настроить политики следующим способом:

1. Раскройте подузел **Административные шаблоны (Administrantive Templates)** узла **Конфигурация компьютера (Computer Configuration)** или **Конфигурация пользователя (User Configuration)**, в зависимости от типа политики, с которой собираетесь работать.
2. В левой панели щелкните узел, содержащий политики, которые вы хотите настроить. Список политик будет отображен на правой панели.
3. Дважды щелкните политику или щелкните ее правой кнопкой и выберите команду **Свойства (Properties)**, чтобы отобразить диалоговое окно свойств политики.
4. Щелкните вкладку **Объяснение (Explain)**, если она есть, чтобы прочитать описание политики.
5. Чтобы задать состояние политики, щелкните вкладку **Параметр (Setting)** и установите один из переключателей:
   - **Не задан (Not Configured)** Политика не настроена.
   - **Включить (Enabled)** Политика действует.
   - **Отключить (Disabled)** Политика отключена.
6. Если вы включили политику, задайте дополнительные параметры на вкладке **Параметр (Setting)** и щелкните **Применить (Apply)**.
7. Используйте кнопки **Предыдущий параметр (Previous Setting)** и **Следующий параметр (Next Setting)** для управления другими политиками текущего узла.
8. Завершив управление политиками, щелкните **OK**.

Добавление и удаление шаблонов

Чтобы добавить или удалить узлы шаблонов, выполните следующие действия:

1. Зайдите в редактор управления групповой политикой нужного сайта, домена или подразделения.
2. В узле **Конфигурация компьютера (Computer Configuration)** или **Конфигурация пользователя (User Configuration)** щелкните правой кнопкой узел **Административные шаблоны (Administrative Templates)** и выберите команду **Добавление и удаление шаблонов (Add/Remove Templates)**. Откроется одноименное диалоговое окно.
3. Для добавления шаблона щелкните кнопку **Добавить (Add)**. В диалоговом окне **Шаблоны политики (Policy Templates)** выберите нужный шаблон и щелкните **Открыть (Open)**.
4. Для удаления шаблона выделите его щелкните **Удалить (Remove)**.
5. Завершив добавление и удаление шаблонов, щелкните **Закрыть (Close)**.

Политики управления файлами и данными

Каждый системный администратор должен разбираться в политиках управления файлами и данными. Они определяют объем данных, которые пользователю разрешено хранить в системе, способ использования автономных файлов и в каких случаях работает восстановление системы.

Политики дисковых квот

Политики, управляющие дисковыми квотами, применяются на уровне системы. Получить доступ к этим политикам можно посредством подузла **Административные шаблоны (Administrative Templates)** узла **Конфигурация компьютера (Computer Configuration)** — в подузле **Система\Дисковые квоты (System\Disk Quotas)**. Доступные политики указаны в табл. 3-1.

Табл. 3-1. Политики дисковых квот

Политика	Описание
Применить политику к съемным носителям (Apply Policy To Removable Media)	Определяет, будет ли применяться квотирование к томам NTFS на сменных носителях. Если эта политика не включена, квотирование применяется только к постоянным носителям
Предел квоты по умолчанию и уровень предупреждения (Default Quota Limit And Warning Level)	Устанавливает размер квоты по умолчанию и уровень предупреждения для всех пользователей. Этот параметр аннулирует другие параметры и применяется только к новым пользователям тома
Включить дисковые квоты (Enable Disk Quotas)	Включает или отключает квотирование на всех NTFS-томах компьютера и предотвращает изменение этого параметра пользователями

Табл. 3-1. (*окончание*)

Политика	Описание
Задать предел дисковой квоты (Enforce Disk Quota Limit)	Указывает, будет ли ограничение, установленное квотой, принудительным. В случае принудительного ограничения пользователям, превысившим квоту, не предоставляется дисковое пространство. Этот параметр отменяет параметры, заданные на вкладке **Квота (Quota)** свойств тома NTFS
Записывать в журнал события при превышении предела квоты (Log Event When Quota Limit Exceeded)	Определяет, будет ли при превышении пользователем квоты вноситься событие в журнал; запрещает пользователям изменять параметры ведения журнала
Записывать в журнал события, возникающие при превышении уровня предупреждения квоты (Log Event When Quota Warning Level Exceeded)	Определяет, будет ли вноситься в журнал сообщение о достижении пользователем уровня предупреждения

Работая с квотами, как правило, следует использовать на всех системах стандартный набор политик. Обычно не стоит включать все политики. Задействуйте политики выборочно и применяйте их в сочетании со стандартными возможностями NTFS для управлениями квотами на различных томах. Для включения квот выполните следующие действия:

1. Откройте для редактирования групповую политику компьютера, сайта, домена или подразделения. В категории **Административные шаблоны (Administrative Templates)** раскройте узлы **Конфигурация компьютера (Computer Configuration)**, **Система (System)** и **Дисковые квоты (Disk Quotas)**.
2. Дважды щелкните политику **Включить дисковые квоты (Enable Disk Quotas)**. Установите переключатель **Включить (Enabled)** и щелкните **OK**.
3. Дважды щелкните политику **Задать предел дисковой квоты (Enforce Disk Quota Limit)**. Если вы хотите включить принудительное квотирование на всех томах NTFS, установите переключатель **Включить (Enabled)**. В противном случае установите переключатель **Отключить (Disabled)** и задайте конкретные ограничения для каждого тома, как описано в главе 14. Щелкните **OK**.
4. Дважды щелкните политику **Предел квоты по умолчанию и уровень предупреждения (Default Quota Limit And Warning Level)**. Откроется диалоговое окно, показанное на рис. 3-6. Установите переключатель **Включить (Enabled)**.

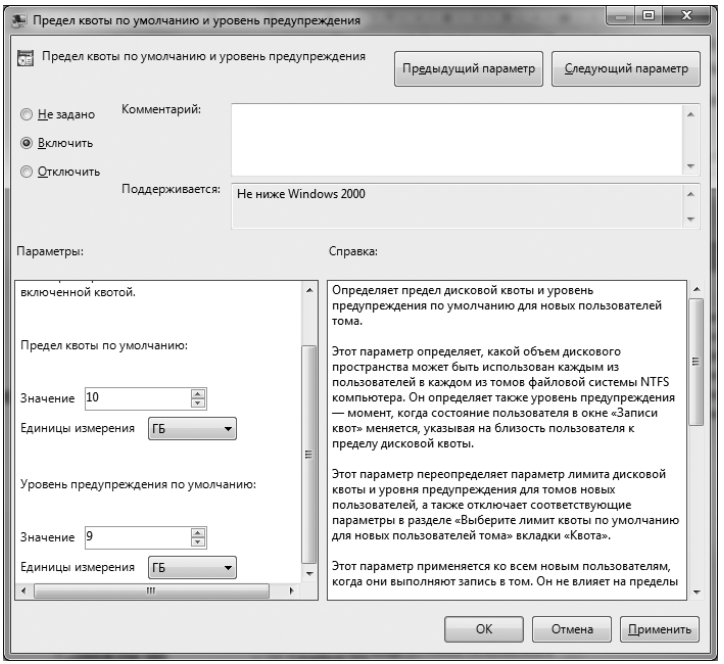

Рис. 3-6. Задайте параметры дисковых квот

5. В поле **Предел квоты по умолчанию (Default Quota Limit)** задайте ограничение, по умолчанию применяемое к новым пользователям при первой операции записи на квотированный том. Это ограничение не применяется к текущим пользователям и не влияет на текущие ограничения. На корпоративном ресурсе общего доступа уместен предел между одним и тремя гигабайтами. Естественно, он зависит от объема данных, с которыми постоянно работают пользователи. Например, дизайнерам и инженерам может понадобиться большее пространство.
6. Прокрутите раздел параметров вниз, чтобы задать уровень предупреждения. Обычно оно составляет 90% квоты, то есть при квоте в 10 Гб уровень предупреждения следует установить равным 9 Гб. Щелкните **OK**.
7. Дважды щелкните политику **Записывать в журнал события при превышении предела квоты (Log Event When Quota Limit Exceeded)**. Установите переключатель **Включить (Enabled)** и щелкните **OK**.
8. Дважды щелкните политику **Записывать в журнал события, возникающие при превышении уровня предупреждения квоты (Log Event When Quota Warning Level Exceeded)**. Установите переключатель **Включить (Enabled)** и щелкните **OK**.
9. Дважды щелкните политику **Применить политику к съемным носителям (Apply Policy To Removable Media)**. Установите переключатель **Отключить (Disabled)**, чтобы квоты применялись только к стационарным томам компьютера. Щелкните **OK**.

Политики восстановления системы

Функция восстановления системы призвана сохранить состояние томов системы и предоставить пользователям возможность восстановить систему в случае сбоя. Это возможность весьма ценна для среднего пользователя, однако ее обеспечение требует огромных объемов дискового пространства. Как будет рассказано в главе 6, функцию восстановления системы можно отключить для некоторых дисков или для всех дисков компьютера.

В консоли редактора групповой политики параметры политик восстановления системы находятся в подузле **Административные шаблоны (Administrative Templates)** узла **Конфигурация компьютера (Computer Configuration)** — в папке **Система\Восстановление системы (System\System Restore)**. Доступны следующие параметры:

- **Отключить восстановление системы (Turn off system restore)** Включив эту политику, вы отключите восстановление системы и лишитесь возможности управлять этой функцией посредством утилиты Система (System) и мастера восстановления системы. При отключении этой политики восстановление системы приобретает принудительный характер и не может быть отключено.
- **Отключить конфигурацию (Turn off configuration)** Включение этой политики не дает настраивать восстановление системы, но сохраняет возможность отключения этой функции. Если вы отключите эту политику, пользователи смогут открывать диалоговое окно с параметрами системы восстановления, но не смогут их изменять. Возможность отключить функцию сохраняется.

Для настройки политик восстановления системы выполните следующие действия:

1. Откройте групповую политику компьютера, сайта, домена или подразделения. Откройте узлы **Конфигурация компьютера (Computer Configuration)**, **Административные шаблоны (Administrative Templates)**, **Система (System)** и **Восстановление системы (System Restore)**.
2. Для включения или отключения восстановления системы дважды щелкните политику **Отключить восстановление системы (Turn Off System Restore)** и установите переключатель **Включить (Enabled)** или **Отключить (Disabled)**. Щелкните **OK**.
3. Для включения или отключения конфигурации восстановления системы дважды щелкните политику **Отключить конфигурацию (Turn Off Configuration)** и установите переключатель **Включить (Enabled)** или **Отключить (Disabled)**. Щелкните **OK**.

Политики автономных файлов

Политики автономных файлов задаются как на уровне компьютера, так и на уровне пользователя и на обоих уровнях называются одинаково. Работая с одинаковыми политиками разных уровней, помните, что компьютерные

политики обладают большим приоритетом, чем пользовательские. Кроме того, эти политики применяются в разное время.

Наиболее типичные политики перечислены в табл. 3-2. Как видите, большая часть политик влияет на доступ, синхронизацию, кеширование и шифрование. Политики автономных файлов находятся в узлах **Конфигурация компьютера (Computer Configuration)** или **Конфигурация пользователя (User Configuration)**, **Административные шаблоны (Administrative Templates)**, **Сеть (Network)**, **Автономные файлы (Offline Files)**.

Табл. 3-2. Политики автономных файлов

Тип политики	Название	Описание
Компьютер	Включить прозрачное кэширование (Enable Transparent Caching)	Управляет кешированием сетевых файлов через медленные соединения. Включена: кеширование на клиенте оптимизируется для сокращения числа передач по медленным соединениям. Отключена: прозрачное кеширование не используется
Компьютер	Включить экономичное использование административно назначенных автономных файлов (Turn on Economical Application of Administratively Assigned Offline Files)	Определяет, как будут синхронизированы при входе в систему административно назначенные файлы. Включена: синхронизируются только новые файлы и папки. Отключена: синхронизируются все файлы и папки
Компьютер	Исключить файлы из числа кэшируемых (Exclude Files from Being Cached)	Позволяет указать расширения файлов, которые не следует кешировать
Компьютер	Настроить режим медленного подключения (Configure Slow-Link Mode)	Управляет использованием медленных соединений. Включена: для каждой общей папки с автономными файлами настроены значения медленных соединений. Отключена: режим медленного соединения для автономных файлов не используется
Компьютер	Настроить фоновую синхронизацию (Configure Background Sync)	Управляет фоновой синхронизацией медленных соединений. Включена: периодически происходит фоновая синхронизация общих папок на сервере и клиенте. Отключена: фоновая синхронизация работает согласно параметрам по умолчанию

Табл. 3-2. (*продолжение*)

Тип политики	Название	Описание
Компьютер	Некэшируемые файлы (Files Not Cached)*	Список типов или расширений файлов, которые нельзя использовать автономно
Компьютер	Ограничить размер дискового пространства, используемого автономными файлами (Limit Disk Space Used by Offline Files)	Ограничивает размер дискового пространства для хранения автономных файлов
Компьютер	При выходе из системы удалять локальную копию автономных файлов пользователя (At Logoff, Delete Local Copy of User's Offline Files)*	Очищает кеш автономных файлов локального компьютера при выходе из системы
Компьютер	Размер кэша по умолчанию (Default Cache Size)*	Ограничивает размер автоматически кешируемых автономных файлов и предотвращает изменение соответствующих параметров пользователями. Включена: можно вручную задать размер кеша. Отключена: размер кеша ограничен 10% дискового пространства
Компьютер	Разрешить автономный доступ ко вложенным папкам (Subfolders Always Available Offline)*	Делает подпапки доступными автономно, если родительские папки доступны автономно
Компьютер	Разрешить или запретить использование автономных файлов (Allow or Disallow Use of The Offline Files Feature)	Принудительно включает или отключает возможность использования автономных файлов и предотвращает изменение этого параметра пользователями. Разрешает административное управление параметрами автономных файлов системы
Компьютер	Шифрование кэша автономных файлов (Encrypt the Offline Files Cache)	Определяет, будут ли шифроваться автономные файлы
Компьютер/ Пользователь	Административно назначенные автономные файлы (Administratively Assigned Offline Files)	Позволяет задать UNC-путь к постоянно доступным автономным файлам и папкам

Табл. 3-2. (*продолжение*)

Тип политики	Название	Описание
Компьютер/ Пользователь	Действие при отключении от сервера (Action on Server Disconnect)*	Определяет, как система реагирует на недоступность файлового сервера. Действие Работа в автономном режиме (Work Offline) обеспечивает доступность автономных файлов
Компьютер/ Пользователь	Запретить использование папки «Автономные файлы» (Prevent Use of Offline Files Folder)*	Запрещает пользователям доступ к папке автономных файлов. Пользователи не могут ни просматривать, ни открывать копии кешированных файлов, но могут работать автономно
Компьютер/ Пользователь	Запретить пользовательскую настройку авто-номных файлов (Prohibit User Configuration of Offline Files)*	Запрещает пользователю включение, отключение и настройку автономных файлов. Используются строго параметры автономных файлов по умолчанию
Компьютер/ Пользователь	Запретить применение «Сделать доступными автономно» для этих файлов и папок (Prohibit “Make Available Offline” for These Files and Folders)*	Запрещает пользователям делать автономными определенные файлы и папки. Укажите путь к соответствующим ресурсам в формате UNC
Компьютер/ Пользователь	Синхронизировать автономные файлы перед приостановкой (Synchronize Offline Files Before Suspend)*	Включает принудительную синхронизацию файлов перед переходом компьютера в ждущий или спящий режим. Можно указать полную или быструю синхронизацию
Компьютер/ Пользователь	Синхронизировать автономные файлы при входе в систему (Synchronize All Offline Files When Logging on)*	Включает принудительную полную синхронизацию при входе пользователя в систему и предотвращает изменение времени синхронизации
Компьютер/ Пользователь	Синхронизировать перед выходом из системы (Synchronize All Offline Files Before Logging Off)*	Включает принудительную полную синхронизацию перед выходом пользователя из системы и предотвращает изменение времени синхронизации
Компьютер/ Пользователь	Удалить «Сделать доступными автономно» (Remove “Make Available Offline”)	Не позволяет пользователям делать файлы доступными автономно

Табл. 3-2. (*окончание*)

Тип политики	Название	Описание
Компьютер/ Пользователь	Уровень регистрации событий (Event Logging Level)*	Обеспечивает сохранение событий, связанных с автономными файлами, в журнал приложений

* Не применяется в Windows 7, Windows Server 2008 Release 2 и более поздних версиях

Настройка автономных файлов

Настройкой автономных файлов легко управлять при помощи групповых политик. Можно, например, разрешить пользователям указывать, какие файлы и папки должны быть доступны автономно, запретить им настройку автономных файлов, разрешить пользователям работать автономно, одновременно запретив доступ к другим кешированным ресурсам. Чтобы задать политики настройки автономных файлов, выполните следующие действия:

1. Откройте групповые политики для компьютера, сайта, домена или подразделения, с которым вы собираетесь работать. Большую часть политик автономных файлов можно настроить как через конфигурацию компьютера, так и через конфигурацию пользователя с помощью узла **Автономные файлы (Offline Files)**. Чтобы получить доступ к этому узлу, последовательно раскройте узлы **Конфигурация компьютера (Computer Configuration)** или **Конфигурация пользователя (User Configuration)**, **Административные шаблоны (Administrative Templates)** и **Сеть (Network)**.
2. Для управления доступностью автономных файлов дважды щелкните политику **Разрешить или запретить использование автономных файлов (Allow or Disallow Use of the Offline Files Feature)**. Установите переключатель **Включить (Enabled)** или **Отключить (Disabled)**. Затем щелкните **OK**. Теперь пользователи смогут выбирать конкретные файлы и папки, которые должны быть доступны автономно. Чтобы самому выбирать эти файлы и предотвратить изменение вашего выбора пользователями, запретите этот компонент и определите автономные файлы административно.
3. Чтобы запретить изменение пользователями параметров автономных файлов, дважды щелкните политику **Запретить пользовательскую настройку автономных файлов (Prohibit User Configuration of Offline Files)** и установите переключатель **Включить (Enabled)**. После установки этой политики пользователи не смогут настраивать параметры автономных файлов.
4. Чтобы закрыть пользователям доступ к папке автономных файлов с сохранением возможности автономной работы, дважды щелкните политику **Запретить использование папки «Автономные файлы» (Prevent Use of Offline Files Folder)** и установите переключатель **Включить (Enabled)**. После установки этой политики пользователи не смогут использовать

папку Автономные файлы (Offline files) для просмотра или открытия копий кешированных файлов, но смогут сохранять текущую работу и использовать активные файлы, находясь в автономном режиме.

Административное управление автономными файлами и папками

Административное управление файлами и папками, доступными для автономного использования, обычно нужно на файловых серверах или других системам с общим доступом к ресурсам. Есть несколько способов административного управления автономной доступностью ресурсов.

Чтобы запретить пользователям делать файлы доступными автономно и назначить эти файлы самолично, выполните следующие действия:

1. Откройте групповые политики для компьютера, сайта, домена или подразделения, с которым вы собираетесь работать. Последовательно раскройте узлы **Конфигурация компьютера (Computer Configuration)** или **Конфигурация пользователя (User Configuration)**, **Административные шаблоны (Administrative Templates)**, **Сеть (Network)** и **Автономные файлы (Offline Files)**.
2. Чтобы не допустить изменения пользователями состояния автономной доступности файлов, дважды щелкните политику **Удалить «Сделать доступными автономно» (Remove "Make Available Offline")**. Установите переключатель **Включить (Enabled)** и щелкните **OK**. После установки политики пользователи не смогут задавать автономное использование конкретных файлов.
3. Чтобы назначить ресурсы, которые автоматически должны быть доступны автономно, дважды щелкните политику **Административно назначенные автономные файлы (Administratively Assigned Offline Files)** и установите переключатель **Включить (Enabled)**. Затем щелкните кнопку **Показать (Show)**. В диалоговом окне **Вывод содержания (Show Contents)** укажите UNC-пути ресурсов, например \\corpserver84\data (рис. 3-7).

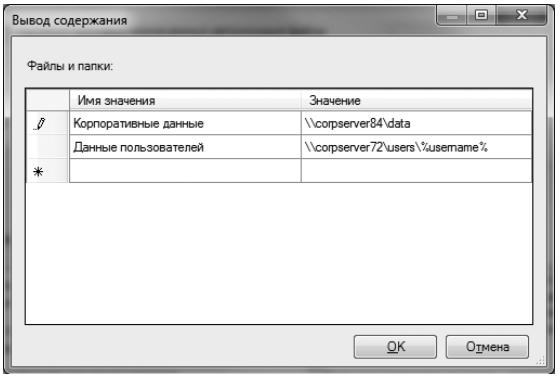

Рис. 3-7. Укажите UNC-пути ресурсов, которые должны быть доступны автономно

Внимание! Вдумчиво назначайте автоматически автономные ресурсы. Чем больше ресурсов работают этим способом, тем больше трафика расходуется на поддержку кеша автономных файлов.

Чтобы сделать конкретные файлы автоматически доступными и предотвратить автономное использование других файлов на компьютерах под управлением Windows XP, выполните следующие действия:

1. Откройте групповые политики для компьютера, сайта, домена или подразделения, с которым вы собираетесь работать. Последовательно раскройте узлы **Конфигурация компьютера (Computer Configuration)** или **Конфигурация пользователя (User Configuration)**, **Административные шаблоны (Administrative Templates)**, **Сеть (Network)** и **Автономные файлы (Offline Files)**.
2. Для выбора ресурсов, автоматически доступных автономно, дважды щелкните политику **Административно назначенные автономные файлы (Administratively Assigned Offline Files)**. Установите переключатель **Включить (Enabled)** и щелкните кнопку **Показать (Show)**. В диалоговом окне **Вывод содержания (Show Contents)** укажите UNC-пути ресурсов, например \\corpserver84\data.
3. Чтобы запретить пользователям делать файлы доступными автономно, дважды щелкните политику **Запретить применение «Сделать доступными автономно» для этих файлов и папок (Prohibit "Make Available Offline" for These Files and Folders)** и установите переключатель **Включить (Enabled)**. Щелкните кнопку **Показать (Show)**. В диалоговом окне **Вывод содержания (Show Contents)** укажите UNC-пути ресурсов, например \\corpserver84\data. Этот параметр не помешает автоматическому кешированию ресурсов, заданных на предыдущем шаге.
4. Щелкайте **OK**, пока не закроются все диалоговые окна.

Синхронизация автономных файлов

Синхронизацией автономных файлов можно управлять через Центр синхронизации (Sync Center), доступ к которому открывает одноименная команда из подменю **Стандартные (Accessories)** меню **Пуск (Start)**. Однако при помощи политик можно задать способ и расписание синхронизации. Различают полную синхронизацию (все файлы проверены на завершенность и актуальность) и быструю синхронизацию (файлы проверены на завершенность, но не на актуальность).

В Windows 7 автономные файлы синхронизируются автоматически. При наличии медленного соединения синхронизация проводится в фоновом режиме. Медленным считается соединение с задержкой более 80 микросекунд. Чтобы компьютер с Windows 7 не переходил в режим медленного соединения и не использовал фоновую синхронизацию, отключите политику **Настроить режим медленного подключения (Configure Slow-Link Mode)**.

Для настройки политик синхронизации в Windows Server 2003, Windows XP и Windows 2000, выполните следующие действия:

1. Откройте групповые политики для компьютера, сайта, домена или подразделения, с которым вы собираетесь работать. Последовательно раскройте узлы **Конфигурация компьютера (Computer Configuration)**, **Административные шаблоны (Administrative Templates)**, **Сеть (Network)** и **Автономные файлы (Offline Files)**.
2. Синхронизацией управляют политики **Синхронизировать автономные файлы при входе в систему (Synchronize All Offline Files When Logging on)**, **Синхронизировать перед выходом из системы (Synchronize All Offline Files Before Logging Off)** и **Синхронизировать автономные файлы перед приостановкой (Synchronize Offline Files Before Suspend)**. Дважды щелкните нужную политику и установите переключатель **Включить (Enabled)**. При настройке политики **Синхронизировать автономные файлы перед приостановкой (Synchronize Offline Files Before Suspend)** выберите в списке **Действие (Action)** нужный вариант — **Полный режим (Full)** или **Быстрый режим (Quick)**. Щелкните **ОК**.

Совет Полная синхронизация обеспечивает сохранение последней версии автономных файлов перед изменением энергорежима. Быстрая синхронизация обеспечивает только доступность файлов, но не обязательно последней версии.

Кеширование автономных файлов

Продуманная настройка размера кеша автономных файлов — основа управления нагрузкой на компьютер и на сеть, возникающей вследствие использования автономных файлов. Максимальный размер кеша, его шифрование и типы файлов, которые не должны кешироваться, можно задать в центре синхронизации, но об этом будет говориться в главе 14. Для настройки соответствующих политик на компьютерах с прежними версиями Windows, выполните следующие действия:

1. Откройте групповые политики для компьютера, сайта, домена или подразделения, с которым вы собираетесь работать. Последовательно раскройте узлы **Конфигурация компьютера (Computer Configuration)**, **Административные шаблоны (Administrative Templates)** и **Сеть (Network)**.
2. Чтобы задать размер кеша, дважды щелкните политику **Размер кэша по умолчанию (Default Cache Size)** и установите переключатель **Включить (Enabled)**. Затем введите нужное значение в поле **Размер кэша по умолчанию (Default Cache Size)**, как показано на рис. 3-8. Вводимое значение — доля дискового пространства, умноженная на 10000. Если вы, например, введете в это поле число 1500, кеш сможет занять до 15% дискового пространства.

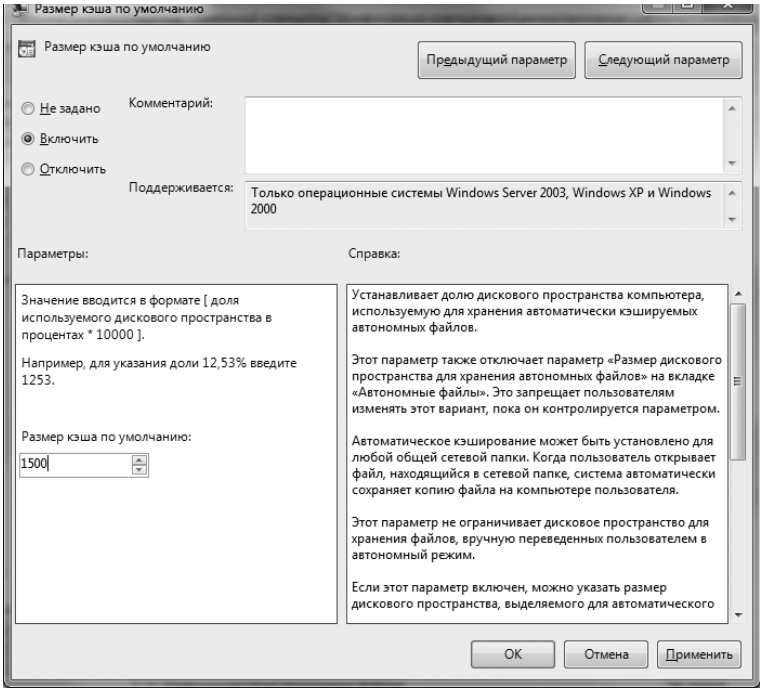

Рис. 3-8. Установка размера по умолчанию для кеша автономных файлов

Примечание Если не настроить политику **Размер кэша по умолчанию (Default Cache Size)** или отключить ее, кеш будет ограничен 10% дискового пространства.

3. Для указания некешируемых типов файлов дважды щелкните политику **Некэшируемые файлы (Files Not Cached)** и установите переключатель **Включить (Enabled)**. Затем введите в поле **Расширения (Extensions)** список расширений файлов, которые не будут кешироваться, разделяя их точками с запятой. Например, чтобы запретить кеширование временных файлов, введите ***.wbk; *.tmp; *.lnk; *.ndx**.
4. Чтобы зашифровать кеш, дважды щелкните политику **Шифрование кэша автономных файлов (Encrypt the Offline Files Cache)** и установите переключатель **Включить (Enabled)**. После включения этой политики все существующие и новые файлы в кеше будут зашифрованы. Пользователь сможет просмотреть свои файлы, но другие пользователи не смогут их видеть.

Политики доступа и подключений

Политики доступа и связи управляют сетевыми и модемными соединениями, а также настройками удаленной помощи. Эти политики влияют на подключение системы к сети и удаленный доступ к системе.

Сетевые политики

К вашим услугам много сетевых политик. На компьютерном уровне настраиваются политики общего подключения к Интернету, брандмауэра и сетевого моста. На уровне пользователя настраиваются политики, управляющие соединениями по локальной сети, настройками TCP/IP и удаленным доступом. Основные политики перечислены в табл. 3-3. Сетевые политики расположены в узле **Сеть\Сетевые подключения (Network\Network Connections)** узла **Административные шаблоны (Administrative Templates)** в категориях **Конфигурация компьютера (Computer Configuration)** и **Конфигурация пользователя (User Configuration)**.

Табл. 3-3. Сетевые политики

Тип политики	Название	Описание
Компьютер	Запрет использования брандмауэра подключения к Интернету в DNS-домене (Prohibit Use of Internet Connection Firewall on your DNS Domain Network)*	Определяет, могут ли пользователи включить брандмауэр Интернета. Применяется только к тому домену, где включена политика
Компьютер	Запрет использования общего Интернет-подключения в DNS-домене (Prohibit Use of Internet Connection Sharing on your DNS Domain Network)*	Определяет, могут ли администраторы включать и настраивать общее подключение к Интернету. Применяется только к тому домену, где включена политика
Компьютер	Запрет установки и настройки сетевого моста в сети DNS-домена (Prohibit Installation and Configuration of Network Bridge on your DNS Domain Network)	Определяет, могут ли пользователи устанавливать и настраивать сетевые мосты. Применяется только к тому домену, где включена политика
Компьютер	Маршрутизировать весь трафик через внутреннюю сеть (Route All Traffic through the Internal Network)	Используется совместно с DirectAccess. Определяет, будет ли у удаленных компьютеров доступ к Интернету через внутреннюю корпоративную сеть или собственное подключение к Интернету
Компьютер	Требовать повышения прав пользователей домена при задании сетевого ресурса (Require Domain Users to Elevate when Setting a Network's Location)	Определяет, будет ли отображаться приглашение на повышение полномочий перед установкой сетевого расположения

Табл. 3-3. (*окончание*)

Тип политики	Название	Описание
Пользователь	Возможность включения/разрыва подключения локальной сети (Ability to Enable/Disable a LAN Connection)*	Определяет, могут ли пользователи включать или отключать соединения по локальной сети
Пользователь	Возможность изменить свойства всех пользовательских подключений удаленного доступа (Ability to Change Properties of an All User Remote Access Connection)	Определяет, могут ли пользователи просматривать и изменять свойства соединений удаленного доступа, доступных всем пользователям компьютерам
Пользователь	Возможность удалить все подключения удаленного доступа пользователей (Ability to Delete All User Remote Access Connections)*	Определяет, могут ли пользователи удалять соединения удаленного доступа, доступные всем пользователям компьютерам
Пользователь	Запрет доступа к свойствам компонентов подключений удаленного доступа (Prohibit Access to Properties of Components of a Remote Access Connection)*	Определяет, получат ли пользователи доступ к свойствам компонентов удаленных соединений и смогут ли они их изменить
Пользователь	Запрет доступа к свойствам подключений локальной сети (Prohibit Access to Properties of a LAN Connection)*	Определяет, могут ли пользователи изменять свойства соединений по локальной сети
Пользователь	Запретить дополнительные настройки TCP/IP (Prohibit TCP/IP Advanced Configuration)*	Определяет, получат ли пользователи доступ к дополнительным параметрам TCP/IP
Пользователь	Запретить удаление подключений удаленного доступа (Prohibit Deletion of Remote Access Connections)	Определяет, могут ли пользователи удалять соединения удаленного доступа

* Не применяется в Windows 7, Windows Server 2008 Release 2 и более поздних версиях

Как видно из табл. 3-3, сетевые политики для компьютеров призваны ограничить полномочия по работе с сетью. Эти ограничения лишат пользователей соответствующего домена таких возможностей, как общее подключение к Интернету. Это повысит защищенность корпоративных сетей, но не помешает пользователям портативных компьютеров, например, унести эти компьютеры домой и использовать подключение к Интернету в домашней сети. Чтобы включить или выключить эти ограничения, выполните следующие действия:

1. Откройте групповые политики для компьютера, сайта, домена или подразделения, с которым вы собираетесь работать. Последовательно раскройте узлы **Конфигурация компьютера (Computer Configuration)**, **Административные шаблоны (Administrative Templates)**, **Сеть (Network)** и **Сетевые подключения (Network Connections)**.
2. Дважды щелкните нужную политику и установите переключатель **Включить (Enabled)** или **Отключить (Disabled)**. Затем щелкните **OK**.

Пользовательские политики сетевых соединений, как правило, закрывают доступ к некоторым возможностям настройки, например, к дополнительным параметрам TCP/IP. Для настройки этих политик выполните следующие действия:

1. Откройте групповые политики для компьютера, сайта, домена или подразделения, с которым вы собираетесь работать. Последовательно раскройте узлы **Конфигурация пользователя (User Configuration)**, **Административные шаблоны (Administrative Templates)**, **Сеть (Network)** и **Сетевые подключения (Network Connections)**.
2. Дважды щелкните нужную политику и установите переключатель **Включить (Enabled)** или **Отключить (Disabled)**. Затем щелкните **OK**.

Политики удаленной помощи

Политики удаленной помощи позволяют запретить или разрешить удаленную помощь на компьютере. Как правило, политики удаленной помощи устанавливаются для отклонения непрошеных предложений удаленной помощи, разрешая при этом запрошенные. Также через политики можно указать срок истечения действия приглашений вместо установки этого ограничения через диалоговое окно свойств системы на каждом компьютере. Чтобы повысить безопасность, примените сильное шифрование приглашений, хоть это ограничит круг тех, кто может ответить на приглашение, пользователями Windows Vista и более поздних версий Windows.

Чтобы настроить политики удаленной помощи, выполните следующие действия:

1. Откройте групповые политики для компьютера, сайта, домена или подразделения, с которым вы собираетесь работать. Последовательно раскройте узлы **Конфигурация компьютера (Computer Configuration)**, **Административные шаблоны (Administrative Templates)**, **Система (System)** и **Удаленный помощник (Remote Assistance)**.
2. Дважды щелкните политику **Запрос удаленной помощи (Solicited Remote Assistance)** и установите переключатель **Включить (Enabled)**. В этом случае политика позволит авторизованным пользователям запрашивать удаленную помощь.
3. Задайте один из двух уровней доступа для помощников. В списке **Разрешить удаленное управление этим компьютером (Permit Remote Control of This Computer)** есть два варианта:

- **Помощники могут управлять компьютером (Allow helpers to remotely control the computer)** Разрешает просмотр и удаленное управление компьютером.
- **Помощники могут только наблюдать (Allow helpers to only view this computer)** Разрешает только просмотр, но не внесение изменений.

4. Как показано на рис. 3-9, задайте в полях **Максимальное время билета (значение) (Maximum Ticket Time (Value))** и **Максимальное время билета (объекты) (Maximum Ticket Time (Units))** максимальное время действия приглашения. По умолчанию оно равно 1 часу. Щелкните **ОК**.

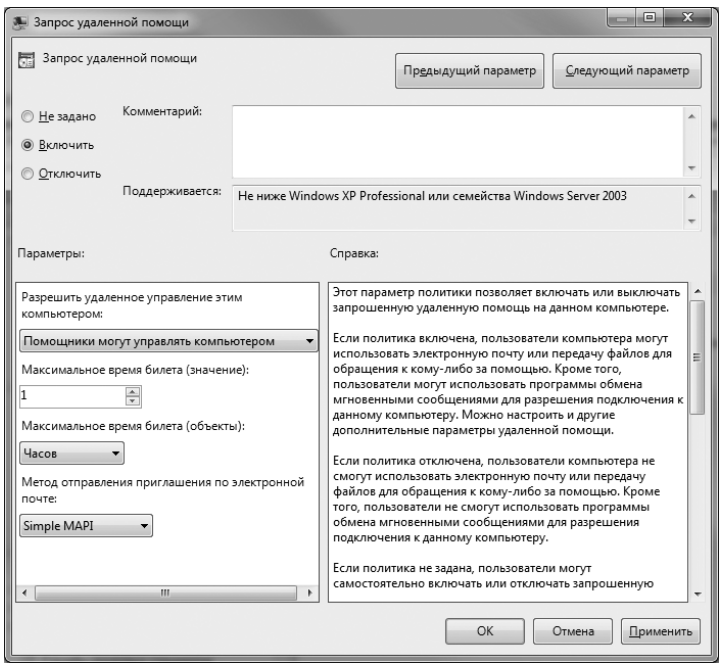

Рис. 3-9. Задайте время действия запросов на удаленную помощь

Ближе к реальности Для отсылки приглашений по электронной посте можно использовать варианты **Mailto** и **Simple MAPI**. Техника Mailto передачи почты опирается на программу-обозреватель. При ее использовании получатель приглашения подключается через Интернет-соединение. В варианте Simple MAPI используется интерфейс Messaging Application Programming Interface (MAPI): запрос отправляется как приложение к сообщению электронной почты. Если компьютеры могут установить соединение друг с другом через порт 80 и в наличии имеется стандартный почтовый клиент, например Microsoft Outlook или Windows Mail, стоит использовать Mailto.

5. Дважды щелкните политику **Предлагать удаленную помощь (Offer Remote Assistance)**. В диалоговом окне свойств политики установите переключатель **Отключить (Disabled)**. Это приведет к запрету незапрошенных предложений помощи. Щелкните **ОК**.

6. Чтобы использовать сильное шифрование приглашений и разрешить только соединения от компьютеров под управлением Windows Vista, Windows 7 и более поздних выпусков Windows, дважды щелкните политику **Разрешать подключения только с компьютеров под управлением Windows Vista или более новых систем (Allow Only Vista or Later Connections)**. В диалоговом окне политики установите переключатель **Включить (Enabled)** и щелкните **ОК**.

Для отказа от удаленной помощи и удаленного управления выполните следующие действия:

1. Откройте групповые политики для компьютера, сайта, домена или подразделения, с которым вы собираетесь работать. Откройте узел **Удаленный помощник (Remote Assistance)**.
2. Дважды щелкните политику **Запрос удаленной помощи (Solicited Remote Assistance)**. Установите переключатель **Отключить (Disable)** и щелкните **ОК**.
3. Дважды щелкните политику **Предлагать удаленную помощь (Offer Remote Assistance)**. Установите переключатель **Отключить (Disabled)** и щелкните **ОК**.

Политики сценариев

Политики сценариев управляют поведением и назначением компьютерных и пользовательских сценариев. Имеется четыре типа сценариев:

- **Сценарий загрузки (startup script)** Выполняется во время запуска компьютера.
- **Сценарий завершения работы (shutdown script)** Выполняется перед отключением компьютера.
- **Сценарий входа (logon script)** Выполняется при входе пользователя в систему.
- **Сценарий выхода (logoff script)** Выполняется при выходе пользователя из системы.

В качестве сценариев можно использовать пакетные файлы интерпретатора команд, а также сценарии Windows или Windows PowerShell. В пакетных файлах применяется язык интерпретатора команд, в сценариях Windows — сервер Windows Script Host (WSH) и язык сценариев, например Microsoft Visual Basic Scripting Edition (VBScript) или Microsoft JScript. Сценарии Windows PowerShell написаны на языке PowerShell. Обратите внимание, что часто от необходимости применения компьютерных и пользовательских сценариев избавляет использование предпочтений политик.

Управление сценариями при помощи политик

Политики, управляющие поведением сценариев, расположены в узлах административных шаблонов для категорий **Конфигурация компьютера (Com-**

puter Configuration) и **Конфигурация пользователя (User Configuration)**, в подузле **Система/Сценарии (System\Scripts)**. Основные политики описаны в табл. 3-4.

Табл. 3-4. Политики компьютерных и пользовательских сценариев

Тип политики	Название	Описание
Компьютер	Выполнить сценарии Windows PowerShell при запуске компьютера, завершить работу компьютера (Run Windows PowerShell Scripts First at Computer Startup, Shutdown)	Определяет, будут ли сценарии Windows PowerShell при загрузке и выключении запускаться прежде иных типов сценариев
Компьютер	Выполнять сценарии завершения работы с отображением команд (Run Shutdown Scripts Visible)	Отображает команды сценариев завершения в процессе их выполнения
Компьютер	Выполнять сценарии загрузки асинхронно (Run Startup Scripts Asynchronously)	Позволяет системе запускать сценарии одновременно, а не по очереди
Компьютер	Выполнять сценарии загрузки с отображением команд (Run Startup Scripts Visible)	Отображает команды сценарией загрузки в процессе их выполнения
Компьютер	Максимальное время выполнения сценариев групповой политики (Maximum Wait Time for Group Policy Scripts)	Задает максимальное время ожидания завершения сценариев. По умолчанию 600 секунд (10 минут)
Компьютер/ Пользователь	Выполнить сценарии Windows PowerShell при входе пользователя в систему, завершить сеанс (Run Windows PowerShell Scripts First At User Logon, Logoff)	Определяет, будут ли сценарии Windows PowerShell при входе и выходе из системы запускаться прежде иных типов сценариев
Компьютер/ Пользователь	Выполнять сценарии входа в систему синхронно (Run Logon Scripts Synchronously)	Определяет, будет ли система задерживать отображение интерфейса Windows до завершения сценариев входа в систему
Пользователь	Выполнять сценарии входа прежних версий в фоновом режиме (Run Legacy Logon Scripts Hidden)	Скрывает сценарии, настроенные через редактор системных политик Windows NT 4
Пользователь	Выполнять сценарии входа с отображением команд (Run Logon Scripts Visible)	Отображает команды сценариев входа в систему в процессе их выполнения

Табл. 3-4. (*окончание*)

Тип политики	Название	Описание
Пользователь	Выполнять сценарии выхода с отображением команд (Run Logoff Scripts Visible)	Отображает команды сценариев выхода из системы в процессе их выполнения

Есть много способов управления поведением сценариев, но, как правило, от них требуется следующее:

- В первую очередь выполняются сценарии Windows PowerShell.
- Сценарии загрузки и входа в систему должны выполняться одновременно (чаще всего).
- Все сценарии должны быть скрытыми.
- Система должна ожидать завершения сценария не более одной минуты (чаще всего).

Чтобы настроить такое поведение, выполните следующие действия:

1. Откройте групповые политики для компьютера, сайта, домена или подразделения, с которым вы собираетесь работать. Для настройки поведения сценариев используется узел **Сценарии (Scripts)**. Чтобы получить доступ к этому узлу, последовательно раскройте узлы **Конфигурация компьютера (Computer Configuration)**, **Административные шаблоны (Administrative Templates)** и **Система (System)**.
2. Дважды щелкните политику **Выполнить сценарии Windows PowerShell при запуске компьютера, завершить работу компьютера (Run Windows PowerShell Scripts First at Computer Startup, Shutdown)**. Установите переключатель **Включить (Enabled)** и щелкните **OK**.
3. Дважды щелкните политику **Выполнить сценарии Windows PowerShell при входе пользователя в систему, завершить сеанс (Run Windows PowerShell Scripts First At User Logon, Logoff)**. Установите переключатель **Включить (Enabled)** и щелкните **OK**.
4. Дважды щелкните политику **Выполнять сценарии входа в систему синхронно (Run Logon Scripts Synchronously)**. Установите переключатель **Отключить (Disable)** и щелкните **OK**.
5. Дважды щелкните политику **Выполнять сценарии загрузки асинхронно (Run Startup Scripts Asynchronously)**. Установите переключатель **Включить (Enabled)** и щелкните **OK**.
6. Дважды щелкните политику **Выполнять сценарии загрузки с отображением команд (Run Startup Scripts Visible)**. Установите переключатель **Отключить (Disable)** и щелкните **OK**.
7. Дважды щелкните политику **Выполнять сценарии завершения работы с отображением команд (Run Shutdown Scripts Visible)**. Установите переключатель **Отключить (Disable)** и щелкните **OK**.
8. Дважды щелкните политику **Максимальное время выполнения сценариев групповой политики (Maximum Wait Time for Group Policy Scripts)**.

Установите переключатель **Включить (Enabled)** и введите **60** в поле **Секунды (Seconds)**. Щелкните **ОК**.

9. Перейдите в узел **Административные шаблоны (Administrative Templates)** категории **Конфигурация пользователя (User Configuration)** и откройте узлы **Система (System)** и **Сценарии (Scripts)**.
10. Дважды щелкните политику **Выполнять сценарии входа прежних версий в фоновом режиме (Run Legacy Logon Scripts Hidden)**. Установите переключатель **Включить (Enabled)** и щелкните **OK**.
11. Дважды щелкните политику **Выполнять сценарии входа с отображением команд (Run Logon Scripts Visible)**. Установите переключатель **Отключить (Disable)** и щелкните **OK**.
12. Дважды щелкните политику **Выполнять сценарии выхода с отображением команд (Run Logoff Scripts Visible)**. Установите переключатель **Отключить (Disable)** и щелкните **OK**.
13. Дважды щелкните политику **Выполнить сценарии Windows PowerShell при входе пользователя в систему, завершить сеанс (Run Windows PowerShell Scripts First At User Logon, Logoff)**. Установите переключатель **Включить (Enabled)** и щелкните **OK**.

Назначение сценариев загрузки и завершения работы

Сценарии загрузки и выключения компьютера назначаются через групповую политику. При этом вы добьетесь, что сценарии будут автоматически запускаться при запуске и выключении компьютера всеми его пользователями, а также на всех компьютерах — членах сайта, домена или подразделения.

Для назначения сценариев загрузки и завершения работы выполните следующие действия:

1. Скопируйте нужные сценарии в папки Scripts\Startup и Scripts\Shutdown. На контроллерах доменов сценарии хранятся в папке %SystemRoot%\Sysvol\Sysvol*%UserDnsDomain%*\Policies*GUID*\Machine, а на рабочих станциях под управлением Windows 7 — в папке %WinDir%\System32\GroupPolicy\Machine.
2. Откройте для редактирования групповую политику ресурса, с которым собираетесь работать. Далее зайдите в политики настроек компьютера в узле **Конфигурация Windows\Сценарии (Windows Settings\Scripts)** категории **Конфигурация компьютера (Computer Configuration)**.
3. Для работы со сценариями загрузки щелкните правой кнопкой узел **Автозагрузка (Startup)** и выберите команду **Свойства (Properties)**. Для работы со сценариями завершения щелкните правой кнопкой узел **Завершение работы (Shutdown)** и выберите команду **Свойства (Properties)**.
4. Щелкните кнопку **Показать файлы (Show Files)**. Должны отобразиться скопированные вами сценарии.
5. Щелкните кнопку **Добавить (Add)**. Откроется диалоговое окно **Добавление сценария (Add a Script)**. Введите в поле **Имя сценария (Script**

Name) имя сценария, скопированного, соответственно, в папки Scripts\Startup или Scripts\Shutdown. Введите в поле **Параметры сценария (Script Parameters)** дополнительные аргументы командной строки для передачи их сценарию. Повторите это действие для добавления других сценариев.

6. В процессе запуска или выключения компьютера сценарии будут исполняться в том порядке, в каком они указаны в диалоговом окне свойств. При необходимости измените порядок следования сценариев при помощи кнопок **Вверх (Up)** и **Вниз (Down)**.
7. Чтобы изменить имя или параметры запуска сценария, выделите его в списке и щелкните кнопку **Изменить (Edit)**.
8. Чтобы удалить сценарий, выделите его в списке и щелкните **Удалить (Remove)**.

Назначение сценариев входа и выхода

Пользовательские сценарии также назначаются с помощью групповой политики. В этом случае назначенные сценарии будут автоматически выполняться при входе и выходе из системы для всех пользователей, заходящих на компьютер или являющихся членами сайта, домена или подразделения.

Для назначения пользовательских сценариев выполните следующие действия:

1. Скопируйте сценарии в папки Scripts\Logon и Scripts\Logoff, соответственно. На контроллерах доменов пользовательские сценарии хранятся в папке %SystemRoot%\Sysvol\Sysvol*%UserDnsDomain%*\Policies*GUID*\User, на рабочих станциях под управлением Windows 7 — в папке %WinDir%\System32\GroupPolicy\User .
2. Откройте для редактирования групповую политику ресурса, с которым собираетесь работать. Далее зайдите в политики настроек компьютера в узле **Конфигурация Windows\Сценарии (Windows Settings\Scripts)** категории **Конфигурация пользователя (User Configuration)**.
3. Для работы со сценариями входа в систему щелкните правой кнопкой узел **Вход в систему (Logon)** и выберите команду **Свойства (Properties)**. Для работы со сценариями выхода из системы щелкните правой кнопкой узел **Выход из системы (Logoff)** и выберите команду **Свойства (Properties)**.
4. Щелкните кнопку **Показать файлы (Show Files)**. Должны отобразиться скопированные вами сценарии.
5. Щелкните кнопку **Добавить (Add)**. Откроется диалоговое окно **Добавление сценария (Add a Script)**. Введите в поле **Имя сценария (Script Name)** имя сценария, скопированного, соответственно, в папки Scripts\Logon или Scripts\Logoff. Введите в поле **Параметры сценария (Script Parameters)** дополнительные аргументы командной строки для передачи их сценарию. Повторите это действие для добавления других сценариев.

6. В процессе входа в систему и выхода из нее сценарии будут исполняться в том порядке, в каком они указаны в диалоговом окне свойств. При необходимости измените порядок следования сценариев при помощи кнопок **Вверх (Up)** и **Вниз (Down)**.
7. Чтобы изменить имя или параметры запуска сценария, выделите его в списке и щелкните кнопку **Изменить (Edit)**.
8. Чтобы удалить сценарий, выделите его в списке и щелкните **Удалить (Remove)**.

Политики загрузки и входа в систему

В Windows 7 имеется набор политик для управления входа в систему. Некоторые из них позволяют настраивать выполнение программ при входе в систему, что делает их похожими на сценарии входа. Другие политики меняют вид экранов приветствия и входа в систему. В табл. 3-5 приведены основные политики загрузки и входа в систему. Для доступа к этим политикам откройте узлы **Конфигурация компьютера (Computer Configuration)** и **Конфигурация пользователя (User Configuration)**, **Административные шаблоны (Administrative Templates)**, **Система (System)** и **Вход в систему (Logon)**.

Табл. 3-5. Политики загрузки и входа в систему

Тип политики	Название	Описание
Компьютер	Всегда ждать сеть при запуске и входе в систему (Always Wait for the Network at Computer Startup And Logon)	Требует ожидания полной инициализации сети. Во время запуска эта политика будет применяться полностью, а не через фоновое обновление. При входе в систему это не позволит авторизоваться по кешированным учетным данным — авторизация будет возможна только через контроллер домена
Компьютер	Всегда использовать настраиваемый фон входа в систему (Always Use Custom Logon Background)	Позволяет использовать пользовательский фон на экране входа в систему
Компьютер	Всегда классический вход в систему (Always Use Classic Logon)	В качестве экрана приветствия вместо простого экрана входа в систему по умолчанию будет использоваться экран входа в систему предыдущих версий Windows
Компьютер/ Пользователь	Выполнять эти программы при входе в систему (Run these Programs at User Logon)	Задает программы, которые должны запускаться при входе в систему. Указывайте полный путь (кроме программ в %SystemRoot%)

Табл. 3-5. (*окончание*)

Тип политики	Название	Описание
Компьютер/ Пользователь	Не обрабатывать список запуска старых программ (Do not Process the Legacy Run List)	Запрещает запуск приложений из устаревшего списка запуска, кроме установленных через редактор системной политики Windows NT 4
Компьютер/ Пользователь	Не обрабатывать список однократного запуска программ (Do not Process the Run-Once List)	Задает игнорирование пользовательских списков однократного запуска

Классический экран и простой экран приветствия

В Windows 7 реализован простой экран приветствия. По умолчанию для авторизации применяется именно он, но некоторые пользователи, вероятно, предпочтут классическое окно входа в систему. Для использования классического входа в систему выполните следующие действия:

1. Откройте групповую политику для компьютера, с которым собираетесь работать. Откройте узлы **Конфигурация компьютера (Computer Configuration)**, **Административные шаблоны (Administrative Templates)**, **Система (System)** и **Вход в систему (Logon)**.
2. Дважды щелкните политику **Всегда классический вход в систему (Always Use Classic Logon)**. Установите переключатель **Включить (Enabled)** и щелкните **OK**.

Примечание Подробнее об экранах входа — в главе 5.

Установка автозапуска программ посредством политик

Пользователи могут настраивать автозапуск программ сами, но обычно разумнее проделать это через групповые политики, особенно в условиях предприятия, когда многим пользователям требуется одно и то же приложение. Чтобы задать автозапуск программы при входе в систему, выполните следующие действия:

1. Откройте групповую политику для компьютера, с которым собираетесь работать. Откройте узлы **Конфигурация компьютера (Computer Configuration)**, **Административные шаблоны (Administrative Templates)**, **Система (System)** и **Вход в систему (Logon)**.
2. Дважды щелкните политику **Выполнять эти программы при входе в систему (Run These Programs at User Logon)**. Установите переключатель **Включить (Enabled)**.
3. Щелкните кнопку **Показать (Show)**. В диалоговом окне **Вывод содержания (Show Contents)** укажите полный путь к файлу приложения

в обычном формате или формате UNC, например C:\Program Files (x86)\Internet Explorer\Iexplore.exe или \\DCServ01\Apps\Stats.exe.

4. Закройте все открытые диалоговые окна.

Отключение списков запуска посредством политик

С помощью групповых политик можно отключить устаревшие списки запуска и однократного запуска. Списки запуска хранятся в реестре в разделах HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run и HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run.

Администраторы создают списки однократного запуска для указания программ, которые надо запустить только при очередной загрузке системы, но не нужно запускать при последующих загрузках. Списки однократного запуска хранятся в реестре в разделах HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce и HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce.

Для отключения списков запуска выполните следующие действия:

1. Откройте групповую политику для компьютера, с которым собираетесь работать. Откройте узлы **Конфигурация компьютера (Computer Configuration)**, **Административные шаблоны (Administrative Templates)**, **Система (System)** и **Вход в систему (Logon)**.
2. Дважды щелкните политику **Не обрабатывать список однократного запуска программ (Do Not Process the Run Once List)**. Установите переключатель **Включить (Enabled)** и щелкните **OK**.
3. Дважды щелкните политику **Не обрабатывать список запуска старых программ (Do Not Process the Legacy Run List)**. Установите переключатель **Включить (Enabled)** и щелкните **OK**.

Глава 4

Автоматическая настройка Windows 7

Предпочтения групповой политики (Group Policy preference) позволяют автоматически настраивать и развертывать ОС, а также управлять параметрами ОС и приложений, включая параметры источников данных, сопоставления дисков, переменные среды, общие сетевые ресурсы, папки и ярлыки. Когда нужно развернуть и настроить компьютеры, проще сделать это при помощи предпочтений групповой политики, чем выполнять все необходимые действия вручную на каждом компьютере, при помощи образов Windows или сценариев загрузки, входа, выхода и завершения работы.

Эта глава познакомит вас с предпочтениями и позволит приобрести необходимые навыки по управлению предпочтениями групповой политики. В следующих главах речь пойдет об автоматизации настройки компьютеров под управлением Windows в малых, средних и крупных компаниях.

Предпочтения групповой политики

Предпочтения настраивают в групповой политике Active Directory. В локальной групповой политике предпочтений нет. Предпочтения групповой политики не применяются строго и не хранятся в ветвях реестра, относящихся к политикам. В реестре предпочтения записываются в те же разделы, что используются компонентами ОС или приложениями для хранения соответствующих параметров. Таким образом, предпочтения доступны приложениям и компонентам ОС, которые не связаны с групповой политикой.

Предпочтения не отключают приложения и компоненты ОС в пользовательском интерфейсе. Пользователям разрешается изменять параметры, заданные в предпочтениях групповой политики. Но предпочтения перезаписывают существующие параметры, и способа восстановить эти параметры нет.

В групповой политике предпочтения, как и параметры, обновляются с постоянным интервалом, по умолчанию составляющим 90-120 мин. Это означает, что настроенные вами предпочтения периодически применяются на компьютере пользователя. Обновление отдельных предпочтений групповой политикой можно запретить, установив их однократное применение.

Способ работы с предпочтениями зависит от того, будет ли настраиваемый элемент применяться принудительно. Если не будет, примените пред-

почтения политики, а затем отключите автоматическое обновление. Чтобы настроить элемент с принудительным применением параметров, настройте предпочтения при помощи параметров политики, а затем включите автоматическое обновление.

Предпочтения применимы к параметрам конфигурации компьютера и пользователя. Поэтому как в разделе **Конфигурация компьютера (Computer Configuration)**, так и в разделе **Конфигурация пользователя (User Configuration)** имеется узел **Настройки (Preferences)**. В обоих случаях этот узел разделяется на два подузла:

- **Конфигурация Windows (Windows Settings)** Управление общими предпочтениями ОС и приложений.
- **Параметры панели управления (Control Panel Settings)** Управление предпочтениями панели управления.

В табл. 4-1 приведены доступные предпочтения и сведения об их расположении.

Табл. 4-1. Настраиваемые предпочтения групповой политики

Тип предпочтения	Где находится	Область конфигурирования
INI-файлы (Ini Files)	Конфигурация Windows (Windows Settings)	Конфигурация компьютера (Computer Configuration) и Конфигурация пользователя (User Configuration)
Главное меню (Start Menu)	Параметры панели управления (Control Panel Settings)	Конфигурация пользователя (User Configuration)
Источники данных (Data Sources): Пользовательский источник данных (User Data Source)	Параметры панели управления (Control Panel Settings)	Конфигурация пользователя (User Configuration)
Источники данных (Data Sources): Системный источник данных (System Data Source)	Параметры панели управления (Control Panel Settings)	Конфигурация компьютера (Computer Configuration) и Конфигурация пользователя (User Configuration)
Локальные пользователи и группы (Local Users And Groups)	Параметры панели управления (Control Panel Settings)	Конфигурация компьютера (Computer Configuration) и Конфигурация пользователя (User Configuration)
Назначенные задания (Scheduled Tasks): Запланированное задание (Scheduled Task)	Параметры панели управления (Control Panel Settings)	Конфигурация компьютера (Computer Configuration) и Конфигурация пользователя (User Configuration)

Табл. 4-1. (*продолжение*)

Тип предпочтения	Где находится	Область конфигурирования
Назначенные задания (Scheduled Tasks): Немедленная задача (Immediate Task)	Параметры панели управления (Control Panel Settings)	Конфигурация компьютера (Computer Configuration) и Конфигурация пользователя (User Configuration)
Общие сетевые ресурсы (Network Shares)	Конфигурация Windows (Windows Settings)	Конфигурация компьютера (Computer Configuration)
Папки (Folders)	Конфигурация Windows (Windows Settings)	Конфигурация компьютера (Computer Configuration) и Конфигурация пользователя (User Configuration)
Приложения (Applications)	Конфигурация Windows (Windows Settings)	Конфигурация пользователя (User Configuration)
Принтеры (Printers): TCP/IP-принтер (TCP/IP Printer)	Параметры панели управления (Control Panel Settings)	Конфигурация компьютера (Computer Configuration) и Конфигурация пользователя (User Configuration)
Принтеры (Printers): Локальный принтер (Local Printer)	Параметры панели управления (Control Panel Settings)	Конфигурация компьютера (Computer Configuration) и Конфигурация пользователя (User Configuration)
Принтеры (Printers): Общий принтер (Shared Printer)	Параметры панели управления (Control Panel Settings)	Конфигурация пользователя (User Configuration)
Региональные параметры (Regional Options)	Параметры панели управления (Control Panel Settings)	Конфигурация пользователя (User Configuration)
Реестр (Registry)	Конфигурация Windows (Windows Settings)	Конфигурация компьютера (Computer Configuration) и Конфигурация пользователя (User Configuration)
Свойства папки (Folder Options): Дополнительные параметры папки (Advanced folder options)	Параметры панели управления (Control Panel Settings)	Конфигурация пользователя (User Configuration)
Свойства папки (Folder Options): Открыть с помощью (Open With)	Параметры панели управления (Control Panel Settings)	Конфигурация пользователя (User Configuration)
Свойства папки (Folder Options): Тип файла (File Type)	Параметры панели управления (Control Panel Settings)	Конфигурация компьютера (Computer Configuration)

Табл. 4-1. (*окончание*)

Тип предпочтения	Где находится	Область конфигурирования
Сетевые параметры (Network Options): VPN-подключение (VPN Connection)	Параметры панели управления (Control Panel Settings)	Конфигурация компьютера (Computer Configuration) и Конфигурация пользователя (User Configuration)
Сетевые параметры (Network Options): Подключение удаленного доступа (Dial-Up Connection)	Параметры панели управления (Control Panel Settings)	Конфигурация компьютера (Computer Configuration) и Конфигурация пользователя (User Configuration)
Службы (Services)	Параметры панели управления (Control Panel Settings)	Конфигурация компьютера (Computer Configuration)
Сопоставления дисков (Drive Maps)	Конфигурация Windows (Windows Settings)	Конфигурация пользователя (User Configuration)
Среда (Environment): Пользовательская переменная (User Variable)	Конфигурация Windows (Windows Settings)	Конфигурация компьютера (Computer Configuration) и Конфигурация пользователя (User Configuration)
Среда (Environment): Системная переменная (System Variable)	Конфигурация Windows (Windows Settings)	Конфигурация компьютера (Computer Configuration) и Конфигурация пользователя (User Configuration)
Устройства (Devices)	Параметры панели управления (Control Panel Settings)	Конфигурация компьютера (Computer Configuration) и Конфигурация пользователя (User Configuration)
Файлы (Files)	Конфигурация Windows (Windows Settings)	Конфигурация компьютера (Computer Configuration) и Конфигурация пользователя (User Configuration)
Электропитание (Power Options)	Параметры панели управления (Control Panel Settings)	Конфигурация компьютера (Computer Configuration) и Конфигурация пользователя (User Configuration)
Ярлыки (Shortcuts)	Конфигурация Windows (Windows Settings)	Конфигурация компьютера (Computer Configuration) и Конфигурация пользователя (User Configuration)

Настройка предпочтений групповой политики

Настройка и управление предпочтениями существенно отличаются от настройки и управления параметрами политики. Чтобы настроить предпочте-

ние нужно указать управляющее действие, состояние редактирования или и то, и другое сразу.

Управляющие действия

Большинство предпочтений поддерживают следующие управляющие действия:

- **Создать (Create)** Создание элемента предпочтения на компьютере пользователя. Элемент предпочтения создается лишь в том случае, если он еще не существует.
- **Заменить (Replace)** Удаление и повторное создание существующего элемента предпочтения, или создание элемента, если он еще не создан. У большинства предпочтений есть дополнительные параметры, точно определяющие поведение операции замены. Пример см. на рис. 4-1.
- **Обновить (Update)** Изменение заданных параметров элемента предпочтения. Это действие отличается от замены тем, что воздействует только на параметры, определенные в самом элементе предпочтения. Все остальные параметры остаются без изменений. Если элемент предпочтения не существует, в ходе обновления он создается.
- **Удалить (Delete)** Удаление элемента предпочтения с компьютера пользователя. У большинства предпочтений есть дополнительные свойства, точно определяющие поведение операции удаления. Часто они совпадают с дополнительными свойствами операции замены.

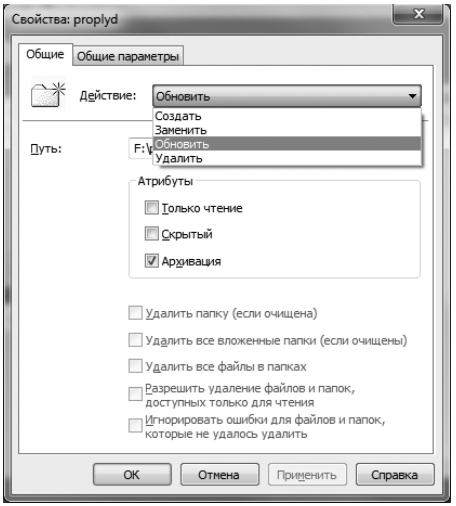

Рис. 4-1. Назначение управляющего действия

Применение предпочтения и его удаление регулируются управляющим действием. Предпочтения с поддержкой управляющих действий используются для настройки:

- источников данных;

- общих сетевых ресурсов;
- папок;
- приложений;
- реестра;
- сопоставлений дисков;
- среды;
- файлов;
- ярлыков.

Состояние редактирования

Состояния редактирования (editing state) поддерживаются немногими предпочтениями и управляются посредством графического интерфейса панели управления. В этом типе предпочтений применение элемента зависит от состояния редактирования каждого параметра соответствующего интерфейса. Примененное состояние редактирования нельзя отменить. Также нельзя удалить более не применяющиеся состояния редактирования.

Предпочтения с поддержкой состояний редактирования используются для настройки параметров:

- главного меню;
- обозревателя;
- папок;
- региональных;
- электропитания.

Интерфейс программы или Windows от версии к версии может изменяться, поэтому реальные параметры зависят от версии. В частности, элементы предпочтений параметров папок для Internet Explorer 7 и Internet Explorer 8 должны настраиваться по отдельности.

По умолчанию, когда вы работаете с данным типом предпочтений, на компьютере клиента будет обработан и применен каждый параметр, который есть в интерфейсе, даже если вы не задали его значение. То есть, по сути, переписываются все существующие параметры, настраиваемые в интерфейсе. Состояние редактирования соответствующих параметров отображается графически (рис. 4-2).

- Сплошной зеленой линией обозначены параметры, которые будут доставлены на клиентский компьютер и обработаны на нем.
- Красным пунктиром выделены параметры, которые не будут доставлены на клиентский компьютер или обработаны на нем.

Если подчеркивание невозможно из-за ограниченного размера интерфейса, вместо сплошной зеленой линии (параметр будет доставлен и обработан на клиенте) рисуется зеленый кружок. Красный кружок используется как эквивалент красного пунктира (параметр не будет доставлен или обработан на клиенте). Пример см. на рис. 4-3.

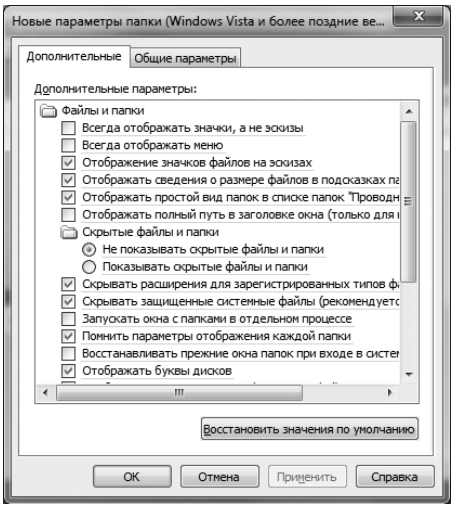

Рис. 4-2. Значки состояния редактирования

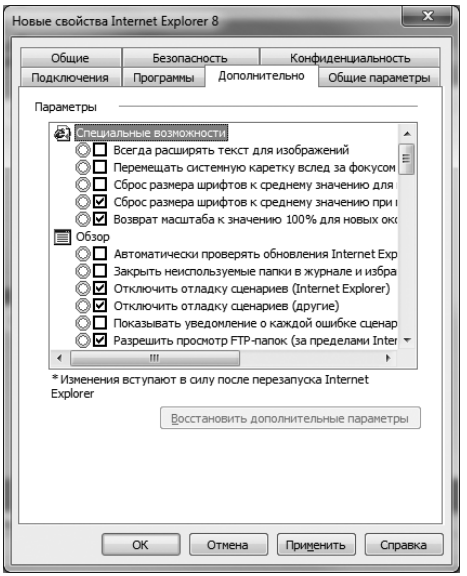

Рис. 4-3. Альтернативные значки состояния редактирования

Для управления состоянием редактирования предназначены следующие функциональные клавиши:

- **F5** Обработка всех параметров на выбранной вкладке. Используйте ее, если вы сначала отключили некоторые параметры, а затем решили обрабатывать все параметры на вкладке.
- **F6** Обработка текущего параметра, выбранного на вкладке. Используйте ее, если вы, отключив параметр, позже вы все-таки решили его обработать.

- **F7** Отключение обработки текущего параметра, выбранного на вкладке. Применяется для запрета обработки одного параметра на клиенте.
- **F8** Отключение обработки всех параметров на выбранной вкладке. Применяется для запрета обработки на клиенте всех параметров вкладки, а также для выбора небольшого количества параметров.

Примечание Помните, что значение параметра не связано с состоянием редактирования. Задание и сброс параметра не влияют на состояние редактирования.

Альтернативные действия и состояния

Несколько предпочтений не поддерживают ни управляющие действия, ни состояния редактирования. К этому типу относятся предпочтения настройки устройств, немедленных заданий (immediate task) и служб.

Включить и отключить конкретный тип устройств можно в списке **Действие (Action)**, показанном на рис. 4-4. В случае немедленных задач соответствующее предпочтение создает задачу. После выполнения задача автоматически удаляется. При помощи предпочтений служб осуществляется настройка существующей службы.

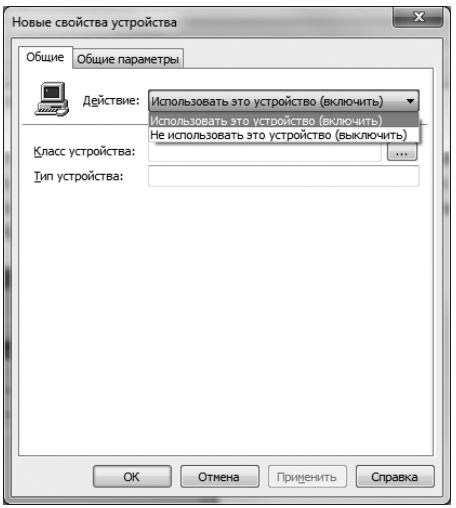

Рис. 4-4. Включение и отключение устройства при помощи действия

Управление элементами предпочтения

Для работы с предпочтениями необходимо открыть для редактирования объект групповой политики (GPO) в редакторе управления групповыми политиками, как описано в главе 3. Дальнейшее управление предпочтениями как для компьютера, так и для пользователя осуществляется следующими способами:

- Чтобы настроить предпочтения, применяемые к компьютеру независимо от работающего на нем пользователя, дважды щелкните узлы **Конфигура-**

ция компьютера (Computer Configuration) и **Настройки (Preferences)**, а затем выберите нужную категорию предпочтений.

- Чтобы настроить предпочтения, применяемые к пользователям независимо от компьютера, на который выполнен вход, дважды щелкните узел **Конфигурация пользователя (User Configuration)** и **Настройки (Preferences)**, а затем выберите нужную категорию предпочтений.

Создание и управление элементом предпочтения

Управляйте элементами предпочтения по отдельности. Выберите категорию предпочтений и работайте с соответствующим элементом в области сведений. Чтобы в категории создать новый элемент, щелкните правой кнопкой пустое место в области сведений, раскройте подменю **Создать (New)** и выберите тип создаваемого элемента. Элементы можно создавать только в выбранной категории. Например, находясь в категории **Принтеры (Printers)** узла **Конфигурация компьютера (Computer Configuration)**, можно создать предпочтение **TCP/IP-принтер (TCP/IP Printer)** или **Локальный принтер (Local Printer)**.

Чтобы управлять элементом, щелкните его правой кнопкой (рис. 4-5). Те же команды доступны на панели инструментов при выделении элемента. Чтобы открыть диалоговое окно свойств элемента, щелкните его правой кнопкой и выберите команду **Свойства (Properties)** или просто дважды щелкните элемент. Окно свойств предназначено для просмотра и редактирования параметров элемента предпочтения.

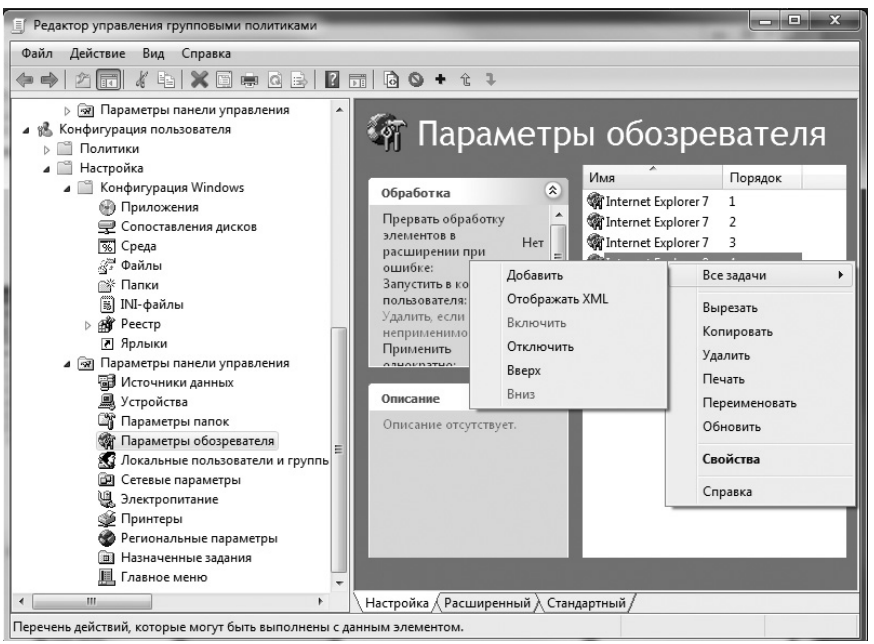

Рис. 4-5. Управление элементами предпочтений в редакторе управления групповыми политиками

На клиентских компьютерах элементы предпочтений обрабатываются клиентом групповой политики, исходя из их приоритета. Элемент предпочтения с наименьшим приоритетом (последний из списка) обрабатывается первым. Далее следует элемент предпочтения с более высоким приоритетом и т. д., вплоть до элемента с наивысшим приоритетом (первого в списке).

Такой порядок обработки обусловлен необходимостью обеспечить преимущество элементов предпочтения с высоким приоритетом над элементами с более низким приоритетом. В случае возникновения конфликта между параметрами элементов предпочтения, действуют параметры, записанные последними. Для изменения приоритета выберите категорию предпочтений в дереве консоли, а затем в области сведений щелкните нужный элемент. На панели инструментов появятся дополнительные команды, в частности **Переместить выделенный объект вверх (Move The Selected Item Up)** и **Переместить выделенный объект вниз (Move The Selected Item Down)**. Чтобы повысить приоритет выбранного элемента, щелкните первую команду. Чтобы понизить приоритет, щелкните вторую команду.

Установка параметров на вкладке Общие параметры (Common)

В окнах свойств всех элементов предпочтения есть вкладка **Общие параметры (Common)**, на которой находятся общие для всех элементов предпочтения параметры. Полный список общих параметров зависит от элемента, но у большинства элементов имеются параметры, показанные на рис. 4-6.

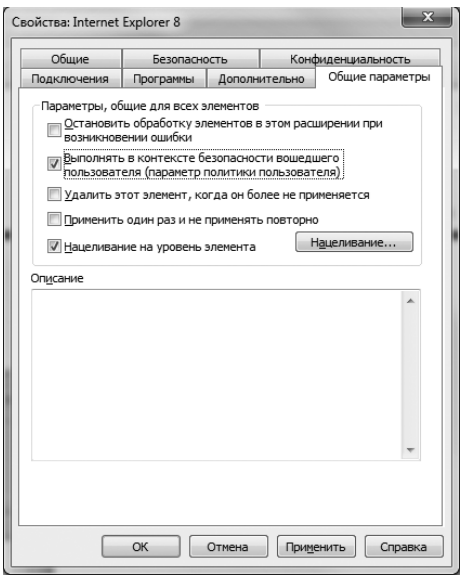

Рис. 4-6. Дополнительные параметры на вкладке Общие параметры (Common)

Вот как используются общие параметры:

- **Остановить обработку элементов в этом расширении при возникновении ошибки (Stop Processing Items In This Extension If An Error Oc-**

curs) По умолчанию при сбое в обработке одного элемента предпочтения обработка других элементов будет продолжена. Чтобы изменить это правило, установите флажок **Остановить обработку элементов в этом расширении при возникновении ошибки (Stop Processing Items In This Extension If An Error Occurs)**. Теперь в случае сбоя элемента остальные элементы предпочтения в этом расширении для данного объекта GPO обрабатываться не будут. Этот параметр не влияет на обработку внутри других объектов GPO.

- **Выполнять в контексте безопасности вошедшего пользователя (Run In Logged-On User's Security Context)** По умолчанию предпочтения пользователя обрабатываются клиентом групповой политики в контексте безопасности учетной записи System (для Windows Vista и более поздних версий) или Winlogon (для предшествующих версий). В этом контексте расширение ограничено доступом только к тем переменным среды и ресурсам системы, которые доступны для компьютера. В качестве альтернативы предпочтения пользователя могут быть обработаны клиентом в контексте безопасности пользователя, выполнившего вход в систему. Расширение при этом получит доступ к ресурсам от имени пользователя, а не от имени системной службы. Это нужно при использовании сопоставлений дисков или других предпочтений, когда у компьютера нет разрешений на доступ к нужным ресурсам или когда необходимо работать с переменными среды пользователя.
- **Удалить этот элемент, когда он более не применяется (Remove This Item When It Is No Longer Applied)** Если параметры политики в объекте GPO более не применяются к пользователю или компьютеру, они по умолчанию удаляются, поскольку не задаются в области групповой политики реестра. В отличие от них, стандартные элементы предпочтения не удаляются автоматически, даже если объект GPO более не применяется к пользователю или компьютеру. Чтобы изменить такое поведение, установите этот флажок. Если он установлен, присутствие элемента предпочтения в области видимости определяется расширением. Если элемент предпочтения находится вне области видимости, связанные с ним параметры удаляются.

Ближе к реальности В общем случае, когда предпочтения с поддержкой управляющих действий более не применяются, их можно удалить. А вот предпочтения с поддержкой состояния редактирования удалить нельзя. Если вы установите флажок **Удалить этот элемент, когда он более не применяется (Remove This Item When It Is No Longer Applied)**, для элемента будет задано управляющее действие Заменить (Replace). В результате при обработке расширением групповой политики сначала выполняется операция Удалить (Delete), а затем — Создать (Create). Далее, если элемент предпочтения выпадает из области видимости для пользователя или компьютера (более не применяется), результаты элемента предпочтения удаляются (но не воссоздаются). Причиной выпадения элемента предпочтения из области видимости может также стать нацеливание конечных объектов на уровне элемента.

- **Применить один раз и не применять повторно (Apply Once And Do Not Reapply)** Предпочтения записываются групповой политикой в те же расположения реестра, что используются для хранения параметров компонентами ОС или приложений. Поэтому пользователи вольны изменять параметры, заданные при помощи предпочтений. Но по умолчанию результаты элементов предпочтения переписываются при каждом обновлении групповой политики. Это обеспечивает применение элементов предпочтения в соответствии с замыслом администраторов. Чтобы изменить такое поведение, установите этот флажок. Когда он установлен, результаты элемента предпочтения применяются расширением предпочтения только один раз без повторного применения.
- **Нацеливание на уровень элемента (Item-Level Targeting)** Нацеливание на уровень элемента позволяет применять элемент предпочтения только к выбранным пользователям или компьютерам. Когда предпочтение конечного объекта проверяется клиентом групповой политики, каждому элементу конечного объекта присваивается значение «истина» или «ложь». Если результирующее значение «истина», элемент применяется и обрабатывается. В значении «ложь» элемент не применяется и не обрабатывается. Установив этот флажок, щелкните кнопку **Нацеливание (Targeting)**, чтобы открыть окно **Редактор нацеливания (Targeting Editor)**, и настройте целевой объект.

Ближе к реальности Целевые объекты на уровне элемента проверяются как логическое выражение. Оно может включать переменные среды, поскольку переменные среды присутствуют в контексте текущего пользователя. После создания логического выражения убедитесь, что в выражении есть смысл. Если вместо переменной среды в код включить значение, определение конечных объектов может работать неправильно.

Глава 5

Управление доступом и безопасность

Компьютеры под управлением Windows 7 могут принадлежать к домашней группе, рабочей группе или домену. Если рабочая станция входит в состав домашней или рабочей группы, параметры доступа пользователей и параметры безопасности настраиваются непосредственно на самой рабочей станции. У станции, являющейся членом домена, есть два уровня доступа и безопасности: уровень локальной системы и уровень домена. Параметры доступа пользователей к физическому компьютеру задаются на уровне локальной системы, доступ к другим системам и ресурсам текущего леса Active Directory настраивается на уровне домена. Прочитав эту главу, вы научитесь управлять локальными учетными записями и параметрами доступа к локальной системе. Сведения по настройке разрешений и параметров доступа в домене вы найдете в книге *Windows Server 2008 Administrator's Pocket Consultant,* Second Edition (Microsoft Press, 2010). Для выполнения любой задачи из этой и последующих глав достаточно войти в систему локально или через подключение удаленного рабочего стола.

Учетные записи пользователей и групп

В Windows 7 используются учетные записи пользователей и учетные записи групп (членами которых могут быть пользователи). Учетные записи пользователей предназначены для отдельных личностей. Учетные записи групп (или для краткости просто группы) — это инструмент для управления несколькими пользователями. Вход в систему выполняется только с учетной записью пользователя.

Учетные записи делятся на два общих типа:

- **Учетная запись локального пользователя** Определяется только на локальном компьютере. Доступ локального пользователя ограничен локальным компьютером. Для добавления и удаления учетных записей локальных пользователей используйте категорию Учетные записи пользователей (User Accounts)* панели управления или утилиту Локальные

* Если компьютер Windows 7 является членом рабочей (домашней) группы, этот элемент называется «Учетные записи пользователей и семейная безопасность». Когда компьютер подключается к домену, название меняется на «Учетные записи пользователей». — *Прим. перев.*

пользователи и группы (Local Users And Groups) из оснастки Управление компьютером (Computer Management).

- **Учетная запись пользователя домена** Определяется в Active Directory. В режиме единого входа (single sign-on) с ее помощью можно получить доступ к ресурсам всего леса. Если компьютер входит в состав домена Active Directory, для создания учетных записей пользователей домена используется оснастка Active Directory — пользователи и компьютеры (Active Directory Users And Computers). Вы найдете ее в меню Администрирование (Administrative Tools), установив на компьютер компонент RSAT.

Существуют стандартные и административные учетные записи локального пользователя и пользователя домена. Стандартная учетная запись на локальном компьютере обладает ограниченными полномочиями, тогда как полномочия учетной записи администратора расширены.

Учетная запись локального пользователя

У всех учетных записей пользователей имеется имя для входа (logon name). В Windows 7 оно состоит из двух частей:

- **Имя пользователя** Отображаемый на экране текст.
- **Компьютер или домен пользователя** Компьютер или домен, к которому относится учетная запись пользователя.

Например, полное имя для входа в Windows 7 пользователя Evgeny, учетная запись которого создана на компьютере ENGPC85, выглядит как ENGPC85\Evgeny. Учетная запись на локальном компьютере позволяет выполнить вход на локальную рабочую станцию и работать с ее ресурсами без права доступа к ресурсам домена.

В домене полное имя для входа выражается двумя способами:

- **Имя учетной записи, отделенное символом «@» от полного доменного имени** Например, полное имя для входа пользователя Evgeny в домене technology.microsoft.com будет *Evgeny@technology.microsoft.com*.
- **Имя учетной записи, отделенное от домена обратной косой чертой «\»** Например, полное имя для входа пользователя Evgeny в домене technology будет *technology\Evgeny*.

В Windows 7 полномочия и разрешения учетной записи отображаются с указанием имени пользователя, однако истинным идентификатором учетной записи является идентификатор безопасности (security identifier, SID), который генерируется во время создания участника безопасности (security principal). Идентификатор SID состоит из комбинации префикса идентификатора безопасности компьютера или домена и уникального относительного идентификатора пользователя (relative ID). В Windows 7 идентификаторы SID обеспечивают независимое отслеживание имен и учетных записей пользователей. Они используются для различных целей, но наиболее важны две — возможность изменить имя пользователя и возможность удалить

учетную запись, не беспокоясь о том, что кто-то сможет получить доступ к ресурсам, создав учетную запись с тем же именем.

Если вы измените имя пользователя, в Windows 7 с новым именем попрежнему будет сопоставлен существующий SID. После удаления учетной записи ее SID становится недействительным. Даже если вы создадите учетную запись с точно таким же именем пользователя, полномочия и разрешения новой учетной записи будут иными, так как с ней будет сопоставлен другой SID.

С учетной записью пользователя могут быть связаны пароли и сертификаты. Сертификат представляет собой комбинацию открытого и закрытого ключей для идентификации пользователя. При помощи пароля выполняется интерактивный вход в систему. Для входа с сертификатом используется закрытый ключ, который хранится на смарт-карте и считывается специальным устройством.

В процессе установки Windows 7 на компьютер устанавливаются стандартные учетные записи пользователей. Их несколько, и служат они тем же целям, что и учетные записи, создаваемые в домене Windows. Ключевые среди них:

- **Администратор (Administrator)** Стандартная учетная запись с полным доступом к файлам, папкам, службам и прочим средствам. Ее нельзя удалить или отключить. В Active Directory полномочия учетной записи администратора охватывают весь домен. На локальной рабочей станции доступ администратора ограничен ее пределами.
- **Гость (Guest)** Предназначена для предоставления разового или нерегулярного доступа. Системные полномочия гостей весьма ограничены. Тем не менее, используйте эту учетную запись с особой осторожностью, ибо она может стать причиной взлома системы. Риск настолько велик, что по умолчанию после установки Windows 7 эта учетная запись отключена.

По умолчанию перечисленные учетные записи являются членами различных групп. Прежде чем изменять любую из встроенных учетных записей, обратите внимание на свойства и членство в группах. Членство в группах — способ управления доступом учетной записи к определенным системным ресурсам. В частности, учетная запись Администратор (Administrator) является членом группы Администраторы (Administrators), а учетная запись Гость (Guest) входит в группу Гости (Guests). Членство в группе дает учетной записи возможность пользоваться полномочиями и правами группы.

Помимо встроенных в Windows 7 существуют системные учетные записи, используемые для выполнения отдельных системных действий. Системные учетные записи есть только в локальной системе. Их параметры нельзя изменить средствами администрирования пользователей. Кроме того, с их помощью нельзя выполнить вход на компьютер. Системные учетные записи таковы:

- **Локальная система (LocalSystem)** Применяется для выполнения системных процессов и обработки задач на уровне системы. Обладает пра-

вом Вход в качестве службы (Log On As A Service), поэтому от ее имени выполняется большинство служб. В некоторых случаях у этих служб есть полномочия на взаимодействие с рабочим столом. Службы, которым нужны меньшие полномочия или права, выполняются с учетными записями Локальная служба (LocalService) или Сетевая служба (NetworkService). От имени учетной записи Локальная система (LocalSystem) выполняются такие службы, как Браузер компьютеров (Computer Browser), Диспетчер печати (Print Spooler), Клиент групповой политики (Group Policy Client), Сетевой вход в систему (Netlogon), Сетевые подключения (Network Connections), Служба профилей пользователей (User Profile Service) и Фоновая интеллектуальная служба передачи (Background Intelligent Transfer Service).

- **Локальная служба (LocalService)** Предназначена для служб, которым требуется меньше полномочий и прав входа в локальную систему. По умолчанию службам, выполняющимся с данной учетной записью, предоставляются право Вход в качестве службы (Log On As A Service) и следующие разрешения: Настройка квот памяти для процесса (Adjust Memory Quotas For A Process), Изменение системного времени (Change The System Time), Изменение часового пояса (Change The Time Zone), Создание аудитов безопасности (Generate Security Audits) и Замена маркера уровня процесса (Replace A Process Level Token). От имени учетной записи Локальная служба (LocalService) выполняются такие службы, как Веб-клиент (WebClient), Модуль поддержки NetBIOS через TCP/IP (TCP/IP NetBIOS Helper), Обнаружение SSDP (SSDP Discovery Service), Служба шлюза уровня приложения (Application Layer Gateway Service), Смарт-карта (Smart Card) и Удаленный реестр (Remote Registry).
- **Сетевая служба (NetworkService)** Применяется для служб, которым нужно немного полномочий и прав входа в локальную систему, но необходим доступ к сетевым ресурсам. Как и учетной записи Локальная служба (LocalService), учетной записи Сетевая служба (NetworkService) предоставлено право Вход в качестве службы (Log On As A Service) и следующие разрешения: Настройка квот памяти для процесса (Adjust Memory Quotas For A Process), Создание аудитов безопасности (Generate Security Audits) и Замена маркера уровня процесса (Replace A Process Level Token). От имени учетной записи Сетевая служба (NetworkService) выполняются такие службы, как BranchCache, DNS-клиент (DNS Client), Координатор распределенных транзакций (Distributed Transaction Coordinator), Службы удаленных рабочих столов (Remote Desktop Services) и Удаленный вызов процедур (Remote Procedure Call). Учетная запись Сетевая служба (NetworkService) может проходить проверку подлинности на удаленных системах в качестве учетной записи компьютера.

Учетная запись группы

Существующие в Windows 7 группы используются для предоставления пользователям однотипных разрешений, что упрощает администрирование. Если пользователь входит в состав группы, у которой есть доступ к некоему ресурсу, он также имеет доступ к этому ресурсу. Чтобы предоставить пользователю доступ к различным ресурсам, достаточно включить его в нужную группу. С учетной записью пользователя можно войти в систему; с учетной записью группы этого сделать нельзя. В разных доменах Active Directory или на разных компьютерах могут существовать группы с одинаковыми именами. Поэтому имена групп часто указывают в виде *Домен\ИмяГруппы* или *Компьютер\ИмяГруппы* (скажем, в домене или на компьютере с именем Technology группа GMarketing может называться Technology\GMarketing).

В Windows 7 используются группы трех типов:

- **Локальные группы** Определяются на локальном компьютере и используются только на нем. Локальные группы создаются при помощи утилиты Локальные пользователи и группы (Local Users And Groups).
- **Группы безопасности** Иногда с ними связаны дескрипторы безопасности. Группы безопасности определяются в домене при помощи консоли Active Directory — пользователи и компьютеры (Active Directory Users And Computers) на сервере под управлением Windows.
- **Группы распространения** Используются в качестве списков рассылки электронной почты. Дескрипторы безопасности с ними не связаны. В домене группы распространения создают в консоли Active Directory — пользователи и компьютеры (Active Directory Users And Computers).

Учетной записи группы, как и учетной записи пользователя, соответствует уникальный идентификатор SID. Это означает, что в случае удаления и повторного создания учетной записи группы разрешения и полномочия восстановлены не будут. У новой группы будет свой идентификатор SID, и все разрешения и полномочия старой группы будут утрачены.

Задавая уровень доступа пользователя, вы можете сделать его членом предопределенных групп:

- **Администраторы (Administrators)** Члены этой группы — локальные администраторы, имеющие полный доступ к рабочей станции. Они могут создавать учетные записи пользователей, изменять членство в группах, устанавливать принтеры, управлять общими ресурсами и т. д. Учетная запись администратора имеет полный доступ к компьютеру, поэтому соблюдайте осторожность, добавляя пользователей в эту группу.
- **Гости (Guests)** Пользователи со строго ограниченными полномочиями. Члены этой группы имеют право на удаленное обращение к системе и ее ресурсам, но не могут выполнять подавляющее большинство задач.
- **Криптографические операторы (Cryptographic Operators)** Члены группы могут управлять параметрами шифрования, IP-безопасности (IPSec), цифровыми идентификаторами и сертификатами.

- **Операторы архива (Backup Operators)** Члены этой группы имеют право проводить на рабочей станции архивацию и восстановление файлов и папок, а также имеют право входа на локальный компьютер и завершение его работы. Особенность конфигурации этой группы позволяет ее членам архивировать файлы независимо от наличия доступа на чтение и запись этих файлов. Однако операторам архива не разрешен доступ к файлам или выполнение других административных задач.

  У членов группы Backup Operators достаточно полномочий, чтобы решать узко специальную задачу — создавать резервную копию файловой системы. По умолчанию в группу операторов не входят другие учетные записи пользователей и групп. Это нужно, чтобы группе операторов можно было предоставить строго определенный набор полномочий.
- **Операторы настройки сети (Network Configuration Operators)** Члены группы имеют право управлять сетевыми параметрами рабочей станции. Кроме того, им разрешено настраивать параметры TCP/IP и выполнять общие операции по настройке сети.
- **Опытные пользователи (Power Users)** В предыдущих версиях Windows эта группа применялась для пользователей, которым разрешено изменять параметры компьютера и устанавливать программы. В Windows 7 она оставлена лишь для совместимости со старыми приложениями.
- **Пользователи (Users)** Пользователь — это человек, который большую часть работы выполняет на одной рабочей станции Windows 7. У членов группы пользователей больше ограничений, чем полномочий. Они могут локально войти на рабочую станцию Windows 7, хранить локальный профиль, блокировать рабочую станцию и завершать ее работу.
- **Пользователи журналов производительности (Performance Log Users)** Члены группы могут просматривать счетчики производительности и управлять ими, а также управлять регистрацией событий производительности.
- **Пользователи системного монитора (Performance Monitor Users)** Члены группы могут просматривать счетчики и журналы производительности.
- **Пользователи удаленного рабочего стола (Remote Desktop Users)** Члены группы могут выполнять удаленный вход в систему при помощи Служб удаленного рабочего стола (Remote Desktop Services). После входа разрешения пользователя на рабочей станции определяются другими группами, членом которых он является. Этим полномочием автоматически обладают члены группы Администраторы (Administrators). (Однако прежде администратору нужно включить удаленный доступ.)
- **Репликатор (Replicator)** Члены группы могут управлять репликацией файлов на локальном компьютере. В основном, файловая репликация применяется на серверах под управлением Windows в доменах Active Directory.

- **Читатели журнала событий (Event Log Readers)** Члены группы имеют право на просмотр журналов событий на локальном компьютере.

В большинстве случаев доступ пользователей определяется членством в группах пользователей и администраторов. Чтобы настроить пользовательский или административный уровень доступа, задайте тип учетной записи, открыв панель управления и перейдя в категорию **Учетные записи пользователей (User Accounts)**. Чтобы сделать пользователя членом группы, используйте элемент **Локальные пользователи и группы (Local Users And Groups)** в консоли **Управление компьютером (Computer Management)**.

Доменный и локальный вход в систему

Как правило, если компьютер является членом домена, для входа на компьютер и в домен используются учетные записи домена. У всех администраторов домена есть доступ к ресурсам рабочих станций, являющихся членами домена. Пользователи, в свою очередь, имеют право на доступ к ресурсам только тех локальных рабочих станций, на которые им разрешено входить. В домене любой пользователь, обладающий действующей учетной записью домена, по умолчанию может войти на любой компьютер домена. Выполнив вход, пользователь получает доступ ко всем ресурсам, доступным ему в рамках учетной записи или группы, к которой принадлежит учетная запись. При этом пользователю доступны ресурсы как локального компьютера, так и домена.

Чтобы запретить пользователю вход на определенные рабочие станции, откройте консоль **Active Directory — пользователи и компьютеры (Active Directory Users and Computers)**. Щелкните правой кнопкой учетную запись пользователя, выберите в контекстном меню команду **Свойства (Properties)**. В диалоговом окне **Свойства (Properties)** на вкладке **Учетная запись (Account)** щелкните **Вход на (Log On To)** и укажите в диалоговом окне **Рабочие станции для входа в систему (Logon Workstations)** рабочие станции, на которые разрешено входить пользователю.

Иногда на компьютер нужно войти локально. На компьютерах рабочей группы есть только локальные учетные записи. К тому же, иногда локальный вход требуется даже для администрирования компьютера, входящего в домен. Для локального входа необходима учетная запись локального пользователя. Войдя в систему локально, пользователь получает доступ ко всем ресурсам компьютера, которые открыты данной учетной записи или группе, к которой принадлежит запись.

Контроль учетных записей и повышение прав

Появление функции контроля учетными записями (user account control, UAC) сильное повлияло на конфигурирование учетных записей пользователей. Компонент UAC затрагивает полномочия обычных пользователей и администраторов, установку и выполнение приложений и многое другое. В данном разделе мы продолжим разговор, начатый в главе 1, и рассмотрим

влияние UAC на учетные записи пользователей и администраторов. Это необходимо знать при управлении Windows 7.

Примечание Понимать действие UAC обязан каждый администратор. Внедрение UAC потребовало переработки многих аспектов ОС Windows. Одно из наиболее значительных изменений связано с процессами установки и запуска приложений. Более подробное обсуждение того, как изменения в архитектуре ОС повлияли на работу программ в Windows 7, вы найдете в главе 9.

Перераспределение полномочий пользователя и администратора

В Windows XP и более ранних версиях Windows административными полномочиями обладает большинство учетных записей пользователей, что делает их отличной мишенью для злоумышленников. Благодаря этому вредоносное ПО способно не только самостоятельно устанавливаться, но и пользоваться повышенными полномочиями для уничтожения системы: программы, установленные администраторами, могут записывать информацию в защищенные области реестра и файловой системы.

Для борьбы с этой угрозой в организациях блокируют компьютеры, требуют от пользователей выполнять вход с обычной учетной записью, обязывают администраторов выполнять административные задачи посредством команды **Запуск от имени (Run As)**. К сожалению, подобные процедурные изменения плохо сказываются на производительности труда: обычному пользователю в Windows XP не разрешено выполнять даже некоторые базовые действия, например, изменять параметры даты, времени и часового пояса или параметры электропитания. Множество программ, разрабатывавшихся для Windows XP, просто не в состоянии нормально работать, не имея полномочий локального администратора — эти права необходимы им для записи информации в системные расположения в процессе установки и работы. К тому же, Windows XP не сообщает о необходимости предоставления административных полномочий для выполнения данной задачи.

Цель введения контроля учетных записей заключена в том, чтобы сделать работу более удобной, одновременно укрепив безопасность за счет перераспределения полномочий обычных и административных учетных записей. Функция UAC — существенный сдвиг в организации работы на компьютере. Она формирует среду, в которой область действия административных полномочий ограничена и всем приложениям предписывается выполнение в определенном пользовательском режиме. Таким образом, UAC исключает случайное изменение пользователями системных параметров и защищает компьютер от несанкционированной установки и запуска ПО.

Благодаря UAC, в Windows 7 определены учетные записи пользователей двух уровней: обычный и административный. Также определены два режима (уровня) выполнения для приложений: режим обычного пользователя и режим администратора. Хотя обычные пользователи могут использовать

большую часть программ и изменять системные параметры, не влияющие на других пользователей или на безопасность компьютера, полным доступом к компьютеру обладают только администраторы. Если приложение запущено администратором, к приложению применяются маркер доступа администратора и связанные с маркером административные полномочия. Это позволяет программе выполняться на локальном компьютере с правами и полномочиями администратора. Если приложение запускается обычным пользователем, к приложению применяется маркер доступа данного пользователя и связанные с ним полномочия. Тем самым права и полномочия программы на локальном компьютере ограничены правами обычного пользователя. Далее, конкретный режим выполнения приложений задается в процессе их установки. При этом в ходе установки для приложения, работающего в обычном режиме, определяются все задачи, для выполнения которых требуются административные полномочия. На их выполнения требуется разрешение пользователя.

В Windows 7 изменен набор полномочий, предоставляемых обычному пользователю. Вот задачи, которые можно выполнить с пользовательской учетной записью:

- установка шрифтов, просмотр системного времени и даты, изменение часового пояса;
- изменение параметров монитора и электропитания;
- добавление принтеров и других устройств (если необходимые драйверы установлены на компьютере или предоставлены администратором);
- загрузка и установка обновлений (если программы установки обновлений совместимы с UAC);
- создание и настройка VPN-подключений (виртуальные частные сети используются для безопасного подключения к корпоративным сетям через Интернет);
- установка протокола WEP для подключения к защищенным беспроводным сетям (протокол безопасности WEP обеспечивает дополнительную защиту беспроводных сетей).

В Windows 7 определено два уровня выполнения приложений — обычный и административный. С большинством приложений и процессов, для выполнения которых необходимы повышенные полномочия, сопоставляются маркеры безопасности. Если приложению присвоен обычный маркер или оно не рассматривается как административное, значит, для его выполнения повышенные полномочия не требуются, и по умолчанию оно выполняется в обычном режиме. Для запуска программы с маркером администратора необходимы повышенные полномочия. В этом случае перед запуском программы от пользователя требуется разрешение или подтверждение.

Процесс получения подтверждения перед запуском программы в административном режиме или перед выполнением задач, влияющих на конфигурацию системы, называется повышением прав (elevation). Оно нужно

для укрепления безопасности и защиты от вредоносного ПО, поскольку пользователь предупреждается о том, что предстоящее действие способно повлиять на параметры системы, а приложению не удается использовать административные полномочия без согласия пользователя. Повышение прав также защищает административные приложения от атак со стороны обычных приложений. Подробнее о повышении прав и о том, как UAC работает с приложениями, рассказано в главе 9.

По умолчанию перед выводом запроса на повышение прав Windows 7 переводится в режим безопасного рабочего стола (secure desktop). В этом режиме ограничивается работа программ и процессов, имеющих доступ к компьютеру, что уменьшает вероятность того, что к процессу, выполняющемуся с повышенными полномочиями, получит доступ злоумышленник или вредоносное ПО. Если вы не хотите переключаться в режим безопасного рабочего стола перед запросом на повышение прав, установите соответствующие параметры. Однако компьютер при этом станет более уязвим для программ злоумышленников и атак.

Оптимизация UAC и режим одобрения администратором

На каждом компьютере есть встроенная учетная запись локального администратора. Она не защищена компонентом UAC, и потому ее использование для администрирования потенциально опасно. Чтобы защитить компьютеры при использовании локального администрирования, создайте другую учетную запись с правами локального администратора и работайте с ней.

Для любой учетной записи компонент UAC можно включать и отключать. Отключая UAC для учетной записи пользователя, вы подвергаете компьютер риску, отказываясь от дополнительных мер безопасности. При отключении или повторном включении UAC изменения вступают в силу после перезагрузки.

Ключевой элемент UAC — режим одобрения администратором (Admin Approval Mode), определяющий поведение запроса на повышение прав во время запуска административных приложений. По умолчанию режим одобрения администратором работает следующим образом:

- все администраторы, включая встроенную учетную запись локального администратора, работают в режиме одобрения администратором;
- в этом режиме все администраторы, включая встроенную учетную запись локального администратора, видят запрос на повышение полномочий на экране при запуске административных приложений.

Выполнив вход в качестве администратора, вы можете изменить параметры UAC для всех пользователей, выполнив следующие действия:

1. Откройте панель управления и щелкните категорию **Система и безопасность (System and Security)**. В разделе **Центр поддержки (Action Center)** щелкните ссылку **Изменение параметров контроля учетных записей (Change User Account Control Settings)**.

2. В окне **Параметры управления учетными записями пользователей (User Account Control Settings)**, показанном на рис. 5-1, установите нужный уровень оповещения при помощи бегунка и щелкните **OK**. Доступные параметры приведены в табл. 5-1.

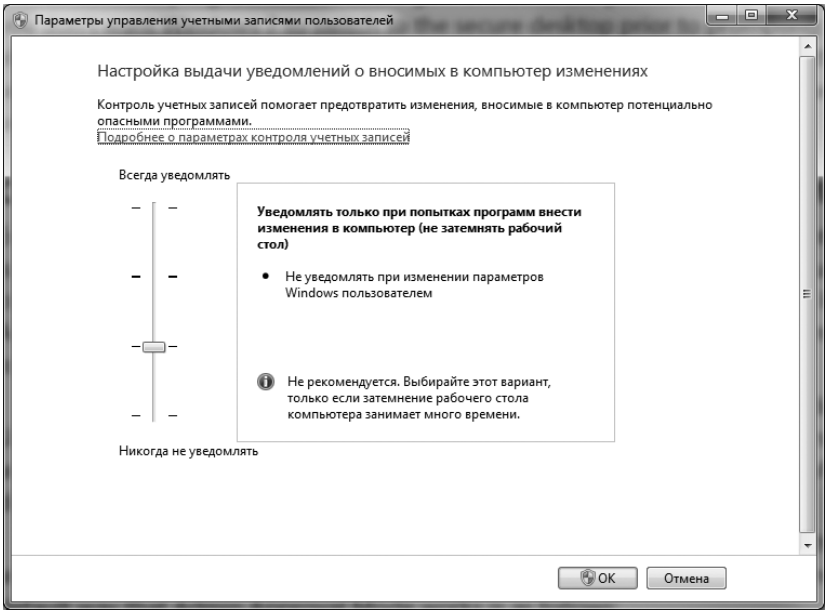

Рис. 5-1. Настройка параметров контроля учетных записей

Табл. 5-1. Параметры контроля учетных записей

Параметр	Описание	Применяется…	Безопасный рабочий стол
Всегда уведомлять (Always Notify)	Текущий пользователь всегда получает оповещения при попытках программ установить ПО или изменить систему, а также когда пользователь изменяет параметры Windows	Когда необходимо максимально защитить компьютер, если пользователи часто устанавливают ПО и посещают незнакомые веб-сайты	Да
По умолчанию (Default)	Текущий пользователь получает уведомления только о попытках программ изменить компьютер, но не об изменении параметров Windows	Когда защита компьютера необходима, но хочется сократить количество уведомлений, которые будут отображаться пользователям	Да

Табл. 5-1. (*окончание*)

Параметр	Описание	Применяется...	Безопасный рабочий стол
Уведомлять только... (не затемнять рабочий стол) (Notify Me Only When ... (Do Not Dim My Desktop))	От предыдущего варианта отличается только тем, что при выводе запроса не включается защищенный рабочий стол	Когда пользователи работают в доверенной среде и не посещают незнакомые вебсайты	Нет
Никогда не уведомлять (Never Notify)	Все оповещения UAC отключены	Когда безопасности можно уделить меньше внимания, а пользователи работают в доверенной среде с программами, не прошедшими сертификацию для Windows 7 из-за отсутствия в них поддержки UAC	Нет

Режим одобрения администратором и параметры запросов на повышение полномочий настраиваются в групповой политике, в узле **Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности (Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options)**. Доступны следующие параметры безопасности:

- **Контроль учетных записей: режим одобрения администратором для встроенной учетной записи администратора (User Account Control: Admin Approval Mode For The Built-In Administrator Account)** Определяет возможность включения режима одобрения администратором для пользователей и процессов, выполняющихся от имени встроенной учетной записи локального администратора. По умолчанию параметр включен. Это значит, что встроенная учетная запись локального администратора работает в режиме одобрения администратором, получая запросы на повышение прав, как учетная запись с административными полномочиям. Если параметр отключен, режим одобрения администратором для встроенной учетной записи локального администратора не работает; запрос на повышение прав не поступает.
- **Контроль учетных записей: разрешить UIAccess-приложениям запрашивать повышение прав, не используя безопасный рабочий стол (User Account Control: Allow UIAccess Applications To Prompt For Elevation Without Using The Secure Desktop)** Определяет, могут ли UIAccess-программы автоматически отключать безопасный рабочий стол для за-

просов на повышение прав обычного пользователя. Если параметр включен, для программ UIAccess, например Удаленного помощника Windows (Windows Remote Assistance), безопасный рабочий стол будет отключен.

- **Контроль учетных записей: поведение запроса на повышение прав для администраторов в режиме одобрения администратором (User Account Control: Behavior Of The Elevation Prompt For Administrators In Admin Approval Mode)** Определяет необходимость вывода запроса на повышение прав для администраторов при запуске административных приложений, а также поведение запроса на повышение прав. По умолчанию администраторы должны разрешать запуск приложений, требующих полномочий, в среде безопасного рабочего стола. Допустимые варианты: запрашивать согласие администратора при включенном безопасном рабочем столе; требовать ввод учетных данных при включенном или отключенном безопасном рабочем столе (так же, как и для обычных пользователей); запрашивать согласие только для сторонних двоичных файлов (не Windows). Кроме того, можно вообще отключить запрос для администраторов. При этом права администраторов будут повышаться автоматически. Любое значение этого параметра администратор может обойти, щелкнув ярлык приложения правой кнопкой и выбрав команду **Запуск от имени администратора (Run As Administrator)**.
- **Контроль учетных записей: поведение запроса на повышение прав для обычных пользователей (Behavior Of The Elevation Prompt For Standard Users)** Определяет необходимость запроса на повышение прав для обычных пользователей при выполнении ими приложений, требующих повышенных полномочий. По умолчанию, когда обычные пользователи выполняют административные задачи или запускают приложения, требующие особых полномочий, им предлагается ввести учетные данные администратора в режиме безопасного рабочего стола. Другие варианты: запрос учетных данных в среде обычного рабочего стола; автоматическое отклонение запроса на повышение прав (пользователи не смогут повышать права, даже предоставляя учетные данные администратора). Последнее значение пользователь может обойти, щелкнув ярлык приложения правой кнопкой и выбрав команду **Запуск от имени администратора (Run As Administrator)**.
- **Контроль учетных записей пользователей: все администраторы работают в режиме одобрения администратором (Run All Administrators In Admin Approval Mode)** Определяет возможность включения режима одобрения для пользователей с административными полномочиями. По умолчанию параметр включен. Это означает, что администраторы работают в режиме одобрения администратором, получая запросы на повышение прав в соответствии со своими административными полномочиям. Если параметр отключен, режим одобрения администратором для учетных записей с административными полномочиями не работает; запрос на повышение прав не выводится.

- **Контроль учетных записей: повышать права для UIAccess-приложений только при установке в безопасных местах (User Account Control: Only Elevate UIAccess Applications That Are Installed in Secure Locations)** Определяет, что необходимым условием для повышения прав UIAccess-програм является их установка в защищенном месте файловой системы. Если параметр включен, UIAccess-программы должны быть размещены в папках %SystemRoot%\Program Files, %SystemRoot%\Program Files(x86) или %SystemRoot%\Windows\System32.
- **Контроль учетных записей: повышение прав только для подписанных и проверенных исполняемых файлов (User Account Control: Only Elevate Executables That Are Signed And Validated)** Определяет необходимость подписи и проверки приложений для повышения прав. Если параметр включен, повышаются права только приложений, прошедших проверку подлинности, чьи сертификаты имеются в хранилище доверенных издателей. Рекомендуется использовать это значение для обеспечения максимальной безопасности, когда все используемые приложения имеют достоверную подпись.

В домене для применения параметров безопасности к нескольким компьютерам используется групповая политика Active Directory. Чтобы настроить эти параметры на отдельном компьютере, используйте локальную политику безопасности, выполнив следующие действия:

1. Последовательно щелкните **Пуск (Start)**, **Все программы (All Programs)**, **Администрирование (Administrative Tools)**, **Локальная политика безопасности (Local Security Policy)**.

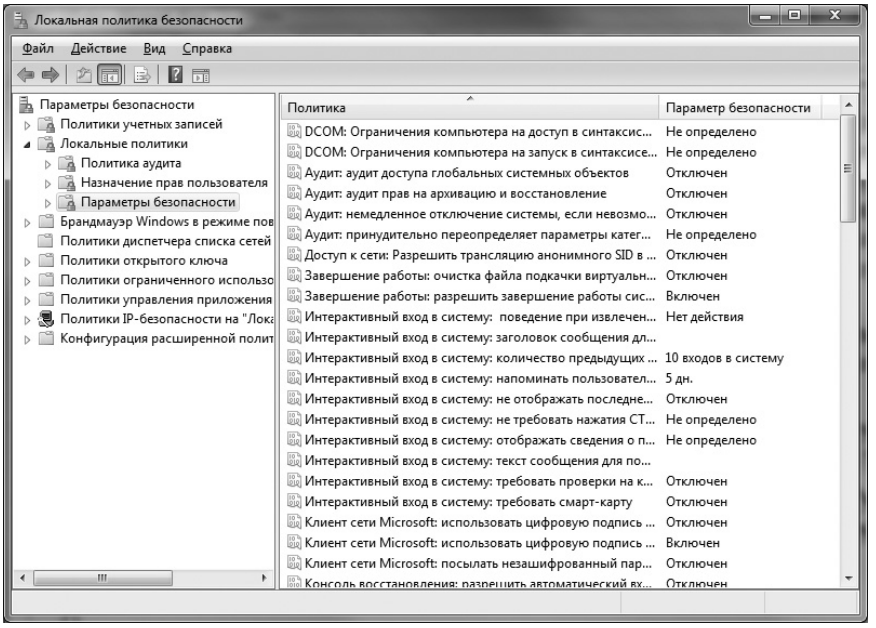

Рис. 5-2. Консоль Локальная политика безопасности (Local Security Policy)

2. В консоли **Локальная политика безопасности (Local Security Policy)** в узле **Параметры безопасности (Security Settings)** разверните **Локальные политики (Local Policies)** и щелкните узел **Параметры безопасности (Security Options)**, как показано на рис. 5-2.
3. Дважды щелкните нужный параметр, внесите необходимые изменения и щелкните **OK**. Аналогичным образом при необходимости измените другие параметры безопасности.

Управление локальным входом в систему

Все учетные записи на локальном компьютере должны иметь пароль. Если пароля нет, доступ к незащищенной учетной записи открыт для всех. С локальной учетной записи без пароля нельзя получить удаленный доступ к компьютеру.

Далее мы поговорим о том, как нужно создавать и работать с учетными записями локальных пользователей. Локальные учетные записи присутствуют на всех компьютерах, независимо от членства компьютера в домашней группе, рабочей группе или домене.

Создание учетной записи локального пользователя в домашней или рабочей группе

Чтобы создать учетную запись локального пользователя на компьютере, входящем в домашнюю или рабочую группу, выполните следующие действия:

1. Откройте панель управления. В разделе **Учетные записи пользователей (User Accounts)** щелкните **Добавление или удаление учетных записей пользователей (Add Or Remove User Accounts)**. На открывшейся странице **Управление учетными записями (Manage Accounts)** перечислены все учетные записи пользователей на локальном компьютере, упорядоченные по типу, и краткие сведения об их параметрах (рис. 5-3). Учетные записи с парольной защитой имеют метку **Защищена паролем (Password Protected)**. У отключенных учетных записей также есть соответствующая метка.
2. Щелкните команду **Создание учетной записи (Create A New Account)**. На странице **Создание новой учетной записи (Create A New Account)** введите имя учетной записи. Оно будет отображаться на приветственном экране и в меню **Пуск (Start)**.
3. Задайте тип учетной записи: **Обычный доступ (Standard User)** или **Администратор (Administrator)**. Учетная запись администратора дает пользователю все права на локальном компьютере.
4. Щелкните кнопку **Создание учетной записи (Create Account)**.

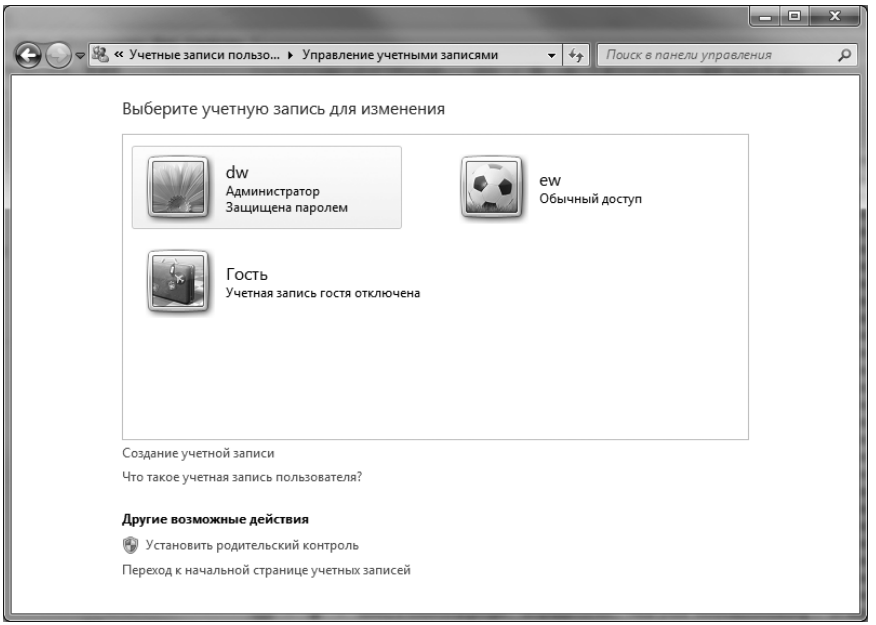

Рис. 5-3. Страница Управление учетными записями (Manage Accounts) для добавления, удаления и редактирования пользовательских учетных записей

Предоставление доменной учетной записи права на локальный вход

Когда пользователю необходима возможность локального входа на компьютер и у него при этом есть учетная запись домена, вы можете предоставить ему разрешение на локальный вход следующим образом:

1. Откройте панель управления. В разделе **Учетные записи пользователей (User Accounts)** щелкните **Изменение типа учетной записи (Change Account Type)**. В открывшемся диалоговом окне **Учетные записи пользователей (User Accounts)** перечислены все доступные учетные записи пользователей на локальном компьютере, сгруппированные по домену, а также сведения об их членстве в группах (рис. 5-4).
2. Щелкните **Добавить (Add)**, чтобы открыть мастер **Добавление нового пользователя (Add New User)**.
3. Введите в соответствующие поля имя учетной записи домена пользователя и имя домена.
4. Задайте тип учетной записи пользователя.
   - Учетная запись пользователя с обычным доступом входит в локальную группу Пользователи (Users). Чтобы предоставить пользователю разрешения обычного пользователя, установите переключатель **Обычный доступ (Standard User)**.

- Учетная запись администратора входит в локальную группу Администраторы (Administrators). Чтобы предоставить пользователю административные полномочия, установите переключатель **Администратор (Administrator)**.
- Учетная запись неопределенного типа является членом указанной вами группы. Чтобы предоставить пользователю разрешения особой группы, щелкните **Другой (Other)** и выберите группу.

5. Щелкните **Готово (Finish)**. Если требуется задать другие разрешения или добавить пользователя в другие локальные группы, выполните шаги из раздела «Управление учетными записями локальных пользователей и групп», описанные далее в этой главе.

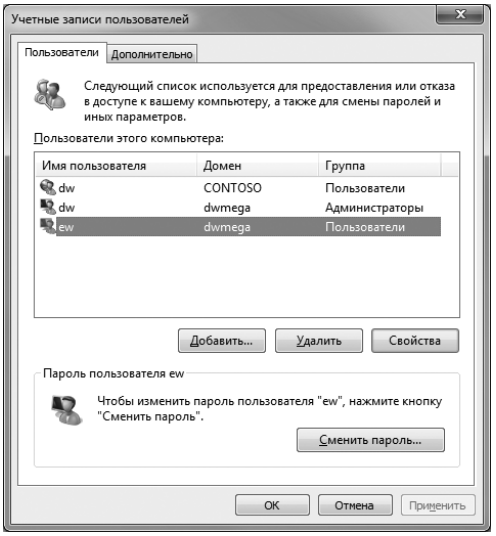

Рис. 5-4. Управление учетными записями локальных пользователей на компьютере, присоединенном к домену

Изменение типа учетной записи локального пользователя

Утилита **Учетные записи пользователей (User Accounts)** позволяет оперативно изменить тип учетной записи, задав для нее один из двух стандартных типов. Для более тонкой настройки и назначения членства учетной записи в группах применяют оснастку **Локальные пользователи и группы (Local Users And Groups)** (см. далее раздел « Добавление и удаление членов локальной группы»).

Чтобы изменить тип локальной учетной записи пользователя на компьютере, принадлежащем к домашней или рабочей группе, выполните следующие действия:

1. Откройте панель управления. В разделе **Учетные записи пользователей (User Accounts)** щелкните **Добавление или удаление учетных записей пользователей (Add Or Remove User Accounts**).

2. На открывшейся странице **Управление учетными записями (Manage Accounts)** щелкните нужную учетную запись и команду **Изменение типа учетной записи (Change The Account Type)**.
3. На странице **Изменение типа учетной записи (Change The Account Type)** установите уровень доступа для пользователя — **Обычный доступ (Standard User)** или **Администратор (Administrator)**. Щелкните кнопку **Изменение типа учетной записи (Change The Account Type)**.

Чтобы изменить тип локальной учетной записи пользователя на компьютере, принадлежащем к домену, выполните следующие действия:

1. Откройте панель управления и щелкните **Учетные записи пользователей (User Accounts)**. На странице **Учетные записи пользователей (User Accounts)** щелкните **Изменение типа учетной записи (Change Account Type)**.
2. В открывшемся диалоговом окне **Учетные записи пользователей (User Accounts)** перейдите на вкладку **Пользователи (Users)**, выберите нужную учетную запись пользователя и щелкните **Свойства (Properties)**.

   В диалоговом окне **Свойства (Properties)** откройте вкладку **Членство в группах (Group Membership)**.
3. Установите тип учетной записи: **Обычный доступ (Standard User)**, **Администратор (Administrator)** или **Другой (Other)**, выбрав нужную группу.
4. Дважды щелкните **OK**.

Создание пароля локальной учетной записи пользователя

В домашней и рабочей группе учетные записи локальных пользователей по умолчанию не имеют пароля. Это значит, что для входа пользователю достаточно щелкнуть имя учетной записи на экране приветствия или **OK** на классическом экране входа в систему. Но в целях обеспечения безопасности пароли нужно назначить всем локальным учетным записям.

Проще всего сделать это, входя в систему с каждой учетной записью, которую нужно защитить паролем, и задавая пароль при помощи утилиты Учетные записи пользователей (User Accounts). Вход от имени пользователя при создании пароля — это гарантия сохранности зашифрованных данных пользователя. Если вы создадите пароль для учетной записи пользователя, не входя в систему от его имени, пользователь утратит доступ к личным зашифрованным файлам, электронной почте, личным сертификатам и сохраненным паролям. Это произойдет потому, что основной ключ пользователя, требующийся для доступа к личному сертификату шифрования и расшифровки данных, шифруется при помощи хеша, основанного на пустом пароле. После создания пароля хеш изменится, и разблокировать данные не удастся. Единственный способ решения проблемы — восстановить первоначальные параметры, удалив пароль учетной записи, после чего пользователь получит доступ к личным зашифрованным файлам. (Сказанное справедливо только для локальных учетных записей пользователей компьютеров, но не для учетных записей пользователей домена.)

Примечание Подсказку для восстановления забытого или утраченного пароля можно задать только в утилите Учетные записи пользователей (User Accounts). Еще один способ восстановления пароля — использование диска (дискеты или флешнакопителя) сброса пароля. Если вы не хотите потерять данные, не прибегайте к другим способам восстановления пароля учетной записи локального пользователя, и вот почему. Хотя администратор волен создавать, сбрасывать или удалять пароль учетной записи пользователя, это действие приведет к удалению всех личных сертификатов и сохраненных паролей, связанных с данной учетной записью. В результате пользователь не сможет получить доступ к файлам или личным сообщениям электронной почты, зашифрованным при помощи личного ключа пользователя. Также он утратит сохраненные пароли для веб-сайтов и ресурсов сети. Важно понимать, что это относится только к учетным записям локальных пользователей. Администраторы могут изменять и сбрасывать пароли учетных записей пользователей домена, и это не повлияет на доступ к зашифрованным данным.

Чтобы создать пароль для учетной записи локального пользователя, выполните следующие действия:

1. Войдите в систему от имени пользователя, для которого создается пароль. Откройте панель управления. В разделе **Учетные записи пользователей (User Accounts)** щелкните команду **Добавление или удаление учетных записей пользователей (Add Or Remove User Accounts)**.
2. На странице **Управление учетными записями (Manage Accounts)** выберите нужную учетную запись пользователя — ту учетную запись, с которой вы вошли в систему. Помните, что у учетной записи, уже обладающей паролем, стоит метка **Защищена паролем (Password Protected)**.

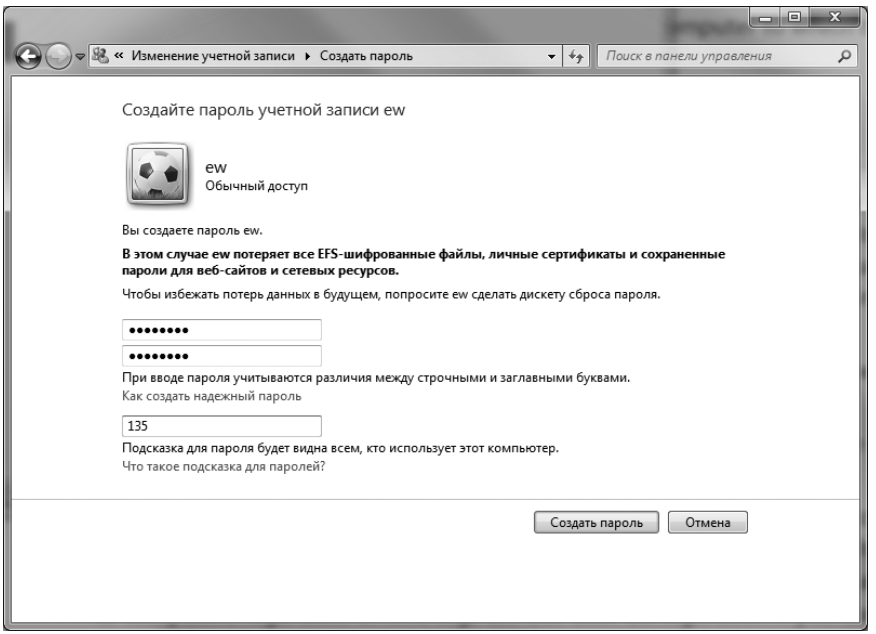

Рис. 5-5. Создание пароля и подсказки

3. Щелкните **Создать пароль (Create A Password)**. Введите пароль и подтвердите его, как показано на рис. 5-5. Далее введите уникальную подсказку — слово или фразу, которая напомнит об утерянном или забытом пароле. Она будет видна всем пользователям компьютера.
4. Щелкните кнопку **Создать пароль (Create Password)**.

Восстановление пароля учетной записи локального пользователя

Как уже отмечалось, для сохранения доступа ко всем сохраненным паролям и зашифрованным данным восстановление пароля более предпочтительно, чем изменение или удаление.

В Windows 7 существует два способа восстановления пользовательского пароля:

- **Подсказка к паролю** Отображается на экране приветствия. Обычно экран приветствия показывается на включенном компьютере, когда в системе нет пользователей. Если кто-либо из них выполнил вход на рабочую станцию, попросите этого пользователя выйти. Щелкните имя пользователя. Чтобы просмотреть подсказку, щелкните голубую кнопку входа в систему рядом со строкой ввода пароля. Вполне вероятно, что подсказка поможет пользователю вспомнить пароль. Если нет — воспользуйтесь диском сброса пароля.
- **Диск сброса пароля** Его можно создать для любой локальной учетной записи пользователя, защищенной паролем. Диск позволяет изменить пароль локальной учетной записи, не зная старого пароля. Поскольку изменить пароль учетной записи может любой обладатель диска, храните диск в надежном месте. Если пользователям разрешено создавать собственные диски сброса пароля, объясните им важность надежного хранения таких дисков.

Примечание В среде домена работа с паролями организована несколько иначе. Во-первых, паролями учетных записей пользователей домена управляют только администраторы. Во-вторых, для сброса забытых паролей используется консоль Active Directory — пользователи и компьютеры (Active Directory Users And Computers).

О том, как создать диск сброса пароля для текущего пользователя, написано в главе 1. Там же вы найдете инструкции по сбросу пароля локальной учетной записи.

Режим входа в систему: экран приветствия или классический вход

По умолчанию, если компьютер под управлением Windows 7 принадлежит к рабочей или домашней группе, после его включения отображается *экран приветствия* (Welcome screen). Если компьютер подключен к домену, отображается *экран входа в систему* (Logon screen). Важно понимать разницу между этими экранами.

Экран приветствия отображается на компьютере домашней или рабочей группы, если на компьютер не выполнен вход или при использовании соответствующей экранной заставки. На экране приветствия содержится список имеющихся на компьютере учетных записей. Чтобы войти в систему, щелкните учетную запись и при необходимости введите пароль. Вопреки распространенному мнению, на экране приветствия отображаются не все учетные записи, созданные на компьютере. Некоторые из них, например Администратор (Administrator), автоматически скрыты.

Удобство экрана приветствия состоит в том, что для входа в систему достаточно щелкнуть нужную учетную запись. Но для повышения безопасности в домашней или рабочей группе список учетных записей можно не отображать, используя вместо экрана приветствия экран входа в систему. В домене экран входа в систему отображается автоматически, если на компьютер не выполнен вход или при использовании соответствующей экранной заставки. На экране входа в систему необходимо ввести имя для входа — список имен отсутствует.

Существует несколько настраиваемых параметров экрана входа в систему. По умолчанию в диалоговом окне входа в Windows в поле **Имя пользователя (User Name)** отображается имя последнего входившего в систему пользователя. Чтобы повысить безопасность, скройте имя последнего пользователя. Тогда пользователям необходимо будет знать допустимое имя учетной записи на компьютере. Для этого в меню **Администрирование (Administrative Tools)** выберите команду **Локальная политика безопасности (Local Security Policy)** или введите **secpol.msc** в командной строке с повышенными полномочиями. В узле **Локальные политики\Параметры безопасности (Local Policies\Security Options)** дважды щелкните **Интерактивный вход в систему: не отображать последнее имя пользователя (Interactive Logon: Do Not Display Last User Name)**. Установите переключатель **Включен (Enabled)** и щелкните **OK**.

Запретить использование экрана приветствия можно при помощи параметра **Всегда классический вход в систему (Always Use Classic Logon)** групповой политики. Варианты возможных действий:

- включить политику и использовать экран входа в систему вместо экрана приветствия;
- отключить политику и использовать экран приветствия;
- оставить значение по умолчанию — **Не задано (Not Configured)**, — при этом используется экран приветствия.

В домене для применения параметров безопасности к нескольким компьютерам используется групповая политика Active Directory. Чтобы настроить данный параметр на отдельном компьютере, используйте локальную политику безопасности. Для настройки отображения экрана входа в систему вместо экрана приветствия на компьютере рабочей или домашней группы используйте оснастку Редактор объектов групповой политики (Group Policy

Object Editor). Чтобы добавить ее в пустую консоль, выполните следующие действия:

1. Щелкните **Пуск (Start)**, введите **gpedit.msc** и нажмите Enter. В открывшемся окне **Редактор локальной групповой политики (Local Group Policy)** для редактирования будет выбран объект локальной групповой политики верхнего уровня.
2. Последовательно разверните узлы: **Политика «Локальный компьютер» (Local Computer Policy)**, **Конфигурация компьютера (Computer Configuration)**, **Административные шаблоны (Administrative Templates)**, **Система (System)** и **Вход в систему (Logon)**, как показано на рис. 5-6.

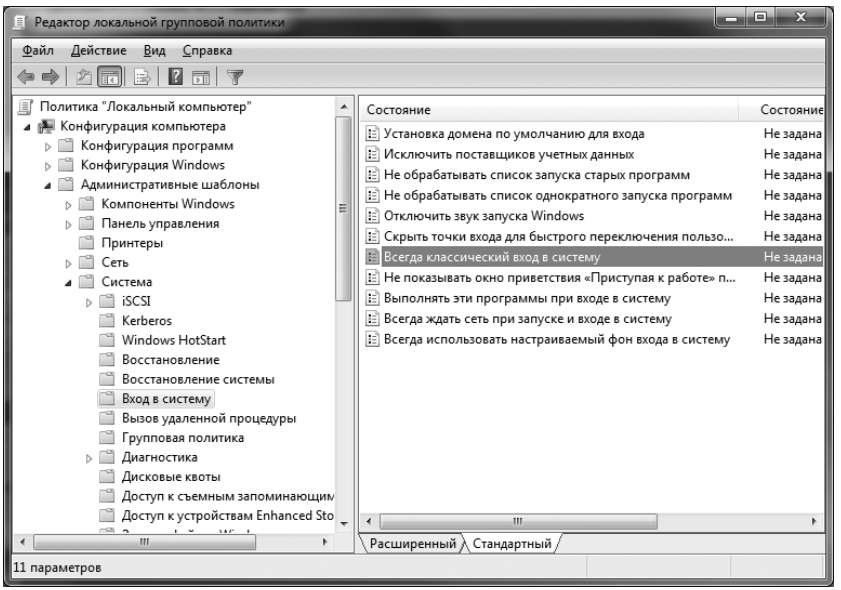

Рис. 5-6. Задайте использование экрана входа в систему вместо экрана приветствия

3. Дважды щелкните параметр **Всегда классический вход в систему (Always Use Classic Logon)**.
4. Установите переключатель **Включен (Enabled)** и щелкните **OK**.

Чтобы открыть диалоговое окно входа в систему в домене, по умолчанию требуется нажать клавиши Ctrl+Alt+Del. Вы можете отменить это требование, но при этом пострадает безопасность. Чтобы сделать это, откройте консоль **Локальная политика безопасности (Local Security Policy)**, разверните узел **Локальные политики\Параметры безопасности (Local Policies\Security Options)** и дважды щелкните **Интерактивный вход в систему: не требовать нажатия Ctrl+Alt+Del (Interactive Logon: Do Not Require Ctrl+Alt+Del)**. Установите переключатель **Включен (Enabled)** и щелкните **OK**.

Удаление учетных записей и запрет на локальный доступ к рабочим станциям

Администраторы домена автоматически получают доступ к локальным ресурсам на рабочих станциях. Прочие пользователи имеют доступ к локальным ресурсам только тех компьютеров, на которых им разрешено выполнять вход. При перемещении рабочих станций в пределах предприятия у прежних владельцев компьютеров может сохраниться доступ к их ресурсам. Кроме того, в списке доступа могут остаться пользователи, которым был предоставлен временный доступ.

В домене вы ограничиваете доступ пользователей на рабочие станции, изменяя свойства учетной записи в консоли Active Directory — пользователи и компьютеры (Active Directory Users And Computers). Дважды щелкните учетную запись, чтобы открыть диалоговое окно **Свойства (Properties)**. На вкладке **Учетная запись (Account)** щелкните кнопку **Вход на (Log On To)**.

Чтобы удалить локальную учетную запись пользователя и запретить пользователю вход на компьютер домашней или рабочей группы, выполните следующие действия:

1. Войдите в систему в качестве пользователя с полномочиями локального администратора. Откройте панель управления. В разделе **Учетные записи пользователей (User Accounts)** щелкните команду **Добавление или удаление учетных записей пользователей (Add Or Remove User Accounts)**.
2. На странице **Управление учетными записями (Manage Accounts)** щелкните учетную запись, которую нужно удалить.
3. Щелкните команду **Удаление учетной записи (Delete The Account)**.
4. Перед удалением учетной записи вы можете сохранить содержимое рабочего стола пользователя и папок с документами в папку на рабочем столе текущего пользователя. Чтобы сохранить рабочий стол и документы пользователя, щелкните **Сохранение файлов (Keep Files)**. Для удаления файлов щелкните **Удалить файлы (Delete Files)**.
5. Подтвердите удаление, щелкнув **Удаление учетной записи (Delete Account)**.

Помните, что при отсутствии в домене дополнительных ограничений на вход пользователь сможет получить доступ к рабочей станции, войдя в систему с учетной записью домена.

Сохраненные учетные данные

В Windows 7 учетные данные, используемые для автоматизированного доступа пользователей к серверам, веб-сайтам и программам, при помощи диспетчера учетных данных могут сохраняться в электронном хранилище, что обеспечивает быстрый доступ к необходимым ресурсам независимо от их расположения. Если у пользователя часто возникают сбои при подклю-

чении к защищенным ресурсам, например к интрасети компании или вебсайту, создайте и сохраните учетные данные для каждого ресурса, к которому обращается пользователь.

Программа Диспетчер учетных данных (Credential Manager) поддерживает сохранение учетных данных трех видов:

- **Учетные данные Windows (Windows credential)** Учетные данные, в которых используется стандартная проверка подлинности Windows (NTLM или Kerberos). В них включаются расположение ресурса, имя для входа учетной записи и пароль.
- **Учетные данные на основе сертификата (Certificate-based credential)** Учетные данные, включающие расположение ресурса. В них для проверки подлинности используется сертификат, хранящийся в личном хранилище диспетчера учетных данных.
- **Общие учетные данные (Generic credential)** Используются для базовой или нестандартной проверки подлинности. Включают расположение ресурса, имя для входа учетной записи и пароль.

В следующих разделах рассказано о способах работы с сохраненными учетными данными.

Добавление учетных данных Windows и общих учетных данных

Уникальное *хранилище Windows* (Windows vault) есть у каждой учетной записи. Записи хранилища находятся в параметрах профиля пользователя и содержат информацию, требуемую для доступа к защищенным ресурсам. Если вы создадите запись хранилища Windows, войдя на компьютер с учетной записью домена, обладающей перемещаемым профилем пользователя (не локальным или обязательным), то сохраненная вами информация будет доступна при входе на любой компьютер в домене. В противном случае информация хранилища Windows доступна только на том компьютере, на котором она была создана.

Ближе к реальности Сохраненные учетные данные очень удобны на предприятиях, где вместо доменов применяются рабочие или домашние группы. Допустим, компьютер Теда входит в рабочую группу. Теду приходится ежедневно запрашивать данные с нескольких различных серверов, находящихся в разных расположениях или доменах. В этом случае создание учетных данных Windows для каждого ресурса сэкономит уйму времени. Кроме того, независимо от применяемого Тедом способа доступа к серверам, учетные данные Windows позволяют проходить проверку подлинности автоматически, без предоставления альтернативных учетных данных. В частности, если вы настроите учетные данные для доступа к серверу FileServer84, то при подключении сетевого диска, находящегося на этом сервере, Теду не придется использовать другие учетные данные.

Чтобы добавить запись в хранилище Windows текущего пользователя, выполните следующие действия:

1. Войдите в систему от имени пользователя, хранилище Windows которого нужно обновить. Откройте панель управления, щелкните категорию

Учетные записи пользователей (User Accounts) и выберите команду **Диспетчер учетных данных (Credential Manager)**. На странице диспетчера учетных данных (рис. 5-7) показан текущий список записей (если они есть), которые упорядочены по типу.

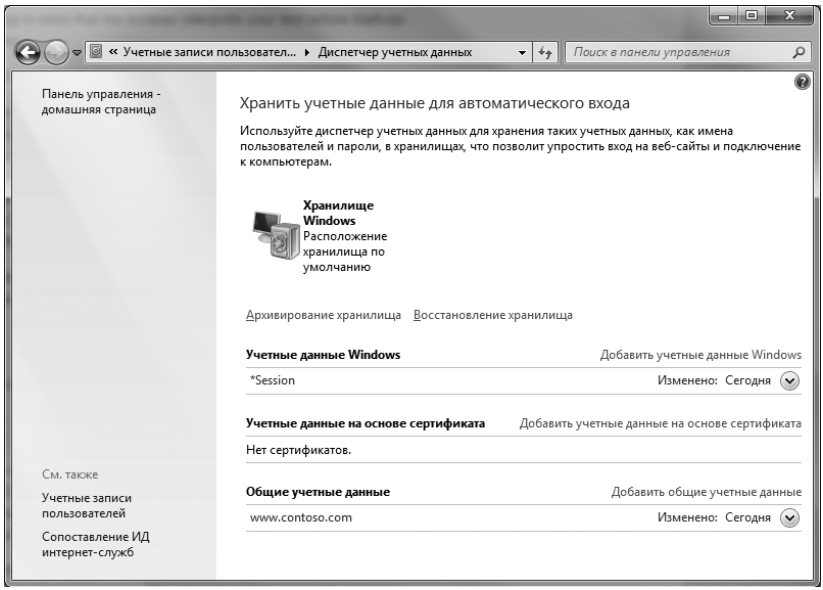

Рис. 5-7. Список доступных учетных данных и возможные действия

2. Щелкните **Добавить учетные данные Windows (Add A Windows Credential)** или **Добавить общие учетные данные (Add A Generic Credential)**. Настройте параметры учетных данных (рис. 5-8), заполнив следующие поля:
   - **Адрес в Интернете или сети (Internet Or Network Address)** Адрес сетевого ресурса или ресурса в Интернете, для которого выполняется настройка записи хранилища. В качестве адреса можно использовать имя сервера, например *fileserver86*; полное доменное имя Интернет-ресурса, например *www.microsoft.com*; адрес, содержащий знак подстановки, например **.microsoft.com*. Если вы укажете имя сервера или полное доменное имя, с такой записью можно получить доступ к конкретному серверу или службе. Знак подстановки позволяет обращаться к любому серверу указанного домена. К примеру, запись **.microsoft.com* можно использовать для доступа к серверам *www.microsoft.com, ftp.microsoft.com, smtp.microsoft.com* и *extranet.microsoft.com*.
   - **Имя пользователя (User Name)** Имя пользователя, необходимое для передачи на сервер, включая необходимые квалификаторы домена. Если ресурс находится в домене по умолчанию, введите только имя пользователя, например, *Elena*. Для домена, отличного от домена по умолчанию, введите полное доменное имя и имя учетной записи:

technology\Elena. При подключении к службе Интернета введите полное имя учетной записи службы, например *Elena@msn.com*.

- **Пароль (Password)** Пароль для доступа к серверу. Добрая половина пользователей после смены своего пароля на сервере часто забывает сделать это в хранилище Windows. Если пользователь забыл сменить пароль в хранилище Windows, неоднократные попытки подключиться к серверу или службе могут привести к блокированию учетной записи.

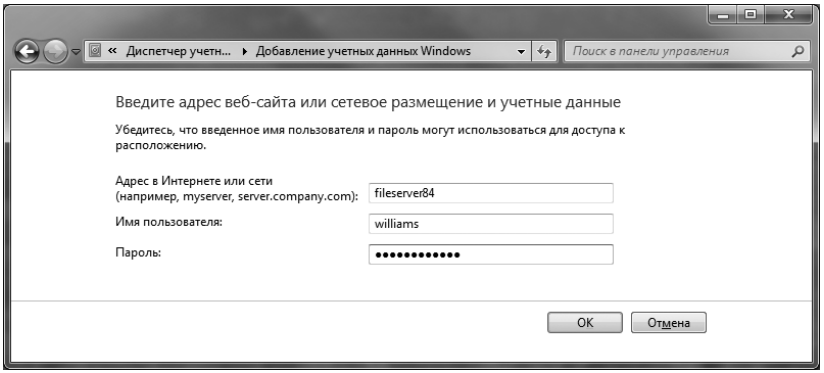

Рис. 5-8. Создание записи хранилища Windows на основе регистрационных данных

3. Щелкните **OK**, чтобы сохранить учетные данные.

Добавление учетных данных на основе сертификатов

В личном хранилище сертификатов, которое находится в профиле пользователя, хранятся сертификаты для прохождения пользователем проверки подлинности. Добавив сертификат пользователя, создайте учетные данные для доступа к ресурсу при помощи этого сертификата.

Чтобы добавить запись учетных данных на основе сертификата в хранилище Windows текущего пользователя, выполните следующие действия:

1. Войдите в систему от имени пользователя, хранилище Windows которого нужно обновить. Откройте панель управления, щелкните **Учетные записи пользователей (User Accounts)** и **Диспетчер учетных данных (Credential Manager)**.
2. Щелкните **Добавить учетные данные на основе сертификата (Add A Certificate-Based Credential)**. В поле **Адрес в Интернете или сети (Internet Or Network Address)** введите имя сетевого ресурса или ресурса в Интернете, для которого выполняется настройка записи хранилища Windows. В качестве адреса можно использовать имя сервера, полное доменное имя Интернет-ресурса или адрес, содержащий символ подстановки.
3. Щелкните кнопку **Выбор сертификата (Select Certificate)**. В одноименном диалоговом окне **Выбор сертификата (Select Certificate)** найдите личный сертификат, предназначенный для доступа к ресурсу, и щелкните **OK**.
4. Еще раз щелкните **OK**, чтобы сохранить сертификат.

Редактирование записей хранилища Windows

Редактируя записи хранилища Windows, следует помнить, что записи локального хранилища видны только на том компьютере, на котором они были созданы. Это означает, что для изменения записи необходимо войти на ту локальную рабочую станцию, на которой запись создавалась. Единственным исключением являются пользователи с перемещаемым профилем. Записи хранилища Windows для таких пользователей можно редактировать на любом компьютере, на который пользователь выполнит вход.

Чтобы отредактировать запись хранилища Windows пользователя, выполните следующие действия:

1. Войдите в систему от имени пользователя, хранилище Windows которого нужно обновить. Откройте панель управления, щелкните **Учетные записи пользователей (User Accounts)** и **Диспетчер учетных данных (Credential Manager)**.
2. Щелкните запись учетных данных, которую хотите редактировать.
3. Щелкните кнопку **Правка (Edit)**.
4. Введите новые значения имени пользователя, пароля или сертификата, связанного с учетными данными.
5. Щелкните **Сохранить (Save)**.

Архивация и восстановление хранилища Windows

Архивация хранилища Windows подразумевает резервное копирование сохраненных учетных данных пользователя. Чтобы восстановить учетные данные или перенести их на другой компьютер, достаточно восстановить хранилище Windows. В большинстве случаев хранилище Windows следует архивировать на съемный носитель.

Для архивации хранилища Windows выполните следующие действия:

1. Войдите в систему от имени пользователя, хранилище Windows которого нужно архивировать. Откройте панель управления, щелкните **Учетные записи пользователей (User Accounts)** и **Диспетчер учетных данных (Credential Manager)**.
2. Щелкните команду **Архивирование хранилища (Back Up Vault)**.
3. На странице **Сохранение имен пользователей и паролей (Stored User Names And Passwords)** щелкните кнопку **Обзор (Browse)**. В диалоговом окне **Сохранить архивный файл как (Save Backup File As)** выберите расположение и введите имя архивного файла. Архивные файлы учетных данных имеют расширение .crd. Щелкните **Сохранить (Save)**.
4. Щелкните **Далее (Next)**. Нажмите клавиши Ctrl+Alt+Del, чтобы продолжить работу в режиме безопасного рабочего стола. Введите и подтвердите пароль архивного файла учетных данных.
5. Щелкните **Далее (Next)**, затем щелкните **Готово (Finish)**.

Чтобы восстановить хранилище Windows на исходном или другом компьютере, выполните следующие действия:

1. Войдите в систему от имени пользователя, хранилище Windows которого нужно восстановить. Откройте панель управления, щелкните **Учетные записи пользователей (User Accounts)** и **Диспетчер учетных данных (Credential Manager)**.
2. На странице диспетчера учетных данных щелкните **Восстановление хранилища (Restore Vault)**.
3. На странице **Сохранение имен пользователей и паролей (Stored User Names And Passwords)** щелкните **Обзор (Browse)**. В диалоговом окне **Открыть архивный файл (Open Backup File As)** найдите файл архива учетных данных и щелкните **Открыть (Open)**.
4. Щелкните **Далее (Next)**. Нажмите клавиши Ctrl+Alt+Del, чтобы продолжить работу в режиме безопасного рабочего стола. Введите пароль для архивного файла учетных данных.
5. Щелкните **Далее (Next)**, затем щелкните **Готово (Finish)**.

Удаление записей хранилища Windows

Записи, которые больше не нужны пользователю, следует удалять. Чтобы сделать это, выполните следующие действия:

1. Войдите в систему от имени пользователя, запись которого нужно удалить. Откройте панель управления, щелкните **Учетные записи пользователей (User Accounts)** и **Диспетчер учетных данных (Credential Manager)**.
2. Выберите запись учетных данных, которую нужно удалить.
3. Щелкните **Удаление из хранилища (Remove From Vault)**. Подтвердите действие, щелкнув **Да (Yes)**.

Как уже отмечалось, записи локального хранилища Windows можно удалить только на том компьютере, на котором они были созданы. Но записи хранилища пользователя с перемещаемым профилем можно редактировать на любом компьютере, на который пользователь выполнил вход.

Управление учетными записями локальных пользователей и групп

Учетные записи локальных пользователей и группы по способам управления во многом похожи на учетные записи домена. Вы можете создавать учетные записи, настраивать их свойства, сбрасывать учетные записи при блокировке или отключении и т. д. Учетные записи локальных пользователей создаются в панели управления, в предпочтениях политики или в утилите Локальные пользователи и группы (Local Users And Groups). При этом помните следующее:

- утилита Локальные пользователи и группы (Local Users And Groups) применяется для управления учетными записями локальных пользователей на одном компьютере;

- предпочтения политики применяются для управления учетными записями локальных пользователей на нескольких компьютерах в домене.

При работе с предпочтениями политики управление пользователями и группами выполняется в узлах **Конфигурация компьютера (Computer Configuration)** и **Конфигурация пользователя (User Configuration)**. Узел **Конфигурация компьютера (Computer Configuration)** используется, когда нужно применить предпочтения к компьютерам независимо от вошедшего в систему пользователя. Узел **Конфигурация пользователя (User Configuration)** используется, чтобы применять предпочтения к пользователям независимо от компьютера, на который они выполнили вход.

Создание учетной записи локального пользователя

Чтобы создать учетную запись пользователя в утилите Локальные пользователи и группы (Local Users And Groups), выполните следующие действия:

1. Последовательно щелкните **Пуск (Start)**, **Все программы (All Programs)**, **Администрирование (Administrative Tools)** и **Управление компьютером (Computer Management)**. Можно также открыть панель управления, щелкнуть категорию **Система и безопасность (System And Security)**, затем в нижней части списка выбрать команду **Администрирование (Administrative Tools)** и дважды щелкнуть **Управление компьютером (Computer Management)**.
2. В дереве консоли щелкните правой кнопкой узел **Управление компьютером (Computer Management)**. В контекстном меню выберите команду **Подключиться к другому компьютеру (Connect To Another Computer)**. В открывшемся окне выберите рабочую станцию под управлением Windows 7. (На контроллерах домена локальные пользователи и группы отсутствуют.)
3. В узле **Служебные программы (System Tools)** дважды щелкните **Локальные пользователи и группы (Local Users And Groups)** и выберите узел **Пользователи (Users)**. В области сведений находятся определенные на данный момент учетные записи пользователей.
4. Щелкните правой кнопкой узел **Пользователи (Users)** и выберите команду **Новый пользователь (New User)**. Откроется диалоговое окно **Новый пользователь (New User)**, показанное на рис. 5-9. Заполните следующие поля:
   - **Пользователь (User Name)** Имя для входа учетной записи пользователя. Оно должно соответствовать локальной политике имен пользователей.
   - **Полное имя (Full Name)** Полное имя пользователя.
   - **Описание (Description)** Сведения о пользователе. Обычно здесь указывают должность, например веб-мастер. Можете указать также отдел.

- **Пароль (Password)** Пароль учетной записи пользователя. Должен соответствовать требованиям политики паролей.
- **Подтверждение (Confirm Password)** Это поле предназначено для проверки правильности ввода пароля. Введите пароль еще раз.
- **Требовать смены пароля при следующем входе в систему (User Must Change Password At Next Logon)** Если установлен этот флажок, пользователь должен сменить пароль при входе в систему.
- **Запретить смену пароля пользователем (User Cannot Change Password)** Если установлен этот флажок, пользователь не может изменять пароль.
- **Срок действия пароля не ограничен (Password Never Expires)** Если установлен этот флажок, пароль для данной учетной записи будет действовать всегда. Данный параметр перекрывает локальную политику учетных записей.
- **Отключить учетную запись (Account Is Disabled)** Если установлен этот флажок, учетная запись отключена и не может быть использована. При помощи этого параметра можно временно запретить пользователям использовать эту учетную запись.

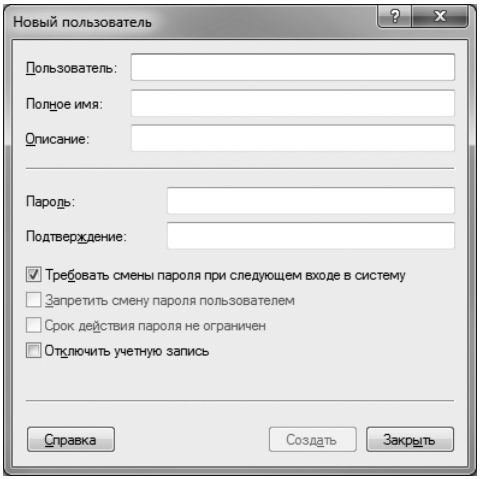

Рис. 5-9. Диалоговое окно Новый пользователь (New User)

5. Настроив новую учетную запись, щелкните **Создать (Create)**.

Чтобы создать учетную запись пользователя в групповой политике при помощи элемента предпочтения, выполните следующие действия:

1. В оснастке **Редактор управления групповыми политиками (Group Policy Management Editor)** откройте объект GPO для редактирования. Чтобы настроить предпочтения для компьютера, последовательно разверните узлы **Конфигурация компьютера\Настройка\Параметры панели управления (Computer Configuration\Preferences\Control Panel Settings)** и выберите **Локальные пользователи и группы (Local Users**

And Groups). Чтобы настроить предпочтения для пользователей, последовательно разверните узлы **Конфигурация пользователя\Настройка\Параметры панели управления (User Configuration\Preferences\Control Panel Settings)** и выберите **Локальные пользователи и группы (Local Users And Groups)**.

2. Щелкните правой кнопкой узел **Локальные пользователи и группы (Local Users And Groups)**, раскройте подменю **Создать (New)** и выберите **Локальный пользователь (Local User)**. Откроется диалоговое окно, показанное на рис. 5-10.
3. В списке **Действие (Action)** выберите команду **Создать (Create)**. Остальные параметры настройте по аналогии с предыдущей процедурой.
4. На вкладке **Общие параметры (Common)** укажите способ применения предпочтения. Обычно новая учетная запись создается только один раз, поэтому установите флажок **Применить один раз и не применять повторно (Apply Once And Do Not Reapply)**.
5. Щелкните **OK**. Во время следующего обновления политики элемент предпочтения будет применен к объекту GPO, в котором вы его определили.

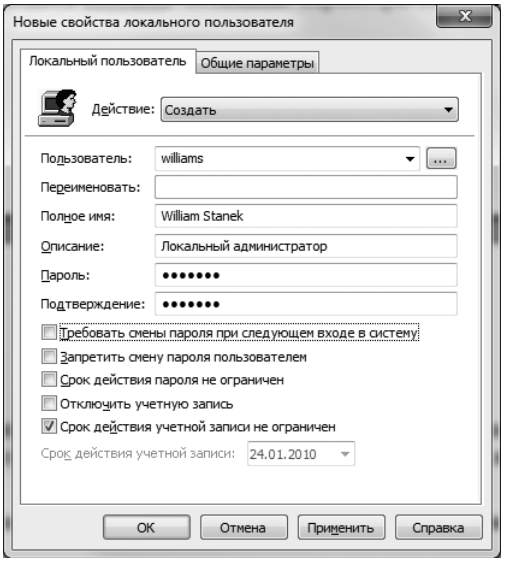

Рис. 5-10. Настройка новой учетной записи локального пользователя в групповой политике

Создание локальных групп на рабочей станции

Локальные группы создаются при помощи утилиты Локальные пользователи и группы (Local Users And Groups) или в групповой политике. Чтобы создать учетную запись пользователя в утилите Локальные пользователи и группы (Local Users And Groups), выполните следующие действия:

1. Последовательно щелкните **Пуск (Start)**, **Все программы (All Programs)**, **Администрирование (Administrative Tools)** и **Управление компьютером (Computer Management)**. Также можно открыть панель управления, щелкнуть категорию **Система и безопасность (System And Security)**, выбрать команду **Администрирование (Administrative Tools)**, а затем дважды щелкнуть **Управление компьютером (Computer Management)**.
2. В дереве консоли щелкните правой кнопкой узел **Управление компьютером (Computer Management)** и выберите команду **Подключиться к другому компьютеру (Connect To Another Computer)**. В открывшемся окне выберите рабочую станцию под управлением Windows 7. (На контроллерах домена локальные пользователи и группы отсутствуют.)
3. В узле **Служебные программы (System Tools)** дважды щелкните **Локальные пользователи и группы (Local Users And Groups)** и выберите узел **Группы (Groups)**. В области сведений показаны определенные в данный момент учетные записи групп.
4. Щелкните правой кнопкой узел **Группы (Groups)** и выберите команду **Создать группу (New Group)**. На рис. 5-11 показано диалоговое окно **Новая группа (New Group)**.

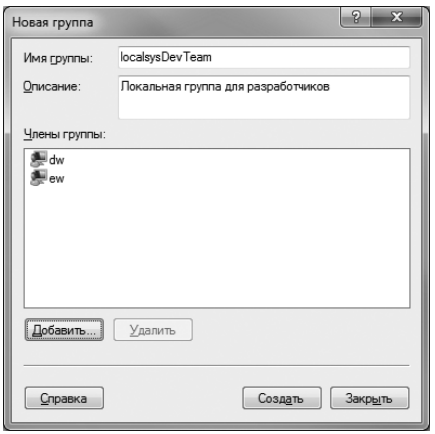

Рис. 5-11. Добавление локальной группы в диалоговом окне Новая группа (New Group)

5. Введите имя и описание новой группы и щелкните **Добавить (Add)**.
6. В открывшемся диалоговом окне **Выбор: «Пользователи» (Select Users)** щелкните **Размещение (Locations)** и выберите компьютер или домен, в котором расположены учетные записи пользователей.
7. В поле **Введите имена выбираемых объектов (Enter The Object Names To Select)** введите имя пользователя и щелкните **Проверить имена (Check Names)**. При наличии совпадений выберите нужную учетную запись и щелкните **OK**. Если совпадения не найдены, попробуйте ввести имя заново и повторите поиск. При необходимости повторите данный шаг. Затем щелкните **OK**.

8. Выбранные пользователи помещены в окно **Новая группа (New Group)**. Если вы указали пользователя ошибочно, выделите его имя и щелкните **Удалить (Remove)**.
9. Указав всех членов группы, щелкните **Создать (Create)**.

Чтобы создать локальную группу в групповой политике при помощи элемента предпочтений, выполните следующие действия:

1. В оснастке **Редактор управления групповыми политиками (Group Policy Management Editor)** откройте объект GPO для редактирования. Чтобы настроить предпочтения для компьютера, последовательно разверните узлы **Конфигурация компьютера\Настройка\Параметры панели управления (Computer Configuration\Preferences\Control Panel Settings)** и выберите **Локальные пользователи и группы (Local Users And Groups)**. Чтобы настроить предпочтения для пользователей, последовательно разверните узлы **Конфигурация пользователя\Настройка\Параметры панели управления (User Configuration\Preferences\Control Panel Settings)** и выберите **Локальные пользователи и группы (Local Users And Groups)**.
2. Щелкните правой кнопкой узел **Локальные пользователи и группы (Local Users And Groups)**, раскройте подменю **Создать (New)** и выберите команду **Локальная группа (Local Group)**. На рис. 5-12 показано диалоговое окно **Новые свойства локальной группы (New Local Group Properties)**.

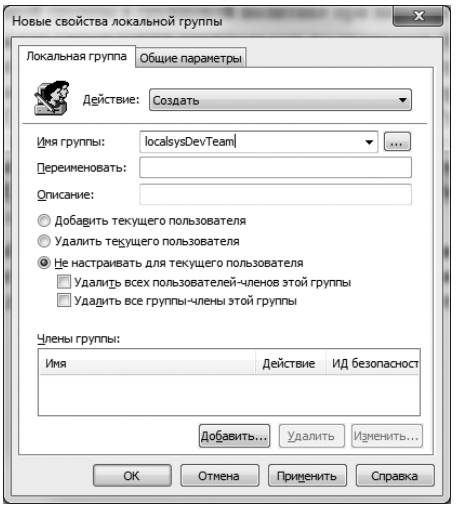

Рис. 5-12. Настройка новой учетной записи локальной группы в групповой политике

3. Выберите в списке действий команду **Создать (Create)**. Введите имя и описание группы.
4. Укажите, следует ли добавлять в новую группу текущего пользователя, или установите параметр **Не настраивать для текущего пользователя (Do Not Configure For The Current User)**.

5. Чтобы добавить членов в группу, щелкните **Добавить (Add)**. В диалоговом окне **Член локальной группы (Local Group Member)** щелкните кнопку с тремя точками. В диалоговом окне **Выбор: «Пользователь», «Компьютер» или «Группа» (Select User, Computer Or Group)** выберите пользователя или группу, которую нужно добавить, затем дважды щелкните **OK**. Повторите шаг по мере надобности.
6. Укажите способ применения предпочтения на вкладке **Общие параметры (Common)**. Обычно новая учетная запись создается только один раз. Установите флажок **Применить один раз и не применять повторно (Apply Once And Do Not Reapply)**.
7. Щелкните **OK**. Во время следующего обновления политики элемент предпочтения будет применен к объекту GPO, в котором вы его определили.

Добавление и удаление членов локальной группы

Для добавления и удаления членов локальных групп используется оснастка **Локальные пользователи и группы (Local Users And Groups)**. Выполните следующие действия:

1. Откройте консоль **Управление компьютером (Computer Management)** и разверните узел **Локальные пользователи и группы (Local Users And Groups)**. На левой панели выделите папку **Группы (Groups)**. Дважды щелкните нужную группу.
2. Чтобы добавить в группу учетные записи пользователей, щелкните **Добавить (Add)**. В открывшемся диалоговом окне **Выбор: «Пользователи» (Select Users)** в поле **Введите имена выбираемых объектов (Enter The Object Names To Select)** введите имя пользователя и щелкните **Проверить имена (Check Names)**. При наличии совпадений выберите нужную учетную запись и щелкните **OK**. Если совпадения не найдены, попробуйте ввести имя заново и повторите поиск. При необходимости повторите этот шаг, а затем щелкните **OK**.
3. Чтобы удалить учетную запись пользователя из группы, выделите ее и щелкните **Удалить (Remove)**.
4. Завершив работу, щелкните **OK**.

Чтобы добавить или удалить членов локальной группы в групповой политике при помощи элемента предпочтений, выполните следующие действия:

1. В оснастке **Редактор управления групповыми политиками (Group Policy Management Editor)** откройте объект GPO для редактирования. Чтобы настроить предпочтения для компьютера, последовательно разверните узлы **Конфигурация компьютера\Настройка\Параметры панели управления (Computer Configuration\Preferences\Control Panel Settings)** и выберите **Локальные пользователи и группы (Local Users And Groups)**. Чтобы настроить предпочтения для пользователей, последовательно разверните узлы **Конфигурация пользователя\Настрой-**

ка\Параметры панели управления (User Configuration\Preferences\Control Panel Settings) и выберите **Локальные пользователи и группы (Local Users And Groups)**.

2. Щелкните правой кнопкой узел **Локальные пользователи и группы (Local Users And Groups)**, раскройте подменю **Создать (New)** и выберите команду **Локальная группа (Local Group)**.
3. В открывшемся диалоговом окне **Новые свойства локальной группы (New Local Group Properties)** выберите в списке **Действие (Action)** вариант **Обновить (Update)**, чтобы обновить параметры настройки группы. Если вы укажете команду **Заменить (Replace)**, произойдет удаление и повторное создание группы с указанными вами параметрами. Во время обновления группу можно переименовать, введя имя в поле **Переименовать (Rename To)**.
4. Укажите, следует ли добавлять в новую группу текущего пользователя, или установите флажок **Не настраивать для текущего пользователя (Do Not Configure For The Current User)**.
5. Укажите, следует ли удалять всех существующих пользователей и (или) группы.
6. Чтобы добавить или удалить членов групп, щелкните **Добавить (Add)**. В диалоговом окне **Член локальной группы (Local Group Member)** выберите в списке **Действие (Action)** вариант **Добавить в эту группу (Add To This Group)** или **Удалить из этой группы (Remove From This Group)**. Затем щелкните кнопку с тремя точками и выберите в диалоговом окне **Выбор: «Пользователь», «Компьютер» или «Группа» (Select User, Computer Or Group)** пользователя или группу, которую нужно добавить в локальную группу. Затем дважды щелкните **OK**. Повторите шаг при необходимости.
7. Укажите способ применения предпочтения на вкладке **Общие параметры (Common)**. Во время следующего обновления политики элемент предпочтения будет применен к объекту GPO, в котором вы его определили.

Включение и отключение учетных записей локальных пользователей

Существует несколько причин, по которым учетная запись может быть отключена. Если пользователь забыл пароль и пытается вспомнить его путем подбора вариантов, он может превысить допустимое политикой количество неудачных входов в систему. Отключить учетную запись может другой администратор, если пользователь находится в отпуске. Ниже приведены методы включения учетной записи после того, как она была отключена или заблокирована.

Чтобы включить ранее отключенную учетную запись на локальном компьютере, выполните следующие действия:

1. Откройте консоль **Управление компьютером (Computer Management)** и разверните узел **Локальные пользователи и группы (Local Users And Groups)**. На левой панели выделите папку **Пользователи (Users)**.
2. На правой панели дважды щелкните имя учетной записи пользователя и сбросьте флажок **Отключить учетную запись (Account Is Disabled)**.
3. Щелкните **OK**.

Чтобы включить заблокированную учетную запись на локальном компьютере, выполните следующие действия:

1. В узле **Локальные пользователи и группы (Local Users And Groups)** выделите папку **Пользователи (Users)**.
2. На правой панели дважды щелкните имя учетной записи пользователя и сбросьте флажок **Заблокировать учетную запись (Account Is Locked Out)**.
3. Щелкните **OK**.

Чтобы включить, отключить учетную запись или настроить ее параметры при помощи предпочтения политики, выполните следующие действия:

1. В оснастке **Редактор управления групповыми политиками (Group Policy Management Editor)** откройте объект GPO для редактирования. Чтобы настроить предпочтения для компьютера, последовательно разверните узлы **Конфигурация компьютера\Настройка\Параметры панели управления (Computer Configuration\Preferences\Control Panel Settings)** и выберите **Локальные пользователи и группы (Local Users And Groups)**. Чтобы настроить предпочтения для пользователей, последовательно разверните узлы **Конфигурация пользователя\Настройка\Параметры панели управления (User Configuration\Preferences\Control Panel Settings)** и выберите **Локальные пользователи и группы (Local Users And Groups)**.
2. Дважды щелкните имя учетной записи пользователя на правой панели, чтобы открыть диалоговое окно свойств.
3. В списке действий выберите вариант **Обновить (Update)**. Внесите необходимые изменения и щелкните **OK**. Во время следующего обновления политики элемент предпочтения будет применен к объекту GPO, в котором вы его определили.

Обеспечение безопасности учетной записи гостя

В некоторых средах для посетителей необходима учетная запись Гость (Guest). В большинстве случаев гостевую учетную запись настраивают на отдельном компьютере (компьютерах), внимательно следя за ее использованием. Ниже приводятся рекомендации по созданию безопасной учетной записи гостя:

- **Включите учетную запись Гость (Guest)** По умолчанию учетная запись гостя отключена. Чтобы ею воспользоваться, ее необходимо включить. Откройте консоль **Управление компьютером (Computer Management)**, разверните узел **Локальные пользователи и группы (Local Users And**

Groups) и выделите папку **Пользователи (Users)**. Дважды щелкните элемент **Гость (Guest)**, сбросьте флажок **Отключить учетную запись (Account Is Disabled)** и щелкните **OK**.

- **Задайте для учетной записи гостя безопасный пароль** По умолчанию у гостевой учетной записи пустой пароль. Чтобы повысить безопасность компьютера, установите для нее более защищенный пароль. В узле **Локальные пользователи и группы (Local Users And Groups)** щелкните правой кнопкой элемент **Гость (Guest)** и выберите команду **Задать пароль (Set Password)**. В окне предупреждения щелкните **Продолжить (Proceed)**. Введите новый пароль и подтвердите его. Дважды щелкните **OK**.
- **Запретите использование учетной записи гостя в сети** Закройте доступ к гостевой учетной записи через сеть. В противном случае ее смогут использовать для входа пользователи с других компьютеров. Откройте меню **Администрирование (Administrative Tools)** и запустите утилиту **Локальная политика безопасности (Local Security Policy)** или введите **secpol.msc** в командной строке с повышенными полномочиями. В узле **Локальные политики\Назначение прав пользователя (Local Policies\User Rights Assignment)** убедитесь, что учетная запись Гость (Guest) значится в политике **Отказать в доступе к этому компьютеру из сети (Deny Access To This Computer From The Network)**.
- **Запретите учетной записи гостя завершать работу компьютера** Во время выключения или включения компьютера существует вероятность несанкционированного доступа к нему пользователя с правами гостя (как и всех, у кого есть локальный доступ). Чтобы этого не произошло, убедитесь, что учетная запись гостя не обладает правом Завершение работы системы (Shut Down The System). Откройте утилиту **Локальная политика безопасности (Local Security Policy)** и разверните узел **Локальные политики\Назначение прав пользователя (Local Policies\User Rights Assignment)**. Убедитесь, что в списке политики **Завершение работы системы (Shut Down The System)** нет учетной записи гостя.
- **Запретите учетной записи гостя просматривать журналы регистрации событий** Чтобы поддерживать безопасность системы, не следует разрешать просмотр журналов событий с учетной записью гостя. Запустите редактор реестра, введя в командной строке **regedit**. Откройте раздел **HKLM\SYSTEM\CurrentControlSet\services\Eventlog**. Среди прочих, здесь есть три важных подраздела — **Application**, **Security** и **System**. Проследите за тем, чтобы во всех трех подразделах параметр RestrictGuestAccess типа DWORD имеел значение 1.

Переименование учетных записей локальных пользователей и групп

В процессе переименования учетной записи ей присваивается новая метка. Идентификатор SID не меняется, следовательно, разрешения и свойства

учетной записи остаются прежними. Чтобы переименовать учетную запись, войдите на локальный компьютер и выполните следующие действия:

1. В узле **Локальные пользователи и группы (Local Users And Groups)** выделите папку **Пользователи (Users)** или **Группы (Groups)**.
2. Щелкните правой кнопкой имя учетной записи и выберите команду **Переименовать (Rename)**. Введите новое имя и щелкните другую запись.

Чтобы переименовать учетную запись в групповой политике, выполните следующие действия:

1. В оснастке **Редактор управления групповыми политиками (Group Policy Management Editor)** откройте объект GPO для редактирования. Чтобы настроить предпочтения для компьютера, последовательно разверните узлы **Конфигурация компьютера\Настройка\Параметры панели управления (Computer Configuration\Preferences\Control Panel Settings)** и выберите **Локальные пользователи и группы (Local Users And Groups)**. Чтобы настроить предпочтения для пользователей, последовательно разверните узлы **Конфигурация пользователя\Настройка\Параметры панели управления (User Configuration\Preferences\Control Panel Settings)** и выберите **Локальные пользователи и группы (Local Users And Groups)**.
2. Выполните одно из следующих действий:
   - Если элемент предпочтения для пользователя или группы уже существует, дважды щелкните имя пользователя или группы, чтобы открыть соответствующее окно свойств. В списке действий выберите команду **Обновить (Update)**. В поле **Переименовать (Rename To)** введите новое имя учетной записи и щелкните **OK**.
   - Если элемента предпочтения для пользователя или группы не существует, создайте его, как было описано ранее. Для переименования пользователя или группы выберите в списке действий вариант **Обновить (Update)** и введите новое имя учетной записи в поле **Переименовать (Rename To)**.

Удаление учетных записей локальных пользователей и групп

Учетные записи удаляются безвозвратно. Выполнив удаление и создав другую учетную запись с таким же именем, вы не получите автоматически прежних разрешений, т. к. новой учетной записи будет присвоен идентификатор SID, отличный от прежнего идентификатора.

Удаление встроенных учетных записей может иметь далеко идущие последствия для рабочей станции, поэтому в Windows 7 их удалить нельзя. Другие типы учетных записей удалить можно. Для этого в узле **Локальные пользователи и группы (Local Users And Groups)** выделите учетную запись и нажмите на клавишу Delete или щелкните учетную запись правой кнопкой и выберите команду **Удалить (Delete)**. Затем подтвердите действие.

Примечание При удалении учетной записи пользователя в узле **Локальные пользователи и группы (Local Users And Groups)** профиль пользователя, личные файлы и домашняя папка не удаляются. Их придется удалить вручную.

Чтобы удалить учетную запись в групповой политике, выполните следующие действия:

1. В оснастке **Редактор управления групповыми политиками (Group Policy Management Editor)** откройте объект GPO для редактирования. Чтобы настроить предпочтения для компьютера, последовательно разверните узлы **Конфигурация компьютера\Настройка\Параметры панели управления (Computer Configuration\Preferences\Control Panel Settings)** и выберите **Локальные пользователи и группы (Local Users And Groups)**. Чтобы настроить предпочтения для пользователей, последовательно разверните узлы **Конфигурация пользователя\Настройка\Параметры панели управления (User Configuration\Preferences\Control Panel Settings)** и выберите **Локальные пользователи и группы (Local Users And Groups)**.
2. Выполните одно из следующих действий:
   - Если элемент предпочтения для пользователя или группы уже существует, дважды щелкните имя пользователя или группы, чтобы открыть соответствующее окно свойств. В списке действий выберите команду **Удалть (Delete)**. На вкладке **Общие параметры (Common)** установите необходимые параметры, например **Применить один раз и не применять повторно (Apply Once And Do Not Reapply)**. Щелкните **OK**.
   - Если элемент предпочтения для пользователя или группы не существует, создайте его, как было описано ранее. В списке действий щелкните **Удалить (Delete)**, после чего задайте необходимые параметры на вкладке **Общие параметры (Common)**.

Управление удаленным доступом к рабочим станциям

В Windows 7 имеется несколько возможностей удаленного доступа. В программе Удаленный помощник (Remote Assistance) вы можете отправлять приглашения специалистам из службы техподдержки, позволяя им управлять компьютером на расстоянии. Удаленный рабочий стол (Remote Desktop) — это инструмент для удаленного подключения к компьютеру и доступа к его ресурсам. Этот раздел посвящен настройке удаленного помощника и удаленного рабочего стола. Обычно оба этих компонента отключены, и включить их нужно вручную.

Удаленный помощник и удаленный рабочий стол способны работать через брандмауэры NAT. В удаленном помощнике есть встроенные средства диагностики. Для облегчения диагностики расширения масштаба поддержки к удаленному компьютеру могут одновременно подключиться два специалиста поддержки. Если для поиска и устранения неисправностей требуется перезагрузка, после перезагрузки сеанс удаленного помощника автоматически восстанавливается.

До начала сеанса удаленного помощника от пользователя может потребоваться пошаговая запись событий, приведших к возникновению неисправности. Сделать это позволяет несложный инструмент Средство записи действий по воспроизведению неполадок (Problem Steps Recorder). Чтобы включить этот инструмент и работать с ним, выполните следующие действия:

1. Щелкните кнопку **Пуск (Start)**, введите **psr** в строке поиска и нажмите Enter. После запуска инструмента необходимо подготовить рабочую среду и приступить к записи неисправности.
2. Чтобы включить запись, щелкните **Начать запись (Start Record)**. Выполните действия, приведшие к возникновению ошибки, сопровождая их необходимыми комментариями.
3. После возникновения неполадки остановите запись кнопкой **Остановить запись (Stop Record)**.
4. На экране появится диалоговое окно **Сохранить как (Save As)**. Выберите место сохранения и имя для Zip-файла, содержащего запись неисправности в формате .mht.
5. Направьте Zip-файл специалисту при помощи электронной почты или сохраните его на общем сетевом ресурсе. Для просмотра записанной неисправности дважды щелкните Zip-файл. В Проводнике Windows дважды щелкните файл с расширением .mht, который откроется в Internet Explorer.
6. Просмотрите экранные снимки всех шагов, предпринятых во время записи неисправности. Под экранными снимками находятся дополнительные сведения о каждом шаге, сгенерированные автоматически. Эта информация, наряду с комментариями пользователя, поможет вам найти и устранить неисправность.

Настройка удаленного помощника

Удаленный помощник (Remote Assistance) — компонент весьма полезный как для корпоративной, так и для внешней службы поддержки. Пользователь передает управление своим компьютером специалистам, получая возможность освоить тонкости процесса или просто понаблюдать за ходом настройки системы. Ключевым моментом здесь является предоставляемый вами уровень доступа.

Если удаленный помощник включен, по умолчанию это дает возможность специалистам просматривать и управлять компьютером. Пользователи могут отправлять приглашения во внутренние и внешние ресурсы, что может быть небезопасно для предприятия. Во избежание неприятностей службе техподдержки можно позволить просматривать компьютеры, но не управлять ими. Нововведение Windows 7 заключается в появившейся возможности разрешать подключения только от компьютеров под управлением Windows 7 или более новых версий. Это позволит снять проблемы совместимости и обеспечит применение во время сеанса компонентов безопасности Windows 7 и последующих ОС.

Еще одним ключевым аспектом настройки является ограничение срока действия приглашений. По умолчанию максимальное ограничение по времени составляет 6 часов. Наибольший срок действия приглашения составляет 30 дней. С одной стороны, приглашения на столь долгий срок гарантируют, что у технического специалиста будет достаточно времени, чтобы разобраться с проблемой. С другой стороны, это означает, что приглашением можно воспользоваться в течение 30 дней для *любого* доступа к компьютеру. Представьте себе, что вы отправили приглашение с 30-дневным сроком действия человеку, который справился с неполадкой за один день. Тогда у него останется еще 29 дней на доступ к компьютеру, что нежелательно по соображениям безопасности. Чтобы уменьшить риск, значительно сократите максимальный интервал времени действия приглашения, скажем, до 1 часа. Если проблема не устранена за отведенное время, вы можете сгенерировать новое приглашение.

Чтобы настроить удаленный помощник, выполните следующие действия:

1. Откройте панель управления, щелкните **Система и безопасность (System And Security)** и **Система (System)**.
2. В левой части страницы **Система (System)** щелкните **Настройка удаленного доступа (Remote Settings)**. На экране появится диалоговое окно **Свойства системы (System Properties)**, открытое на вкладке **Удаленный доступ (Remote)**, как показано на рис. 5-13.
3. Чтобы отключить удаленный помощник, сбросьте флажок **Разрешить подключения удаленного помощника к этому компьютеру (Allow Remote Assistance Connections To This Computer)** и щелкните **OK**. Пропустите следующие шаги.
4. Чтобы включить удаленный помощник, установите флажок **Разрешить подключения удаленного помощника к этому компьютеру (Allow Remote Assistance Connections To This Computer)**.

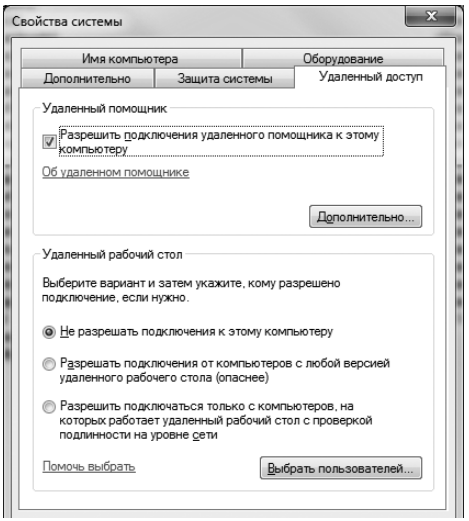

Рис. 5-13. Настройка параметров удаленного доступа к компьютеру

5. Щелкните **Дополнительно (Advanced)**, чтобы открыть диалоговое окно **Параметры удаленного помощника (Remote Assistance Settings)**, показанное на рис. 5-14.

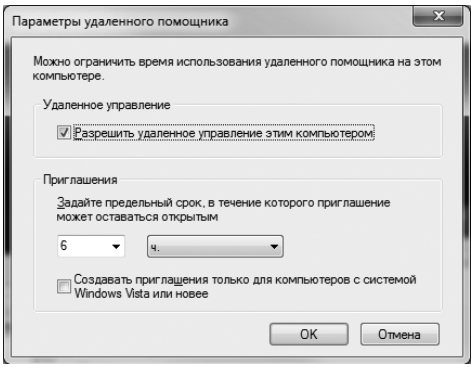

Рис. 5-14. Установка срока действия приглашения для удаленного помощника

6. Полномочия специалистов определяются флажком **Разрешить удаленное управление этим компьютером (Allow This Computer To Be Controlled Remotely)**. Если флажок включен, помощникам разрешено просматривать компьютер и управлять им. Чтобы оставить доступ только на просмотр, сбросьте этот флажок.
7. Наибольший срок действия приглашений задается в разделе **Приглашения (Invitations)**. Можно задать значения в минутах, часах или днях, с максимальной продолжительностью до 30 дней. Если предельный срок равен 10 дням, пользователь сможет создать приглашение, срок действия которого не превышает 10 дней. Максимальный срок действия по умолчанию составляет 6 часов.
8. Завершив настройку параметров удаленного помощника, дважды щелкните **OK**.

Для настройки удаленного помощника в групповой политике используются параметры политики, перечисленные в табл. 5-2. Они находятся в узле **Конфигурация компьютера\Административные шаблоны (Computer Configuration\Administrative Templates)** по указанному в таблице пути.

Табл. 5-2. Параметры политики, управляющие удаленным помощником

Параметр	Путь
Разрешать подключения только с компьютеров под управлением Windows Vista или более новых систем (Allow Only Vista Or Later Connections)	\Система\Удаленный помощник (\System\Remote Assistance)
Запретить запуск Windows Messenger (Do Not Allow Windows Messenger To Be Run)	\Компоненты Windows\Windows Messenger (\Windows Components\Windows Messenger)

Табл. 5-2. (*окончание*)

Параметр	Путь
Предлагать удаленную помощь (Offer Remote Assistance)	\Система\Удаленный помощник (\System\Remote Assistance)
Запрос удаленной помощи (Solicited Remote Assistance)	\Система\Удаленный помощник (\System\Remote Assistance)
Включить ведение журнала сеанса (Turn On Session Logging)	\Система\Удаленный помощник (\System\Remote Assistance)

Настройка доступа для удаленного рабочего стола

В отличие от удаленного помощника, позволяющего просматривать только рабочий стол текущего пользователя, Удаленный рабочий стол (Remote Desktop) предоставляет несколько уровней доступа:

- Если пользователь, выполнивший локальный вход, входит в систему удаленно, локальный рабочий стол блокируется, а пользователь начинает работать со всеми открытыми приложениями так, как будто бы он сидит непосредственно за компьютером. Преимущество заключается в том, что пользователи, работающие дома или в других местах за пределами офиса, могут продолжать работу с приложениями и документами, с которыми они работали в офисе.
- Если пользователь, внесенный в список доступа удаленного рабочего стола, не выполнил локальный вход на компьютер, он может начать новый сеанс работы с Windows. При этом поведение сеанса будет таким, как будто пользователь сидит за компьютером, даже если на компьютер выполнили вход другие пользователи. Таким образом, ресурсами одной рабочей станции могут пользоваться сразу несколько пользователей.

По умолчанию удаленный рабочий стол отключен. Чтобы разрешить удаленный доступ к рабочей станции, его необходимо включить отдельно. Если удаленный рабочий стол включен, подключиться к рабочей станции может любой член группы Администраторы (Administrators). Чтобы доступ к рабочей станции могли получить другие пользователи, их необходимо поместить в список пользователей удаленного рабочего стола. Чтобы настроить удаленный рабочий стол, выполните следующие действия:

1. Откройте панель управления, щелкните **Система и безопасность (System And Security)** и **Система (System)**.
2. В левой части страницы **Система (System)** щелкните **Настройка удаленного доступа (Remote Settings)**. Диалоговое окно **Свойства системы (System Properties)** откроется на вкладке **Удаленный доступ (Remote)**.
3. Чтобы отключить удаленный рабочий стол, установите переключатель **Не разрешать подключения к этому компьютеру (Don't Allow Connections To This Computer)** и щелкните **OK**. Пропустите следующие шаги.
4. Выберите вариант включения удаленного рабочего стола:

- Подключению от компьютеров под управлением любой версии Windows соответствует переключатель **Разрешать подключения от компьютеров с любой версией удаленного рабочего стола (Allow Connections From Computers Running Any Version Of Remote Desktop)**.
- Подключению от компьютеров под управлением Windows 7 и последующих версий, а также компьютеров с безопасной сетевой проверкой подлинности, соответствует переключатель **Разрешать подключения только от компьютеров с удаленным рабочим столом с сетевой проверкой подлинности (Allow Connections Only From Computers Running Remote Desktop With Network Level Authentication)**.

5. Щелкните **Выбрать пользователей (Select Users)**. Откроется диалоговое окно **Пользователи удаленного рабочего стола (Remote Desktop Users)**, показанное на рис. 5-15.

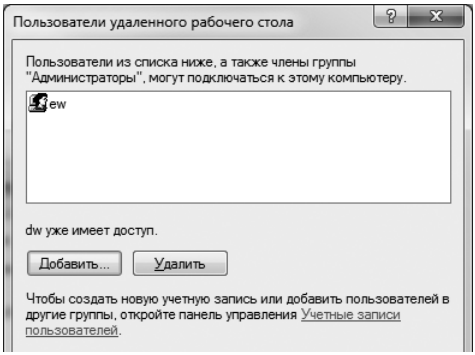

Рис. 5-15. Укажите пользователей, которым разрешено устанавливать подключение удаленного рабочего стола

6. Чтобы предоставить пользователю доступ к удаленному рабочему столу, щелкните **Добавить (Add)**. В открывшемся диалоговом окне **Выбор: «Пользователи» (Select Users)** щелкните **Размещение (Locations)** и выберите компьютер или домен, в котором расположены учетные записи пользователей. В поле **Введите имена выбираемых объектов (Enter The Object Names To Select)** введите имя пользователя и щелкните **Проверить имена (Check Names)**. При наличии совпадений выберите нужную учетную запись и щелкните **OK**. Если совпадения не найдены, попробуйте ввести имя заново и повторите поиск. При необходимости повторите этот шаг. Затем щелкните **OK**.
7. Чтобы отозвать разрешение на доступ учетной записи пользователя, выделите учетную запись и щелкните **Удалить (Remove)**.
8. Завершив работу, два раза щелкните **OK**.

В брандмауэре Windows необходимо настроить исключения, разрешающие входящие подключения удаленного рабочего стола. Сделать это можно по отдельности на каждом компьютере для профиля домена и стандартного профиля. Для настройки исключения и управления удаленным рабо-

чим столом в групповой политике используются параметры, приведенные в табл. 5-3. Они находятся в узле **Конфигурация компьютера\Административные шаблоны (Computer Configuration\Administrative Templates)** по указанному в таблице пути.

Табл. 5-3. Параметры политики, управляющие удаленным рабочим столом

Параметр	Путь
	В узле Компоненты Windows\Службы удаленных рабочих столов (WINDOWS COMPONENTS\REMOTE DESKTOP SERVICES)
Разрешать RDP-файлы от неизвестных издателей (Allow .Rdp Files From Unknown Publishers)	\Клиент подключения к удаленному рабочему столу (\Remote Desktop Connection Client)
Разрешать RDP-файлы от допустимых издателей и пользовательские параметры RDP, заданные по умолчанию (Allow .Rdp Files From Valid Publishers And User's Default .Rdp Settings)	\Клиент подключения к удаленному рабочему столу (\Remote Desktop Connection Client)
Всегда запрашивать пароль при подключении (Always Prompt For Password Upon Connection)	\Узел сеансов удаленных рабочих столов\Безопасность (\Remote Desktop Session Host\Security)
Автоматическое переподключение (Automatic Reconnection)	\Узел сеансов удаленных рабочих столов \Подключения (\Remote Desktop Session Host\Connections)
Настройка проверки подлинности клиента на сервере (Configure Server Authentication For Client)	\Клиент подключения к удаленному рабочему столу (\Remote Desktop Connection Client)
Запретить завершение консольного сеанса администратора (Deny Logoff Of An Administrator Logged In To The Console Session)	\Узел сеансов удаленных рабочих столов\Подключения (\Remote Desktop Session Host\Connections)
Не разрешать локальным администраторам настраивать разрешения (Do Not Allow Local Administrators To Customize Permissions)	\Узел сеансов удаленных рабочих столов \Безопасность (\Remote Desktop Session Host\Security)
Запретить сохранение паролей (Do Not Allow Passwords To Be Saved)	\Клиент подключения к удаленному рабочему столу (\Remote Desktop Connection Client)
Наибольшая глубина цвета (Limit Maximum Color Depth)	\Узел сеансов удаленных рабочих столов\Среда удаленных сеансов (\Remote Desktop Session Host\Remote Session Environment)

Табл. 5-3. (*окончание*)

Параметр	Путь
Ограничить максимальное разрешение экрана (Limit Maximum Display Resolution)	\Узел сеансов удаленных рабочих столов\Среда удаленных сеансов (\Remote Desktop Session Host\Remote Session Environment)
Ограничить максимальное количество мониторов (Limit Maximum Number Of Monitors)	\Узел сеансов удаленных рабочих столов\Среда удаленных сеансов (\Remote Desktop Session Host\Remote Session Environment)
Ограничить размер кэша всех перемещаемых профилей пользователей (Limit The Size Of The Entire Roaming User Profile Cache)	\Узел сеансов удаленных рабочих столов\Profiles (\Remote Desktop Session Host\Профили)
Требовать использование специального уровня безопасности для удаленных подключений по методу RDP (Require Use Of Specific Security Layer For Remote (Rdp) Connections)	\Узел сеансов удаленных рабочих столов\Безопасность (\Remote Desktop Session Host\Security)
Установить уровень шифрования для клиентских подключений (Set Client Connection Encryption Level)	\Узел сеансов удаленных рабочих столов\Безопасность (\Remote Desktop Session Host\Security)
Задание алгоритма сжатия для данных RDP (Set Compression Algorithm For Rdp Data)	\Узел сеансов удаленных рабочих столов\Среда удаленных сеансов (\Remote Desktop Session Host\Remote Session Environment)
Указать отпечатки SHA1 сертификатов, представляющих доверенных издателей RDP (Specify Sha1 Thumbprints Of Certificates Representing Trusted .Rdp Publishers)	\Клиент подключения к удаленному рабочему столу (\Remote Desktop Connection Client)
	Прочие пути
Запретить удаленное управление рабочим столом (Disable Remote Desktop Sharing)	\Компоненты Windows\NetMeeting (\Windows Components\NetMeeting)
Брандмауэр Windows: Разрешить исключения для входящих сообщений удаленного управления рабочим столом (Windows Firewall: Allow Inbound Remote Desktop Exceptions)	\Сеть\Сетевые подключения\Брандмауэр Windows\Профиль домена (\Network\Network Connections\Windows Firewall\Domain Profile)
Брандмауэр Windows: Разрешить исключения для входящих сообщений удаленного управления рабочим столом (Windows Firewall: Allow Inbound Remote Desktop Exceptions)	\Сеть\Сетевые подключения\Брандмауэр Windows\Стандартный профиль (\Network\Network Connections\Windows Firewall\Standard Profile)

Подключение к удаленному рабочему столу

Вы, как администратор, можете устанавливать подключения к удаленному рабочему столу серверов и рабочих станций под управлением Windows. В Windows 2000 Server для подключения к удаленному рабочему столу необходимо установить Службы терминалов (Terminal Services), которые затем настраиваются в режиме удаленного доступа. В Windows XP Professional и последующих версиях удаленный рабочий стол устанавливается автоматически, но его требуется включить, как описано в предыдущем разделе. После включения удаленного рабочего стола разрешения на удаленный доступ к компьютеру получают все администраторы. Другим пользователям можно тоже предоставить доступ.

Чтобы подключиться к удаленному рабочему столу сервера или рабочей станции, выполните следующие действия:

1. Введите **mstsc** в командной строке или последовательно щелкните **Пуск (Start)**, **Все программы (All Programs)**, **Стандартные (Accessories)** и **Подключение к удаленному рабочему столу (Remote Desktop Connection)**. Щелкните **Параметры (Options)**. Откроется диалоговое окно **Подключение к удаленному рабочему столу (Remote Desktop Connection)**, показанное на рис. 5-16.

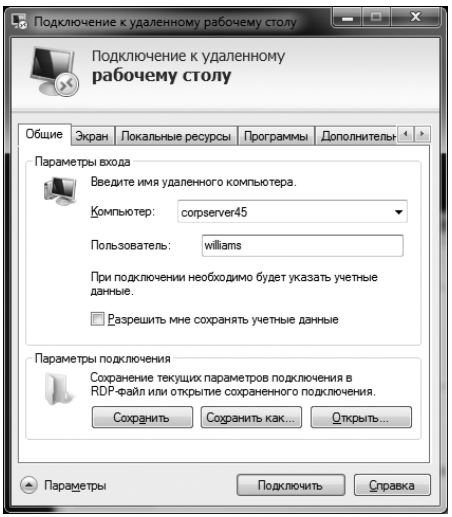

Рис. 5-16. Введите имя компьютера, к которому нужно подключиться, и щелкните Подключить (Connect)

2. В поле **Компьютер (Computer)** введите имя компьютера, к которому выполняется подключение. Если вы не знаете имя, выберите его из раскрывающегося списка или щелкните **Поиск других (Browse For More)**, чтобы просмотреть список доменов и компьютеров в доменах.
3. При необходимости задайте дополнительные параметры. Если для данного компьютера настроены сохраненные учетные данные, они будут ис-

пользованы автоматически. При необходимости вы вольны редактировать или удалить учетные данные.

4. Щелкните **Подключить (Connect)**. Если учетные данные компьютера, к которому выполняется подключение, не были сохранены ранее, введите их и щелкните **OK**. В случае успешного подключения на удаленном компьютере откроется окно **Подключение к удаленному рабочему столу (Remote Desktop)**, а вы сможете работать с ресурсами этого компьютера. Если подключиться не удалось, проверьте правильность введенной информации и попытайтесь подключиться снова.

Примечание Чтобы задать дополнительные параметры создания и сохранения подключений, в диалоговом окне **Подключение к удаленному рабочему столу (Remote Desktop Connection)** щелкните кнопку **Параметры (Options)**. Это позволит изменить размер экрана удаленного рабочего стола, управлять подключениями к локальным ресурсам (принтерам, последовательным портам, дисковым накопителям и т. д.), при подключении автоматически запускать программы, включать или отключать локальное кеширование и сжатие данных.

Глава 6

Конфигурирование компьютера

Едва ли не главной задачей администратора является управление параметрами конфигурации ОС. С этой точки зрения Windows 7 сильно отличается от Windows XP и предшествующих версий Windows. Суть различий — в архитектурных изменениях, впервые представленных в Windows Vista и продолженных в Windows 7. Среди этих изменений:

- **Модульная структура и распространение двоичных файлов на дисках с записанными на них WIM-образами** Это позволяет управлять пакетами, драйверами, компонентами, а также параметрами локализации в WIM-файлах и на виртуальных жестких дисках (.vhd) при помощи утилиты DISM (Deployment Image Servicing and Management). Также работать с vhd-файлами можно при помощи обновленных утилит Управление дисками (Disk Management) и DiskPart.
- **Предзагрузочная среда, в которой управление запуском и загрузкой выбранного вами приложения загрузки осуществляется Диспетчером загрузки Windows (Windows Boot Manager)** При загрузке ОС Windows 7, в отличие от предыдущих версий Windows, файлы Ntldr и Boot.ini не используются. Изменились и параметры загрузки. В частности, вы можете загрузить на компьютер ОС, находящуюся в vhd-файле. Один из способов сделать это – создать базовый образ загрузки. Во время запуска vhd-файл копируется на указанный диск при помощи утилиты Xcopy.
- **Функция Контроль учетных записей пользователей (UAC) для управления запуском приложений и определения прав приложений при их взаимодействии с ОС** Обработка полномочий и прав доступа в Windows 7 реализована иначе, чем в прежних версиях Windows. В главе 5 говорилось, что вы вольны отключить вывод запросов UAC, но это не приводит к отключению других функциональных возможностей UAC, например виртуализации приложений.

Помимо этих усовершенствований вам необходимо также знать о том, как настраивать Windows 7 при помощи обновленных инструментов. Об этом и пойдет речь в данной главе.

Поддержка компьютеров под управлением Windows 7

Для успешного управления компьютером, диагностики и исправления сбоев необходимо знание конфигурации компьютера. Ниже перечислены инструменты для сбора сведений о компьютере:

- **Управление компьютером (Computer Management)** Консоль, обеспечивающая доступ к важным средствам для управления системой, службам и устройствами хранения данных.
- **Производительность (Performance)** Наблюдение за производительностью системы и поиск факторов, отрицательно сказывающихся на производительности.
- **Монитор ресурсов (Resource Monitor)** Позволяет просматривать подробные сведения об использовании системных ресурсов, включая процессоры, память, диски и сети. Монитор ресурсов используется, когда не хватает информации, предоставляемой диспетчером задач.
- **Система (System)** Позволяет просматривать основные сведения о компьютере и управлять свойствами системы.
- **Сведения о системе (System Information)** Отображение подробной статистики о конфигурации и доступности ресурсов. Эта утилита полезна и при поиске неисправностей.
- **Диспетчер задач (Task Manager)** Позволяет просматривать сведения об использовании системных ресурсов.

В этом разделе мы поговорим о работе с перечисленными выше инструментами.

Консоль Управление компьютером (Computer Management)

Консоль Управление компьютером (Computer Management) предназначена для выполнения базовых задач по администрированию локальной или удаленной системы. Если вы добавили меню **Администрирование (Administrative Tools)** в меню **Пуск (Start)**, для запуска консоли последовательно щелкните **Пуск (Start)**, **Администрирование (Administrative Tools)** и **Управление компьютером (Computer Management)**. Есть и другой способ открыть эту консоль:

1. При помощи меню **Пуск (Start)** откройте панель управления. В списке **Просмотр по (View By)** выберите вариант **Категория (Category)**.
2. Щелкните категорию **Система и безопасность (System And Security)**.
3. Выберите вариант **Администрирование (Administrative Tools)** и дважды щелкните команду **Управление компьютером (Computer Management)**.

Панели главного окна консоли похожи на панели проводника Windows (рис. 6-1). Для навигации и и выбора средств применяется дерево консоли, расположенное в левой панели. Панель **Действия (Actions)**, расположенная справа, представляет собой аналог контекстного меню, вызываемого правым щелчком объекта. Чтобы показать или скрыть панель действий, щелкните

кнопку **Отображение или скрытие панели действий (Show/Hide Action Pane)** на панели инструментов. Инструменты делятся на три категории:

- **Служебные программы (System Tools)** Управление системой и просмотр системных сведений.
- **Запоминающие устройства (Storage)** Программы для управления дисками.
- **Службы и приложения (Services And Applications)** Просмотр и управление свойствами служб и приложений, установленных на сервере.

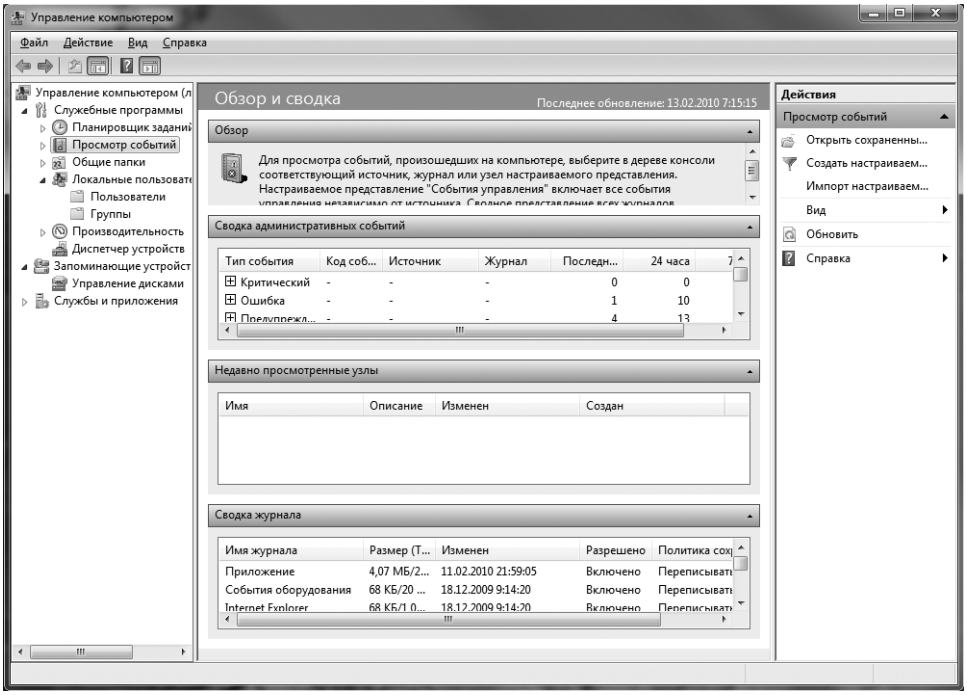

Рис. 6-1. Консоль Управление компьютером (Computer Management) предназначена для управления сетевыми компьютерами и ресурсами сети

В категориях располагаются следующие инструментальные средства:

- **Планировщик заданий (Task Scheduler)** Просмотр и управление запланированными заданиями, которые применяются для автоматизации таких процессов, как очистка дисков или диагностическая проверка. Задания, выполняющиеся по расписанию, и автоматизация описаны в главе 17.
- **Просмотр событий (Event Viewer)** Просмотр журналов регистрации событий на указанном компьютере. Журналы предназначены для записи информации о важных событиях, произошедших на компьютере. Они помогают найти проблемы конфигурации и прочие неисправности. События и журналы событий рассмотрены в главе 17.
- **Общие папки (Shared Folders)** Управление и просмотр общих папок, сеансов работы с ними и открытых файлов. Общие папки рассматриваются в главе 13.

- **Локальные пользователи и группы (Local Users And Groups)** Управление локальными пользователями и группами на заданном компьютере (не путайте их с пользователями и группами домена). Работа с локальными пользователями и группами описана в главе 5.
- **Производительность (Performance)** Средства для мониторинга и создания отчетов о текущей производительности компьютера и о ее изменении со временем.
- **Диспетчер устройств (Device Manager)** Главный инструмент для проверки состояния всех установленных на компьютере устройств и драйверов. Также может использоваться при поиске неисправностей оборудования. Управлению устройствами посвящена глава 8.
- **Управление дисками (Disk Management)** Управление жесткими дисками, разделами и наборами томов. В Windows 7 поддерживаются составные и чередующиеся тома. *Составным* (spanned) называется один том, расположенный на нескольких дисках. *Чередование* (striping) — это распределение данных по нескольким дискам для ускорения доступа. Ни одна из двух этих технологий не обеспечивает отказоустойчивости. В случае сбоя одного из дисков составного или чередующегося тома выходит из строя весь том.
- **Службы (Services)** Просмотр системных служб, выполняющихся на компьютере, и управление ими. В Windows 7 для каждой службы предусмотрена политика восстановления. В случае сбоя службы производится попытка автоматического запуска службы с автоматической обработкой зависимостей. Перед перезапуском сбойной службы запускаются зависимые службы и компоненты. Работе со службами посвящена глава 8.
- **Управляющий элемент WMI (WMI Control)** Управление инструментарием управления Windows (Windows Management Instrumentation, WMI). Служба WMI отвечает за сбор сведений о системе, наблюдение за работоспособностью системы и управление компонентами. Дополнительные сведения вы найдете далее в разделе «Управляющий элемент WMI».

Чтобы в консоли **Управление компьютером (Computer Management)** подключиться к удаленному компьютеру, выполните следующие действия:

1. В дереве консоли щелкните правой кнопкой узел **Управление компьютером (Computer Management)** и выберите команду **Подключиться к другому компьютеру (Connect To Another Computer)**.
2. В открывшемся диалоговом окне **Выбор компьютера (Select Computer)** щелкните **Другим компьютером (Another Computer)** и введите полное имя компьютера, например *cspc85.microsoft.com*, где *cspc85* — имя компьютера, а *microsoft.com* — доменное имя. Чтобы найти компьютер, щелкните **Обзор (Browse)**.
3. Щелкните **OK**.

Основные сведения о системе и производительности

Для просмотра и настройки свойств системы предназначена консоль Система (System). Чтобы открыть ее, выполните следующие действия:

1. Откройте панель управления.
2. Щелкните **Система и безопасность (System And Security)**.
3. Выберите пункт **Система (System)**.

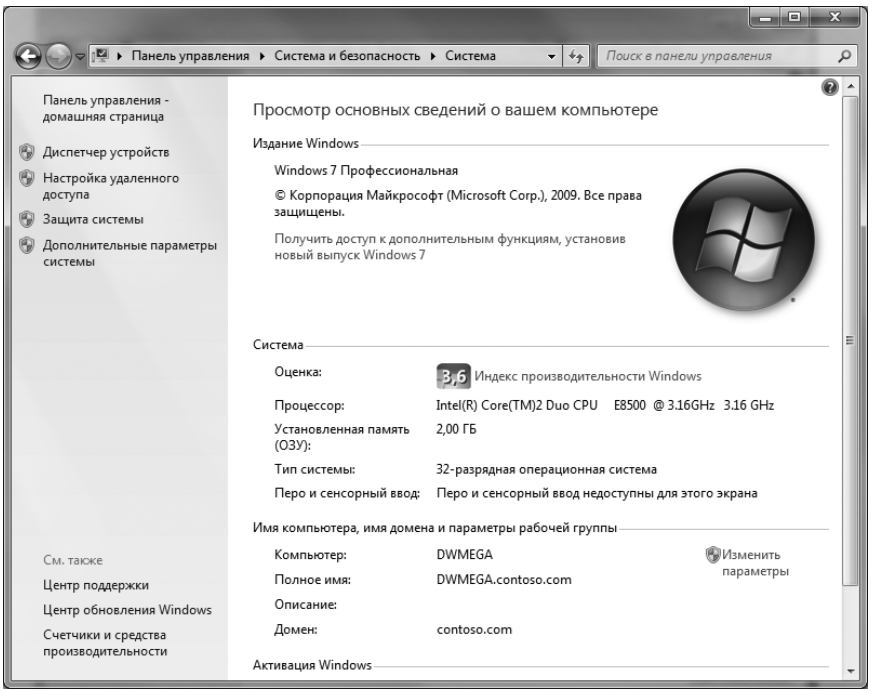

Рис. 6-2. Консоль Система (System) предназначена для просмотра и настройки свойств системы

Консоль Система (System) состоит из четырех областей (рис. 6-2), в которых находятся ссылки на команды для выполнения общих задач и сводка системных параметров:

- **Издание Windows (Windows Edition)** Сведения об издании и версии Windows.
- **Система (System)** Сведения о процессоре, ОЗУ, индексе производительности и типе установленной ОС (32-разрядная и 64-разрядная).
- **Имя компьютера, имя домена и параметры рабочей группы (Computer Name, Domain, And Workgroup Settings)** Здесь содержится имя компьютера, а также сведения о домене, домашней или рабочей группе. Чтобы изменить эту информацию, перейдите по ссылке **Изменить параметры (Change Settings)**, после чего в диалоговом окне **Свойства системы (System Properties)** щелкните **Идентификация (Network ID)**.
- **Активация Windows (Windows Activation)** Указывает на состояние активации ОС и ключ продукта. Если Windows 7 еще не активирована,

перейдите по соответствующей ссылке и следуйте подсказкам на экране. Чтобы изменить ключ продукта щелкните **Изменить ключ продукта (Change Product Key)** и введите новый ключ.

Ссылки, расположенные на левой панели консоли Система (System), предназначены для быстрого доступа к ключевым средствам поддержки:

- Диспетчер устройств (Device Manager);
- Дополнительные параметры системы (Advanced System Settings);
- Защита системы (System Protection);
- Настройка удаленного доступа (Remote Settings).

Ссылка **Изменить параметры (Change Settings)** в области **Имя компьютера, имя домена и параметры рабочей группы (Computer Name, Domain, And Workgroup Settings)** открывает доступ к диалоговому окну **Свойства системы (System Properties)**. Подробнее об этом окне мы расскажем далее, в разделе «Управление свойствами системы».

Индекс производительности Windows (Windows Experience Index) важен при определении функциональных возможностей ОС, поддерживаемых компьютером. В большинстве случаев оценка выполняется программой установки Windows после завершения установки. Дополнительную информацию об оценке производительности компьютера вы найдете, щелкнув ссылку **Индекс производительности Windows (Windows Experience Index)** на странице **Счетчики и средства производительности (Performance Information And Tools)**, показанной на рис. 6-3.

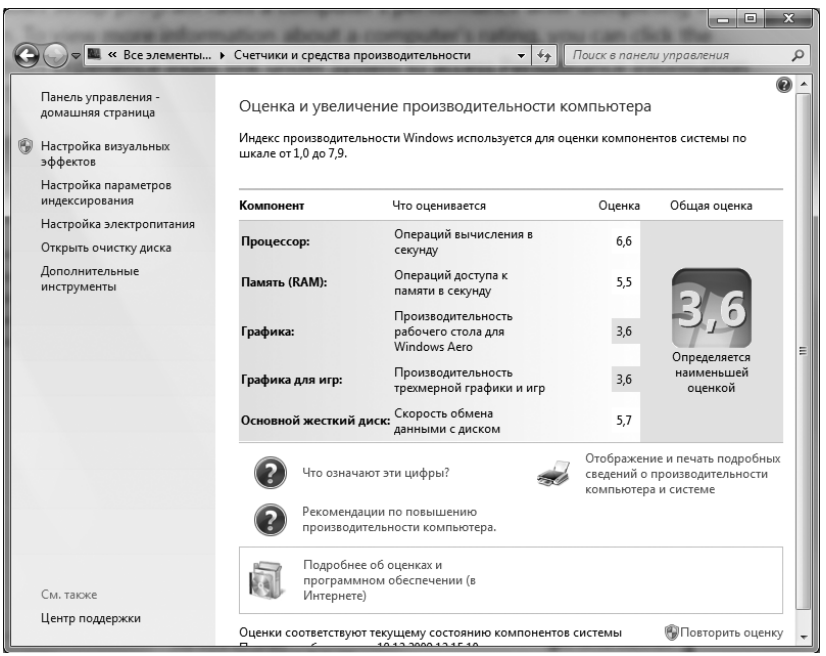

Рис. 6-3. Оценка компьютера и просмотр сведений о производительности в консоли Счетчики и средства производительности (Performance Information And Tools)

Ближе к реальности Если после установки ОС оценка компьютера не была произведена автоматически, у компьютера не будет индекса производительности. В таком случае откройте страницу **Счетчики и средства производительности (Performance Information And Tools)**, щелкнув ссылку **Оценка системы недоступна (System Rating Not Available)**, и произведите оценку системы. После установки нового оборудования оценка компьютера может измениться. При изменениях в конфигурации на экран выводится уведомление, в котором вам предлагается обновить индекс производительности Windows. Перейдите по соответствующей ссылке в окно **Счетчики и средства производительности (Performance Information And Tools)** и щелкните **Оценить компьютер (Refresh Now)**.

Еще один способ открыть страницу **Счетчики и средства производительности (Performance Information And Tools)** таков: последовательно щелкните **Пуск (Start)** и **Панель управления (Control Panel)**, затем в списке **Просмотр по (View By)** выберите вариант **Мелкие значки (Small Icons)** или **Крупные значки (Large Icons)** и щелкните **Счетчики и средства производительности (Performance Information And Tools)**. В окне приводится общая оценка системы и оценки оборудования, разделенные на пять категорий:

- процессор;
- ОЗУ;
- графика;
- графика для игр;
- основной жесткий диск.

Общая оценка компьютера и оценки оборудования применяются для определения рекомендуемых компонентов персонализации Windows 7. Если оценка компьютера низка, некоторые компоненты, например Windows Aero, будет рекомендовано отключить, чтобы увеличить производительность. Эволюция производительности также может стать поводом для рекомендации по отключению или изменению компонентов.

Совет На индексе производительности отрицательно сказывается ряд факторов, в частности, нехватка свободного места на жестком диске. Установив на компьютер новое оборудование или предприняв меры по повышению производительности, скажем, очистив свободное место на диске, щелкните **Оценить компьютер (Refresh Now)** или **Выполнить повторную оценку (Re-Run The Assessment)**, чтобы обновить оценку компьютера.

На левой панели страницы **Счетчики и средства производительности (Performance Information And Tools)** содержатся ссылки для быстрого доступа к некоторым полезным аспектам конфигурации:

- **Настройка визуальных эффектов (Adjust Visual Effects)** Управление визуальными эффектами, распределением времени процессора, виртуальной памятью и средством предотвращения выполнения данных в диалоговом окне **Параметры быстродействия (Performance Options)**.
- **Настройка параметров индексирования (Adjust Indexing Options)** Управление индексированием и его параметрами в диалоговом окне **Параметры индексирования (Indexing Options)**.

- **Настройка электропитания (Adjust Power Settings)** Настройка планов электропитания, действия при нажатии кнопки включения питания, времени отключения монитора и перехода в спящий режим на странице **Электропитание (Power Options)**.

На левой панели страницы **Счетчики и средства производительности (Performance Information And Tools)** есть очень удобная ссылка — **Дополнительные инструменты (Advanced Tools)**. Она открывает быстрый доступ к средствам обслуживания системы (рис. 6-4). Здесь вы найдете прямые ссылки на следующие компоненты:

- **Диспетчер задач (Task Manager)**, обычно открывающийся при нажатии клавиш Ctrl+Alt+Del.
- **Монитор ресурсов (Resource Monitor)**, обычно открывающийся кнопкой **Монитор ресурсов (Resource Monitor)** в диспетчере задач.
- **Просмотр дополнительных сведений о системе (Advanced system details for System Information)**, обычно открываемый командой Msinfo32.
- **Отчет о работоспособности системы (System diagnostics reports)**, который обычно генерируется только при проведении расширенной диагностики.

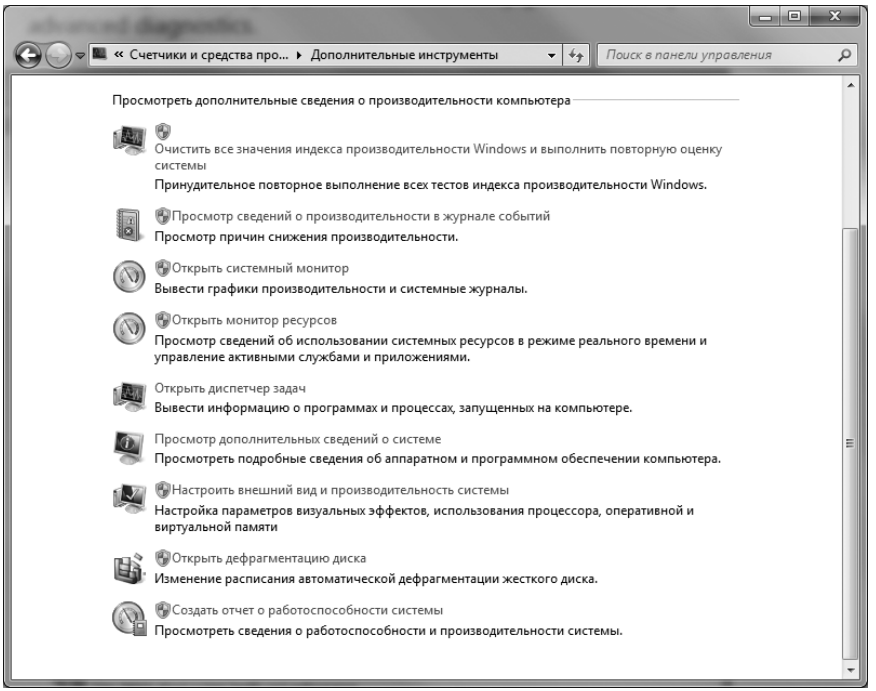

Рис. 6-4. Быстрый доступ к дополнительным инструментам для работы с компьютером

Если вы вошли в систему с учетной записью администратора, для создания отчета по результатам диагностики системы щелкните **Создать отчет о работоспособности системы (Generate A System Health Report)**. Создание

отчета занимает примерно 1 минуту (или больше). В отчете отражены сведения о состоянии аппаратных ресурсов, времени отклика системы и процессах, выполняющихся на компьютере, а также системная информация и данные конфигурации (рис. 6-5). В отчете также содержатся рекомендации по устранению неисправностей, повышению производительности и снижению издержек. Чтобы сохранить отчет в формате HTML, в меню **Файл (File)** выберите команду **Сохранить как (Save As)**, а затем укажите расположение и имя файла отчета в диалоговом окне **Сохранить как (Save As)**. Чтобы сохранить отчет в качестве вложения для сообщения электронной почты, в меню **Файл (File)** выберите команду **Отправить (Send To)**.

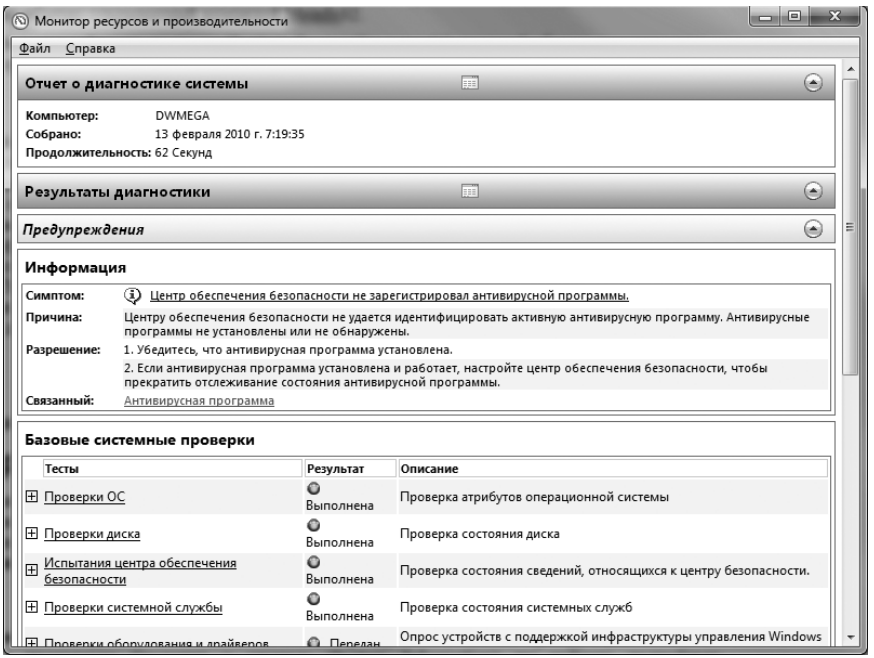

Рис. 6-5. Отчет о работоспособности помогает устранить проблемы производительности

Просмотр расширенных сведений о системе

Программа Сведения о системе (System Information) предназначена для получения подробной информации о системе на локальном или удаленном компьютере. Щелкните кнопку **Пуск (Start)** введите **msinfo32** в строку поиска и нажмите Enter. Чтобы просмотреть сводку по системе (рис. 6-6), выберите узел **Сведения о системе (System Summary)**. Представленные данные о конфигурации собраны при помощи службы WMI.

При помощи программы Сведения о системе (System Information) вы найдете подробную информацию по нескольким важным аспектам ОС:

- **Аппаратные ресурсы (Hardware Resources)** Подробная информация о вводе-выводе, прерываниях, памяти, канале DMA и устройствах Plug

and Play. При наличии в системе аппаратных проблем прежде всего просмотрите узел **Конфликты и совместное использование (Conflicts/Sharing)**. Здесь перечислены устройства, которые используют общие ресурсы или являются причиной системных конфликтов.

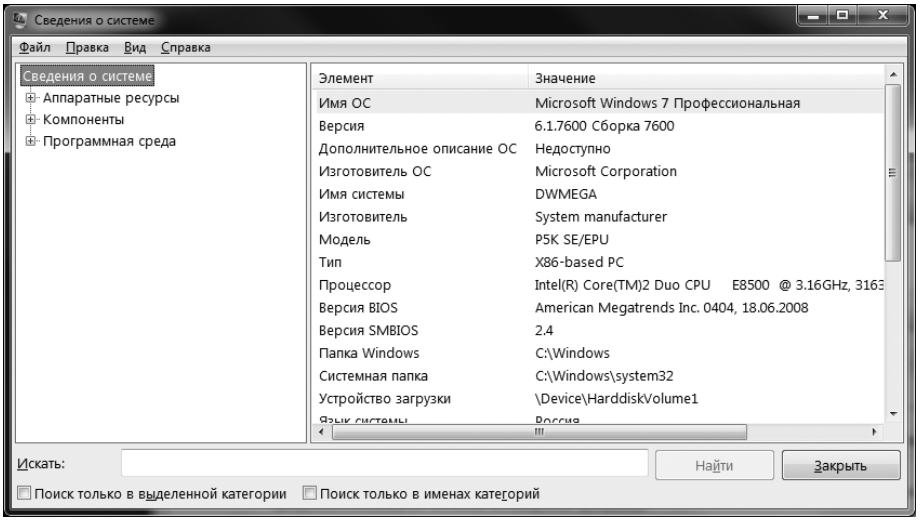

Рис. 6-6. Расширенные сведения о системе полезны при диагностике конфигурации

- **Компоненты (Components)** Подробная информация об установленных компонентах от аудио-кодеков до устройств ввода и портов универсальной последовательной шины USB. При возникновении в системе неполадок, связанных с компонентами, просмотрите узел **Устройства с неполадками (Problem Devices)**. Здесь вы найдете информацию о компонентах, работающих с ошибками.
- **Программная среда (Software Environment)** Подробная информация о текущей конфигурации ОС. Область **Программная среда (Software Environment)** особенно полезна при диагностике удаленной системы. В дополнение к драйверам, переменным среды, заданиям печати и сетевым подключениям вы проверите выполняющиеся задачи, службы, группы программ и автозагрузку.

Чтобы получить сведения о конфигурации удаленного компьютера, выполните следующие действия:

1. Откройте программу **Сведения о системе (System Information)** и выберите в меню **Вид (View)** команду **Удаленный компьютер (Remote Computer)**.
2. В открывшемся диалоговом окне **Удаленный компьютер (Remote Computer)** щелкните **Удаленный компьютер в сети (Remote Computer On The Network)**.
3. Введите имя компьютера и щелкните **OK**.

Ваша учетная запись при этом должна обладать административными полномочиями в домене или на локальном компьютере. Если при получении информации от удаленной системы возникли проблемы, проверьте пространство имен, используемое службой WMI (см. следующий раздел).

Управляющий элемент WMI

Инструментарий управления Windows (Windows Management Instrumentation, WMI) — ключевое звено Windows 7. Он предназначен для сбора системной статистики, наблюдения за работоспособностью системы и управления ее компонентами. Правильную работу компонента WMI обеспечивает служба WMI, которую необходимо запустить и настроить соответственно среде.

Настройка конфигурации службы WMI на локальном или удаленном компьютере выполняется в консоли **Управляющий элемент WMI (WMI Control)**. Чтобы открыть ее, выполните следующие действия:

1. Щелкните **Пуск (Start)**, выберите **Все программы (All Programs)**, **Администрирование (Administrative Tools)** и **Управление компьютером (Computer Management)**. Другой способ: откройте панель управления, перейдите по ссылкам **Система и безопасность (System And Security)**, **Администрирование (Administrative Tools)**, затем дважды щелкните **Управление компьютером (Computer Management)**.
2. В дереве консоли щелкните правой кнопкой узел **Управление компьютером (Computer Management)** и выберите команду **Подключиться к другому компьютеру (Connect To Another Computer)**. Выберите систему, службами которой вы собираетесь управлять.
3. Разверните узел **Службы и приложения (Services And Applications)** и выберите **Управляющий элемент WMI (WMI Control)**. (Это необходимо для считывания управляющего элемента.) Правой кнопкой щелкните **Управляющий элемент WMI (WMI Control)** и выберите **Свойства (Properties)**. Настройте службу WMI в диалоговом окне свойств управляющего элемента WMI.

На рис. 6-7 показаны вкладки диалогового окна **Свойства: Управляющий элемент WMI (WMI Control Properties)**:

- **Общие (General)** Краткая сводка сведений о системе и службе WMI. При получении службой WMI системной информации используются учетные данные текущего пользователя.
- **Архивация или восстановление (Backup/Restore)** Статистические данные, собранные службой WMI, помещаются в хранилище, по умолчанию расположенное в папке %SystemRoot%\System32\Wbem\Repository. Резервное копирование статистической информации выполняется автоматически через равные промежутки времени. На этой вкладке можно выполнить архивацию вручную.
- **Безопасность (Security)** Параметры безопасности определяют пользователей, имеющих доступ к различным уровням статистики службы

WMI. По умолчанию полный доступ к службе WMI имеет группа Администраторы (Administrators), а группа Прошедшие проверку (Authenticated Users) обладает разрешениями на выполнение методов, включение учетных записей и запись собранной статистики.

- **Дополнительно (Advanced)** Дополнительные параметры определяют пространство имен по умолчанию для службы WMI. При написании сценариев WMI пространство имен по умолчанию применяется в случае, если для объекта WMI на задан полный путь к пространству имен. Чтобы изменить умолчание, щелкните **Изменить (Change)**, выберите новое пространство имен, используемое по умолчанию, и щелкните **OK**.

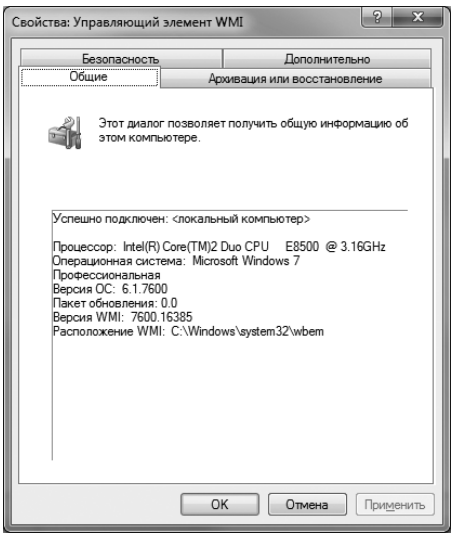

Рис. 6-7. Управляющий элемент WMI (WMI Control) предназначен для управления конфигурацией службы WMI

Примечание Журналы ошибок, используемые при диагностике службы WMI, обслуживаются управляющим элементом WMI. По умолчанию журналы находятся в папке %SystemRoot%\System32\Wbem\Logs. Файлы обслуживания WMI, журналов и хранилищ могут занимать значительное место на диске. На моих тестовых системах им требовалось в среднем 65 Мб. В основном, это были файлы резервной копии хранилища (40–50 Мб).

Информация, собранная WMI, сохраняется в наборе системных файлов, так называемом *хранилище* (repository). По умолчанию файлы хранилища находятся в папке %SystemRoot%\System32\Wbem\Repository. Хранилище — центральный элемент WMI и системы справки и поддержки. Информация перемещается в хранилище при помощи промежуточного файла. В случае повреждения данных хранилища или промежуточного файла служба WMI может работать неправильно. Обычно это временное явление, избежать которого можно при помощи ручной архивации файла хранилища.

Чтобы выполнить резервное копирование хранилища WMI вручную, выполните следующие действия:

1. Откройте диалоговое окно **Свойства: Управляющий элемент WMI (WMI Control Properties)**.
2. На вкладке **Архивация и восстановление (Backup/Restore)** щелкните **Архивировать (Back Up Now)**. В диалоговом окне **Укажите имя файла архива (Specify A Name For Your Backup File)** задайте расположение и имя файла резервной копии WMI. Щелкните **Сохранить (Save)**.

   Ход резервного копирования отображается в окне **Выполняется архивация (Backup In Progress)**. Файл восстановления имеет расширение .rec, а его размер зависит от количества сохраненной в нем информации. Обычно размер файла равен 20–30 Мб.

Чтобы восстановить хранилище WMI из архива, выполните следующие действия:

1. Откройте диалоговое окно **Свойства: Управляющий элемент WMI (WMI Control Properties)**.
2. На вкладке **Архивация и восстановление (Backup/Restore)** щелкните **Восстановить (Restore Now)**. В диалоговом окне **Укажите имя файла архива для восстановления (Specify A Name For Your Backup File)** задайте расположение и имя файла архива WMI. Щелкните **Открыть (Open)**.
3. На экране появится диалоговое окно **Восстановление (Restore In Progress)**, после чего будет выведено предупреждение. Щелкните **OK**.
4. Произойдет отключение от управляющего элемента WMI, восстановить которое можно после завершения операции восстановления. Для этого закройте и снова откройте диалоговое окно **Свойства: Управляющий элемент WMI (WMI Control Properties)**. Подключение управляющего элемента WMI к локальному или удаленному компьютеру будет восстановлено, но только после завершения операции восстановления.

Примечание Ошибка подключения обычно свидетельствует о продолжающемся восстановлении хранилища управляющего элемента WMI. Подождите 30-60 секунд и попробуйте еще раз.

Инструментарий поддержки системы

В операционную систему Windows 7 включен большой набор средств поддержки:

- **Резервное копирование** Программа **Архивация и восстановление (Backup And Restore)** предназначена для резервного копирования и восстановления системных и пользовательских файлов. Подробнее — в главе 17.
- **Встроенные средства диагностики** Служат для проверки системы и выявления проблем аппаратной и программной конфигурации. Полученные сведения используются при поиске и устранении несоответствий

между производительностью и параметрами конфигурации. Средства диагностики рассмотрены в этой и последующих главах.

- **Средство диагностики DirectX (DirectX Diagnostic Tool, Dxdiag.exe)** Инструмент для выявления ошибок Microsoft DirectX. Технология DirectX применяется для ускорения работы приложений, при условии что оборудование поддерживает DirectX.
- **Очистка диска (Cleanmgr.exe)** Утилита **Очистка диска (Disk Cleanup)** предназначена для поиска на диске ненужных файлов. По умолчанию проверяются временные файлы, корзина и различные типы автономных файлов, после чего они удаляются, если это возможно.
- **Дефрагментация диска (Dfrgui.exe)** Утилита **Дефрагментация диска (Disk Defragmenter)** используется для проверки дисков на наличие фрагментированных областей и их дефрагментации. Диск с большим количеством фрагментированных файлов может замедлить работу системы. Подробнее — в главе 12.
- **Проверка подписи файла (Signature Verification Utility, Sigverif.exe)** Проверка файлов ОС, имеющих цифровую подпись. В список попадают все критически важные файлы, не имеющие цифровой подписи. Полный список всех проверенных файлов находится в файле журнала %SystemRoot%\Sigverif.txt.
- **Предложение удаленной помощи** Вы вольны предложить пользователю свою удаленную помощь. Если пользователь примет предложение, вы сможете заняться поиском и устранением неисправностей на его компьютере (см. главу 17).
- **Удаленный помощник (Remote Assistance)** Вы можете создать приглашение удаленного помощника, чтобы получить помощь специалиста. Подробнее об удаленном помощнике — в главе 17.
- **Конфигурация системы (System Configuration, Msconfig.exe)** Позволяет управлять данными настройки системы. В вашем распоряжении обычный, диагностический и выборочный режимы запуска системы.
- **Восстановление системы (System Restore, Rstrui.exe)** При помощи этой утилиты можно создавать точки восстановления или возврата системы к состоянию на момент создания точки восстановления. Дополнительные сведения о программе Восстановление системы (System Restore) — в главе 17.

Здесь мы подробнее остановимся на инструментах для очистки диска, проверки подписи файла и настройки системы.

Очистка диска

Утилита Очистка диска (Disk Cleanup) предназначена для поиска на диске ненужных файлов. Для начала работы с ней выполните следующие действия:

1. В меню **Пуск (Start)** последовательно выберите **Программы (Programs)** или **Все программы (All Programs)**, **Стандартные (Accessories)**, **Служебные (System Tools)** и **Очистка диска (Disk Cleanup)**.

Примечание Исполняемый файл программы — Cleanmgr.exe. Для быстрого запуска очистки диска щелкните кнопку **Пуск (Start)**, введите **cleanmgr** в поле поиска и нажмите Enter.

2. Если на компьютере установлено несколько жестких дисков, сначала будет выведено диалоговое окно **Выбор устройств (Drive Selection)**. В раскрывающемся списке **Диски (Drives)** выберите целевой диск и щелкните **OK**.

   Указанный диск будет проверен на наличие файлов пользователей, которые можно удалить, и файлов-кандидатов на удаление. Чем больше файлов на диске, тем больше времени займет процесс поиска.
3. После начального прохода очистки диска отметьте для удаления временные системные файлы, а также системные файлы, предлагаемые для удаления. Щелкните **Очистить системные файлы (Clean Up System Files)**, выберите системный диск и щелкните **OK**. На экране появится отчет (рис. 6-8).

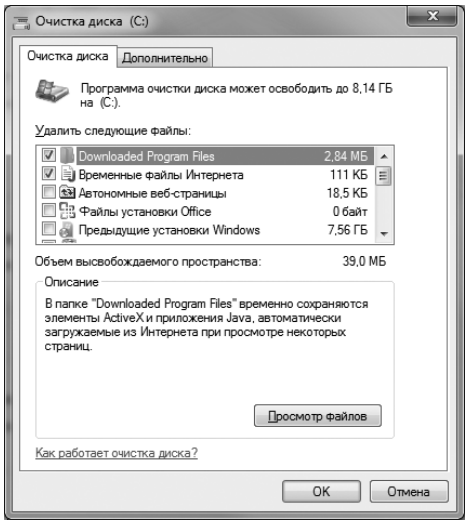

Рис. 6-8. Программа Очистка диска (Disk Cleanup) предназначена для поиска файлов, которые можно удалить

В отчете представлены следующие категории файлов:

- **Загруженные файлы приложений (Downloaded Program Files)** Программы, загруженные для выполнения в браузере, например, элементы управления ActiveX и приложения Java. Это временные файлы, которые можно удалить.

- **Файлы, выброшенные обновлением Windows (Files DiscardedBy Windows Upgrade)** Файлы предыдущего обновления Windows, не помеченные как системные файлы Windows. Когда вы сохраните все необходимые данные из предыдущих установок Windows, включая данные пользователей, удалите эти файлы, освободив тем самым место на диске.
- **Очистка файлов режима гибернации (Hibernation File Cleaner)** Сведения о состоянии компьютера до перехода в режим гибернации. Если режим гибернации не используется, этот файл можно удалить.
- **Временные файлы Microsoft Office (Microsoft Office Temporary Files)** Временные файлы и журналы, используемые программами Microsoft Office. Их можно удалить.
- **Автономные файлы (Offline Files)** Локальные копии сетевых файлов, предназначенные для автономного использования. Эти файлы сохраняются, чтобы обеспечить доступ к содержащейся в них информации в автономном режиме. Их можно удалить.
- **Автономные веб-страницы (Offline Web Pages)** Локальные копии веб-страниц, предназначенные для автономного использования. Эти файлы сохраняются, чтобы обеспечить доступ к содержащейся в них информации в автономном режиме. Их можно удалить.
- **Предыдущие установки Windows (Previous Windows Installation(s))** В папке %SystemDrive%\Windows.old находятся файлы предыдущих установок Windows. Сохранив все необходимые данные из предыдущих установок Windows, включая данные пользователей, эти файлы можно удалить, освободив тем самым место на диске.
- **Временные автономные файлы (Temporary Offline Files)** Временные данные и рабочие файлы для недавно использовавшихся сетевых файлов. Эти файлы сохраняются, чтобы обеспечить работу в автономном режиме, и могут быть удалены.
- **Корзина (Recycle Bin)** Удаленные файлы, которые можно восстановить. Если очистить корзину, файлы будут удалены безвозвратно.
- **Временные файлы (Temporary Files)** Информация, содержащаяся в папке Temp. Главным образом, это временные данные или рабочие файлы приложений.
- **Временные файлы Интернета (Temporary Internet Files)** Веб-странцы, сохраняемые для поддержки кеша страниц браузера. Это временные файлы, которые можно удалить.
- **Эскизы (Thumbnails)** Здесь размещены эскизы страниц, видео и документов, создаваемые Windows 7. Когда вы открываете папку в первый раз, в Windwos 7 создаются эскизы страниц, видео и документов. Эскизы сохраняются, чтобы ускорить их вывод при следующем открытии папки. Если вы удалите эскизы, при следующем открытии папки они будут созданы вновь.

4. В списке **Удалить следующие файлы (Files To Delete)** установите флажки у файлов, которые нужно удалить. Затем щелкните **OK**. Подтвердите действие, щелкнув **Да (Yes)**.

Проверка подписи системных файлов

Критически важные файлы ОС имеют цифровую подпись, которая подтверждает подлинность файлов. Благодаря подписи проще найти изменения, способные негативно отразиться на состоянии системы. Когда возникают необъяснимые неполадки, например после установки приложения система работает нестабильно, убедитесь, что критически важные системные файлы не были изменены. Делается это в утилите Проверка подписи файла (Signature Verification Utility), исполняемый файл которой — Sigverif.exe. Далее приведен пример работы с утилитой Проверка подписи файла (Signature Verification Utility):

1. Чтобы запустить программу Проверка подписи файла (Signature Verification Utility), щелкните кнопку **Пуск (Start)**, введите **sigverif** и нажмите Enter (рис. 6-9).

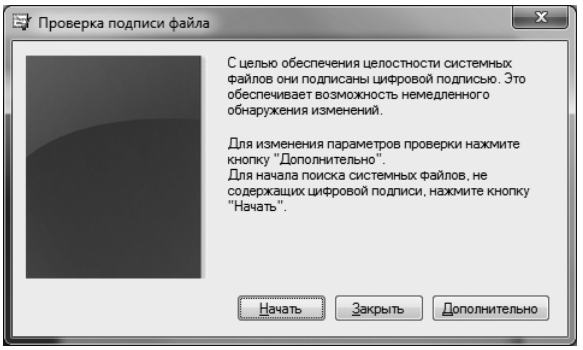

Рис. 6-9. Проверка системных файлов в программе Проверка подписи файла (Signature Verification Utility)

2. По умолчанию системные файлы, не имеющие цифровой подписи, выводятся на экран и записываются в файл %SystemRoot%\System32\Sigverif.txt. Перед проверкой файлов задайте параметры журнала, щелкнув **Дополнительно (Advanced)**. Откроется окно, показанное на рис. 6-10. В файле Sigverif.txt результаты предыдущей проверки переписываются результатами текущей проверки. Чтобы найти изменения в файлах, результаты нужно добавлять, а не переписывать: так вы быстрее найдете несоответствия. Настроив параметры журнала, щелкните **OK** для возврата в главное окно.

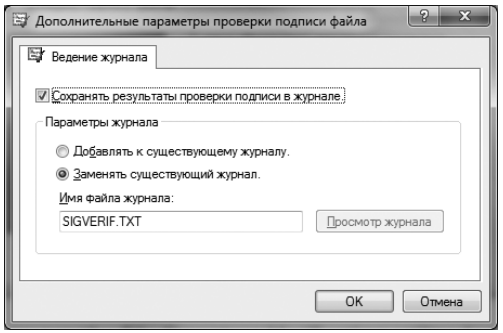

Рис. 6-10. Изменение стандартных параметров журнала

3. Щелкните кнопку **Начать (Start).** В окне результатов проверки (рис. 6-11) просмотрите получившийся список. Файлы, находящиеся в списке, не имеют цифровой подписи. Это может свидетельствовать об их подмене злоумышленниками. Для возврата в главное окно щелкните **Закрыть (Close)**. Если у вас возникли подозрения, проверьте журналы регистрации событий и прочие отчеты об ошибках. Возможно, эти файлы фигурируют и там.

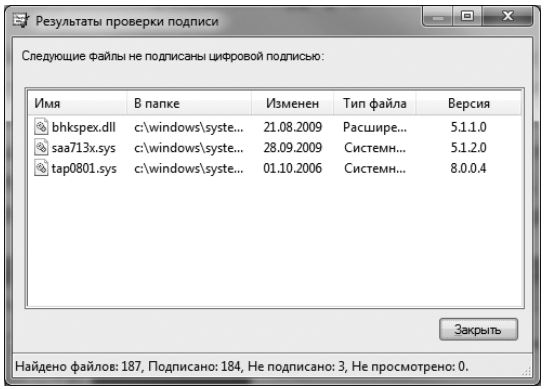

Рис. 6-11. Просмотр результатов проверки

4. Чтобы просмотреть журнал проверки, щелкните **Дополнительно (Advanced)** и **Просмотр журнала (View Log)**. Вы также вольны открыть журнал проверки, который по умолчанию находится в файле %SystemRoot%\System32\Sigverif.txt, в программе Блокнот (Notepad). Ищите файлы, которые были изменены после их установки. Файлы отсортированы по состоянию: Подписано (Signed) и Не подписано (Not Signed). Обращайте внимание на дату изменения и версию файла. Если неполадки компьютера начались в определенный день, и в этот же день были изменены критически важные файлы, возможно, в этом и заключается проблема. Например, при установке программы версия критически важного файла могла быть заменена на старую.

Управление конфигурацией, запуском и загрузкой системы

Если нужно обновить файлы системной конфигурации или найти и устранить неисправность, возникающую при запуске системы, используйте утилиту Конфигурация системы (System Configuration) — инструмент для управления сведениями о конфигурации. С его помощью вы настроите следующие элементы:

- параметры запуска ОС;
- автозагрузка;
- параметры запуска служб.

В следующих разделах мы рассмотрим ключевые задачи, решаемые при помощи утилиты Конфигурация системы (System Configuration), исполняемый файл — Msconfig.exe. Для запуска программы щелкните **Пуск (Start)** введите в строке поиска **msconfig** и нажмите Enter.

Режимы запуска и диагностика запуска системы

Программа Конфигурация системы (System Configuration) позволяет запустить компьютер в одном из трех режимов:

- **Обычный запуск (Normal Startup)** Система загружается обычным способом. В этом режиме загружаются все файлы системной конфигурации и драйверы устройств, запускаются все приложения, загружаемые автоматически, и включенные службы.
- **Диагностический запуск (Diagnostic Startup)** Применяется для поиска и устранения неисправностей в системе. В режиме диагностики загружаются драйверы только для основных устройств и самых необходимых служб. Режим диагностики позволяет изменять параметры системы для решения проблем с конфигурацией.
- **Выборочный запуск (Selective Startup)** Используется для точного выявления проблемных областей конфигурации. Здесь вы можете применить измененную конфигурацию загрузки, запустить только избранные службы и элементы автозагрузки. Это позволяет найти и при необходимости исправить параметры, лежащие в основе неисправности системы.

По умолчанию система запускается в обычном режиме. При возникновении неполадок запустите систему в другом режиме, выполнив следующие действия:

1. Щелкните кнопку **Пуск (Start)**, введите **msconfig** и нажмите Enter.
2. В окне **Конфигурация системы (System Configuration)**, показанном на рис. 6-12, на вкладке **Общие (General)** выберите **Диагностический запуск (Diagnostic Startup)** или **Выборочный запуск (Selective Startup)**. При выборочном запуске укажите элементы, которые должны использоваться системой, при помощи следующих параметров:
   - **Загружать системные службы (Load System Services)** Во время запуска системы будут загружены службы Windows. Выбрав этот вари-

ант, укажите на вкладке **Службы (Services)** службы, которые следует запускать.

- **Загружать элементы автозагрузки (Load Startup Items)** Во время загрузки будут запущены приложения, выполняющиеся автоматически. Выбрав этот параметр, включите или выключите автоматический запуск приложений на вкладке **Автозагрузка (Startup)**.
- **Использовать оригинальную конфигурацию загрузки (Use Original Boot Configuration)** Загрузка будет выполнена с оригинальной конфигурацией, без изменений, внесенных вами в параметры загрузки.

Примечание Если вы внесли изменения в параметры на вкладках **Загрузка (Boot)**, **Службы (Services)** или **Автозагрузка (Startup)**, переключатель **Выборочный запуск (Selective Startup)** и связанные с ним флажки на вкладке **Общие (General)** будут установлены автоматически.

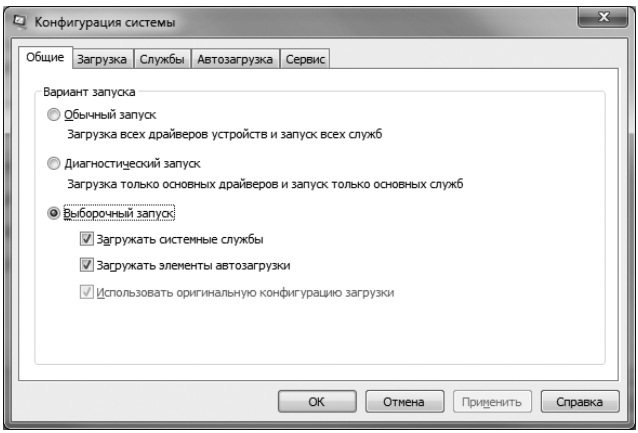

Рис. 6-12. Выбор варианта запуска системы на вкладке Общие (General)

3. Для продолжения настройки щелкните **OK** и перезагрузите систему. Если во время перезагрузки возникнут неисправности, перезапустите систему в безопасном режиме и повторите процедуру. Безопасный режим автоматически появляется в числе вариантов загрузки после неудачной попытки загрузки.

Изменение параметров загрузки

Для запуска Windows 7 используются диспетчер загрузки Windows (Windows Boot Manager) и приложение загрузки. В стандартной конфигурации Windows 7 файл Boot.ini и прочие файлы загрузки не применяются. Во время поиска и устранения неисправностей вы можете изменить загрузочный раздел, метод загрузки и параметры загрузки ОС на вкладке **Загрузка (Boot)** окна утилиты Конфигурация системы (System Configuration).

На рис. 6-13 показано окно **Конфигурация системы (System Configuration)**, открытое на вкладке **Загрузка (Boot)**. Здесь перечислены операционные системы, которые можно загрузить на компьютере. Чтобы исполь-

зовать ОС, отличную от текущей, достаточно щелкнуть соответствующую запись, и задать следующие параметры:

- **Использовать по умолчанию (Set As Default)** Указанный загрузочный раздел будет сделан разделом по умолчанию. Загрузка с установленного по умолчанию раздела начнется автоматически, если по истечении времени ожидания не будет выбран другой вариант.
- **Таймаут (Timeout)** Время ожидания до начала загрузки из раздела по умолчанию.
- **Удалить (Delete)** Удаление записи ОС. Восстановить запись не так просто, поэтому удалять ее следует только в случае крайней необходимости.

Примечание На компьютерах с одной ОС кнопки **Использовать по умолчанию (Set As Default)** и **Удалить (Delete)** недоступны. Для ОС, загружаемой по умолчанию, параметр **Использовать по умолчанию (Set As Default)** недоступен. Текущую ОС невозможно удалить.

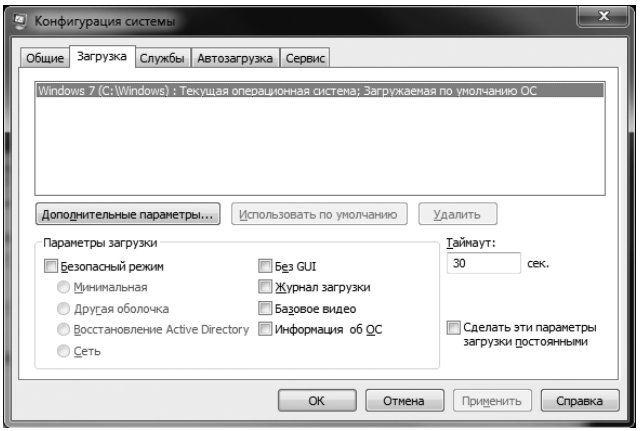

Рис. 6-13. Изменение загрузочного раздела, метода и параметров загрузки ОС

Вы можете задать следующие параметры загрузки:

- **Безопасный режим (Safe Boot)** Загрузка в безопасном режиме с дополнительными параметрами для минимальной и сетевой загрузки, для восстановления Active Directory (Dsrepair), а также для загрузки с другой оболочкой. Загрузка системы в безопасном режиме позволяет изменять параметры системы при выявлении проблем конфигурации.
- **Без GUI (No GUI Boot)** Компьютер загружается в режиме командной строки без загрузки графических компонентов ОС. Загрузка в режиме командной строки используется при неисправности графических компонентов Windows 7.
- **Журнал загрузки (Boot Log)** Включение записи ключевых событий загрузки в журнал.
- **Базовое видео (Base Video)** Применение параметров дисплея VGA. Данный режим используется при несоответствии параметров экрана, например, если размер экрана не поддерживается монитором.

- **Информация об ОС (OS Boot Information)** При запуске компьютера перед загрузкой графических компонентов Windows выводится подробная информация относительно действий во время загрузки.

Внеся изменения, щелкните **OK** и перезагрузите компьютер, чтобы применить их. Для возврата к обычному запуску после применения изменений на вкладке **Общие (General)** установите переключатель **Обычный запуск (Normal Startup)** и щелкните **OK**. Чтобы обычные параметры вступили в силу, перезагрузите компьютер.

На вкладке **Загрузка (Boot)** есть кнопка **Дополнительные параметры (Advanced Options)**, щелкнув которую вы можете задать параметры процессоров, памяти, блокировки PCI и отладки в диалоговом окне **Дополнительные параметры загрузки (BOOT Advanced Options)**, показанном на рис. 6-14. Эти параметры применяются при диагностике. Например, если проблема, на ваш взгляд, связана с работой нескольких процессоров, можно задать здесь использование одного процессора. Если возможная причина связана с тем, что объем ОЗУ превышает 4 Гб, задайте максимальный объем памяти, скажем, 4096 Мб. По завершению диагностики установите для этих параметров обычные значения.

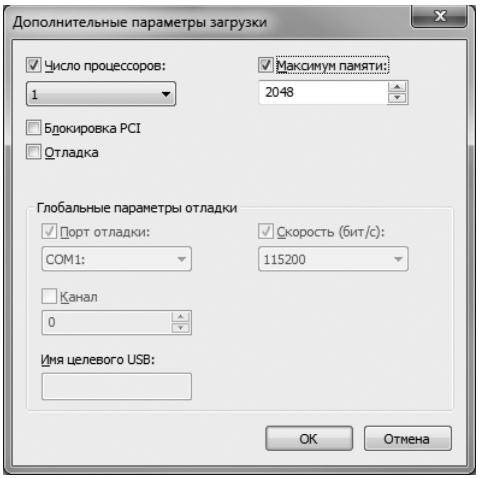

Рис. 6-14. Дополнительные параметры загрузки используются при диагностике

Чтобы сделать заданные вами стандартные и дополнительные параметры загрузки постоянными, на вкладке **Загрузка (Boot)** установите флажок **Сделать эти параметры загрузки постоянными (Make All Boot Settings Permanent)** и щелкните **OK**. Как правило, диагностические и отладочные параметры не следует использовать постоянно, поэтому не забудьте отказаться от них.

Диагностика: включение и отключение приложений автозагрузки

Проверить, не является ли причиной неполадок в системе приложение, загружаемое автоматически, очень легко. Отключите автоматический запуск

программы и перезагрузите систему. Если неисправность пропала, значит вы правильно локализовали проблему, и для ее решения достаточно отключить автоматическую загрузку программы. Если неисправность не устранена, повторите действия для других приложений автозагрузки.

Чтобы отключить автоматическую загрузку приложения, выполните следующие действия:

1. Щелкните кнопку **Пуск (Start)**, введите **msconfig** и нажмите Enter.
2. В окне **Конфигурация системы (System Configuration)** перейдите на вкладку **Автозагрузка (Startup)**. Здесь перечислены программы, загружаемые при запуске системы (рис. 6-15).

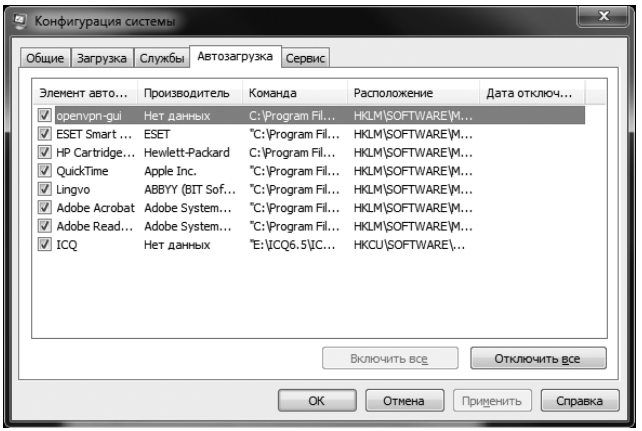

Рис. 6-15. Список приложений автозагрузки на вкладке Автозагрузка (Startup)

3. Сбросьте флажок приложения, которое не следует загружать при запуске.

Внимание! Отключайте только те программы, которые могут приводить к сбою, и только в том случае, если вы знаете, как они используются ОС. Если вы не знаете, что делает программа, не отключайте ее. Иногда дополнительные сведения о программе автозагрузки можно найти в ее установочной папке, где находится исполняемый файл.

4. Щелкните **OK**. Для проверки внесенных изменений необходимо перезагрузить систему. Щелкните **Да (Yes)** в ответ на соответствующее предложение или выполните перезагрузку вручную.
5. При необходимости повторяйте процедуру, пока не выявите программу, ставшую причиной сбоев в системе. Если найти сбойное приложение не удается, проблема может заключаться в компоненте Windows, службе или драйвере устройства.

Диагностика: включение и отключение служб

Службы, настроенные на автоматический запуск, как и приложения автозагрузки, могут стать причиной неполадок в системе. Для проведения диагностики временно отключите службу при помощи утилиты Конфигурация системы (System Configuration), перезагрузите систему и проверьте, не ис-

чезла ли неисправность. Если она устранена, значит, вы нашли настоящую причину. После этого службу придется отключить или проверить наличие обновлений у ее производителя.

Чтобы временно отключить службу, выполните следующие действия:

1. Щелкните кнопку **Пуск (Start)**, введите **msconfig** и нажмите Enter.
2. В окне **Конфигурация системы (System Configuration)** перейдите на вкладку **Службы (Services)**, показанную на рис. 6-16. Здесь перечислены все установленные на компьютере службы, их состояние — **Работает (Running)** или **Остановлена (Stopped)** — и производитель службы. Чтобы упростить поиск служб сторонних производителей, установите флажок **Не отображать службы Майкрософт (Hide All Microsoft Services)**.

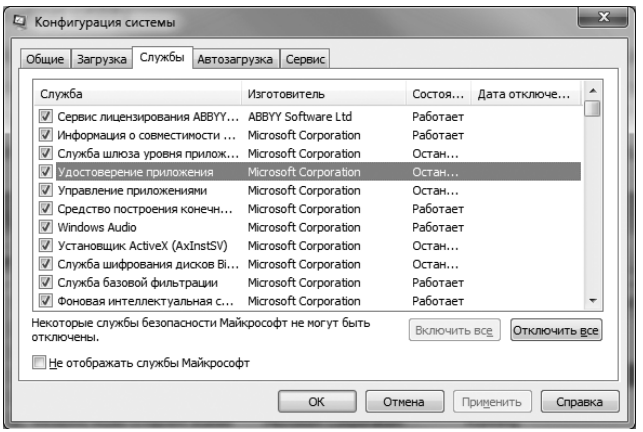

Рис. 6-16. Диагностика служб Windows

3. Сбросьте флажок службы, чтобы отменить ее автоматический запуск.

Внимание! Отключайте только те службы, которые могут приводить к сбою, и только в том случае, если вы знаете, как они используются ОС. Если вы не знаете назначение службы, не отключайте ее. О конкретном назначении служб можно узнать в консоли Службы (Services). Чтобы просмотреть описание, выделите службу и дважды щелкните ее.

4. Щелкните **OK**. Для проверки внесенных изменений необходимо перезагрузить систему. Щелкните **Да (Yes)** в ответ на соответствующее предложение или выполните перезагрузку вручную.
5. При необходимости повторяйте процедуру, пока не выявите службу, ставшую причиной сбоев в системе. Если таким образом не удается найти сбойную службу, проблема может заключаться в компоненте Windows, приложении автозагрузки или драйвере устройства.

Управление свойствами системы

Для управления свойствами системы применяется диалоговое окно **Свойства системы (System Properties)**. В следующих разделах описаны ключевые аспекты ОС, настраиваемые в этом диалоговом окне.

Вкладка Имя компьютера (Computer Name)

Чтобы просмотреть и изменить сетевую идентификацию компьютера, воспользуйтесь вкладкой **Имя компьютера (Computer Name)** диалогового окна **Свойства системы (System Properties)**, показанной на рис. 6-17. Как видите, здесь отображено полное имя компьютера, а также домен или группа, к которой он присоединен. По сути, полное имя компьютера — это его DNS-имя, определяющее место компьютера в иерархии Active Directory.

Чтобы открыть диалоговое окно **Свойства системы (System Properties)** на вкладке **Имя компьютера (Computer Name)**, выполните следующие действия:

1. Откройте панель управления, щелкните **Система и безопасность (System And Security)** и **Система (System)**.
2. В консоли Система (System) щелкните ссылку **Изменить параметры (Change Settings)** или **Дополнительные параметры системы (Advanced System Settings)** на левой панели и перейдите на вкладку **Имя компьютера (Computer Name)**.

Параметры вкладки **Имя компьютера (Computer Name)** позволяют выполнить следующие действия:

- **Присоединить компьютер к домену** Щелкните **Идентификация (Network ID)** и измените положение компьютера в сети при помощи мастера присоединения к домену или рабочей группе.
- **Переименовать компьютер** Чтобы изменить имя компьютера, а также связанный с ним домен или группу, щелкните **Изменить (Change)**.

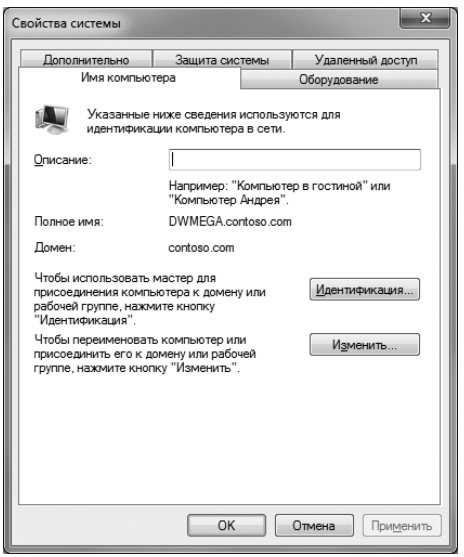

Рис. 6-17. Просмотр и настройка идентификации системы на вкладке Имя компьютера (Computer Name)

Ближе к реальности Прежде чем заняться присоединением компьютера к домену, проверьте правильность параметров IP, включая параметры DNS, для сети, к которой подключен компьютер. Чтобы клиентский компьютер мог использовать DNS, ему необходимо соответствующее имя и правильно настроенный основной суффикс DNS. Разработайте схему именования, чтобы имена имели смысл как для пользователей, так и для администраторов. В системе DNS имя компьютера — это имя узла, а основным DNS-суффиксом определяется домен, к которому присоединен компьютер для разрешения имен. Все неполные имена, задаваемые на компьютере, разрешаются при помощи основного DNS-суффикса. Например, на компьютере с основным DNS-суффиксом *tech.cpandl.com* команда *ping CorpSvr28* будет адресована узлу *corpsvr28.tech.cpandl.com*.

При необходимости основной DNS-суффикс компьютера можно изменить. Скажем, чтобы упростить разрешение имен в масштабной иерархии DNS, основной DNS-суффикс компьютера *seattle.tech.cpandl.com* можно заменить на *cpandl.com*. Чтобы изменить основной DNS-суффикс компьютера, на вкладке **Имя компьютера (Computer Name)** щелкните **Изменить (Change)**, а затем щелкните **Дополнительно (More)**. Введите новый основной DNS-суффикс в соответствующее поле и закройте все открытые диалоговые окна, трижды щелкнув **OK**.

Вкладка Оборудование (Hardware)

Вкладка **Оборудование (Hardware)** диалогового окна **Свойства системы (System Properties)** открывает доступ к Диспетчеру устройств (Device Manager) и Параметрам установки устройств (Device Installation Settings). Чтобы открыть диалоговое окно **Свойства системы (System Properties)** на вкладке **Оборудование (Hardware)**, выполните следующие действия:

1. Откройте панель управления, щелкните **Система и безопасность (System And Security)** и щелкните **Система (System)**.
2. В консоли Система (System) щелкните **Изменить параметры (Change Settings)** или **Дополнительные параметры системы (Advanced System Settings)**.
3. Перейдите на вкладку **Оборудование (Hardware)**.

Диспетчер устройств (Device Manager) также входит в виде оснастки в консоль Управление компьютером (Computer Management). При подключении к Windows 7 нового устройства при помощи Центра обновления Windows (Windows Update) выполняется автоматический поиск драйверов. Если вы хотите включить или отключить автоматический поиск драйверов, щелкните **Параметры установки устройств (Device Installation Settings)** и выберите **Да, делать это автоматически (Yes, Do This Automatically)** или **Нет, предоставить возможность выбора (No, Let Me Choose What To Do)**. Затем щелкните **OK**.

Примечание В отличие от предыдущих версий Windows, на вкладке **Оборудование (Hardware)** нет доступа к параметрам подписывания драйверов или профилям оборудования. Они настраиваются в групповой политике на основе Active Directory или в локальной групповой политике.

Вкладка Дополнительно (Advanced)

На вкладке **Дополнительно (Advanced)** диалогового окна **Свойства системы (System Properties)** собраны элементы управления многими ключевыми особенностями ОС Windows, включая быстродействие приложений, порядок использования виртуальной памяти, профили пользователей, переменные среды, а также параметры загрузки и восстановления.

Примечание В профиле пользователя хранятся глобальные параметры пользователя и сведения о конфигурации. Они создаются при первом входе пользователя на локальный компьютер или в домен. Профили локальных учетных записей отличаются от профилей учетных записей домена. Профиль пользователя обслуживает среду рабочего стола, поэтому рабочий стол остается неизменным при последующих входах пользователя в систему. Исчерпывающую информацию о профилях пользователей вы найдете в книге Windows Server 2008 Administrator's Pocket Consultant Second Edition (Microsoft Press, 2010).

Настройка быстродействия Windows

Интерфейс Windows 7 содержит много графических усовершенствований. К ним относятся визуальные эффекты меню, панелей инструментов, окон и панели задач. Чтобы настроить быстродействие Windows, выполните следующие действия:

1. Откройте панель управления, щелкните **Система и безопасность (System And Security)** и щелкните **Система (System)**.
2. В консоли Система (System) щелкните **Изменить параметры (Change Settings)** или **Дополнительные параметры системы (Advanced System Settings)**.
3. В диалоговом окне **Свойства системы (System Properties)** перейдите на вкладку **Дополнительно (Advanced)** и щелкните **Параметры (Settings)** на панели **Быстродействие (Performance)**.
4. Диалоговое окно **Параметры быстродействия (Performance Options)** откроется на вкладке **Визуальные эффекты (Visual Effects)**. Воспользуйтесь возможностями для управления визуальными эффектами:
   - **Восстановить значения по умолчанию (Let Windows Choose What's Best For My Computer)** Параметры быстродействия определяются ОС, исходя из аппаратной конфигурации. На новом компьютере этот вариант, скорее всего, будет тождественен варианту **Обеспечить наилучший вид (Adjust For Best Appearance)**. Однако его ключевая особенность состоит в том, что этот вариант задан системой на основе имеющегося оборудования и его производительности.
   - **Обеспечить наилучший вид (Adjust For Best Appearance)** Включение всех визуальных эффектов для всех графических интерфейсов, включение анимации и затухания для меню и панели задач, сглаживание экранных шрифтов, плавное прокручивание списков, эскизы папок и т. д. Эта настройка обеспечивает наилучший внешний вид Windows.

- **Обеспечить наилучшее быстродействие (Adjust For Best Performance)** Отключение визуальных эффектов (плавные переходы, сглаживание шрифтов), потребляющих большое количество ресурсов. Остается лишь базовый набор визуальных эффектов.
- **Особые эффекты (Custom)** Вы можете настроить визуальные эффекты при помощи соответствующих флажков в диалоговом окне **Параметры быстродействия (Performance Options)**. Если сбросить все флажки, визуальные эффекты использоваться не будут.

5. Завершив настройку визуальных эффектов, щелкните **Применить (Apply)**. Дважды щелкните **OK**, чтобы закрыть открытые диалоговые окна.

Настройка быстродействия приложений

Быстродействие приложений связано с заданными параметрами распределения времени процессора. Распределение времени процессора влияет на скорость отклика приложений, выполняющихся интерактивно (по сравнению с фоновыми приложениями, которые выполняются в качестве служб). Чтобы управлять быстродействием приложений, выполните следующие действия:

1. Откройте панель управления, щелкните **Система и безопасность (System And Security)** и щелкните **Система (System)**.
2. В консоли Система (System) щелкните **Изменить параметры (Change Settings)** или **Дополнительные параметры системы (Advanced System Settings)**.
3. В диалоговом окне **Свойства системы (System Properties)** перейдите на вкладку **Дополнительно (Advanced)**. Щелкните **Параметры (Settings)** на панели **Быстродействие (Performance)**.
4. В диалоговом окне **Параметры быстродействия (Performance Options)** есть несколько вкладок. Перейдите на вкладку **Дополнительно (Advanced)**. На панели **Распределение времени процессора (Processor Scheduling)** доступны следующие параметры:
   - **Программ (Programs)** Чтобы обеспечить интерактивным приложениям лучшее время отклика и большую долю доступных ресурсов, установите переключатель **Программ (Programs)**. Как правило, такой вариант подходит для рабочих станций под управлением Windows 7.
   - **Служб, работающих в фоновом режиме (Background Services)** Чтобы обеспечить фоновым приложениям лучшее время отклика по сравнению с активными программами, установите переключатель **Служб, работающих в фоновом режиме (Background Services)**. Обычно так поступают, когда компьютер под управлением Windows 7 является сервером (на нем установлены серверные роли, и он не используется в качестве рабочей станции). Например, компьютер с Windows 7 может быть сервером печати для отдела.
5. Щелкните **OK**.

Настройка виртуальной памяти

Виртуальная память позволяет расширить доступный объем ОЗУ за счет записи данных из оперативной памяти на жесткий диск, в файл подкачки. При необходимости данные извлекаются из файла подкачки обратно в ОЗУ.

Исходный файл подкачки создается автоматически на системном диске. По умолчанию на других дисках файла подкачки нет. Если есть необходимость, их нужно создать. При создании файла подкачки задается исходный и максимальный объем. Имя файла подкачки — Pagefile.sys.

Ближе к реальности В отличие от предыдущих версий, в Windows 7 значительно усовершенствован процесс автоматического управления виртуальной памятью. Обычно объем виртуальной памяти в Windows 7 равен или превышает объем всей физической памяти компьютера. Это нужно, чтобы уменьшить фрагментацию файла подкачки, следствием которой может стать снижение производительности системы. Определяя размер файла подкачки вручную, сделайте его больше общего объема физической памяти, чтобы уменьшить фрагментацию. Для компьютеров с объемом ОЗУ до 4 Гб максимальный объем файла должен быть больше объема ОЗУ в два или более раз. Для компьютеров с объемом ОЗУ более 4 Гб максимальный объем должен в полтора и более раз превышать объем ОЗУ. Тем самым вы обеспечите непрерывность файла подкачки и записываемых в него блоков (при наличии достаточного места на диске).

Чтобы вручную настроить виртуальную память, выполните следующие действия:

1. Откройте панель управления, щелкните **Система и безопасность (System And Security)** и щелкните **Система (System)**.
2. В консоли Система (System) щелкните **Изменить параметры (Change Settings)** или **Дополнительные параметры системы (Advanced System Settings)**.
3. В диалоговом окне **Свойства системы (System Properties)** перейдите на вкладку **Дополнительно (Advanced)**.
4. Щелкните кнопку **Параметры (Settings)** в разделе **Быстродействие (Performance)**.
5. На вкладке **Дополнительно (Advanced)** диалогового окна **Параметры быстродействия (Performance Options)** щелкните кнопку **Изменить (Change)**. В открывшемся диалоговом окне **Виртуальная память (Virtual Memory)** приводятся следующие сведения (рис. 6-18):
   - **Диск [Метка тома] (Drive [Volume Label])** и **Файл подкачки (Мб) (Paging File Size)** Текущая конфигурация виртуальной памяти в системе. Каждому тому в списке соответствует файл подкачки (если он есть). Указаны также исходный и максимальный размеры файла подкачки.
   - **Размер файла подкачки для каждого диска (Paging File Size For Each Drive)** Здесь представлены сведения о текущем выбранном диске. Также вы можете задать размер файла подкачки. В строке **Свободно (Space Available)** указан доступный объем места на диске.

- **Общий объем файла подкачки на всех дисках (Total Paging File Size For All Drives)** Сведения о рекомендуемом и текущем объеме виртуальной памяти в системе. Обратите внимание, что здесь указан рекомендуемый объем для системного диска. Чтобы использовать это значение, установите переключатель **Размер по выбору системы (System Managed Size)**.

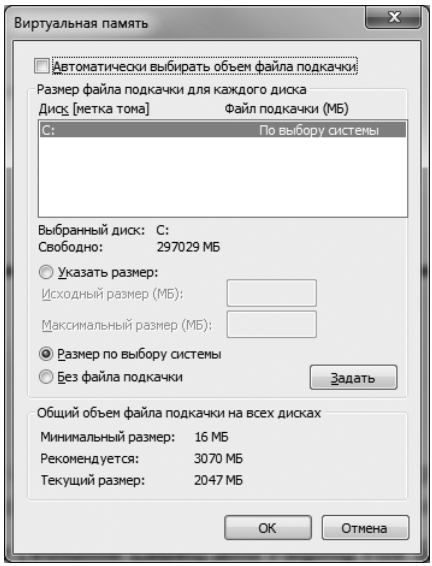

Рис. 6-18. Объем виртуальной памяти превышает объем физической памяти (ОЗУ) системы

6. По умолчанию размеры файлов подкачки на всех дисках задаются Windows 7. Чтобы настроить виртуальную память вручную, сбросьте флажок **Автоматически выбирать объем файла подкачки (Automatically Manage Paging File Size For All Drives)**.
7. В списке **Диск (Drive)** выберите том для конфигурирования.
8. Щелкните **Указать размер (Custom Size)**, затем введите исходный и максимальный размеры.
9. Чтобы сохранить изменения, щелкните **Задать (Set)**.
10. Повторите шаги 7–9 для каждого из настраиваемых томов.
11. Щелкните **OK**. Если система предложит перезаписать существующий файл Pagefile.sys, щелкните **Да (Yes)**.
12. После обновления файла подкачки, используемого в данный момент, будет выведено сообщение о том, что для применения изменений необходимо перезагрузить систему. Щелкните **OK**.
13. Дважды щелкните **OK**, чтобы закрыть открытые диалоговые окна. Закрывая окно утилиты Система (System), вы увидите сообщение о том, что внесенные изменения будут применены после перезагрузки компьютера.

Чтобы настроить автоматическое управление виртуальной памятью в Windows 7, выполните следующие действия:

1. В диалоговом окне **Свойства системы (System Properties)** перейдите на вкладку **Дополнительно (Advanced)**.
2. В разделе **Быстродействие (Performance)** щелкните кнопку **Параметры (Settings)**.
3. На вкладке **Дополнительно (Advanced)** диалогового окна **Параметры быстродействия (Performance Options)** щелкните кнопку **Изменить (Change)**.
4. В открывшемся диалоговом окне **Виртуальная память (Virtual Memory)** установите флажок **Автоматически выбирать объем файла подкачки (Automatically Manage Paging File Size For All Drives)**.
5. Щелкните **OK** три раза, чтобы закрыть открытые диалоговые окна.

Совет В целях безопасности рекомендуется очищать файл подкачки при завершении работы компьютера. Для этого нужно включить политику **Завершение работы: очистка файла подкачки виртуальной памяти (Shutdown: Clear Virtual Memory Pagefile)**. Вы найдете его в папке **Локальные политики\Параметры безопасности (Local Policies\Security Options)**.

Настройка DEP

Технология предотвращения выполнения данных (Data Execution Prevention, DEP) предназначена для защиты памяти. При использовании DEP все адреса памяти в приложении отмечаются процессором, как неисполняемые, за исключением адресов, содержащих явный исполняемый код. Если производится попытка выполнить код из страницы памяти, отмеченной как неисполняемая, процессор вызывает исключение и предотвращает выполнение кода. Это позволяет избежать внедрения постороннего кода, например вируса, в большую часть областей памяти.

Примечание В 32-разрядных версиях Windows поддерживается технология DEP, реализованная в процессорах AMD с функцией NX (No eXecute). Такие процессоры работать в режиме расширения физических адресов (PAE), чтобы поддерживать большие объемы памяти. В 64-разрядных версиях Windows функция процессора NX также поддерживается, однако режим PAE для работы с большими объемами памяти не нужен.

Для совместимости с DEP приложение должно «уметь» явно отмечать области памяти разрешением на запуск. Программы, неспособные это делать, несовместимы с функцией процессора NX. Если во время работы приложений возникают проблемы, связанные с памятью, найдите сбойные программы и внесите их в список исключений, не отключая функцию DEP. Таким образом, у вас останется защита памяти, которая будет отключена для программ, не поддерживающих функцию процессора NX.

Технология DEP применяется к программам, работающим как в режиме пользователя, так в режиме ядра. В режиме пользователя попытка выполнения данных приводит к исключению STATUS_ACCESS_VIOLATION.

В большинстве процессов такое исключение не обрабатывается и приводит к завершению процесса. И такое поведение правильно: программы редко нарушают правила с дружественными намерениями, в основном, это вирусы и черви.

Защиту от выполнения данных для драйверов, работающих в режиме ядра, нельзя выборочно включать или отключать, в отличие от защиты приложений. Более того, в совместимых 32-разрядных системах защита от выполнения данных применяется к стеку по умолчанию. В совместимых 64-разрядных системах защита по умолчанию применяется к стеку, выгружаемому пулу и пулу сеанса. В режиме ядра для драйвера устройства нарушение доступа к памяти вызывает исключение ATTEMPTED_EXECUTE_OF_NOEXECUTE_MEMORY.

Узнать, поддерживает ли ваш компьютер технологию DEP, позволяет утилита Система (System). Если компьютер поддерживает DEP, для ее настройки выполните следующие действия:

1. Откройте панель управления, щелкните **Система и безопасность (System And Security)** и щелкните **Система (System)**.
2. В консоли Система (System) щелкните **Изменить параметры (Change Settings)** или **Дополнительные параметры системы (Advanced System Settings)**.
3. В диалоговом окне **Свойства системы (System Properties)** перейдите на вкладку **Дополнительно (Advanced)**. Щелкните **Параметры (Settings)** в разделе **Быстродействие (Performance)**.
4. В открывшемся диалоговом окне **Параметры быстродействия (Performance Options)** перейдите на вкладку **Предотвращение выполнения данных (Data Execution Prevention)**. В нижней части вкладки вы найдете ответ на вопрос о поддержке технологии DEP вашим компьютером.
5. Если компьютер поддерживает DEP и правильно настроен, к вашим услугам следующие возможности настройки DEP:
   - **Включить DEP только для основных программ и служб Windows (Turn On DEP For Essential Windows Programs And Services Only)** Включение технологии DEP только для служб, программ и компонентов ОС. Этот вариант выбран по умолчанию.
   - **Включить DEP для всех программ и служб кроме выбранных ниже (Turn On DEP For All Programs Except Those I Select)** Настройка DEP с возможностью исключений. Выберите этот параметр и щелкните **Добавить (Add)**, чтобы задать программы, которые следует запускать без защиты от выполнения данных. Таким образом, защита будет работать для всех программ, кроме тех, которые указали вы.
6. Щелкните **OK**.

Настройка системных и пользовательских переменных среды

Чтобы настроить системные и пользовательские переменные среды, в диалоговом окне **Свойства системы (System Properties)** перейдите на вкладку **Дополнительно (Advanced)** и щелкните кнопку **Переменные среды (Environment Variables)**, чтобы открыть диалоговое окно **Переменные среды (Environment Variables)**, показанное на рис. 6-19.

Примечание Созданные или измененные вами системные переменные среды вступят в силу после перезагрузки компьютера. Созданные или измененные переменные среды пользователя будут применены при следующем входе пользователя в систему.

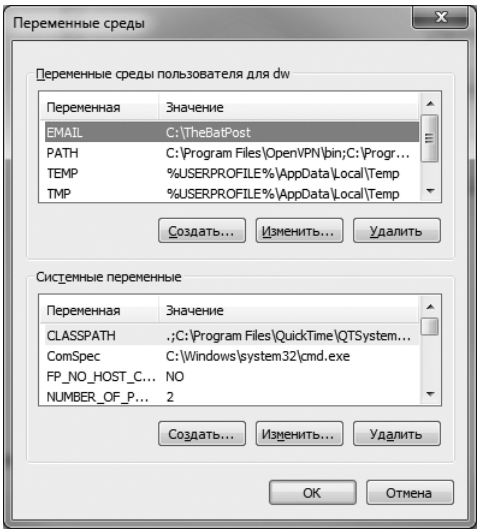

Рис. 6-19. Настройка системных и пользовательских переменных в диалоговом окне

Создание переменной среды

Чтобы создать переменную среды, выполните следующие действия:

1. В разделе **Переменные среды пользователя (User Variables)** или **Системные переменные (System Variables)** щелкните кнопку **Создать (New)**.
2. В открывшемся диалоговом окне **Новая пользовательская переменная (New User Variable)** или **Новая системная переменная (New System Variable)**, соответственно, введите имя переменной в поле **Имя переменной (Variable Name)**. В поле **Значение переменной (Variable Value)** введите значение переменной. Щелкните **OK**.

Ближе к реальности Пути к исполняемым файлам заданы в переменной PATH. Редактирование этой переменной описано в главе 9.

Чтобы создать переменную среды на компьютерах домена, используйте групповую политику и элемент предпочтения:

1. В оснастке Редактор управления групповыми политиками (Group Policy Management Editor) откройте объект GPO для редактирования. Чтобы

настроить предпочтения для компьютеров, разверните узел **Конфигурация компьютера\Настройки\Конфигурация Windows (Computer Configuration\Preferences\Windows Settings)**. Чтобы настроить предпочтения для пользователей, разверните узел **Конфигурация пользователя\Настройки\Конфигурация Windows (User Configuration\Preferences\Windows Settings)**.

2. Щелкните правой кнопкой узел **Среда (Environment)**, выберите команду **Создать (New)** и щелкните **Переменные среды (Environment Variable)**.
3. В открывшемся диалоговом окне **Новые свойства среды (New Environment Properties)**, в списке **Действия (Action)** выберите вариант **Создать (Create)**. Затем укажите, какую переменную среды нужно создать: **Пользовательская переменная (User Variable)** или **Системная переменная (System Variable)**.
4. В поле **Имя (Name)** введите имя переменной. В поле **Значение (Value)** введите значение переменной.
5. При помощи параметров на вкладке **Общие параметры (Common)** задайте методы применения переменной. Как правило, новая переменная создается только один раз. В этом случае щелкните **Применить один раз и не применять повторно (Apply Once And Do Not Reapply)**.
6. Щелкните **OK**. Во время следующего обновления политики элемент предпочтения будет применен к объекту GPO, в котором вы его определили.

Редактирование переменной среды

Чтобы отредактировать переменную среды, выполните следующие действия:

1. Выберите переменную в списке **Переменные среды пользователя (User Variables)** или **Системные переменные (System Variables)**.
2. Щелкните кнопку **Изменить (Edit)** в разделе **Переменные среды пользователя (User Variables)** или **Системные переменные (System Variables)**.
3. В открывшемся диалоговом окне **Изменение пользовательской переменной (Edit User Variable)** или **Изменение системной переменной (Edit System Variable)** введите новое значение в поле **Значение переменной (Variable Value)** и щелкните **OK**.

Чтобы обновить переменную среды на компьютерах домена, используйте групповую политику и элемент предпочтения:

1. В оснастке Редактор управления групповыми политиками (Group Policy Management Editor) откройте объект GPO для редактирования. Чтобы редактировать предпочтения для компьютеров, разверните узел **Конфигурация компьютера\Настройки\Конфигурация Windows (Computer Configuration\Preferences\Windows Settings)**. Чтобы редактировать предпочтения для пользователей, разверните узел **Конфигурация пользователя\Настройки\Конфигурация Windows (User Configuration\Preferences\Windows Settings)**.

2. Щелкните правой кнопкой узел **Среда (Environment)**, выберите команду **Создать (New)** и щелкните **Переменные среды (Environment Variable)**.
3. В открывшемся диалоговом окне **Новые свойства среды (New Environment Properties)** выберите в списке **Действия (Action)** вариант **Обновить (Update)**, чтобы обновить переменную, или **Заменить (Replace)**, чтобы удалить и заново создать переменную. Затем укажите, какую переменную среды нужно создать: **Пользовательская переменная (User Variable)** или **Системная переменная (System Variable)**.
4. В поле **Имя (Name)** введите имя обновляемой переменной. В поле **Значение (Value)** введите значение переменной.
5. При помощи параметров вкладки **Общие параметры (Common)** задайте методы применения переменной. Как правило, новая переменная создается только один раз, поэтому щелкните **Применить один раз и не применять повторно (Apply Once And Do Not Reapply)**.
6. Щелкните **OK**. Во время следующего обновления политики элемент предпочтения будет применен к объекту GPO, в котором вы его определили.

Удаление переменной среды

Чтобы удалить переменную среды, выделите ее и нажмите Del. Чтобы удалить переменную среды на компьютерах домена при помощи групповой политики, выполните следующие действия:

1. В оснастке Редактор управления групповыми политиками (Group Policy Management Editor) откройте объект GPO для редактирования. Чтобы настроить предпочтения для компьютеров, разверните узел **Конфигурация компьютера\Настройки\Конфигурация Windows (Computer Configuration\Preferences\Windows Settings)**. Чтобы настроить предпочтения для пользователей, разверните узел **Конфигурация пользователя\Настройки\Конфигурация Windows (User Configuration\Preferences\Windows Settings**.
2. Выполните одно из следующих действий:
   - Если элемент предпочтения для переменной уже существует, дважды щелкните имя переменной, чтобы открыть соответствующее диалоговое окно **Свойства (Properties)**. В списке **Действия (Action)** выберите команду **Удалить (Delete)**. На вкладке **Общие параметры (Common)** задайте необходимые параметры, например **Применить один раз и не применять повторно (Apply Once And Do Not Reapply)**, и щелкните **OK**.
   - Если элемента предпочтения для переменной не существует, создайте его, как было описано ранее. В списке **Действия (Action)** выберите команду **Удалить (Delete)** и задайте необходимые параметры на вкладке **Общие параметры (Common)**.

Настройка загрузки и восстановления системы

Свойства загрузки и восстановления настраиваются в диалоговом окне **Загрузка и восстановление (Startup And Recovery)**, показанном на рис. 6-20. Чтобы открыть его, в диалоговом окне **Свойства системы (System Properties)** перейдите на вкладку **Дополнительно (Advanced)** и на панели **Загрузка и восстановление (Startup And Recovery)** щелкните кнопку **Параметры (Settings)**.

Настройка параметров загрузки

В диалоговом окне **Загрузка и восстановление (Startup And Recovery)** параметры загрузки настраиваются в области **Загрузка операционной системы (System Startup)**. Чтобы на компьютере с несколькими операционными системами установить ОС, загружаемую по умолчанию, ее в списке **Операционная система, загружаемая по умолчанию (Default Operating System)**. Параметры загрузки записываются в параметры конфигурации Диспетчера загрузки Windows (Windows Boot Manager).

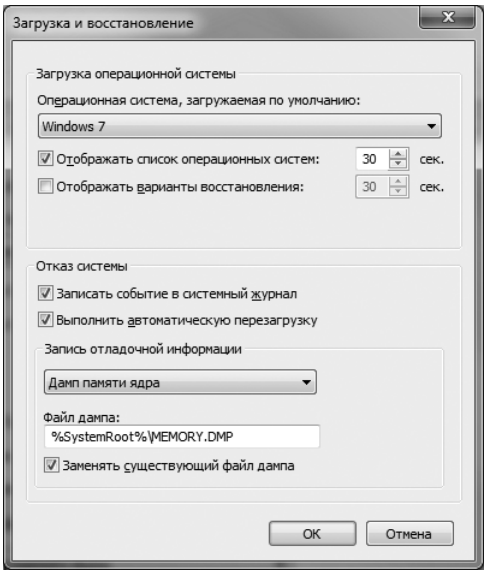

Рис. 6-20. Настройка загрузки и восстановления системы в диалоговом окне Загрузка и восстановление (Startup And Recovery)

По умолчанию во время загрузки компьютера, на котором установлено несколько ОС, в течение 30 секунд отображается меню конфигурации загрузки. Вот как можно управлять его поведением:

- Для немедленной загрузки ОС по умолчанию сбросьте флажок **Отображать список операционных систем (Time To Display List Of Operating Systems)**.
- Для вывода имеющихся вариантов в течение указанного времени установите флажок **Отображать список операционных систем (Time To Display List Of Operating Systems)** и укажите время задержки в секундах.

Обычно в большинстве систем задается задержка от 3 до 5 сек. Этого достаточно для принятия пользователем решения и не затягивает процесс загрузки.

В режиме восстановления во время загрузки системы также можно просматривать параметры восстановления. По аналогии с вариантами загрузки, есть два способа настройки вариантов восстановления. Для немедленной загрузки компьютера с вариантом восстановления по умолчанию сбросьте флажок **Отображать варианты восстановления (Time To Display Recovery Options When Needed)**. А для вывода на экран имеющихся вариантов в течение указанного времени установите флажок **Отображать варианты восстановления (Time To Display Recovery Options When Needed)** и задайте время отображения в секундах.

Настройка параметров восстановления

В диалоговом окне **Загрузка и восстановление (Startup And Recovery)** параметры восстановления системы задаются в областях **Отказ системы (System Failure)** и **Запись отладочной информации (Write Debugging Information)**. Параметры восстановления позволяют администратору точно регулировать процессы, происходящие в системе при возникновении фатальной ошибки (STOP-ошибки). Доступные параметры области **Отказ системы (System Failure)** таковы:

- **Записать событие в системный журнал (Write An Event To The System Log)** Запись ошибки в журнал событий системы. Это позволяет в дальнейшем просмотреть сведения об ошибке в консоли Просмотр событий (Event Viewer).
- **Выполнить автоматическую перезагрузку (Automatically Restart)** Перезагрузка системы в случае возникновения фатальной ошибки.

Примечание Автоматическая перезагрузка — не такой уж беспроигрышный вариант. Иногда лучше остановить систему, чем перезагружать ее: это скорее привлечет внимание. Иначе вы рискуете узнать о том, что система была перезагружена, только после просмотра системных журналов или если случайно окажетесь рядом в момент перезагрузки.

Выбор типа отладочных сведений, которые будут записаны в файл дампа, можно сделать при помощи меню **Запись отладочной информации (Write Debugging Information)**. Файл дампа, в свою очередь, пригодится при диагностике системных сбоев. Варианты файла дампа:

- **Нет (None)** Отладочная информация записана не будет.
- **Малый дамп памяти (Small Memory Dump)** В дамп будет выгружен сегмент физической памяти, в котором произошла ошибка. Размер малого дампа составляет 256 Кб.
- **Дамп памяти ядра (Kernel Memory Dump)** В дамп будет выгружена область физической памяти, используемая ядром Windows. Размер дампа зависит от размера ядра Windows.

Для записи файла дампа необходимо указать его расположение. Стандартные расположения таковы: %SystemRoot%\Minidump для малых дампов и %SystemRoot%\Memory.dmp для остальных дампов памяти. При необходимости включите параметр **Заменять существующий файл дампа (Overwrite Any Existing File)**. Это обеспечит перезапись существующих файлов дампа в случае возникновения новой STOP-ошибки.

Ближе к реальности Файл дампа записывается только при правильной настройке системы. На системном диске должен быть достаточно большой файл подкачки (его размер настраивается на вкладке **Дополнительно (Advanced)**), а сам диск должен обладать достаточным объемом свободного места. Для файла дампа памяти ядра необходимо пространство, равное 35-50% объема ОЗУ. Например, в моей системе, где объем ОЗУ равен 4096 Мб, для корректного создания дампа ядра с отладочной информацией необходимо иметь 2048 Мб свободного места.

Вкладка Защита системы (System Protection)

На вкладке **Защита системы (System Protection)** диалогового окна **Свойства системы (System Properties)** содержатся параметры для настройки программы Восстановление системы (System Restore). В Windows 7 в состав программы Восстановление системы (System Restore) входит компонент Предыдущие версии (Previous Versions). В следующих разделах мы поговорим о способах настройки программы Восстановление системы (System Restore) и о работе с ней. Восстановление компьютера из контрольных точек описано в главе 17.

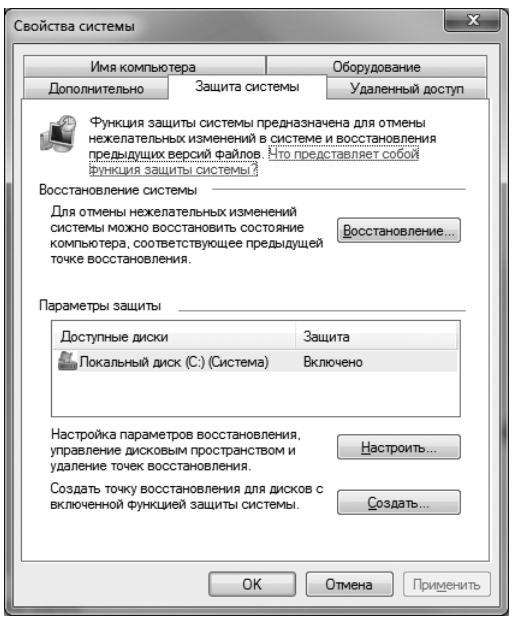

Рис. 6-21. Управление точками восстановления системы

Восстановление системы и предыдущие версии

При включенной функции восстановления системы на компьютере периодически создаются снимки конфигурации системы и (или) предыдущих версий файлов. Такие снимки называются точками восстановления (restore point). К числу отслеживаемых параметров системы относятся параметры Windows и списки установленных программ. Если компьютер не загружается или работает неправильно из-за изменений, внесенных в конфигурацию, вы можете восстановить конфигурацию системы до состояния на момент создания снимка. Допустим, система работала нормально, пока вы не установили новый пакет исправлений для Microsoft Office. После этого компьютер начал генерировать ошибки, а программы пакета Office перестали работать. Вы пытались установить обновления, но это не помогло. Правильное решение в этой ситуации — запустить программу Восстановление системы (System Restore). Она позволяет восстанавливать систему по снимку, сделанному перед установкой обновления.

Примечание В программе Восстановление системы (System Restore) можно создавать точки восстановления нескольких типов. Один из них, системная точка восстановления (System Checkpoint), создается ОС по расписанию через регулярные интервалы времени. Другой тип, точка восстановления установки (Installation Restore Point), создается автоматически на основе событий, генерируемых ОС во время установки приложений. Снимки, известные под названием точек восстановления пользователя (Manual Restore Point), создаются пользователями. Рекомендуйте пользователям перед выполнением потенциально опасных для системы действий создавать пользовательские точки восстановления.

Программа Восстановление системы (System Restore) предназначена для управления точками восстановления отдельного для каждого диска. Изменения конфигурации необходимо отслеживать на всех дисках с критически важными приложениями и системными файлами. По умолчанию функция Восстановление системы (System Restore) включена только для системного диска. Но вы вольны установить наблюдение и за другими дисками. Если в программе Восстановление системы (System Restore) не задан мониторинг диска, изменения конфигурации диска не отслеживаются и восстановить диск будет невозможно.

В Windows 7 предыдущие версии файлов и папок создаются автоматически, в составе точки восстановления. Все файлы и папки, измененные после создания точки восстановления, сохраняются и могут быть восстановлены. Единственным исключением являются системные файлы и папки. Предыдущие версии системных папок, например C:\Windows, восстановить нельзя.

Предыдущие версии позволяют восстановить файлы, которые вы случайно изменили, удалили или повредили. Если на диске включена функция Восстановление системы (System Restore), ежедневно выполняется резервное копирование измененных файлов и папок на этом диске. Вы также можете создать копии измененных файлов и папок в точке восстановления при помощи функций вкладки Защита системы (System Protection).

Примечание Точки защиты создаются ежедневно для каждого диска, наблюдение за которым ведется в программе Восстановление системы (System Restore). Однако при этом в качестве предыдущих версий сохраняются только те версии файлов, которые действительно отличаются от текущей версии. Чтобы включить (отключить) создание предыдущих версий для диска, нужно включить (отключить) функцию Восстановление системы (System Restore) для этого диска. Предыдущие версии сохраняются в составе точек восстановления тома, создаваемых вручную или автоматически.

Настройка восстановления системы

Параметры восстановлением системы задаются на вкладке **Защита системы (System Restore)** диалогового окна **Свойства системы (System Properties)**. За мониторинг изменений конфигурации и приложений отвечает Служба восстановления системы (System Restore Service). Она запускается автоматически от имени учетной записи Локальная система (LocalSystem). Если служба остановлена или не настроена, программа Восстановление системы (System Restore) будет работать неправильно.

В программе Восстановление системы (System Restore) сохраняется информация обо всех системных точках восстановления. Для этого на системном томе должно быть не менее 300 Мб свободного места. При необходимости для нужд восстановления системы автоматически резервируется дополнительное пространство вплоть до 100% общего объема диска, но это дополнительное пространство доступно для пользователей и приложений. При необходимости вы вольны освободить дополнительное пространство, используемое программой Восстановление системы (System Restore). Если для работы программы не хватает места, ранее созданные точки восстановления перезаписываются новыми.

Вы вольны регулировать объем дискового пространства, занимаемый программой Восстановление системы (System Restore). По умолчанию для хранения точек восстановления резервируется не менее 1% от общего объема диска. В частности, на жестком диске общим объемом 930 Гб резерв программы по умолчанию составит 9,3 Гб.

Чтобы настроить функцию Восстановление системы (System Restore) для каждого диска, выполните следующие действия:

1. Откройте панель управления, щелкните **Система и безопасность (System And Security)** и **Система (System)**.
2. В левой панели консоли Система (System) щелкните **Защита системы (System Protection)**.
3. Чтобы задать параметры восстановления для тома, выберите том в списке **Параметры защиты (Protection Settings)** и щелкните **Настроить (Configure)**. Откроется диалоговое окно **Защита системы для (System Protection For)**, показанное на рис. 6-22.

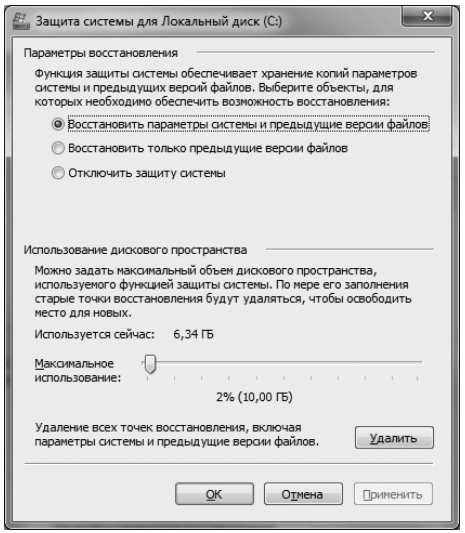

Рис. 6-22. Настройка программ Восстановление системы (System Restore) для диска

4. Выберите один из следующих вариантов:
   - **Восстановить параметры системы и предыдущие версии файлов (Restore System Settings And Previous Versions Of Files)** Сохранение копий системных параметров и предыдущих версий файлов. Рекомендуется для системного тома и позволяет восстановить компьютер и предыдущие версии файлов с данными.
   - **Восстановить только предыдущие версии файлов (Only Restore Previous Versions Of Files)** Сохранение только предыдущих версий файлов; параметры системы не сохраняются. Рекомендуется для томов, на которых нет данных системы, и позволяет восстанавливать предыдущие версии файлов с данными.
   - **Отключить защиту системы (Turn Off System Protection)** Отключение программы Восстановление системы (System Restore). Не рекомендуется, так как при этом нет возможности восстановления компьютера или предыдущих версий файлов.
5. Укажите при помощи бегунка **Максимальное использование (Disk Space Usage)** наибольший объем дискового пространства, доступный программе Восстановление системы (System Restore). При заполнении отведенного объема, старые точки восстановления будут удалены, а на их место будут записаны новые.
6. Щелкните **OK**. Если вы отключили защиту системы, вам придется подтвердить действие щелчком кнопки **Да (Yes)**. После этого будут удалены все сохраненные параметры системы и предыдущие версии файлов. Когда удаление всех точек восстановления будет завершено, щелкните **Закрыть (Close)**.

Если программа Восстановление системы (System Restore) используется для защиты компьютера, и вы абсолютно уверены в стабильности системы, удалите все сохраненные параметры системы и предыдущие версии файлов. При этом вы освободите место на дисках и исключите возможность применения пользователями одной из точек восстановления. Для этого выполните следующие действия:

1. Откройте панель управления, щелкните **Система и безопасность (System And Security)** и **Система (System)**.
2. В левой панели консоли Система (System) щелкните **Защита системы (System Protection)**.
3. В списке **Параметры защиты (Protection Settings)** выберите нужный том и щелкните **Настроить (Configure)**.
4. Щелкните **Удалить (Delete)**. Подтвердите удаление сохраненных параметров системы и предыдущих версий файлов, щелкнув **Продолжить (Continue)**. Когда данные всех точек восстановления будут удалены, щелкните **Закрыть (Close)**.

Восстановление предыдущих версий

Щелкните правой кнопкой файл или папку в программе Проводник Windows (Windows Explorer), выберите команду **Свойства (Properties)** и перейдите на вкладку **Предыдущие версии (Previous Versions)**. Здесь перечислены предыдущие версии файла или папки, если они имеются. Выделите предыдущую версию, затем щелкните кнопку:

- **Открыть (Open)** — открытие любой предыдущей версии;
- **Копировать (Copy)** — создание копии предыдущей версии;
- **Восстановить (Restore)** — возврат к выделенной предыдущей версии файла или папки.

Есть несколько причин отсутствия на компьютере предыдущих версий файла:

- Программа Восстановление системы (System Restore) для данного диска отключена. Если восстановление системы для тома отключено, предыдущие версии создаваться не будут.
- Вы пытаетесь восстановить автономный файл. Автономные файлы — это копии сетевых файлов. На клиентских компьютерах предыдущие версии автономных файлов не создаются. Предыдущие версии могут быть на сервере, где хранятся оригиналы.
- Вы пытаетесь восстановить системный файл. Предыдущие версии системных файлов не создаются. Изменения, вносимые в системные файлы, отслеживаются в точках восстановления. Для возврата компьютера в предыдущее состояние необходимо восстановить его из точки восстановления.
- Папка, в которой хранился файл, удалена. Откройте окно свойств папки, в которой находилась удаленная папка. На вкладке **Предыдущие версии**

(Previous Versions) восстановите папку, затем откройте ее, чтобы восстановить предыдущую версию искомого файла.

- Со времени создания и сохранения файла не было создано точки восстановления.

Вкладка Удаленное использование (Remote)

В диалоговом окне **Свойства системы (System Properties)** на вкладке **Удаленное использование (Remote)** располагаются параметры приглашений удаленного помощника и параметры подключений удаленного рабочего стола. Описание этих параметров вы найдете в разделе «Управление удаленным доступом к рабочим станциям» главы 5.

Настройка параметров электропитания

Параметры электропитания определяют потребление компьютером энергии в различных ситуациях, скажем, при питании от батарей или сети. Параметры электропитания позволяют экономить энергию на любом компьютере, а на ноутбуках это еще и способ достичь баланса производительности и энергопотребления. Иногда можно понизить быстродействие ноутбука и его общую производительность ради увеличения времени работы аккумулятора. Это позволит пользователю дольше проработать без доступа к розетке. В других случаях необходимо обеспечить среднюю производительность и среднее время работы от батареи или максимально поднять производительность без оглядки на аккумулятор.

Основные свойства управления электропитанием собраны в *планах электропитания* (power plan). Как и схемы электропитания, применявшиеся в Windows XP и более ранних версиях Windows, план электропитания представляет собой набор параметров, регулирующих потребление энергии. На компьютере может быть несколько планов электропитания, но только один из них активен в данный момент. Помимо планов электропитания на большинстве компьютеров определено действие при нажатии на кнопку питания или кнопку сна, а на ноутбуках определено также действие, выполняемое при закрытии крышки. Обычно при закрытии крышки компьютер переходит в спящий режим, продолжительное нажатие на кнопку питания приводит к завершению работы компьютера, а нажатие на кнопку сна переводит компьютер в спящий режим.

Управление параметрами электропитания из командной строки

В Windows 7 для управления параметрами электропитания из командной строки предназначена утилита Powercfg.exe (Power Configuration). Чтобы просмотреть список ее параметров, введите в командной строке **powercfg /?**. Наиболее часто используются следующие параметры:

- **-a** Список доступных состояний спящего режима с пояснениями, почему некоторые состояния не поддерживаются.

- **–d [guid]** Удаление плана электропитания, указанного глобально уникальным идентификатором GUID.
- **–devicequery all_devices_verbose** Вывод списка устройств компьютера с подробными сведениями об электропитании. Не забудьте перенаправить вывод команды в файл — он будет длинный и подробный.
- **–energy** Проверка системы на наличие типичных проблем, связанных с конфигурацией, устройствами и батареей. В результате проверки в текущей рабочей папке создается отчет в формате HTML.
- **–h** Включение и отключение режима гибернации.
- **–l** Вывод списка планов электропитания компьютера по имени и GUID.
- **–q [guid]** Вывод списка элементов плана электропитания, указанных идентификаторами GUID. Если GUID не указан, будут перечислены элементы активного плана электропитания.
- **–requests** Вывод всех запросов питания драйверов устройств. При наличии отложенных запросов для любого устройства, включая монитор, компьютер не сможет автоматически перейти в режим пониженного энергопотребления. Например, наличие отложенных запросов для монитора помешает компьютеру автоматически выключить его.
- **–s [guid]** Активация плана электропитания, указанного GUID.
- **–x [параметры] [значение]** Задание значения для параметра активного плана электропитания.

Примечание По умолчанию на компьютерах под управлением Windows 7 вместо режима гибернации используется гибридный спящий режим. Перед настройкой режима гибернации обязательно проверьте совместимость.

Далее приведен пример вывода команды **powercfg –l**:

```
Существующие схемы управления питанием (* - активные)
---------------------------------
GUID схемы питания: 381b4222-f694-41f0-9685-ff5bb260df2e (Сбалансированный)
GUID схемы питания: 8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c (Высокая
производительность)
GUID схемы питания: a1841308-3541-4fab-bc81-f71556f20b4a (Экономия энергии)
GUID схемы электропитания: c1d97820-3148-42a9-a587-
75d618a9bb2b (Graphics Dept) *
```

Активный план отмечен звездочкой. Из листинга следует, что на компьютере имеется четыре плана электропитания, причем активен пользовательский план Graphics Dept.

Настройка плана электропитания или изменение параметров плана при помощи утилиты Powercfg выполняются в командной строке с повышенными полномочиями. Если для параметра требуется ввод GUID, введите в командной строке с повышенными полномочиями команду **powercfg –l**, затем скопируйте нужное значение GUID в соответствующий план. Например, чтобы сделать план Сбалансированный (Balanced) планом по умолчанию

для компьютера из предыдущего примера, введите в командной строке с повышенными полномочиями:

```
powercfg -s 381b4222-f694-41f0-9685-ff5bb260df2e
```

Чтобы определить поддерживаемые компьютером режимы питания, введите в командной строке **powercfg –a**. На выходе будет дан список поддерживаемых и не поддерживаемых режимов.

```
В данной системе доступны следующие состояния спящего режима: Ждущий режим
(S1 S3)
Гибернация Гибридный спящий режим
Следующие состояния спящего режима недоступны в данной системе: Ждущий режим (S2)
Системные микропрограммы не поддерживают ждущий режим.
```

Команда **powercfg –a** полезна для диагностики неисправностей, возникающих при переходе в режим сна или гибернации. Если режим не поддерживается микропрограммами, иногда (очень редко) можно исправить проблему, обновив прошивку. Если причиной неполадки стало устройство, которое не поддерживает определенный режим, замените устройство на совместимое.

Если вам нужно оценить параметры конфигурации электропитания и совместимость устройств компьютера, создайте диагностический отчет об эффективности энергопотребления. Для этого в командной строке введите команду **powercfg –energy**. Она создает отчет в формате HTML с названием Energy-Report.html. В отчете вы найдете результаты проверки совместимости управления электропитанием с устройствами. Все устройства, не поддерживающие полностью управление электропитанием, заносятся в список ошибок. Например, если устройство с интерфейсом USB не может быть корректно остановлено, в отчете будет подробное описание конфигурации устройства и возникающих ошибок. Вы узнаете, была ли из-за несовместимости отключена возможность управления питанием. Например, если функция PCI Express Active-State Power Management не поддерживается оборудованием и поэтому отключена, это будет отражено в отчете. Кроме того, в отчете содержатся предупреждения и дополнительные сведения об устройствах и совместимости, включая информацию о поддерживаемых состояниях спящего режима и вариантах питания процессора.

Ближе к реальности Для владельцев ноутбуков важна информация о зарядке и времени работы батареи. Если ресурс батареи подходит к концу, вы узнаете, что она уже не держит заряд должным образом. Такую батарею лучше заменить.

Еще более детальные сведения о неполадках питания вы найдете в информации о поддержке электропитания для каждого устройства. Введите команду:

```
powercfg -devicequery all_devices_verbose > power.txt
```

где Power.txt — имя файла в текущей папке.

Настроив оболочку Windows PowerShell для удаленной работы, вы легко сможете выполнять команду *Powercfg* на удаленных компьютерах. Введите имя проверяемого компьютера в отдельной строке файла Computers.txt и сохраните файл. Затем откройте командную строку PowerShell с повышенными полномочиями и введите следующие команды:

```
$comp = get-content c:\computers.txt
$s = new-pssession -computername $comp
invoke-command -session $s { powercfg.exe -energy }
```

Здесь C:\Computers.txt — путь к файлу Computers.txt. Укажите путь, соответствующий нужному месту хранения файла. Файл Energy-Report.html будет создан на каждом компьютере в папке по умолчанию учетной записи, при помощи которой вы обратились к компьютеру. Чтобы не извлекать документ HTML на каждом компьютере, запишите отчет на общий ресурс, назвав его именем компьютера, как показано в примере:

```
$comp = get-content c:\computers.txt
$s = new-pssession -computername $comp
invoke-command -session $s { powercfg.exe -energy -output
«\\fileserver46\data\$env:computername.html»}
```

Здесь отчет записывается на общий ресурс *\\fileserver46\data*, имя файла взято из значения переменной среды *ComputerName*. Помните, что когда вы работаете с PowerShell и ссылаетесь на команды, содержащие исполняемые объекты, вместе с именем программы следует указывать расширение .exe.

Планы электропитания

На панели задач в ноутбуках и планшетных ПК есть значок **Электропитание (Power)**. При наведении на него указателя мыши отображается состояние заряда батареи и используемый план электропитания. Если щелкнуть значок **Электропитание (Power)** правой кнопкой, откроется контекстное меню с командой для быстрого доступа к утилите Электропитание (Power Options). С Windows 7 поставляется три плана электропитания:

- **Сбалансированный (Balanced)** План, в котором соблюдается баланс между потреблением энергии и производительностью системы. Работа процессора ускоряется, когда используется больше ресурсов, и замедляется, когда используется меньше ресурсов. Этот план электропитания используется по умолчанию. Он подходит для пользователей, умеренно использующих графику, например работающих в Microsoft Office Power Point.
- **Высокая производительность (High Performance)** План с высоким потреблением энергии, при котором производительность компьютера повышается за счет времени работы от батареи. Питания хватает для работы с графически интенсивными программами или играми. Применяйте этот план, если вам важнее всего быстродействие, если пользователи

работают с приложениями, требующими высокой графической производительности, или выполняют сложные вычисления.

- **Экономия энергии (Power Saver)** Экономичный план с низким энергопотреблением. Процессор работает медленнее, а время работы от батареи максимально увеличивается. План подходит пользователям, работающим, в основном, с графически нейтральными приложениями, например Microsoft Word и Microsoft Outlook.

Параметры плана электропитания разделяются на две основные категории: базовые и дополнительные. Базовые параметры определяют время, через которое отключаются монитор и сам компьютер. По умолчанию в Windows 7 в плане Сбалансированный (Balanced) монитор отключается через 10 мин, а компьютер переходит в спящий режим через 30 мин простоя. В плане Экономия энергии (Power Save) монитор отключается через 5 мин, а компьютер переходит в спящий режим через 15 мин простоя. В плане Высокая производительность (High Performance) монитор отключается через 15 мин простоя, а перевод компьютера в спящий режим не предусмотрен.

Дополнительные параметры определяют возможность и время отключения компонентов электропитания и параметры производительности этих компонентов. Наличие дополнительных параметров питания зависит от конфигурации компьютера. Вот некоторые из них:

- **Батарея\Уровень резервной батареи (Battery\Reserve Battery Level)** Уровень заряда батареи, при котором компьютер переходит в режим питания от резервной батареи. Стандартное значение — 7%. Это означает, что компьютер перейдет на резервную батарею, когда заряд батареи снизится до 7%. Вы можете задать любое значением, но рекомендуется уровень от 5% до 18%.
- **Параметры фона рабочего стола\Показ слайдов (Desktop Background Settings\Slide Show)** Возможность показа слайдов на фоне рабочего стола. По умолчанию установлено значение **Доступно (Available)**. Если параметр имеет значение **Приостановлено (Paused)**, показ слайдов на фоне рабочего стола будет отключен.
- **Экран\Отключать экран через (Display\Turn Off Display After)** Время отключения монитора для экономии энергии. Чтобы отключить эту функцию, установите значение **Никогда (Never)**. Укажите время в минутах, в течение которого компьютер должен бездействовать для отключения монитора.
- **Жесткий диск\Отключать жесткий диск через (Hard Disk\Turn Off Hard Disk After)** Время отключения жесткого диска для экономии энергии. Чтобы не отключать жесткий диск, установите значение **Никогда (Never)**. Укажите время в минутах, в течение которого компьютер должен бездействовать до отключения жесткого диска. За значением 1 в сторону уменьшения следует значение Никогда (Never). Ввод значения 0 также интерпретируется как **Никогда (Never)**.

- **Параметры мультимедиа\При воспроизведении видео (Multimedia Settings\When Playing Video)** Режим оптимизации электропитания во время воспроизведения видео. Если задано значение **Оптимизация качества видео (Optimize Video Quality)**, видео воспроизводится с наилучшим качеством. Значение **Оптимизация (Balanced)** — это нейтральный режим, при котором качество воспроизведения несколько снижено для экономии энергии. Значение **Оптимизация энергопотребления (Optimize Power Savings)** означает снижение качества воспроизведения для максимальной экономии энергии.
- **Параметры мультимедиа\При общем доступе к мультимедиа (Multimedia Settings\When Sharing Media)** Действия компьютера при воспроизведении записанных на нем данных при помощи другого компьютера или устройства. Значение **Разрешить компьютеру переходить в режим отсутствия (Allow The Computer To Enter Away Mode)** не допускает переход компьютера в спящий режим во время предоставления общего доступа к медиа-файлам для других компьютеров или устройств. Значение **Разрешить компьютеру переход в спящий режим (Allow The Computer To Sleep)** допускает переход в спящий режим после некоторого времени простоя, независимо от предоставления общего доступа для других компьютеров или устройств. Если установлено значение **Запретить переход из состояния простоя в спящий режим (Prevent Idling To Sleep)**, во время предоставления общего доступа к медиа-файлам перевести компьютер в спящий режим сможет только пользователь.
- **PCI Express\Управление питанием состояния связи (PCI Express\Link State Power Management)** Режим энергосбережения, используемый при подключении к компьютеру устройств PCI Express. Доступные значения: **Отключено (Off)**, **Умеренное энергосбережение (Moderate Power Savings)** и **Максимальное энергосбережение (Maximum Power Savings)**.
- **Кнопки питания и крышка\Действие кнопки питания (Power Buttons And Lid\Power Button Action)** Действие при продолжительном нажатии на кнопку питания. Доступные значения: **Действие не требуется (Do Nothing)**, **Сон (Sleep)**, **Гибернация (Hibernate)** и **Завершение работы (Shutdown)**.
- **Кнопки питания и крышка\Действие кнопки спящего режима (Buttons And Lid\Sleep Button Action)** Действие, выполняемое при нажатии на кнопку перехода в спящий режим. Значение этого параметра перекрывает действие, выполняемое компьютером по умолчанию. Доступные значения: **Действие не требуется (Do Nothing)**, **Сон (Sleep)** и **Гибернация (Hibernate)**. Действие, которое не поддерживается компьютером, применить нельзя.
- **Управление питанием процессора\Максимальное состояние процессора (Processor Power Management\Maximum Processor State)** Макси-

мальная производительность процессора. Снижение допустимой максимальной производительности ведет к снижению потребляемой мощности и экономии энергии — за счет ухудшения отклика и снижения скорости расчетов. Снижение производительности процессора на 50% и более приводит к значительному ухудшению производительности, хотя и обеспечивает значительную экономию энергии.

- **Управление питанием процессора\Минимальное состояние процессора (Processor Power Management\Minimum Processor State)** Минимальная производительность процессора. Чтобы уменьшить потребляемую мощность, снизьте допустимое минимальное значение производительности, что приведет к ухудшению отклика и скорости расчетов. Например, значение 5% приведет к увеличению времени, требующегося для ответов на запросы и обработки данных, и одновременно обеспечит серьезную экономию энергии. При значении 50% параметры отклика и производительности улучшаются, при этом обеспечивается умеренное энергосбережение. Значение 100% обеспечивает наилучшие параметры отклика и производительности, но экономии энергии при этом не будет.
- **Управление питанием процессора\Политика охлаждения системы (Processor Power Management\System Cooling Policy)** Управляет увеличением скорости вращения вентилятора перед замедлением процессора. При выборе значения **Пассивный (Passive)** действие этой функции ограничено, и процессор может перегреваться. В значении **Активный (Active)** функция включена, и процессор охлаждается лучше.
- ***ИмяПлана*\Требовать введения пароля при пробуждении (Require A Password On Wakeup)** Задает необходимость ввода пароля при выходе компьютера из спящего режима. Доступные значения: **Да (Yes)** и **Нет (No)**. Если компьютер является членом домена, параметр имеет значение **Да (Yes)**, изменить которое можно лишь в групповой политике.
- **Сон\Разрешить гибридный спящий режим (Sleep\Allow Hybrid Sleep)** Задает использование спящего режима Windows 7 вместо аналогичного режима, реализованного в предыдущих версиях Windows. Доступные значения: **Включено (On)** и **Выключено (Off)**. При переходе в гибридный спящий режим компьютер переходит в состояние пониженного энергопотребления, пока пользователь не продолжит работу. При работе от батареи ноутбук или планшетный ПК продолжает потреблять энергию батареи и в спящем режиме, но это энергопотребление незначительно. Если у компьютера, находящегося в спящем режиме, садится батарея, текущая рабочая среда сохраняется на жесткий диск и компьютер выключается. Последнее состояние похоже на спящий режим, используемый в Windows XP.
- **Сон\Разрешить таймеры пробуждения (Sleep\Allow Wake Timers)** Определяет возможность пробуждения компьютера при наступлении событий. Значение **Отключить (Disable)** запрещает пробуждение компью-

тера при наступлении событий, а значение **Включить (Enable)** — разрешает его.

- **Сон\Гибернация после (Sleep\Hibernate After)** Параметры перевода компьютера в режим гибернации для экономии энергии. Когда компьютер переходит в состояние гибернации, содержимое ОЗУ записывается на жесткий диск. При этом создается снимок рабочей области пользователя и текущей операционной среды. Когда пользователь снова включает компьютер, содержимое памяти считывается с диска. Происходит восстановление рабочей области пользователя и текущей операционной среды. Как правило, в Windows 7 этот параметр не нужен, поскольку стандартная конфигурация предписывает после некоторого периода простоя переходить в спящий режим. Чтобы отключить эту функцию, установите значение **Никогда (Never)**. Укажите время в минутах, в течение которого компьютер должен бездействовать до перехода в режим гибернации.
- **Сон\Сон после (Sleep\Sleep after)** Параметры перевода компьютера в спящий режим для экономии энергии. Чтобы отключить эту функцию, установите значение **Никогда (Never)**. Укажите время в минутах, в течение которого компьютер должен бездействовать до перехода в спящий режим.
- **Параметры USB\Параметры временного отключения USB-порта (USB Settings\USB Selective Suspend Setting)** Возможность временного отключения USB-порта. Если параметр имеет значение **Запрещено (Disabled)**, устройства USB нельзя временно отключить. Если параметр имеет значение **Разрешено (Enabled)**, USB-устройства могут быть временно отключены.
- **Параметры адаптера беспроводной сети\Режим энергосбережения (Wireless Adapter Settings\Power Saving Mode)** Определяет режим экономии энергии для всех беспроводных адаптеров, подключенных к компьютеру. Доступные значения параметра: **Максимальная производительность (Maximum Performance)**, **Минимальное энергосбережение (Low Power Saving)**, **Среднее энергосбережение (Medium Power Saving)** и **Максмальное энергосбережение (Maximum Power Saving)**.

Как видите, именно в дополнительных параметрах заключены основные различия планов электропитания. В частности, план Высокая производительность (High Performance) допускает постоянную работу процессора на 100% потребляемой мощности, тогда как в планах Экономия энергии (Power Saver) и Сбалансированный (Balanced) потребляется меньше энергии за счет снижения потребляемой процессором мощности.

Настраивая параметры плана электропитания, помните о возможности отключения компонентов при простое. Постепенное отключение компонентов позволяет компьютеру плавно перейти в спящий режим. Когда компьютер находится в спящем режиме, отключены все компоненты электропитания. После пробуждения такие компоненты, как монитор и жесткий

диск, включаются, и рабочее пространство пользователя восстанавливается. Спящий режим на ноутбуке следует настраивать так, чтобы при работе от батареи режим сна включался сравнительно быстро, через 20-30 мин простоя.

Несколько планов электропитания позволяют оптимизировать энергопотребление ноутбука в различных ситуациях. Настройте свой план для каждой ситуации. Конфигурация электропитания при работе дома или в офисе может отличаться от конфигурации, применяемой во время презентаций. В первом случае нужно, чтобы ноутбук, работая от батареи, быстро переходил в энергосберегающий режим. Во втором нужно обеспечить постоянную работу жесткого диска и беспроводных адаптеров компьютера.

Выбор и оптимизация плана электропитания

Независимо от количества настроенных на компьютере планов электропитания активным одновременно может быть только один из них. Чтобы выбрать и настроить план электропитания, выполните следующие действия:

1. В панели управления последовательно щелкните **Система и безопасность (System And Security)** и **Электропитание (Power Options)**.
2. Выберите план в списке **Планы, отображаемые на индикаторе батареи (Preferred Plans)**, показанном на рис. 6-23.

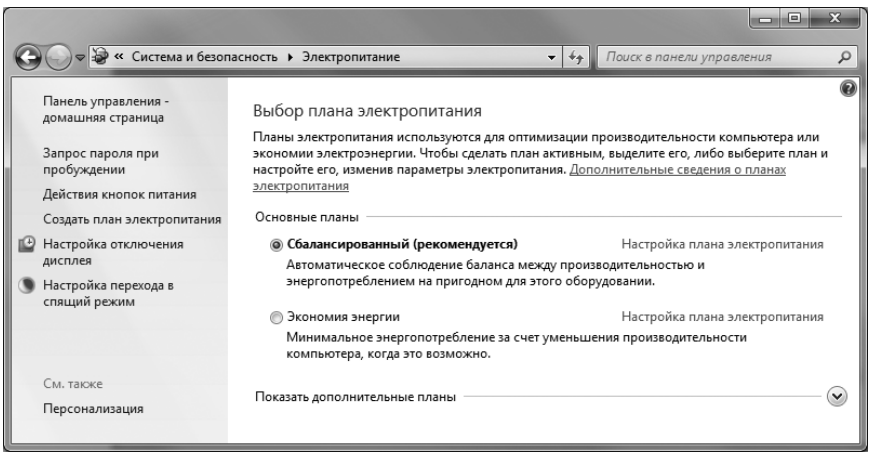

Рис. 6-23. Выбор плана электропитания

3. Щелкните ссылку **Настройка плана электропитания (Change Plan Settings)** рядом с выбранным вами планом. Откроется страница **Изменить параметры плана (Edit Plan Settings)**, показанная на рис. 6-24.
4. В списке **Отключать дисплей (Turn Off The Display)** укажите, когда нужно автоматически отключать дисплей, или откажитесь от этой возможности, установив значение **Никогда (Never)**.
5. В списке **Переводить компьютер в спящий режим (Put The Computer To Sleep)** укажите, когда компьютер должен переходить в спящий ре-

жим, или откажитесь от этой возможности, установив значение **Никогда (Never)**.

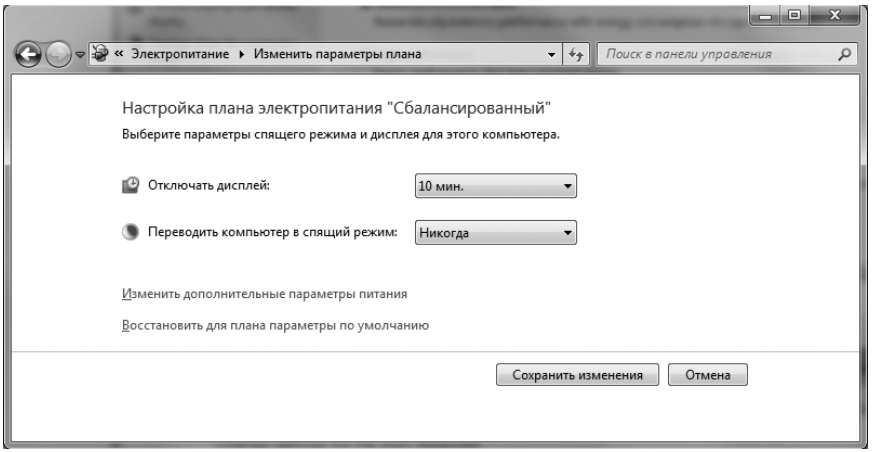

Рис. 6-24. Настройка плана электропитания

6. Для настройки дополнительных параметров щелкните **Изменить дополнительные параметры питания (Change Advanced Power Settings)**. Дополнительные параметры настраиваются в диалоговом окне **Электропитание (Power Options)**, показанном на рис. 6-25. Щелкните **OK**, чтобы сохранить изменения.

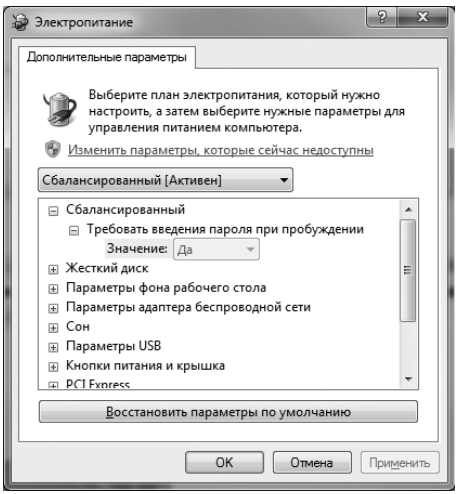

Рис. 6-25. Настройка дополнительных параметров электропитания в диалоговом окне Электропитание (Power Options)

7. Если вы изменили значения параметров **Отключать дисплей (Turn Off The Display)** и **Переводить компьютер в спящий режим (Put The Computer To Sleep)**, щелкните **Сохранить изменения (Save Changes)**, чтобы изменения вступили в силу.

Для оптимизации планов электропитания на компьютерах домена используется групповая политика и элемент предпочтения. Вот как производится настройка:

1. В оснастке Редактор управления групповыми политиками (Group Policy Management Editor) откройте объект GPO для редактирования. Чтобы настроить предпочтения для компьютеров, последовательно разверните узлы **Конфигурация компьютера\Настройки\Параметры панели управления (Computer Configuration\Preferences\Control Panel Settings)**, затем выберите узел **Электропитание (Power Options)**. Чтобы настроить предпочтения для пользователей, последовательно разверните узлы **Конфигурация пользователя\Настройки\Параметры панели управления (User Configuration\Preferences\Control Panel Settings)**, затем выберите узел **Электропитание (Power Options).**
2. Правой кнопкой щелкните узел **Электропитание (Power Options)**, выберите команду **Создать (New)** и щелкните **План электропитания (Windows Vista и более поздние версии) (Power Plan (Windows Vista And Later))**.
3. В открывшемся диалоговом окне **Новые свойства плана электропитания (New Power Plan Properties)** выберите в списке **Действие (Action)** вариант **Обновить (Update)** для обновления параметров плана или вариант **Заменить (Replace)**, чтобы удалить и повторно создать план по заданным вами параметрам.
4. Выберите в списке нужный план электропитания, например **Сбалансированный (Balanced)**.
5. Активируйте план, установив флажок **Задать в качестве текущей схемы управления электропитанием (Set As The Active Power Plan)**.
6. Настройте параметры плана электропитания, указав необходимые значения параметров.
7. Щелкните **OK**. Во время следующего обновления политики элемент предпочтения будет применен к объекту GPO, в котором вы его определили.

Создание плана электропитания

Вы вольны создавать собственные планы в дополнение к стандартным планам электропитания Windows 7. Чтобы создать план электропитания, выполните следующие действия:

1. В панели управления последовательно щелкните **Система и безопасность (System And Security)** и **Электропитание (Power Options)**.
2. На левой панели перейдите по ссылке **Создать план электропитания (Create A Power Plan)**. Откроется окно **Создать план электропитания (Create A Power Plan)**, показанное на рис. 6-26.

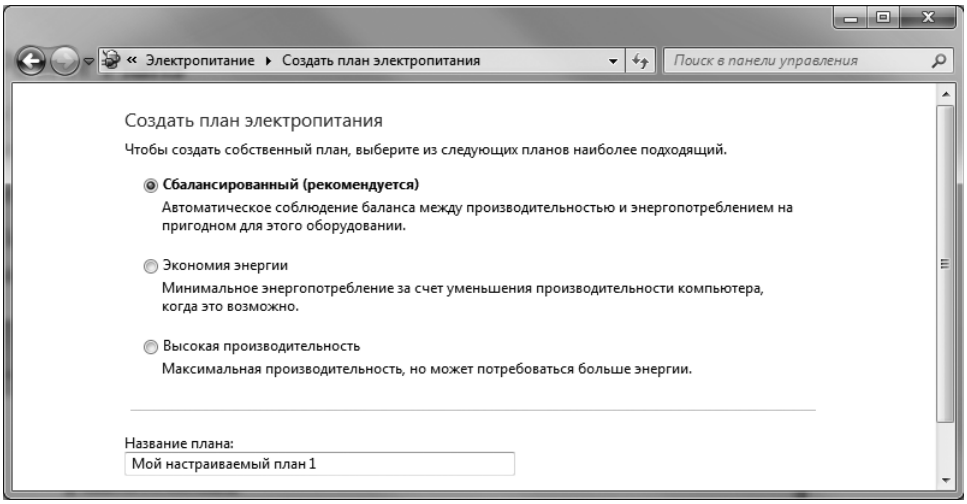

Рис. 6-26. Создание плана электропитания

3. Для предварительной настройки параметров выберите один из стандартных планов, наиболее близкий по типу к создаваемому вами плану.
4. В поле **Название плана (Plan Name)** введите понятное имя плана и щелкните **Далее (Next)**.
5. На открывшейся странице **Изменить параметры плана (Edit Plan Settings)** в списке **Отключать дисплей (Turn Off The Display)**, укажите, когда нужно автоматически отключать дисплей, или откажитесь от этой возможности, установив значение **Никогда (Never)**.
6. В списке **Переводить компьютер в спящий режим (Put The Computer To Sleep)** укажите, когда компьютер должен переходить в спящий режим, или откажитесь от этой возможности, установив значение **Никогда (Never)**.
7. Чтобы создать план, щелкните **Создать (Create)**. На открывшейся странице **Электропитание (Power Options)** созданный вами план находится в списке предпочтительных планов на месте плана, выбранного вами ранее. Исходный план будет перемещен в список дополнительных планов. Чтобы открыть этот список, щелкните **Показать дополнительные планы (Show Additional Plans)**.
8. Созданный вами план используется по умолчанию. Щелкните **Настройка плана электропитания (Change Plan Settings)**. На странице **Изменить параметры плана (Edit Plan Settings)** щелкните **Изменить дополнительные параметры питания (Change Advanced Power Settings)**.
9. После настройки дополнительных параметров питания в диалоговом окне **Электропитание (Power Options)** щелкните **OK**, чтобы сохранить внесенные изменения.

Для создания планов электропитания на компьютерах домена используется групповая политика и элемент предпочтения:

1. В оснастке Редактор управления групповыми политиками (Group Policy Management Editor) откройте объект GPO для редактирования. Чтобы настроить предпочтения для компьютеров, последовательно разверните узлы **Конфигурация компьютера\Настройки\Параметры панели управления (Computer Configuration\Preferences\Control Panel Settings)**, затем выберите узел **Электропитание (Power Options)**. Чтобы настроить предпочтения для пользователей, последовательно разверните узлы **Конфигурация пользователя\Настройки\Параметры панели управления (User Configuration\Preferences\Control Panel Settings)**, затем выберите узел **Электропитание (Power Options)**.
2. Правой кнопкой щелкните узел **Электропитание (Power Options)**, выберите команду **Создать (New)** и щелкните **План электропитания (Windows Vista и более поздние версии) (Power Plan (Windows Vista And Later))**.
3. В открывшемся диалоговом окне **Новые свойства плана электропитания (New Power Plan Properties)** в списке **Действие (Action)** выберите вариант **Создать (Create)**. Для предварительной настройки параметров выберите один из стандартных планов электропитания, наиболее близкий по типу к создаваемому вами плану. Выбрав план, щелкните список и введите название нового плана.
4. Выберите нужный план электропитания из списка, например **Сбалансированный (Balanced)**.
5. Активируйте план, установив флажок **Задать в качестве текущей схемы управления электропитанием (Set As The Active Power Plan).**
6. Настройте параметры плана электропитания.
7. Щелкните **OK**. Во время следующего обновления политики элемент предпочтения будет применен к объекту GPO, в котором вы его определили.

Настройка кнопки питания и ввода пароля при пробуждении

Системные параметры электропитания позволяют определить поведение кнопки питания и ввод пароля при пробуждении для всех пользователей, работающих на компьютере. Кнопку питания можно настроить так, что при нажатии на нее система будет завершать работу, переходить в режим гибернации или сна. Кроме того, вы вольны настроить компьютер таким образом, что при его выводе из спящего режима нужно будет ввести пароль для разблокирования экрана.

Чтобы задать системные параметры электропитания, выполните следующие действия:

1. В панели управления последовательно щелкните **Система и безопасность (System And Security)** и **Электропитание (Power Options)**.
2. На левой панели перейдите по ссылке **Действия кнопок питания (Choose What The Power Buttons Do)**.

3. В списке **При нажатии кнопки питания (When I Press The Power Button)** укажите нужное действие при нажатии на кнопку (рис. 6-27). Выбрать действие, которое не поддерживается компьютером, нельзя.

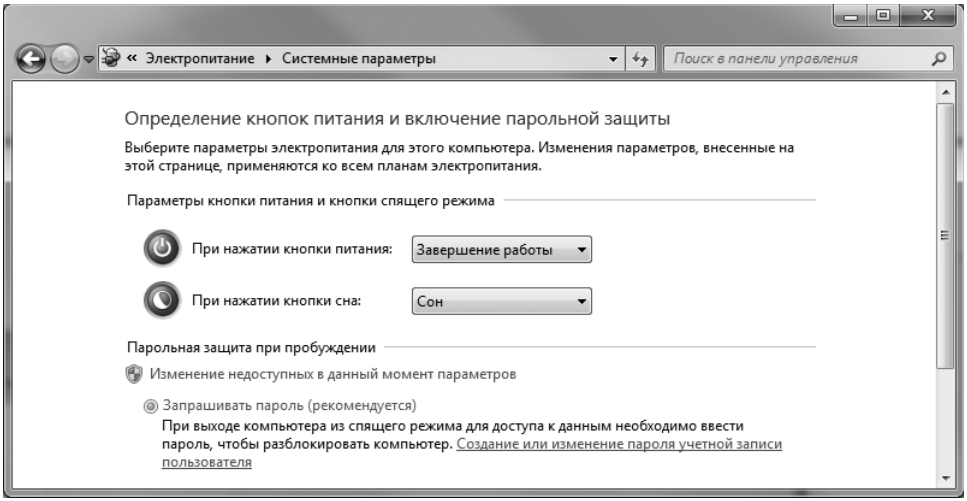

Рис. 6-27. Установка параметров кнопки питания, кнопки сна и защиты паролем при пробуждении

4. В списке **При нажатии кнопки сна (When I Press The Sleep Button)** укажите нужное действие: ничего не делать, сон или гибернация. Здесь также нельзя выбрать действие, которое не поддерживается компьютером.
5. Если параметры раздела **Парольная защита при пробуждении (Password Protection On Wakeup)** недоступны, щелкните ссылку **Изменение недоступных в данный момент параметров (Change Settings That Are Currently Unavailable)**.
6. Чтобы сделать обязательным ввод пароля при пробуждении, задайте параметр **Запрашивать пароль (Require A Password)**. Ввод пароля поможет обеспечить безопасность системы.
7. Завершив настройку, щелкните **Сохранить изменения (Save Changes)**.

Управление электропитанием при помощи параметров политики

В групповой политике параметры управления электропитанием находятся в узле **Конфигурация компьютера\Административные шаблоны\Система\Управление электропитанием (Computer Configuration\Administrative Templates\System\Power Management)**. В нем есть пять вложенных узлов:

- **Параметры кнопок (Button Settings)** Политики, определяющие действия для кнопки питания, кнопки сна или при закрытии крышки ноутбука, когда компьютер работает от сети или от батареи. Здесь также задаются параметры кнопки питания, появляющейся на экране при нажатии клавиш Ctrl+Alt+Del.

- **Параметры жесткого диска (Hard Disk Settings)** Политики, определяющие параметры включения и выключения жестких дисков при работе от сети и от батареи.
- **Параметры уведомления (Notification Settings)** Политики, управляющие уведомлениями и действиями при низком заряде батареи.
- **Параметры режимов сна (Sleep Settings)** Политики, определяющие разрешенные состояния сна для устройств и приложений.
- **Параметры экрана и видео (Video And Display)** Политики, определяющие поведение и яркость экрана, а также показ слайдов на рабочем столе в фоновом режиме при работе от сети или от батареи.

Чтобы применить параметр политики, включите политику и выберите нужное действие.

В групповой политике также можно указать активный план электропитания. Метод работы с политиками узла **Управление электропитанием (Power Management)** зависит от плана электропитания, который предполагается использовать: план, установленный по умолчанию, измененный стандартный план или пользовательский план. Если на всех целевых компьютерах политики предполагается использовать один из стандартных планов электропитания Windows 7, выполните следующие действия:

1. Откройте объект GPO для редактирования. Разверните узел **Конфигурация компьютера\Административные шаблоны\Система\Управление электропитанием (Computer Configuration\Administrative Templates\System\Power Management).**
2. Дважды щелкните параметр **Выберите текущую схему управления питанием (Select An Active Power Plan)**.
3. Щелкните **Включить (Enabled)** и выберите нужный план в списке **Текущая схема управления питанием (Active Power Plan)**. Доступны следующие параметры: **Высокая производительность (High Performance)**, **Экономия энергии (Power Saver)** и **Автоматический (Automatic)**. Для схемы **Автоматический (Automatic)** в большинстве случаев используется план **Сбалансированный (Balanced)**.
4. Щелкните **OK**.

Если на всех целевых компьютерах политики предполагается использовать измененный стандартный план или пользовательский план электропитания, выполните следующие действия:

1. Откройте объект GPO для редактирования. Разверните узел **Конфигурация компьютера\Административные шаблоны\Система\Управление электропитанием (Computer Configuration\Administrative Templates\System\Power Management)**.
2. Дважды щелкните параметр **Укажите настраиваемую схему управления питанием (Select A Custom Active Power Plan)**.

3. Щелкните **Включить (Enabled)**. В текстовом поле **Настраиваемая схема управления питанием (Custom Active Power Plan (GUID))** введите идентификатор GUID используемого плана.
4. Щелкните **OK**.

Совет Чтобы определить идентификаторы GUID планов электропитания, настроенных на компьютере, введите в командной строке с повышенными полномочиями команду **powercfg –l**.

Сигналы и действия

Сигнал (alarm) определяет подачу звукового или визуального оповещения при снижении уровня заряда батареи портативного компьютера до определенного уровня. Существует три уровня сигналов и уведомлений:

- **Сигнал низкого заряда батареи** Предупреждение о снижении уровня заряда батареи. Режим низкого уровня заряда батареи по умолчанию включается, когда уровень батареи достигает 10% от полного заряда. Для батареи, время работы которой составляет 8 часов, 10% — это примерно 48 минут работы.
- **Сигнал почти полной разрядки батареи** Предупреждение о скором отключении батареи. По умолчанию состояние почти полной разрядки включается, когда уровень батареи составляет не более 3%. Для батареи, полное время работы которой составляет 8 часов, 3% — это примерно 14 минут работы.
- **Сигнал резервной батареи** Предупреждение об использовании резервной энергии батареи. Режим резервной батареи по умолчанию включается, когда уровень батареи падает до 1%. Для батареи, время работы которой составляет 8 часов, 1% дает примерно 5 минут работы.

Действия по сигналам низкого заряда и почти полной разрядки — это специальные действия, выполняемые ОС при достижении данного уровня заряда. Среди возможных действий завершение работы компьютера, переход в спящий режим или режим гибернации. Начиная с Windows Vista, вы можете отключить уведомления о низком уровне батарей, включив политику Отключить уведомление при низком уровне заряда батареи (Turn Off Low Battery User Notification). В Windows 7 введен сигнал резервной батареи, уведомляющий пользователя об использовании резервного заряда батареи. В настройке каждого уровня сигналов есть свои тонкости. Далее мы рассмотрим каждый из них в отдельности.

Уведомление и действие при низком заряде батареи

Как уже отмечалось, сигнал о низком заряде батареи свидетельствует о разрядке аккумулятора. При переходе системы в режим пониженного энергопотребления пользователь получает уведомление — текстовое или текстовое со звуковым сигналом. В некоторых случаях можно пойти чуть дальше и вместо вывода предупреждения настроить компьютер на переход в режим ожидания.

Чтобы настроить уведомление низкого заряда батареи и связанное с ним действие, выполните следующие действия:

1. Откройте объект GPO для редактирования. Разверните узел **Конфигурация компьютера\Административные шаблоны\Система\Управление электропитанием\Параметры уведомлений (Computer Configuration\Administrative Templates\System\Power Management\Notification Settings)**.
2. Чтобы задать действие при низком заряде батареи, дважды щелкните параметр **Действие при низком заряде батарей (Low Battery Notification Action)**. Выберите **Включить (Enabled)** и в списке **Действие при низком заряде батареи (Low Battery Notification Action)** укажите действие, например **Режим сна (Sleep)**. Щелкните **OK**.
3. Чтобы задать уровень подачи сигнала о низком заряде батареи, дважды щелкните параметр **Уровень сигнала низкого заряда батареи (Low Battery Notification Level)**. Выберите **Включить (Enabled)**. В поле **Уровень сигнала низкого заряда батареи (Low Battery Notification Level)** укажите требуемый уровень. Щелкните **OK**.

Совет Стандартный уровень подачи сигнала о низком заряде батареи зависит от общей емкости батареи и обычно составляет 10%. Этого достаточно для большинства систем. Однако встречаются системы, особенно, со старыми аккумуляторами, для которых такого уровня недостаточно, и его нужно повысить до 12–15%. В энергосберегающих системах или системах с двумя батареями, наоборот, стандартное значение оказывается слишком большим. Здесь устанавливают такой уровень, при котором пользователь получает уведомление, когда заряда батареи остается примерно на 20 мин. работы.

4. По умолчанию пользователь получает уведомление о снижении уровня заряда батареи. Если нужно отключить эти уведомления, дважды щелкните **Отключить уведомление при низком уровне заряда батареи (Turn Off Low Battery User Notification)**, щелкните **Включить (Enabled)**, а затем щелкните **OK**.

Настройка сигнала при почти полной разрядке батареи

Сигнал почти полной разрядки батареи обеспечивает переход системы в определенный режим до отключения питания. Пользователь получает уведомление о том, что система переходит в режим почти полной разрядки батареи, после чего система переходит в режим сна. В спящем режиме компоненты электропитания компьютера отключаются. На моем компьютере сначала сигнал низкого заряда батареи задает переход компьютера в спящий режим. Затем сигнал почти полной разрядки батареи переводит компьютер в режим гибернации или завершает работу. Эти возможности по управлению электропитанием помогают сохранить систему до отключения питания.

Чтобы настроить действия при низком заряде батареи, выполните следующие действия:

1. Откройте объект GPO для редактирования. Разверните узел **Конфигурация компьютера\Административные шаблоны\Система\Управление**

электропитанием\Параметры уведомлений (Computer Configuration\Administrative Templates\System\Power Management\Notification Settings).

2. Чтобы задать действие при почти полной разрядке батареи, дважды щелкните параметр **Действие при почти полной разрядке батареи (Critical Battery Notification Action)**. Выберите **Включить (Enabled)** и в списке **Действие при почти полной разрядке батареи (Critical Battery Notification Action)** укажите действие, например **Гибернация (Hibernate)** или **Выключение (Shut Down)**. Щелкните **OK**.
3. Чтобы установить уровень подачи сигнала почти полной разрядки батареи, дважды щелкните параметр **Уровень сигнала почти полной разрядки батареи (Critical Battery Notification Level)**. Выберите **Включить (Enabled)**. В поле **Уровень сигнала почти полной разрядки батареи (Critical Battery Notification Level)** укажите требуемый уровень для подачи сигнала. Щелкните **OK**.

Совет Стандартный уровень подачи сигнала почти полной разрядки батареи зависит от общей емкости батареи и обычно составляет 10%. В большинстве случаев этого достаточно. Однако для завершения работы компьютера или его перевода в режим гибернации это значение можно уменьшить. Следует также учесть время работы от батареи. Если компьютер может работать от батареи длительное время, стандартное значение, как правило, слишком велико; а для компьютера со слабым аккумулятором — слишком мало. У меня сигнал почти полного разряда батареи подается, когда до конца работы остается 6–8 минут.

Настройка режима резервной батареи

Режим резервной батареи предназначен для уведомления пользователя о работе батареи на резервном источнике энергии. Чтобы настроить уведомление резервной батареи, выполните следующие действия:

1. Откройте объект GPO для редактирования. **Разверните узел Конфигурация компьютера\Административные шаблоны\Система\Управление электропитанием\Параметры уведомлений (Computer Configuration\Administrative Templates\System\Power Management\Notification Settings)**.
2. Чтобы задать уровень подачи сигнала резервной батареи, дважды щелкните параметр **Уровень сигнала резервной батареи (Reserve Battery Notification Level)**. Выберите **Включить (Enabled)**. В поле **Уровень сигнала резервной батареи (Reserve Battery Notification Level)** укажите требуемый уровень подачи сигнала. Щелкните **OK**.

Глава 7

Настройка рабочего стола и пользовательского интерфейса

Администратору нередко приходится помогать пользователям в настройке рабочего стола и профиля. Не исключено, что вам придется создавать для новых пользователей рабочую среду, соответствующую их потребностям или корпоративному стандарту. Один из способов настроить рабочую среду по умолчанию — создать стандартную учетную запись пользователя, непосредственно модифицировать для нее рабочую среду, а затем использовать эту учетную запись и соответствующий профиль пользователя в качестве базового.

В Windows 7 настройки рабочего стола и экрана выведены на новый уровень. Эти возможности весьма полезны, но могут привести к проблемам, решать которые придется вам. Кроме того, пользователь может попытаться решить их самостоятельно, а вам, возможно, придется ему помогать. Эта глава посвящена настройке и решению проблем в следующих аспектах:

- меню, панель задач, панели инструментов;
- темы и фоновые рисунки рабочего стола;
- настраиваемое содержимое рабочего стола;
- заставки;
- вид и параметры отображения.

Оптимизация меню Windows 7

Меню **Пуск (Start)** и его подменю призваны предоставить удобный доступ к приложениям и утилитам. Однако, чем больше приложений и утилит установлено на компьютере, тем сложнее найти что бы то ни было в этом меню. В этом разделе описаны способы, как избежать захламления различных меню и оптимизировать их.

Настройка параметров меню Пуск (Start)

В Windows 7 весьма удобно управлять меню **Пуск (Start)**: можно выбрать, какие команды в нем отображаются и как они будут распределены, можно добавить команды для открытия окон **Панель управления (Control Panel)**,

Устройства и принтеры (Devices And Printers), **Сетевые подключения (Network Connections)** и запуска других ключевых инструментов, а также настраивать меню **Все программы (All Programs)**.

Чтобы настроить параметры меню **Пуск (Start)**, выполните следующие действия:

1. Щелкните правой кнопкой панель задач и выберите команду **Свойства (Properties)**. Откроется диалоговое окно **Свойства панели задач и меню «Пуск» (Taskbar And Start Menu Properties)**.
2. При помощи списка **Действие кнопки питания (Power Button Action)** на вкладке **Меню «Пуск» (Start Menu)** выберите действие, выполняемое при нажатии кнопки питания. Возможны такие варианты: **Смена пользователя (Switch User)**, **Завершение сеанса (Log Off)**, **Блокировка (Lock)**, **Перезагрузка (Restart)**, **Сон (Sleep)** и **Завершение работы (Shut Down)**. В системе со многими пользователями или круглосуточным режимом работы возможными альтернативами завершению работы будут переключение пользователей, выход из системы или блокировка системы. Для выключения компьютера всегда останется команда **Завершение работы (Shutdown)** в меню **Пуск (Start)**.
3. Щелкните кнопку **Настроить (Customize)**. Откроется диалоговое окно **Настройка меню «Пуск» (Customize Start Menu)**, показанное на рис. 7-1.

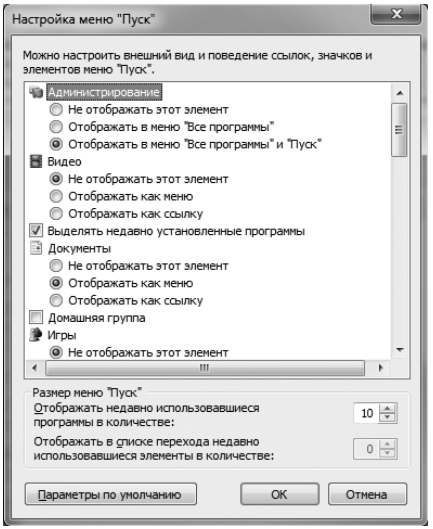

Рис. 7-1. Настройка меню Пуск (Start)

4. Настройте внешний вид меню **Пуск (Start)** при помощи параметров этого диалогового окна.
5. Чтобы закрыть диалоговое окно **Свойства панели задач и меню «Пуск» (Taskbar And Start Menu Properties)**, два раза щелкните **OK**.

Большинство параметров диалогового окна **Настройка меню «Пуск» (Customize Start Menu)** определяют, какие команды будут отображаться в меню **Пуск (Start)** и как они будут распределены. В некоторых случаях имеются дополнительные параметры, например **Отображать как ссылку (Display As A Link)**, **Отображать как меню (Display As A Menu)** и **Не отображать этот элемент (Don't Display This Item)**. Выбрав параметр **Отображать как ссылку (Display As A Link)**, вы укажете, что команда, например **Панель управления (Control Panel)**, будет работать как ссылка; чтобы открыть окно, ее нужно будет щелкнуть один раз. Параметр **Отображать как меню (Display As A Menu)** указывает, что команда открывает доступ к подменю, позволяющему сделать выбор еще из нескольких вариантов. Переключатель **Не отображать этот элемент (Don't Display This Item)** удаляет элемент из меню **Пуск (Start)**.

Далее перечислены другие параметры диалогового окна **Настройка меню «Пуск» (Customize Start Menu)**.

- **Разрешить контекстные меню и перетаскивание элементов (Enable Context Menus And Dragging And Dropping)** Этот флажок разрешает пользователям применять контекстные меню и перетаскивание. Как правило, сбрасывать его следует лишь по соображениям безопасности.
- **Выделять недавно установленные программы (Highlight Newly Installed Programs)** Этот флажок задает цветовое выделение недавно установленных приложений и меню, в которых они расположены.
- **Раскрывать подменю при наведении и задержке указателя мыши (Open Submenus When I Pause On Them With The Mouse Pointer)** Управляет поведением меню. Если этот флажок включен, меню будут открываться при наведении на них указателя. В противном случае они открываются только по щелчку.
- **Сортировать меню «Все программы» по именам (Sort All Programs Menu By Name)** Определяет способ сортировки элементов меню: по алфавиту или по времени установки. Если этот параметр включен, элементы меню сортируются по алфавиту, если выключен — по времени установки.
- **Крупные значки (Use Large Icons)** Определяет размер значков в меню. Чтобы уменьшить размер значков, отключите этот параметр. Если вас устраивает стандартный размер значков, не меняйте этот параметр.
- **Отображать недавно использовавшиеся программы в количестве (Number Of Recent Programs To Display)** Определяет количество элементов списка недавно использованных программ. Допустимы значения от 0 до 30. Количество отображаемых программ зависит также от разрешения экрана и количества других элементов меню **Пуск (Start)**.
- **Отображать в списке перехода недавно использовавшиеся элементы в количестве (Number of Recent Items To Display In Jump List)** Определяет количество ссылок на часто используемые элементы в списках перехода. В списки перехода включаются часто используемые элементы, упорядоченные по программе, которая с ними работает. Эти списки

могут быть как в меню **Пуск (Start)**, так и на панели задач. Допустимы значения от 0 до 60.

Чтобы вернуть исходную конфигурацию меню **Пуск (Start)**, откройте диалоговое окно **Настройка меню «Пуск» (Customize Start Menu)** и щелкните кнопку **Параметры по умолчанию (Use Default Settings)**. Затем дважды щелкните **OK**.

Чтобы настроить меню **Пуск (Start)** на компьютерах домена, воспользуйтесь предпочтениями групповых политик:

1. В редакторе управления групповой политикой откройте GPO для редактирования. Разверните узел **Конфигурация пользователя\Настройки\Параметры панели управления (User Configuration\Preferences\Control Panel Settings)**.
2. Щелкните правой кнопкой узел **Главное меню (Start Menu)**, раскройте подменю **Создать (New)** и выберите команду **Главное меню (Windows Vista и более поздние версии) (Start Menu (Windows Vista And Later))**. Откроется диалоговое окно **Новые свойства меню «Пуск» (Windows Vista и более поздние версии) (New Start Menu (Windows Vista And Later) Properties)**, показанное на рис. 7-2.

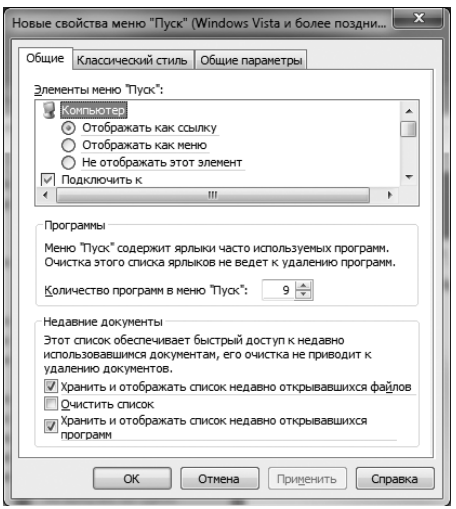

Рис. 7-2. Настройка меню Пуск (Start) в домене

3. Используйте доступные параметры для настройки меню **Пуск (Start)**. На клиентских машинах будут применены все параметры интерфейса, даже если вы не будете явно задавать их значения. Это действие перезапишет все существующие параметры интерфейса рабочего стола пользователей.
4. Для управления применением предпочтения используйте вкладку **Общие параметры (Common)**. Чаще всего стандартизированное меню **Пуск (Start)** создается только однажды. Поэтому установите флажок **Применить один раз и не применять повторно (Apply Once And Do Not Reapply)**.

5. Щелкните **OK**. Предпочтение будет применено к соответствующему объекту групповых политик при следующем обновлении политик.

Изменение меню и их элементов

В файловой системе Windows 7 меню **Пуск (Start)** представлено двумя папками, каждая из которых называется **Главное меню (Start Menu)**. Программы, доступные только текущему пользователю, расположены в подпапке **Главное меню (Start Menu)** профиля пользователя (%UserProfile%\AppData\Roaming\Microsoft\Windows\Start Menu). Программы, доступные всем пользователям компьютера, расположены в общей подпапке **Главное меню (Start Menu)** (%SystemDrive%\ProgramData\Microsoft\Windows\Start Menu).

В процессе загрузки ОС Windows 7 объединяет содержимое обеих папок и создает единое меню **Пуск (Start)**. В каждой папке **Главное меню (Start Menu)** есть подпапка **Программы (Programs)**. Ее подпапки, в свою очередь, представляют собой подменю, а ярлыки внутри этих папок являются элементами меню и указывают на конкретные программы. Есть несколько способов изменить структуру меню **Пуск (Start)**, в частности, напрямую работая с представлением меню в файловой системе или непосредственно с самими меню.

Перестановка элементов меню Пуск (Start)

Простейший способ изменить положение меню и их элементов внутри меню **Пуск (Start)** — непосредственная работа с системой меню. Выполните следующие действия:

1. Щелкните кнопку **Пуск (Start)** и разверните подменю **Все программы (All Programs)**.
2. Наведите указатель на элемент, который собираетесь переставить.
3. Нажмите и удерживайте левую кнопку мыши.
4. Перетащите элемент на новое положение в меню или подменю. Чтобы открыть подменю, наводите на них указатель. Горизонтальная линия показывает, куда будет помещен выбранный элемент.
5. Отпустите кнопку мыши.

Примечание Для перемещения элементов меню требуются полномочия администратора. Чтобы увидеть изменения, текущему пользователю в большинстве случаев придется выйти из системы и зайти в нее заново.

Если вы перетащите элемент меню в левый верхний угол меню **Пуск (Start)**, он попадет в *список прикрепленных элементов* (pinned items list). Когда указатель мыши будет в нужном положении, появится горизонтальная линия, показывающая, куда попадет текущий элемент меню, если отпустить кнопку мыши. Есть и другие способы добавить элемент в этот список:

- Чтобы добавить элемент, дважды щелкните его и выберите команду **Закрепить в меню «Пуск» (Pin To Start Menu)**.

- Чтобы удалить элемент из прикрепленного списка, щелкните элемент правой кнопкой и выберите команду **Удалить из этого списка (Remove From This List)**. Также в контекстном меню есть команда **Изъять из меню «Пуск» (Unpin From Start Menu)**. Она удалит элемент из прикрепленного списка, но оставит его в списке часто используемых элементов (если он там есть). Команда **Удалить из этого списка (Remove From This List)** удалит элемент отовсюду.

Реорганизация элементов меню

Обычно меню **Все программы (All Programs)** упорядочено так, что выше отображаются подменю, а ниже — индивидуальные элементы. Содержимое обеих категорий упорядочено по алфавиту.

При добавлении или перемещении элементов меню они автоматически переупорядочиваются. Если они не отсортированы по алфавиту, вероятно, кто-то сбросил флажок **Сортировать меню «Все программы» по именам (Sort All Programs Menu By Name)** в диалоговом окне **Настройка меню «Пуск» (Customize Start Menu)** текущего пользователя. Чтобы упорядочить меню **Все программы (All Programs)** целиком и сохранять алфавитный порядок далее, выполните следующие действия:

1. Щелкните правой кнопкой панель задач и выберите команду **Свойства (Properties)**. Откроется диалоговое окно **Свойства панели задач и меню «Пуск» (Taskbar And Start Menu Properties)**.
2. Щелкните кнопка **Настройка (Customize)** на вкладке **Меню «Пуск» (Start Menu)**. Прокрутив список параметров вниз, установите флажок **Сортировать меню «Все программы» по именам (Sort All Programs Menu By Name)**.
3. Дважды щелкните **OK**.

Добавление, изменение и удаление меню

Как уже говорилось, в файловой системе меню **Пуск (Start)** представлено папкой, до которой можно добраться через данные профиля конкретного пользователя или через данные общего профиля. Чтобы зайти в папку Главное меню (Start Menu) текущего пользователя, щелкните правой кнопкой кнопку **Пуск (Start)**, выберите команду **Открыть проводник (Open indows Explorer)** и зайдите в скрытую папку %UserProfile%\AppData\Roaming\Microsoft\Windows\Start Menu. Чтобы зайти в папку Главное меню (Start Menu), общую для всех пользователей, щелкните правой кнопкой панель задач, выберите в контекстном меню команду **Открыть проводник (Open Windows Explorer)**, зайдите в скрытую папку %SystemDrive%\ProgramData\Microsoft\Windows\Start Menu. С папкой Главное меню (Start Menu) можно работать так же, как и с любыми другими папками. В частности, можно:

- добавлять новые подменю в меню **Все программы (All Programs)**, создавая подпапки внутри папки Программы (Programs) или в ее подпапках, кроме папки Автозагрузка (Startup).

- изменять меню, перенося папки и ярлыки внутри папки Программы (Programs);
- переименовывать папки и ярлыки, чтобы изменить их имена в меню **Все программы (All Programs)**.

Переименовывать команды меню **Все программы (All Programs)** можно и через систему меню. Откройте меню **Все программы (All Programs)**, щелкните правой кнопкой элемент, который хотите переименовать, и выберите команду **Переименовать (Rename)**.

Примечание Если скрытые папки не видны или не открываются, измените настройки папок проводника Windows. Выберите в меню **Упорядочить (Organize)** команду **Параметры папок и поиска (Folder And Search Options)**. На вкладке **Вид (View)** установите переключатель **Показывать скрытые файлы, папки и диски (Show Hidden Files, Folders, And Drives)** и щелкните **OK**.

Внимание! Удаляйте все ненужные папки и ярлыки, чтобы удалить из меню **Все программы (All Programs)** соответствующие элементы. Еще один способ удаления — через систему меню. Откройте меню **Все программы (All Programs)**, щелкните правой кнопкой элемент, который хотите удалить, и выберите команду **Удалить (Delete)**. Не удаляйте и не переименовывайте папку Автозагрузка (Startup) — она содержит ярлыки программ, запускающихся автоматически после запуска системы. Если ее изменить, Windows 7, возможно, не сможет с ней работать. Кроме того, не стоит ни удалять, ни переименовывать меню **Администрирование (Administrative Tools)**. Доступ к нему задается параметрами окна **Свойства панели задач и меню «Пуск» (Taskbar And Start Menu Properties)**.

Добавление и удаление команд в меню Пуск (Start)

Команды меню представлены ярлыками файловой системы Windows 7. Это означает, что создавать новые элементы меню можно, просто добавляя ярлыки в папку Программы (Programs) и ее подпапки. Создав ярлык, к нему можно добавить комментарий, который будет отображаться при наведении указателя на соответствующий элемент меню. Чтобы создать элемент меню для текущего пользователя, выполните следующие действия:

1. Щелкните кнопку **Пуск (Start)** правой кнопкой мыши, выберите команду **Открыть проводник (Open Windows Explorer)** и зайдите в скрытую папку %UserProfile%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs.
2. В левой панели проводника Windows выделите папку, в которую хотите добавить элемент меню.
3. Щелкните правой кнопкой пустое место на в области сведений, раскройте подменю **Создать (New)** и выберите **Ярлык (Shortcut)**. Откроется мастер Создать ярлык (Create Shortcut).
4. Введите полный путь к программе или файлу, с которым хотите связать создаваемый ярлык. Если путь неизвестен, щелкните кнопку **Обзор (Browse)** и найдите путь в диалоговом окне **Обзор файлов и папок (Browse For Files Or Folders)**.

5. Щелкните **Далее (Next)** и введите имя ярлыка. Введенное вами значение будет именем элемента меню в меню **Пуск (Start)**.
6. Щелкните **Готово (Finish)**. Чтобы ввести комментарии к ярлыку, щелкните его правой кнопкой и выберите команду **Свойства (Properties)**. Введите комментарий в поле **Комментарий (Comment)** вкладки **Ярлык (Shortcut)**. Щелкните **OK**.

Отображение меню Администрирование (Administrative Tools)

В Windows 7 меню **Администрирование (Administrative Tools)** по умолчанию не отображается. Чтобы включить его в меню пользователей, обладающими полномочиями администратора, требуется настройка меню **Пуск (Start)**. Чтобы добавить меню **Администрирование (Administrative Tools)** в меню **Пуск (Start)** или в меню **Все программы (All Programs)**, выполните следующие действия:

1. Щелкните правой кнопкой кнопку **Пуск (Start)** и выберите команду **Свойства (Propeties)**. Откроется диалоговое окно **Свойства панели задач и меню «Пуск» (Taskbar And Start Menu Properties)**.
2. Щелкните кнопку **Настройка (Customize)**. Найдите раздел **Администрирование (System Administrative Tools)**.
3. Выберите один из двух переключателей:
   - Чтобы включить меню **Администрирование (Administrative Tools)** в меню **Все программы (All Programs)**, установите переключатель **Отображать в меню «Все программы» (Display On The All Programs Menu)**.
   - Чтобы включить меню **Администрирование (Administrative Tools)** в меню **Пуск (Start)** и в меню **Все программы (All Programs)**, установите переключатель **Отображать в меню «Все программы» и «Пуск» (Display On The All Programs Menu And The Start Menu)**.
4. Дважды щелкните **OK**.

Работа с меню, рабочими столами и автозагрузкой

В ОС Windows меню, рабочие столы и автозапуск настраиваются при помощи ярлыков. Расположение ярлыка определятся тем, как он будет использоваться. Например, чтобы добавить элемент в меню пользователя, нужно добавить ярлык в соответствующую папку **Программы (Programs)** или **Главное меню (Start Menu)**. Для настройки автозапуска приложений для всех пользователей добавляйте ярлыки в папку AllUsersStartup. Эти приложения автоматически запустятся при локальном входе пользователя в систему.

Создание ярлыков меню, рабочего стола, автозапуска и прочего

Проводник Windows позволяет изменять меню, рабочие столы и приложения автозапуска для конкретного пользователя, войдя на его компьютер и создавая ярлыки в соответствующих папках. В групповой политике ярлыки

меню, рабочих столов, приложений автозапуска и др. создаются посредством предпочтений **Ярлыки (Shortcuts)**. Эти предпочтения автоматически применяются ко всем компьютерам, обрабатывающим соответствующий GPO.

Для настройки предпочтений **Ярлыки (Shortcuts)** выполните следующие действия:

1. Откройте GPO для редактирования в редакторе управления групповой политики. Чтобы настроить предпочтения для компьютеров, разверните узел **Конфигурация компьютера\Настройка\Конфигурация Windows (Computer Configuration\Preferences\Windows Settings)** и выделите элемент **Ярлыки (Shortcuts)**. Чтобы настроить предпочтения для пользователей, разверните узел **Конфигурация пользователя\Настройка\Конфигурация Windows (User Configuration\Preferences\Windows Settings)** и выделите узел **Ярлыки (Shortcuts)**.
2. Щелкните узел **Ярлыки (Shortcuts)** правой кнопкой, разверните подменю **Создать (New)** и выберите команду **Ярлык (Shortcut)**. Откроется диалоговое окно **Новые свойства ярлыка (New Shortcut Properties)**, показанное на рис. 7-3.
3. Выберите в списке **Действие (Action)** вариант **Создать (Create)**, **Обновить (Update)** или **Заменить (Replace)** и переходите к другим параметрам, описанным в этом разделе.
4. При помощи параметров вкладки **Общие параметры (Common)** определите, как будет применяться предпочтение. Часто его нужно применить лишь единожды, поэтому выбирайте **Применить один раз и не применять повторно (Apply Once And Do Not Reapply)**.
5. Щелкните **OK**. При следующем обновлении политик предпочтение будет применено к соответствующему объекту групповой политики.

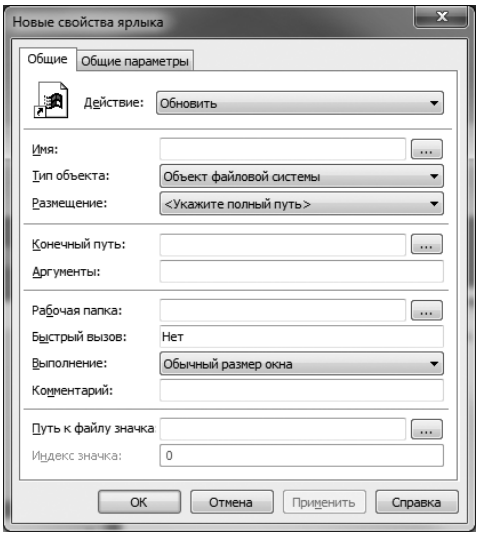

Рис. 7-3. Создание ярлыка при помощи предпочтений

В списке **Размещение (Location)** перечислены папки, в которые можно помещать ярлыки. Они описаны в табл. 7-1.

Табл. 7-1. Папки, предназначенные для работы с ярлыками

Папка	Применение
AllUsers/Рабочий стол (AllUsers/Desktop)	Ярлыки на рабочих столах всех пользователей
AllUsers/Программы (AllUsers/Programs)	Элементы меню **Программы (Programs)** для всех пользователей
AllUsers/Главное меню (AllUsers/StartMenu)	Элементы меню **Пуск (Start)** для всех пользователей
AllUsers/Автозагрузка (AllUsersStartup)	Приложения автозапуска для всех пользователей
Рабочий стол (Desktop)	Ярлыки на рабочем столе конкретного пользователя
Избранное Internet Explorer (Explorer Favorites)	Ярлыки меню **Избранное (Favorites)** конкретного пользователя
Ссылки Internet Explorer (Explorer Links)	Ссылки конкретного пользователя
Шрифты (Fonts)	Ярлыки папки **Шрифты (Fonts)** конкретного пользователя
Программы (Programs)	Элементы меню **Программы (Programs)** конкретного пользователя
Недавние (Recent)	Ярлыки недавно использованных документов конкретного пользователя
Отправить (SendTo)	Ярлыки меню **Отправить (SendTo)** конкретного пользователя
Главное меню (StartMenu)	Ярлыки меню **Пуск (Start)** конкретного пользователя
Автозагрузка (Startup)	Приложения автозапуска конкретного пользователя

Ярлыки могут указывать как на локальные файлы и файлы локальной сети, так и на удаленные ресурсы Интернета. Ярлыки локальных файлов или файлов локальной сети называются *ссылками* (link). Ярлыки ресурсов Интернета называются *URL*.

Ссылки обычно используются для запуска приложений или доступа к документам, а не для открытия URL в обозревателе. В связи с этим параметры ссылок и URL отличаются (табл. 7-2). При некорректной настройке

параметров или при задании параметров, несвойственных соответствующему приложению, ярлык может не создаться или работать некорректно.

Один из самых ценных параметров — **Аргументы (Arguments)**. Его можно использовать для передачи аргументов запускаемому приложению. При помощи этого параметра можно создать ярлык, открывающий определенный документ Microsoft Word, указав путь к исполняемому файлу Word и использовав имя файла в качестве аргумента.

Ярлыки можно запускать сочетаниями клавиш, которые должны включать в себя как минимум одну вспомогательную клавишу (Alt, Ctrl, Shift, клавиша Windows) и одну определяющую клавишу.

Табл. 7-2. Свойства ссылок

Свойство	Описание	Пример
Аргументы (Arguments)	Аргументы, передаваемые приложению, которое запускается ярлыком	«C:\Gettingstarted.doc»
Быстрый вызов (Shortcut Key)	Сочетание клавиш, активирующее ярлык. Применимо только к ярлыкам рабочего стола и меню **Пуск (Start)**	Alt+Shift+Z
Выполнение (Run)	Стиль окна приложения, запускаемого ярлыком. Доступны стили Обычный размер окна (Normal Window), Свернутое в значок (Minimized) и Развернутое на весь экран (Maximized)	Обычный размер окна (Normal Window)
Имя (Name)	Имя ярлыка	«Getting Started»
Индекс значка (Icon Index)	Устанавливает индекс значка ярлыка. Очень немногие приложения используют несколько значков, так что индекс почти всегда 0	0
Комментарий (Comment)	Комментарий к ярлыку	«Открывает документ Getting Started»
Конечный путь (Target Path)	Путь к запускаемому файлу	%WinDir%\Notepad.exe
Путь к файлу значка (Icon File Path)	Расположение значка, используемого ярлыком. Если не указано, используется ярлык по умолчанию	C:\Program Files\Internet Explorer\Iexplore.exe
Рабочая папка (Start In)	Рабочая папка приложения, запускаемого ярлыком	C:\Working
Размещение (Location)	Указывает, где создать ярлык	Рабочий стол (Desktop)

Табл. 7-2. (*окончание*)

Свойство	Описание	Пример
Тип объекта (Target Type)	Тип файла, для которого создается ярлык. Для ссылок выбирайте тип Объект файловой системы (File System Object), для URL — тип URL-адрес (URL), для ярлыков оболочки Explorer — Объект оболочки (Shell Object)	Объект файловой системы (File System Object)

Регистры можно сочетать как угодно, но комбинации не должны повторяться. К определяющим клавишам относятся буквы и цифры, а также Backspace, Clear, Del, Esc, End, Home, Enter, Space и Tab. Например, допустима комбинация Shift+Alt+G.

Ярлыки приложений, как правило, отмечаются значком приложения. Например, по умолчанию значок ярлыка для Internet Explorer — большая буква «E». При создании ярлыков к документам, как правило, используется значок по умолчанию.

Чтобы использовать другие значки, измените значение поля **Путь к файлу значка (Icon File Path)**. Обычно это имя программы, например Iexplore.exe или Notepad.exe, и индекс 0. Если по указанному пути нет исполняемого файла, задать значок не получится. Поэтому надо указывать полный путь к исполняемому файлу.

В поле **Рабочая папка (Start In)** задается рабочая папка приложения по умолчанию. Эта папка будет использоваться при первом открытии или сохранении файла.

URL-ярлыки призваны открывать Интернет-документы в соответствующем приложении. Например, веб-страницы открываются в обозревателе по умолчанию. У URL-ярлыков нет параметров **Аргументы (Arguments)**, **Рабочая папка (Start In)**, **Выполнение (Run)** и **Комментарий (Comment)**.

Создание меню и элементов меню

При помощи предпочтений легко добавлять элементы в существующие меню высшего уровня, например **Все программы (All Programs)** или **Пуск (Start)**. Для этого достаточно установить в качестве расположения ярлыка папку **Программы (Programs)** или **Главное меню (Start Menu)**.

Также при помощи предпочтений можно создавать новые меню. Используйте предпочтение **Папки (Folders)** для добавления папки в существующую специальную папку, например **Главное меню (Start Menu)** или **Программы (Programs)**. После создания меню в него можно добавить элементы, создавая ярлыки с новым меню в качестве местоположения.

Посредством предпочтений можно обновить или заменить параметры любого ярлыка или элемента меню, создав новый ярлык с тем же именем и выбрав действие **Обновить (Update)** или **Заменить (Replace)**.

Чтобы удалять ярлыки и элементы меню, создайте предпочтение с действием **Удалить (Delete)**. Меню удаляется при помощи предпочтения **Папки (Folders)** с действием **Удалить (Delete)**.

Добавление и удаление приложений автозапуска

При помощи папки Автозагрузка (Startup) можно управлять фоновыми приложениями, независимо от того кто их установил, администратор или пользователь. Программы автозапуска для текущего пользователя помещаются в папку Автозагрузка (Startup), расположенную в профиле этого пользователя (%UserProfile%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs). Общие программы автозапуска помещаются в общую папку Автозагрузка (Startup) (%SystemDrive%\ProgramData\Microsoft\Windows\Start Menu\Programs).

Чтобы добавить или удалить программу автозапуска для всех пользователей, выполните следующие действия:

1. Щелкните правой кнопкой кнопку **Пуск (Start)**, выберите команду **Открыть проводник (Open Windows Explorer)** и зайдите в скрытую папку %SystemDrive%\ProgramData\Microsoft\Windows\Start Menu.
2. Щелкните папку Программы (Programs) в главном меню и зайдите в папку Автозагрузка (Startup).
3. Теперь добавляйте и удаляйте программы автозапуска для всех пользователей. Чтобы добавить программу в меню автозапуска, поместите в эту папку ее ярлык. Для удаления программы из меню автозапуска удалите соответствующий ярлык.

Чтобы добавить или удалить программу автозапуска для конкретного пользователя, выполните следующие действия:

1. Зайдите в систему от имени пользователя. Щелкните правой кнопкой кнопку **Пуск (Start)**, выберите команду **Открыть проводник (Open Windows Explorer)** и зайдите в скрытую папку %UserProfile%\AppData\Roaming\Microsoft\Windows\Start Menu.
2. Щелкните папку Программы (Programs) главного меню и зайдите в папку Автозагрузка (Startup).
3. Теперь добавляйте и удаляйте программы автозапуска для конкретного пользователя. Чтобы добавить программу в меню автозапуска, поместите ее ярлык в эту папку. Для удаления программы из меню автозапуска удалите соответствующий ярлык.

Примечание На самом деле входить в систему от имени пользователя необязательно, просто так легче провести настройку. Вместо этого можно зайти в папку Пользователи (Users) на системном диске и найти там нужную папку в профиле пользователя. Они называются так же, как учетные записи.

При помощи предпочтений групповых политик вы указываете, какие приложения должны запускаться при входе пользователя в систему, создавая для них ярлыки в папке AllUsers/Автозагрузка (AllUsers/Startup) или

Автозагрузка (Startup). Папка AllUsers/Автозагрузка (AllUsers/Startup) содержит ярлыки программ, запускающихся при входе в систему любого пользователя. Папка Автозагрузка (Startup) содержит ярлыки приложений, запускающиеся при входе в систему конкретного пользователя.

При создании ярлыков чаще других задаются параметры **Имя (Name)**, **Тип объекта (Target Type)**, **Размещение (Location)** и **Конечный путь (Target Path)**. Порой также приходится задавать рабочую папку и аргументы командной строки.

Для удаления приложения из меню автозапуска создайте предпочтение с действием **Удалить (Delete)**.

Настройка панели задач

Панель задач обеспечивает быстрый доступ к часто используемой информации и запущенным приложениям. Есть несколько способов изменить поведение и свойства панели задач. Об основных рассказано в этом разделе.

Зачем нужна панель задач

Панель задач нередко недооценивают, уделяя ее настройке недостаточное внимание. Между тем, она используется постоянно, обеспечивая быстрый доступ практически ко всему, что связано с ОС Windows. Если у пользователей возникают проблемы с доступом к компонентам Windows или приложениям, задумайтесь о том, чтобы настроить панель задач под их нужды. Панель задач может содержать несколько панелей инструментов, способных разными способами облегчить жизнь пользователя.

Порой можно значительно увеличить эффективность работы, просто добавив на панель задач часто используемое приложение. Например, многие постоянно тратят время на поиск документов. Они копаются в Веб или в локальной сети в поисках нужной информации, открывают документы Microsoft Word, Excel, PowerPoint или других приложений, отыскивая документы по одному, запускают приложения для чтения этих документов. Добавив на панель задач панель **Адрес (Address)**, вы дадите пользователям возможность обращаться к документам напрямую. Соответствующее приложение запустится автоматически; достаточно просто ввести путь к документу и нажать Enter. С течением времени накопится история (адресная панель запоминает недавние документы), что еще больше облегчит доступ к необходимой информации.

Вынесение ярлыков на панель задач

В Windows 7 нет панели быстрого запуска. Вместо этого имеется возможность напрямую вынести ярлыки часто используемых программ на панель задач. Это можно сделать в любой момент при помощи меню **Пуск (Start)**. Щелкните правой кнопкой ярлык, который хотите добавить на панель задач, и выберите команду **Закрепить программу в панели задач (Pin To Taskbar)**.

Положение ярлыков, вынесенных на панель задач, можно изменять перетаскиванием мышью. Чтобы убрать ярлык с панели задач, щелкните его правой кнопкой и выберите команду **Изъять программу из панели задач (Unpin This Program From Taskbar)**.

Изменение размера и расположения панели задач

По умолчанию панель задач размещена внизу экрана и имеет размер, позволяющий видеть одну строку кнопок. Если панель задач не закреплена, ее можно прикрепить к любому краю экрана и изменить ее размер. Чтобы переместить панель задач, перетащите ее мышью к другому краю экрана. При перетаскивании панель задач «перескакивает» к ближайшему краю рабочего стола. Если вы отпустите кнопку мыши, панель останется на новом месте. Чтобы изменить размер панели задач, подведите указатель к краю панели задач и перетащите его вверх или вниз.

Автоматическое скрытие, закрепление и управление видимостью панели задач

Есть несколько способов управления видимостью панели задач. Можно включить ее автоматическое скрытие: панель задач не будет отображаться в те моменты, когда она не используется. Можно закрепить панель задач, чтобы случайно не передвинуть ее и не поменять ее размер, или поместить панель задач в определенное место и придать ей определенный вид. Поэтому сначала разместите панель задач, настройте ее размер, а затем закрепите. В этом случае панель задач всегда будет на одном месте, и пользователям не придется ее искать.

Чтобы настроить панель задач, выполните следующие действия:

1. Щелкните панель задач правой кнопкой и выберите команду **Свойства (Properties)**.
2. В диалоговом окне **Свойства панели задач и меню «Пуск» (Taskbar And Start Menu Properties)** перейдите на вкладку **Панель задач (Taskbar)**.
3. Задайте параметры в разделе **Оформление панели задач (Taskbar Appearance)**. Панель задач можно закрепить, включить автоматическое скрытие и уменьшить размер значков.
4. Выберите в списке **Положение панели задач на экране (Taskbar Location On Screen)** подходящее положение панели задач. Доступны варианты **Снизу (Bottom)**, **Слева (Left)**, **Справа (Right)** и **Сверху (Top)**.
5. При помощи списка **Кнопки панели задач (Taskbar Buttons)** укажите, будут ли группироваться кнопки на панели задач и будут ли отображаться метки. Чтобы всегда группировать кнопки одного типа и скрывать метки, выберите вариант **Всегда группировать, скрывать метки (Always Combine, Hide Labels)**. Чтобы группировать кнопки, только когда панель задач заполнена, выберите **Группировать при заполнении панели задач (Combine When Taskbar Is Full)**. Чтобы запретить группировку, выберите **Не группировать (Never Combine)**.

6. Чтобы получить возможность временно уменьшить окна и отображать рабочий стол при наведении указателя на правое окончание панели задач, выберите **Использовать Aero Peek для предварительного просмотра рабочего стола (Use Aero Peek To Preview The Desktop)**.
7. Щелкните **OK**.

Совет Закрепление панели задач очень полезно. Закрепив правильно настроенную панель задач, вы избавите пользователей от случайного изменения ее настроек. Для изменения настроек панели задач достаточно щелкнуть ее правой кнопкой, выбрать команду **Свойства (Properties)** и сбросить флажок **Закрепить панель задач (Lock The Taskbar)**.

Управление областью уведомлений

Область уведомлений, или системная область (system tray), находится на правом краю панели задач. В ней отображаются часы, а также уведомления приложений. По умолчанию уведомления идут от Центра действий (Action Center) и консоли Сеть (Network). При наведении указателя мыши на значок в области уведомлений появляется всплывающая подсказка с информацией о текущем состоянии приложения. Для управления приложением щелкните его значок правой кнопкой. Появится список возможных действий, свой для каждого приложения.

Область уведомлений также можно настроить, задав параметры, управляющие отображением системных значков — часов, регулятора громкости, сетевых подключений и других.

Управление отображением значков в области уведомлений

В области уведомлений могут отображаться как системные значки, так и значки приложений. Значки приложений появляются в области уведомлений в нескольких случаях. Значки некоторых программ, управляемых самой ОС Windows, например Центра действий (Action Center), появляются в системной области при наличии уведомлений. Значок в области уведомлений размещают и программы, запускаемые при загрузке системы и работающие в фоновом режиме, например антивирусы. Отображение значков можно включить или отключить через настройки соответствующих приложений, но в Windows 7 есть и общий интерфейс для управления значками в области уведомлений. Для каждого приложения можно указать, как и когда будут отображаться его значки.

Чтобы настроить отображение значков в области уведомлений, выполните следующие действия:

1. Щелкните правой кнопкой мыши панель задач и выберите команду **Свойства (Properties)**.
2. В диалоговом окне **Свойства панели задач и меню «Пуск» (Taskbar And Start Menu Properties)** перейдите на вкладку **Панель задач (Taskbar)**.

3. Чтобы открылась страница **Значки области уведомлений (Notification Area Icons)**, показанная на рис. 7-4, щелкните кнопку **Настроить (Customize)** в разделе **Область уведомлений (Notification Area)**.

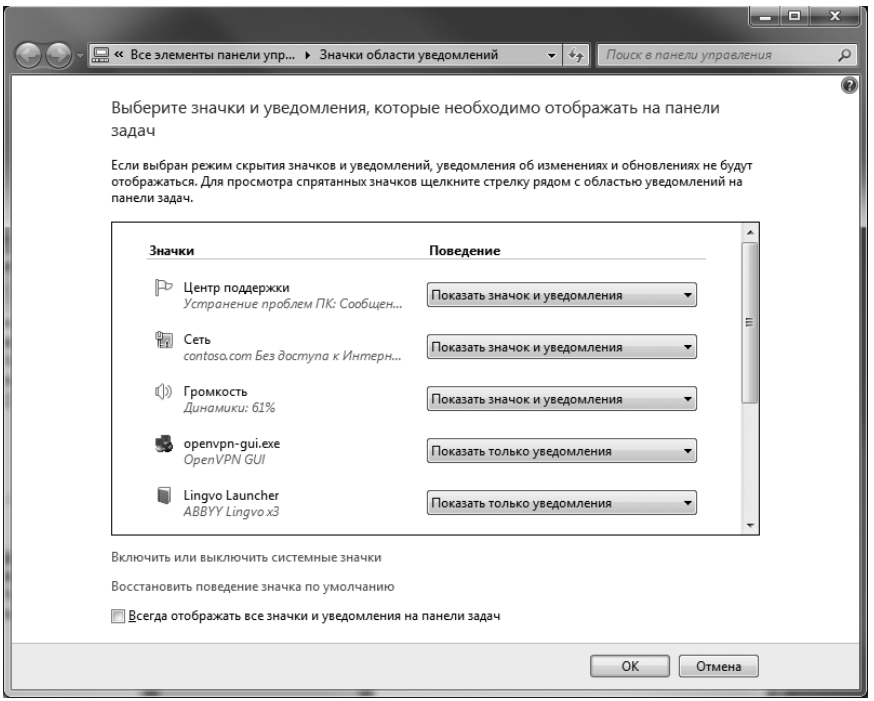

Рис. 7-4. Настройка значков уведомлений

4. Чтобы значки отображались, установите флажок **Всегда отображать все значки и уведомления на панели задач (Always Show All Icons And Notifications On The Taskbar)** и щелкните **OK**. Пропустите оставшиеся шаги.
5. Если нужно изменить действие области уведомлений, сбросьте флажок **Всегда отображать все значки и уведомления на панели задач (Always Show All Icons And Notifications On The Taskbar)** и выберите нужный вариант. Для каждой записи в левом столбце в правом столбце есть несколько вариантов выбора:
   - **Скрыть значок и уведомления (Hide Icon And Notifications)** Никогда не показывать значок и уведомления.
   - **Показать только уведомления (Only Show Notifications)** Показывать только уведомления.
   - **Показать значок и уведомления (Show Icon And Notifications)** Всегда показывать значок и уведомления.
6. Завершив настройку уведомлений, два раза щелкните **OK**.

Настройка панелей инструментов

На панели задач могут использоваться несколько панелей инструментов. Большинство пользователей знакомо с панелью быстрого запуска из предшествующих версий Windows. Она предназначалась для быстрого доступа к часто используемым программам и рабочему столу. В Windows 7 на смену ей пришел набор панелей инструментов, кроме того, пользователи могут создавать собственные панели инструментов.

Отображение панелей инструментов

На панели задач могут находиться следующие панели инструментов:

- **Адрес (Address)** В поле **Адрес (Address)** можно ввести URL или любой другой адрес объекта, к которому нужен доступ. Он может быть в Интернете, в локальной сети или на компьютере. Если указан полный путь к файлу, для его отображения файла будет запущено приложение, ассоциированное с указанным типом.
- **Ссылки (Links)** Предоставляет доступ к папке **Ссылки (Links)** из меню **Избранное (Favorites)** Internet Explorer. Чтобы добавить ссылку на файл, веб-страницу или другой ресурс, перетащите на эту панель инструментов соответствующий ярлык. Для удаления ссылки щелкните ее правой кнопкой и выберите команду **Удалить (Delete)** и подтвердите это действие, щелкнув **Да (Yes)**.
- **Рабочий стол (Desktop)** Предоставляет доступ к ярлыкам рабочего стола, чтобы не нужно было сворачивать приложения или нажимать на кнопку отображения рабочего стола в правом конце панели задач.

Для отображения или скрытия панелей инструментов выполните следующие действия:

1. Щелкните панель задач правой кнопкой мыши.
2. Раскройте подменю **Панели инструментов (Toolbars)** и выберите имя панели задач из списка. Это действие включит или отключит отображение панели.

Совет По умолчанию на всех панелях инструментов отображается их название. Это можно отменить, щелкнув панель правой кнопкой и выбрав команду **Показать заголовок (Show Title)**, чтобы снять флажок с этого пункта. Если панель инструментов закреплена, сначала ее нужно разблокировать, сняв флажок команды **Закрепить панель задач (Lock The Taskbar)** из контекстного меню.

Создание панелей инструментов

Пользователи могут создавать и собственные панели инструментов, основанные на существующих папках. Чаще всего создаются панели инструментов, указывающие на общий сетевой ресурс. Например, если у всех пользователей есть доступ к папке CorpData с персональной информацией, имеет смысл создать панель инструментов, указывающую на этот ресурс. Для до-

ступа к нему пользователю достаточно будет щелкнуть мышью соответствующую кнопку на панели инструментов.

Чтобы создать панель инструментов, выполните следующие действия:

1. Щелкните панель задач правой кнопкой мыши. Раскройте подменю **Панели (Toolbars)** и выберите команду **Создать панель инструментов (New Toolbar)**. Откроется диалоговое окно **Новая панель инструментов — Выбор папки (New Toolbar—Choose A Folder)**, похожее на диалоговое окно **Открыть (Open)**.
2. Найдите папку, на которой будет основана новая панель инструментов.
3. Щелкните **Выбор папки (Select Folder)**, и папка появится на панели задач в виде панели инструментов. Когда вы добавите ярлыки на эту панель, ярлыки будут добавлены в соответствующую папку. Аналогично, при удалении элементов с панели инструментов они будут удаляться и из папки.

Примечание Есть две новости про пользовательские панели инструментов — хорошая и плохая. Хорошая состоит в том, что большинство пользователей находят их весьма полезными. Плохая — если пользователь закроет такую панель инструментов, чтобы вернуть ее на панель задач, ее придется создавать заново.

Темы рабочего стола

Темы рабочего стола — это набор фоновых рисунков и звуков, значков и других инструментов настройки рабочей среды. Администраторы, как правило, ненавидят темы; пользователи, как правило, их обожают. В этом разделе вы узнаете, как применять, настраивать и удалять темы.

Применение и удаление тем

Существуют темы нескольких типов. Часть тем устанавливается вместе с ОС. Для применения темы выполните следующие действия:

1. Щелкните правой кнопкой мыши свободную область рабочего стола и выберите команду **Персонализация (Personalize)**. Откроется одноименная категория панели управления, показанная на рис. 7-5.
2. Выберите тему из списка. Если вы хотите использовать тему с сайта Майкрософт, щелкните команду **Другие темы в Интернете (Get More Themes Online)**, чтобы открыть веб-сайт Майкрософт в обозревателе по умолчанию. Чтобы использовать тему из сети, выделите ее и щелкните **Сохранить (Save)**. Выберите место для сохранения. По окончании загрузки щелкните кнопку **Открыть (Open)** в окне **Загрузка завершена (Download Complete)**. Теперь тема готова к использованию.
3. В нижней части окна **Персонализация (Personalize)** показаны варианты внешнего вида темы. Щелкните нужный вариант.

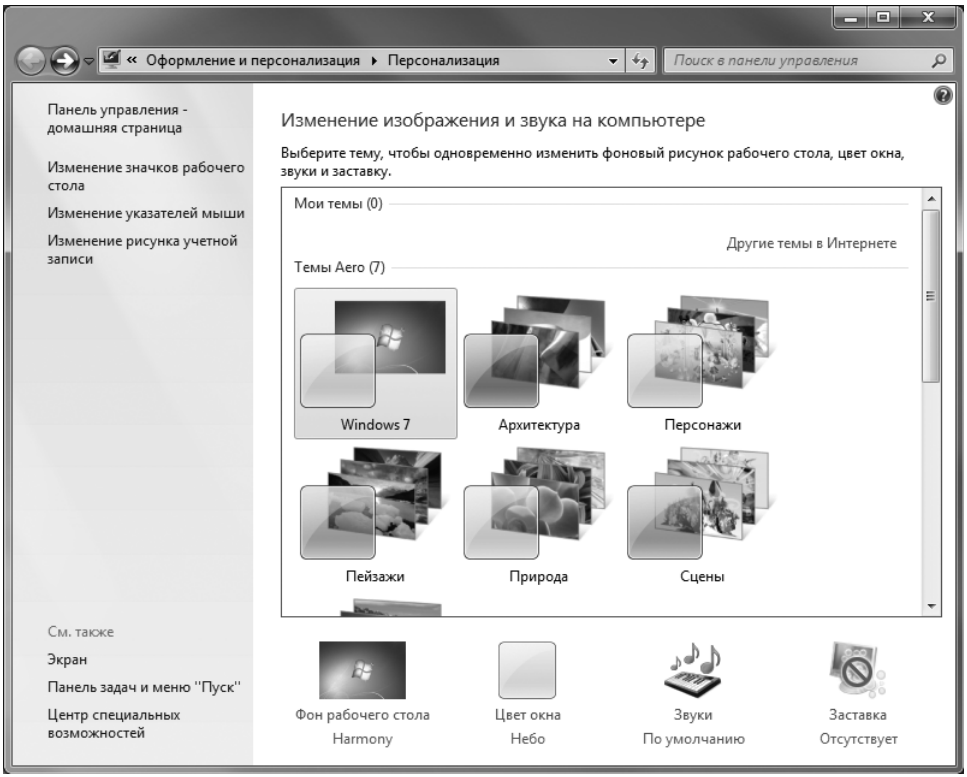

Рис. 7-5. Используйте окно Персонализация (Personalization) для настройки тем, параметров экрана и др.

Чтобы восстановить исходную тему рабочего стола, выполните следующие действия:

1. Щелкните правой кнопкой мыши свободную часть рабочего стола и выберите команду **Персонализация (Personalize)**.
2. Выберите тему **Windows 7** или **Windows 7 — упрощенный стиль (Windows 7 Basic)**.

Совет Отображением тем управляет служба Themes. При необходимости быстро отключить темы, не изменяя их настроек, например при решении каких-нибудь проблем, просто остановите эту службу, введя в командной строке с повышенными полномочиями команду **net stop themes**. Для перезапуска службы Themes введите в командную строку с повышенными полномочиями **net start themes**.

Настройка и сохранение тем

Тема изменяет многие параметры рабочего стола. Как правило, пользователю нравится тема в целом, но не нравится какая-то конкретная ее деталь, например звуки. Чтобы решить этот вопрос, измените нелюбимый пользователем параметр и сохраните обновленную тему, чтобы впоследствии к ней можно было вернуться.

Темы управляются в окне **Персонализация (Personalization)**, для открытия которого служит одноименная команда из контекстного меню рабочего стола. Основные параметры, затрагиваемые темами, таковы:

- **Заставки (Screen savers)** Чтобы изменить заставку, щелкните команду **Заставка (Screen Saver)**. В диалоговом окне **Параметры экранной заставки (Screen Saver Settings)**, выберите нужную заставку или вариант **Нет (None)**, чтобы ее отключить. Щелкните **OK**.
- **Звуки (Sounds)** Чтобы изменить звуки, щелкните команду **Звуки (Sounds)**. В диалоговом окне **Звук (Sound)** выберите в списке **Звуковая схема (Sound Scheme)** подходящий набор звуков. Чтобы вернуться к стандартным звукам, выберите вариант **По умолчанию (Windows Default)**. Для отключения звуков выберите вариант **Без звука (No Sounds)**. Щелкните **OK**. Скорее всего, стоит также снять флажок **Проигрывать мелодию запуска Windows (Play Windows Startup Sound)**.
- **Указатели мыши (Mouse pointers)** Для изменения указателей мыши щелкните команду **Изменение указателей мыши (Change Mouse Pointers)**. В диалоговом окне **Свойства: Мышь (Mouse Properties)** на вкладке **Указатели (Pointers)** расположен список **Схема (Scheme)**. Выберите подходящий набор указателей и щелкните **OK**.
- **Фон рабочего стола (Desktop background)** Для изменения фонового рисунка рабочего стола выберите команду **Фон рабочего стола (Desktop Background)**. Выберите место расположения фоновых рисунков в списке **Расположение изображения (Picture Location)**. Щелкните **Обзор (Browse)**, чтобы открыть диалоговое окно **Обзор папок (Browse For)**. Также можно воспользоваться фоновыми рисунками Windows, по умолчанию расположенными в папке %SystemRoot%\Web\Wallpaper. Выберите рисунок и его расположение, а затем щелкните **Сохранить изменения (Save Changes)**.
- **Цветовые схемы (Color schemes)** Для изменения цветовых схем щелкните **Цвет окна (Window Color)**. Щелкните нужный цвет, установите или сбросьте флажок **Включить прозрачность (Enable Transparency)** и щелкните **Сохранить изменения (Save Changes)**.

Удаление пользовательских тем

Темы, установленные пользователями, могут занимать много места на жестком диске. Чтобы удалить тему и относящиеся к ней файлы, выполните следующие действия:

1. Щелкните правой кнопкой мыши свободную область рабочего стола и выберите команду **Персонализация (Personalize)**.
2. Найдите тему в разделе **Мои темы (My Themes)**, щелкните ее правой кнопкой мыши и выберите команду **Удалить тему (Delete Theme)**. Windows удалит тему и относящиеся к ней файлы.

Совет По умолчанию файлы тем, установленных Windows, размещаются в папке %WinDir%\Resources\Themes, а темы, созданные пользователями — в их профилях. Чтобы определить, сколько места занимают темы, проверьте объем этих папок с подпапками. Не стоит вручную удалять файлы из этих папок. Воспользуйтесь описанным выше способом.

Оптимизация рабочего стола

Когда вы запускаете программу или открываете папку, соответствующее окно открывается на рабочем столе. Окна можно упорядочить, вызвав контекстное меню панели задач и выбрав в нем команду **Окна каскадом (Cascade Windows)**, **Отображать окна стопкой (Show Windows Stacked)** или **Отображать окна рядом (Show Windows Side By Side)**. Если выберете команду **Показать рабочий стол (Show The Desktop)**, система свернет все открытые окна и покажет рабочий стол. Команда **Показать все окна (Show Open Windows)** вернет свернутые окна в их предшествующее состояние.

На рабочем столе можно разместить файлы, папки и ярлыки. Файл или папка, сохраненные на рабочем столе, отображаются на нем. Файл или папка, перетащенные из окна проводника Windows на рабочий стол, там и останутся. Чтобы положить файл или папку на рабочий стол, щелкните соответствующий объект правой кнопкой мыши, раскройте подменю **Отправить (Send To)** и выберите команду **Рабочий стол (создать ярлык) (Desktop (Create Shortcut))**.

Наряду с этими простыми приемами существует еще много других методов оптимизации рабочей среды. Один из них — добавить в стандартный фон рабочего стола логотип компании или другой символ. В частности, это удобно, когда компания выдает сотрудникам портативные компьютеры. Например, можно сделать логотип с надписью вроде «Выдано техническим подразделением». Можно также использовать гаджеты Windows для размещения на рабочем столе собственного содержимого.

Фон рабочего стола

В Windows 7 имеется несколько наборов фоновых рисунков, которые хранятся в подпапках папки %WinDir%\Web\Wallpaper. Например, изображения в папке Пейзажи (Landscapes) отображаются как набор фоновых рисунков с пейзажами.

В качестве фоновых рисунков могут использоваться изображения в форматах .bmp, .gif, .jpg, .jpeg, .dib и .png. Добавьте изображение в одном из этих форматов в любую подпапку папки %WinDir%\Web\Wallpaper, и оно появится в соответствующей группе фоновых рисунков. Чтобы создать новую группу, создайте новую подпапку в папке %WinDir%\Web\Wallpaper и поместите туда соответствующие изображения.

Чтобы установить фон рабочего стола, выполните следующие действия:

1. Щелкните правой кнопкой мыши свободную область рабочего стола и выберите команду **Персонализация (Personalize)**. В окне **Персона-**

лизация (Personalization) щелкните **Фон рабочего стола (Desktop Background)**. Откроется страница **Фоновый рисунок рабочего стола (Desktop Background)**, показанная на рис. 7-6.

2. Выбрав в списке **Расположение изображения (Picture Location)** вариант **Фоны рабочего стола Windows (Windows Desktop Backgrounds)**, вы увидите несколько групп изображений. Для выбора нужной группы используйте полосу прокрутки.
3. Щелкните нужное изображение. Если такового не обнаружится, воспользуйтесь кнопкой **Обзор (Browse)**, чтобы найти подходящее изображение в файловой системе или сети.

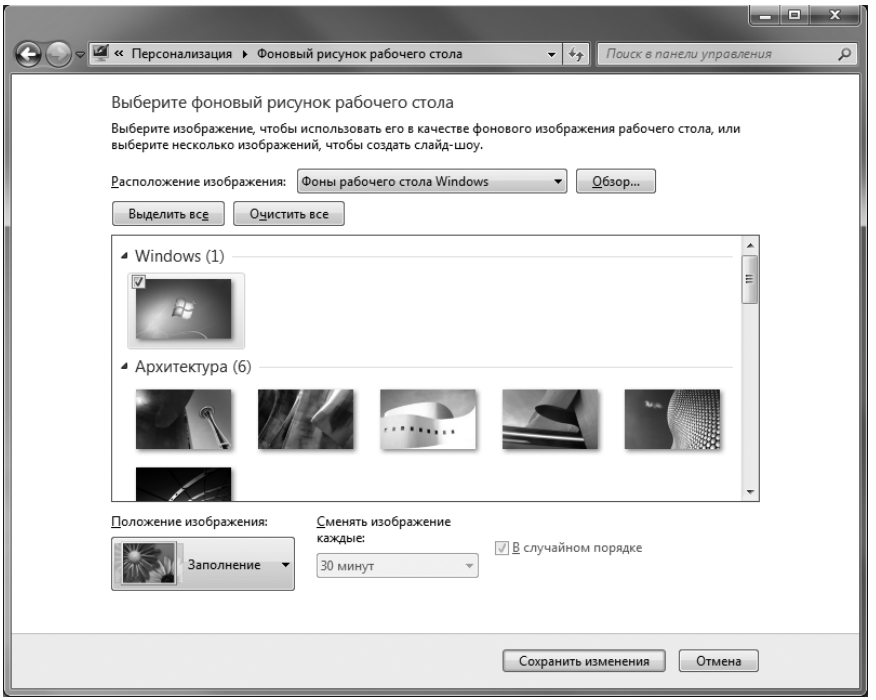

Рис. 7-6. Выбор фонового рисунка рабочего стола

4. Выберите способ отображения рисунка в списке **Положение изображения (Picture Position)**. Доступны следующие варианты:
   - **По центру (Center)** Фоновый рисунок центрируется. В областях, в которые не попадает рисунок, используется текущий цвет рабочего стола.
   - **Заполнение (Fill)** Изображение полностью закрывает рабочий стол. Стороны изображения могут оказаться обрезанными.
   - **По размеру (Fit)** Рисунок масштабируется с сохранением пропорций. Этот вариант подходит для фотографий и больших изображений, которым нежелательно растяжение по высоте или длине.

- **Растянуть (Stretch)** Рисунок растягивается до заполнения фона. Пропорции, по возможности, сохраняются; для заполнения пустого места используется растяжение по высоте.
- **Замостить (Tile)** Рабочий стол закрывается копиями изображения. Хорошо подходит для маленьких изображений и значков.

5. Закончив работу с фоном рабочего стола, щелкните **Сохранить изменения (Save Changes)**.

Работа со значками на рабочем столе

По умолчанию на рабочем столе присутствует только **Корзина (Recycle Bin)**. Дважды щелкнув ее, можно просмотреть файлы, подготовленные к удалению. Выбрав в контекстном меню команду **Очистить корзину (Empty The Recycle Bin)** вы окончательно удалите содержимое корзины.

Другие значки, которые можно добавить на рабочий стол, таковы:

- **Компьютер (Computer)** Двойной щелчок этого значка открывает окно, предоставляющее доступ к жестким дисками и устройствам со сменным носителем. Выбрав в контекстном меню этого значка команду **Управление (Manage)**, вы откроете консоль Управление компьютером (Computer Management). Команда **Подключить сетевой диск (Map Network Drive)** позволит подключиться к общим сетевым папкам. Команда **Отключить сетевой диск (Disconnect Network Drive)** служит для отключения от общей сетевой папки.
- **Панель управления (Control Panel)** Дважды щелкнув этот значок, вы откроете панель управления, предоставляющую доступ к настройке системы и инструментам управления.
- **Сеть (Network)** Дважды щелкнув этот значок, вы откроете окно, предоставляющее доступ к компьютерам и другим устройствам сети. Команда **Подключить сетевой диск (Map Network Drive)** из контекстного меню этого значка позволит подключиться к общим сетевым папкам. Команда **Отключить сетевой диск (Disconnect Network Drive)** служит для отключения от общей сетевой папки.
- **Файлы пользователя (User's Files)** Двойной щелчок этого значка открывает личную папку.

Чтобы добавить или удалить значок рабочего стола, выполните следующие действия:

1. Щелкните правой кнопкой свободную область рабочего стола и выберите команду **Персонализация (Personalize)**.
2. Щелкните **Изменение значков рабочего стола (Change Desktop Icons)**. Откроется диалоговое окно **Параметры значков рабочего стола (Desktop Icon Settings)**, показанное на рис. 7-7.

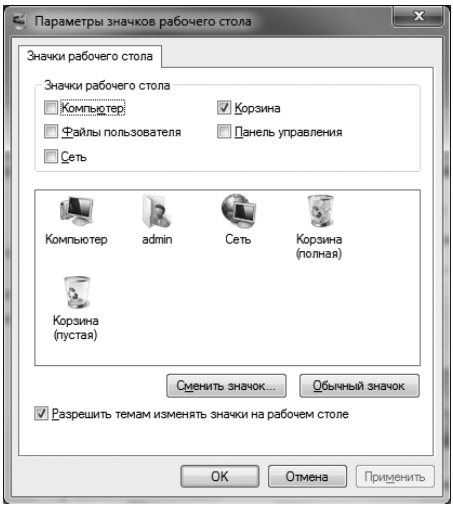

Рис. 7-7. Выберите значки для отображения на рабочем столе

3. В диалоговом окне **Параметры значков рабочего стола (Desktop Icon Settings)** есть флажки для каждого стандартного значка. Чтобы удалить значок, сбросьте флажок, чтобы добавить его, установите флажок.
4. Щелкните **OK**.

Чтобы спрятать все значки на рабочем столе, щелкните правой кнопкой мыши свободную область рабочего стола, раскройте подменю **Вид (View)** и выберите команду **Отображать значки рабочего стола (Show Desktop Icons)**. Если эту процедуру повторить, спрятанные значки будут восстановлены.

Чтобы удалить значок или ярлык с рабочего стола, щелкните его правой кнопкой мыши и выберите команду **Удалить (Delete)**. Затем подтвердите действие, щелкнув **Да (Yes)**. Обратите внимание: если удалить с рабочего стола значок (не ярлык) папки или файла, файл или папка со всем содержимым будут удалены.

Что делать и чего не делать с заставкой

Заставки включаются, когда компьютер простаивает определенное время. Изначально они задумывались как способ спасти ЭЛТ-мониторы от износа за счет отображения постоянно меняющейся картинки. Современные дисплеи не страдают этой проблемой, однако заставки уже прочно заняли свое место. Правда, теперь основное назначение заставок — автоматическая блокировка системы на время отсутствия пользователя.

Защита заставки паролем

Пароль предотвращает неавторизованный доступ к компьютеру. Это важно для защиты как личных данных пользователя, так и для защиты интеллектуальной собственности организации. Администратор обязан настроить пароль для всех заставок на компьютерах

Чтобы защитить заставку паролем, выполните следующие действия:

1. Щелкните правой кнопкой свободную область рабочего стола и выберите команду **Персонализация (Personalize)**.
2. Щелкните ссылку **Заставка (Screen Saver)**, чтобы открыть диалоговое окно **Параметры экранной заставки (Screen Saver Settings)**, показанное на рис. 7-8.

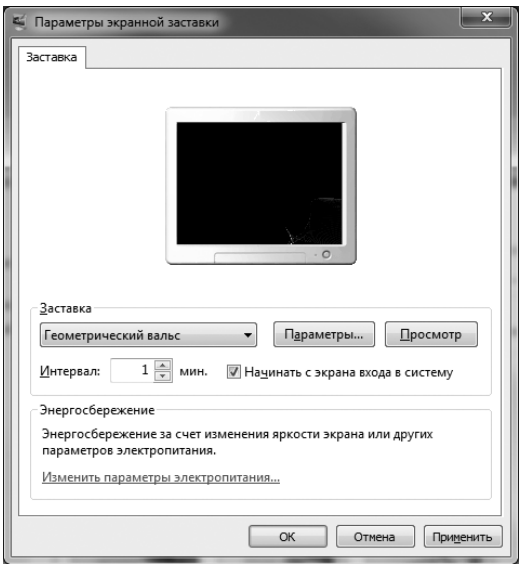

Рис. 7-8. Защитите заставку паролем, чтобы обеспечить безопасность данных

3. Выберите заставку в списке **Заставка (Screen Saver)**. Чтобы отключить заставку, выберите вариант **Нет (None)** и пропустите оставшиеся шаги.

Ближе к реальности К сожалению, заставки могут быть весьма требовательными к ресурсам компьютера, что приведет к лишним затратам энергии и занятости памяти и процессора. Некоторые заставки, особенно трехмерные, очень сильно загружают процессор, что связано с большой сложностью обработки трехмерных изображений. Советы по сокращению загруженности ресурсов при работе заставок вы найдете в двух следующих разделах.

4. Установите флажок **Начинать с экрана входа в систему (On Resume, Display Logon Screen)**.
5. Укажите в поле **Интервал (Wait)**, после какого времени простоя будет включаться заставка. Разумное значение — между десятью и пятнадцатью минутами.
6. Щелкните **OK**.

Примечание Одна из лучших заставок — это слайд-шоу, в котором по умолчанию используются изображения из библиотеки Изображения (Pictures). Однако вы вольны выбрать в качестве источника изображений любую папку. Также можно выбрать скорость слайд-шоу и включить показ в случайном порядке.

Сокращение использования ресурсов

Не стоит использовать «тяжелые» заставки на компьютерах под управлением Windows 7, занятых фоновой работой или сетевыми задачами, наподобие печати. На таких компьютерах стоит использовать простую заставку вроде пустого экрана. Также можно уменьшить ресурсоемкость тяжелых заставок. Обычно это достигается за счет уменьшения числа прорисовок и обновлений изображения.

Чтобы сократить использование ресурсов, выполните следующие действия:

1. Щелкните правой кнопкой свободную область рабочего стола и выберите команду **Персонализация (Personalize)**.
2. Щелкните ссылку **Заставка (Screen Saver)**, чтобы открыть диалоговое окно **Параметры экранной заставки (Screen Saver Settings)**.
3. Если вам нужно сэкономить ресурсы без дополнительных настроек, выберите простую заставку, наподобие пустого экрана или эмблемы Windows.
4. Чтобы уменьшить потребление ресурсов трехмерными заставками, выберите нужную заставку и щелкните кнопку **Параметры (Settings)**. В открывшемся диалоговом окне уменьшите значения параметров **Разрешение (Resolution)**, **Размер (Size)**, **Скорость вращения (Rotational Speed)** или других аналогичных полях, управляющих прорисовкой и обновлением заставки.
5. Щелкните **OK** во всех открытых диалоговых окнах.

Настройка энергосбережения для мониторов

Многие новые мониторы способны отключаться после некоторого периода простоя для экономии энергии. Использование этой возможности сократит счета компании за электричество, поскольку в ходе работы мониторы потребляют довольно много энергии. В некоторых случаях эта возможность используется автоматически, однако для этого необходимо, чтобы система правильно определила монитор и установила необходимый драйвер.

Энергосбережение особенно важно на портативных компьютерах при работе от аккумулятора. Настроив отключение экрана при простое, вы увеличите время автономной работы компьютера.

Чтобы настроить параметры энергосбережения, выполните следующие действия:

1. Щелкните правой кнопкой свободную область рабочего стола и выберите команду **Персонализация (Personalize)**.
2. Щелкните команду **Заставка (Screen Saver)**, чтобы открыть диалоговое окно **Параметры экранной заставки (Screen Saver Settings)**.
3. Щелкните ссылку **Изменить параметры электропитания (Change Power Settings)**. Откроется страница **Электропитание (Power Options)** панели управления.

4. Щелкните **Настройка подключения дисплея (Choose When To Turn Off Display)**.
5. Выберите в списке время, по прошествии которого нужно отключать монитор.
6. Щелкните **Сохранить изменения (Save Changes)**.

Примечание Некоторые параметры могут быть недоступны, если монитор не поддерживает энергосбережение. Если настройка проводится с удаленного монитора и он отличается от того, с которым будет работать пользователь, подключите монитор, аналогичный пользовательскому, и повторите процесс.

Ближе к реальности Как правило, монитор стоит отключать после 15-20 минут простоя. На моем офисном компьютере заставка включается после семи минут простоя, а монитор отключается после 15 минут простоя. На ноутбуке это время составляет 5 и 10 минут, соответственно.

Внешний вид экрана и параметры изображения

Внешний вид и параметры изображения значительно влияют на восприятие рабочего стола Windows 7 и его графических элементов. К параметрам внешнего вида относятся параметры окон, кнопок, цветов и шрифтов. Параметры изображения — это разрешение, количество цветов, частота обновления, аппаратное ускорение и настройки цветов.

Настройка цвета и внешнего вида окон

В интерфейсе Windows Aero есть возможность прорисовки прозрачных границ окон, динамических миниатюр, плавного перемещения окон, анимации при закрытии и открытии окон и пр. В ходе установки Windows 7 проверяет производительность и на основании этого анализа определяет, подходит ли компьютер для использования Windows Aero, включая следующие факторы:

- Поддержка модели WDDM (Windows Display Driver Model). В Windows Vista появилась WDDM 1.0. В Windows 7 большую производительность обеспечат драйверы изображения с поддержкой WDDM 1.1. Они сэкономят до 50% памяти на прорисовке окон.
- Поддержка DirectX в графическом ускорителе с не менее 128 Мб видеопамяти. В WDDM 1.1 поддерживается DirectX 11 с новыми возможностями и более высокой производительностью.

Ближе к реальности Определить, сколько в системе доступно видеопамяти и поддерживает ли видеоадаптер WDDM, можно при помощи консоли Счетчики и средства производительности (Performance Information And Tools). В панели управления выберите в списке **Просмотр (View By)** способ просмотра **Мелкие значки (Small Icons)** или **Крупные значки(Large Icons)**, чтобы открыть страницу **Все элементы панели управления (All Control Panel Items)**. Щелкните ссылку **Счетчики и средства производительности (Performance Information And Tools)**, а затем — ссылку **Отображение и печать подробных сведений о производительности компьютера и системе (View And Print Detailed Performance And System Information)**. В элементе

Тип видеоадаптера (Component) из раздела **Графика (Graphics)** будет показан тип видеоадаптера и уровень поддержки WDDM. В разделе **Графика (Graphics)** есть и другие важные сведения, включая объем используемой видеопамяти и поддерживаемую версию DirectX.

На совместимых системах Windows 7 использует Aero по умолчанию. Интерфейс Aero позволяет настраивать три ключевые детали внешнего вида: цветовые схемы, прозрачность окон и интенсивность цвета. Для их настройки выполните следующие действия:

1. Щелкните правой кнопкой свободную область рабочего стола и выберите команду **Персонализация (Personalize)**.
2. Щелкните ссылку **Цвет окна (Window Color)**, чтобы открыть страницу **Цвет и внешний вид окна (Window Color And Appearance)**, показанную на рис. 7-9.

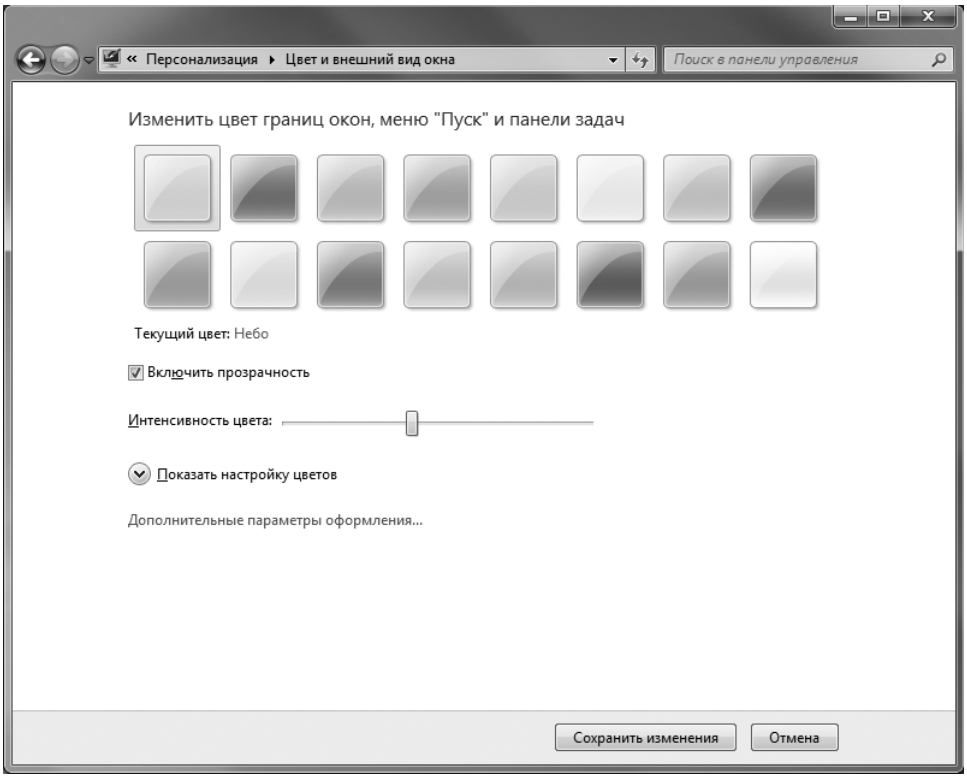

Рис. 7-9. Настройте внешний вид при помощи страницы Цвет и внешний вид окна (Window Color And Appearance)

3. Измените цвет окон, щелкнув один из доступных вариантов. Чтобы создать собственный цвет, щелкните кнопку **Показать настройку цветов (Show Color Mixer)** и создайте цвет при помощи бегунков **Оттенок (Hue)**, **Насыщенность (Saturation)** и **Яркость (Brightness)**.

4. Для включения эффекта прозрачного стекла (на компьютерах с достаточным объемом видеопамяти) установите флажок **Включить прозрачность (Enable Transparency)**. Края окон станут полупрозрачными.

Совет Прозрачность использует больше ресурсов, чем другие графические эффекты, в особенности на компьютерах с драйвером изображения WDDM 1.0. При наличии проблем, связанных с нехваткой памяти или перегруженностью процессора, прозрачность стоит отключить. В WDDM 1.1 производительность существенно улучшена, и для прозрачности требуется меньше ресурсов.

5. Задайте интенсивность цвета и уровень прозрачности при помощи бегунка **Интенсивность цвета (Color Intensity)**. Увеличьте интенсивность, чтобы сделать цвет насыщеннее и уменьшить прозрачность. Уменьшите насыщенность, чтобы сделать цвет тусклее и повысить прозрачность.
6. Щелкните **Сохранить изменения (Save Changes)**.

Можно использовать и классический стиль, однако в этом случае внешний вид большинства окон будет совсем другим. Кроме того, будут недоступны некоторые эффекты, например прозрачность и стекло Aero. Чтобы задать классический стиль отображения, выполните следующие действия:

1. Щелкните правой кнопкой свободную область рабочего стола и выберите команду **Персонализация (Personalize)**.
2. Выберите тему **Windows 7 — упрощенный стиль (Windows 7 Basic)** или другую упрощенную тему.
3. Теперь, когда в окне **Персонализация (Personalize)** вы пойдете по ссылке **Цвет окна (Window Color)**, отображается классическое окно **Цвет и внешний вид окна (Window Color And Appearance)**.

При работе с любым стилем внешнего вида возможна отдельная настройка индивидуальных графических элементов, например рабочего стола или сообщений системы. Для этого используется диалоговое окно **Цвет и внешний вид окна (Window Color And Appearance)**. Чтобы открыть его и провести необходимые настройки, выполните следующие действия:

1. Щелкните правой кнопкой свободную область рабочего стола и выберите команду **Персонализация (Personalize)**.
2. Щелкните ссылку **Цвет окна (Window Color)**, затем щелкните **Дополнительные параметры оформления(Advanced Appearance Settings)**.
3. Выберите в списке **Элемент (Item)** элементы интерфейса, с которыми собираетесь работать, и задайте размер, цвет, шрифт. (Для некоторых элементов доступны не все параметры.) Изменения вступают в силу сразу после внесения, что позволяет настроить несколько элементов, прежде чем щелкнуть **OK**, чтобы сохранить эти изменения.
4. Для графических элементов с текстом доступно поле **Шрифт (Font)**, позволяющее выбрать шрифт, а также его начертание, размер и цвет.
5. Щелкните **OK** и **Сохранить изменения (Save Changes)**.

Совет В Windows 7 имеется механизм устранения проблем Windows Aero, позволяющий обнаруживать и устранять неисправности без помощи технической поддержки. Чтобы воспользоваться этим механизмом, щелкните значок **Центр поддержки (Action Center)** в области уведомлений и выберите **Открыть центр поддержки (Open Action Center)**. В центре действий перейдите по ссылке **Устранение неполадок (Troubleshooting)**. Отобразятся все доступные механизмы устранения проблем. В группе **Оформление и персонализация (Appearance And Personalization)** выберите **Отображение настольных эффектов Aero (Display Aero Desktop Effects)**. Для выявления неисправности Aero вам будет задано несколько вопросов. По умолчанию предложенные решения применяются автоматически. В случае невозможности автоматического устранения неисправности вы увидите сообщение об этом. Обнаруженная неисправность будет внесена в список найденных проблем.

Оптимизация читаемости текста

Сложности с чтением текста можно испытывать и при работе с широкоэкранными 27-дюймовыми мониторами, и с обычными 19-дюймовыми. Зачастую читаемость ухудшается при увеличении разрешения, поскольку это приводит к уменьшению размера текста. Чтобы понять, почему это происходит, надо вникнуть в суть параметра DPI.

При печати на принтере количество точек на дюйм (DPI) определяет качество печати. В целом, чем выше DPI, тем качественнее печать, поскольку изображения и текст выглядят четче. Например, изображение высокого разрешения обычно выглядит гораздо лучше при печати с разрешением 1200 × 600 DPI, чем при печати с разрешением 300 × 300 DPI. Однако, если вы прибегнете к масштабированию, чтобы отпечатать изображение размером 9 × 12 см как изображение размера 10 × 15 см, результат, как правило, плачевен — из-за масштабирования изображение становится зернистым.

На компьютерах под управлением Windows для большинства мониторов по умолчанию устанавливается разрешение 96 DPI. Windows 7 не является исключением из этого правила и по умолчанию отображает все элементы пользовательского интерфейса, включая текст, с разрешением 96 DPI. Изменяя разрешение, вы изменяете и масштаб элементов интерфейса. Например, если оптимальное разрешение монитора 1920 × 1200, а работает он в разрешении 800 × 600, элементы интерфейса будут выглядеть большими и зернистыми, поскольку вы заставляете компьютер растягивать элементы с разрешением 800 × 600 на пространство, оптимизированное для разрешения 1920 × 1200 точек.

Проще всего определить оптимальное разрешение умножением ширины и высоты экрана в дюймах на 96. Допустим, 27-дюймовый монитор имеет 20 дюймов в ширину и 12,5 в высоту. В этом случае, оптимальным для него будет разрешение 1920 × 1200. Однако в этом случае текст и элементы интерфейса будут выглядеть очень мелкими, и вам придется изменять настройки для улучшения читаемости. Один из способов сделать это — воспользоваться средствами приложений. Например, в Microsoft Word есть список **Масштаб (Zoom)** для масштабирования текста.

В Windows имеется возможность общего масштабирования текста и других элементов экрана. В этом случае производится увеличение размера текста и элементов интерфейса на указанную величину. Масштабирование индивидуально для каждого пользователя компьютера. Чтобы задать масштабирование текста и интерфейса, выполните следующие действия:

1. В панели управления щелкните категорию **Оформление и персонализация (Appearance And Personalization)**. Щелкните **Изменение размеров текста и других элементов (Make Text And Other Items Larger Or Smaller)** под заголовком **Экран (Display)**.
2. Параметры, доступные по умолчанию, позволяют выбрать масштаб 100% (по умолчанию), 125% или 150%. Чтобы воспользоваться одним из этих значений, щелкните соответствующий переключатель и кнопку **Применить (Apply)**.
3. Чтобы использовать другой масштаб от 100% до 500%, щелкните ссылку **Другой размер шрифта (точек на дюйм) (Set Custom Text Size (DPI))** на левой панели и используйте **Масштаб (Scale)** для выбора или ввода масштаба.
4. Чтобы изменения вступили в силу, выйдите из системы и снова зарегистрируйтесь.

Внимание! Если выбрать масштаб более 200%, интерфейс и текст могут оказаться слишком большими для нормальной работы, так что у вас не получится даже зайти в панель управления, чтобы вернуть предыдущий масштаб. Если такое случилось, введите в командной строке или в поле поиска меню **Пуск (Start)** команду **dpiscaling**. Откроется страница **Экран (Display)**, на которой можно восстановить масштабирование.

Ближе к реальности Если в выбранном масштабе текст размыт или нечитаем в конкретном приложении, отключите масштабирование для этого приложения. Щелкните правой кнопкой ярлык приложения и выберите команду **Свойства (Properties)**. На вкладке **Совместимость (Compatibility)** задайте параметр **Отключить масштабирование изображения при высоком разрешении экрана (Disable Display Scaling On High DPI Settings)** и щелкните **OK**.

Настройка параметров видео

Параметры видео определяют разрешение экрана, количество цветов, частоту обновления, аппаратное ускорение и управление цветом. В этом разделе описано, как обеспечить корректное определение видеоплаты и монитора Windows 7 и настроить связанные с ними параметры.

Проверка текущего видеоадаптера и монитора

На каждом компьютере есть драйверы монитора и видеоадаптера. Драйвер монитора предоставляет Windows сведения о возможностях монитора, драйвер видеоадаптера — сведения о возможностях видеоплаты.

От точности информации о видеоплате и мониторе зависит качество изображения. Корректная установка драйвера крайне важна для определения

правильного разрешения, подходящего количества цветов и частоты обновления. Если видеоплата и монитор определены неправильно, Windows 7 не сможет воспользоваться всеми их возможностями.

Текущие настройки видеоадаптера или монитора могут оказаться неверными в силу многих обстоятельств. Порой технология Plug and Play не обнаруживает устройство, и вам приходится использовать универсальный драйвер, или Windows 7 неправильно обнаруживает устройство, например, ошибается с моделью. В этом случае устройство, скорее всего, будет работать, но не в полную силу.

Чтобы проверить текущие настройки видеоадаптера и монитора, выполните следующие действия:

1. Щелкните правой кнопкой свободную область рабочего стола и выберите команду **Разрешение экрана (Screen Resolution)**.
2. На странице **Разрешение экрана (Screen Resolution)**, показанной на рис. 7-10, в списке **Экран (Display)** перечислены определенные системой мониторы. В списках **Разрешение (Resolution)** и **Ориентация (Orientation)** указаны возможные для них разрешение и ориентация. Если текущего монитора в этом списке нет или если вам нужно просмотреть другие настройки монитора, обратитесь к разделу «Смена монитора» далее в этой главе.

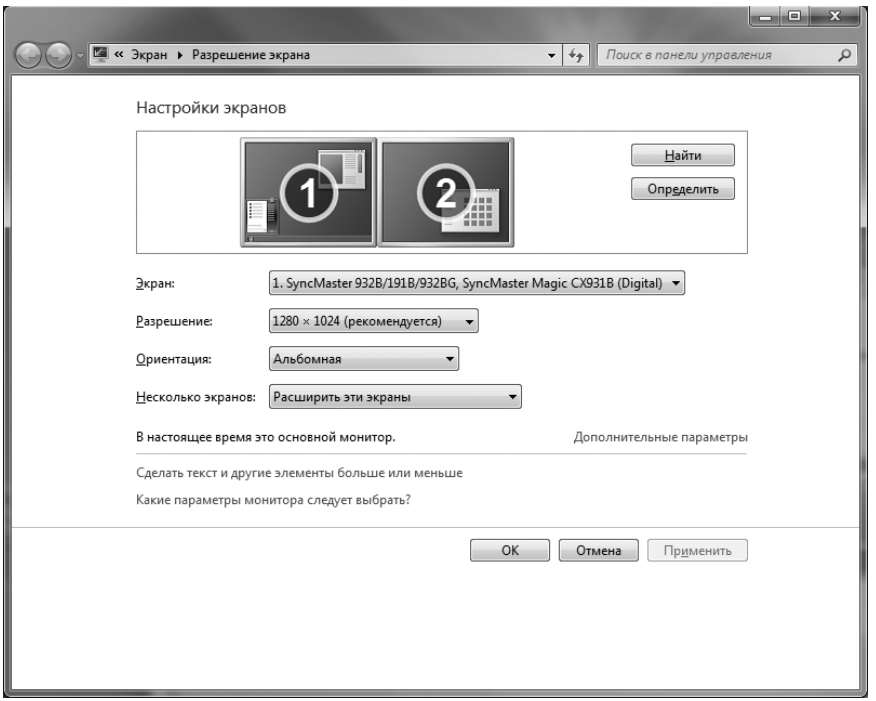

Рис. 7-10. Проверьте настройки монитора и видеоадаптера

3. Выберите монитор в списке **Экран (Display)** и щелкните ссылку **Дополнительные параметры (Advanced Settings)**. Появится список видеоадаптеров, подключенных к этому монитору. Если правильного видеоадаптера в списке нет или если вам нужно более глубоко проанализировать настройки драйвера, обратитесь к следующему разделу.
4. Дважды щелкните **OK**.

Смена видеодрайвера

Если в ходе выполнения предыдущих указаний выяснилось, что обнаруженный видеодрайвер не совпадает с реальным, вам стоит попробовать установить другой драйвер. Например, если на компьютере используется универсальный видеодрайвер S3, а физически в нем установлен видеоадаптер NVIDIA GeForce, вам нужно поменять видеодрайвер.

Чтобы корректно определить изготовителя и модель видеоплаты, необходимо знать конфигурацию системы. Ее можно посмотреть в системной документации. Кроме того, это могут знать другие администраторы. Как правило, сотрудники технической поддержки знают, какие видеоадаптеры стоят на разных компьютерах. Если указанные источники не помогли, у вас есть еще несколько вариантов. Если сейчас система работает, просто оставьте ее в покое. Также для определения производителя и модели видеоадаптера можно использовать следующие способы:

- Выключите компьютер и снова включите его (но не при помощи кнопки Restart, поскольку в этом случае некоторые компьютеры пропускают часть этапа инициализации). Внимательно смотрите на экран при включении компьютера. Название видеоплаты может ненадолго появиться перед загрузкой Windows 7.
- Выключите компьютер и снимите корпус. Поищите производителя и модель на самой видеоплате. Если монитор все еще подключен к задней стенке системного блока, кабель от него подходит именно к видеоплате.
- Если видеоадаптер встроен в материнскую плату (то есть не является отдельной платой), осмотрите материнскую плату и найдите микросхему, на которой написано что-нибудь про видео. Или перепишите название материнской платы и выясните тип видеоадаптера на сайте производителя.

Определив название изготовителя и модели видеоадаптера, попробуйте загрузить драйвер с сайта изготовителя. С некоторыми видеоадаптерами продаются установочные диски, на которых могут быть драйверы. Запустите программу установки с диска или установите их вручную.

Подготовившись к установке драйвера видеоплаты, выполните следующие действия:

1. Щелкните правой кнопкой свободную область рабочего стола и выберите команду **Разрешение экрана (Screen Resolution)**.
2. Если в системе несколько мониторов или видеоплат, выберите в списке **Экран (Display)** тот, с которым собираетесь работать.

3. Щелкните **Дополнительные параметры (Advanced Settings)**. На вкладке **Адаптер (Adapter)**, показанной на рис. 7-11, обратите внимание на информацию в разделах **Тип адаптера (Adapter Type)** и **Сведения об адаптере (Adapter Information)**. Щелкните кнопку **Свойства (Properties)**.

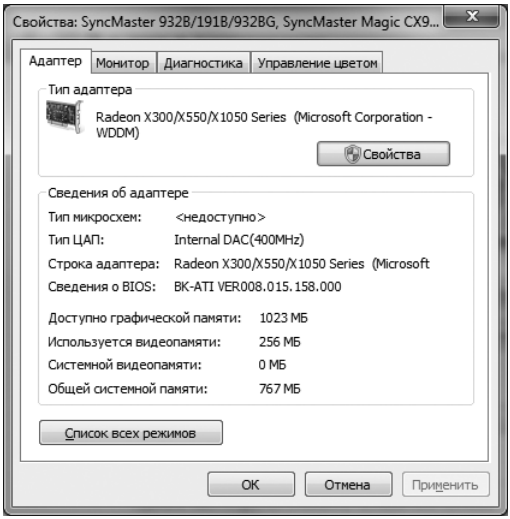

Рис. 7-11. Обратите внимание на текущую информацию об адаптере

4. Щелкните кнопку **Обновить (Update Driver)** на вкладке **Драйвер (Driver)**. Запустится мастер Обновление драйверов (Update Driver Software).
5. Укажите, воспользуетесь ли вы автоматическим поиском, или укажете расположение драйвера вручную.
6. Если вы выберете автоматический поиск драйвера, Windows 7 произведет поиск более новой версии драйвера и, если найдет, то установит. В противном случае Windows 7 сохранит текущий драйвер. В обоих случаях щелкните **Закрыть (Close)**, чтобы завершить процесс, и пропустите оставшиеся шаги.
7. Если вы решили указать драйвер самостоятельно, у вас есть следующие возможности:
   - **Искать драйвер на компьютере** Щелкните кнопку **Обзор (Browse)**, чтобы задать область поиска. Выберите начальную папку поиска в диалоговом окне **Обзор папок (Browse For Folder)** и щелкните **OK**. Поиск автоматически производится во всех подпапках выбранной папки, так что можно выбрать корневой каталог, например, C:, чтобы искать на всем диске.
   - **Выбрать драйвер самостоятельно** Если вы хотите самостоятельно выбрать драйвер для установки, щелкните **Выбрать драйвер из списка уже установленных драйверов (Let Me Pick From A List Of Device Drives On My Computer)**. Мастер откроет список совместимого аппаратного обеспечения. Выберите устройство, совпадающее с видео-

платой вашего компьютера. Чтобы расширить список, сбросьте флажок **Только совместимые устройства (Show Compatible Hardware)**. Появится список всех производителей видеоплат. Найдите в нем производителя платы и выберите подходящую модель из списка на правой панели.

8. Выбрав драйвер, щелкните **Далее (Next)**. Затем щелкните **Закрыть (Close)**, когда установка закончится. Если мастер не находит подходящий драйвер, раздобудьте драйвер и повторите процедуру. Помните, что в некоторых случаях для активации нового или обновленного драйвера потребуется перезагрузка системы.

Смена монитора

Общее качество изображения определяется возможностями монитора и видеоадаптера. У большинства компьютеров есть хотя бы один выход на монитор. Поддерживаются следующие виды разъемов:

- **HDMI (High-Definition Multimedia Interface)** Современный стандарт соединения цифровых видеоустройств. Может использоваться для мониторов, но лучше приспособлен для использования в других видеоустройствах верхнего эшелона. Существуют переходники HDMI-DVI, однако на большинстве компьютеров с выходом HDMI, есть и выход DVI.
- **DVI (Digital Video Interface)** Стандарт цифровой передачи текста и графики, генерируемых компьютером. DVI бывает нескольких форматов. Форматы DVI-I и DVI-A можно перевести в VGA, а формат DVI-D — нет. Двухканальный DVI поддерживает мониторы высокого разрешения и необходим для достижения оптимального качества изображения на некоторых мониторах особо широкого формата. Кабели DVI могут поддерживать как один, так и несколько форматов, так что проверьте, правильные ли кабели используются.
- **VGA (Video Graphics Array)** Аналоговый стандарт соединения мониторов с компьютерами. Существуют 15- и 9-контактные кабели VGA, причем 9-контактные совместимы с 15-контактными. Мониторы с такими видеовходами все еще широко распространены, однако рекомендуется по возможности использовать новые интерфейсы DVI и HDMI.

Примечание Монитор может поставляться вместе с кабелем VGA. Если это не оптимальный вид соединения и кабель можно заменить, сделайте это.

Совет На многих компьютерах есть разъемы для адаптеров DisplayPort. Он поддерживает автоматическое преобразование в VGA, DVI или HDMI, в зависимости от монитора, порта и используемого переходника.

Если ваш монитор поддерживает стандарт Plug and Play, Windows 7 скорее всего правильно определила монитор или воспользовалась похожим драйвером, если определить изготовителя и модель не удалось. Для достижения наивысшего качества должен использоваться подходящий драйвер.

Чтобы изменить настройку монитора, выполните следующие действия:

1. Щелкните правой кнопкой свободную область рабочего стола и выберите команду **Разрешение экрана (Screen Resolution)**.
2. Если в системе несколько мониторов или видеоплат, выберите нужный монитор в списке **Экран (Display)**.
3. Щелкните **Дополнительные параметры (Advanced Settings)**. На вкладке **Монитор (Monitor)** щелкните кнопку **Свойства (Properties)**.
4. На вкладке **Драйвер (Driver)** щелкните **Обновить (Update Driver)**. Запустится мастер Обновление драйверов (Update Driver Software).
5. Продолжите обновление драйвера, как описано в пунктах 5-8 предыдущей процедуры.

Настройка поддержки нескольких мониторов

Большинство современных видеоплат способно работать с двумя мониторами, так как у них есть несколько видеовыходов. Если в вашем компьютере именно такой видеоадаптер, вы можете присоединить к нему несколько мониторов, расширив рабочий стол пользователя. При этом на странице **Разрешение экрана (Screen Resolution)** будут значки для всех мониторов. Первый монитор помечается единицей, второй — двойкой и т. д. Щелчок значка монитора эквивалентен выбору монитора из списка **Экран (Display)**.

Если монитор соединен с компьютером, но его значок не отображается, проверьте соединение и включите монитор. Затем щелкните кнопку **Найти (Detect)**. Windows должна автоматически определить монитор.

Номер монитора можно определить, щелкнув кнопку **Определить (Identify)** — на каждом мониторе будет показан его номер в виде большой белой цифры. Если расположение значков на странице **Разрешение экрана (Screen Resolution)** отличается от физического расположения мониторов, перетащите значки так, чтобы их положение совпадало с физическим положением мониторов.

Настроив мониторы, распределите по ним изображения. Щелкните значок второго монитора или выберите его в списке **Экран (Display)**, и выберите в списке **Несколько экранов (Multiple Displays)** вариант **Расширить эти экраны (Extend These Displays)**. Отметка **В настоящее время это основной монитор (This Is Currently Your Main Display)** должна быть на экране 1.

Смена разрешения и качества цветов

Разрешение экрана и качество цветов — ключевые элементы качества изображения. Разрешение — это число точек на экране. Качество цвета — число цветов, одновременно отображаемых на экране.

Старые модели мониторов поддерживают разрешения 640 × 480, 800 × 600 и 1024 × 768. Новым моделям доступны разрешения 1280 × 1024, 1600 × 1200, 1920 × 1200, 2048 × 1536 и даже выше. Оптимальное разрешение зависит от размера монитора и вида выполняемой на нем работы. Дизайнерам и разработчикам нужно много рабочего пространства, поэтому им нужно высокое

разрешение, например 1920 × 1200. Пользователи, большую часть времени работающие с электронной почтой или текстовым процессором, обойдутся и более низким разрешением, например 1280 × 1024. В этом разрешении лучше видны элементы экрана и меньше устают глаза. Для широкоформатных мониторов необходимо использовать разрешения, оптимизированные для них.

Качество цвета сильно зависит от разрешения экрана и варьируется от 16 цветов для стандартного VGA до 4 миллиардов цветов (32-разрядный цвет). Многие видеоплаты способны работать в высоком разрешении только с малым числом цветов. Это означает, что компьютер может работать с 16-разрядным, 24-разрядным или 32-разрядным цветом, но для наилучшего качества цветопередачи придется уменьшить разрешение. В большинстве случаев, чем больше количество цветов, тем лучше. Имейте в виду, что объем видеопамяти, необходимой для поддержки изображения, определяется произведением количества точек экрана (разрешением) на количество разрядов в одной точке (глубиной цвета). Кроме того, наилучшее допустимое сочетание разрешения и количества цветов зависит от памяти видеоплаты.

Чтобы установить разрешение экрана и количество цветов, выполните следующие действия:

1. Щелкните правой кнопкой мыши свободную область рабочего стола и выберите команду **Разрешение экрана (Screen Resolution)**.
2. На системе с несколькими мониторами или видеоплатами выберите нужный монитор в списке **Экран (Display)**.
3. Выберите в списке **Разрешение (Resolution)** нужное разрешение экрана, например 1024 × 768.
4. Чтобы задать глубину цвета, щелкните **Дополнительные параметры (Advanced Settings)**. На вкладке **Монитор (Monitor)** выберите в списке **Качество цветопередачи (Colors)** нужное качество цветопередачи.
5. Дважды щелкните **OK**.

Смена частоты обновления экрана

Частота обновления определяет, как часто перерисовывается картинка на экране. Чем выше частота обновления, тем слабее мерцание экрана. Глаза часто не замечают такого мерцания, однако низкая частота обновления (ниже 72 Гц) при длительной работе вызовет излишнюю усталость глаз.

Чтобы посмотреть или изменить скорость обновления экрана, выполните следующие действия:

1. Щелкните правой кнопкой мыши свободную область рабочего стола и выберите команду **Разрешение экрана (Screen Resolution)**.
2. Если мониторов или видеоплат несколько, выберите нужный монитор в списке **Экран (Display)**.
3. Щелкните **Дополнительные параметры (Advanced Settings)**. На вкладке **Адаптер (Adapter)** щелкните кнопку **Список всех режимов (List All Modes)**. Будут показаны возможные разрешения и частоты обновления экрана.

4. На вкладке **Монитор (Monitor)** выберите нужную частоту обновления в списке **Частота обновления экрана (Screen Refresh Rate)**.

Внимание! В большинстве случаев флажок **Скрыть режимы, которые монитор не может использовать (Hide Modes That This Monitor Cannot Display)** заблокирован, и сбросить его нельзя. Если его удается сбросить, помните, что выбор частоты обновления, превосходящей возможности монитора и видеоплаты, может привести к искажению изображения и повреждению монитора и видеоплаты.

Устранение проблем с изображениями

Как уже говорилось, на каждом компьютере есть драйвер монитора и драйвер видеоадаптера. Драйвер монитора сообщает Windows о возможностях монитора, а драйвер видеоплаты — о возможностях видеоплаты.

Очевидно, что драйверы монитора и видеоплаты играют важную роль в работе компьютера. При установке или обновлении видеосистемы убедитесь, что драйверы надежны и проверены в рабочей среде. Если вы подозреваете, что с драйверами возникли проблемы, постарайтесь их обновить. Если проблемы связаны с конфигурацией компьютера, запустите его в безопасном режиме и измените настройки по умолчанию.

Прежде чем взяться за устранение проблем, обнаруженных пользователем, определите, какие программы он запускал. У программ, написанных для версий Windows до Windows XP, могут возникать проблемы с совместимостью. Закройте все программы и проверьте, какое режим экрана используют приложения, совместимость которых под вопросом. Если программе требуется режим, отличный от режима рабочего стола, и переключение режимов приводит к сбоям, возможно, избавиться от этих проблем помогут параметры совместимости. Щелкните правой кнопкой ярлык приложения и выберите команду **Свойства (Properties)**. В открывшемся окне перейдите на вкладку **Совместимость (Compatibility)**. Задайте нужные параметры в разделе **Параметры (Settings)**, например **Использовать разрешение экрана 640x480 (Run In 640x480 Screen Resolution)**. Если вы не уверены в том, какой вариант совместимости задействовать, щелкните ярлык правой кнопкой и выберите команду **Исправление неполадок совместимости (Troubleshoot Compatibility)**. Затем следуйте инструкциям мастера Совместимость программы (Program Compatibility).

Многие проблемы мониторов связаны с соединением монитора и компьютера. Если на экране имеются пятна, диагональные или горизонтальные полосы, или другие дефекты, в первую очередь проверьте соединение. Если соединение в порядке, отключите монитор на 10 секунд и включите снова. Если и это не помогло, понадобится дополнительная диагностика.

Дрожание изображения может быть вызвано как неудачными настройками, так и проблемами размещения. Если сбой вызван частотой обновления, ее можно решить, изменив настройки, как было описано выше. Если проблема связана с размещением, попробуйте передвинуть кабели или устрой-

ства, которые могут наводить электромагнитные помехи, включая силовые кабели, большие колонки и настольные лампы. Если проблема не исчезла, примените экранированный кабель и убедитесь, что монитор расположен достаточно далеко от кондиционеров, микроволновых печей, больших люминесцентных ламп и т. д.

Если монитор обладает возможностью автонастройки, воспользуйтесь ею. Чаще всего она запускается отдельной кнопкой.

Если после проверки соединения на мониторе остались дефекты вроде цветных пятен или линий, попробуйте провести размагничивание. Эта операция снимает остаточные магнитные поля вокруг монитора, которые могут быть причиной искажений. Часть мониторов размагничивается автоматически при выключении и включении, часть позволяет сделать это вручную, в некоторых сочетаются обе возможности. Найдите кнопку Degauss или пункт меню монитора с таким же названием. При размагничивании изображение может искажаться; это нормально. Если размагничивание произведено вручную, подождите 15-20 минут перед повторной попыткой.

Если проблема остается и после этих действий, соедините монитор с компьютером напрямую. Удалите все удлинители между монитором и видеоадаптером. Также снимите все антибликовые экраны или аналогичные устройства, закрывающие экран монитора. Проверьте, нет ли на видеокабеле изгибов, изломов, все ли контакты на месте. Хотя отсутствие некоторых контактов может быть частью конструкции, отсутствие или изгиб других приводят к потере качества изображения. Если в разъеме есть погнутые контакты, отключите монитор, вытащите вилку из розетки и попробуйте поправить контакты пинцетом или плоскогубцами.

Глава 8

Устройства и драйверы

Управление аппаратной конфигурацией компьютера заключается, главным образом, в установке и обслуживании компонентов ОС, оборудования и драйверов устройств. Причем методы управления конфигурацией оборудования, реализованные в Windows 7, заметно отличаются от методов, применяемых в Windows XP и более ранних версиях. Как и в Windows Vista, многие аспекты конфигурации Windows 7 отслеживаются и обновляются автоматически. Вы избавлены от необходимости их настройки и обслуживания, как в предыдущих выпусках Windows. Вот какими средствами располагает Windows 7:

- Автоматическое обновление компонентов ОС.
- Встроенная диагностика — наблюдение за параметрами оборудования, памяти, сети и быстродействия.
- Диагностика проблем — поиск решений для проблем, которые не удается устранить автоматически.
- Обновление драйверов — получение необходимых драйверов и обновлений для обнаруженных устройств.
- Отчеты о проблемах — попытка автоматического устранения проблем в конфигурации и производительности.

Перечисленные функциональные возможности начинают работать с самого момента установки Windows 7 и существенно помогают администратору в настройке и обслуживании системы. Для каждого направления диагностики, включая диагностику оборудования, памяти, сети и производительности, имеются отдельные инструменты.

Кроме того, для настройки и обслуживания оборудования предназначены Диспетчер устройств (Device Manager), страница **Устройства и принтеры (Devices And Printers)**, а также мастер Установка оборудования (Add A Device). Эти средства используются, когда нужно установить или удалить устройство или драйвер, а также устранить неисправность. Другие инструментальные средства предназначены для управления отдельными типами оборудования, например клавиатурой или звуковой платой. Управление автоматическим обновлением и обновлением драйверов выполняется в утилите панели управления **Центр обновления Windows (Windows Update)**.

Автоматизированная справочная система

Работа и обслуживание ОС фундаментально изменились благодаря дополнительным возможностям справочной системы Windows 7. Администратор должен ясно понимать структуру и принцип действия справочной системы, а также способы ее настройки.

Работа с системой справки и поддержки

Как и в Windows Vista, в Windows 7 реализована обширная система диагностики и устранения неисправностей. В Windows XP и предыдущих выпусках Windows также имеются определенные средства диагностики, однако в большинстве своем они не обладают возможностью самокоррекции и самодиагностики. Инструменты Windows 7 способны обнаруживать различные типы неисправностей оборудования, памяти и производительности, автоматически устранять их или предоставить пользователю необходимую для их устранения информацию.

С Windows 7 поставляются более надежные и производительные драйверы устройств, в которых исключены многие типичные причины зависаний и сбоев системы. Модернизированная функция отмены ввода-вывода для драйверов устройств обеспечивает возможность легкого восстановления после блокирующих вызовов, а также сокращение числа блокирующих операций ввода-вывода на диске.

Процесс обновления Windows 7 организован так, чтобы сократить время простоя и число перезапусков при установке и обновлении приложений. Используемые файлы, которые нуждаются в обновлении, помечаются, чтобы быть обновленными при следующем запуске приложения. В некоторых случаях ОС сохраняет данные приложения, закрывает приложение, обновляет используемые файлы, а потом приложение запускается вновь. Увеличение общей производительности и сокращение времени отклика системы достигается за счет более эффективного использования памяти, упорядоченного выполнения групп потоков и нового механизма распределения времени процессов. Оптимизация использования памяти и процессов в Windows 7 не дает фоновым приложениям существенно влиять на быстродействие системы.

Дополнено руководство по причинам отсутствия отклика системы на действия пользователя. Дополнительные сведения об ошибках, включаемые в журналы регистрации событий Windows 7, упрощают поиск и устранение неисправностей. Для автоматического восстановления службы после сбоя в Windows 7 более широко по сравнению с предыдущими версиями применяются политики восстановления служб. При восстановлении службы происходит автоматическая обработка всех зависимостей. В Windows 7 перед запуском сбойной службы запускаются все зависимые службы и системные компоненты.

В Windows XP и прежних версиях системы зависшее или прекратившее работу приложение, расценивается как не отвечающее, и у пользователя есть

только возможность выйти из программы и запустить ее заново. В Windows 7 предпринимаются попытки решить проблему неотвечающего приложения при помощи диспетчера перезапуска. В Диспетчере перезапуска (Restart Manager) неотвечающие приложения автоматически закрываются и запускаются повторно. Благодаря ему мы избавлены от необходимости «бороться» с зависшей программой.

Неудачные попытки установки приложений и их зависание отслеживаются в Центре поддержки (Action Center). Иногда решить проблему помогает встроенный механизм диагностики. Просмотреть список текущих проблем можно одним из следующих способов:

- В области уведомлений щелкните значок **Устранение проблем с ПК (Action Center)** и перейдите по ссылке **Открыть центр поддержки (Open Action Center)**.
- На панели управления последовательно щелкните **Система и безопасность (System And Security)** и **Центр поддержки (Action Center)**.

В окне **Центр поддержки (Action Center)**, показанном на рис. 8-1, текущие сбои перечислены в двух областях: **Безопасность (Security)** и **Обслуживание (Maintenance)**.

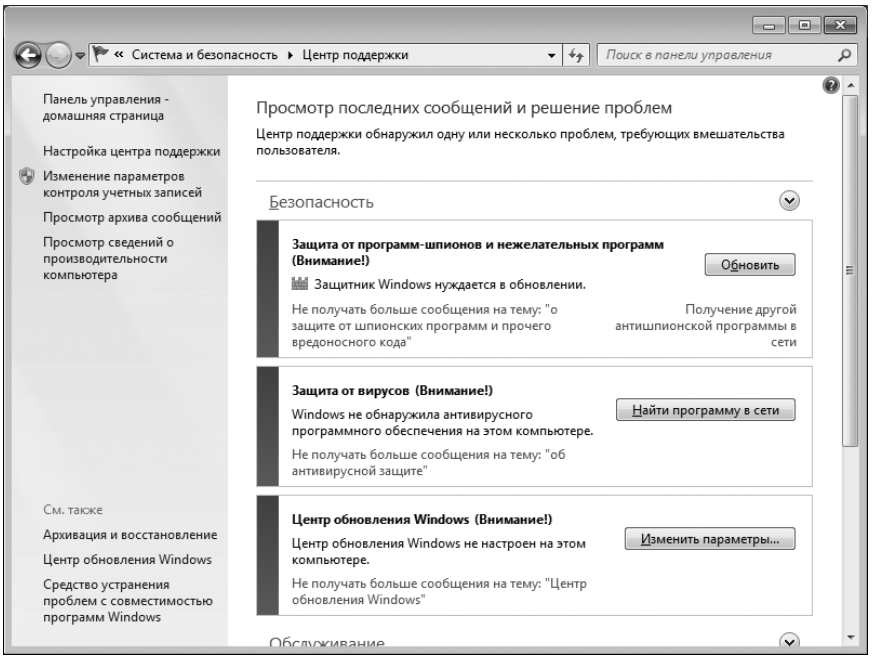

Рис. 8-1. Текущие проблемы в окне Центра поддержки (Action Center)

Цвет записи говорит о характере проблемы:

- Красный — проблема серьезна и требует вашего внимания. Например, красным отмечено предупреждение об отсутствии на компьютере антивирусной программы.

- Оранжевый — проблема заслуживает внимания. В частности, если компьютер давно не проверялся при помощи Защитника Windows (Windows Defender), выводится оранжевое предупреждение.

Чтобы развернуть раздел и просмотреть более подробные сведения, щелкните заголовок **Безопасность (Security)** или **Обслуживание (Maintenance)**. В области **Безопасность (Security)** содержится следующая информация:

- Состояние сетевого брандмауэра, центра обновления Windows, защиты от вирусов и вредоносных программ.
- Параметры безопасности Интернета, контроля учетных записей и защиты доступа к сети.

В области **Обслуживание (Maintenance)** вы найдете следующую информацию:

- Ссылки для управления конфигурацией отчетов о проблемах.
- Состояние архивации и действия, которые необходимо выполнить в Центре обновления Windows (Windows Update).
- Состояние системы устранения неполадок и ссылки, позволяющие изменить ее параметры.

Если вы хотите найти сбои на только что настроенном компьютере или подозреваете наличие неопознанных проблем, запустите средство автоматического поиска неисправностей, выполнив следующие действия:

1. В Центре поддержки (Action Center) щелкните заголовок **Обслуживание (Maintenance)**.

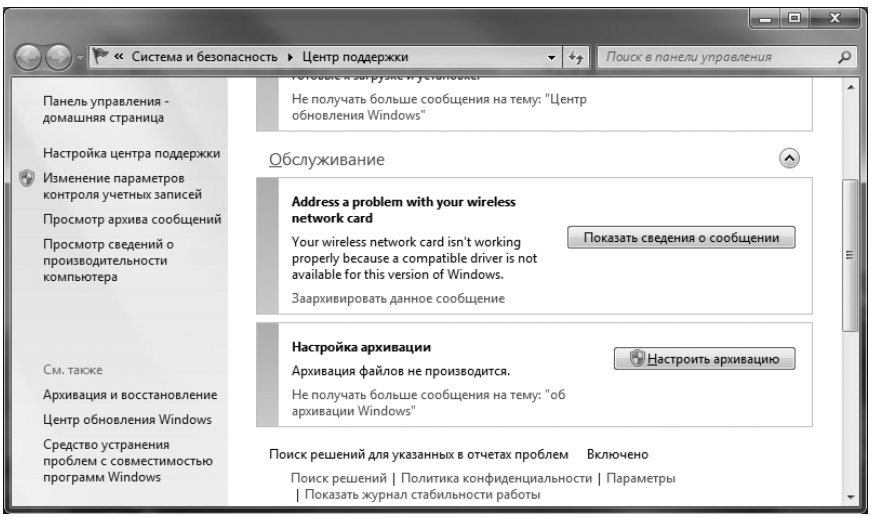

Рис. 8-2. Просмотр обнаруженных неисправностей

2. В нижней части списка текущих неисправностей расположена область **Поиск решений для указанных в отчетах проблем (Check For Solutions To Problem Reports)** и соответствующие ссылки (рис. 8-2). Чтобы на-

чать автоматический поиск неисправностей, щелкните **Поиск решений (Check For Solutions)**. По завершению процесса в Центре поддержки (Action Center) будут перечислены все обнаруженные проблемы и известные способы их решения.

3. Если во время автоматической диагностики находятся неполадки, не имеющие известных решений, в окне будут показаны дополнительные сведения. Для их просмотра в диалоговом окне **Отчеты о проблемах (Problem Reports And Solutions)** щелкните **Показать сведения о сообщении (View Problem Details)**. Чтобы устранить неисправность самостоятельно, используйте ссылки для извлечения данных. Данные копируются в папку Temp профиля текущего пользователя. Прежде чем продолжить работу, создайте копию этих данных.
4. В диалоговом окне **Отчеты о проблемах (Problem Reports And Solutions)** щелкните **Отправить сведения (Send Information)**, чтобы отправить сведения о проблеме в Майкрософт. Для выхода из диалогового окна **Отчеты о проблемах (Problem Reports And Solutions)** без отправки информации щелкните **Отмена (Cancel)**. При отправке сведений в Майкрософт диагностические данные извлекаются в папку Temp профиля текущего пользователя, отправляются в Майкрософт, а затем удаляются из папки Temp. Объем извлекаемых и отправляемых данных может оказаться большим.

Чтобы устранить проблему, для которой есть известные способы решения, выполните следующие действия:

1. Каждой неполадке соответствует кнопка для ее устранения. Для решения проблем с безопасностью, как правило, требуется найти программы в сети или проверить компьютер на наличие нежелательного ПО. При решении проблем, связанных с обслуживанием, обычно требуется щелкнуть кнопку **Показать решение проблемы (View Problem Response)** и просмотреть дополнительные сведения.
2. Просмотрите страницу **Сведения о сообщении (More Information)**, показанную на рис. 8-3. Если причина сбоя заключается в драйвере или программе, здесь вы найдете ссылку для загрузки последних обновлений для драйвера или ПО. Если неполадка связана с конфигурацией, будет выведено описание проблемы и ее решение с пошаговой инструкцией по изменению конфигурации. Иногда информация бывает доступна не на всех языках.
3. Устранив неполадку при помощи установки обновлений, сохраните сообщение о сбое на будущее. Установите флажок **Заархивировать данное сообщение (Archive This Message)** и щелкните **OK**, чтобы закрыть страницу **Сведения о сообщении (More Information)**.

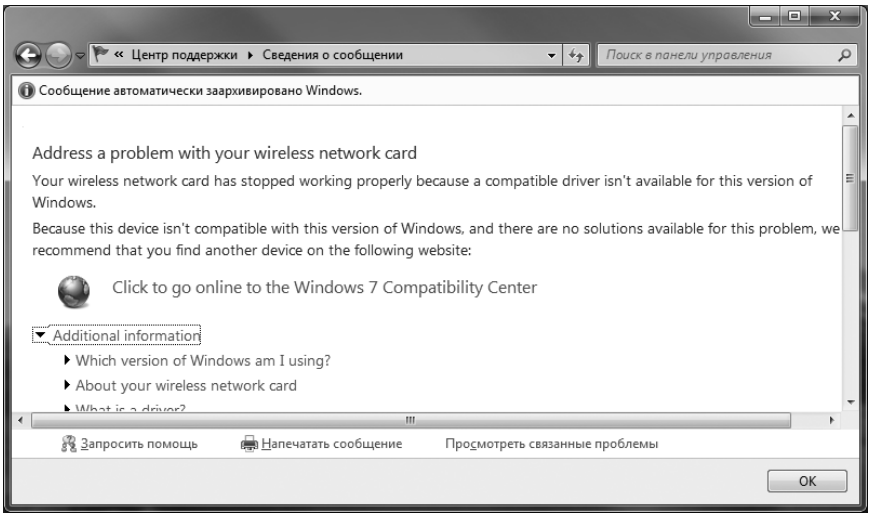

Рис. 8-3. Чтобы устранить неисправность, выполните показанную инструкцию

В Центре поддержки (Action Center) есть ссылка на журнал надежности компьютера, в котором отображается история возникавших на компьютере проблем с оборудованием и ПО. С его помощью вы определите степень устойчивости работы компьютера, а также выявите устройства и программы, ставшие причиной неполадок. Чтобы открыть Монитор стабильности системы (Reliability Monitor), выполните следующие действия:

1. В Центре поддержки (Action Center) щелкните заголовок **Обслуживание (Maintenance)**.
2. В нижней части списка текущих неисправностей расположена область **Поиск решений для указанных в отчетах проблем (Check For Solutions To Problem Reports)** и соответствующие ссылки. Щелкните ссылку **Показать журнал стабильности работы (View Reliability History)**.
3. На экране появится графическое отображение стабильности работы компьютера (рис. 8-4) по дням или неделям. По умолчанию просмотр организован по дням. Для понедельного просмотра в разделе **Просмотр по (View By)** щелкните **Недели (Weeks)**. На графике кривая устойчивости работы компьютера варьируется от 0 (крайне нестабильно) до 10 (наибольшая стабильность).
4. События, повлиявшие на устойчивую работу, показаны на диаграмме в виде значков уведомлений и предупреждений. Чтобы просмотреть сведения о событии в списке **Сведения о стабильности (Reliability Details)**, щелкните значок. События в списке упорядочены по источнику, описанию и дате. В столбце **Действие (Action)** содержится ссылка на возможное действие. Рядом с проблемой, решенной Windows автоматически, отображается ссылка **Показать решение проблемы (View Problem Response)**. По ней содержится информация о том, как была решена проблема. В других случаях отображается ссылка **Показать технические**

подробности (View Technical Details). Щелкнув ее, вы найдете дополнительные сведения (рис. 8-5).

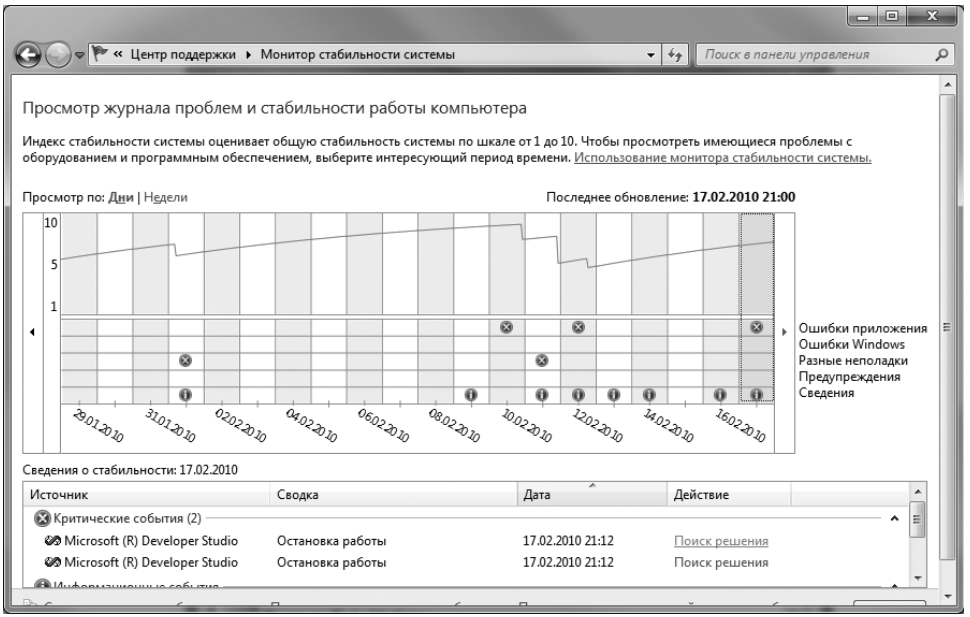

Рис. 8-4. Графическое представление устойчивости работы компьютера

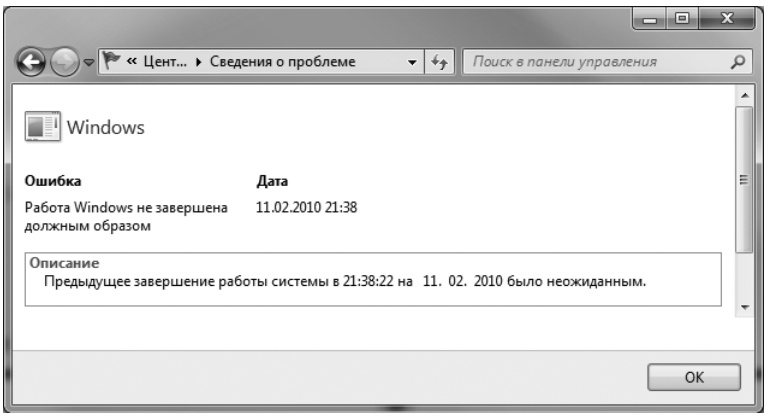

Рис. 8-5. Дополнительные сведения о проблеме

5. В нижней части окна **Монитор стабильности системы (Reliability Monitor)** задайте дополнительные параметры:
   - **Сохранить журнал стабильности (Save Reliability History)** Сохранение всех сведений о стабильности работы компьютера для последующего анализа. Информация сохраняется в виде отчета монитора стабильности в формате XML. Щелкните ссылку **Сохранить журнал стабильности (Save Reliability History)**, чтобы открыть диалоговое

окно для выбора места сохранения и имени отчета. Чтобы просмотреть отчет в Internet Explorer, дважды щелкните файл отчета.

- **Просмотреть все отчеты о проблемах (View All Problem Reports)** Отображение всех известных неполадок и их состояния в окне **Отчеты о проблемах (Problem History)**. Для очистки списка неполадок щелкните **Очистить все отчеты о проблемах (Clear All Problem Reports)**.
- **Проверить наличие решений для всех проблем (Check For Solutions To All Problems)** Создание отчета о проблемах. По завершению процесса в Центре поддержки (Action Center) будут перечислены все обнаруженные проблемы и известные способы их решения.

Настройка системы справки и поддержки

В Windows 7 есть много параметров для управления системой справки и поддержки. Вы вольны, например, задать типы уведомлений, отображаемых в Центре поддержки (Action Center). Можно также задать параметры вывода отчетов о проблемах и действия по устранению неисправностей.

Параметры уведомлений на компьютере различны для каждого пользователя. Чтобы задать типы отображаемых в Центре поддержки (Action Center) уведомлений, выполните следующие действия:

1. В Центре поддержки (Action Center) щелкните ссылку **Настройка центра поддержки (Change Action Center Settings)**.
2. На странице **Настройка центра поддержки (Change Action Center Settings)** установите флажки уведомлений, которые должен получать пользователь, и сбросьте флажки уведомлений, которые пользователь получать не должен (рис. 8-6).

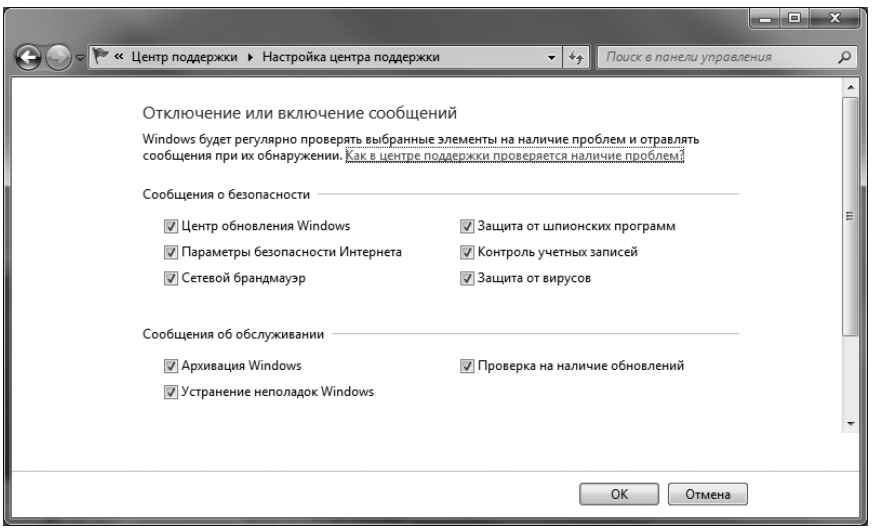

Рис. 8-6. Настройка уведомлений, отображаемых в Центре поддержки (Action Center)

3. По умолчанию сведения об использовании отправляются Майкрософт в рамках программы улучшения качества программного обеспечения. Если вы не хотите участвовать в программе, щелкните ссылку **Параметры программы улучшения качества ПО (Customer Experience Improvement Program Settings)**, затем щелкните **Нет, я не хочу участвовать в программе (No, I Don't Want To Participate In The Program)** и **Сохранить изменения (Save Changes)**.
4. Щелкните **OK**.

В стандартной конфигурации для каждого пользователя компьютера заданы свои параметры отчетов о проблемах. Но администраторы вольны задать одинаковые для всех пользователей параметры отчетов. Чтобы настроить отчеты о неполадках для текущего пользователя или для всех пользователей, выполните следующие действия:

1. На левой панели Центра поддержки (Action Center) перейдите по ссылке **Настройка центра поддержки (Change Action Center Settings)**.
2. На странице **Настройка центра поддержки (Change Action Center Settings)** в области **Связанные параметры (Related Settings)** перейдите по ссылке **Параметры отчета о неполадках (Problem Reporting Settings)**.
3. На экране будет отображена конфигурация отчетов для текущего пользователя. Если вы можете изменить параметры, значит, право настраивать параметры отчета о неполадках есть и у остальных пользователей. Недоступность параметров говорит о том, что параметры отчета одинаковы для всех пользователей.
4. Если параметры отчета о неисправности задаются отдельно для каждого пользователя, задайте интересующий вас параметр и щелкните **OK**, чтобы сохранить изменения. Доступны следующие параметры:
   - Автоматически проверять наличие решений (Automatically Check For Solutions).
   - Автоматически проверять на наличие новых решений и при необходимости отправлять дополнительные данные отчета (Automatically Check For Solutions And Send Additional Report Data, If Needed).
   - Каждый раз при возникновении проблемы отображать запрос до проверки на наличие решений (Each Time A Problem Occurs, Ask Me Before Checking For Solutions).
   - Не проверять на наличие новых решений (Never Check For Solutions).
5. Если параметры отчета о проблемах заданы на уровне компьютера, щелкните **Изменить параметры отчета для всех пользователей (Change Report Settings For All Users)**, задайте нужный параметр и щелкните **OK**, чтобы сохранить изменения. Доступны следующие параметры:
   - Автоматически проверять наличие решений (Automatically Check For Solutions);

- Автоматически проверять на наличие новых решений и при необходимости отправлять дополнительные данные (Automatically Check For Solutions And Send Additional Data, If Needed).
- Каждый раз при возникновении проблемы отображать запрос до проверки на наличие решений (Each Time A Problem Occurs, Ask Me Before Checking For Solutions).
- Не проверять на наличие новых решений (Never Check For Solutions).
- Разрешить каждому пользователю изменять параметры (Allow Each User To Choose Settings).

Включив создание отчетов о неисправностях, вы можете исключить из отчетов некоторые программы. Выполните следующие действия:

1. На левой панели Центра поддержки (Action Center) перейдите по ссылке **Настройка центра поддержки (Change Action Center Settings)**.
2. На странице **Настройка центра поддержки (Change Action Center Settings)** в области **Связанные параметры (Related Settings)** перейдите по ссылке **Параметры отчета о неполадках (Problem Reporting Settings)**. Далее щелкните ссылку **Выбрать программы, исключаемые из отчета (Select Programs To Exclude From Reporting).**
3. На странице **Дополнительные параметры отчетов о проблемах (Advanced Problem Reporting Settings)** показан список исключенных в данный момент программ. Выполните одно из следующих действий:
   - чтобы добавить программы в список программ, исключенных из отчетов, щелкните **Добавить (Add)** и в открывшемся диалоговом окне выберите исполняемый файл (.exe) программы. Щелкните **Открыть (Open)**;
   - чтобы удалить программы из списка программ, исключенных из отчетов, выделите программу в списке и щелкните **Удалить (Remove)**.

Параметры устранения неисправностей различны для каждого пользователя компьютера. Чтобы настроить параметры устранения неисправностей, выполните следующие действия:

1. В Центре поддержки (Action Center) щелкните заголовок **Обслуживание (Maintenance)**.
2. Под списком текущих неисправностей расположена область **Устранение неполадок: обслуживание системы (Troubleshooting: System Maintenance)**. Перейдите по ссылке **Изменить настройки устранения неполадок (Change Troubleshooting Settings)**.
3. На странице **Настройка (Change Settings)** отображены текущие параметры решения проблем (рис. 8-7). По умолчанию в Windows выполняется периодический поиск решений обычных проблем обслуживания. Если проблему можно решить при помощи внутренних средств для устранения неполадок, отображаются уведомления об этом. Например, пользователь получает уведомления о неиспользуемых файлах и ярлыках.

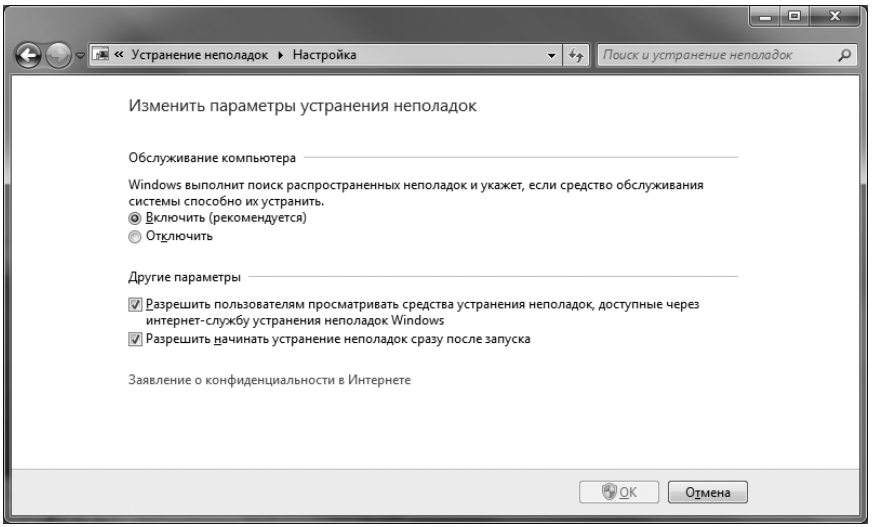

Рис. 8-7. Настройка параметров устранения неполадок

4. Периодически в сети появляются дополнительные инструменты Майкрософт для устранения неисправностей. По умолчанию пользователям разрешено устанавливать и использовать эти средства. Если вы хотите запретить пользователям находить и использовать подобные программы, сбросьте флажок **Разрешить пользователям просматривать средства устранения неполадок, доступные через Интернет-службу устранения неполадок Windows (Allow Users To Browse For Troubleshooters Available From The Windows Online Troubleshooting Service).**
5. По умолчанию после запуска инструмента устранения неполадок его работа начинается незамедлительно. Чтобы затребовать от пользователя подтверждение устранения неполадок, сбросьте флажок **Разрешить начинать устранение неполадок сразу после запуска (Allow Troubleshooting To Begin Immediately When Started)**.
6. Щелкните **OK**, чтобы сохранить параметры.

Автоматическое устранение неполадок обеспечивается компонентом Windows PowerShell 2.0 и связанными системными службами. Инструмент устранения неполадок будет работать, при условии что на компьютере установлен компонент PowerShell (он устанавливается по умолчанию) и работают необходимые службы. Стандартные инструменты устранения неполадок таковы:

- **Aero** Диагностика и устранение неисправностей, нарушающих правильное отображение интерфейса Windows Aero.
- **Оборудование и устройства (Hardware And Device)** Диагностика и устранение неисправностей, препятствующих правильной работе устройств.
- **Домашняя группа (Homegroup Networking** Диагностика и устранение неисправностей, препятствующих общему доступу к файлам в домашней группе.

- **Подключения к Интернету (Internet Connectivity)** Диагностика и устранение неисправностей, нарушающих подключение к Интернету и сетевой доступ.
- **Обслуживание системы (Maintenance)** Выполнение обычных задач обслуживания, которые не выполнены пользователем.
- **Сетевой адаптер (Network Adapter)** Диагностика и решение проблем, связанных с сетевыми адаптерами Ethernet, беспроводными и другими сетевыми адаптерами.
- **Быстродействие (Performance)** Диагностика и устранение неисправностей, влияющих на общую производительность компьютера.
- **Воспроизведение звука (Play Sound)** Диагностика и устранение неисправностей, препятствующих воспроизведению звука.
- **Питание (Power)** Диагностика и устранение неисправностей, влияющих на управление электропитанием, режимы сна, гибернации и выход из этих состояний.
- **Принтер (Printer)** Диагностика и устранение неисправностей, нарушающих работу с принтером.
- **Совместимость программы (Program Compatibility)** Диагностика и устранение неисправностей, мешающих выполнению программ на компьютере.
- **Запись звука (Record Sound)** Диагностика и устранение неисправностей, препятствующих записи звука.
- **Безопасность Internet Explorer (Web Browsing Safety)** Выявление параметров, угрожающих безопасности компьютера и пользователя в Интернете.
- **Windows Media** Диагностика и устранение неисправностей, мешающих воспроизведению музыки и DVD-дисков на компьютере. С его помощью можно вернуть параметры, заданные для проигрывателя Windows Media (Windows Media Player) по умолчанию.

Чтобы открыть любой из этих инструментов, в Центре поддержки (Action Center) прокрутите окно вниз и щелкните **Устранение неполадок (Troubleshooting)**. В открывшемся окне **Устранение неполадок (Troubleshooting)** все инструменты упорядочены по категориям (рис. 8-8):

- **Программы (Programs)** Диагностика и устранение неполадок совместимости приложений, созданных для предыдущих версий Windows.
- **Оборудование и звук (Hardware And Sound)** Диагностика и устранение неполадок устройств для записи и воспроизведения звука.
- **Сеть и Интернет (Network And Internet)** Диагностика и устранение неисправностей сетевых подключений и доступа к общим папкам на других компьютерах.
- **Оформление и персонализация (Appearance And Personalization)** Диагностика и устранение неполадок, связанных с оформлением экрана и па-

раметрами персонализации. Чтобы запустить инструмент устранения неполадок эффектов рабочего стола Aero, перейдите по ссылке **Отображение настольных эффектов Aero (Display Aero Desktop Effects)**.

- **Система и безопасность (System And Security)** Диагностика и устранение неисправностей, связанных с Центром обновления Windows (Windows Update), электропитанием и производительностью. Щелкните **Запуск задач обслуживания (Run Maintenance Tasks)**, чтобы удалить ненужные файлы и ярлыки, а также выполнить другие общие задачи обслуживания.

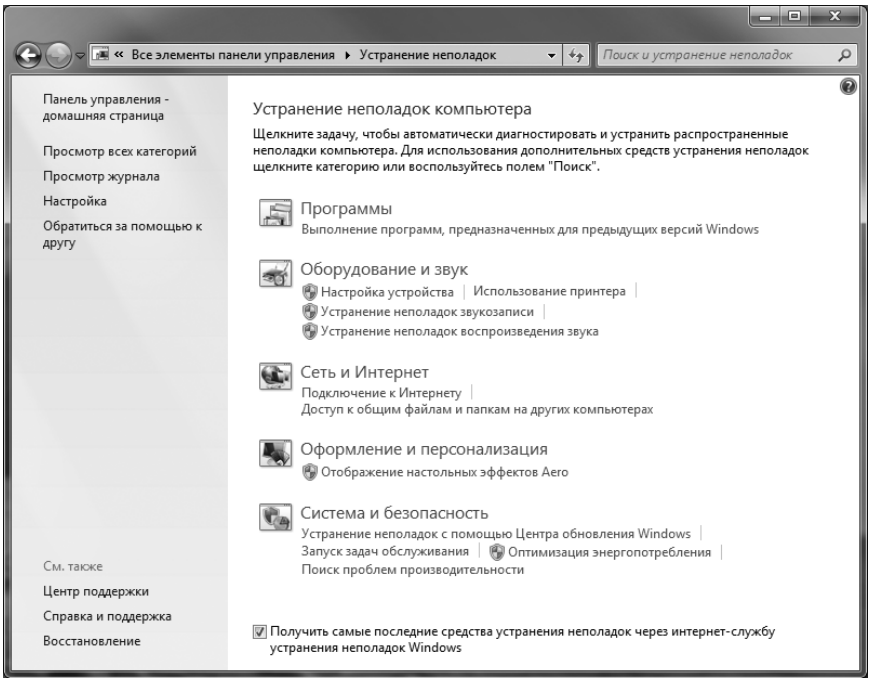

Рис. 8-8. Инструменты для диагностики и устранения неисправностей

По умолчанию в Windows проводится автоматический поиск и установка средств устранения неполадок в сети. Если вы предпочитаете этого не делать, сбросьте флажок **Получить самые последние средства устранения неполадок через Интернет-службу устранения неполадок Windows (Get The Most Up-To-Date Troubleshooters From The Windows Online Troubleshooting Service)**.

В групповой политике параметры диагностики и устранения неисправностей определяются в узле **Конфигурация компьютера\Административные шаблоны\Система\Диагностика (Computer Configuration\Administrative Templates\System\Troubleshooting And Diagnostics)**. Дополнительные сведения о соответствующих политиках приводятся в табл. 8-1.

Табл. 8-1. Политики управления Центром поддержки (Action Center) и связанные с ними политики

Название политики	Описание	Расположение в узле Административные шаблоны (Administrative Templates)
Устранение неполадок: разрешить пользователям доступ к сведениям об устранении неполадок, расположенным на серверах корпорации Майкрософт, из компонента «Устранение неполадок» панели управления (через интернет-службу устранения неполадок Windows (WOTS)) (Troubleshooting: Allow UsersTo Access Online Trouble-shooting Content On Microsoft Servers From The Troubleshooting Control Panel)	Если политика включена или не настроена, пользователи при наличии подключения к Интернету получат доступ к содержимому и смогут выполнять поиск инструментов устранения неполадок. Пользователю достаточно будет щелкнуть **Да (Yes)** в ответ на предложение получить новейшие инструменты устранения неполадок в Центре поддержки (Action Center)	Конфигурация компьютера (Computer Configuration)...Система\Диагностика\Диагностика со сценариями (System\Troubleshooting And Diagnostics\Scripted Diagnostics)
Устранение неполадок: разрешить пользователям запускать мастера устранения неполадок (Troubleshooting: Allow Users To Access And Run Troubleshooting Wizards)	Если политика включена или не задана, пользователи могут запускать инструменты устранения неполадок в Центре поддержки (Action Center)	Конфигурация компьютера (Computer Configuration)...Система\Диагностика\Диагностика со сценариями (System\Troubleshooting And Diagnostics\Scripted Diagnostics)
Удалить значок центра поддержки (Remove The Action Center Icon)	Если эта политика включена, в области уведомлений на панели задач перестает отображаться значок **Центр поддержки (Action Center)**. Это не помешает пользователям открыть Центр поддержки (Action Center) при помощи панели управления	Конфигурация пользователя (User Configuration)...Меню «Пуск» и панель задач (Start Menu And Taskbar)
Отключить программу по улучшению качества программного обеспечения Windows (Turn Off Windows Customer Experience Improvement Program)	Если политика включена, пользователи не участвуют в программе. Если политики отключена, пользователи принимают участие в программе	Конфигурация компьютера (Computer Configuration)...Система\Управление связью через Интернет\Параметры связи через Интернет (System\Internet Communication Management\Internet Communication Settings)

Табл. 8-1. (*продолжение*)

Название политики	Описание	Расположение в узле Административные шаблоны (Administrative Templates)
Отключение доступа к разделу решения проблем производительности (Turn Off Access To The Solutions To Performance Problems Section)	Если политика включена, у пользователей не будет доступа к решениям проблем производительности. В противном случае, пользователи смогут использовать эти решения	Конфигурация компьютера (Computer Configuration) и Конфигурация пользователя (User Configuration)...Система\Панель управления производительностью (System\Performance Control Panel)
Уведомлять о блокированных драйверах (Notify Blocked Drivers)	Если политика включена или не задана, будут выводиться уведомления о драйверах, заблокированных из-за проблем совместимости	Конфигурация компьютера (Computer Configuration)...Система\Диагностика\Диагностика совместимости приложений (System\Troubleshooting And Diagnostics\Application Compatibility Diagnostics)
Обнаруживать сбои приложений, вызванные устаревшими COM-объектами (Detect Application Failures Caused By Deprecated COM Objects)	Если политика включена или не задана, выявляются программы, пытающиеся создавать устаревшие COM-объекты, а пользователи получают уведомления об этом	Конфигурация компьютера (Computer Configuration)...Система\Диагностика\Диагностика совместимости приложений (System\Troubleshooting And Diagnostics\Application Compatibility Diagnostics)
Обнаружение сбоев приложений, вызванных устаревшими библиотеками DLL Windows (Detect Application Failures Caused By Deprecated COM Objects)	Если политика включена или не задана, выявляются программы, пытающиеся использовать устаревшие библиотеки DLL, а пользователи получают уведомления об этом	Конфигурация компьютера (Computer Configuration)...Система\Диагностика\Диагностика совместимости приложений (System\Troubleshooting And Diagnostics\Application Compatibility Diagnostics)
Отключение обработчика совместимости программ (Turn Off Application Compatibility Engine)	Если политика включена, перед запуском приложений БД совместимости не просматривается	Конфигурация компьютера (Computer Configuration)...Компоненты Windows\Совместимость приложений (Windows Components\Application Compatibility)

Табл. 8-1. (*окончание*)

Название политики	Описание	Расположение в узле Административные шаблоны (Administrative Templates)
Отключение помощника по совместимости программ (Turn Off Program Compatibility Assistant)	Если политика включена, то в процессе выполнения запущенных пользователями программ поиск известных проблем совместимости проводится не будет	Конфигурация компьютера (Computer Configuration) и Конфигурация пользователя (User Configuration)... Компоненты Windows\Совместимость приложений (Windows Components\Application Compatibility)
Настроить очередь отчетов (Configure Report Queue)	Если политика включена и настроена, администратор может задавать параметры очереди и уведомлений, связанных с отчетом об ошибке	Конфигурация компьютера (Computer Configuration) и Конфигурация пользователя (User Configuration)...Компоненты Windows\Отчеты об ошибках\Параметры расширенного отчета об ошибках (Windows Components\Windows Error Reporting\Advanced Error Reporting Settings)
Отключить отчеты об ошибках Windows (Disable Windows Error Reporting)	Если политика включена, в Майкрософт не будут отправляться отчеты об ошибках Windows. В противном случае, информация будет отправлена	Конфигурация компьютера (Computer Configuration) и Конфигурация пользователя (User Configuration)...Компоненты Windows\Отчеты об ошибках (Windows Components\Windows Error Reporting)

Службы поддержки

Средства автоматической диагностики и устранения неполадок Windows 7 поддерживаются отдельными компонентами и инструментами, которые предназначены для управления диагностикой, отчетами и средствами поддержки пользователей. Работа компонентов зависит от наличия служб поддержки, установленных в ОС. В узле **Службы (Services)** категории **Службы и приложения (Services And Applications)** консоли **Управление компьютером (Computer Management)** вы увидите целый ряд служб, предназначенных для поддержки системы диагностики и поддержки.

Ключевые службы поддержки Windows 7 перечислены в табл. 8-2. Диагностические компоненты в значительной мере опираются на службы Служба политики диагностики (Diagnostic Policy Service) и Узел системы диагностики (Diagnostic System Host). Связанная с ними служба Узел службы диагностики (Diagnostic Service Host) запускается только при необходимости.

Табл. 8-2. Службы поддержки Windows 7

Название	Описание
Superfetch	Повышение производительности за счет предварительной выборки данных компонентов и приложений на основе статистики использования
Вторичный вход в систему (Secondary Logon)	Обеспечение запуска процессов с другими учетными данными
Диспетчер сеансов диспетчера окон рабочего стола (Desktop Window Manager Session Manager)	Предоставление служб рабочего стола, участвующих в смене пользователя и других функциях управления рабочим столом
Журнал событий Windows (Windows Event Log)	Регистрация событий
Инструментарий управления Windows (Windows Management Instrumentation)	Предоставление сведений об управлении системой
Информация о совместимости приложений (Application Experience)	Обработка запросов к кешу совместимости приложений
Планировщик заданий (Task Scheduler)	Позволяет пользователям настраивать и планировать задания
Поддержка элемента панели управления «Отчеты о проблемах и их решениях» (Problem Reports and Solutions Control Panel Support)	Поддержка отчетов о системных неполадках
Сведения о приложении (Application Information)	Возможность запуска пользователями приложений с дополнительными административными полномочиями
Служба времени Windows (Windows Time)	Синхронизация системного времени с мировым временем
Служба политики диагностики (Diagnostic Policy Service)	Обнаружение проблем, устранение неисправностей и разрешение вопросов, связанных с работой компонентов Windows
Служба помощника по совместимости программ (Program Compatibility Assistant Service)	Поддержка компонента Помощник по совместимости программ (Program Compatibility Assistant)

Табл. 8-2. (*окончание*)

Название	Описание
Служба профилей пользователей (User Profile Service)	Загрузка и выгрузка профилей пользователей во время входа и выхода из системы
Служба регистрации ошибок Windows (Windows Error Reporting Service)	Вывод отчетов об ошибках при зависании приложений и извлечение решений
Служба уведомления о системных событиях (System Event Notification Service)	Наблюдение за системными событиями и уведомления
Служба удаленного управления Windows (Windows Remote Management)	Обеспечение взаимодействия оболочки Windows PowerShell и протокола WS-Management для удаленного управления
Темы (Themes)	Позволяет использовать на компьютере темы и управлять ими
Узел системы диагностики (Diagnostic System Host)	Диагностика, выполняемая в контексте учетной записи Локальная система (LocalSystem)
Узел службы диагностики (Diagnostic Service Host)	Диагностика, выполняемая в контексте учетной записи Локальная служба (LocalService)
Управление приложениями (Application Management)	Обработка запросов на установку, удаление и перечисление ПО, установленного посредством групповой политики
Установщик модулей Windows (Windows Modules Installer)	Поддержка обновлений Windows для рекомендуемых и необязательных компонентов
Фоновая интеллектуальная служба передачи (Background Intelligent Transfer Service)	Передача файлов в фоновом режиме с использованием незанятой полосы пропускания сети
Центр обновления Windows (Windows Update)	Обновление компонентов Windows и других программ

По количеству служб поддержки вы можете оценить сложность справочной системы Windows 7. Она предназначена для автоматического наблюдения за работоспособностью системы, проведения профилактических мероприятий и составления отчетов о сбоях. Данные о производительности и надежности также поставляются программами Монитор производительности (Performance Monitor) и Монитор стабильности системы (Reliability Monitor).

Службы поддержки лежат в основе дополнительных функциональных возможностей поддержки Windows 7. Если критические службы не выполняются или не настроены должным образом, в работе некоторых функций поддержки возможны неполадки. Чтобы просмотреть состояние этих и других служб в консоли **Управление компьютером (Computer Management)**, выполните следующие действия:

1. В меню **Администрирование (Administrative Tools)** выберите команду **Управление компьютером (Computer Management)**. Или откройте панель управления и последовательно щелкните **Система и безопасность (System And Security)** и **Администрирование (Administrative Tools)**. Затем дважды щелкните **Управление компьютером (Computer Management)**.
2. В дереве консоли щелкните правой кнопкой узел **Управление компьютером (Computer Management)** и выберите команду **Подключиться к другому компьютеру (Connect To Another Computer)**. Теперь выберите систему, службы которой вы собираетесь просматривать.

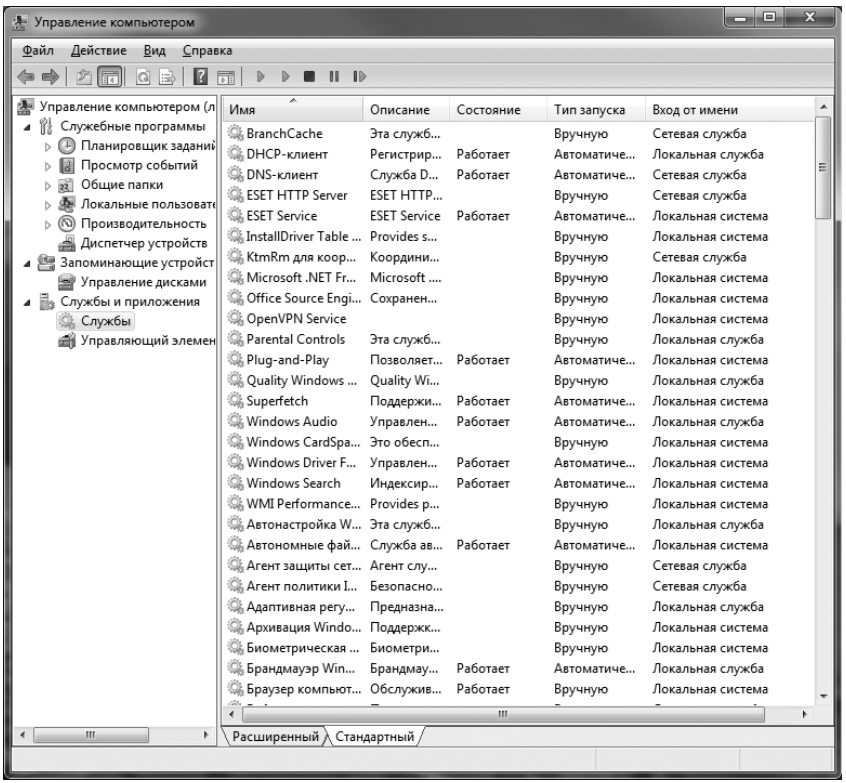

Рис. 8-9. Консоль Службы (Services) предназначена для управления службами Windows 7

3. Разверните узел **Службы и приложения (Services And Applications)**. Выберите элемент **Службы (Services)**, как показано на рис. 8-9. На экране появится полный список установленных в системе служб. По умолчанию службы перечислены в алфавитном порядке. Ключевые поля этого окна таковы:
   - **Имя (Name)** Имя службы. Указаны только установленные в системе службы. Для настройки способа запуска службы дважды щелкните ее.
   - **Описание (Description)** Краткое описание службы и ее назначения.

- **Состояние (Status)** Состояние службы: работает, приостановлена или остановлена (пустое поле — признак того, что служба остановлена).
- **Тип запуска (Startup Type)** Способ запуска службы. Автоматически запускаемые службы запускаются во время загрузки. Службы с ручным запуском должны запускаться пользователями или другими службами. Отключенные службы нельзя запустить, пока они отключены.
- **Вход от имени (Log On As)** Учетная запись, от имени которой служба входит в систему. В большинстве случаев по умолчанию используется учетная запись Локальная система (LocalSystem).

4. У консоли Службы (Services) есть два представления: расширенное (extended) и стандартное (standard). Для переключения между представлениями щелкните соответствующую вкладку в нижней части области сведений. В расширенном представлении отображаются ссылки для быстрого управления службами. Чтобы запустить остановленную службу, щелкните **Запустить (Start)**. Чтобы остановить, а затем снова запустить службу, щелкните **Перезапустить (Restart)**. Для выделенной службы отображается ее описание.

Запуск, остановка и приостановка служб

Администраторам нередко приходится запускать, останавливать и приостанавливать службы Windows. Чтобы запустить, остановить или приостановить службу, выполните следующие действия:

1. В консоли **Управление компьютером (Computer Management)** разверните узел **Службы и приложения (Services And Applications)** и выберите узел **Службы (Services)**.
2. Правой кнопкой щелкните интересующую вас службу и выберите команду **Запустить (Start), Остановить (Stop)** или **Приостановить (Pause)**.

Примечание Команда **Перезапустить (Restart)** останавливает службу и перезапускает ее после небольшой паузы. Если служба приостановлена, для возобновления ее работы щелкните **Продолжить (Resume)**. При сбое в службе, настроенной на автоматический запуск, поле состояния службы пусто. Об этом событии вы, как правило, получите уведомление. Сбои в работе служб могут регистрироваться в журналах событий системы. В Windows 7 можно задать дополнительные действия, предпринимаемые при сбое службы, например, автоматический перезапуск.

Настройка запуска службы

Запуск служб Windows 7 выполняется вручную или автоматически. Также есть возможность отключения службы. Чтобы настроить способ запуска службы, выполните следующие действия:

1. В консоли **Управление компьютером (Computer Management)** разверните узел **Службы и приложения (Services And Applications)** и выберите узел **Службы (Services)**.
2. Правой кнопкой щелкните нужную службу и выберите команду **Свойства (Properties)**.

3. На вкладке **Общие (General)** задайте нужный способ запуска в раскрывающемся списке **Тип запуска (Startup Type)** и щелкните **OK**. Доступны следующие варианты:
   - **Авто (Automatic)** Запуск службы во время загрузки ОС.
   - **Автоматически (отложенный запуск) (Automatic (Delayed Start))** Задержка запуска службы до того момента, когда будут запущены службы, автоматически запускаемые без такой задержки.
   - **Вручную (Manual)** Запуск службы вручную.
   - **Отключена (Disabled)** Служба отключена.

Настройка учетной записи службы

Служб Windows 7 может выполняться от имени системы или от имени конкретного пользователя. Для настройки учетной записи службы, выполните следующие действия:

1. В консоли **Управление компьютером (Computer Management)** разверните узел **Службы и приложения (Services And Applications)** и выберите узел **Службы (Services)**.
2. Правой кнопкой щелкните нужную службу и выберите **Свойства (Properties)**.
3. Перейдите на вкладку **Вход в систему (Log On)**. Выполните одно из следующих действий:
   - Щелкните переключатель **С системной учетной записью (Local System Account)**, если служба должна выполняться от имени системы (стандартный вариант для большинства служб). Если у службы имеется пользовательский интерфейс, установите флажок **Разрешить взаимодействие с рабочим столом (Allow Service To Interact With Desktop)**, чтобы позволить пользователям управлять службой.
   - Щелкните переключатель **С учетной записью (This Account)** для запуска службы от имени учетной записи конкретного пользователя. В соответствующие поля введите имя учетной записи и пароль. Чтобы найти учетную запись, щелкните **Обзор (Browse)**.
4. Щелкните **OK**.

Настройка параметров восстановления службы

Во время установки Windows 7 параметры восстановления критических системных служб настраиваются автоматически. В большинстве случаев, критические службы настроены на автоматический перезапуск при сбое. Их параметры изменить нельзя.

Для настройки параметров восстановления другой службы выполните следующие действия:

1. В консоли **Управление компьютером (Computer Management)** разверните узел **Службы и приложения (Services And Applications)** и выберите узел **Службы (Services)**.

2. Правой кнопкой щелкните нужную службу и выберите **Свойства (Properties)**.
3. Перейдите на вкладку **Восстановление (Recovery)**.
4. Задайте параметры для первой, второй и последующих попыток восстановления. Доступны следующие варианты:
   - **Не выполнять никаких действий (Take No Action)** При данном сбое попыток восстановления предпринято не будет, но такие попытки могут быть предприняты при следующем сбое или могли быть предприняты при прошлом сбое.
   - **Перезапуск службы (Restart The Service)** Остановка и запуск службы после непродолжительной паузы.
   - **Запуск программы (Run A Program)** В случае сбоя будет выполнена программа или сценарий (пакетный файл или сценарий Windows). Выбрав этот вариант, укажите полный путь к исполняемой программе и задайте необходимые параметры командной строки, которые следует передать в программу во время запуска.
   - **Перезагрузка компьютера (Restart The Computer)** Завершение работы и перезагрузка компьютера. Прежде чем выбрать этот вариант, тщательно проверьте параметры в диалоговом окне **Загрузка и восстановление (Startup And Recovery)**. Они должны обеспечивать быструю загрузку системы с параметрами по умолчанию.

Совет Для критических служб следует выбирать такие параметры восстановления: перезапуск службы при первой и второй попытке восстановления, а при третьей попытке — перезагрузка компьютера.

5. Настройте остальные параметры, исходя из заданных вами параметров восстановления. Затем щелкните **OK**. Если в качестве способа восстановления задан запуск программы, настройте параметры на панели **Выполнение программы (Run Program)**. Для перезапуска службы задайте задержку перезапуска. Как правило, достаточно 1–2 минут.

Отключение неиспользуемых служб

В обязанности администратора входит обеспечение безопасности компьютера и сети. При этом работа неиспользуемых служб представляет потенциальную угрозу безопасности. Например, во многих организациях, столкнувшихся с проблемами безопасности, я отмечал работу на компьютерах пользователей лишних компонентов, например Службы веб-публикации (Worldwide Web Publishing Service), протокола SMTP и Службы FTP-публикации (File Transfer Protocol Publishing Service). К сожалению, именно эти службы позволяют анонимным пользователям получать доступ к компьютерам и в отсутствие правильной настройки открывают их для атак.

Обнаружив неиспользуемую службу, вы можете поступить двумя способами. Если служба установлена в составе компонента, возможно, стоит удалить весь компонент. Кроме того, неиспользуемые службы можно просто отключить.

Чтобы отключить службу, выполните следующие действия:

1. В консоли **Управление компьютером (Computer Management)** разверните узел **Службы и приложения (Services And Applications)** и выберите узел **Службы (Services)**.
2. Правой кнопкой щелкните службу и выберите **Свойства (Properties)**.
3. На вкладке **Общие (General)** в раскрывающемся списке **Тип запуска (Startup Type)** выберите **Отключена (Disabled)**.

Отключение работающей службы не приводит к ее остановке. Отключенная служба всего лишь не будет запущена во время следующей загрузки компьютера, поэтому угроза безопасности по-прежнему есть. Чтобы исключить ее, на вкладке **Общие (General)** диалогового окна свойств службы щелкните **Остановить (Stop)**, а затем щелкните **OK**.

Управление службами при помощи предпочтений

Чтобы не настраивать службы на каждом компьютере по отдельности, используйте элементы предпочтения групповой политики. С их помощью вы настроите службы сразу на всех компьютерах, обрабатывающих данный объект GPO. Во время настройки службы при помощи предпочтений по умолчанию установлено значение **Без изменений (No Change)**, для изменения которого необходимо задать новое значение. Как и при ручной настройке служб, предпочтения групповой политики позволяют выполнять следующие действия:

- запускать, останавливать и перезапускать службы;
- изменять способ запуска (вручную, автоматически, автоматически с задержкой, отключено);
- указывать учетную запись, используемую для входа службы в систему;
- задавать параметры восстановления, обрабатываемые при сбое службы.

Далее приводится пример создания элемента предпочтения для управления службой:

1. Откройте объект GPO в оснастке **Редактор управления групповыми политиками (Group Policy Management Editor)** для редактирования. Разверните узел **Конфигурация компьютера\Настройка\Параметры панели управления (Computer Configuration\Preferences\Control Panel Settings)**.
2. Щелкните правой кнопкой узел **Службы (Services)**, выберите команду **Создать (New)** и щелкните **Служба (Service)**. Откроется диалоговое окно **Новые свойства службы (New Service Properties)**, показанное на рис. 8-10.
3. Введите имя настраиваемой службы в поле **Имя службы (Service Name)**. Имя службы отличается от отображаемого имени. Если вы не знаете имени службы, щелкните кнопку справа от поля и выберите службу в списке служб, доступных на данном компьютере. Учтите, что некоторых служб,

работающих на вашем компьютере, может не быть на компьютерах пользователей, и наоборот.

4. Настройте параметры службы для компьютеров пользователей. Параметр обрабатывается только в том случае, если не установлен переключатель **Без изменений (No Change)**.
5. При помощи параметров вкладки **Общие параметры (Common)** задайте методы применения параметров. Как правило, конфигурация службы применяется только один раз. Щелкните **Применить один раз и не применять повторно (Apply Once And Do Not Reapply)**.
6. Щелкните **OK**. Во время следующего обновления политики элемент предпочтения будет применен к объекту GPO, в котором вы его определили.

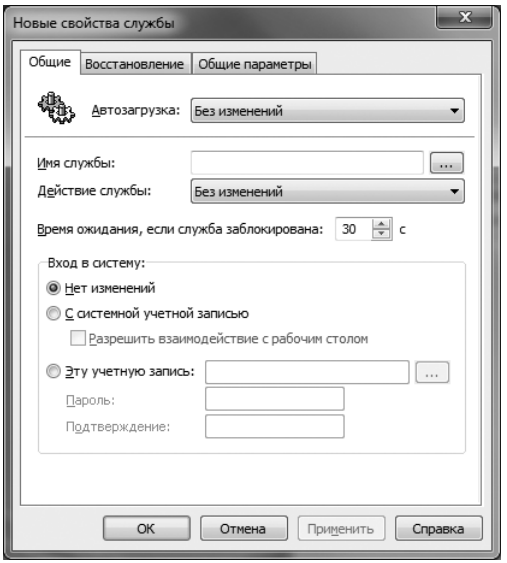

Рис. 8-10. Настройка служб для объекта GPO

Установка и управление оборудованием

На компьютер устанавливаются или подключаются устройства различных типов. Основные типы устройств перечислены ниже:

- **Платы и адаптеры** Платы и адаптеры, устанавливаемые в слоты расширения материнской платы системного блока или в боковые слоты портативного компьютера. Большинство плат и адаптеров имеют разъемы для подключения других устройств.
- **Встроенные дисковые накопители** Существуют накопители разных типов, от Zip-накопителей, CD- и DVD-дисководов до гибких и жестких дисков. К встроенному дисковому накопителю обычно идет два кабеля. Первый предназначен для подключения к материнской плате, другим накопителям или интерфейсной плате, второй — к источнику питания компьютера.

- **Внешние диски и устройства** Подключаются к портам компьютера. Существуют стандартные порты, например, LPT1 или COM1; порты на платах; высокоскоростные последовательные порты, например USB или IEEE-1394 (также называемый FireWire). К внешним устройствам относятся принтеры, сканеры, USB-накопители и большинство цифровых фотоаппаратов.
- **Память** Для расширения общего объема физической памяти, установленной на компьютере, применяются микросхемы памяти. Память устанавливается на материнскую плату или отдельное устройство, например видеоплату. Наиболее широко распространена память с произвольным доступом (RAM).

С точки зрения настройки оборудования Windows 7 отличается от Windows XP и прежних версий. Настройка устройств, установленных на компьютере, но не обнаруженных в процессе обновления или установки ОС, отличается от настройки вновь устанавливаемых устройств.

Установка подключенных устройств

В отличие от Windows XP и предшествующих выпусков, в Windows 7 обнаруживаются устройства, которые не были установлены автоматически во время обновления или установки ОС. Если устройство не установлено из-за отсутствия драйвера, в большинстве случаев оно обнаруживается при помощи встроенных средств диагностики. Затем во время следующего запуска нужный драйвер извлекается из Центра обновления Windows (Windows Update), при условии что обновление Windows включено и вы разрешили обновление драйверов вместе с ОС.

Драйверы, загруженные из Центра обновления Windows, автоматически не устанавливаются. После обновления или установки ОС проверьте наличие обновлений для драйверов и примените обновления, прежде чем устанавливать драйверы другими способами. Ниже перечислены основные этапы проверки наличия обновлений (подробнее об автоматическом обновлении — в главе 17):

1. Щелкните кнопку **Пуск (Start)** и выберите **Панель управления (Control Panel)**.
2. На панели управления последовательно щелкните **Система и безопасность (System And Security)** и **Центр обновления Windows (Windows Update)**.
3. На странице **Центр обновления Windows (Windows Update)** перейдите по ссылке **Поиск обновлений (Check For Updates)**.

Обычно обновления для драйверов устройств отображаются как необязательные. Исключения составляют основные устройства — видеоадаптер, звуковая плата, жесткий диск. Чтобы узнать о наличии обновлений для драйвера устройства, просмотрите все доступные для компьютера обновления, а не только важные. Чтобы установить доступные обновления драйверов устройств, выполните следующие действия:

1. Щелкните кнопку **Пуск (Start)** и выберите **Панель управления (Control Panel)**.
2. На панели управления последовательно щелкните **Система и безопасность (System And Security)** и **Центр обновления Windows (Windows Update)**.
3. На левой панели страницы **Центр обновления Windows (Windows Update)** перейдите по ссылке **Поиск обновлений (Check For Updates)**. В результате поиска важных обновлений может не оказаться (рис. 8-11).

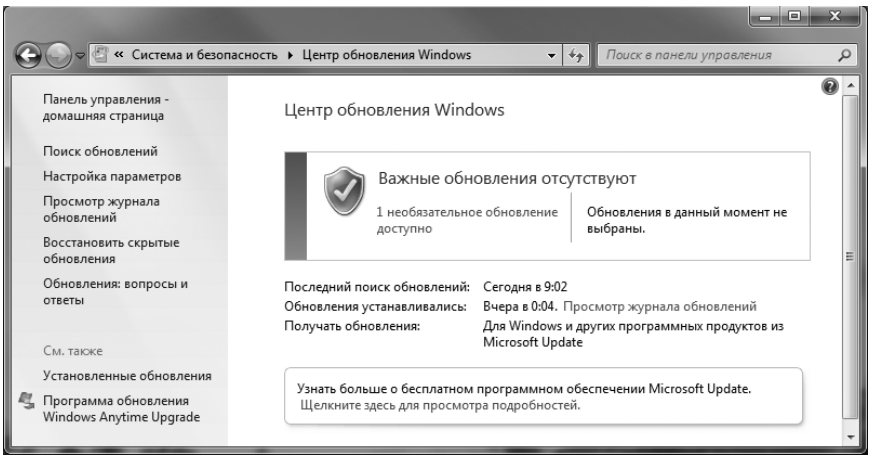

Рис. 8-11. Поиск обновлений

4. Просмотрите необязательные обновления, перейдя по соответствующей ссылке (рис. 8-12).

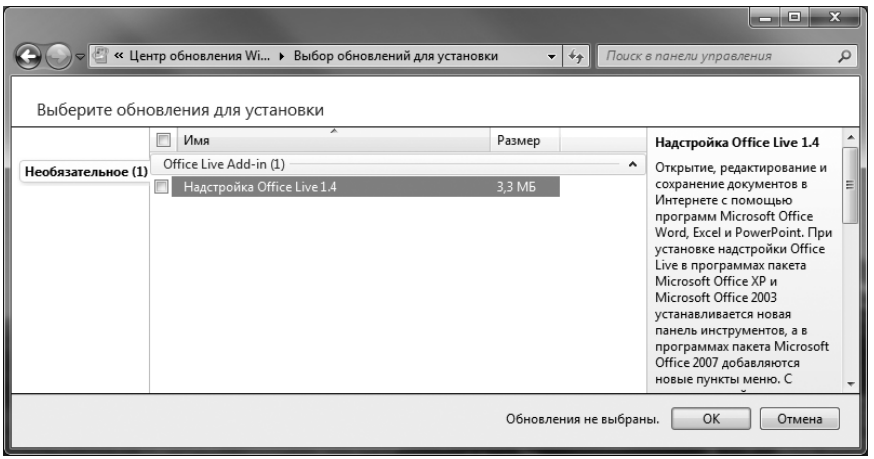

Рис. 8-12. Выберите устанавливаемые обновления

5. Необязательные обновления не устанавливаются по умолчанию. Для установки обновления установите соответствующий флажок, а затем щелкните **OK**, чтобы загрузить и установить обновление.

В течение нескольких минут после установки драйвера устройство будет обнаружено Windows и автоматически установлено. Если устройство обнаружено, но его автоматическая установка невозможна, вы найдете соответствующее решение в Центре поддержки (Action Center). На рис. 8-13 показано возможное решение проблем с оборудованием.

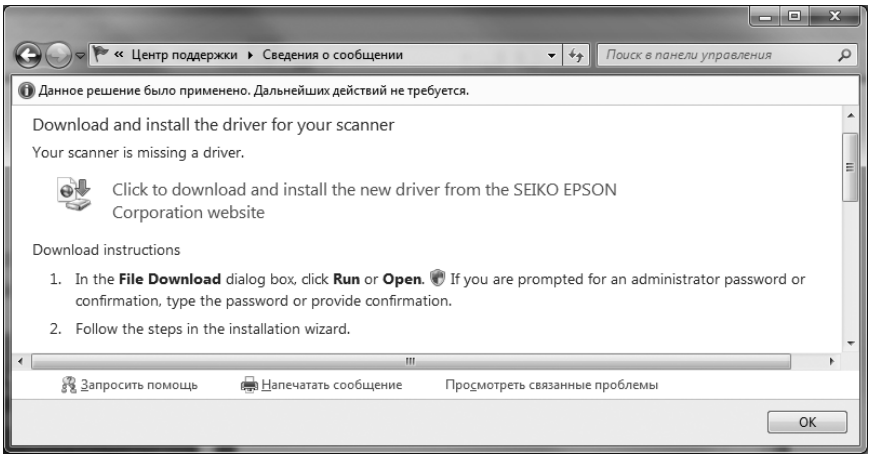

Рис. 8-13. В Центре поддержки (Action Center) вам будет предложено возможное решение проблемы

Установка встроенного оборудования и устройств USB и FireWire

Большинство новых устройств поддерживают технологию Plug and Play. А значит, при их установке, как правило, применяется один из следующих способов:

- Устанавливая встроенное оборудование, ознакомьтесь с инструкцией по установке, поскольку перед установкой устройства может понадобиться предварительная установка драйвера. Затем выключите компьютер, вставьте устройство в соответствующий разъем или подключите его к компьютеру. Включите компьютер, чтобы автоматически обнаружить новое устройство средствами Windows 7.
- Устройства с интерфейсом USB и FireWire следует просто вставить в разъем или подключить к компьютеру, после чего оно будет обнаружено автоматически.

Примечание Как правило, устройства USB и FireWire поддерживают технологию Plug and Play. Если это не так, установите устройство при помощи ПО производителя.

Устройство обнаруживается, а затем устанавливается автоматически при помощи встроенного драйвера Windows 7 (рис. 8-14). На рис. 8-15 показан результат установки в окне **Установка драйверов (Driver Software Installation)**. По завершению установки устройство сразу же начинает работать. Точнее, должно начать работать, что все-таки бывает не всегда. Успех автоматического обнаружения и установки зависит от совместимости устройства с технологией Plug and Play и наличия драйвера устройства.

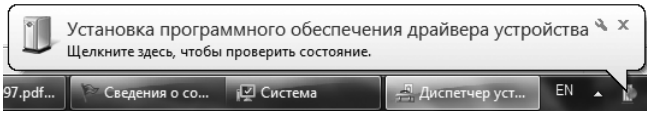

Рис. 8-14. Обнаружение устройства средствами Windows

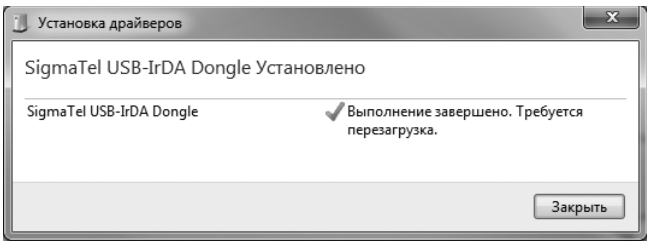

Рис. 8-15. Установка драйвера устройства средствами Windows

В стандартный комплект Windows 7 включено множество драйверов, и устройства, как правило, устанавливаются автоматически. Если параметры Центра обновления Windows (Windows Update) позволяют обновлять драйверы при подключении нового устройства или при его первом обнаружении Windows 7, поиск драйверов проводится автоматически. **В Центре обновления Windows (Windows Update)** драйверы автоматически не устанавливаются. Поэтому для поиска нужного драйвера необходимо проверить наличие обновлений.

Примечание Подробные сведения о поиске драйверов средствами Центра обновления Windows (Windows Update) вы найдете в главе 6, в разделе «Вкладка Оборудование (Hardware)». Из главы 17 вы узнаете, что для работы этой функции необходимо включить Центр обновления Windows (Windows Update).

После обнаружения нового устройства Windows 7 с его установкой в компоненте **Установка программного обеспечения драйвера (Driver Software Installation)** могут возникнуть проблемы. В этом случае будет выведено сообщение об ошибке (рис. 8-16). При этом вы будете немедленно перенаправлены в Центр поддержки (Action Center), где найдете описание проблемы (рис. 8-17).

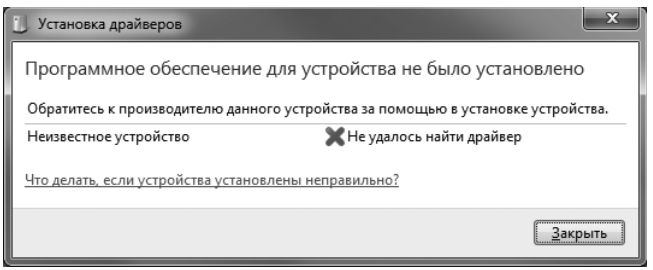

Рис. 8-16. Сбой установки устройства средствами Windows

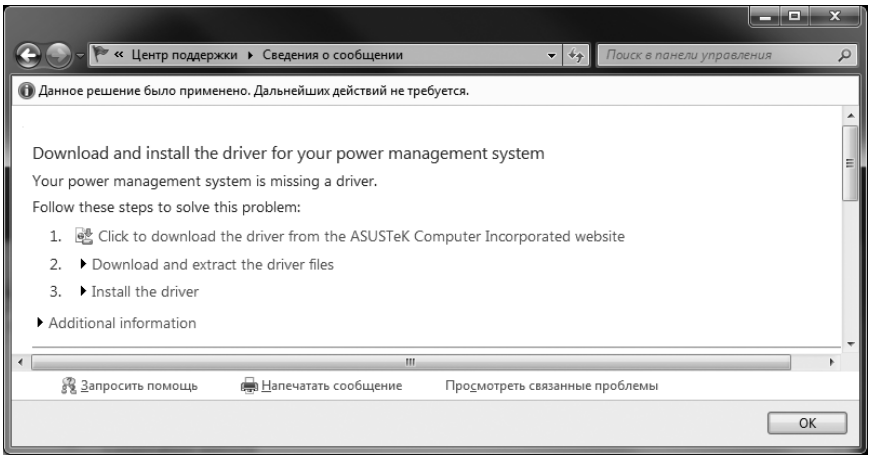

Рис. 8-17. Описание проблемы в Центре поддержки (Action Center)

Если устройство не обнаружено и не установлено средствами Windows 7, попытайтесь найти совместимое ПО для его установки на сайте производителя. При наличии программы установки запустите ее и следуйте инструкциям. Устройство должно установиться правильно.

Примечание Если устройство не удается установить средствами Windows, причина может заключаться в неисправности самого устройства, сбое в драйвере или конфликтом с уже установленным оборудованием. Дополнительные сведения о поиске и устранении неисправностей вы найдете далее, в разделе «Поиск и устранение неисправностей оборудования».

После успешной установки устройства необходимо периодически обслуживать и само устройство, и его драйвер. После выхода новых драйверов протестируйте их в тестовой лаборатории, чтобы выяснить, способны ли новые драйверы решить проблемы, с которыми столкнулись пользователи. Если установка драйверов прошла без неожиданностей и насущные проблемы удалось решить, установите обновленные драйверы на рабочие компьютеры. Чтобы обновить драйвер, выполните следующие действия:

1. Перед установкой нового драйвера почитайте сведения об устройстве и драйвере на каждом компьютере. Обратите особое внимание на расположение, версию и имя файла существующего драйвера.
2. Создайте точку восстановления системы, как описано в главе 17.
3. Установите обновленный драйвер и при необходимости перезагрузите компьютер. Если после перезагрузки компьютер и устройство работают нормально, обновление можно считать успешным.
4. При возникновении сбоев в работе компьютера или устройства после установки драйвера, откатите новый драйвер при помощи Диспетчера устройств (Device Manager). Если компьютер не загружается и драйвер откатить нельзя, восстановите систему с последней удачной конфигурацией, а затем восстановите систему до точки восстановления, созданной на шаге 2.

Установка беспроводных и сетевых устройств, а также устройств Bluetooth

Количество беспроводных и сетевых устройств, а также устройств, поддерживающих технологию Bluetooth, постоянно увеличивается. Среди них беспроводные сетевые адаптеры, накопители, телефоны, клавиатуры, мыши и мультимедийные устройства. Часто они снабжены программами установки, однако перед установкой этих программ убедитесь, что они совместимы с Windows 7. Если совместимости нет, проверьте наличие обновлений ПО на сайте изготовителя.

Некоторые устройства подключаются непосредственно к компьютеру. Другие подключаются к компьютеру через сеть. Чтобы подключить беспроводное устройство или устройство Bluetooth непосредственно к компьютеру, выполните следующие действия:

1. Многие беспроводные устройства и устройства Bluetooth для подключения к компьютеру требуют подключения к нему также и приемника. В других устройствах есть собственный приемник. Например, при подключении комплекта, состоящего из беспроводной клавиатуры и мыши, в разъем USB на компьютере вставляется один общий приемник.
2. Расположите компьютер и приемник таким образом, чтобы приемник находился в зоне распространения сигнала подключаемого устройства. В частности, клавиатура и мышь должны находиться на расстоянии не более 1,8 м от приемника. Расстояние от беспроводного адаптера до маршрутизатора может достигать 30 м.
3. Настройте устройство и подключите электропитание. Перед подключением к компьютеру беспроводного сетевого устройства, его нужно настроить в соответствии с вашей беспроводной сетью. Для обнаружения некоторых беспроводных сетевых устройств их необходимо переключить в режим обнаружения WPS (Wireless Protected Setup).
4. Обнаружение и установка устройства происходит автоматически. Если этого не произошло, выберите в меню **Пуск (Start)** команду **Устройства и принтеры (Devices And Printers)**. Убедитесь, что устройство отсутствует на странице **Устройства и принтеры (Devices And Printers)**. Если устройство не доступно, щелкните **Добавление устройства (Add A Device)** и выполните указания.
5. Если не удается подключить устройство, попытайтесь устранить неполадку следующим образом:
   - Убедитесь, что устройство включено, батареи устройства заряжены и оно не находится в спящем режиме. На корпусах некоторых беспроводных устройств есть кнопка, которую необходимо нажать для установки подключения. В меню других устройств, например, телефонов с Bluetooth, есть параметры, которые необходимо задать, чтобы сделать устройство видимым. На приемнике устройства также может

быть кнопка, включающая режим поиска совместимых беспроводных устройств.

- Если беспроводное устройство или устройство Bluetooth встроено в компьютер, включите соответствующий передатчик. На большинстве ноутбуков есть внешний выключатель передатчика.
- Если устройство расположено далеко от компьютера, переместите его ближе. Если между компьютером и устройством есть стена, попытайтесь установить компьютер и устройство в одной комнате.
- Если проблема связана с размещением, уберите кабели и устройства, вызывающие электромагнитные помехи, например провода питания других устройств, крупные динамики или настольные лампы. Кроме того, устанавливайте устройства подальше от кондиционеров, микроволновых печей и т. п.

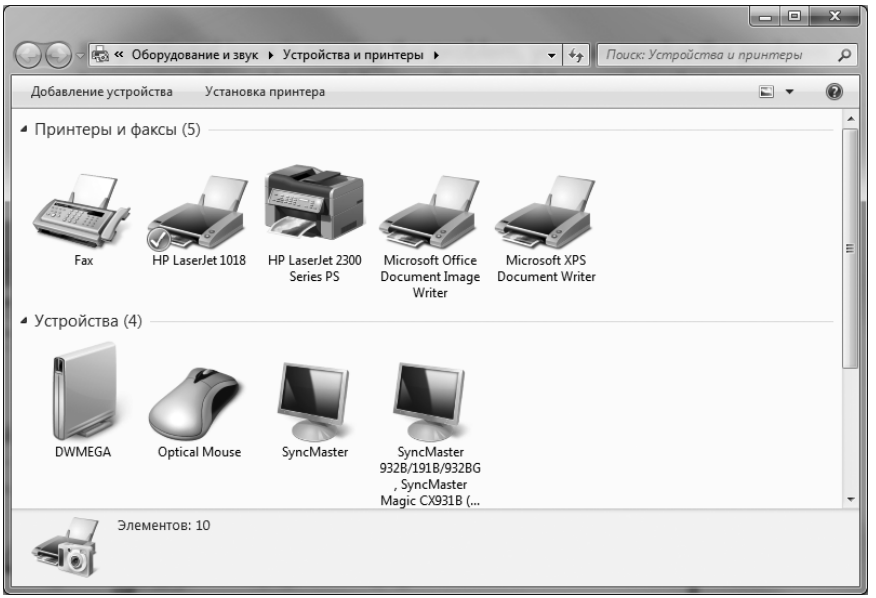

Рис. 8-18. Поиск устройства на странице Устройства и принтеры (Devices And Printers)

Чтобы подключить проводное устройство, беспроводное устройство или устройство Bluetooth через сеть, выполните следующие действия:

1. Подключите устройство к сети и включите его. Затем установите начальные параметры устройства в соответствии с параметрами сети. Например, в параметрах TCP/IP можно задать DHCP или статический IP-адрес.
2. Дождитесь обнаружения устройства. На это может потребоваться до 30 секунд. Обнаружение и установка устройства происходят автоматически. Если этого не произошло, в меню **Пуск (Start)** щелкните **Устройства и принтеры (Devices And Printers)**. На странице **Устройства и принтеры (Devices And Printers)** убедитесь, что устройство есть и оно доступно. Если устройство недоступно, щелкните **Добавление устройства (Add A Device)** и следуйте инструкциям.

3. Если подключить устройство не удается, попытайтесь устранить неполадку следующим образом:
   - Убедитесь, что возможность подключения устройства не блокируется брандмауэром. Чтобы разрешить доступ от компьютера к устройству, может понадобиться открытие порта брандмауэра.
   - Убедитесь, что устройство включено и подключено к той же сети, к которой подключен компьютер. Если сеть состоит из нескольких собой подсетей, попытайтесь подключить устройство и компьютер к одной подсети.
   - Убедитесь, что параметры устройства позволяют ему передавать в сеть информацию о своем присутствии. Большинство устройств делают это автоматически.
   - Проверьте корректность IP-адреса устройства и правильность настройки сети. Если используется протокол DHCP, при подключении устройств к сети IP-адреса присваиваются им автоматически.

Примечание Не все обнаруженные устройства можно подключить к компьютеру. Сведения о возможности подключения устройства к компьютеру вы найдете в документации устройства или на сайте изготовителя.

Ближе к реальности Параметры сетевого обнаружения влияют на способность компьютера находить другие компьютеры в сети и способность других компьютеров находить этот компьютер. По умолчанию сетевое обнаружение блокируется брандмауэром Windows (Windows Firewall). Чтобы включить сетевое обнаружение, выполните следующие действия:

1. Откройте панель управления и щелкните **Сеть и Интернет (Network And Internet)**.
2. Щелкните **Центр управления сетями и общим доступом (Network And Sharing Center)**.
3. На левой панели щелкните **Изменить дополнительные параметры общего доступа (Change Advanced Sharing Settings)**.
4. В области **Сетевое обнаружение (Network Discovery)** щелкните **Включить сетевое обнаружение (Turn On Network Discovery)**, затем щелкните **Сохранить изменения (Save Changes)**.

Установка локальных и сетевых принтеров

Существуют различные способы подключения принтеров к компьютеру. Некоторые принтеры подключаются непосредственно к компьютеру и называются *локальными* (local). Другие подключаются к компьютеру через сеть — это *сетевые* (network) принтеры. К сетевым относятся все принтеры сети, включая принтеры с интерфейсом Bluetooth, беспроводные принтеры, а также принтеры, подключенные к другому компьютеру, если к ним открыт общий доступ по сети.

Большинство принтеров снабжено программами установки, используемыми для первоначальной настройки принтера. Если принтер непосред-

ственно подключен к компьютеру, такое ПО обычно используется один раз для установки принтера и подключения к нему. Программу установки сетевого принтера, как правило, запускают один раз на управляющем компьютере. С ее помощью принтер подготавливается к работе, и на каждом компьютере, на котором он будет использоваться, создаются подключения к принтеру.

Установка локального принтера

Принтер с интерфейсом USB подключается непосредственно к компьютеру и автоматически обнаруживается и устанавливается средствами Windows. Если принтер подключается через последовательный или параллельный порт, его придется установить вручную. Чтобы установить принтер вручную, выполните следующее:

1. Включите питание принтера. В меню **Пуск (Start)** откройте **Устройства и принтеры (Devices And Printers)**. На странице **Устройства и принтеры (Devices And Printers)** убедитесь, что принтера нет в списке доступных устройств. Если принтер недоступен, установите его, выполнив оставшиеся шаги.
2. На странице **Устройства и принтеры (Devices And Printers)** щелкните **Установка принтера (Add A Printer)**. В мастере Установка принтера (Add Printer) выберите **Добавить локальный принтер (Add A Local Printer)**.
3. В списке **Использовать существующий порт (Use An Existing Port)** укажите порт, к которому подключен принтер, и щелкните **Далее (Next)**.
4. Выберите производителя и модель принтера. Щелкните **Далее (Next)**.
5. Если принтер отсутствует в списке, но у вас есть установочный диск, щелкните **Установить с диска (Have Disk)**, затем найдите папку с драйверами для принтера. Справочную информацию вы найдете в инструкции к принтеру.
6. Если установочного диска нет, щелкните **Центр обновления Windows (Windows Update)** и дождитесь завершения поиска имеющихся драйверов.
7. Выполните оставшиеся шаги в программе установки. Затем щелкните **Готово (Finish)**. Чтобы убедиться в работоспособности принтера, напечатайте пробную страницу.

Управление локальными принтерами при помощи предпочтений групповой политики рекомендуется в тех случаях, когда настройка выполняется только для компьютеров, на которых действительно установлены локальные принтеры.

Чтобы создать элемент предпочтения для создания, обновления, замены или удаления локальных принтеров, выполните следующие действия:

1. В оснастке **Редактор управления групповыми политиками (Group Policy Management Editor)** откройте для редактирования объект GPO. Чтобы настроить предпочтения для компьютеров, последовательно разверните узлы **Конфигурация компьютера\Настройки\Параметры панели**

управления (Computer Configuration\Preferences\Control Panel Settings) и выделите **Принтеры (Printers)**. Чтобы настроить предпочтения для пользователей, последовательно разверните узлы **Конфигурация пользователя\Настройки\Параметры панели управления (User Configuration\Preferences\Control Panel Settings)** и выберите **Принтеры (Printers)**.

2. Щелкните правой кнопкой узел **Принтеры (Printers)**, выберите команду **Создать (New)** и щелкните **Локальный принтер (Local Printer)**.
3. В открывшемся диалоговом окне **Новые свойства локального принтера (New Local Printer Properties)** в списке **Действие (Action)** выберите **Создать (Create)**, **Обновить (Update)**, **Заменить (Replace)** или **Удалить (Delete)**.
4. В поле **Имя (Connection)** введите имя принтера. В случае создания принтера оно будет использовано для нового локального принтера. При обновлении, замене или удалении принтера это имя должно совпадать с именем целевого принтера.
5. В списке **Порт (Port)** выберите порт, к которому подключен локальный принтер.
6. В поле **Путь к принтеру (Printer Path)** введите путь к общему принтеру в формате UNC. Тип общего принтера должен совпадать с типом локального принтера. В элементе предпочтения он будет использован как источник файлов для установки драйверов.
7. Укажите способ применения предпочтения на вкладке **Общие параметры (Common)**. Вы собираетесь принудительно применить элемент управления, поэтому данный параметр должен применяться при каждом обновлении групповой политики. Не устанавливайте параметр **Применить один раз и не применять повторно (Apply Once And Do Not Reapply)**.
8. Щелкните **OK**. Во время следующего обновления политики элемент предпочтения будет применен к объекту GPO, в котором вы его определили.

Чтобы создать элемент предпочтения для управления общим локальным принтером, выполните следующие действия:

1. В оснастке **Редактор управления групповыми политиками (Group Policy Management Editor)** откройте объект GPO для редактирования. Последовательно разверните узлы **Конфигурация пользователя\Настройки\Параметры панели управления (User Configuration\Preferences\Control Panel Settings)** и выделите **Принтеры (Printers)**.
2. Щелкните правой кнопкой узел **Принтеры (Printers)**, выберите команду **Создать (New)** и щелкните **Общий принтер (Shared Printer)**.
3. В открывшемся диалоговом окне **Новые свойства общего принтера (New Shared Printer Properties)** в списке **Действие (Action)** выберите **Создать (Create)**, **Обновить (Update)**, **Заменить (Replace)** или **Удалить (Delete)**. Если предпочтение создается для удаления, вы можете попутно удалить все подключения общего принтера. Выберите действие **Удалить**

(Delete) и установите флажок **Удалить все подключения общих принтеров (Delete All Shared Printer Connections)**.

4. В поле **Путь к общему ресурсу (Share Path)** введите путь к общему принтеру в формате UNC.
5. Если нужно, сделайте принтер принтером по умолчанию. Если вы создаете, обновляете или заменяете подключение общего принтера и хотите, чтобы подключение было доступно при каждом входе пользователя в систему, включите параметр **Повторное подключение (Reconnect)**.
6. При необходимости укажите локальный порт, с которым сопоставлено общее подключение. Если настраивается действие **Удалить (Delete)**, общий принтер, связанный с данным локальным портом, будет удален. В качестве альтернативы при выборе действия **Удалить (Delete)** можно отменить сопоставление со всеми локальными портами.
7. Укажите способ применения предпочтения на вкладке **Общие параметры (Common)**. Вы собираетесь принудительно применить элемент управления, поэтому данный параметр должен применяться при каждом обновлении групповой политики. Не устанавливайте параметр **Применить один раз и не применять повторно (Apply Once And Do Not Reapply)**.
8. Щелкните **OK**. Во время следующего обновления политики элемент предпочтения будет применен к объекту GPO, в котором вы его определили.

Установка сетевого и беспроводного принтера, а также принтера с интерфейсом Bluetooth

Если в принтере используется беспроводное подключение или подключение Bluetooth, подготовка компьютера и принтера выполняется так же, как и в случае других устройств. Подробно это описано в разделе «Установка беспроводных и сетевых устройств, а также устройств Bluetooth», за исключением того что подключение к принтеру выполняется аналогично подключению к сетевому принтеру.

Чтобы подключиться к сетевому принтеру, в меню **Пуск (Start)** откройте **Устройства и принтеры (Devices And Printers)**. На странице **Устройства и принтеры (Devices And Printers)** убедитесь, что принтера нет в списке доступных устройств. Если принтер недоступен, выполните следующие действия:

1. На странице **Устройства и принтеры (Devices And Printers)** щелкните **Установка принтера (Add A Printer)**. В мастере Установка принтера (Add Printer) выберите **Добавить сетевой, беспроводной или Bluetooth-принтер (Add A Network, Wireless Or Bluetooth Printer)**.
2. В списке доступных принтеров выберите нужный принтер и щелкните **Далее (Next)**.
3. При необходимости установите на компьютер драйвер принтера.
4. Выполните инструкции программы установки. Завершив работу, щелкните **Готово (Finish)**. Чтобы убедиться в работоспособности принтера, напечатайте пробную страницу.

5. Если подключить принтер не удается, попытайтесь устранить неполадку следующим образом:
   - Убедитесь, что возможность подключения к принтеру не блокирована брандмауэром. Чтобы разрешить доступ от компьютера к принтеру, может понадобиться открытие порта брандмауэра.
   - Убедитесь, что принтер включен и подключен к той же сети, что и компьютер. Если сеть состоит из нескольких подсетей, попытайтесь подключить принтер и компьютер к одной подсети.
   - Убедитесь, что параметры принтера позволяют ему передавать в сеть информацию о своем присутствии. Большинство сетевых принтеров делают это автоматически.
   - Проверьте наличие у принтера IP-адреса и правильность настройки сети. Если используется протокол DHCP, при подключении устройств к сети им автоматически присваиваются IP-адреса.

Сетевыми принтерами можно управлять при помощи предпочтений групповой политики. Чтобы создать, обновить, заменить или удалить подключение к сетевому принтеру, выполните следующие действия:

1. В оснастке **Редактор управления групповыми политиками (Group Policy Management Editor)** откройте объект GPO для редактирования. Чтобы настроить предпочтения для компьютеров, последовательно разверните узлы **Конфигурация компьютера\Настройка\Параметры панели управления (Computer Configuration\Preferences\Control Panel Settings)** и выделите **Принтеры (Printers)**. Чтобы настроить предпочтения для пользователей, последовательно разверните узлы **Конфигурация пользователя\Настройка\Параметры панели управления (User Configuration\Preferences\Control Panel Settings)** и выберите **Принтеры (Printers)**.
2. Щелкните правой кнопкой узлы **Принтеры (Printers)**, выберите команду **Создать (New)** и щелкните **TCP/IP-принтер (TCP/IP Printer)**.
3. В открывшемся диалоговом окне **Новые свойства TCP/IP-принтера (New TCP/IP Printer Properties)** в списке **Действие (Action)** выберите **Создать (Create)**, **Обновить (Update)**, **Заменить (Replace)** или **Удалить (Delete)**.
4. Выполните одно из следующих действий:
   - Для подключения к принтеру при помощи IP-адреса введите адрес в поле **IP-адрес (IP Address)**.
   - Чтобы подключиться к принтеру при помощи DNS-имени, задайте параметр **Использовать DNS-имя (Use DNS Name)** и введите FQDN-имя принтера.
5. В поле **Локальное имя (Local Name)** введите локальное имя принтера. Если вы создаете подключение принтера, данное имя будет отображаться на компьютерах пользователей. При обновлении, замене или удалении подключения принтера это имя должно совпадать с именем целевого принтера.

6. В поле **Путь к принтеру (Printer Path)** введите путь к общему принтеру в формате UNC. Тип общего принтера должен совпадать с типом настраиваемого сетевого принтера. В элементе предпочтения принтер будет использован как источник файлов для установки драйверов.
7. Если нужно, сделайте принтер принтером по умолчанию.
8. На вкладке **Параметры порта (Port Settings)** укажите протокол, номер порта и другие параметры.
9. Укажите способ применения предпочтения на вкладке **Общие параметры (Common)**. Вы собираетесь принудительно применить элемент управления, поэтому данный параметр должен применяться при каждом обновлении групповой политики. Не устанавливайте параметр **Применить один раз и не применять повторно (Apply Once And Do Not Reapply)**.
10. Щелкните **OK**. Во время следующего обновления политики элемент предпочтения будет применен к объекту GPO, в котором вы его определили.

Знакомство с диспетчером устройств

Диспетчер устройств (Device Manager) предназначен для просмотра и настройки оборудования. Вам предстоит много работать с этой программой, поэтому она заслуживает отдельного рассмотрения.

Чтобы открыть Диспетчер устройств (Device Manager) и просмотреть подробный список всех установленных на компьютере устройств, выполните следующие действия:

1. В меню **Администрирование (Administrative Tools)** выберите команду **Управление компьютером (Computer Management)**. Или откройте панель управления и последовательно щелкните **Система и безопасность (System And Security)** и **Администрирование (Administrative Tools)**. Затем дважды щелкните **Управление компьютером (Computer Management)**.

Примечание Для подключения к удаленному компьютеру правой кнопкой щелкните узел **Управление компьютером (Computer Management)** и выберите команду **Подключиться к другому компьютеру (Connect To Another Computer)**. Щелкните **Другим компьютером (Another Computer)** и введите полное имя целевого компьютера или найдите компьютер, щелкнув **Обзор (Browse)**. Щелкните **OK**.

2. В консоли Управление компьютером (Computer Management) разверните узел **Служебные программы (System Tools)** и выберите узел **Диспетчер устройств (Device Manager)**. На экране появится полный список установленных в системе устройств (рис. 8-19). По умолчанию устройства упорядочены по типу.
3. Щелкните значок «+» рядом с типом устройства, чтобы просмотреть список конкретных экземпляров устройств данного типа.

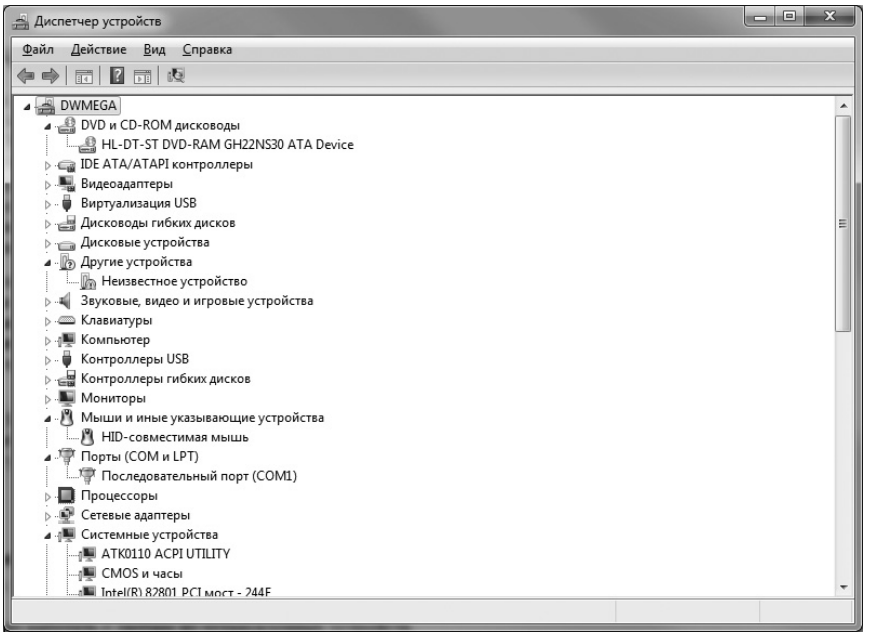

Рис. 8-19. Работа с оборудованием в Диспетчере устройств (Device Manager)

В Диспетчере устройств (Device Manager) можно работать с любым из установленных устройств. Щелкните запись устройства правой кнопкой, чтобы открыть контекстное меню. Команды меню зависят от типа устройства, но есть и общие для всех команды:

- **Свойства (Properties)** Отображение диалогового окна свойств устройства.
- **Удалить (Uninstall)** Удаление устройства и его драйверов.
- **Отключить (Disable)** Отключение устройства без удаления.
- **Задействовать (Enable)** Включение отключенного устройства.
- **Обновить драйверы (Update Driver Software)** Запуск мастера Обновление драйверов (Hardware Update).
- **Обновить конфигурацию оборудования (Scan For Hardware Changes)** Повторная проверка конфигурации оборудования.

Совет В списке оборудования устройства с неполадками отмечены предупреждающими знаками. Желтый треугольник с восклицательным знаком указывает на наличие неполадки в устройстве. Красный крестик свидетельствует о неправильной установке или отключении устройства пользователем или администратором.

Меню **Вид (View)** консоли **Управление компьютером (Computer Management)** позволяет изменять типы отображаемых устройств и порядок сортировки. Доступны следующие возможности:

- **Устройства по типу (Devices By Type)** Отображение установленных устройств по типу оборудования, например дисковый накопитель или

принтер. Под типом указано имя устройства. Этот способ отображения используется по умолчанию.

- **Устройства по подключению (Devices By Connection)** Отображение устройств по типу подключения, например, устройств подключенных к шине PCI компьютера.
- **Ресурсы по типу (Resources By Type)** Отображение состояния выделенных ресурсов по типу устройства, использующего ресурс. Типы ресурсов таковы: каналы прямого доступа к памяти (DMA), порты ввода-вывода, запросы на прерывание (IRQ) и адреса памяти.
- **Ресурсы по подключению (Resources By Connection)** Отображение состояния выделенных ресурсов по типу подключения, а не по типу устройства. Данное представление позволяет, в частности, выполнять трассировку ресурсов в соответствии с их подключением к шине PCI, портам и т. д.
- **Показать скрытые устройства (Show Hidden Devices)** Отображение не только стандартных, но и скрытых устройств. Добавляются устройства, не поддерживающие технологию Plug and Play, а также физически отключенные устройства, драйверы для которых не были удалены.

Драйверы устройств

Каждому установленному на компьютере устройству соответствует связанный с ним драйвер. В драйвере содержится описание того, как ОС следует управлять устройством на уровне аппаратных абстракций (HAL). На этом уровне обрабатываются низкоуровневые задачи взаимодействия ОС и оборудования. В ходе установки оборудования вы сообщаете системе о том, какой драйвер устройства следует использовать. С этого момента драйвер устройства загружается автоматически и работает как часть ОС.

Общие сведения о драйверах устройств

В Windows 7 имеется обширная библиотека драйверов. В базовой установке ОС драйверы находятся в *репозитории* (file repository) хранилища драйверов. Иногда обновления хранилища драйверов включают в пакеты обновлений. На 32-разрядных компьютерах хранилище 32-разрядных драйверов находится в папке %SystemRoot%\System32\DriverStore. На 64-разрядных компьютерах хранилище 64-разрядных драйверов находится в папке %SystemRoot%\System32\DriverStore, а 32-разрядные драйверы хранятся в папке %SystemRoot%\SysWOW64\DriverStore. В папке DriverStore есть вложенные папки, содержащие локализованные сведения о драйверах. Каждому языковому компоненту, установленному в системе, соответствует вложенная папка. Например, сведения о драйверах, локализованных для России, находятся в папке ru-RU.

Все драйверы хранилища имеют сертификаты, подтверждающие полную совместимость с Windows 7. Их подлинность подтверждена цифровой под-

писью Майкрософт. Во время установки нового устройства Plug and Play в хранилище драйверов производится поиск совместимого драйвера. Если драйвер найден, устройство устанавливается автоматически.

У каждого драйвера есть свой информационный файл установки с расширением INF. Это текстовый файл с подробными сведениями о конфигурации устанавливаемого устройства. В информационном файле перечислены также все исходные файлы (с расширением SYS), используемые драйвером. Кроме того, в драйверах используются файлы с расширениями PNF и DLL. С некоторыми драйверами сопоставлены манифесты компонентов (.AMX) в формате XML. В них содержатся подробные сведения о цифровой подписи драйвера и информация Plug and Play, используемая при автоматической самонастройке устройства.

В папке Drivers у всех установленных в системе драйверов имеется исходный файл (SYS). Во время установки нового драйвера он записывается в папку, вложенную в папку Drivers, а параметры конфигурации сохраняются в реестре. Файл INF драйвера предназначен для управления установкой и записью параметров реестра. Если драйвера еще нет в хранилище, то в системе нет ни его INF-файла, ни других связанных с ним файлов. В этом случае во время установки устройства INF-файл и другие связанные с драйвером файлы записываются в подпапку папки DriverStore\FileRepository.

Подписанные и неподписанные драйверы устройств

Все драйверы устройств, находящиеся в кеше драйверов, имеют цифровую подпись, указывающую, что драйвер прошел всестороннее тестирование в лаборатории Windows Hardware Quality Lab. Драйверы с цифровыми подписями Майкрософт не могут стать причиной выхода из строя или нестабильности системы. Наличие цифровой подписи Майкрософт также гарантирует подлинность драйвера. Если у драйвера нет цифровой подписи Майкрософт, значит он не прошел тестирование или его файлы были изменены после установки другой программой. Неподписанные драйверы скорее станут причиной зависаний или отказа ОС, чем все установленные программы.

Во избежание проблем с неподписанными драйверами при попытке установить неподписанный драйвер устройства в Windows 7 по умолчанию выводится предупреждение. Кроме того, в Windows можно запретить установку устройств некоторых типов. Управление параметрами драйверов устройств на компьютерах организации осуществляется в групповой политике. Также в групповой политике определяется возможность и способ установки драйверов.

Параметры установки устройств для отдельных компьютеров находятся в узле **Конфигурация компьютера\Административные шаблоны\Система\Установка устройства (Computer Configuration\Administrative Templates\System\Device Installation)**.

Совет Неудачная попытка установить устройство может быть следствием ограничений, примененных в групповой политике. Чтобы установить устройство, необходимо перекрыть групповую политику.

Получение сведений о драйвере

У всех драйверов, используемых в системе, есть связанные с ними файлы. Чтобы просмотреть расположение файлов драйвера и другие сведения о них, выполните следующие действия:

1. Откройте консоль **Управление компьютером (Computer Management)** и разверните узел **Служебные программы (System Tools)**.
2. Выберите **Диспетчер устройств (Device Manager)**. На экране появится полный список устройств, установленных в системе. По умолчанию устройства упорядочены по типу.
3. Правой кнопкой щелкните нужное устройство и выберите команду **Свойства (Properties)**. Откроется диалоговое окно **Свойства (Properties)**.
4. На вкладке **Драйвер (Driver)** щелкните **Сведения (Driver)**, чтобы открыть диалоговое окно **Сведения о файлах драйверов (Driver File Details)**. Здесь вы найдете следующую информацию (рис. 8-20):
   - **Файлы драйверов (Driver Files)** Отображение полного пути к файлу драйвера.
   - **Поставщик (Provider)** Создатель драйвера.
   - **Версия файла (File Version)** Версия файла.

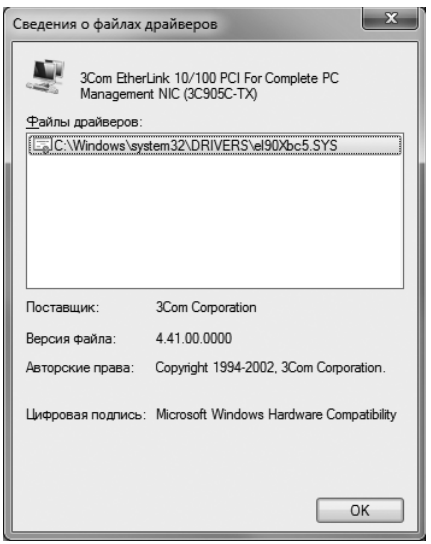

Рис. 8-20. В диалоговом окне Сведения о файлах драйверов (Driver File Details) приводится информация о расположении файлов драйвера, поставщике и версии

Установка и обновление драйверов устройств

Необходимым условием работы без сбоев является обновление драйверов устройств. Установка и обновление драйверов выполняется в программах **Новое оборудование (Found New Hardware)**, **Установка оборудования (Add Hardware)** и **Обновление драйверов (Update Driver Software)**. По умолчанию поиск обновлений драйверов устройств выполняется в следующих расположениях:

- локальный компьютер;
- установочный компакт-диск;
- сайт Центр обновления Windows (Windows Update) или сервер обновлений предприятия.

Далее перечислены параметры групповой политики, управляющие получением сведений об устройствах и поиском драйверов:

- **Отключить доступ ко всем возможностям Центра обновления Windows (Turn Off Access To All Windows Update Features)** Этот параметр расположен в узле **Конфигурация компьютера\Административные шаблоны\Система\Управление связью через Интернет\Параметры связи через Интернет (Computer Configuration\Administrative Templates\System\Internet Communication Management\Internet Communication Settings)**. Если он включен, все возможности Центра обновления Windows (Windows Update) блокируются, становясь недоступными для пользователей. Пользователи также не смогут посетить сайт Центр обновления Windows (Windows Update).
- **Отключение поиска драйвера устройств в Центре обновления Windows (Turn Off Windows Update Device Driver Searching)** Этот параметр расположен в узле **Конфигурация компьютера\Административные шаблоны\Система\Управление связью через Интернет\Параметры связи через Интернет (Computer Configuration\Administrative Templates\System\Internet Communication Management\Internet Communication Settings)**. По умолчанию при установке устройства имеется поиска драйверов в Центре обновления Windows (Windows Update). Если включить этот параметр, во время установки нового устройства поиск драйвера в Центре обновления Windows (Windows Update) проводится не будет. Если параметр отключен, поиск в Центре обновления Windows (Windows Update) будет выполняться при каждой установке нового устройства, при условии отсутствии драйверов в локальной системе.
- **Задать порядок поиска в исходных расположениях драйверов устройств (Specify Driver Source Search Order)** Этот параметр расположен в узле **Конфигурация компьютера\Административные шаблоны\Система\Установка устройства (Computer Configuration\Administrative Temp-lates\System\Device Installation)**. Если он отключен или не задан, вы можете задать расположение для поиска драйверов на каждом

компьютере. Включив параметр политики, можно сделать так, что поиск драйверов в Центре обновления Windows (Windows Update) во время установки устройства будет проводиться в первую или в последнюю очередь, либо не будет проводиться вообще.

- **Настроить время ожидания установки устройства (Configure Device Installation Time-Out)** Этот параметр расположен в узле **Конфигурация компьютера\Административные шаблоны\Система\Установка устройства (Computer Configuration\Administrative Templates\System\Device Installation)**. Если он отключен или не задан, время ожидания завершения установки устройства составляет 5 мин. Затем установка будет отменена. Включив данную политику, вы сможете задать другое время ожидания отмены установки.
- **Запретить получение метаданных устройств из Интернета (Prevent Device Metadata Retrieval From The Internet)** Этот параметр расположен в узле **Конфигурация компьютера\Административные шаблоны\Система\Установка устройства (Computer Configuration\Administrative Templates\System\Device Installation)**. Если он отключен или не задан, для обновления устройств используются метаданные установленных устройств, загруженные из Интернета. Если включить параметр, метаданные установленных устройств не будут извлекаться из Интернета.

Чтобы установить или обновить драйверы устройства, выполните следующие действия:

1. Откройте консоль **Управление компьютером (Computer Management)** и разверните узел **Служебные программы (System Tools)**.
2. Выделите элемент **Диспетчер устройств (Device Manager)**. На экране появится полный список установленных в системе устройств. По умолчанию устройства упорядочены по типу.
3. Правой кнопкой щелкните нужное устройстве и выберите команду **Обновить драйверы (Update Driver Software)**. Дальнейшие действия выполняются в мастере Обновление драйверов (Update Driver Software).

Ближе к реальности Обновление драйверов расширяет функциональность устройства, улучшает его рабочие характеристики и устраняет неполадки. Но старайтесь не устанавливать самые новые драйверы на компьютеры пользователей без тестирования в тестовой среде. Сначала тестирование, потом установка.

4. Выберите автоматическую или ручную установку драйверов посредством выбора драйвера из списка или поиска драйвера в указанном расположении (рис. 8-21).
5. При автоматической установке драйвера выполняется поиск и последующая установка его новейшей версии. Если более новой версии драйвера не найдено, сохраняется текущий драйвер. Щелкните **Закрыть (Close)** для завершения процесса обновления. Пропустите оставшиеся шаги.
6. Если вы выбрали ручную установку драйвера, выберите одну из следующих возможностей:

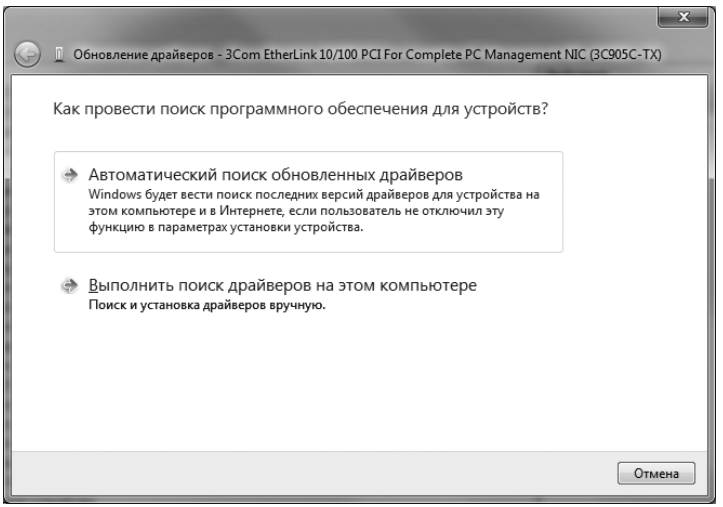

Рис. 8-21. Ручная и автоматическая установка драйвера

- **Поиск драйвера** Щелкните **Обзор (Browse)** и задайте место поиска в диалоговом окне **Обзор папок (Browse For Folder)**. Затем щелкните **OK**. Поиск автоматически выполняется во всех вложенных папках указанной папки. Для поиска на всем диске укажите корневой путь диска, например **C:**.
- **Выбор драйвера, из списка** Щелкните **Выбрать драйвер из списка уже установленных драйверов (Let Me Pick From A List Of Device Drivers On My Computer)**. Будет выведен список совместимого оборудования. Щелкните устройство, параметры которого совпадают с параметрами вашего устройства. Чтобы расширить область поиска, сбросьте флажок **Только совместимые устройства (Show Compatible Hardware)**. Появится полный список производителей устройств этого типа. Прокручивая список производителей, найдите изготовителя устанавливаемого устройства, затем выберите подходящее устройство на правой панели (рис. 8-22).

Примечание Если вы не находите в списке изготовителя или конкретное устройство, вставьте установочную дискету или CD-диск и щелкните кнопку **Установить с диска (Have Disk)**. Следуйте инструкциям.

7. Выбрав драйвер устройства, щелкните **Далее (Next)**, чтобы продолжить установку. По завершению установки драйвера щелкните **Закрыть (Close)**. Если не удается найти подходящий драйвер, найдите его и повторите процедуру. Помните, что иногда для включения вновь установленного или обновленного драйвера устройства требуется перезагрузить систему.

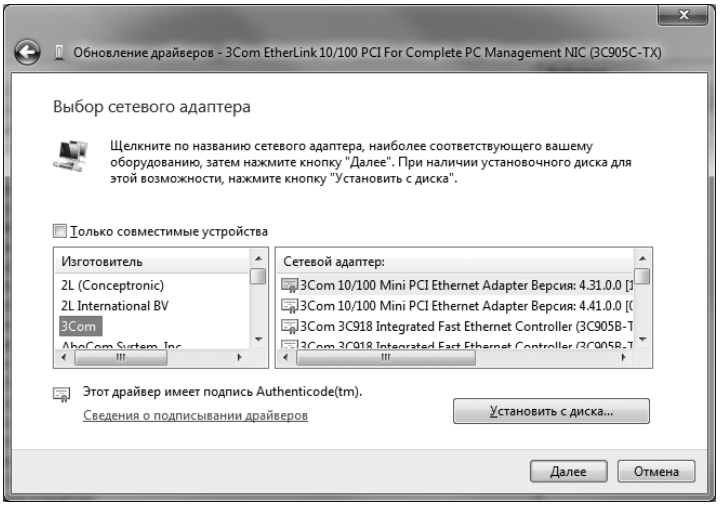

Рис. 8-22. Выбор драйвера для устанавливаемого устройства

Включение и отключение типов устройств

Предпочтения групповой политики позволяют управлять оборудованием (включать и отключать его), используемым на компьютерах, к которым применен объект групповой политики (GPO):

- **Класс устройства** Объединяет широкий круг однотипных устройств, например дисководы DVD/CD-ROM.
- **Тип устройства** Отдельные устройства внутри класса, например NEC DVD-ROM RW ND-3530A ATA.

Примечание Для управления устройствами по типу нужные устройства необходимо настроить на управляющем компьютере, а затем создать на нем элементы предпочтения. Управляющий компьютер — это компьютер, на котором установлены средства управления, в том числе компонент RSAT.

Чтобы создать элемент предпочтения для включения или отключения устройств по классу или типу, выполните следующие действия:

1. В оснастке **Редактор управления групповыми политиками (Group Policy Management Editor)** откройте объект GPO для редактирования. Чтобы настроить предпочтения для компьютеров, последовательно разверните узлы **Конфигурация компьютера\Настройка\Параметры панели управления (Computer Configuration\Preferences\Control Panel Settings)** и выделите **Устройства (Devices)**. Чтобы настроить предпочтения для пользователей, последовательно разверните узлы **Конфигурация пользователя\Настройка\Параметры панели управления (User Configuration\Preferences\Control Panel Settings)** и выберите **Устройства (Devices)**.
2. Щелкните правой кнопкой узел **Устройства (Devices)**, выберите команду **Создать (New)** и щелкните **Устройство (Device)**.

3. В открывшемся диалоговом окне **Новые свойства устройства (New Device Properties)** в списке **Действие (Action)** выберите один из вариантов:
   - **Использовать это устройство (включить) (Use This Device (Enable))** Выберите это действие, если нужно включить устройства по классу или типу.
   - **Не использовать это устройство (выключить) (Do Not Use This Device (Disable))** Выберите это действие, если нужно отключить устройства по классу или типу.
4. Щелкните кнопку справа от поля **Класс устройства (Device Class)** и выполните одно из следующих действий:
   - Выберите класс устройства, чтобы управлять устройствами по классу.
   - Разверните узел класса устройств и выберите тип устройства, чтобы управлять устройствами по типу.
5. При помощи параметров на вкладке **Общие параметры (Common)** задайте методы применения переменной. Вы собираетесь принудительно применить элемент управления, поэтому данный параметр должен применяться при каждом обновлении групповой политики. Не устанавливайте параметр **Применить один раз и не применять повторно (Apply Once And Do Not Reapply)**.
6. Щелкните **OK**. Во время следующего обновления политики элемент предпочтения будет применен к объекту GPO, в котором вы его определили.

Ограничение на установку устройств в групповой политике

Помимо задания цифровых подписей и параметров поиска в групповой политике можно разрешить или запретить установку устройств определенного класса. Устройства с однотипной установкой и настройкой сгруппированы в *класс установки устройств* (device setup class). Каждому классу сопоставлен глобально уникальный идентификатор (GUID). Для ограничения установки устройств в групповой политике необходимо знать GUID соответствующего класса.

В реестре ключ для каждого стандартного класса установки устройств находится в разделе HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class. Имена разделов реестра соответствуют идентификаторам GUID класса. В разделе реестра, соответствующем GUID класса, значение Class указывает на класс установки устройств, которому присвоен этот GUID. Например, классу установки устройств CD-ROM соответствует значение {4d36e965-e325-11ce-bfc1-08002be10318}.

Параметры политики для управления установкой устройств находятся в узле **Конфигурация компьютера\Административные шаблоны\Система\Установка устройства\Ограничения на установку устройств (Computer Configuration\Administrative Templates\System\Device Installation\Device Installation Restrictions)**. Вот некоторые из них:

- Время (сек.) до принудительной перезагрузки при необходимости введения параметров политики в действие (Time (In Seconds) To Force Reboot When Required For Policy Changes To Take Effect);
- Запретить установку съемных устройств (Prevent Installation Of Removable Devices);
- Запретить установку устройств с указанными кодами устройств (Prevent Installation Of Devices That Match Any Of These Device IDs);
- Запретить установку устройств, не описанных другими параметрами политики (Prevent Installation Of Devices Not Described By Other Policy Settings);
- Разрешить администраторам заменять политики ограничения установки устройств (Allow Administrators To Override Device Installation Restriction Policies);
- Разрешить установку устройств с использованием драйверов, соответствующих этим классам установки устройств (Allow Installation Of Devices Using Drivers That Match These Device Setup Classes);
- Разрешить установку устройств, соответствующих какому-либо из этих кодов устройств (Allow Installation Of Devices That Match Any Of These Device IDs).

Чтобы настроить параметры политики, выполните следующие действия:

1. В оснастке **Редактор управления групповыми политиками (Group Policy Management Editor)** откройте для редактирования объект GPO.
2. Разверните узел **Конфигурация компьютера\Административные шаблоны\Система\Установка устройства\Ограничения на установку устройств (Computer Configuration\Administrative Templates\System\Device Installation\Device Installation Restrictions)**.
3. Откройте диалоговое окно **Свойства (Properties)** политики, дважды щелкнув ее.
4. Если вы не хотите применять параметр политики, установите переключатель **Не задано (Not Configured)**. Чтобы применить параметр, установите переключатель **Включено (Enabled)**; а чтобы заблокировать использование параметра, установите переключатель **Отключено (Disabled)** (в соответствии с конфигурацией групповой политики).
5. Если вы включите политику, станет доступной кнопка **Показать (Show)**. Щелкните ее и в открывшемся диалоговом окне **Вывод содержания (Show Contents)** укажите идентификаторы устройств, на которые распространяется действие политики. Щелкните **OK**. В программе **Редактор реестра (Registry Editor)** идентификатору соответствует имя раздела, включая фигурные скобки ({ и }). Чтобы скопировать имя раздела и вставить его в диалоговое окно **Вывод содержания (Show Contents)**, выполните такие действия:
   a) Откройте Редактор реестра (Registry Editor): щелкните кнопку **Пуск (Start)**, введите **regedit** в поле поиска и нажмите Enter.

б) В программе Редактор реестра (Registry Editor) щелкните правой кнопкой имя узла и выберите команду **Копировать имя раздела (Copy Key Name)**.

в) В диалоговом окне **Вывод содержания (Show Contents)** дважды щелкните поле **Значение (Value)**. При этом обычный курсор изменится на курсор ввода. Щелкните поле правой кнопкой и выберите команду **Вставить (Paste)**.

г) Удалите путь, предшествующий значению GUID — *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class*.

д) Чтобы добавить GUID для других классов установки устройств, повторите шаги б-г.

6. Щелкните **OK**.

Отмена установки драйвера

Иногда установленный драйвер устройства становится причиной отказа устройства или возникновения критических системных ошибок. Если это случилось, восстановите систему и задействуйте ранее установленный драйвер устройства, выполнив следующие действия:

1. При возникновении проблем с загрузкой системы загрузите систему в безопасном режиме (см. главу 17).
2. Откройте консоль **Управление компьютером (Computer Management)**. Разверните узел **Служебные программы (System Tools)**.
3. В консоли **Управление компьютером (Computer Management)** выберите **Диспетчер устройств (Device Manager)**. На экране появится полный список установленных в системе устройств. По умолчанию устройства упорядочены по типу.
4. Правой кнопкой щелкните нужное устройство и выберите **Свойства (Properties)**.
5. В открывшемся диалоговом окне **Свойства (Properties)** перейдите на вкладку **Драйвер (Driver)** и щелкните **Откатить (Roll Back Driver)**. Подтвердите действие, щелкнув **Да (Yes)**.
6. Щелкните **Закрыть (Close)**, чтобы закрыть диалоговое окно **Свойства (Properties)**.

Примечание Если драйвер не обновлялся, у него нет и предыдущей версии. В этом случае кнопка **Откатить (Roll Back Driver)** недоступна.

Удаление драйвера удаленного устройства

Обычно после удаления устройства из системы драйверы этого устройства также автоматически удаляются. Но иногда удаление устройства остается незамеченным системой, и драйверы приходятся удалять вручную. Чтобы удалить драйвер устройства, выполните следующие действия:

1. Откройте консоль **Управление компьютером (Computer Management)**. Разверните узел **Служебные программы (System Tools)**.
2. В консоли **Управление компьютером (Computer Management)** выберите **Диспетчер устройств (Device Manager).**
3. Правой кнопкой щелкните нужное устройство и выберите **Удалить (Uninstall)**.
4. Подтвердите действие, щелкнув **OK**.

Удаление, повторная установка и отключение драйвера устройства

Удаление драйвера означает удаление соответствующего устройства. В некоторых случаях, когда устройство работает неправильно, для восстановления нормальной работы можно удалить устройство, перезагрузить систему и повторно установить устройство. Выполните следующие действия:

1. Откройте консоль **Управление компьютером (Computer Management)** и разверните узел **Служебные программы (System Tools)**.
2. В консоли **Управление компьютером (Computer Management)** выберите **Диспетчер устройств (Device Manager)**. На экране появится полный список установленных в системе устройств. По умолчанию устройства упорядочены по типу.
3. Правой кнопкой щелкните нужное устройство и выберите **Удалить (Uninstall)**.
4. Подтвердите действие, щелкнув **OK**.
5. Перезагрузите систему. Система вновь обнаружит устройство и установит необходимый драйвер. Если повторная установка драйвера не выполняется автоматически, установите драйвер вручную, как описано ранее в разделе «Установка и обновление драйверов устройств».

Чтобы запретить повторную установку устройства, отключите устройство, но не удаляйте его. Чтобы отключить устройство, правой кнопкой щелкните запись устройства в **Диспетчере устройств (Device Manager)** и выберите команду **Отключить (Disable)**.

Включение и отключение устройства

Неправильно работающее устройство можно отключить или удалить. При удалении разрывается связь устройства с драйвером, поэтому на какое-то время создается впечатление, что устройство удалено из системы. Во время следующего запуска Windows 7 попытается установить устройство повторно. Как правило, устройства Plug and Play в Windows 7 переустанавливаются автоматически. Однако если устройство не поддерживает Plug and Play, автоматическая повторная установка не выполняется.

При отключении устройства налагается запрет на его использование. Отключенное устройство не использует системные ресурсы и не может стать

причиной конфликтов в системе. Чтобы удалить или отключить устройство, выполните следующие действия:

1. Откройте консоль **Управление компьютером (Computer Management)**. Разверните узел **Служебные программы (System Tools)**.
2. В консоли **Управление компьютером (Computer Management)** выберите **Диспетчер устройств (Device Manage**r). На экране появится полный список установленных в системе устройств. По умолчанию устройства упорядочены по типу.
3. Правой кнопкой щелкните устройство и выберите одно из следующих действий:
   - Удалить (Uninstall).
   - Отключить (Disable).
4. Подтвердите действие, щелкнув **Да (Yes)** или **OK**.

Поиск и устранение неисправностей оборудования

Встроенные средства диагностики Windows 7 позволяют обнаруживать многие типы сбоев в оборудовании. При выявлении неисправности на экран выводится информационное сообщение **Отчеты о проблемах и их решениях (Problem Reports And Solutions)**. Щелкнув сообщение, вы откроете окно **Центр поддержки (Action Center)**. Консоль **Отчеты о проблемах и их решениях (Problem Reports And Solutions)** можно открыть и из панели управления, последовательно щелкнув ссылки **Система и безопасность (System And Security)** и **Центр поддержки (Action Center)**.

При неправильной установке или иной неисправности устройства в **Диспетчере устройств (Device Manager)** появляется предупреждение, указывающее на неполадку. Дважды щелкните устройство и просмотрите код ошибки на вкладке **Общие (General)** диалогового окна **Свойства (Properties)**. При устранении неисправности полезно понимать смысл кода ошибки (табл. 8-3). Для большинства корректирующих действий необходимо открыть диалоговое окно **Свойства (Properties)** на вкладке **Общие (General)**.

Табл. 8-3. Типичные ошибки устройств и способы их устранения

Сообщение об ошибке	Код	Исправление
Это устройство настроено неправильно (This device is not configured correctly)	1	Найдите совместимый драйвер устройства, затем щелкните **Обновить (Update Driver)**, чтобы открыть мастер Обновление драйверов (Update Driver Software)
Драйвер для данного устройства может быть поврежден, или в системе недостаточно памяти или иных ресурсов (The driver for this device might be corrupted, or your system might be running low on memory or other resources)	3	Откройте мастер Обновление драйверов (Update Driver Software): на вкладке **Драйвер (Driver)** щелкните **Обновить (Update Driver)**. Иногда из-за этой ошибки во время загрузки появляется сообщение о нехватке памяти

Табл. 8-3. (*продолжение*)

Сообщение об ошибке	Код	Исправление
Не удается запустить устройство (This device cannot start)	10	Откройте мастер Обновление драйверов (Update Driver Software): на вкладке **Драйвер (Driver)** щелкните **Обновить (Update Driver)**. Не пытайтесь найти драйвер автоматически. Выберите ручную установку и самостоятельно укажите устройство
Недостаточно свободных ресурсов для работы устройства (This device cannot find enough free resources that it can use)	12	Выделенные устройству ресурсы конфликтуют с другим устройством, или неправильно настроена микропрограмма. Проверьте микропрограмму и проверьте, нет ли на вкладке **Ресурсы (Resources)** диалогового окна **Свойства (Properties)** информации о конфликтах ресурсов
Это устройство не может работать правильно, пока компьютер не будет перезагружен (This device cannot work properly until you restart your computer)	14	Драйвер установлен правильно, но загрузить его нельзя без перезагрузки компьютера
Не удается установить все ресурсы, используемые этим устройством (Windows cannot identify all the resources this device uses)	16	Попытайтесь найти подписанный драйвер для этого устройства. Если такой драйвер есть и установлен, необходимо вручную выделить устройству ресурсы. Для этого откройте диалоговое окно **Свойства (Properties)** на вкладке **Ресурсы (Resources)**
Нужно заново установить драйверы этого устройства (Reinstall the drivers for this device)	18	Если вы установили ОС, обновив предыдущую систему, для завершения установки устройств войдите в систему с административной учетной записью. В других случаях переустановите драйвер, щелкнув кнопку **Обновить (Update Driver)** на вкладке **Драйвер (Driver)**
Возможно, поврежден реестр (Your registry might be corrupted)	19	Удалите и повторно установите устройство. Тем самым из реестра будут удалены ошибочные или конфликтующие параметры
Устройство будет удалено (Windows is removing this device)	21	Устройство будет удалено системой, вероятно, из-за повреждения реестра. Если сообщение продолжает выводиться, перезагрузите компьютер

Табл. 8-3. (*продолжение*)

Сообщение об ошибке	Код	Исправление
Устройство отключено (This device is disabled)	22	Устройство отключено в Диспетчере устройств (Device Manager). Чтобы включить устройство, в диалоговом окне **Свойства (Properties)** на вкладке **Общие (General)** щелкните кнопку **Включить (Enable Device)**
Устройство отсутствует, работает неправильно, или для него установлены не все драйверы (This device is not present, is not working properly, or does not have all its drivers installed)	24	Свидетельствует о неисправности устройства или оборудования. Данная ошибка может возникать при работе со старыми устройствами. Чтобы устранить ее, обновите драйвер
Для устройства не установлены драйверы (The drivers for this device are not installed)	28	Найдите совместимый драйвер для устройства, затем щелкните **Обновить (Update Driver)**, чтобы открыть мастер Обновление драйверов (Update Driver Software)
Устройство отключено, так как управляющая микропрограмма устройства не получила затребованные ресурсы от системы (This device is disabled because the firmware of the device did not give it the required resources)	29	Найдите сведения о выделении ресурсов в документации устройства. Возможно, придется обновить микропрограмму устройства или включить устройство в микропрограмме системы
Это устройство работает неправильно, т.к. Windows не удается загрузить для него нужные драйверы (This device is not working properly because Windows cannot load the drivers required for this device)	31	Возможно, драйвер устройства несовместим с Windows 7. Найдите совместимый драйвер, затем щелкните **Обновить (Update Driver)**, чтобы открыть мастер Обновление драйверов (Update Driver Software)
Драйвер для этого устройства был отключен. Возможно, необходимые функции исполняет другой драйвер (A driver (service) for this device has been disabled. An alternate driver may be providing this functionality)	32	Служба, от которой зависит работа устройства, отключена. Чтобы определить, какие службы необходимо включить и запустить, просмотрите журналы регистрации событий
Невозможно определить, какие ресурсы требуются для данного устройства (Windows cannot determine which resources are required for this device)	33	Вероятно, устройство или оборудование неисправно. Эта ошибка может возникать при работе со старыми устройствами. Обновите драйвер и (или) обратитесь к документации о выделении ресурсов

Табл. 8-3. (*продолжение*)

Сообщение об ошибке	Код	Исправление
Не удается определить параметры настройки для этого устройства (Windows cannot determine the settings for this device)	34	Старое устройство, которое нужно настроить вручную. Проверьте перемычки или параметры микропрограммы, затем настройте устройство и выделите для него ресурсы в диалоговом окне **Свойства (Properties)** на вкладке **Ресурсы (Resources)**
Аппаратные средства защиты программного обеспечения не содержат достаточной информации для правильной настройки и использования этого устройства (Your computer's system firmware does not include enough information to properly configure and use this device)	35	Такая ошибка характерна для многопроцессорных систем. Обновите микропрограмму и проверьте параметр, определяющий использование многопроцессорной спецификации (MPS) 1.1 или MPS 1.4. Обычно применяется спецификация MPS 1.4
Устройство запрашивает прерывание PCI, а в параметрах настройки указаны прерывания ISA (или наоборот) (This device is requesting a PCI interrupt but is configured for an ISA interrupt (or vice versa))	36	Нельзя путать прерывания для старого устройства. Ошибка может возникать при подключении устройства к слоту PCI, когда слот не зарезервирован для использования со старыми устройствами. Измените параметры настройки микропрограммы
Не удалось инициализировать драйвер этого устройства (Windows cannot initialize the device driver for this hardware)	37	Запустите мастер Обновление драйверов (Update Driver Software): на вкладке **Драйвер (Driver)** щелкните **Обновить (Update Driver)**
Не удалось загрузить драйвер этого устройства, поскольку предыдущий экземпляр этого драйвера все еще находится в памяти (Windows cannot load the device driver for this hardware because a previous instance of the device driver is still in memory)	38	Причиной конфликта стал драйвер устройства, находящийся в памяти. Перезагрузите компьютер
Не удалось загрузить драйвер этого устройства. Возможно, драйвер поврежден или отсутствует (Windows cannot load the device driver for this hardware. The driver might be corrupted or missing)	39	Проверьте правильность установки и подключения устройства, а также электропитание. Если устройство правильно установлено и подключено, найдите обновление для драйвера или переустановите текущий драйвер

Табл. 8-3. (*продолжение*)

Сообщение об ошибке	Код	Исправление
Не удалось получить доступ к этому оборудованию, поскольку информация раздела его службы в реестре отсутствует или неправильна (Windows cannot access this hardware because its service key information in the registry is missing or recorded incorrectly)	40	Элемент реестра для драйвера устройства недействителен. Переустановите драйвер
Драйвер этого устройства успешно загружен, но само устройство не обнаружено (Windows successfully loaded the device driver for this hardware but cannot find the hardware device)	41	Если устройство удалено, удалите драйвер, установите устройство и повторно установите драйвер, щелкнув **Обновить конфигурацию оборудования (Scan For Hardware Changes)**. Если устройство не было удалено или не поддерживает технологию Plug and Play, установите новый драйвер или обновите существующий. Чтобы установить устройство, не поддерживающее Plug and Play, откройте мастер Установка оборудования (Add Hardware). В Диспетчере устройств (Device Manager) щелкните **Действие (Action)** и выберите команду **Установить старое устройство (Add Legacy Hardware)**
Не удалось загрузить драйвер этого устройства, поскольку такое же устройство уже работает в системе (Windows cannot load the device driver for this hardware because there is a duplicate device already running in the system)	42	Обнаружена копия устройства. Такая ошибка возникает, когда драйвером шины ошибочно создаются два устройства с одним именем, или при обнаружении устройства с последовательным номером в новом расположении до того, как оно было удалено из старого расположения. Для решения проблемы перезагрузите компьютер
Это устройство было остановлено, поскольку оно сообщило о возникновении неполадок (Windows has stopped this device because it has reported problems)	43	Устройство было остановлено ОС. Удалите и повторно установите его. Проблема может быть связана с функцией защиты от выполнения (no-execute) процессора. Попробуйте найти новый драйвер
Приложение или служба выполнили завершение работы этого устройства (An application or service has shut down this hardware device)	44	Устройство было остановлено приложением или службой. Перезагрузите компьютер. Проблема может быть связана с функцией защиты от выполнения (no-execute) процессора. Попробуйте найти новый драйвер

Табл. 8-3. (*окончание*)

Сообщение об ошибке	Код	Исправление
В данный момент это устройство не подключено к этому компьютеру (Currently, this hardware device is not connected to the computer)	45	Если присвоить переменной среды DEVMGR_SHOW_NONPRESENT_DEVICES значение 1 и запустить Диспетчер устройств (Device Manager), в списке отображаются все устройства, которые подключались ранее, но в данный момент отсутствуют. Им и присваивается данная ошибка. Чтобы убрать это сообщение, подключите устройство к компьютеру или откройте Диспетчер устройств (Device Manager), не задавая указанную переменную среды
Windows не удалось получить доступ к этому устройству, поскольку операционная система находится в процессе завершения работы (Windows cannot gain access to this hardware device because the operating system is in the process of shutting down)	46	Устройство недоступно, так как выполняется завершение работы компьютера. Устройство станет доступным после перезапуска компьютера
Windows не может использовать это устройство, поскольку оно было подготовлено для «безопасного извлечения», но так и не было извлечено из компьютера (Windows cannot use this hardware device because it has been prepared for safe removal, but it has not been removed from the computer)	47	Если вы готовите устройство к извлечению в программе Безопасное извлечение устройств и дисков (Safe Removal) или при помощи физической кнопки извлечения, эта ошибка выводится, когда устройство готово к извлечению. Чтобы продолжить использование устройства, отсоедините и снова присоедините или перезагрузите компьютер
Запуск программного обеспечения для этого устройства был заблокирован, поскольку известно, что оно не может нормально работать под управлением Windows. Обратитесь к изготовителю для получения нового драйвера (The software for this device has been blocked from starting because it is known to have problems with Windows. Contact the hardware vendor for a new driver)	48	Драйвер данного устройства невозможно загрузить, так как он несовместим с Windows. Обратитесь к поставщику оборудования за новым или обновленным драйвером
Windows не удалось запустить новые устройства, поскольку системный куст реестра слишком велик (превышен допустимый размер реестра) (Windows cannot start new hardware devices because the system hive is too large (exceeds the Registry Size Limit))	49	Превышен максимальный размер системы. Новые устройства не смогут работать, пока вы не уменьшите размер системы. Ошибка вызвана тем, что устройства больше нельзя подключить к компьютеру, но они присутствуют в системном кусте реестра. Удалите все неиспользуемое оборудование

Глава 9

Установка и обслуживание программ

Одна из основных задач администратора и сотрудника службы поддержки — установка и настройка приложений на настольных компьютерах. Вам придется устанавливать и настраивать программы перед развертыванием новых компьютеров, устанавливать их на новых компьютерах и при необходимости обновлять программы при появлении новых версий. Кроме того, иногда вам придется исправлять или удалять программы, установленные пользователями. Как правило, большинство сбоев при установке программ устраняются очень легко — если вы знаете, где искать их причину. Но иногда случаются и серьезные неполадки, разобраться с которыми будет непросто. Из этой главы вы узнаете, как на установку и запуск приложений влияет функция контроля учетных записей (User Account Control, UAC), а также о различных способах установки, удаления и обслуживания программ.

Управление уровнями виртуализации и запуска приложений

Применение функции UAC существенно меняет способ установки и запуска, расположение данных, записываемых приложениями и присваиваемые им разрешения. В этом разделе мы рассмотрим различные аспекты влияния UAC на работу с приложениями — на маркеры безопасности, на виртуализацию файлов и реестра, на уровни запуска. Эта информация очень важна при установке и обслуживании приложений в Windows 7.

Маркеры доступа приложений и виртуализация расположения

Все приложения, работающие в Windows 7, делятся на две общие категории:

- **UAC-совместимое** Приложение, написанное специально для Windows Vista или Windows 7. Приложение, имеющее сертификат соответствия архитектуре Windows 7, имеет эмблему UAC-совместимости.
- **Устаревшее** Приложение, написанное для Windows XP или для прежней версии ОС.

Различие между UAC-совместимыми приложениями и устаревшими приложениями весьма существенно, потому что поддержка UAC требует из-

менений в архитектуре программы. В UAC-совместимых приложениях эта функция применяется для сокращения контактной зоны операционной системы. При использовании UAC неавторизованным приложениям не удастся установиться на компьютере без ведома пользователя; при этом полномочия приложений по умолчанию ограничены. Соблюдение этих мер затрудняет вредоносным программам получение власти над компьютером.

Примечание За работу UAC в Windows 7 отвечает служба Информация о совместимости приложений (Application Information). Она облегчает запуск интерактивных приложений с «администраторским» маркером доступа. Чтобы увидеть разницу между маркерами доступа администратора и обычного пользователя, откройте два окна командной строки. Одно из них запустите с повышенными полномочиями, щелкнув команду для открытия командной строки правой кнопкой и выбрав команду **Запуск от имени администратора (Run As Administrator)**. В обоих окнах введите команду **whoami /all** и сравните результаты. У обоих маркеров будет один и тот же идентификатор безопасности (SID), но в окне с повышенными полномочиями у маркера доступа больше полномочий.

Для всех приложений, работающих в Windows 7, контекст безопасности выбирается на основе маркера доступа текущего пользователя. По умолчанию UAC считает любого пользователя обычным, даже если он является членом группы Администраторы (Administrators). Если администратор действительно намерен воспользоваться своими полномочиями, для него создается новый маркер доступа. Он содержит все полномочия пользователя, и именно этот маркер (а не маркер доступа обычного пользователя) применятся для запуска приложения или процесса.

В Windows 7 большую часть приложений можно запускать, используя маркер доступа обычного пользователя. Необходимость запуска приложения с административными полномочиями может возникнуть, если оно выполняет какие-то специфические действия. Приложения, которым необходимы административные полномочия, называются *административными приложениями* (administrator user application). Далее перечислены их отличия от приложений, которым административные полномочия не нужны, то есть от *стандартных приложений* (standard user application):

- Административным приложениям повышенные полномочия требуются для выполнения ключевых задач. Будучи запущенным с административными полномочиями, такое приложение получает право выполнять административные действия и осуществлять запись в системные разделы реестра и файловой системы.
- Стандартным приложениям для выполнения ключевых задач административные полномочия не требуются. Будучи запущенным с полномочиями обычного пользователя, выполнять административные действия приложение сможет, только запросив повышение полномочий. Для решения всех остальных задач использовать повышенные полномочия приложение не должно. Осуществлять запись ему разрешается только в несистемные разделы реестра и файловой системы.

Приложения, написанные не для Windows 7, по умолчанию работают маркером доступа обычного пользователя. Чтобы «встроиться» в архитектуру UAC, эти приложения запускаются в специальном режиме совместимости и работают с «виртуализованными» представлениями файловой системы и реестра. Когда приложение пытается осуществить запись в системную область, Windows 7 выдает ему собственную копию файла или параметра реестра. Любые изменения записываются в эту копию, и она сохраняется в данных профиля пользователя. Когда приложение в следующий раз попытается прочитать содержимое этой области или что-то записать в нее, оно будет работать с копией, сохраненной в профиле. По умолчанию, если при работе с виртуализованными данными возникает ошибка, в уведомлении об ошибке и в журнальной записи указывается виртуальное расположение, а не подлинное расположение, с которым пытается работать приложение.

Целостность приложения и уровни запуска

Различие между пользовательскими и административными полномочиями меняет также общие разрешения, необходимые для установки и запуска приложений. В Windows XP и более старых версиях Windows полномочиями, необходимыми для выполнения основных системных действий при установке и запуске приложений, наделялась группа Опытные пользователи (Power Users). Приложениям, написанным для Windows 7, эта группа не нужна, и потому в Windows 7 она оставлена только для совместимости со старыми приложениями.

Благодаря UAC, Windows 7 по умолчанию выявляет попытки установки приложения и предлагает пользователю повысить уровень полномочий для продолжения установки. В установочных пакетах для UAC-совместимых приложений для определения необходимых полномочий применяется манифест приложения с обозначенным уровнем запуска. В манифесте полномочия приложения определяется одним из следующих способов:

- **RunAsInvoker** Приложение работает с полномочиями пользователя, который его запустил. Запустить приложение может любой пользователь. Он может быть обычным пользователем или администратором, но приложение все равно работает с обычным маркером доступа. С повышенными полномочиями приложение работает лишь в случае, если запустивший его процесс обладает административным маркером доступа. Например, если вы открыли окно командной строки с повышенными полномочиями и запустили приложение из этого окна, приложение будет работать с маркером доступа администратора.
- **RunAsHighest** Приложение работает с наивысшими полномочиями пользователя. Приложение могут запускать как администраторы, так и обычные пользователи. Действия, доступные приложению, зависят от полномочий пользователя. Если приложение запущено обычным пользователем, оно работает с обычным маркером доступа. Если пользователь

является членом группы с дополнительными полномочиями, наподобие групп Операторы архива (Backup Operators), Операторы сервера (Server Operators) или Операторы учета (Account Operators), приложение работает с частичным маркером доступа администратора, который содержит только предоставленные пользователю полномочия. Если пользователь является членом группы Администраторы (Administrators), приложение работает с полным маркером доступом администратора.

- **RunAsAdmin** Приложение работает с административными полномочиями. Запустить его может только администратор. Обычный пользователь или член группы с дополнительными полномочиями сможет запустить его, если он предоставит учетные данные администратора или если приложение запускается процессом с повышенными полномочиями, например из командной строки с повышенными полномочиями. Будучи запущенным членом группы Администраторы (Administrators), приложение работает с административным маркером доступа.

Чтобы защитить процессы приложения, Windows 7 присваивает им уровни целостности, от высокого до низкого. Приложения, изменяющие системные данные, например оснастка Управление дисками (Disk Management), считаются приложениями высокой целостности. Приложения, действие которых способно повредить безопасности системы, например Internet Explorer 8, считаются приложениями низкой целостности. Приложениями низкой целостности не разрешается изменять данные приложений высокой целостности.

Windows 7 определяет издателя для любого приложения, которое пытается работать с полным маркером доступа администратора. Затем в зависимости от издателя Windows 7 относит приложение к одной из трех категорий:

- Windows Vista / Windows 7;
- издатель проверен (подписано);
- издатель не проверен (не подписано).

Чтобы вам проще было оперативно оценить потенциальный риск для безопасности, связанный с установкой или запуском приложения, предложение повысить полномочия имеет определенный цветовой код и содержит определенный текст:

- Если издатель приложения заблокирован или само оно заблокировано групповой политикой, окно повышения полномочий имеет красный фон, а текст в нем гласит, что запуск приложения заблокирован.
- При запуске административного приложения, например консоли Управление компьютером (Computer Management), окно имеет сине-зелёный фон и содержит сообщение о том, что для продолжения работы Windows нуждается в вашем разрешении.
- Если приложение подписано Authenticode и является доверенным на локальном компьютере, у окна повышения полномочий серый фон и в нем написано, что для продолжения работы программа нуждается в вашем разрешении.

- Если приложение не подписано (или подписано, но не является доверенным), у окна повышения полномочий желтый фон и в нем написано, что доступ к компьютеру пытается получить неизвестная программа.

Для вящей безопасности процесса повышения полномочий его можно производить на безопасном рабочем столе. Он не дает злоумышленнику перехватить информацию, вводимую в приглашении на повышение полномочий. По умолчанию безопасный рабочий включен в групповой политике, о чем говорилось в главе 5.

Уровни запуска

По умолчанию в повышенном режиме работают только приложения с административным маркером доступа. Иногда вам нужно перевести в режим повышенных полномочий приложение с обычным маркером доступа. Например, иногда нужно запустить с повышенными полномочиями командную строку, чтобы выполнить какие-либо административные действия.

Помимо манифестов приложений (о которых говорилось в предыдущем разделе), в Windows 7 есть два способа задать уровень запуска приложения:

- один раз запустить приложение от имени администратора;
- всегда запускать приложение от имени администратора.

Чтобы один раз запустить приложение от имени администратора, щелкните правой кнопкой ярлык приложения или команду меню для его запуска и выберите команду **Запуск от имени администратора (Run As Administrator)**. Если вы работаете от имени обычной учетной записи и у вас включены запросы на повышение полномочий, на экран будет выведен запрос на продолжение работы программы. Если вы работаете от имени обычной учетной записи и запросы на повышение полномочий выключены, приложение не будет запущено. Если вы используете учетную запись администратора и у вас включены запросы на повышение полномочий, на экран будет выведен запрос на продолжение работы программы.

Windows 7 позволяет указывать приложения, которые всегда должны работать от имени администратора. Этот подход полезен, когда вы ищете причины проблем с совместимостью старых приложений, которым требуются административные полномочия. Бывают также UAC-совместимые приложения, которые обычно работают в стандартном режиме, но иногда применяются для решения административных задач. Вот пара типичных ситуаций:

- Обычное приложение, написанное для Windows 7, регулярно применяется для администрирования и потому должно работать с повышенными полномочиями. Чтобы каждый раз не щелкать ярлык приложения правой кнопкой, выбирая команду **Запуск от имени администратора (Run As Administrator)**, задайте для него постоянный запуск от имени администратора.
- Административные полномочия требуются приложению, написанному для Windows XP или для прежней версии Windows. В Windows 7 по умолчанию для этой программы задан обычный режим работы, поэтому программа не

работает должным образом и приводит к появлению большого количества ошибок. Чтобы разрешить проблему с совместимостью, вы можете создать клин (shim) совместимости приложений при помощи Windows Application Compatibility Toolkit (ACT) версии 5.5 или более поздней. В качестве временной меры задайте для приложения запуск от имени администратора.

Примечание Задать постоянный запуск от имени администратора для системных приложений и процессов нельзя. На этом уровне могут работать только несистемные приложения.

Ближе к реальности Решение Windows Application Compatibility Toolkit (ACT) предназначено для администраторов и не требует перепрограммирования приложения. Пакет ACT поможет вам разрешить типичные проблемы с совместимостью. Например, некоторые программы работают только в определенной версии ОС или только от имени администратора. При помощи ACT вы можете создать клин, который будет отвечать на запрос приложения об операционной системе или уровне пользователя значением True, что позволяет приложению работать без сбоев. ACT также позволяет создавать более глубокие решения для приложений, которые пытаются осуществлять запись в защищенные области ОС или использовать повышенные полномочия там, где они на самом деле не нужны. Чтобы загрузить ACT, обратитесь в Центр загрузки Майкрософт (*http://download.microsoft.com*).

Чтобы приложение всегда запускалось от имени администратора, выполните следующие действия:

1. Щелкните кнопку **Пуск (Start)** и найдите программу, которую хотите запускать от имени администратора.
2. Щелкните правой кнопкой ярлык приложения и выберите команду **Свойства (Properties)**.
3. Перейдите на вкладку **Совместимость (Compatibility)**, показанную на рис. 9-1.

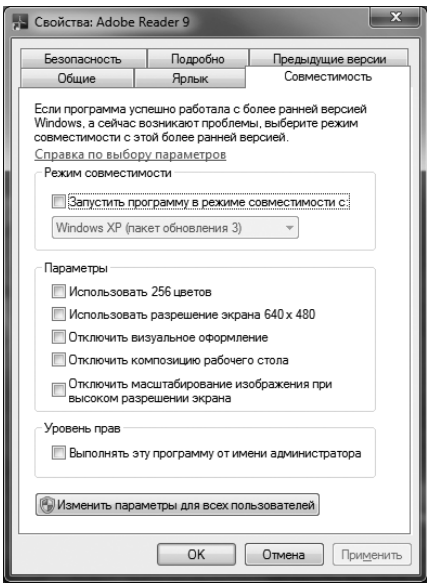

Рис. 9-1. Вкладка Совместимость (Compatibility)

4. Выполните одно из следующих действий:
   - Чтобы применить параметр к текущему пользователю, установите флажок **Выполнять эту программу от имени администратора (Run This Program As An Administrator)** и щелкните **OK**.
   - Чтобы применить параметр ко всем пользователям компьютера независимо от способа запуска приложения, щелкните кнопку **Изменить параметры для всех пользователей (Change Setting For All Users)**. Откроется диалоговое окно свойств исполняемого файла приложения. Установите флажок **Выполнять эту программу от имени администратора (Run This Program As An Administrator)** и дважды щелкните **OK**.

Примечание Недоступность флажка **Выполнять эту программу от имени администратора (Run This Program As An Administrator)** объясняется следующими причинами: возможность работы приложения в повышенном режиме заблокирована, для запуска приложения не требуются административные полномочия, вы работаете не от имени администратора.

Теперь приложение всегда будет работать с административным маркером доступа. Помните: если вы работаете от имени простого пользователя и у вас отключена выдача запросов на повышение полномочий, запустить приложение не удастся.

Оптимизация виртуализации и запросов на установку

С точки зрения приложений настройке поддаются две области UAC:

- автоматическое детектирование установки и выдача запроса;
- виртуализация сбоев при записи.

В групповой политике эти компоненты настраиваются в узле **Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности (Windows Settings\Security Settings\Local Policies\Security Options)** в административных шаблонах конфигурации компьютера. Параметры безопасности таковы:

- **Контроль учетных записей: обнаружение установки приложений и запрос на повышение прав (User Account Control: Detect Application Installations And Prompt For Elevation)** Определяет, должна ли Windows 7 автоматически обнаруживать установку приложения и запрашивать повышение полномочий или подтверждение. (В Windows 7 этот параметр по умолчанию включен.) Если вы отключите этот параметр, пользователям не будут выдаваться запросы на повышение полномочий. Соответственно, пользователь не сможет ввести учетные данные администратора и не сможет установить приложение.
- **Контроль учетных записей: при сбоях записи в файл или реестр виртуализация в место размещения пользователя (User Account Control: Virtualize File And Registry Write Failures To Per-User Locations)** Управляет включением и отключением виртуализации файлов и реестра. По

умолчанию этот параметр включен, и потому уведомления об ошибках и записи в журналах, относящиеся к виртуализованным файлам и значениям реестра, записываются в виртуальные расположения, а не в те реальные расположения, в которые приложение пытается их записать. Если вы отключите этот параметр, приложение при попытке записи в защищенные папки или параметры реестра просто обрушится без вывода дополнительной информации.

В домене нужная конфигурация параметров безопасности применяется к набору компьютеров при помощи групповой политики на базе Active Directory. Локальная политика безопасности позволяет применить эти же параметры к конкретному компьютеру. Выполните следующие действия:

1. Щелкните кнопку **Пуск (Start)**, разверните меню **Все программы (All Programs)**, **Администрирование (Administrative Tools)** и щелкните **Локальная политика безопасности (Local Security Policy)**. Откроется консоль Локальная политика безопасности (Local Security Policy).
2. В дереве консоли разверните узлы **Параметры безопасности (Security Settings)**, **Локальные политики (Local Policies)** и выделите элемент **Параметры безопасности (Security Options)**.
3. Щелкните дважды нужный параметр, внесите нужные изменения и щелкните **OK**.

Основные сведения об установке программ

В принципе, в установке программ нет ничего сложного. Сложнее разобраться в многочисленных проблемах, которые могут возникнуть в ходе этого процесса. Для этого вам необходимо разобраться в деталях процесса установки. Во многих случаях он начинается с программы автозапуска (Autorun), которая в свою очередь запускает программу установки. Процесс установки, среди прочего, состоит в проверке учетных данных пользователя, чтобы убедиться в наличии у него прав на установку программы, или в выводе запроса на повышение полномочий, если у пользователя таких прав нет. Вам также предстоит указать, у кого должен быть доступ к устанавливаемой программе: у всех пользователей компьютера или только у некоторых.

В некоторых случаях Windows не удается определить полномочия, необходимые для установки. Это происходит, если в манифесте установки программы имеется внедренный параметр RequestedExecutionLevel, которому присвоено значение RequireAdministrator. Поскольку параметр RequestedExecutionLevel отменяет значение, которое установщик обнаруживает в Windows, процесс установки завершается сбоем, если вы запускаете его с разрешениями обычного пользователя. Чтобы решить эту проблему, отмените сбойный процесс установки, найдите исполняемый файл установщика, щелкните его правой кнопкой и выберите команду **Запуск от имени администратора (Run As Administrator)**, чтобы перезапустить процесс установки с полномочиями администратора.

Кроме того, важно понимать, что в Windows 7 и Windows Server 2008 Release 2 на смену политикам ограниченного использования программ (Software Restriction) пришли политики управления приложениями (Application Control). Политики ограниченного использования программ задают, какие приложения пользователям разрешается устанавливать и запускать в Windows 2000, Windows XP и Windows Vista. Политики управления приложениями играют аналогичную роль в Windows 7 и Windows Server 2008 Release 2. Помните о следующем:

- Когда вы редактируете объект групповой политики Group Policy (GPO), настройку политик ограниченного использования программ для компьютера осуществляйте в узле **Конфигурация компьютера\Политики\Конфигурация Windows\Параметры безопасности\Политики ограниченного использования программ (Computer Configuration\Policies\Windows Settings\Security Settings\Software Restriction Policies)**, а политики для пользователей настраивайте в узле **Конфигурация пользователя\Политики\Конфигурация Windows\Параметры безопасности\Политики ограниченного использования программ (User Configuration\Policies\Windows Settings\Security Settings\Software Restriction Policies)**. Будет или нет файл считаться исполняемым, зависит от его расширения.
- Создавая политики управления приложениями для компьютера и настраивая их, используйте узел **Конфигурация компьютера\Политики\Конфигурация Windows\Параметры безопасности\Политики управления приложениями (Computer Configuration\Policies\Windows Settings\Security Settings\Application Control Policies)**. Вы можете создавать отдельные правила для исполняемых файлов, файлов установщика Windows и сценариев. Правила применяются по издателю, пути к файлу или хешу файла. Правило издателя обеспечивает вам максимальную гибкость, позволяя задавать разрешенные продукты и версии. Допустим, можно разрешить только использование версии Microsoft Word 2003 или более поздней.

Автозапуск

Когда вы вставляете в дисковод установочный CD- или DVD-диск, Windows 7 проверяет, есть на нем файл Autorun.inf. В нем задается действие, которое должна предпринять ОС, а также могут задаваться другие параметры установки. Autorun.inf — это текстовый файл, который можно открыть в любом текстовом редакторе. Заглянув в такой файл, вы увидите что-то подобное:

```
[autorun]
OPEN=SETUP.EXE AUTORUN=1
ICON=SETUP.EXE,4
SHELL=OPEN
```

```
DisplayName=Microsoft Digital Image Suite 9
ShortName=PIS
PISETUP=PIP\pisetup.exe
```

Этот файл определяет, что при вставке в дисковод CD- или DVD-диска должен открываться файл Setup.exe. Поскольку Setup.exe — программа, его открытие означает запуск. Также в файле Autorun.inf задается значок, который нужно использовать, состояние оболочки, отображаемое имя программы, короткое имя программы и дополнительный параметр для обозначения еще одной программы, которую нужно запустить.

В файле Autorun.inf необязательно задавать открытие программы. Взгляните на другой пример:

```
[autorun]
OPEN=Autorun\ShelExec default.htm
```

Этот файл Autorun.inf выполняется через оболочку и открывает файл Default.htm в веб-браузере. Важно отметить, что и в этом случае документ, открытый в веб-браузере, содержит ссылки, указывающие на программу установки.

Совет Если CD- или DVD-диск установлен в дисковод, для перезапуска процесса Autorun просто откройте и закройте дисковод.

Настройка и совместимость приложения

У большинства приложений имеется программа установки, основанная на применении InstallShield, Wise Install или Microsoft Windows Installer. Когда вы запускаете программу установки, установщик помогает отслеживать процесс установки, а также при необходимости безболезненно отменить установку программы. Если вы устанавливаете старую программу, в программе установки может использоваться старая версия одного из этих установщиков. Это означает, что и отмена установки может пройти не совсем чисто.

Даже если вы абсолютно уверены, что в программе используется современный установщик, нужно быть готовым к тому, что вам придется восстанавливать систему после какого-либо сбоя установки. Чтобы обезопасить себя, убедитесь, что восстановление системы включено на диске, куда вы собираетесь устанавливать программу, так что перед установкой программы будет создана автоматическая точка восстановления.

Установщики большинства современных приложений автоматически инициируют создание точки восстановления перед любыми изменениями на компьютере, но у старых установщиков может не быть такой возможности. Создайте точку восстановления вручную, как описано в главе 17. Если у вас потом начнутся сбои, вы либо отмените установку программы, либо восстановите систему к состоянию, предшествовавшему установке программы.

Прежде чем устанавливать любое приложение, проверьте, совместимо ли оно с Windows 7. Для этого нужно сделать следующее:

- Осмотрите упаковку приложения. На ней должны быть указаны сведения о совместимости. Ищите эмблему Windows 7.
- Посмотрите список совместимых ОС на веб-сайте разработчика.

Совет Попутно с проверкой совместимости посмотрите, имеются ли для приложения обновления и исправления. Если они есть, после установки программы установите и их.

Перед установкой приложения Windows 7 пытается выявить потенциальные проблемы с совместимостью. Если проблемы обнаружены, после запуска программы установщика на экране может появиться диалоговое окно **Помощник по совместимости программ (Program Compatibility Assistant)**. В этом окне содержится информация об известных проблемах совместимости для этой программы, а также (во многих случаях) возможные способы их решения. Например, там может содержаться совет перед запуском программы установить для нее последний пакет обновлений. В некоторых случаях Помощник по совместимости программ (Program Compatibility Assistant) выводит на экран сообщение о том, что из-за проблем с совместимостью программа заблокирована. Это означает, что у программы есть известная проблема с устойчивой работой в Windows, и нет прямого способа устранить эту проблему. При этом выбор у вас небогатый: щелкнуть кнопку **Поиск решений в Интернете (Check For Solutions Online)** или кнопку **Отмена (Cancel)**. В первом случае вам, скорее всего, будет предложено приобрести обновленную версию программы. Во втором случае вы просто остановите процесс установки без поиска возможного решения.

Диалоговое окно помощника по совместимости отображается также, если процесс установки по какой-либо причине прерывается до полного завершения или не способен должным образом уведомить ОС о своем завершении. Если вы уверены, что программа должным образом установлена, щелкните **Эта программа установлена правильно (This Program Installed Correctly)**. Если программа не установлена, щелкните **Переустановите, используя рекомендуемые параметры (Reinstall Using Recommended Settings)**, чтобы помощник по совместимости применил одно или несколько исправлений совместимости, а затем снова запустил установщик.

Когда вы запускаете программу, Windows 7 использует помощник по совместимости для устранения известных проблем с совместимостью приложения. Если такая проблема обнаружена, помощник уведомит вас о ней и предложит возможные варианты ее автоматического решения. Далее вы можете указать помощнику, что он должен перенастроить приложения, или перенастроить его вручную, как описано далее в разделе «Настройка совместимости программы».

Если вы имеете дело со старыми приложениями, попробуйте воспользоваться администратором совместимости (Compatibility Administrator, Compatadmin.exe) из комплекта Windows Application Compatibility Toolkit, чтобы создать манифест приложения, в котором задается уровень ее запуска. Администратор совместимости также поможет вам выявить другие по-

тенциальные сбои в совместимости старых приложений. Чтобы загрузить комплект Windows Application Compatibility Toolkit (ACT), обратитесь в Центр загрузки Майкрософт (*http://download.microsoft.com*).

Определение пользователей, имеющих доступ к программе

Обычно установленная на компьютере программа доступна всем его пользователям. Это происходит потому, что ярлыки программы помещаются в папку Программы (Programs) главного меню (%SystemDrive%\ProgramData\Microsoft\Windows\Start Menu\Programs) всех пользователей. Доступ к программе будут иметь все пользователи, зарегистрировавшиеся на компьютере. Некоторые программы в ходе установки предлагают вам сделать программу доступной для всех пользователей или только для текущего пользователя. Другие программы по умолчанию доступны только текущему пользователю.

Если установщик сделал программу доступной только текущему пользователю, а вы хотите открыть доступ к ней всем пользователям, выполните одно из следующих действий:

- Зарегистрируйтесь на компьютере с учетной записью каждого пользователя, которому необходим доступ к программе, и перезапустите установщик. Если в будущем на компьютере будут создаваться новые учетные записи, процесс установки нужно будет повторять.
- Если программе не нужны индивидуальные настройки в реестре для каждого пользователя, в некоторых случаях, чтобы сделать программу доступной всем пользователям, достаточно добавить соответствующий ярлык в папку Программы (Programs) главного меню всех пользователей, скопировав его из аналогичной папки конкретного пользователя.

Чтобы скопировать или переместить ярлык программы, выполните следующие действия:

1. Щелкните правой кнопкой мыши кнопку **Пуск (Start)** и выберите команду **Открыть проводник (Open Windows Explorer)**. В окне проводника найдите папку Программы (Programs) текущего пользователя. Это скрытая подпапка папки %UserProfile%\AppData\Roaming\Microsoft\Windows\Start Menu.
2. Щелкните правой кнопкой подпапку нужной группы программ или ярлык и выберите команду **Копировать (Copy)** или **Вырезать (Cut)**.
3. Перейдите в папку Программы (Programs) всех пользователей. Это скрытая подпапка папки %SystemDrive%\ProgramData\Microsoft\Windows\Start Menu.
4. Щелкните пустое пространство папки правой кнопкой и выберите команду **Вставить (Paste)**. Теперь группа программ или ярлык будут доступны всем пользователям компьютера.

Примечание В папке %SystemDrive%\Users есть подпапка Общие (All Users). Если вы знаете об этой папке, у вас, вероятно, возник вопрос, почему мы не скопировали нашу программную группу или ярлык в подпапку именно этой папки. Причина проста: папка %SystemDrive%\Users\All Users на самом деле всего лишь ссылка на папку %SystemDrive%\ProgramData. Чтобы просмотреть ссылки и точки входа в текущей папке из командной строки, введите **dir /al**.

Чтобы сделать программу доступной только текущему пользователю, переместите ее ярлык, выполнив следующие действия:

1. Щелкните правой кнопкой мыши кнопку **Пуск (Start)** и выберите команду **Открыть проводник (Open Windows Explorer)**. В окне проводника перейдите в папку главного меню для всех пользователей. Это скрытая подпапка папки %SystemDrive%\ProgramData\Microsoft\Windows\Start Menu.
2. В папке Программы (Programs) щелкните правой кнопкой нужную папку программной группы или ярлык и выберите команду **Вырезать (Cut)**.
3. В окне проводника перейдите в папку Программы (Programs) текущего пользователя. Это скрытая подпапка папки %UserProfile%\AppData\Roaming\Microsoft\Windows\Start Menu.
4. Щелкните правой кнопкой пустое пространство папки и выберите команду **Вставить (Paste)**. Теперь программная группа или ярлык доступны только текущему пользователю.

Примечание Перемещение программной группы или ярлыка всего лишь скрывает присутствие программы на компьютере. Другие пользователи по-прежнему смогут запустить ее при помощи диалогового окна **Выполнить (Run)** или проводника Windows.

Развертывание приложений при помощи групповой политики

Групповая политика позволяет открыть доступ к приложению для всех пользователей сети. Применение групповой политики для развертывания приложений возможно в двух вариантах:

- **Назначьте приложение пользователям или компьютерам** Когда вы назначаете приложение компьютеру, оно устанавливается на нем при следующем запуске компьютера и становится доступным для всех пользователей этого компьютера. Если приложение назначено пользователю, оно устанавливается при следующем входе пользователя в сеть. Назначенное приложение можно также настроить на установку при первой попытке запуска. В этой конфигурации доступ к приложению открывается при помощи ярлыка на рабочем столе пользователя или команды в главном меню. Приложение будет установлено, когда пользователь щелкнет этот ярлык или выберет команду, чтобы впервые запустить приложение.
- **Опубликуйте приложение и сделайте его доступным для установки** Когда вы публикуете приложение, доступ к нему открывается при акти-

вации расширения. Это означает, что приложение устанавливается, когда пользователь впервые пытается открыть файл, расширение которого ассоциировано с этим приложением. Например, когда пользователь дважды щелкает файл с расширением .doc или .docx, производится автоматическая установка Microsoft Word.

Для развертывания приложений на компьютере используются файлы установщика Microsoft Windows Installer (.msi) и политики из узла **Конфигурация компьютера\Политики\Конфигурация программ\Установка программ (Computer Configuration\Policies\Software Settings\Software Installation)**. Развертывание приложений для пользователей осуществляется при помощи файлов установщика Windows (.msi) и политик из узла **Конфигурация пользователя\Политики\Конфигурация программ\Установка программ (User Configuration\Policies\Software Settings\Soft-ware Installation)**. Базовые этапы развертывания приложений при помощи групповой политики таковы:

1. Чтобы у клиентов был доступ к пакету установщика Windows, он должен располагаться на общем сетевом ресурсе. При необходимости скопируйте пакет .msi на ресурс, доступный всем пользователям.
2. Откройте в редакторе управления групповой политикой нужный объект GPO, при помощи которого вы хотите развернуть приложение. Это приложение будет доступно всем клиентам, к которым применим данный GPO, то есть всем компьютерам и пользователям из соответствующего домена, сайта или подразделения.
3. Разверните узел **Конфигурация компьютера\Политики\Конфигурация программ (Computer Configuration\Policies\Software Settings)** или **Конфигурация пользователя\Политики\Конфигурация программ (User Configuration\Policies\Software Settings)**, щелкните правой кнопкой элемент **Установка программ (Software Installation)**, раскройте подменю **Создать (New)** и выберите команду **Пакет (Package)**.
4. При помощи диалогового окна **Открыть (Open)** найдите пакет установщика Windows для приложения и щелкните кнопку **Открыть (Open)**. Выберите метод развертывания: **Публичный (Published)**, **Назначенный (Assigned)** или **Особый (Advanced)**.
5. Чтобы опубликовать программу или назначить ее, выберите вариант **Публичный (Published)** или **Назначенный (Assigned)** и щелкните **OK**. Если вы настраиваете политику для компьютера, программа будет доступна при очередном запуске компьютера, к которому применяется этот GPO. Если вы настраиваете политику для пользователя, программа будет доступна любому пользователю домена, сайта или подразделения при его очередном входе в систему. Если пользователь зарегистрирован в сети в момент создания политики, для установки приложения пользователю нужно будет выйти из системы и снова войти в нее.

6. Чтобы настроить дополнительные параметры развертывания программы, щелкните кнопку **Особый (Advanced)**.

Настройка совместимости программы

Установка 16-разрядного приложения или приложения MS-DOS требует вдумчивого отношения. Кроме того, чтобы заставить работать старые программы, иногда требуется настраивать параметры совместимости. В следующих разделах обсуждаются различные способы задания этих параметров.

Особенности установки 16-разрядных приложений и программ MS-DOS

Многие 16-разрядные программы и программы MS-DOS, которым не требуется прямой доступ к оборудованию, устанавливаются и работают в Windows 7 без малейших трудностей. Помните однако, что большинством подобных программ не поддерживаются длинные имена файлов. Чтобы обеспечить совместимость с этими программами, в Windows 7 при необходимости в соответствие длинным именам ставятся короткие имена. Это гарантирует, что длинные имена файлов защищены от изменения 16-разрядными программами или программами MS-DOS. Кроме того, важно помнить, что для этих программ требуются 16-разрядные драйверы, которые в Windows 7 не поддерживаются. В результате эти программы работать не будут.

Большинство 16-разрядных программ и программ MS-DOS изначально разрабатывались для Windows 3.0 и Windows 3.1. В Windows 7 эти старые программы запускаются при помощи виртуальной машины, которая имитирует усовершенствованный режим 386-го процессора, применявшийся в Windows 3.0 и Windows 3.1. В отличие от прежних версий Windows, в Windows 7 все такие приложения работают как отдельные потки в одной виртуальной машине. Если вы запускаете несколько 16-разрядных и MS-DOS-приложений, все они работают в одной общей области памяти. К сожалению, зависание одной из этих программ часто приводит к зависанию и всех остальных.

Чтобы не дать одной 16-разрядной программе или программе MS-DOS обрушить или подвесить остальные подобные программы, запустите ее в отдельной области памяти, выполнив следующие действия:

1. Щелкните правой кнопкой ярлык программы и выберите команду **Свойства (Properties)**. Если у программы нет ярлыка, создайте его.
2. На вкладке **Ярлык (Shortcut)** окна свойств ярлыка щелкните кнопку **Дополнительно (Advanced)**. Откроется диалоговое окно **Дополнительные свойства (Advanced Properties)**.
3. Установите флажок **Запускать в отдельной области памяти (Run In Separate Memory Space)**.
4. Два раза щелкните **OK**, чтобы закрыть все открытые диалоговые окна и сохранить изменения.

Примечание Запуск программы в отдельной области памяти приводит к использованию большего объема памяти, но одновременно и ускоряет работу программы. Еще одно преимущество состоит в том, что вы сможете запускать несколько экземпляров программы, при условии что все они работают в отдельных областях памяти.

Совет Командная строка Windows 7 (Cmd.exe) — 32-разрядное приложение. Чтобы запустить 16-разрядную командную строку MS-DOS, запустите программу Command.com: введите **command** в диалоговом окне **Выполнить (Run)**.

Принудительная совместимость программы

Иногда в Windows 7 не удается установить или запустить программы, которые прекрасно работали в предыдущих версиях Windows. Если проблемы с совместимостью программы, которую вы пытаетесь установить, уже проявлялись в прошлом, Windows 7, вероятно, выведет на экран предупреждение об этом. Как правило, это означает, что установку или запуск программы нужно прекратить, особенно если речь идет о системной утилите, например антивирусной программе или программе для работы с разделами диска. В этом случае запуск несовместимой программы может обернуться крупными неприятностями. Впрочем, запуск других несовместимых программ тоже небезопасен, особенно если они пытаются осуществить запись в системные области диска.

Помня о вышесказанном, знайте, что программу, которая не устанавливается или не запускается в Windows 7, можно все-таки заставить работать, настроив ее параметры совместимости. В Windows 7 предусмотрено два способа управления этими параметрами: использование мастера Совместимость программы (Program Compatibility) или прямое редактирование параметров совместимости программы в диалоговом окне ее свойств. Оба способа эквивалентны, но только при помощи мастера можно изменять параметры программ на общих сетевых дисках, CD- или DVD-дисках, а также на других съемных носителях.

Мастер Совместимость программы (Program Compatibility)

Параметры совместимости можно задавать только для программ, установленных вами. Настраивать совместимость программ из состава операционной системы нельзя. Чтобы автоматически выявить проблемы совместимости при помощи мастера Совместимость программы (Program Compatibility), выполните следующие действия:

1. Найдите ярлык программы в главном меню, щелкните его правой кнопкой и выберите команду **Исправление неполадок совместимости (Troubleshoot Compatibility)**. Будет запущен мастер Совместимость программы (Program Compatibility), показанный на рис. 9-2.

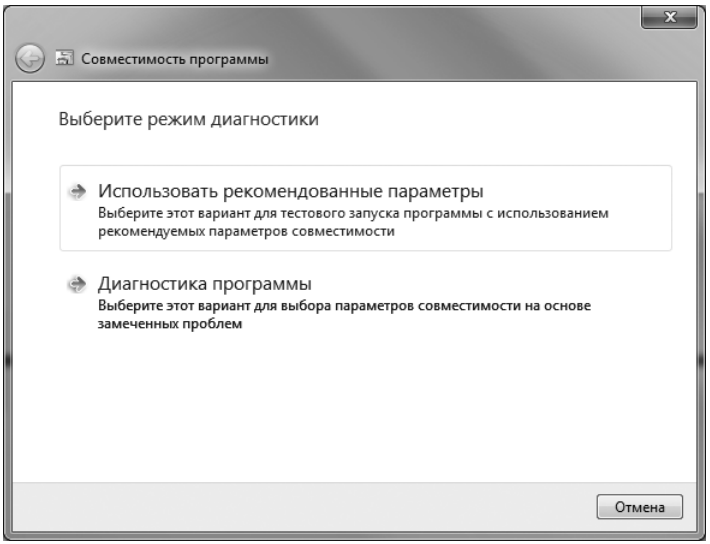

Рис. 9-2. Поиск проблем с совместимостью

2. Мастер попытается автоматически выявить проблемы с совместимостью. Чтобы попытаться запустить программу с рекомендованными изменениями, щелкните **Использовать рекомендованные параметры (Try Recommended Settings)**. Просмотрите изменения, которые предполагается внести, и щелкните **Запуск программы (Start The Program)**.
3. После запуска программы щелкните **Далее (Next)** и выполните одно из следующих действий:
   - Щелкните **Да, сохранить эти параметры для программы (Yes, Save These Settings For This Program)**, если исправление параметров совместимости устранило сбой.
   - Щелкните **Нет, попытаться использовать другие параметры (No, Try Again Using Different Settings)**, если исправление параметров совместимости не устранило сбой и вы хотите повторить процесс с начала.
   - Щелкните **Нет, отправить сообщение об этой проблеме в корпорацию Майкрософт и найти решение в Интернете (No, Report The Problem To Microsoft And Check Online For A Solution)**, если исправление параметров совместимости не устранило сбой, и вы хотите поискать решение в Интернете.
   - Щелкните **Отмена (Cancel)**, чтобы отменить изменение параметров совместимости и прекратить работу мастера.

Чтобы провести более детальную диагностику и задать параметры совместимости при помощи мастера Совместимость программы (Program Compatibility), выполните следующие действия:

1. Найдите ярлык программы в главном меню, щелкните его правой кнопкой и выберите команду **Исправление неполадок совместимости (Trou-**

bleshoot Compatibility). Будет запущен мастер Совместимость программы (Program Compatibility).

2. Щелкните **Диагностика программы (Troubleshoot Program)**. На странице **Какие проблемы заметны (What Problems Do You Notice?)** укажите вид отмеченного вами сбоя. От него зависит вид следующих страниц мастера. Возможны следующие варианты:
   - **Программа работала в предыдущих версиях Windows, но не устанавливается или не запускается сейчас (The Program Worked On Earlier Versions Of Windows But Won't Install Or Run Now)** Если вы установите этот флажок, на одной из следующих страниц мастера вам будет предложено указать, в какой именно версии ОС вы работали с этой программой. От ответа на этот вопрос зависит выбор режима совместимости, поэтому по возможности выбирайте конкретно ту ОС, для которой разрабатывалась программа. Во время запуска программы Windows 7 будет имитировать среду заданной ОС.
   - **Программа открывается, но отображается неправильно (The Program Opens But Doesn't Display Correctly)** Выбирайте этот вариант, если вы имеете дело с игрой, учебной программой или иным приложением, которому требуются особые параметры дисплея и которое разрабатывалось, скажем, для Windows 98. От вашего выбора зависят ограничения на параметры монитора, например 256 цветов и разрешение 640 × 480. Это поможет вам решить проблемы с программами, которым не удается работать при больших разрешениях и большем количестве цветов. Вы также можете отключить темы, видеоэффекты и масштабирование при высоких разрешениях.
   - **Для программы необходимы дополнительные разрешения (The Program Requires Additional Permissions)** Если вы выберете этот вариант, программа будет настроена на запуск с административными полномочиями.
   - **Я не вижу моей проблемы в списке (I Don't See My Problem Listed)** Если вы выберете этот вариант, мастер отобразит дополнительные страницы, на которых вы сможете уточнить суть сбоя. Мастер также задает для программы работу с административными полномочиями. К этой же последовательности дальнейшей работы приводит одновременный выбор всех трех предыдущих параметров.
3. Просмотрите параметры совместимости, которые будут применены к программе. Если их набор вас не устраивает, щелкните **Отмена (Cancel)** и повторите процедуру, выбрав другие параметры. Если вы готовы применить параметры, щелкните **Запуск программы (Start The Program)**. Мастер запустит программу с заданными параметрами.
4. После запуска программы щелкните **Далее (Next)**. Вам будет предложено указать, удалось ли устранить неполадку. Выполните одно из следующих действий:

- Если заданные параметры устранили сбой и вы хотите их сохранить, щелкните **Да, сохранить эти параметры для программы (Yes, Save These Settings For This Program)**.
- Если заданные параметры не устранили сбой и вы хотите повторить процесс сначала, щелкните **Нет, попытаться использовать другие параметры (No, Try Again Using Different Settings)**.
- Если заданные параметры не устранили сбой и вы хотите поискать решение в Интернете, щелкните **Нет, отправить сообщение об этой проблеме в корпорацию Майкрософт и найти решение в Интернете (No, Report The Problem To Microsoft And Check Online For A Solution)**.
- Чтобы отказаться от заданных параметров и прекратить работу мастера, щелкните **Отмена (Cancel)**.

Примечание Если вы настроили для приложения собственные параметры дисплея, система будет переходить в режим с этими параметрами при каждом запуске приложения. Чтобы восстановить исходные параметры дисплея, выйдите из программы.

Непосредственное задание параметров совместимости

Если установленная вами программа не работает должным образом, возможно, вы захотите исправить параметры непосредственно, не прибегая к помощи мастера. Выполните следующие действия:

1. Щелкните ярлык правой кнопкой и выберите команду **Свойства (Properties)**.
2. В диалоговом окне свойств перейдите на вкладку **Совместимость (Compatibility)**. Любой заданный вами параметр применяется к запуску приложения текущим пользователем. Чтобы применить параметр ко всем пользователям компьютера, независимо от того какой ярлык используется для запуска приложения, щелкните **Изменить параметры для всех пользователей (Change Setting For All Users)**. Откроется окно свойств исполняемого файла приложения. Задайте параметры совместимости, которые должны применяться для всех пользователей компьютера.

Примечание В режиме совместимости не могут работать программы, являющиеся частью ОС Windows 7. В окнах свойств этих программ параметры вкладки **Совместимость (Compatibility)** недоступны.

3. Установите флажок **Запустить программу в режиме совместимости с (Run This Program In Compatibility Mode For)** и выберите в списке операционную систему, для которой разрабатывалась программа.
4. При необходимости используйте параметры в разделе **Параметры (Settings)**, чтобы ограничить параметры дисплея. Задайте использование 256 цветов, разрешения 640 × 480 или и того, и другого.
5. При необходимости отключите темы, визуальные эффекты и масштабирование дисплея при высоких разрешениях.

6. Щелкните **OK**. Дважды щелкните ярлык, чтобы запустить программу и проверить параметры совместимости. Если программа все равно работает со сбоями, попробуйте задать другие параметры совместимости.

Управление установленными и работающими программами

В Windows 7 имеется несколько инструментов для управления программами, в том числе:

- **Диспетчер задач (Task Manager)** Позволяет просматривать работающие программы и управлять ими, а также следить за использованием ресурсов и производительностью.
- **Программы (Programs)** Содержит утилиты для просмотра установленных программ, добавления и удаления программ, просмотра установленных обновлений и пр.
- **Программы по умолчанию (Default Programs)** Позволяет просматривать и настраивать на компьютере глобальные программы по умолчанию, программы по умолчанию для конкретных пользователей, параметры автозапуска для мультимедиа и ассоциации файлов.
- **Компоненты Windows (Windows Features)** Позволяет просматривать установленные компоненты Windows и управлять ими.
- **Assoc** Просмотр и управление ассоциациями типов файлов.
- **Ftype** Просмотр и управление определениями типов файлов.

Эти инструменты и связанные с ними параметры конфигурации обсуждаются в следующих разделах.

Управление работающими программами

В Windows 7 для работы с активными программами и процессами предназначен Диспетчер задач (Task Manager). Чтобы открыть его, нажмите Ctrl+Alt+Del и щелкните кнопку **Запустить диспетчер задач (Start Task Manager)**. Как видно на рис. 9-3, в окне Диспетчера задач (Task Manager) для работы с активными программами предназначено две вкладки:

- **Приложения (Applications)** На этой вкладке перечислены программы, которые в данный момент работают в основном режиме, с указанием их имени и состояния, например **Работает (Running)** или **Не отвечает (Not Responding)**. Чтобы завершить работу программы, например, если она зависла, выделите ее имя в столбце **Задача (Task)** и щелкните кнопку **Снять задачу (End Task)**.
- **Процессы (Processes)** На этой вкладке перечислены все программы и процессы, работающие в основном и фоновом режимах с указанием имени образа, имени пользователя и используемых ресурсов. Чтобы остановить процесс, выделите его и щелкните **Завершить процесс (End Process)**.

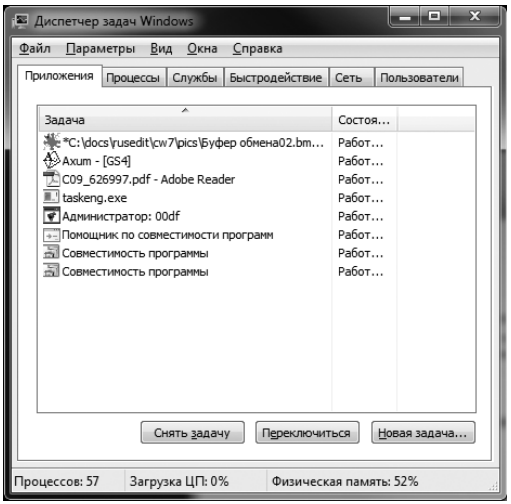

Рис. 9-3. Диспетчер задач (Task Manager) предназначен для управления активными программами и процессами

Сведения о количестве процессов, использовании ресурсов и физической памяти приводятся для всего компьютера, но в списке по умолчанию даны только процессы, запущенные текущим пользователем и ОС. Чтобы просмотреть активные процессы для всех пользователей, щелкните **Отображать процессы всех пользователей (Show Processes From All Users)**.

Совет Чтобы на вкладке **Процессы (Processes)** получить доступ к дополнительным возможностям управления процессами, щелкните нужный процесс правой кнопкой и выберите подходящую команду. Команда **Открыть место хранения файла (Open File Location)** открывает в окне проводника папку, содержащую исполняемый файл процесса. Команда **Завершить дерево процессов (End Process Tree)** останавливает процесс и все зависимые процессы. Команда **Создать файл дампа памяти (Create Dump File)** предназначена для создания дампа памяти выделенного процесса. Щелкнув команду **Свойства (Properties)**, вы откроете окно свойств исполняемого файла.

Управление, восстановление и удаление программ

В Windows 7 установленной считается любая программа, локально установленная на компьютере или доступная для сетевой установки. В Windows XP и более ранних версиях для установки приложений и управления ими применяется утилита Установка и удаление программ (Add Or Remove Programs). В Windows 7 для установки приложения применяется его установочная программа, а для управления установленными приложениями предназначена страница **Программы (Installed Programs)** панели управления.

Чтобы просмотреть, добавить, удалить или восстановить установленную программу при помощи страницы **Программы (Installed Programs)**, выполните следующие действия:

1. Щелкните кнопку **Пуск (Start)** и выберите команду **Панель управления (Control Panel)**. Щелкните категорию **Программы (Programs)**.

2. Щелкните **Программы и компоненты (Programs And Features)**. Будет отображен список установленных программ.
3. В списке **Имя (Name)** щелкните правой кнопкой нужную программу и выберите одну из следующих команд:
   - **Удалить (Uninstall)** Отмена установки программ.
   - **Изменить (Change)** Изменение конфигурации программы.
   - **Восстановить (Repair)** Восстановление программы.

   Отменяя установку программы, помните о следующем:

- Windows предупредит вас, если вы удаляете программу в то время, когда на компьютере работают другие пользователи. Как правило, перед удалением программы следует убедиться, что другие пользователи вышли из системы. В противном случае они могут потерять данные или столкнуться с другими проблемами.
- Windows позволяет удалять лишь программы, установщик которых совместим с Windows. У большинства современных приложений программа установки построена на основе InstallShield, Wise Install или Microsoft Windows Installer, но у старых программ могут быть собственные установщики. У некоторых старых приложений установка заключается в простом копировании файлов в папку программы. В этом случае для отмены установки достаточно удалить соответствующую папку.
- При удалении ряда программ их установщики оставляют в системе некоторые данные — либо ненамеренно, либо с какой-то целью. Поэтому зачастую в папке Program Files остаются подпапки отсутствующих программ. Удаляя эти подпапки, помните, что в них могут содержаться файлы данных или параметры конфигурации, которые можно будет использовать при повторной установке программы.
- Иногда процесс отмены установки завершается сбоем. Часто исправить ситуацию помогает простой перезапуск удаления программы. В других случаях после отмены установки требуется дополнительно «почистить» систему — удалить файлы программы и связанные с ней параметры реестра. В очистке реестра вам поможет программа Windows Installer Cleanup. Подробную информацию о ней и ссылку для загрузки вы найдете по адресу *http://support.microsoft.com/kb/290301*.

Выбор программ по умолчанию

Программы по умолчанию применяются для открытия файлов определенных типов и для обработки файлов на CD- и DVD-дисках, а также на съемных носителях. Настройка программ по умолчанию для всех пользователей компьютера или для конкретного пользователя основана на типах файлов, которые поддерживаются этими программами. Настройки конкретного пользователя обладают более высоким приоритетом, чем глобальные настройки. Допустим, вы сделали Windows Media Player глобальной программой по умолчанию для открытия файлов всех типов, которые поддер-

живаются этой программой, то есть для воспроизведения звуковых, аудио- и видеофайлов. Если один из пользователей предпочитает использовать для воспроизведения мультимедийных файлов Apple iTunes, сделайте это приложение плеером по умолчанию для этого пользователя.

Чтобы настроить программы по умолчанию для всех пользователей компьютера, выполните следующие действия:

1. Щелкните кнопку **Пуск (Start)** и выберите команду **Панель управления (Control Panel)**. Щелкните категорию **Программы (Programs)**.
2. Щелкните **Программы по умолчанию (Default Programs)** и **Настройка доступа программ и умолчаний (Set Program Access And Computer Defaults)**. Откроется диалоговое окно, показанное на рис. 9-4.

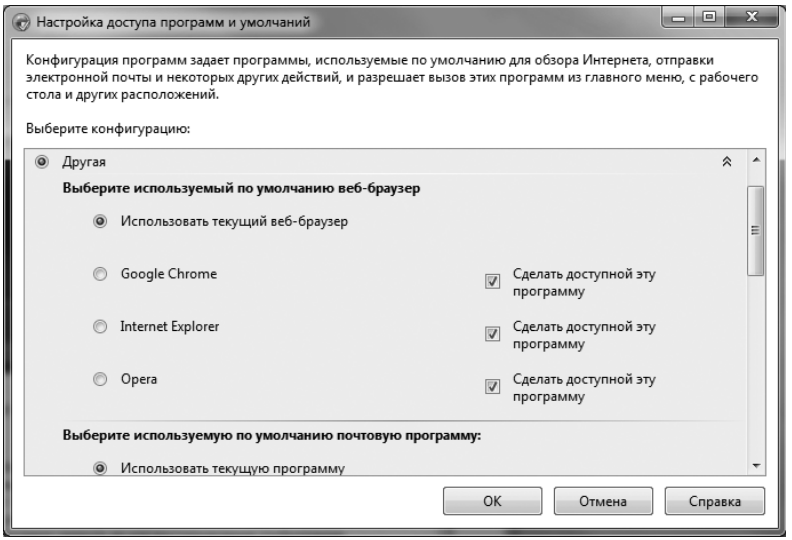

Рис. 9-4. Выберите глобальные программы по умолчанию

3. Выберите один из следующих вариантов:
   - **Microsoft Windows** Задает в качестве программ по умолчанию для просмотра веб, отправки электронной почты, воспроизведения мультимедиа и пр. установленные в данный момент программы Windows.
   - **Не Microsoft (Non-Microsoft)** Задает установленные в данный момент программы в качестве программ по умолчанию для просмотра веб, отправки электронной почты, воспроизведения мультимедиа и пр.
   - **Другая(Custom)** Позволяет задать программы для просмотра веб, отправки электронной почты, воспроизведения мультимедиа и пр. по вашему выбору.
4. Щелкните **OK**, чтобы сохранить изменения.

Чтобы переписать глобальные определения, задайте программы по умолчанию для конкретного пользователя. Чтобы настроить их для текущего пользователя, выполните следующие действия:

1. Щелкните кнопку **Пуск (Start)** и выберите команду **Панель управления (Control Panel)**. Щелкните категорию **Программы (Programs)**.
2. Щелкните **Программы по умолчанию (Default Programs)** и **Задание программ по умолчанию (Set Your Default Programs)**.
3. Выберите нужную программу в списке **Программы (Programs)**.
4. Если вы хотите использовать программу в качестве программы по умолчанию для всех поддерживаемых ею типов файлов и протоколов, щелкните **Использовать эту программу по умолчанию (Set This Program As Default)**.
5. Если вы хотите по умолчанию использовать программы лишь для определенных типов файлов и протоколов, щелкните **Выбрать умолчания для этой программы(Choose Defaults For This Program)**. Выберите нужные типы файлов и щелкните **Сохранить (Save)**.

Управление путем к программам

Для поиска исполняемых файлов в Windows применяется командный путь. Чтобы просмотреть его текущее значение, введите команду **path** в командной строке. В консоли Windows PowerShell введите **$env:path** и нажмите Enter. Просматривая выводные данные программы, обратите внимание, что отдельные пути разделены точками с запятой.

Путь к командам задается в процессе входа в систему на основе системных и пользовательских переменных среды. Основу составляет путь, заданный в системной переменной PATH. В пользовательской переменной PATH этот путь дополняется другими при помощи следующего синтаксиса:

```
%PATH%;ДополнительныеПути
```

Здесь переменная %PATH% включает в строку текущий системный путь, а вместо переменной *ДополнительныеПути* подставляются реальные пути к программам.

Внимание! Неправильно заданный путь может стать причиной серьезных сбоев. Обязательно проверяйте каждый путь перед использованием в рабочей среде. Поскольку путь задается при входе в систему, чтобы оценить влияние внесенных вами изменений вы должны выйти из системы и снова войти в нее.

Учитывайте также применяемый в Windows порядок поиска: если путь стоит в переменной PATH последним, то и поиск в нем осуществляется в последнюю очередь. Иногда это приводит к замедленному выполнению программ и сценариев. Чтобы Windows быстрее находила нужные файлы, поместите соответствующий путь ближе к началу значения переменной.

Задавая командный путь, будьте внимательны. По неосторожности вы легко можете переписать важную информацию. Допустим, можно в пользовательском пути случайно удалить системную переменную %PATH%, тем самым удалив информацию обо всех остальных путях. Чтобы застраховаться от подобных неприятностей, всегда полезно хранить копию пути в файле:

- В командной строке для записи в файл текущего значения командного пути введите команду **path > orig_path.txt**. Помните, что при работе в обычной командной строке без административных полномочий вы не сможете осуществлять запись в защищенные системные расположения. Запишите файл в папку, к которой у вас есть доступ, или в личный профиль. Чтобы просто просмотреть значение командного пути, введите **path**.
- В консоли PowerShell для записи в файл текущего значения командного пути введите команду **$env:path > orig_path.txt**. Если вы используете обычную консоль без административных полномочий, вам не удастся записать файл в защищенные системные области. Запишите файл в папку, к которой у вас есть доступ, или в личный профиль. Чтобы просто просмотреть значение командного пути в консоли PowerShell, введите **$env:path**.

Как в командной строке, так и в окне PowerShell для изменения командного пути применяется утилита Setx.exe. Чтобы отредактировать командный путь, выполните следующие действия:

1. В панели управления щелкните **Система и безопасность (System And Security)** и **Система (System)**.
2. На странице **Система (System)** щелкните **Изменить параметры (Change Settings)** или **Дополнительные параметры системы (Advanced System Settings)**.
3. На вкладке **Дополнительно (Advanced)** диалогового окна **Свойства системы (System Properties)** и щелкните кнопку **Переменные среды (Environment Variables)**.
4. Выберите в списке **Системные переменные (System Variables)** переменную PATH. Щелкните кнопку **Изменить (Edit)**.
5. По умолчанию значение пути выделено. Нажмите клавишу Стрелка Вправо, не нажимая никаких иных клавиш. При этом выделение со значения переменной будет снято, а курсор будет помещен в конец значения.
6. Введите точку с запятой и путь, который хотите добавить. Повторите это действие нужное количество раз, а затем три раза щелкните **OK**.

Чтобы изменить командный путь при помощи предпочтений групповой политики, выполните следующие действия:

1. Откройте объект GPO для редактирования в редакторе управления групповой политикой. Чтобы настроить предпочтения для компьютеров, разверните узел **Конфигурация компьютера\Настройка\Конфигурация Windows (Computer Configuration\Preferences\Windows Settings)** и выделите элемент **Среда (Environment)**. Чтобы настроить предпочтения для пользователей, разверните узел **Конфигурация пользователя\Настройка\Конфигурация Windows (User Configuration\Preferences\Windows Settings)** и выделите элемент **Среда (Environment)**.
2. Щелкните узел **Среда (Environment)** правой кнопкой, разверните подменю **Создать (New)** и выберите команду **Переменные среды (Environ-**

ment Variable). Откроется диалоговое окно **Новые свойства среды (New Environment Properties)**.

3. В списке **Действие (Action)** выберите вариант **Обновить (Update)**, чтобы обновить значение пути, или вариант **Заменить (Replace)**, чтобы удалить переменную PATH и создать ее заново. Затем установите переключатель **Пользовательская переменная (User Variable)**, чтобы работать с пользовательскими переменными.
4. В поле **Имя (Name)** введите **Path**. В поле **Значение (Value)** введите значение переменной. Как правило, в данном случае вводится **%PATH%;**, а затем пути, которые вы хотите добавить, разделяя их точками с запятой. Если на компьютерах, связанных с данным GPO, имеются собственные пользовательские переменные PATH, введите в переменную их значения, чтобы программы на компьютере сохранили работоспособность.
5. При помощи параметров на вкладке **Общие параметры (Common)** задайте способ применения предпочтения. В большинстве случаев значение переменной PATH задается лишь однажды. Если в вашем случае это так, задайте параметр **Применить один раз и не применять повторно (Apply Once And Do Not Reapply)**.
6. Щелкните **OK**. При следующем обновлении политики предпочтение будет применено согласно параметрам GPO, в котором оно определено.

Внимание! Некорректное задание пути может стать причиной серьезных проблем. Прежде чем развертывать обновленный путь на нескольких компьютерах, обязательно проверьте конфигурацию, например создайте в Active Directory объект GPO, применяющийся только к изолированному испытательному компьютеру. Создайте в этом GPO нужный элемент предпочтения, а затем дождитесь обновления политики или примените ее при помощи команды GPUpdate. Если вы зарегистрированы на компьютере, вам придется выйти из системы и снова войти в нее, чтобы оценить результаты.

Управление ассоциациями и расширениями файлов

Запуск программ существенным образом определяется расширениями и ассоциациями файлов. От расширения файла зависит, будет ли Windows считать файл исполняемым. Расширение позволяет пользователю для запуска команды вводить только ее имя. Ассоциации файлов позволяют для открытия файла просто дважды щелкнуть его, и он автоматически откроется в нужном приложении. Применяются расширения файлов двух видов:

- **Расширения исполняемых файлов** Исполняемые файлы определяются в системной переменной %PATHEXT%. Для ее задания, как и для задания переменной PATH, используются диалоговое окно **Переменные среды (Environment Variables)** и предпочтения групповой политики. Для просмотра текущего значения введите команду **set pathext** в командной строке или **$env:pathext** в консоли PowerShell. Значение переменной PATHEXT по умолчанию равно «.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC».

- **Расширения файлов приложений** Расширения файлов приложений называют ассоциациями (association). Они позволяют передавать аргументы исполняемым файлам и открывать документы, электронные таблицы и другие документы, дважды щелкая их значки. Для просмотра сведений об ассоциации введите в командной строке команду **assoc** и расширение файла, например **assoc .doc** или **assoc .docx**. Чтобы узнать, какие типы файлов связаны с приложением, введите в командной строке команду **ftype** и имя ассоциацию, например **ftype Word.Document.8** или **ftype Word.Document.12**.

Примечание Команды Assoc и Ftype являются внутренними командами оболочки Cmd.exe. Чтобы воспользоваться командой Assoc в PowerShell, введите **cmd /c assoc** и расширение файла, например **cmd /c assoc .doc**. Чтобы ввести команду Ftype в консоли PowerShell, введите **cmd /c ftype** и имя ассоциации, например **cmd /c ftype Word.Document.8**.

Порядок поиска нужного расширения в командной строке определяется его расположением в переменной %PATHEXT% отдельно для каждой папки. Если в конкретной папке из командного пути есть несколько исполняемых файлов с введенным вами именем и разными расширениями, у файла .com будет больший приоритет, чем у файла .exe и т. д.

Каждому известному расширению файла (даже для исполняемых файлов) в системе соответствует ассоциация и тип файла. В некоторых случаях имя типа файла состоит из имени расширения без точки и ключевым словом «file», например cmdfile, exefile или batfile, а в ассоциации указано, что первый параметр — это имя команды, а остальные параметры должны передаваться приложению. Например, если вы введете **assoc .exe**, чтобы просмотреть имя ассоциации для файлов .exe, а затем введете **ftype exefile**, то увидите, что ассоциация задана следующим образом:

```
exefile=«%1» %*
```

Это означает, что когда вы вводите имя файла .exe, Windows интерпретирует первое введенное значение как имя команды, которую вы хотите запустить, а все остальное — как параметры для этой команды.

Ассоциации и типы файлов хранятся в реестре Windows и задаются при помощи команд Assoc и Ftype, соответственно. Чтобы создать ассоциацию файлов в командной строке, введите **assoc** и расширение, например **assoc .pl=perlfile**. Чтобы создать тип файла в командной строке, задайте сопоставление типа файла, включая использование параметров, передаваемых с именем команды, например **ftype perlfile=C:\Perl\Bin\Perl.exe “%1” %***.

Связать тип файла или протокол с определенной программой можно также, выполнив следующие действия:

1. Щелкните кнопку **Пуск (Start)** и выберите команду **Панель управления (Control Panel)**. В панели управления щелкните **Программы (Programs)**.

2. Щелкните **Программы по умолчанию (Default Programs)** и **Сопоставление типов файлов и протоколов конкретным программам (Associate A File Type Or Protocol With A Program)**.
3. На странице **Задать сопоставления (Set Associations)** перечислены текущие ассоциации с расширениями файлов и их программами по умолчанию. Чтобы изменить ассоциацию для расширения, выделите его и щелкните **Изменить программу (Change Program)**.
4. Выполните одно из следующих действий:
   - В списке **Рекомендуемые программы (Recommended Programs)** перечислены программы, зарегистрированные в ОС в качестве поддерживающих файлы с выделенным расширением. Щелкните рекомендованную программу, чтобы сделать ее программой по умолчанию для выделенного расширения, и щелкните **OK**.
   - В списке **Другие программы (Other Programs)** перечислены программы, которые также способны поддерживать выделенное расширение. Щелкните программу, чтобы сделать ее программой по умолчанию для выделенного расширения, и щелкните **OK**. Или щелкните **Обзор (Browse)**, чтобы найти иную программу для использования в качестве программы по умолчанию.

В групповой политике для настройки расширений и типов файлов применяются предпочтения. Чтобы создать предпочтение для нового типа файлов, выполните следующие действия:

1. Откройте объект GPO для редактирования в редакторе управления групповой политикой. Разверните узел **Конфигурация компьютера\Настройка\Параметры панели управления (Computer Configuration\Preferences\Control Panel Settings)** и выделите элемент **Параметры папок (Folder Options)**.
2. Щелкните правой кнопкой узел **Параметры папок (Folder Options)**, разверните подменю **Создать (New)** и выберите команду **Тип файла (File Type)**. Откроется диалоговое окно **Новые свойства типа файла (New File Type Properties)**.
3. В списке **Действие (Action)** выберите вариант **Создать (Create)**, **Обновить (Update)**, **Заменить (Replace)** или **Удалить (Delete)**.
4. В поле **Расширение (File Name Extension)** введите расширение для типа файлов без точки, например **pl**.
5. В списке **Связанный класс (Associated Class)** выберите зарегистрированный класс, чтобы ассоциировать его с типом файлов.
6. При помощи параметров на вкладке **Общие параметры (Common)** задайте способ применения предпочтения. В большинстве случаев новый тип файлов создается лишь однажды. Если это так, выберите **Применить один раз и не применять повторно (Apply Once And Do Not Reapply)**.
7. Щелкните **OK**. При следующем обновлении политики предпочтение будет применено согласно параметрам GPO, в котором оно определено.

Чтобы создать элемент предпочтения для новой ассоциации, выполните следующие действия:

1. Откройте объект GPO для редактирования в редакторе управления групповой политикой. Разверните узел **Конфигурация пользователя\Настройка\Параметры панели управления (User Configuration\Preferences\Control Panel Settings)** и выделите элемент **Параметры папок (Folder Options)**.
2. Щелкните правой кнопкой узел **Параметры папок (Folder Options)**, разверните подменю **Создать (New)** и выберите команды **Открыть с помощью (Open With)**. Откроется диалоговое окно **Новые свойства окна «Выбор программы» (New Open With Properties)**.
3. В списке **Действие (Action)** выберите вариант **Создать (Create)**, **Обновить (Update)**, **Заменить (Replace)** или **Удалить (Delete)**.
4. В поле **Расширение (File Name Extension)** введите расширение файла без точки, например **pl**.
5. Щелкните кнопку с многоточием справа от поля **Связанная программа (Associated Program)**, а затем при помощи диалогового окна **Открыть (Open)** выберите программу, которую нужно связать с типом файлов.
6. При необходимости установите флажок **Использовать по умолчанию (Set As Default)**, чтобы сделать программу программой по умолчанию для файлов с заданным ранее расширением.
7. При помощи параметров на вкладке **Общие параметры (Common)** задайте способ применения предпочтения. В большинстве случаев новая ассоциация создается лишь однажды. Если это так, выберите **Применить один раз и не применять повторно (Apply Once And Do Not Reapply)**.
8. Щелкните **OK**. При следующем обновлении политики предпочтение будет применено согласно параметрам GPO, в котором оно определено.

Настройка параметров автозапуска

В Windows 7 параметры автозапуска (AutoPlay) определяют обращение с файлами на CD-дисках, DVD-дисках и переносных устройствах. Чтобы настроить параметры автозапуска для каждого типа CD-, DVD-и других носителей, выполните следующие действия:

1. Щелкните кнопку **Пуск (Start)** и выберите команду **Панель управления (Control Panel)**. В панели управления щелкните **Программы (Programs)**.
2. Щелкните **Программы по умолчанию (Default Programs)** и **Настройка параметров автозапуска (Change AutoPlay Settings)**. Откроется страница **Автозапуск (AutoPlay)** панели управления.
3. При помощи списков задайте параметры автозапуска для каждого типа носителей и устройств, как показано на рис. 9-5.

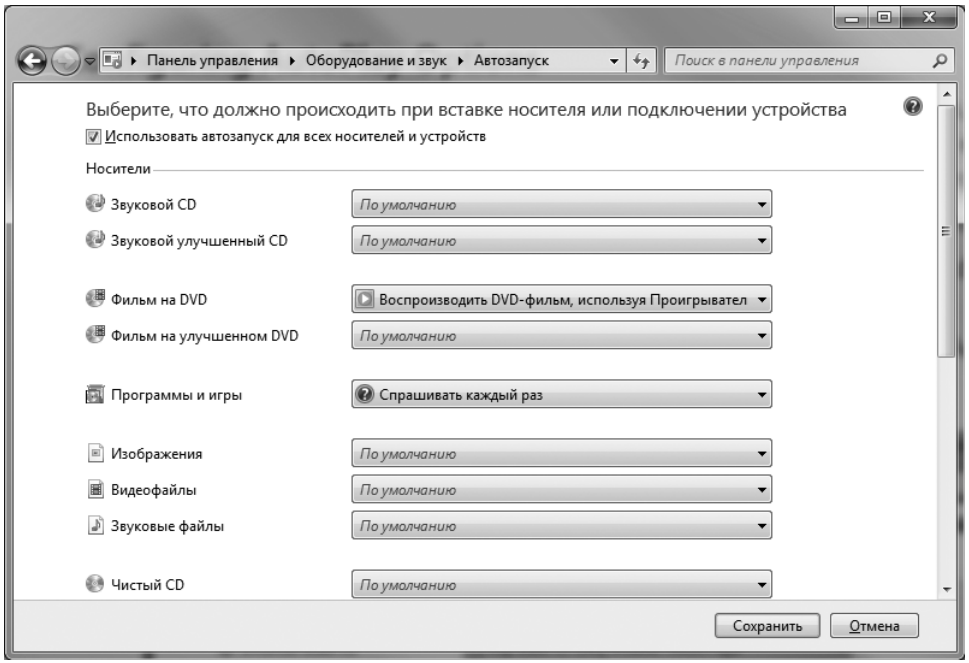

Рис. 9-5. Задайте параметры автозапуска для компакт-дисков и переносных устройств

4. Щелкните **Сохранить (Save)**, чтобы сохранить изменения.

Добавление и удаление компонентов Windows

В Windows XP и прежних версиях Windows для добавления и удаления компонентов ОС применялся компонент Установка компонентов Windows (Add/Remove Windows Components) утилиты Установка и удаление программ (Add Or Remove Programs). В Windows Vista и Windows 7 компоненты Windows не устанавливаются или удаляются, а просто включаются и выключаются.

Чтобы включить или выключить компонент Windows, выполните следующие действия:

1. Щелкните кнопку **Пуск (Start)** и выберите команду **Панель управления (Control Panel)**. В панели управления щелкните **Программы (Programs)**.
2. В разделе **Программы и компоненты (Programs And Features)** щелкните **Включение или отключение компонентов Windows (Turn Windows Features On Or Off)**. Откроется диалоговое окно **Компоненты Windows (Windows Features)**, показанное на рис. 9-6.
3. Установите флажки компонентов, чтобы включить их, и сбросьте флажки компонентов, которые нужно выключить.

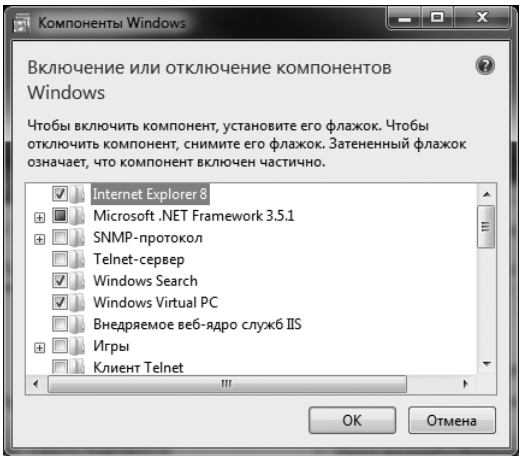

Рис. 9-6. Добавление и удаление компонентов ОС

4. Щелкните **OK**. Windows 7 внесет в конфигурацию компонентов сделанные вами изменения.

Глава 10

Микропрограмма, конфигурация загрузки и запуск

Микропрограмма — главный игрок при запуске компьютера и загрузке ОС. При этом, как ни странно, когда компьютер не загружается или возникает фатальная STOP-ошибка, неисправность зачастую ищут где угодно, только не в микропрограмме. Причина — чрезмерное увлечение диагностикой Windows. А ведь в действительности многие проблемы берут свое начало в микропрограмме: в ее дефектах или неправильной настройке. Чтобы отличать сбои микропрограммы от сбоев ОС, необходимо понимать, как происходит процесс запуска и что происходит на каждом из его этапов. Кроме того, нужно знать, что такое микропрограмма. Опираясь на глубокое понимание предмета, гораздо проще диагностировать и устранять неполадки.

Знакомство с параметрами микропрограммы

В процессе запуска принимают участие микропрограмма, ее интерфейсы и операционная система. Первой при запуске выполняется микропрограмма. Она обеспечивает базовую инициализацию компьютера и работу служб, необходимых для загрузки ОС.

Микропрограмма платформы записана в наборе микросхем материнской платы. Таких наборов микросхем на материнской плате может быть несколько. Микропрограммы на старых материнских платах обновить нельзя. В большинстве новых микросхем обновление микропрограммы поддерживается. *Микропрограмма* (firmware), записанная в наборе микросхем, и базовый *интерфейс микропрограммы* (firmware interface) — совершенно разные вещи.

Интерфейсы микропрограмм и данные загрузки

Интерфейс обеспечивает взаимодействие микропрограммы и ОС в процессе запуска. Способ работы интерфейса и решаемые им задачи зависят от типа интерфейса. На сегодняшний день наиболее распространены интерфейсы, перечисленные ниже:

- базовая система ввода-вывода (Basic Input/Output System, BIOS);

- расширяемый интерфейс микропрограммы (Extensible Firmware Interface, EFI);
- единый расширяемый интерфейс микропрограммы (Unified Extensible Firmware Interface, UEFI).

Интерфейсы BIOS, EFI и UEFI обеспечивают взаимодействие на аппаратном уровне между компонентами оборудования и программным обеспечением. Интерфейсы BIOS, EFI и UEFI, как и сами микросхемы, постоянно обновляются. Благодаря стремительному появлению в 2005-2009 гг. новых разработок в области микросхем, документация и прочие технические сведения, написанные до или во время указанного периода, скорее всего, устарели в отношении современных технологий. Помните о следующем:

- В большинстве справочников интерфейс микропрограммы (firmware interface) называется просто микропрограммой (firmware). В частности, в документации пишут «внести изменения в микропрограмму» или «проверить микропрограмму». Технически же мы вносим изменения в *интерфейс* микропрограммы, а уже он изменяет саму микропрограмму.
- Аббревиатура UEFI используется для обозначения как интерфейса микропрограммы, так и индустриального стандарта. Интерфейс микропрограммы UEFI имеет модульный характер, который может использоваться не только для тех же целей и обеспечивать не только ту же функциональность, чем интерфейсы BIOS и EFI. Стандарт UEFI — это стандарт расширяемых и тестируемых интерфейсов.

Помните также, что микропрограммы BIOS, EFI и UEFI работают совершенно по-разному. Система BIOS используется на компьютерах с процессором x86, 16-разрядной архитектурой реального режима и первоначально предназначалась для запуска компьютера после включения питания. Вот почему взаимодействие и инициализация платформы в BIOS реализованы в направлении от микропрограммы к ОС.

Независимо от типа интерфейса в Windows 7 используется предзагрузочная среда, которая представляет собой расширяемый уровень абстракции, позволяющий ОС работать с интерфейсами различных типов. При этом какая-то специальная архитектура ОС не требуется. В загрузочной среде запуск определяется параметрами из хранилища данных конфигурации загрузки (BCD).

Хранилище BCD есть на всех компьютерах под управлением Windows Vista, Windows 7 и Windows Server 2008. Хранилище BCD находится в файле *реестра BCD* (BCD registry). Расположение реестра зависит от микропрограммы компьютера.

- В системах на основе BIOS реестр BCD расположен в каталоге *\Boot\Bcd* активного раздела.
- В системах на основе EFI реестр BCD находится в системном разделе EFI.

В записях хранилища BCD указан диспетчер загрузки, используемый при запуске, и доступные приложения загрузки. По умолчанию для управления

ходом загрузки применятся Диспетчер загрузки Windows (Windows Boot Manager), в котором можно выбрать приложение загрузки. Приложения загрузки выполняют загрузку конкретной ОС или версии ОС. Загрузкой Windows 7, например, управляет Загрузчик Windows (Windows Boot Loader). Это во многом унифицирует загрузку компьютеров на основе BIOS и EFI.

Как правило, если во время запуска системы нажать клавишу F8 или F12, открывается меню дополнительных вариантов загрузки, в котором можно выбрать один из нескольких дополнительных режимов запуска, включая Безопасный режим (Safe Mode), Ведение журнала загрузки (Enable Boot Logging) и Отключение обязательной проверки подписи драйверов (Disable Driver Signature Enforcement). Эти дополнительные режимы позволяют на время изменить способ запуска ОС в целях диагностики и устранения неисправностей. При этом конфигурация загрузки в хранилище BCD не меняется.

Службы загрузки, службы среды выполнения и прочее

Система BIOS предназначена для управления предзагрузочным обменом данных между ОС и оборудованием, например видеоадаптером, клавиатурой, мышью и жестким диском. При инициализации компьютера BIOS сначала определяет наличие и работоспособность подключенных устройств, а потом начинает загрузку ОС.

В последние годы основные функции BIOS были существенно расширены и включают следующее:

- **Службы загрузки** Набор интерфейсов и протоколов загрузочной среды. Эти службы, как минимум, обеспечивают доступ загрузчика ОС к возможностям платформы, необходимым для завершения загрузки ОС. Эти службы также используются драйверами и приложениями, которым необходим доступ к возможностям платформы. Когда управление компьютером переходит к ОС, службы загрузки останавливаются.
- **Службы среды выполнения** Интерфейсы, предоставляющие доступ к базовому оборудованию платформы, например таймерам. Эти службы выполняются не только в процессе загрузки, но продолжают работать и после остановки служб загрузки системным загрузчиком.
- **Интерфейс ACPI** Табличный интерфейс с системной платой, позволяющий управлять питанием и конфигурацией системы средствами ОС.
- **Службы System Management BIOS (SMBIOS)** Табличный интерфейс, определенный в спецификации Wired for Management Baseline (WMB). Используется для передачи сведений об управлении платформой операционной системе или агенту управления ОС.

Обычно на жестком диске компьютера с системой BIOS есть раздел, содержащий основную загрузочную запись (MBR). Чтобы избавиться от 16-разрядного наследия BIOS, в компании Intel была разработана технология EFI — новая реализация микропрограммы для 64-разрядных процессоров

на базе Itanium. Система EFI применяется с процессорами типа x64 с 64-разрядной архитектурой реального режима. Как и BIOS, система EFI обеспечивает взаимодействие в направлении от микропрограммы к ОС, инициализацию платформы и другие функции. Совместно с EFI, компанией Intel была представлена новая табличная архитектура хранения данных на жестком диске — таблица разделов GUID (GPT). На жестких дисках компьютеров с EFI, как правило, используются разделы GPT.

Унифицированный EFI

Когда компания Intel приступила к разработке EFI, разработчики в Intel и остальном мире пришли к убеждению, что нужно разорвать связь между микропрограммой и архитектурой процессора. Это привело к созданию UEFI. Спецификация UEFI 2.0 была согласована в январе 2006 г., новая редакция — UEFI 2.1 — вышла в январе 2007 г., а следующая редакция — UEFI 2.2 — увидела свет в сентябре 2008 г. В спецификациях UEFI определена модель взаимодействия ОС и микропрограммы. Интерфейс состоит из таблиц с данными, содержащими сведения о платформе, а также вызовов служб загрузки и среды выполнения, доступных для ОС и загрузчика. Интерфейс не зависит от архитектуры процессора, благодаря чему система UEFI работает на компьютерах с 32-разрядной, 64-разрядной и иной архитектурой. Как и в случае EFI, жесткий диск компьютера с системой UEFI состоит обычно из разделов GPT. Между тем, система UEFI не заменяет весь функциональный набор BIOS или EFI, и даже может служить оболочкой для BIOS для EFI.

Ближе к реальности Спецификация UEFI 2.2 состоит более чем из 2000 страниц. На чтение уйдет много времени, поэтому основные сведения о спецификации приведены ниже.

В UEFI микропрограмма выступает в качестве уровня абстрагирования от системы (System Abstraction Level). Микропрограмма абстрагирует отличия в реализациях платформы, предоставляя базовый интерфейс для всех программ более высокого уровня. В спецификации UEFI определены службы загрузки и службы среды выполнения.

К службам загрузки UEFI относятся:

- **Службы событий, таймера и приоритета задач** Нужны для создания, ожидания, уведомления, проверки и закрытия событий; установки таймеров; повышения или восстановления приоритета выполнения заданий.
- **Службы выделения памяти** Отвечают за выделение или освобождение страниц памяти, получение таблиц распределения памяти и выделение (освобождение) памяти в пуле.
- **Службы загрузки модели драйвера** Предназначены для обработки интерфейсов протокола для устройств, открытия и закрытия потоков протоколов, а также подключения и отключения от контроллеров.
- **Службы изображений** Предназначены для загрузки, запуска и выгрузки изображений.

- **Прочие службы** Предназначены для настройки таймеров наблюдения, копирования и задания памяти, установки таблиц конфигурации и выполнения вычислений, связанных с проверкой CRC.

К службам среды выполнения UEFI относятся:

- **Службы переменных** Предназначены для получения и задания значения переменных, а также для запроса значения переменной.
- **Службы времени** Получение и установка текущего времени, а также получение и установка времени пробуждения.
- **Службы виртуальной памяти** Нужны для присвоения виртуальных адресов, сопоставления и преобразования указателей памяти.
- **Прочие службы** Предназначены для перезапуска компьютера, возврата счетчиков и передачи информации в микропрограмму.

В спецификации UEFI определены архитектурно-независимые модели образов, загружаемых посредством EFI, путей к устройствам, драйверов устройств, подписей драйверов и безопасной загрузки. В ней также определено следующее:

- Поддержка консоли, позволяющая выводить простой текст и графику.
- Поддержка спецификации Human Interface Infrastructure, в которой описаны основные механизмы пользовательского ввода и представлены определения связанных протоколов, функций и типов, которые позволяют абстрагировать пользовательский ввод.
- Поддержка носителей — разрешение на ввод-вывод для файловых систем, файлов и носителей.
- Поддержка шин PCI, SCSI и iSCSI, а также загрузки с устройств SCSI или iSCSI.
- Поддержка ввода-вывода через USB хост-контроллер, шины USB и устройств с интерфейсом USB.
- Поддержка сжатия, определяющая алгоритм сжатия и распаковки данных.
- Поддержка установки и удаления таблицы ACPI.
- Поддержка виртуальной машины с байтовой кодировкой. Позволяет загружать и выполнять драйверы устройств EFI.
- Поддержка сетевых протоколов с определениями протоколов SNP (Simple Network Protocol), PXE (Preboot Execution) и BIS (Boot Integrity Services). Протокол SNP определяет интерфейс сетевых адаптеров на уровне пакетов. Протокол PXE используется для сетевого доступа и сетевой загрузки. Протокол BIS применяется при проверке цифровой подписи блока данных на соответствие цифровому сертификату с целью проверки целостности и подлинности. Протокол BIS используется в контексте PXE для проверки полученных по сети образов загрузки перед их выполнением.
- Поддержка управляемых сетевых протоколов с определениями протоколов MNSBP (Managed Network Service Binding Protocol) и MNP (Man-

aged Network Protocol). Эти службы позволяют одновременно использовать сетевые интерфейсы нескольким драйверам, которые активируются событиями. Протокол MNSBP применяется для поиска устройств связи, поддерживаемых дисками MNP, и для управления экземплярами драйверов протокола. Протокол MNP используется в работе драйверов и приложений для простого асинхронного ввода-вывода сетевых пакетов.

- Поддержка протоколов сетевой адресации. Определены протоколы ARP-SBP (Address Resolution Protocol Service Binding Protocol), ARP, DHCPv4, привязка службы DHCPv4, DHCPv6 и привязка службы DHCPv6.
- Поддержка прочих сетевых протоколов. Определены протоколы VLAN, EAP/ EAP Management, TCPv4, привязка службы TCPv4, TCPv6, привязка службы TCPv6, IPv4, привязка службы и конфигурирование IPv4, IPv6, привязка службы и конфигурирование IPv6, конфигурирование IPSec, FTPv4, привязка службы FTPv4, UDPv4, привязка службы UDPv4, UDPv6, привязка службы UDPv6, Multicast TFTPv4 и Multicast TFTPv6.

Важно понимать, что спецификация UEFI не заменяет системы BIOS и EFI. В UEFI используются разные интерфейсы для служб загрузки и служб среды выполнения, но некоторые микропрограммы должны выполнять функции BIOS и EFI, необходимые для конфигурирования и запуска системы, поскольку UEFI этого не делает. Поэтому система UEFI часто располагается над традиционными BIOS и EFI. В этом случае UEFI выступает в роли входных точек инициализации в BIOS или EFI.

Запуск и режимы электропитания

Во время первого запуска компьютера при помощи интерфейса микропрограммы происходит активация всего оборудования, требующегося для его загрузки, в том числе:

- набора микросхем материнской платы;
- процессоров и кеша процессоров;
- системной памяти;
- графических и аудиоконтроллеров;
- внутренних накопителей;
- внутренних плат расширения.

По завершению процесса активации управление компьютером переходит от интерфейса микропрограммы к операционной системе. Что происходит далее, зависит от реализации интерфейса микропрограммы.

- На компьютерах с системой BIOS, работающих под управлением Windows XP и более ранних версий, для загрузки ОС используются файлы Ntldr и Boot.ini. Файл Ntldr предназначен для загрузки ОС, а в файле Boot.ini содержатся параметры запуска системы, включая идентификаторы загрузочных разделов. Параметры файла Boot.ini позволяют добав-

лять свойства, управляющие способом запуска ОС, работой компонентов компьютера и компонентов ОС.

- На компьютерах с системой BIOS, работающих под управлением Windows Vista и последующих версий Windows, для загрузки ОС применяются Диспетчер загрузки Windows (Windows Boot Manager) и Загрузчик Windows (Windows Boot Loader). Диспетчер загрузки Windows (Windows Boot Manager) инициализирует ОС, запуская Загрузчик Windows (Windows Boot Loader), который в свою очередь запускает ОС на основе информации хранилища BCD. Параметры BCD позволяют управлять способом запуска ОС, работой компонентов компьютера и компонентов ОС.
- На компьютерах Itanium загрузка ОС выполняется при помощи файлов Ia64ldr.efi, Diskpart.efi и Nvrboot.efi. Файл Ia64ldr.efi обрабатывает задачу загрузки ОС, а в файле Diskpart.efi содержатся идентификаторы загрузочных разделов. При помощи файла Nvrboot.efi вы можете задать параметры, разрешающие запуск.
- На других компьютерах с системой EFI управление процессом загрузки выполняется в файле Bootmgfw.efi. Затем управление передается Загрузчику Windows (Windows Boot Loader). При помощи файла Bcdedit.exe задаются параметры, разрешающие запуск.
- На компьютерах UEFI, службы загрузки UEFI обеспечивают уровень абстракции. На сегодняшний день этот уровень служит оболочкой для BIOS и EFI. На компьютерах с архитектурой BIOS загрузка ОС выполняется средствами BIOS. На компьютерах с архитектурой EFI ОС загружается средствами EFI.

Интерфейсы микропрограмм

На большинстве компьютеров, чтобы открыть интерфейс микропрограммы, нужно нажать клавишу, которая на первоначальном экране обозначена как клавиша для вызова функции Setup. Как правило, это клавиши F2 или Del. Интерфейс состоит из элементов управления функциональными возможностями оборудования. Вот некоторые из них:

- настройка яркости монитора (на портативных компьютерах);
- настройка уровня шума жесткого диска;
- выбор числа используемых процессоров и их скорости;
- изменение порядка загрузки;
- изменение даты и времени CMOS;
- восстановление исходной конфигурации микропрограммы;
- включение и выключение дополнительных устройств.

В интерфейсах микропрограмм есть также возможность отображения основных сведений о системе, включая следующее:

- параметры адаптера питания (на портативных компьютерах);
- заряд и состояние батареи (на портативных компьютерах);

- тип экрана и исходное разрешение (на портативных компьютерах);
- версия микропрограммы;
- память;
- процессоры;
- накопители;
- видеоадаптер.

В большинстве интерфейсов микропрограмм можно создать пароль-допуск, а также пользовательский и/или общий пароль, которые будут не видны из ОС. Если установлен пароль-допуск, то для изменения конфигурации микропрограммы потребуется ввести пароль. Если установлен пользовательский пароль, то при запуске компьютера для загрузки ОС необходимо ввести пароль. В случае утраты этих паролей, вы не сможете воспользоваться компьютером или изменить параметры микропрограммы до тех пор, пока утерянные пароли не будут сброшены. Причем вместе с паролями будут сброшены и все изменения, внесенные вами в интерфейсе микропрограммы.

Обновление интерфейса микропрограммы часто позволяет решить проблемы или привнести в интерфейс новые функциональные возможности. Если компьютер работает нормально и вам не нужны дополнительные функции интерфейса микропрограммы, не обновляйте интерфейс. Сбой во время обновления интерфейса может привести к повреждению компьютера и невозможности его запуска.

Обзор интерфейсов микропрограмм

Сведения и параметры конфигурации, доступные в интерфейсе микропрограммы, зависят от конкретного компьютера, а также типа и версии интерфейса. Настольные компьютеры, как правило, имеют больше настраиваемых параметров, чем ноутбуки.

На момент написания книги большой популярностью пользовался интерфейс Phoenix TrustedCore. На портативных компьютерах в этом интерфейсе множество страниц меню со сведениями и элементами управления. На странице **Information** собраны основные сведения о конфигурации компьютера, в частности:

- Тип процессора, например: Intel Core2 Duo CPU T5250 at 1.50 GHz.
- Скорость процессора, например: 1500 MHz.
- Тип и модель жесткого диска, например: IDE1, Hitachi HTS541616J9-SA00.
- Серийный номер жесткого диска, например: SB2553SJC9HT1D.
- Модель ATAPI, например: Toshiba DVDW/HD TS-L802A.
- Версия системного BIOS, например: v0.3505.
- Версия VGA BIOS, например: nVidia 0.84.41.00.18.
- Серийный номер.

- Номер бирки.
- Производитель.
- Универсальный уникальный идентификатор (UUID).

На странице **Main** содержатся дополнительные сведения о конфигурации, в том числе (некоторые параметры можно изменять):

- Системное время.
- Системная дата.
- Объем памяти системы.
- Объем расширенной памяти.
- Объем видеопамяти.

Приведенные ниже параметры можно просматривать и изменять:

- **Режим Quiet Boot** Значения: Enabled и Disabled. Если параметр отключен, во время загрузки компьютера выводится экран диагностики.
- **Режим Power On Display** Значения: Auto и Both. Определяет порядок выбора монитора.
- **Режим Network Boot** Значения: Enabled и Disabled. Если параметр включен, выполняется загрузка компьютера по сети.
- **Режим F12 Boot menu** Значения: Enabled и Disabled. Когда параметр включен, то при нажатии клавиши F12 выводится меню загрузки.
- **Режим D2D Recovery** Значения: Enabled и Disabled. Если этот параметр включен, существует возможность восстановления системы из резервной копии на диске.

Страница **Security** предназначена для просмотра и установки паролей-допусков, пользовательских паролей и паролей для жестких дисков. На странице отображено текущее состояние каждого пароля, например:

- Supervisor Password Is: Clear.
- User Password Is: Clear.
- Hard Disk Password Status: Clear.

Управлять паролями позволяют следующие параметры конфигурации:

- **Set Supervisor Password** Защита доступа к интерфейсу микропрограммы.
- **Set User Password** Защита доступа к компьютеру.
- **Set Hard Disk Password** Защита доступа к жесткому диску компьютера.

Чтобы задать пароль, выберите параметр и нажмите клавишу Enter. На предложение системы введите новый пароль, затем подтвердите его. Для продолжения нажмите клавишу Enter.

Приоритет устройств загрузки можно просмотреть и задать на странице **Boot Priority Order**. Вот список, отображающий приоритет загрузочных устройств на ноутбуке Acer:

1. IDE HDD.
2. IDE CD.
3. PCI DEV.

4. USB HDD.
5. USB CDROM.
6. USB FDC.
7. USB KEY.

После включения компьютера производится попытка загрузки с устройства, стоящего в списке на первом месте. В случае неудачи загрузка производится со второго устройства и т. д. Клавишами Стрелка Вверх или Стрелка Вниз выделите устройство, а затем клавишами «+» и «–» переместите устройство вверх или вниз по списку. Нажатием клавиш F или R укажите тип устройства — встроенное (fixed) или съемное (removable). Нажав клавишу X, вы исключите или добавите устройство в список загрузки. Сочетание клавиш Shift+1 включает или отключает устройство.

На странице **Exit** содержатся варианты выхода из интерфейса микропрограммы. В большинстве интерфейсов доступны следующие варианты:

- **Exit Saving Changes** Выйти из интерфейса микропрограммы и сохранить внесенные изменения.
- **Exit Discarding Changes** Выйти из интерфейса микропрограммы, не сохраняя внесенные изменения.
- **Discard Changes** Отмена внесенных изменений и продолжение работы в интерфейсе.
- **Save Changes** Сохранение внесенных изменений и продолжение работы в интерфейсе.

Независимо от страницы меню, на которой вы находитесь, существует стандартный для большинства интерфейсов набор функций.

- Нажмите на клавишу F1 для получения справки.
- Выделение элемента осуществляется клавишами Стрелка Вверх или Стрелка Вниз.
- Выбор страницы меню осуществляется клавишами Стрелка Вправо или Стрелка Влево.
- Изменение значений выполняется при помощи клавиш F5 и F6.
- Клавиша F9 позволяет применить умолчания (вы должны подтвердить действие).
- Нажмите на клавишу Esc, чтобы выйти из интерфейса (вам будет предложено сохранить или отменить изменения).
- Чтобы применить параметр или выполнить команду, нажмите Enter.
- Нажмите F10, чтобы сохранить изменения и выйти из интерфейса микропрограммы.

Как видите, параметров конфигурации не так уж и много. У настольных компьютеров их гораздо больше. Из-за различий в стандартах и соглашениях между производителями интерфейсов названия и значения параметров могут отличаться.

Режимы питания и управление электропитанием

Чтобы лучше разобраться в аппаратных аспектах загрузки, мы рассмотрим свойства оборудования на примере интерфейса ACPI (Advanced Configuration and Power Interface). Чтобы на компьютере работали дополнительные режимы питания ACPI, этот интерфейс должен поддерживаться микросхемами материнской платы, микропрограммой и ОС. Компоненты, поддерживающие интерфейс ACPI, способны наблюдать за состоянием питания компьютера. В ОС, поддерживающей ACPI, есть возможность генерации запроса к интерфейсу микропрограммы на перевод системы в другой режим ACPI, и интерфейс в ответ включает указанный в запросе режим ACPI.

Существует шесть различных режимов электропитания (табл. 10-1): от S0 (система полностью включена и функционирует) до S5 (система полностью выключена). Режимы S1, S2, S3 и S4 называются *спящими*. Система в этих режимах кажется выключенной из-за низкого энергопотребления, но сохраняет достаточный контекст оборудования, чтобы вернуться в рабочий режим без перезагрузки.

Наборы микросхем материнской платы поддерживают определенные режимы питания. Например, одна материнская плата может поддерживать режимы S0, S1, S4 и S5 и не поддерживать режимы S2 и S3. В ОС Windows переход в спящее состояние означает отключение системы с переходом в режим сна или гибернации, а пробуждение — выход системы из режима сна или гибернации. Режимы сна и гибернации позволяют быстрее включать и выключать систему, чем при использовании обычного завершения работы и запуска.

Таким образом, пробуждение компьютера происходит при переходе из состояния Выключено (S5) или любого из спящих режимов (S1-S4) в состояние Включено (S0). Компьютер засыпает при переходе из состояния Включено (S0) в состояние Выключено (S5) или в любой из режимов сна (S1–S4). Переход из одного режима сна в другой режим сна невозможен — для этого компьютер должен сначала перейти в состояние Включено.

Табл. 10-1. Режимы электропитания, поддерживаемые интерфейсом ACPI

Режим	Тип	Описание
S0	Включено	Вся система находится в оперативном режиме, питание полностью включено и работают все составляющие (включая энергозависимые регистры, кеш и ОЗУ)
S1	Режим сна	Система потребляет меньше энергии, чем в режиме S0. Поддерживаются все аппаратные составляющие и процессор
S2	Режим сна	Система потребляет меньше энергии, чем в режиме S1. Прекращается питание процессора, теряется контекст процессора и содержимое кеша

Табл. 10-1. (*окончание*)

Режим	Тип	Описание
S3	Режим сна	Система потребляет меньше энергии, чем в режиме S2. Теряются контекст процессора и оборудования, содержимое кеша и контекст набора микросхем. Сохраняется содержимое системной памяти
S4	Режим гибернации	Энергопотребление системы меньше по сравнению с остальными спящими режимами. Система практически выключена. Данные контекста записаны на жесткий диск, отсутствует энергопотребления контекста. Перезапуск системы производится с сохраненными на диске данными контекста
S5	Выключено	Система полностью отключена, и контекст не сохранен. Для запуска требуется полная перезагрузка

В микропрограмме параметры ACPI находятся на странице **Power**. Ниже приведены возможные параметры питания:

- **After Power Failure или AC Recovery** Режим возобновления работы в случае отключении питания. Возможные параметры продолжения работы: Stay Off, Last State, Power On. При выборе значения Stay Off возобновление работы системы после восстановления питания не производится. Значение Last State означает восстановление системы до состояния, предшествовавшего отключению питания. Значение Power On обеспечивает включение системы после восстановления питания.
- **Wake On LAN From S5 или Auto Power On** Определяет действие при наступлении события пробуждения по спецификации PCI Power Management, когда питание системы выключено. Возможные значения: Stay Off, Power On.
- **ACPI Suspend State или Suspend Mode** Параметры ждущего режима. Обычно ждущий режим реализуется состояниями S1 или S3.

Примечание Для каждого из приведенных выше параметров приведено по два типичных имени. На вашем компьютере имена параметров могут быть иными. Все зависит от версии микропрограммы.

У компаний Intel и AMD имеются дополнительные технологии, позволяющие сократить время запуска и возобновления работы системы. Например, у Intel есть такие параметры питания:

- **Enhanced Intel SpeedStep Technology (EIST)** Параметр может быть включен или выключен.
- **Intel Quick Resume Technology Driver (QRTD)** Параметр может быть включен или выключен.

Технология Enhanced Intel SpeedStep Technology (EIST или SpeedStep) позволяет динамически изменять частоту ядра и подаваемое на процессор напряжение. В результате достигается снижение средних показателей энер-

гопотребления и нагрева. Если используется EIST или другая подобная технология, на странице **Система (System)** панели управления отображаются две разные скорости процессора. Первое значение соответствует штатной скорости процессора. Второе значение — текущая скорость, и ее значение должно быть ниже первого. Если технология отключена, оба значения скорости процессора будут совпадать. Параметры технологии можно изменить в разделе **Управление питанием процессора (Processor Power Management)** вкладки **Дополнительные параметры (Advanced Settings)** диалогового окна **Электропитание (Power Options)**. Как правило, применение данной технологии в Windows 7 не рекомендуется (хотя вполне уместно использовать ее в Windows Vista).

Технология Intel Quick Resume Technology Driver (QRTD) позволяет реализовать мгновенное включение или выключение компьютера после первоначальной загрузки, при условии что компьютер поддерживает технологию Intel Viiv. Это возможно благодаря режиму Quick Resume, в котором работает набор микросхем Intel Viiv. Нажав кнопку питания на компьютере или пульте ДУ, вы переведете компьютер в режим Quick Sleep (быстрый переход в режим сна). Чтобы быстро «разбудить» компьютер (перевести его в режим Quick Resume), достаточно пошевелить мышку, нажать на кнопку включения на клавиатуре (если такая кнопка есть) или нажать на кнопку сна на пульте ДУ. Режим Quick Sleep отличается от обычного режима сна. В режиме Quick Sleep прекращается передача сигнала с видеоплаты на монитор, отключается звук, а индикатор на мониторе указывает на перевод монитора в режим пониженного энергопотребления. Но к работающим компонентам системы — процессору, вентиляторам, и т. д. — питание по-прежнему поступает. Технология создавалась для Windows XP Media Center Edition и в Windows 7 обычно не применяется. Часто она не работает и в Windows Vista. Для нормального перехода Windows Vista в режим сна и пробуждения следует отключить эту функцию в микропрограмме.

Настроив параметры питания, перейдем к имеющимся параметрам загрузки. Вот типичные параметры:

- **Boot Drive Order** Очередность устройств загрузки.
- **Boot To Hard Disk Drive** Возможность загрузки с использованием внутренних дисков. Доступные значения: Disabled и Enabled.
- **Boot To Removable Devices** Возможность загрузки с использованием съемных носителей. Доступные значения: Disabled и Enabled.
- **Boot To Network** Возможность загрузки по сети. Доступные значения: Disabled и Enabled.
- **USB Boot** Возможность загрузки с использованием флеш-накопителя. Доступные значения: Disabled и Enabled.

Как и в случае настроек питания, конкретные имена параметров могут отличаться от тех, что приведены здесь, но смысл их всегда примерно один и тот же. Настройте параметры по своему усмотрению. Если применяется

шифрование дисков BitLocker (BitLocker Drive Encryption), следует включить параметры **Boot To Removable Devices** и (или) **USB Boot**, чтобы USB-накопитель, на котором записан ключ шифрования, был обнаружен системой во время загрузки.

Диагностика и устранение сбоев запуска

Для качественной диагностики и устранения неполадок, возникающих при запуске, необходимо знать последовательность событий, происходящих после нажатия кнопки питания компьютера. Когда вы нажимаете на кнопку питания, происходит следующее:

1. Интерфейс микропрограммы конфигурирует систему — производится процедура *самотестирования при включении питания* (POST).
2. Интерфейс микропрограммы выполняет настройку компьютера — *инициализирует* компьютер.
3. Управление передается от интерфейса микропрограммы в загрузчик ОС — диспетчер загрузки.
4. Диспетчер загрузки запускает программу загрузки. Она использует службы загрузки интерфейса микропрограммы, чтобы завершить загрузку ОС и начать ее запуск ОС. Этапы загрузки ОС таковы:
   а) Загрузка (но не запуск) ядра ОС (Ntoskrnl.exe).
   б) Загрузка (но не запуск) уровня абстрагирования от оборудования (Hal.dll).
   в) Загрузка в память куста реестра HKEY_LOCAL_MACHINE\SYSTEM (из папки %SystemRoot%\System32\Config\System).
   г) Поиск драйверов устройств в разделе HKEY_LOCAL_MACHINE\SYSTEM\Services, затем загрузка в память (без инициализации) драйверов класса загрузки. Драйверы также являются службами (одновременно подготавливаются и драйверы устройств, и системные службы).
   д) Включение функции подкачки памяти.
5. Управление передается от программы загрузки к ядру ОС.
6. Средствами ядра и HAL выполняется инициализация исполняющей системы Windows, в которой обрабатываются сведения о конфигурации, хранящиеся в кусте HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet. Затем происходит запуск драйверов устройств и системных служб.
7. На уровне ядра выполняется запуск Диспетчера сеансов (Session Manager, Smss.exe), который выполняет следующие действия:
   а) Инициализация среды путем создания системных переменных среды.
   б) Запуск подсистемы Win32 (Csrss.exe). На этом этапе монитор переводится из текстового режима в графический.
   в) Запуск Диспетчера входа в систему Windows (Windows Logon Manager, Winlogon.exe), при помощи которого выполняется запуск Диспетчера управления службами (Services Control Manager, Services.exe) и

Администратора локальной безопасности (Local Security Authority, Lsass.exe). После этого система ожидает входа пользователя.

г) Создание дополнительных файлов подкачки.

д) При необходимости после обновления выполняется отложенное переименование файлов, использовавшихся в предыдущем сеансе.

8. Диспетчер входа в систему Windows (Windows Logon Manager) ожидает входа пользователя в систему. Интерфейс входа в систему и поставщик учетных данных по умолчанию получают имя пользователя и пароль. Эта информация передается Администратору локальной безопасности (Local Security Authority) для проверки подлинности.
9. Диспетчер входа в систему Windows (Windows Logon Manager) запускает файл Userinit.exe и Проводник (Windows Explorer). Файл Userinit.exe нужен для инициализации среды пользователя: создания пользовательских переменных среды, выполнения программ автозапуска и других необходимых задач.

Такова последовательность событий при «холодном» пуске компьютера со входом пользователя. При выходе из режима сна, ожидания или гибернации она иная. Последовательность событий зависит также от ОС (если это не Windows) и от ее версии: Windows Vista, Windows 7 или Windows Server 2008.

Иногда найти неисправность помогает точное определение этапа, на котором прервался процесс запуска. В табл. 10-2 перечислены этапы запуска и возможные причины неисправностей на каждом из них. Номера этапов понадобятся нам только для дальнейшего обсуждения.

Табл. 10-2. Неисправности, возникающие при запуске

Этап	Название этапа	Возможная причина неисправности
1	Конфигурирование системы, самотестирование при включении питания	Сбой оборудования или отсутствие устройства
2	Настройка, начальная стадия запуска	Конфигурация микропрограммы, дисковая подсистема или файловая система
3	Загрузчик ОС, диспетчер загрузки	Данные BCD, ошибочный выбор ОС для загрузки или отказ загрузчика
4	Ядро, HAL, исполнительная система Windows	Конфигурация драйвера или службы, зависимости службы
5	Диспетчер сеансов (Session Manager)	Графический режим монитора, системная переменная или конфигурация компонентов

Поиск и устранение неисправностей запуска: этап 1

Сразу после включения компьютера из «холодного» состояния производится конфигурирование системы (самотестирование при включении пита-

ния). На этом этапе средствами микропрограммы выполняются первичная проверка оборудования, проверка наличия необходимых устройств и чтение параметров конфигурации системы из энергонезависимой памяти на материнской плате. Чаще всего в качестве энергонезависимой памяти используется флеш-память. Ее содержимое сохраняется даже после выключения компьютера и отключения питания.

После тестирования и чтения параметров материнской платы микропрограммой тестирование и загрузку параметров проводят дополнительные устройства, обладающие собственным встроенным ПО, например видеоплата и плата хост-контроллера. Если на данном этапе запуск останавливается, скорее всего, произошел сбой оборудования. Кроме того, сбой может свидетельствовать об отсутствии необходимых устройств, например клавиатуры, мыши или жесткого диска. В большинстве случаев интерфейс микропрограммы выведет соответствующее сообщение о неисправности. Если нет изображения, сообщение об ошибке передается в виде серии прерывистых звуковых сигналов.

Если неисправность связана с клавиатурой, мышью или монитором, проверьте надежность их подключения к компьютеру. Если неполадка связана с другим устройством, попробуйте изменить конфигурацию устройства в интерфейсе микропрограммы или замените устройство.

Поиск и устранение неисправностей запуска: этап 2

Вслед за конфигурированием системы идет этап настройки, или начального запуска. Устройства, участвующие в запуске ОС, определяются параметрами интерфейса микропрограммы. На запуск системы влияет очередность устройств загрузки и состояние каждого из них (включено или выключено) во время загрузки. Как уже отмечалось, сначала производится попытка загрузки с первого устройства из списка. В случае неудачи, загрузка производится со второго устройства и т. д. Если загрузить систему не удается ни с одного из устройств, будет выведено примерно следующее сообщение:

```
Non-system disk or disk error
Replace and press any key when ready to continue
```

Проверьте очередность загрузки. Если вы пытаетесь загрузить систему с CD- или DVD-диска, убедитесь в наличии носителя и в том, что включен параметр загрузки с CD/DVD. Пытаясь загрузиться с жесткого диска, убедитесь, что жесткий диск присутствует в списке загрузки и стоит перед USB- и другими съемными носителями. Если жесткий диск установлен недавно, выключите компьютер и отключите питание, а затем проверьте правильность присоединения кабелей и перемычек.

Не всегда параметры загрузки в микропрограмме интуитивно понятны. Поэтому далее я привожу примеры для компьютеров разных производителей. В ноутбуке HP параметры загрузки находятся на странице **System Configuration** в подменю **Boot Options/Boot Order**. В подменю **Boot Options** доступны следующие варианты:

- **F10 And F12 Delay (sec)** Время, отводимое пользователю во время запуска, чтобы нажать на клавиши F10 и F12.
- **CD-ROM Boot** Включение или отключение загрузки с CD-ROM.
- **Floppy Boot** Включение или отключение загрузки с гибкого диска.
- **Internal Network Adapter Boot** Включение или отключение сетевой загрузки.

Клавишами Стрелка Вверх или Стрелка Вниз выделите параметр. Затем нажмите Enter, чтобы просмотреть параметр и задать его значение.

Очередность устройств в подменю **Boot Order** может быть такой:

1. USB Floppy.
2. ATAPI CD/DVD ROM Drive.
3. Notebook Hard Drive.
4. USB Diskette On Key.
5. USB Hard Drive.
6. Network Adapter (только если включена загрузка по сети).

Устройство выделяется клавишами Стрелка Вверх и Стрелка Вниз. Чтобы переместить устройство по списку, нажмите на F5 или F6. Помните, что на многих новых компьютерах различаются внешние USB-накопители разных видов. Флеш-накопители обозначаются как *USB Diskette On Key*, а жесткие диски с интерфейсом USB — как *USB hard drive*. Разницы для пользователей нет никакой.

На компьютере Dell параметры загрузки находятся на странице **System** в подменю **Boot Sequence**. Очередность устройств загрузки такова:

1. Onboard or USB CD-ROM Drive.
2. Onboard SATA Hard Drive.
3. Onboard or USB Floppy Drive (not present).
4. Onboard IDE Hard Drive (not present).
5. Add-in Hard Drive (not present).
6. USB Device (not present).
7. Add-in Hard Drive (not present).

Обратите внимание, что встроенные устройства отмечены словом «Onboard». Выделите устройство клавишами Стрелка Вверх и Стрелка Вниз. Затем, нажимая клавиши U или D, переместите устройство вверх или вниз по списку. Чтобы включить устройство в список или убрать устройство из списка, нажмите Пробел. Если устройство отсутствует и вы хотите окончательно удалить его из списка, нажмите Del.

В меню **Drives** есть следующие подменю:

- **Diskette Drive** Определение конфигурации гибких дисков.
- **Drive 0: SATA-0** Включение и отключение указанного устройства ATA или SATA в интерфейсе микропрограммы.
- **Drive 1: SATA-1** Включение и отключение указанного устройства ATA или SATA в интерфейсе микропрограммы.

- **SATA Operation** Управление конфигурацией аппаратного RAID.

Возможность загрузки компьютера с накопителя USB задается в меню **Onboard Devices/USB Controller**.

Совет Все больше становится настольных компьютеров, оснащенных аппаратными RAID-контроллерами. На моем компьютере Dell такая плата есть. Параметры ее конфигурации находятся на странице **System** в подменю **SATA Operation**. Обычно аппаратный RAID-контроллер поддерживает технологии RAID 0 и RAID 1. Технология RAID 0 не обеспечивает защиты данных, а просто растягивает логический том на несколько физических дисков. Технология RAID 1 обеспечивает защиту данных за счет создания зеркальных дисков. Зеркальные диски представляют собой два физических диска, данные на которых идентичны.

Поиск и устранение неисправностей запуска: этап 3

После настройки управление передается из интерфейса микропрограммы диспетчеру загрузки. В диспетчере загрузки запускается программа загрузки.

На компьютерах с системой BIOS информация считывается из основной загрузочной записи (MBR). Как правило, MBR является первым сектором данных на диске. В ней содержатся загрузочные инструкции и таблица разделов. Программа загрузки находится в первом секторе данных *активного* раздела, который иногда называют еще и *загрузочным*. Данные содержат сведения о файловой системе раздела. Они нужны микропрограмме, чтобы найти и запустить программу Bootmgr из корневого каталога загрузочного раздела. В программе Bootmgr процесс загрузки из реального режима переходит в 32- или 64-разрядный защищенный режим, и выполняется загрузка соответствующей версии Диспетчера загрузки Windows (Windows Boot Manager). Диспетчер загрузки Windows (Windows Boot Manager) находит и запускает Загрузчик Windows (Windows Boot Loader).

Проблемы на этом этапе возникают, если отсутствует активный загрузочный раздел или отсутствуют или повреждены данные загрузочного сектора. Характерные сообщения об ошибках выглядят так:

```
Error loading operating system
```

или

```
Invalid partition table
```

Зачастую восстановить работу удается при помощи инструмента Восстановление запуска (Startup Repair).

В компьютерах с системой EFI имеется встроенный диспетчер загрузки. Во время установки Windows в диспетчер загрузки EFI добавляется запись с заголовком Windows Boot Manager (Диспетчер загрузки Windows), которая указывает на исполняемый файл диспетчера загрузки в системном разделе EFI (\Efi\Microsoft\Boot\Bootmgfw.efi). После этого управление передается от диспетчера загрузки Загрузчику Windows (Windows Boot Loader).

Проблемы могут начаться при установке другой ОС или при изменении параметров диспетчера загрузки EFI. В большинстве случаев восстановить нормальную работу можно при помощи инструмента Восстановление запуска (Startup Repair) или при помощи изменения параметров диспетчера загрузки EFI.

Поиск и устранение неисправностей запуска: этап 4

Для завершения загрузки ОС загрузчику необходимы службы загрузки интерфейса микропрограммы. При помощи загрузчика загружается ядро ОС (Ntoskrnl.exe), а вслед за ним — уровень абстрагирования от оборудования (Hal.dll). Далее в память загружается куст реестра HKEY_LOCAL_MACHINE\SYSTEM (из каталога *%SystemRoot%\System32\Config\System*), а затем выполняется поиск драйверов устройств в ключе HKEY_LOCAL_MACHINE\SYSTEM\Services. В этом кусте реестра загрузчик ищет драйверы класса загрузки, загружая их в память.

После передачи управления от загрузчика к ядру ОС средствами ядра и HAL выполняется инициализация исполняющей системы Windows. В ней обрабатываются сведения о конфигурации, хранящиеся в кусте HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet, после чего запускаются драйверы устройств и системные службы. Запуск драйверов и служб происходит в соответствии с их типом запуска. Это значение задано в подразделе Start раздела HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services*Имя*, где *Имя* — имя устройства или службы. Допустимые значения: 0 (драйвер загрузки), 1 (системный драйвер), 2 (автоматически загружаемый драйвер или служба), 3 (драйвер или служба, загружаемые по требованию), 4 (отключенный и не включенный драйвер или служба) и 5 (служба с отложенным запуском). Запуск драйверов происходит в следующем порядке: загрузочные, системные, автоматически загружаемые, загружаемые по требованию, с отложенным запуском.

Большинство проблем на данном этапе связано с неправильной конфигурацией драйвера или службы. Некоторые драйверы и службы зависят от других компонентов и служб. Если зависимые компоненты или службы недоступны или неправильно настроены, это также может стать причиной сбоя запуска.

В ходе запуска для конфигурирования устройств и служб используются подразделы HKEY_LOCAL_MACHINE\SYSTEM. В подразделе Select для этой цели используется несколько значений:

- **Current** Указатель на подраздел ControlSet, в котором содержатся определения текущей конфигурации для всех устройств и служб.
- **Default** Указатель на подраздел ControlSet, содержащий определения конфигурации, которые будут использованы компьютером во время следующего запуска, при условии что не произойдет никакой ошибки и не будет использована альтернативная конфигурация.

- **Failed** Указатель на подраздел ControlSet, содержащий определение конфигурации, при которой произошел сбой загрузки Windows.
- **LastKnownGood** Указатель на подраздел ControlSet, содержащий определение конфигурации, использованной при последнем удачном входе в систему.

Во время обычного запуска используется набор параметров Default. Вообще, если запуск проходит без ошибок и не выбран вариант загрузки с последней удачной конфигурацией, значения Default, Current и LastKnownGood указывают на определение из одного и того же подраздела ControlSet, например ControlSet001. Если загрузить компьютер не удалось, при обращении к последней удачной конфигурации в дополнительных вариантах загрузки, происходит перезапись значения Failed конфигурацией, использованной при неудавшейся загрузке. В случае успешного запуска, если не было обращения к последней удачной конфигурации, значение LastKnownGood перезаписывается и указывает на определение текущей конфигурации.

Поиск и устранение неисправностей запуска: этап 5

На завершающем этапе средствами ядра выполняется запуск Диспетчера сеансов (Session Manager). С его помощью выполняется инициализация среды путем создания системных переменных среды и запуска подсистемы Win32. Здесь происходит переход из текстового режима, который использовался с начала загрузки, в графический. Как правило, если видеоадаптер неисправен или неправильно установлен, вы не увидите изображения ни в текстовом, ни в графическом режиме. Если же адаптер неправильно настроен, зачастую это становится ясно при переходе в графический режим. В случае неправильной настройки видеоадаптера на экране возникнут полосы (о диагностике проблем монитора читайте в главе 7).

Монитор — лишь один из компонентов, сбой которых может произойти на столь позднем этапе запуска. Если ошибка возникает на данном этапе, сбойные компоненты можно найти при помощи журнала загрузки. Если возникает STOP-ошибка, сведения о сбойном компоненте вы найдете в ее сообщении.

В Диспетчере сеансов (Session Manager) открывается Диспетчер входа в систему Windows (Windows Logon Manager), который запускает Диспетчер управления службами (Services Control Manager — Services.exe) и Администратора локальной безопасности (Local Security Authority). После этого система ожидает входа пользователя. После ввода корректного имени пользователя и пароля в Диспетчере входа в систему Windows (Windows Logon Manager) запускаются программа Userinit.exe и оболочка Проводника Windows. Файл Userinit.exe нужен для инициализации среды пользователя: создания пользовательских переменных, выполнения программ автозапуска и других необходимых задач. Оболочка Проводника Windows отвечает за рабочий стол, панель задач и систему меню.

Проблемы запуска, возникающие непосредственно перед или после входа пользователя в систему, скорее всего, связаны с неверно настроенной службой или приложением запуска. В ходе диагностики допускается временное отключение служб и приложений запуска, но об этом позднее, в разделе «Конфигурация загрузки системы».

Запуск и конфигурация загрузки

В меню **Дополнительные варианты загрузки (Advanced Boot Options)** перечислены дополнительные режимы загрузки. Чтобы открыть это меню, во время запуска ОС нажмите клавишу F8 или F12. Использование дополнительных режимов не вносит постоянных изменений в конфигурацию загрузки или хранилище BCD. Для изменения конфигурации загрузки и хранилища BCD вам придется воспользоваться диалоговым окном **Загрузка и восстановление (Startup And Recovery)**, утилитой Конфигурация системы (System Configuration) или программой BCD Editor. В следующих разделах мы поговорим о работе с этими инструментами.

Настройка запуска и параметров восстановления

Диалоговое окно **Загрузка и восстановление (Startup And Recovery)** предназначено для настройки основных вариантов запуска ОС. Здесь вы задаете ОС, загружаемую по умолчанию, время, в течение которого отображается список доступных ОС, а также, при необходимости, время отображения вариантов восстановления. Независимо от количества установленных на компьютере ОС оптимизация данных параметров позволит сократить время ожидания при запуске и тем самым ускорить процесс загрузки.

Чтобы открыть диалоговое окно **Загрузка и восстановление (Startup And Recovery)**, выполните следующие действия:

1. Откройте панель управления, а затем щелкните **Система и безопасность (System And Security)** и **Система (System)**.
2. На левой панели открывшегося окна **Система (System)** перейдите по ссылке **Дополнительные параметры системы (Advanced System Settings)**. Откроется диалоговое окно **Свойства системы (System Properties)**.
3. На вкладке **Дополнительно (Advanced)** диалогового окна **Свойства системы (System Properties)** в разделе **Загрузка и восстановление (Startup And Recovery)** щелкните **Параметры (Settings)**. Откроется диалоговое окно **Загрузка и восстановление (Startup And Recovery)**, показанное на рис. 10-1.
4. Если на компьютере установлено более одной ОС, в списке **Операционная система, загружаемая по умолчанию (Default Operating System)** укажите систему, которую следует запускать по умолчанию.
5. Задайте временной интервал отображения списка ОС, щелкнув флажок **Отображать список операционных систем (Time To Display List Of Op-**

erating Systems) и введя значение интервала в секундах. Чтобы не затягивать процесс запуска, установите значение, равное 5 сек.

6. Задайте время вывода списка вариантов восстановления, щелкнув флажок **Отображать варианты восстановления (Time To Display Recovery Options When Needed)** и задайте значение интервала в секундах. Чтобы не затягивать процесс запуска, значение не должно превышать 5 сек.
7. В области **Отказ системы (System Failure)** установите флажок **Записать событие в системный журнал (Write An Event To The System Log)**, если нужно записывать события, связанные со сбоем системы. Для автоматического перезапуска компьютера после сбоя установите флажок **Выполнить автоматическую перезагрузку (Automatically Restart)**.
8. Щелкните **OK**, чтобы сохранить параметры.

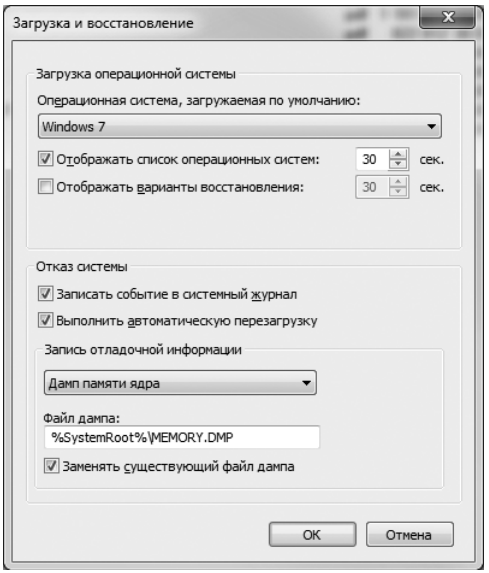

Рис. 10-1. Параметры запуска системы

Конфигурация загрузки системы

Более тонко настроить способ запуска компьютера позволяет утилита Конфигурация системы (System Configuration, Msconfig.exe). Обычно ее используют для диагностики и устранения неисправностей. В частности, в ней можно настроить диагностический запуск компьютера с загрузкой только базовых устройств и служб.

Команду для запуска утилиты Конфигурация системы (System Configuration) вы найдете в меню **Администрирование (Administrative Tools)**. Также программу Конфигурация системы (System Configuration) можно открыть и так: щелкните кнопку **Пуск (Start)** и введите **msconfig.exe** в поле поиска. Окно утилиты разделено на несколько вкладок (рис. 10-2).

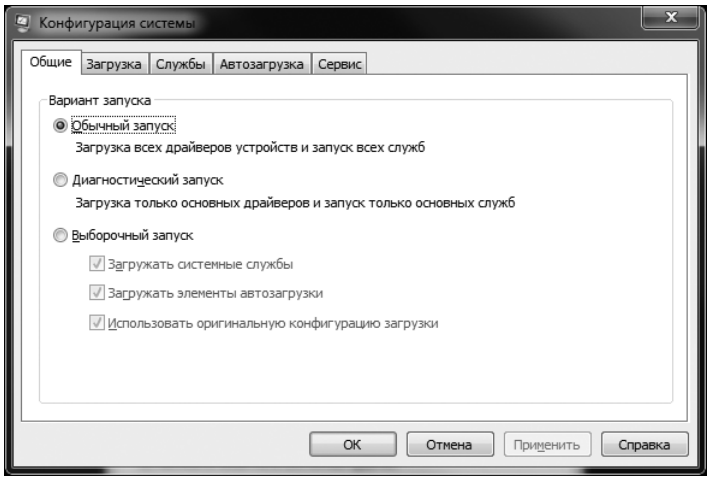

Рис. 10-2. Устранение неисправностей в утилите Конфигурация системы (System Configuration)

Исходный рубеж диагностики и устранения неполадок проходит на вкладке **Общие (General)**, параметры которой определяют способ запуска. Здесь вы можете задать запуск с обычными параметрами, диагностический или выборочный запуск. После перезагрузки компьютера и устранения неисправностей снова откройте утилиту Конфигурация системы (System Configuration), на вкладке **Общие (General)** щелкните **Обычный запуск (Normal Startup)**, а затем щелкните **OK**.

Параметры вкладки **Загрузка (Boot)** позволяют настроить работу отдельных процессов запуска. Здесь можно задать запуск в различных вариантах безопасного режима, а также дополнительные параметры, например **Без GUI (No GUI Boot)**. Если нужно сохранить установленные параметры и после устранения неполадок, установите флажок **Сделать эти параметры загрузки постоянными (Make All Boot Settings Permanent)**, сохранив тем самым параметры в виде записи конфигурации загрузки.

Щелкнув кнопку **Дополнительные параметры (Advanced Options)** на вкладке **Загрузка (Boot)**, вы откроете диалоговое окно **Дополнительные параметры загрузки (BOOT Advanced Options)**, показанное на рис. 10-3. Помимо функций блокировки PCI и включения отладки в вашем распоряжении следующие дополнительные параметры:

- **Количество процессоров, используемых ОС** Здесь учитываются как процессоры в отдельных разъемах, так и ядра одного ЦП. Этот параметр используют, когда заподозрена проблема с дополнительными процессорами и нужно определить, не связана ли неисправность с конфигурацией многопроцессорной системы или параллелизмом. Допустим, на компьютере с одним четырехядерным ЦП неудовлетворительно работает приложение, применяемое на предприятии для управления складскими ресурсами. Одновременно на компьютерах с одним процессором это при-

ложение работает очень хорошо. После того как вы установили режим загрузки компьютера с использованием одного процессора, быстродействие программы намного улучшилось. Вам остается лишь включить все процессоры и довести до сведения разработчиков, что программу следует оптимизировать для параллельной обработки.

- **Наибольший объем памяти, используемый ОС** Параметр используется, если есть подозрение, что проблема связана с установкой дополнительной памяти. Допустим, в стандартной конфигурации на компьютере было установлено ОЗУ объемом 2 Гб. Позже, добавив еще 2 Гб, вы обнаружили, что компьютер не загружается. Чтобы исключить память из списка возможных неисправностей, ограничьте ее объем до 2048 Мб.

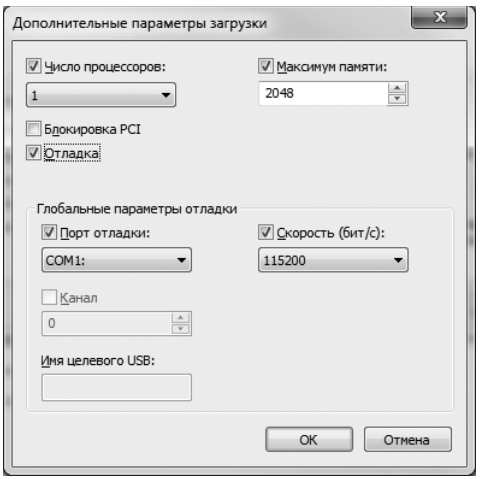

Рис. 10-3. Дополнительные параметры загрузки помогают при диагностике отдельных неисправностей

Если вы полагаете, что сбои при запуске возникают из-за установленных на компьютере служб, это легко проверить: на вкладке **Общие (General)** задайте режим диагностического или выборочного запуска. Временно отключите службы на вкладке **Службы (Services)**, перезагрузите компьютер и проверьте его работоспособность. Если неисправность устранена, значит, вы точно определили ее причину. Отключите службу на постоянной основе или проверьте наличие у поставщика ее новой версии. Для отключения службы сбросьте соответствующий флажок на вкладке **Службы (Services)**.

Если нормальной работе предположительно мешают программы автозагрузки, воспользуйтесь вкладкой **Автозагрузка (Startup)**. Для отключения приложения автозагрузки сбросьте соответствующий флажок. Если неисправность устранена, значит, вы нашли причину. Отключите приложение автозагрузки или проверьте наличие у поставщика новой версии.

Проведя диагностику при помощи утилиты Конфигурация системы (System Configuration), не забудьте отменить параметры выборочного запуска. Когда все проблемы решены и компьютер перезапущен, снова откройте

утилиту Конфигурация системы (System Configuration), восстановите исходные параметры и щелкните **OK**.

Программа BCD Editor

В хранилище BCD содержится много записей. На компьютерах с BIOS вы найдете следующие записи:

- **Одна запись Диспетчера загрузки Windows (Windows Boot Manager)** Существует только один диспетчер загрузки, поэтому и запись диспетчера загрузки только одна.
- **Одна или несколько записей Загрузчика Windows (Windows Boot Loader)** Имеется по одной записи для каждого экземпляра Windows 7, Windows Vista или более поздних версий Windows, установленных на компьютере.

На компьютере с другими ОС имеется также одна запись для старой операционной системы. Она не является приложением загрузки и нужна для инициализации файлов Ntldr и Boot.ini, чтобы загрузить компьютер в Windows XP или более ранней версии Windows. Если на компьютере установлено более одного экземпляра Windows XP или другой ранней версии, сначала выберите запись старой ОС, а затем — выберите конкретный экземпляр.

Диспетчер загрузки Windows (Windows Boot Manager) сам относится к приложениям загрузки. Кроме того, существуют и другие загрузчики, в том числе:

- загрузчик старой ОС (Ntldr);
- загрузчик Windows Vista и более поздних ОС (Osloader);
- приложение загрузочного сектора (Windows Boot Sector Application, Bootsector);
- диспетчер загрузки микропрограмм (Firmware Boot Manager, Fwbootmgr);
- загрузчик возобновления Windows (Windows Resume Loader, Resume).

Для просмотра и управления хранилищем BCD применяется редактор BCD Editor (Bcdedit.exe). Программа BCD Editor — это утилита командной строки. Чтобы просмотреть записи хранилища BCD с ее помощью, выполните следующие действия:

1. Щелкните кнопку **Пуск (Start)**, выберите **Все программы (All Programs)** и щелкните **Стандартные (Accessories)**.
2. Щелкните правой кнопкой команду **Командная строка (Command Prompt)** и выберите команду **Запуск от имени администратора (Run As Administrator)**.
3. В командной строке введите **bcdedit**.

В табл. 10-3 перечислены команды для работы с хранилищем BCD, позволяющие делать следующее:

- создавать, импортировать, экспортировать и идентифицировать запись хранилища BCD;
- создавать, удалять и копировать отдельные записи хранилища BCD;
- задавать и удалять значения параметра записи в хранилище BCD;
- управлять очередностью загрузки и диспетчером загрузки;
- настраивать службы аварийного управления (Emergency Management Services, EMS);
- настраивать и управлять отладкой загрузки, а также отладкой гипервизора.

Табл. 10-3. Команды BCD Editor

Команда	Описание
/bootdebug	Включение и отключение отладки приложения загрузки
/bootems	Включение и отключение служб аварийного управления (Emergency Management Services) для приложения загрузки
/bootsequence	Однократное задание очередности загрузки для диспетчера загрузки
/copy	Копирование записей в хранилище
/create	Создание новых записей в хранилище
/createstore	Создание нового (пустого) хранилища BCD
/dbgsettings	Установка глобальных параметров отладчика
/debug	Включение и отключение отладки ядра для записи ОС
/default	Задание записи для использования диспетчером загрузки по умолчанию
/delete	Удаление записей из хранилища
/deletevalue	Удаление параметров записи из хранилища
/displayorder	Задание очередности отображения элементов в меню вариантов загрузки
/ems	Включение и отключение служб аварийного управления (Emergency Management Services) для записи ОС
/emssettings	Задание глобальных параметров служб аварийного управления (Emergency Management Services)
/enum	Вывод списка записей хранилища
/export	Экспорт содержимого системного хранилища в файл. Позднее, файл можно использовать для восстановления состояния системного хранилища
/hypervisor-settings	Задание параметров гипервизора
/import	Восстановление состояния системного хранилища из файла резервной копии, созданного при помощи команды /export
/mirror	Создание зеркальной копии записей в хранилище

Табл. 10-3. (*окончание*)

Команда	Описание
/set	Присвоение значений параметрам записи в хранилище
/sysstore	Определение устройства системного хранилища (только для систем на базе EFI)
/timeout	Установка значения таймаута для диспетчера загрузки
/toolsdisplay-order	Установка очередности отображения в диспетчере загрузки меню инструментальных средств
/v	Переключение в расширенный режим вывода сведений

Управление хранилищем BCD

Утилита командной строки BCD Editor предназначена для управления конфигурацией предзагрузочной среды. Последующие разделы посвящены редактированию хранилища данных BCD, но делать это рекомендуется только опытным ИТ-специалистам. В целях предосторожности перед внесением любых изменений в хранилище BCD сделайте полную резервную копию компьютера. Почему? Потому что в случае ошибки компьютер, возможно, перестанет загружаться.

Просмотр записей BCD

На компьютерах могут быть системные и несистемные хранилища BCD. Системное хранилище BCD содержит загрузочные записи ОС и связанные с ними параметры загрузки. Работая с утилитой BCD Editor, вы редактируете именно системное хранилище BCD.

На компьютере с одной ОС, записи BCD выглядят примерно так, как показано в листинге 10-1. В этом примере хранилище BCD компьютера содержит две записи: для Диспетчера загрузки Windows (Windows Boot Manager) и для Загрузчика Windows (Windows Boot Loader). Диспетчер загрузки вызывает загрузчик, а тот уже загружает Windows 7 при помощи Winload.exe.

Листинг 10-1. Записи хранилища BCD на компьютере с одной ОС

```
Windows Boot Manager
--------------------
identifier  {bootmgr}
device   partition=L:
description Windows Boot Manager
locale   en-US
inherit  {globalsettings}
default  {current}
resumeobject   {1cafd2de-e035-11dd-bbf6-bdebeb67615f}
displayorder   {current}
   {975a8204-9658-11dd-993e-9aea7965e9da}
   {360a7720-e6ef-11dc-89b8-84b5c301f2c8}
```

```
toolsdisplayorder {memdiag}
timeout  30

Windows Boot Loader
-------------------
identifier  {current}
device   partition=C:
path  \Windows\system32\winload.exe
description Windows 7
locale   en-US
inherit  {bootloadersettings}
recoverysequence  {1cafd2e0-e035-11dd-bbf6-bdebeb67615f}
recoveryenabled   Yes
osdevice partition=C:
systemroot  \Windows
resumeobject   {1cafd2de-e035-11dd-bbf6-bdebeb67615f}
nx OptIn
```

Свойства записей BCD для Диспетчера загрузки Windows (Windows Boot Manager) и Загрузчика Windows (Windows Boot Loader) идентичны и перечислены в табл. 10-4.

Табл. 10-4. Свойства записи BCD

Свойство	Описание
Description	Сведения о типе записи
Device	Отображение физического пути к устройству. Пример для раздела на физическом диске: partition=C:
FileDevice	Отображение пути к устройству, на котором записан файл, например partition=C:
FilePath	Путь к необходимому файлу, например \hiberfil.sys
Identifier	Дескриптор записи. Это может быть тип приложения загрузчика, например Bootmgr или Ntldr, ссылка на текущую запись ОС или глобально уникальный идентификатор (GUID) конкретного объекта
Inherit	Список наследуемых записей
Locale	Национальный стандарт компьютера, например ru-RU. Этим стандартом определяется язык пользовательского интерфейса. В папке \Boot находятся вложенные папки, соответствующие всем поддерживаемым национальным стандартам. В каждой из этих папок содержатся локализованные элементы интерфейса Диспетчера загрузки Windows (Windows Boot Manager) и утилиты Диагностика памяти Windows (Windows Memory Diagnostic, Memdiag.exe)
OSDevice	Путь к устройству, на котором записана ОС, например partition=C:
Path	Действительный путь к файлу загрузчика, например \Windows\System32\winload.exe

При работе с хранилищем BCD и программой BCD Editor вам встретятся ссылки на общеизвестные идентификаторы, которые приведены в табл. 10-5, и GUID. Формат GUID таков (каждый символ N представляет шестнадцатеричное значение):

```
{NNNNNNNN-NNNN-NNNN-NNNN-NNNNNNNNNNNN}
```

Например:

```
{975a8204-9658-11dd-993e-9aea7965e9da}
```

Дефисы в GUID должны стоять точно в указанных местах. Идентификаторы GUID, как и общеизвестные идентификаторы, заключаются в фигурные скобки.

Табл. 10-5. Общеизвестные идентификаторы

Идентификатор	Описание
{badmemory}	Общий список дефектов ОЗУ, наследуемый любой записью загрузчика
{bootloadersettings}	Набор глобальных параметров, наследуемый всеми записями Загрузчика Windows (Windows Boot Loader)
{bootmgr}	Указывает на запись Диспетчера загрузки Windows (Windows Boot Manager)
{current}	Представление виртуального идентификатора, который соответствует загрузочной записи ОС, работающей в данный момент
{dbgsettings}	Глобальные параметры отладки, наследуемые любой записью загрузчика
{default}	Представление виртуального идентификатора, который соответствует записи диспетчера загрузки, используемой по умолчанию
{emssettings}	Глобальные параметры служб аварийного управления (Emergency Management Services), наследуемые любой записью загрузчика
{fwbootmgr}	Указывает на запись диспетчера загрузки микропрограммы. Используется на системах с EFI
{globalsettings}	Набор глобальных параметров, наследуемых всеми записями загрузчика
{hypervisorsettings}	Параметры гипервизора, наследуемые всеми записями загрузчика
{legacy}	Указывает на загрузчик прежних версий ОС Windows (Windows Legacy OS Loader, Ntldr). Он используется для запуска ОС Windows, предшествующих Windows Vista
{memdiag}	Указывает на запись приложения проверки памяти

Табл. 10-5. (*окончание*)

Идентификатор	Описание
{ntldr}	Указывает на загрузчик прежних версий ОС Windows (Windows Legacy OS Loader, Ntldr), используемый для запуска ОС Windows до Windows Vista
{ramdiskoptions}	Дополнительные параметры, необходимые диспетчеру загрузки для виртуальных дисков
{resumeloadersettings}	Набор глобальных параметров, наследуемых всеми записями приложения, которое выполняет возобновление работы из режима гибернации

Если на компьютере установлены дополнительные экземпляры Windows Vista, Windows 7 или более поздних версий Windows, для каждой из них в хранилище BCD есть дополнительные записи. В частности, в хранилище BCD может иметься по одной записи для Диспетчера загрузки Windows (Windows Boot Manager) и Загрузчика Windows (Windows Boot Loader) для каждой ОС.

Если на компьютере установлена старая ОС, то в хранилище BCD ей соответствует три записи: для Диспетчера загрузки Windows (Windows Boot Manager), Загрузчика прежних версий ОС Windows (Windows Legacy OS Loader) и Загрузчика Windows (Windows Boot Loader). Пример записи Загрузчика прежних версий ОС Windows (Windows Legacy OS Loader) приводится в листинге 10-2.

Листинг 10-2. Запись Загрузчика прежних версий ОС Windows (Windows Legacy OS Loader)

```
Windows Legacy OS Loader
------------------------
identifier: {ntldr}
device:  partition=C:
path: \ntldr
description:   Earlier version of Windows
```

Записи Диспетчера загрузки Windows (Windows Boot Manager), Загрузчика прежних версий ОС Windows (Windows Legacy OS Loader) и Загрузчика Windows (Windows Boot Loader) относятся к основному типу записей. Кроме них, в хранилище BCD содержатся сведения о параметрах и утилитах загрузки. В записи Загрузчика Windows (Windows Boot Loader) могут задаваться значения параметров состояния загрузки, в частности, включение или отключение политики защиты выполнения. Запись Загрузчика Windows (Windows Boot Loader) также может содержать сведения о доступных загрузочных утилитах, например Диагностика памяти Windows (Windows Memory Diagnostic).

Для просмотра действительного значения идентификаторов GUID, необходимых для управления записями в хранилище BCD, введите **bcdedit /v** в командной строке с повышенными полномочиями.

Создание и идентификация хранилища BCD

Для создания несистемного хранилища BCD в программе BCD Editor используется команда:

```
bcdedit /createstore Путь
```

где *Путь* — путь к папке, в которой создается несистемное хранилище, например:

```
bcdedit /createstore c:\non-sys\bcd
```

В системах с интерфейсом EFI можно временно назначить устройство системного хранилища при помощи команды /**sysstore**. Синтаксис команды таков:

```
bcdedit /sysstore Устройство
```

где *Устройство* — идентификатор устройства системного хранилища, например:

```
bcdedit /sysstore c:
```

В качестве устройства должен быть указан системный раздел. Этот параметр не сохраняется после перезагрузки и используется только в тех случаях, когда устройство системного хранилища определено неоднозначно.

Импорт и экспорт хранилища BCD

Отдельные команды утилиты BCD Editor предназначены для импорта и экспорта хранилища BCD. Чтобы экспортировать копию системного хранилища BCD в заданную папку, используется команда /**export**. Ее синтаксис:

```
bcdedit /export Путь
```

где *Путь* — действительный путь к папке для сохранения копии системного хранилища, например:

```
bcdedit /export c:\backup\bcd
```

Для восстановления экспортированной копии системного хранилища используется команда /**import**. Ее синтаксис:

```
bcdedit /import Путь
```

где *Путь* — действительный путь к папке, из которой выполняется импорт копии системного хранилища, например:

```
bcdedit /import c:\backup\bcd
```

В системе с интерфейсом EFI у команды /**import** есть параметр /**clean**, предназначенный для удаления всех существующих записей загрузки микропрограммы, например:

```
bcdedit /import c:\backup\bcd /clean
```

Создание, копирование и удаление записей BCD

Команды утилиты BCD Editor позволяют создавать, копировать и удалять записи хранилища BCD. Для создания в хранилище BCD записей идентификатора, приложения и наследования предназначена команда /**create**.

Как видно из табл. 10-5, в программе BCD Editor поддерживается много общеизвестных идентификаторов, например {dbgsettings}, применяемый для создания записи параметров отладчика, {ntldr}, используемый при создании записи Загрузчика прежних версий ОС Windows (Windows Legacy OS Loader), и {ramdiskoptions} для создания записи дополнительных параметров RAM-диска. Синтаксис команды для создания записи идентификатора таков:

```
bcdedit /create ИД /d «Описание»
```

где *ИД* — общеизвестный идентификатор создаваемой записи, например:

```
bcdedit /create {ntldr} /d «Earlier Windows OS Loader»
```

Также вы можете создавать записи специальных приложений загрузчика, в том числе:

- **Bootsector** Указывает на приложение реального режима загрузочного сектора, применяется для задания загрузочного сектора приложения реального режима.
- **Osloader** Указывает на приложение-загрузчик ОС для загрузки Windows Vista и более поздних версий.
- **Resume** Указывает на Загрузчик возобновления Windows (Windows Resume Loader), служащий для вывода ОС из режима гибернации.
- **Startup** Указывает на приложение, работающее в реальном режиме. Используется для идентификации приложения реального режима.

Синтаксис команды таков:

```
bcdedit /create /application Тип /d «Описание»
```

где *Тип* — один из описанных выше типов приложений, например:

```
bcdedit /create /application osloader /d «Windows Vista»
```

Для удаления записей из системного хранилища используется команда /**delete**. Синтаксис ее таков:

```
bcdedit /delete идентификатор
```

При попытке удаления общеизвестного идентификатора необходимо использовать параметр /**f**, чтобы принудительно выполнить удаление, например:

```
bcdedit /delete {ntldr} /f
```

По умолчанию программа выполняется с параметром /**cleanup**. Это значит, что в программе BCD Editor удаляются все остальные ссылки на удаляемую запись. Иными словами, из хранилища данных удаляются все став-

шие недействительными ссылки на удаленный идентификатор. Поскольку ссылки удаляются также из элемента displayorder, выбранной по умолчанию может оказаться другая ОС. Чтобы удалить запись и очистить все ссылки, кроме ссылок в элементе displayorder, используется команда /**nocleanup**.

Присвоение значений записям BCD

После создания записи нужно присвоить значения ее дополнительным параметрам. Вот основной синтаксис присвоения значений:

```
bcdedit /set ИД параметр значение
```

где *ИД* — идентификатор изменяемой записи; *параметр* — определяемый параметр; значение — ***значение*** параметра. Например:

```
bcdedit /set {current} device partition=d:
```

Чтобы удалить параметры и их значения, используется команда /**deletevalue**. Синтаксис ее таков:

```
bcdedit /deletevalue ИД параметр
```

где *ИД* — идентификатор изменяемой записи, а *параметр* — удаляемый параметр. Например:

```
bcdedit /deletevalue {current} badmemorylist
```

Существует несколько способов ввода в параметры логических выражений. Значение True можно обозначить при помощи 1, On, Yes или True. Значение False обозначается как 0, Off, No или False. Чтобы просмотреть записи BCD значения параметров для всех загрузочных утилит, введите в командной строке с повышенными полномочиями **bcdedit /enum all /v**. В выводе команды отображается подробная информация обо всех записях BCD независимо от их текущего состояния. У каждой дополнительной записи есть свое назначение и настраиваемые значения, в том числе:

- **Resume From Hibernate** Отображение текущей конфигурации возобновления работы. В нашем примере предзагрузочная утилита Winresume.exe, управляющая возобновлением работы, находится в папке C:\Windows\System32. Значение параметра Filepath указывает, что данные гибернации хранятся в файле Hiberfil.sys в корневом каталоге устройства, на котором записана ОС (параметр OSDevice). В нашем примере это диск C:. Если на компьютере реализован режим расширения физических адресов (PAE) и включен режим отладки, функция выхода из состояния гибернации работает иначе. Эти компоненты управляются параметрами Pae и Debugoptionenabled.
- **Windows Memory Tester** Отображение текущей конфигурации утилиты Windows Memory Diagnostic. В нашем примере предзагрузочная утилита Memtest.exe, управляющая диагностикой памяти находится в папке C:\Boot. По умолчанию утилита Windows Memory Diagnostic должна об-

наруживать поврежденную память, поэтому параметру Badmemoryaccess присвоено значение Yes. Чтобы отключить эту функцию, введите **bcdedit /set {memdiag} badmemoryaccess NO**. К настраиваемым параметрам диагностики памяти относится Passcount — количество проходов, и Testmix — набор тестов: базовый (Basic) или расширенный (Extended). Например: **bcdedit /set {memdiag} passcount 2 textmix basic**.

- **Windows Legacy OS Loader** Отображение текущей конфигурации загрузки прежних версий Windows. Параметр Device определяет раздел, используемый по умолчанию, например C:. В параметре Path задан стандартный путь к загрузчику, например к файлу *Ntldr*.
- **EMS Settings** Конфигурация, используемая при загрузке при помощи служб аварийного управления (Emergency Management Services). Включение EMS задается в отдельных записях Windows Boot Loader. Если службы EMS предоставляются BIOS и вы хотите применить параметры BIOS, введите **bcdedit /emssettings bios**. Для EMS можно задать порт и скорость передачи данных, например: **bcdedit /emssettings EMSPORT:2 EMSBAUDRATE:115200**. Чтобы включить или отключить EMS в приложении загрузки, используйте параметр /**bootems**. После него укажите идентификатор приложения загрузки и требуемое состояние — On или Off.
- **Debugger Settings** Конфигурация, используемая при загрузке с включенным отладчиком. Включение отладчика задается в отдельных записях Загрузчика Windows (Windows Boot Loader). Чтобы просмотреть параметры отладчика гипервизора, введите **bcdedit /debugsettings**. Когда включен режим отладочной загрузки, параметр DebugType определяет тип отладчика: SERIAL, 1394 или USB. Для отладчика типа SERIAL в параметре DebugPort задается используемый отладчиком последовательный порт, а в параметре BaudRate указана скорость передачи данных отладки. Для отладчика 1394 в параметре Channel задается канал отладки. Для отладчика USB вы можете задать в параметре TargetName имя USB, используемого для отладки. При любом типе отладки параметр /Noumex служит для пропуска исключений пользовательского режима. Примеры установки режима отладки:

```
bcdedit /dbgsettings SERIAL DEBUGPORT:1 BAUDRATE:115200
bcdedit /dbgsettings 1394 CHANNEL:23
bcdedit /dbgsettings USB TARGETNAME:DEBUGGING
```

- **Hypervisor Settings** Отображение конфигурации гипервизора, применяемой для работы с гипервизором при включенном режиме отладки. Включение отладчика задается в отдельных записях Windows Boot Loader. Для просмотра параметров отладки гипервизора выполните команду **bcdedit /hypervisorsettings**. Если включен режим отладки гипервизора, тип отладчика задается в параметре HypervisorDebugType, а параметр HypervisorDebugPort указывает на последовательный порт, используемый при отладке. В параметре HypervisorBaudRate указана скорость передачи

данных отладки. Эти параметры аналогичны параметрам записи Debugger Settings. Пример задания значений: **bcdedit /hypervisorsettings SERIAL DEBUGPORT:1 BAUDRATE:115200**. Шина FireWire также применяется для отладки гипервизора. При этом необходимо отделять слово «channel» от значения двоеточием, как показано в следующем примере: **bcdedit /hypervisorsettings 1394 CHANNEL:23**.

В табл. 10-6 приведены основные параметры записей приложений загрузки. Поскольку Диспетчер загрузки Windows (Windows Boot Manager), Диагностика памяти Windows (Windows Memory Diagnostic), Загрузчик ОС Windows (Windows OS Loader) и Загрузчик возобновления Windows (Windows Resume Loader) относятся к приложениям загрузки, данные параметры применимы и к ним.

Табл. 10-6. Основные параметры записей загрузчика

Параметр	Описание
BadMemoryAccess	При значении True приложению разрешено использовать память из списка поврежденной памяти. При значении False приложениям нельзя использовать память из списка поврежденной памяти
BadMemoryList	Список номеров страничных блоков поврежденной памяти
BaudRate	Целочисленное значение, определяющее скорость передачи для последовательного отладчика
BootDebug	Логическое значение, определяющее включение или отключение отладчика загрузки
BootEMS	Логическое значение, определяющее включение или отключение служб аварийного управления (Emergency Management Services)
Channel	Целочисленное значение, определяющее канал для отладчика 1394
ConfigAccessPolicy	Настройка политики доступа с параметрами DEFAULT или DISALLOWMMCONFIG
DebugAddress	Целочисленное значение, определяющее адрес последовательного порта отладчика
DebugPort	Целочисленное значение, определяющее номер последовательного порта для последовательного отладчика
DebugStart	Значения: ACTIVE, AUTOENABLE или DISABLE
DebugType	Значения: SERIAL, 1394 или USB
EMSBaudRate	Целочисленное значение, определяющее скорость передачи для служб аварийного управления (Emergency Management Services)
EMSPort	Номер последовательного порта для служб аварийного управления (Emergency Management Services)

Табл. 10-6. (*окончание*)

Параметр	Описание
FirstMegaBytePolicy	Значение политики первого мегабайта: USENONE, USEALL или USEPRIVATE
GraphicsModeDisabled	Логическое значение, определяющее включение или отключение графического режима
GraphicsResolution	Разрешение экрана, например 1024×768 или 800×600
Locale	Языковой стандарт приложения загрузки
Noumex	При значении True исключения пользовательского режима пропускаются. При значении False исключения пользовательского режима не пропускаются
NoVESA	Логическое значение, определяющее включение и отключение режимов монитора VESA
RecoveryEnabled	Логическое значение, определяющее возможность использования последовательности восстановления
RecoverySequence	Задание последовательности восстановления
RelocatePhysical	Задание физического адреса, по которому будет перемещена физическая память автоматически выбранного узла NUMA
TargetName	Конечное имя отладчика USB в текстовом формате
TestSigning	Логическое значение, определяющее возможность использования сертификатов подписи предварительного тестового кода
TruncateMemory	Адрес физической памяти, по которому или за пределами которого вся память игнорируется

В табл. 10-7 приведены основные параметры записей приложений загрузчика ОС Windows (Osloader).

Табл. 10-7. Основные параметры приложений загрузчика ОС Windows

Параметр	Описание
AdvancedOptions	Логическое значение, определяющее включение или отключение дополнительных параметров
BootLog	Логическое значение, определяющее включение или отключение отладчика загрузки
BootStatusPolicy	Политика состояния загрузки. Возможные значения: DisplayAllFailures, IgnoreAllFailures, IgnoreShutdownFailures и IgnoreBootFailures
ClusterMode-Addressing	Максимальное число процессоров, включаемых в один кластер APIC (Advanced Programmable Interrupt Controller)
ConfigFlags	Установка флагов конфигурации процессора

Табл. 10-7. (*продолжение*)

Параметр	Описание
DbgTransport	Задание имени файла для транспорта частного отладчика
Debug	Логическое значение, определяющее включение или отключение отладки ядра
DetectHal	Логическое значение, определяющее включение или отключение обнаружения HAL и ядра
DriverLoad-FailurePolicy	Политика ошибки загрузки драйвера. Возможные значения: Fatal и UseErrorControl
Ems	Логическое значение, определяющее включение или отключение служб аварийного управления (Emergency Management Services) ядра
Hal	Задание имени файла для частного уровня HAL
HalBreakPoint	Логическое значение, определяющее включение или отключение особой точки останова HAL
Hypervisor-LaunchType	Настройка типа запуска гипервизора. Возможные значения: Off и Auto
HypervisorPath	Задание пути к частному двоичному файлу гипервизора
IncreaseUserVA	Целочисленное значение (Мб), на которое следует увеличить объем виртуального адресного пространства, используемого процессами пользовательского режима
Kernel	Задание имени файла для частного ядра
LastKnownGood	Логическое значение, определяющее включение или отключение режима загрузки с последней удачной конфигурацией
MaxProc	Логическое значение, определяющее включение или отключение режима отображения наибольшего числа процессоров в системе
Msi	Включение прерываний, отмечаемых сообщениями (MSI). Возможные значения: Default и ForceDisable
NoCrashAutoReboot	Логическое значение, определяющее включение или отключение функции автоматического перезапуска после сбоя
NoLowMem	Логическое значение, определяющее разрешение или запрет на использование нижней области памяти
NumProc	Задание количества процессоров, используемых при запуске
Nx	Управление функцией защиты от выполнения данных. Возможные значения: OptIn, OptOut, AlwaysOn и AlwaysOff

Табл. 10-7. (*окончание*)

Параметр	Описание
OneCPU	Логическое значение, определяющее принудительное использование процессора загрузки
OptionsEdit	Логическое значение, определяющее включение или отключение редактора параметров
OSDevice	Задание устройства, содержащего корневую папку системы
Pae	Управление режимом PAE. Возможные значения: Default, ForceEnable и ForceDisable
PerfMem	Задание размера буфера (Мб) для регистрации данных производительности
QuietBoot	Логическое значение, определяющее включение или отключение экрана загрузки
RemoveMemory	Целочисленное значение (Мб), на которое следует уменьшить объем памяти, используемой ОС
RestrictAPICCluster	Задание наибольшего числа используемых системой кластеров APIC
ResumeObject	Идентификатор объекта возобновления, связанного с данным объектом ОС
SafeBoot	Варианты использования безопасного режима. Возможные значения: Minimal, Network и DsRepair
SafeBootAlternateShell	Логическое значение, определяющее использование альтернативной оболочки при загрузке в безопасном режиме
Sos	Логическое значение, определяющее включение или отключение вывода дополнительных сведений загрузки
SystemRoot	Определение пути к корневой папке системы
UseFirmwarePCISettings	Логическое значение, определяющее разрешение или запрет на использование периферийных устройств (PCI), настроенных в BIOS
UsePhysicalDestination	Логическое значение, определяющее принудительное применение физического контроллера APIC
Vga	Логическое значение, определяющее принудительное применение драйвера VGA
WinPE	Логическое значение, определяющее включение или отключение загрузки предустановочной среды Windows

Предотвращение выполнения данных и режим расширения физических адресов

Технология предотвращения выполнения данных (DEP) предназначена для защиты памяти. Когда на компьютере включена функция DEP, все адреса памяти в приложении отмечаются процессором как неисполняемые, за исключением адресов, в которых явно содержится исполняемый код. При попытке выполнения кода из страницы памяти, которая отмечена как неисполняемая, процессор вызывает исключение и предотвращает выполнение кода. Тем самым предотвращается внедрение постороннего кода, например, вируса, в большую часть областей памяти.

На компьютерах, процессоры которых поддерживают функцию защиты памяти от выполнения (NX), эта функция может работать как под управлением ОС, так и нет. Для этого параметру nx нужно присвоить значение OptIn или OptOut, соответственно, например:

```
bcdedit /set {current} nx optout
```

Если параметру NX присвоено значение OptIn, технология DEP включена только для основных программ и служб Windows. Это значение по умолчанию. Если параметр NX имеет значение OptOut, технология DEP применяется ко всем программам и службам, а не только к стандартным программам и службам Windows. Программы, к которым не нужно применять технологию DEP, следует отдельно исключить, как описано в разделе «Настройка DEP» главы 6. Параметры AlwaysOn и AlwaysOff определяют режим работы защиты NX — всегда включена или всегда выключена. Например:

```
bcdedit /set {current} nx alwayson
```

Процессоры, поддерживающие защиту NX, должны работать в режиме PAE. Для настройки режима PAE предназначен параметр Pae, принимающий значения Default, ForceEnable или ForceDisable. Если параметр pae имеет значение Default, используется стандартная конфигурация режима PAE. Значение ForceEnable предписывает принудительное использование PAE, а значение ForceDisable означает, что режим PAE не используется ОС. Например:

```
bcdedit /set {current} pae default
```

Изменение порядка отображения операционных систем

Очередность отображения на экране диспетчеров загрузки, сопоставленных с отдельными установками Windows Vista, Windows 7 или другими версиями, изменяется при помощи команды /**displayorder**. Синтаксис команды таков:

```
bcdedit /displayorder id1 id2 … idn
```

где *id1* — идентификатор первой ОС в очереди; *id2* — идентификатор второй ОС и т. д. Чтобы изменить очередность отображения ОС, обозначенных в записях BCD, показанных ниже:

```
Windows Boot Loader
-------------------
identifier  {14504de-e96b-11cd-a51b-89ace9305d5e}

Windows Boot Loader
-------------------
identifier  {8b78e48f-02d0-11dd-af92-a72494804a8a}
```

используйте команду:

```
bcdedit /displayorder {14504de-e96b-11cd-a51b-89ace9305d5e}
{8b78e48f-02d0-11dd-af92-a72494804a8a}
```

Чтобы поставить запись ОС на первое место, используется команда /**displayorder** с параметром /**addfirst**, например:

```
bcdedit /displayorder {8b78e48f-02d0-11dd-af92-a72494804a8a} /addfirst
```

Чтобы поставить запись ОС на последнее место, используется команда /**displayorder** с параметром /**addlast**, например:

```
bcdedit /displayorder {8b78e48f-02d0-11dd-af92-a72494804a8a} /addlast
```

Изменение записи ОС, загружаемой по умолчанию

Для изменения записи ОС, загружаемой по умолчанию, предназначена команда /**default**. Синтаксис команды таков:

```
bcdedit /default id
```

где *id* — идентификатор операционной системы в записи загрузчика. Чтобы установить ОС, указанную в данной записи BCD

```
Windows Boot Loader
-------------------
identifier {975a8204-9658-11dd-993e-9aea7965e9da}
```

в качестве ОС, загружаемой по умолчанию, используйте команду:

```
bcdedit /default {975a8204-9658-11dd-993e-9aea7965e9da}
```

Чтобы задать в качестве ОС, загружаемой по умолчанию, операционную систему Windows версии, предшествующей Windows 7, укажите идентификатор Загрузчика прежних версий ОС Windows (Windows Legacy OS Loader). Так выглядит соответствующая запись BCD:

```
Windows Legacy OS Loader
------------------------
identifier  {466f5a88-0af2-4f76-9038-095b170dc21c}
device   partition=C:
path  \ntldr
description Earlier Microsoft Windows Operating System
```

В следующем примере устанавливается загрузка по умолчанию файла Ntldr:

```
bcdedit /default {466f5a88-0af2-4f76-9038-095b170dc21c}
```

Изменение времени ожидания по умолчанию

Время ожидания загрузки ОС по умолчанию задается при помощи команды /**timeout**. Время ожидания указывается в секундах:

```
bcdedit /timeout 30
```

Чтобы ОС по умолчанию загружалась автоматически, установите время ожидания, равное 0 сек.

Временное изменение очередности загрузки

Иногда требуется один раз загрузить какую-либо ОС, а потом вернуться к прежнему порядку загрузки. Для этого предназначена команда /**bootsequence**. В команде необходимо указать идентификатор ОС, которую нужно запустить после перезагрузки, например:

```
bcdedit /bootsequence {975a8204-9658-11dd-993e-9aea7965e9da}
```

После перезагрузки компьютера указанная ОС будет задана в качестве загружаемой по умолчанию, но только до следующей перезагрузки. После следующей перезагрузки будет восстановлена прежняя очередность.

Глава 11

Технологии TPM и BitLocker

В Windows 7 имеется много средств обеспечения безопасности, предназначенных для защиты компьютера от нападения со стороны злоумышленников, получивших доступ к нему через сеть или Интернет. Но как быть с теми, кто получил прямой физический доступ к компьютеру? В таких случаях настройки безопасности Windows уже неприменимы. Если кому-то удалось загрузить ваш компьютер, пусть даже установив на нем другую ОС, он получит доступ к любым данным, сохраненным на компьютере, в том числе, возможно, к конфиденциальным данным вашей организации. Далее, непрерывно растет популярность флеш-накопителей, и потому пользователи часто носят данные с собой. Информация на «флешках», как правило, не имеет никакой защиты. Если накопитель утерян, любой, кто его найдет, сможет получить доступ к данным и прочитать их.

Чтобы защитить компьютеры и данные в подобных ситуациях, в архитектуру Windows 7 включены технологии шифрования BitLocker, BitLocker to Go и службы доверенного платформенного модуля (Trusted Platform Module, TPM). Совместная работа этих функций обеспечивает защиту компьютера и данных, сохраненных на флеш-накопителях. Технология шифрования диска BitLocker позволяет зашифровать весь том, а технология BitLocker To Go представляет собой шифрование виртуального тома для USB-накопителя. Наконец, TPM используется для вящего повышения безопасности совместно с технологией шифрования диска BitLocker.

Создание доверенных платформ

Чтобы в полной мере использовать все преимущества службы TPM, компьютер Windows 7 необходимо оборудовать совместимым TPM-модулем и соответствующим микропрограммным обеспечением. В Windows 7 поддерживаются TPM версии 1.2, и выше и требуется микропрограммное обеспечение, совместимое со стандартами группы Trusted Computing Group (TCG). Микропрограммы, совместимые с TCG, поддерживают статический корень измерения доверия (Statistic Root of Trust Measurement), определенный TCG. В некоторых конфигурациях TPM и BitLocker вам также понадобится микропрограммная поддержка чтения USB-накопителей в момент запуска.

TPM: основы

В Windows 7 включена шифрующая файловая система EFS (Encrypting File System), позволяющая шифровать файлы и папки. При этом доступ к уязвимым данным возможен лишь с использованием сертификата открытого ключа. Сертификаты шифрования сохраняются в профиле пользователя. Если у пользователя есть доступ к своему профилю и ключам, которые в нем содержатся, он получит доступ к зашифрованным файлам.

Система EFS надежно защищает данные от несанкционированного доступа из сети, но не убережет их от злоумышленников, которые получили прямой физический доступ к компьютеру. В случае утери компьютера, его кражи или входа злоумышленника в систему EFS не защитит данные, поскольку злоумышленник получит доступ к компьютеру до начала загрузки, сможет загрузить другую ОС и изменить конфигурацию компьютера. Затем он проникнет в первоначальную ОС и войдет в нее в качестве пользователя или даже локального администратора. Так или иначе, злоумышленник получит полный доступ к компьютеру и к данным на нем.

Чтобы оградить компьютер от физической атаки и обеспечить дополнительный уровень защиты, в Windows 7 включена архитектура доверенного платформенного модуля (TPM). Служба TPM защищает компьютер при помощи специального аппаратного компонента — микросхемы TPM, которую обычно устанавливают на материнскую плату компьютера, соединяя с остальной системой при помощи аппаратной шины. На компьютерах Windows 7 система TPM обеспечивает повышенную защиту данных, своевременное подтверждение целостности загрузочных файлов и выявление попыток проникновения на диск, предпринимавшихся, пока ОС была отключена.

TPM создает криптографические ключи и зашифровывает их так, что расшифровать их можно только при помощи TPM. Этот процесс называется *сокрытием*, или *привязкой*, и защищает ключ от расшифровки. В TPM имеется главный «связывающий» ключ, который называется корневым ключом хранилища (Storage Root Key, SRK). Ключ SRK хранится внутри TPM, чтобы гарантировать безопасность закрытой части ключа.

Компьютеры с установленным модулем TPM способны создавать ключ, который можно не только скрыть, но и запечатать. Процесс запечатывания ключа гарантирует его связь с определенными параметрами платформы. Ключ можно раскрыть лишь при условии, что параметры платформы имеют те же значения, что были у них в момент создания ключа. Именно это обеспечивает компьютерам, оборудованным TPM, повышенную устойчивость к атакам.

Поскольку TPM хранит закрытые части ключей отдельно от памяти, контролируемой ОС, ключи можно закрыть в TPM, обеспечив абсолютную уверенность в надежности системы. Ключи TPM распечатываются только при условии, что целостность системы не нарушена. Кроме того, технология

TPM использует собственные внутренние микропрограммы и логические схемы обработки команд и потому не зависит от ОС и не подвержена уязвимостям внешнего ПО.

TPM может также применяться для запечатывания и распечатывания данных, созданных вне TPM. Собственно, именно в этом и заключается основное преимущество TPM. В Windows 7 для осуществления доступа к TPM и для запечатывания компьютера используется технология шифрования диска BitLocker. Она может применяться в конфигурациях как с TPM, так и без TPM, но самый безопасный вариант — это, все же, использование TPM.

Если вы используете BitLocker и TPM для запечатывания диспетчера загрузки и загрузочных файлов компьютера, распечатать их можно будет только при условии, что они не изменялись с момента последнего запечатывания. Это означает, что вы можете использовать TPM для проверки загрузочных файлов в предоперационной среде. Если вы запечатали жесткий диск с использованием TPM, распечатать его можно будет только при условии, что данные на нем остались неизменными с момента последнего запечатывания. Это гарантирует, что на диск не осуществлялось внешних воздействий, пока ОС была отключена.

Если вы используете технологию BitLocker, но не запечатываете диспетчер загрузки и загрузочные файлы компьютера при помощи TPM, то TPM нельзя использовать для проверки загрузочных файлов компьютера в предоперационной системной среде. В этом случае нельзя гарантировать целостность диспетчера загрузки и загрузочных файлов компьютера.

Запуск и использование TPM

Архитектура служб TPM в Windows 7 обеспечивает выполнение основных функций, необходимых для настройки и развертывания компьютеров, оснащенных TPM. Эта архитектура может быть расширена за счет возможностей шифрования диска BitLocker, речь о которых пойдет далее.

Прежде чем начать использовать TPM, вы должны включить эту функцию в микропрограмме и инициализировать TPM для первого использования. В рамках инициализации вы задаете пароль владельца TPM. После запуска модуля TPM можно управлять его конфигурацией.

Иногда компьютеры, оборудованные TPM-модулем, загружаются с уже включенным TPM. Тем не менее, в большинстве случаев по умолчанию TPM не подключен. На моих компьютерах мне пришлось выполнить следующие действия:

1. Запустите компьютер и в процессе запуска нажмите клавишу F2, чтобы получить доступ к интерфейсу микропрограммы. В системе настройки перейдите к экрану **Advanced**, а затем к экрану **Peripheral Configuration**.
2. На экране **Peripheral Configuration** доверенный платформенный модуль представлен как возможный вариант. Выделите его и нажмите Enter, чтобы вывести меню. В нем выберите команду **Enable** и снова нажмите Enter.

3. Чтобы сохранить изменения настроек и выйти из микропрограммы, нажмите клавишу F10. В окне с просьбой подтвердить выход, нажмите клавишу Y. После этого происходит перезагрузка компьютера.

В Windows 7 есть несколько инструментов для работы с TPM, в том числе:

- **Управление доверенным платформенным модулем (TPM) (Trusted Platform Module Management)** Консоль конфигурации и управления TPM. Чтобы получить доступ к этой консоли, щелкните кнопку **Пуск (Start)**, введите **tpm.msc** в поле поиска и нажмите клавишу Enter.
- **Инициализация TPM (Initialize the TPM Security Hardware)** Мастер создания пароля владельца TPM. Чтобы запустить его, щелкните кнопку **Пуск (Start)**, введите **tpminit** в поле поиска и нажмите Enter.

Ближе к реальности Доступ к консоли управления TPM можно ограничить при помощи групповой политики. Если вам не удается открыть консоль, убедитесь, что в обрабатываемом объекте групповой политики не включены ограничения консолей MMC. Посмотрите узел **Компоненты Windows\Консоль управления (MMC) (Windows Components\Microsoft Management Console)**.

В консоли управления TPM можно определить текущее состояние TPM. Если вы попытаетесь запустить эту консоль, не включив TPM, то получите сообщение об ошибке. Это же произойдет, если вы попытаетесь запустить мастер инициализации TPM, не включив TPM.

Чтобы получить доступ к TPM и работать с соответствующими инструментами, обязательно нужно включить TPM в микропрограмме. Работая с консолью управления TPM, показанной на рис. 11-1, обратите внимание на состояние TPM (см. табл. 11-1) и данные о его производителе. По данным о производителе TPM можно узнать, поддерживается ли в нем спецификация 1.2. Требуется поддержка версии 1.2 и выше.

Табл. 11-1. Индикаторы состояния TPM и их значение

Индикатор состояния	Значение
Владелец TPM отсутствует, TPM включен (The TPM is on and ownership has not been taken)	TPM включен в микропрограммных настройках, но еще не инициализирован
Владелец TPM существует, TPM включен (The TPM is on and ownership has been taken)	TPM включен в микропрограммных настройках и инициализирован
Владелец TPM отсутствует, TPM отключен (The TPM is off and ownership has not been taken)	TPM выключен в микропрограммных настройках и еще не инициализирован
Владелец TPM существует, TPM отключен (The TPM is off and ownership has been taken)	TPM инициализирован, но выключен в микропрограммных настройках

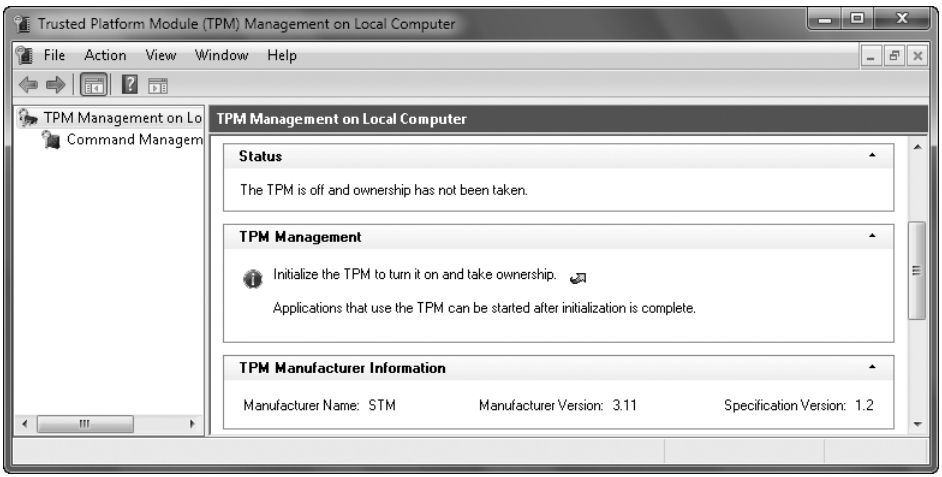

Рис. 11-1. Консоль для инициализации и управления TPM

Инициализация TPM при первом использовании

TPM настраивается в процессе инициализации, который состоит из включения TPM и последующей установки прав владельца TPM. Устанавливая права, вы задаете пароль, который позволяет осуществлять доступ к TPM и управлять им только авторизованному владельцу. Пароль TPM требуется, чтобы выключить TPM, если вы больше не хотите им пользоваться, и чтобы очистить TPM перед утилизацией компьютера. В домене Active Directory сохранение паролей TPM можно настроить при помощи групповой политики.

Для инициализации TPM и создания пароля владельца выполните следующие действия:

1. Откройте консоль управления TPM. В меню **Действие (Action)** выберите команду **Инициализировать TPM (Initialize TPM)**, чтобы запустить мастер инициализации TPM.

Внимание! Если мастер инициализации TPM обнаружит микропрограммы, не соответствующие требованиям к TPM в Windows, или не обнаружит TPM, вы не сможете продолжить работу. Проверьте, включен ли TPM в микропрограммных настройках.

Ближе к реальности Если ранее TPM был инициализирован и затем очищен, для переустановки TPM в микропрограммных настройках вам будет предложено перезапустить компьютер и следовать инструкциям, выводимым на экран в процессе запуска. Когда вы войдете в систему, мастер, теоретически, должен начать работу заново, но на моих системах этого не произошло. Когда я выбрал команду **Перезагрузка (Restart)**, компьютер перезагрузился, и мне пришлось самостоятельно входить в микропрограмму, нажав клавишу F2, и отключить TPM. Я сохранил изменения и вышел из микропрограммы. Произошла автоматическая перезагрузка, в ходе которой я снова вошел в микропрограммные настройки, нажав F2, запустил TPM, сохранил изменения и вышел из микропрограммы. Произошла автоматическая перезагрузка. После загрузки ОС я вошел под своим именем и перезапустил мастер инициализации TPM.

2. На странице **Создайте пароль владельца доверенного платформенного модуля (Create The TPM Owner Password)**, изображенной на рис. 11-2, щелкните команду **Автоматически создать пароль (Automatically Create The Password)**.

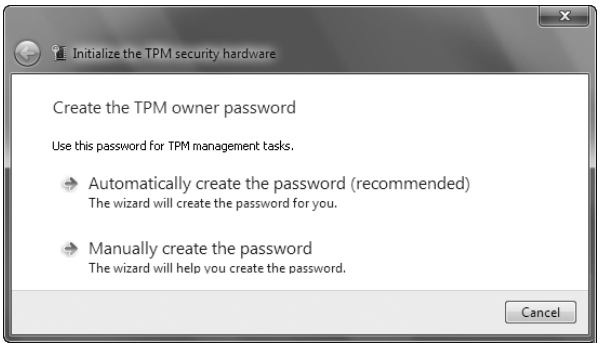

Рис. 11-2. Инициализация TPM

3. На странице **Сохраните свой пароль владельца доверенного платформенного модуля (Save Your TPM Owner Password)** вы увидите пароль владельца из 48 символов. Щелкните команду **Сохранить пароль (Save The Password)**.
4. В диалоговом окне **Сохранить как (Save As)** выберите место для сохранения резервной копии файла пароля и щелкните **Сохранить (Save)**. По умолчанию резервная копия файла пароля сохраняется с именем *Имя-Компьютера*.tpm. В идеале вы должны сохранить пароль владельца TPM на съемном носителе, например на флеш-накопителе.
5. На странице **Сохраните свой пароль владельца доверенного платформенного модуля (Save Your TPM Owner Password)** щелкните **Печатать пароль (Print The Password)**, если хотите иметь копию пароля в печатном виде. Убедитесь, что лист с паролем хранится в безопасном месте, например в сейфе или хотя бы в запираемом шкафу.
6. Щелкните **Инициализировать (Initialize)**. Процесс инициализации может занять несколько минут. После завершения инициализации щелкните **Закрыть (Close).** В консоли управления TPM должно измениться значение состояния.

Включение и выключение TPM после инициализации

Если вы решили не пользоваться TPM, вам придется выключить и очистить TPM. Отключить и очистить TPM нужно также, если вы хотите произвести реконфигурацию компьютера или утилизировать его.

Для выключения TPM выполните следующие действия:

1. Запустите консоль управления TPM. В области **Действие (Action)** выберите команду **Выключить доверенный платформенный модуль (Turn TPM Off)**. Будет запущен мастер управления TPM.

2. На странице **Выключите оборудование безопасности для доверенного платформенного модуля (Turn Off The TPM Security Hardware)**, изображенной на рис. 11-3, введите текущий пароль одним из указанных способов:
   - Если пароль владельца TPM сохранен на съемном носителе, вставьте его и выберите вариант **Имеется архивный файл с паролем владельца TPM (I Have The Owner Password File)**. На странице **Выберите файл резервной копии с паролем владельца доверенного платформенного модуля (Select Backup File With The TPM Owner Password)** выберите команду **Обзор (Browse)** и найдите в диалоговом окне **Открыть (Open)** файл с расширением .tpm, сохраненный на съемном носителе. Выберите команду **Открыть (Open)** и **Выключить доверенный платформенный модуль (Turn TPM Off)**.
   - Если у вас нет съемного носителя с паролем, выберите команду **Ввести вручную пароль владельца TPM (I Want To Enter The Owner Password)**. На странице **Введите свой пароль владельца доверенного платформенного модуля (Type Your TPM Owner Password)** введите пароль TPM и выберите **Выключить доверенный платформенный модуль (Turn TPM Off)**.
   - Если вы не знаете пароля владельца TPM, выберите команду **Нет пароля владельца TPM (I Do Not Have The TPM Owner Password)** и следуйте инструкциям для отключения TPM без введения пароля. Вы сможете отключить TPM, если локально вошли в компьютер под своим именем.
3. В консоли должен отобразиться новый статус TPM. Не удаляйте файл с паролем владельца TPM и не выбрасывайте распечатку. Эта информация потребуется, если вы захотите снова включить TPM.

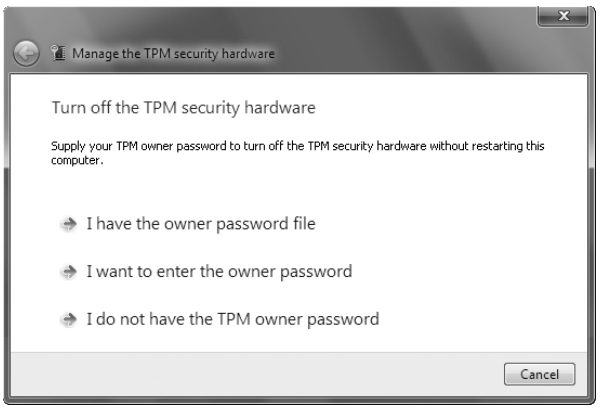

Рис. 11-3. Выберите способ отключения TPM

Выполнив описанную процедуру для программного отключения TPM, вы вольны снова программно включить TPM, выполнив следующие действия:

1. Запустите консоль управления TPM. В области **Действие (Action)** выберите команду **Включить TPM (Turn TPM On)**. Будет запущен мастер управления TPM.
2. На странице **Включите оборудование безопасности для доверенного платформенного модуля (Turn On The TPM Hardware)** введите текущий пароль одним из указанных способов:
   - Если пароль владельца TPM сохранен на съемном носителе, вставьте его и выберите вариант **Имеется архивный файл с паролем владельца TPM (I Have The Owner Password File)**. На странице **Выберите файл резервной копии с паролем владельца доверенного платформенного модуля (Select Backup File With The TPM Owner Password)** выберите команду **Обзор (Browse)** и найдите в диалоговом окне **Открыть (Open)** файл с расширением .tpm, сохраненный на съемном носителе. Выберите команду **Открыть (Open)** и **Включить доверенный платформенный модуль (Turn TPM On)**.
   - Если у вас нет съемного носителя с паролем, выберите команду **Ввести вручную пароль владельца TPM (I Want To Enter The Owner Password)**. На странице **Введите свой пароль владельца доверенного платформенного модуля (Type Your TPM Owner Password)** введите пароль TPM и выберите **Включить доверенный платформенный модуль (Turn TPM On)**.
   - Если вы не знаете пароля владельца TPM, выберите команду **Нет пароля владельца TPM (I Do Not Have The TPM Owner Password)** и следуйте инструкциям для включения TPM без введения пароля. Вы сможете включить TPM, если локально вошли в компьютер под своим именем.
3. В консоли должен отобразиться новый статус TPM. Не удаляйте файл с паролем владельца TPM и не выбрасывайте распечатку. Эта информация потребуется для последующего управления TPM.

Очистка TPM

При очистке TPM права владельца TPM аннулируются, и окончательно подтверждается закрытие TPM. Очищать TPM следует только при условии, что вы собираетесь выбрасывать компьютер.

Чтобы очистить TPM, выполните следующие действия:

1. Запустите консоль управления TPM. В области **Действие (Action)** выберите команду **Очистить доверенный платформенный модуль (Clear TPM)**. Произойдет запуск мастера управления TPM.

Внимание! При очистке TPM происходит возврат к заводским установкам и окончательное закрытие TPM. Вы теряете все ключи и данные, защищенные этими ключами.

2. На странице **Очистить доверенный платформенный модуль (Clear The TPM Security Hardware)** выберите способ ввода пароля:

- Если пароль владельца TPM сохранен на съемном носителе, вставьте его и выберите вариант **Имеется архивный файл с паролем владельца TPM (I Have The Owner Password File)**. На странице **Выберите файл резервной копии с паролем владельца доверенного платформенного модуля (Select Backup File With The TPM Owner Password)** выберите команду **Обзор (Browse)** и найдите в диалоговом окне **Открыть (Open)** файл с расширением .tpm, сохраненный на съемном носителе. Выберите команду **Открыть (Open)** и **Очистить доверенный платформенный модуль (Clear TPM)**.
- Если у вас нет съемного носителя с паролем, выберите команду **Ввести вручную пароль владельца TPM (I Want To Enter The Owner Password)**. На странице **Введите свой пароль владельца доверенного платформенного модуля (Type Your TPM Owner Password)** введите пароль TPM и выберите **Очистить доверенный платформенный модуль (Clear TPM)**.
- Если вы не знаете пароля владельца TPM, выберите команду **Нет пароля владельца TPM (I Do Not Have The TPM Owner Password)** и следуйте инструкциям для очистки TPM без введения пароля. Вы сможете очистить TPM, если локально вошли в компьютер под своим именем.

Изменение пароля владельца TPM

Чтобы изменить пароль TPM, выполните следующие действия:

1. Запустите консоль управления TPM. В области **Действие (Action)** выберите команду **Изменить пароль владельца (Change Owner Password)**. Будет запущен мастер управления TPM.
2. На странице **Изменить пароль владельца TPM (Change TMP Owner Password)** выберите способ ввода текущего пароля:
   - Если пароль владельца TPM сохранен на съемном носителе, вставьте его и выберите вариант **Имеется архивный файл с паролем владельца TPM (I Have The Owner Password File)**. На странице **Выберите файл резервной копии с паролем владельца доверенного платформенного модуля (Select Backup File With The TPM Owner Password)** выберите команду **Обзор (Browse)** и найдите в диалоговом окне **Открыть (Open)** файл с расширением .tpm, сохраненный на съемном носителе. Выберите команду **Открыть (Open)** и **Создать новый пароль (Create New Password)**.
   - Если у вас нет съемного носителя с паролем, выберите команду **Ввести вручную пароль владельца TPM (I Want To Enter The Owner Password)**. На странице **Введите свой пароль владельца доверенного платформенного модуля (Type Your TPM Owner Password)** введите пароль TPM и выберите **Создать новый пароль (Create New Password)**.

3. На странице **Создайте пароль владельца доверенного платформенного модуля (Create The TPM Owner Password)** выберите команду **Автоматически создать пароль (Automatically Create The Password)**, после чего щелкните **Далее (Next)**.
4. На странице **Сохраните свой пароль владельца доверенного платформенного модуля (Save Your TPM Owner Password)** вы увидите пароль владельца из 48 символов. Щелкните команду **Сохранить пароль (Save The Password)**. В диалоговом окне **Сохранить как (Save As)** выберите место для сохранения резервной копии файла пароля и щелкните **Сохранить (Save)**. Если вы сохраняете файл с новым паролем в том же месте и под тем же именем, что и файл со старым паролем, щелкните кнопку **Да (Yes)** при появлении вопроса о замене.
5. На странице **Сохраните свой пароль владельца доверенного платформенного модуля (Save Your TPM Owner Password)** щелкните **Печатать пароль (Print The Password)**, если хотите иметь пароль на бумажном носителе. Убедитесь, что распечатка с паролем хранится в безопасном месте, например в сейфе или запирающемся шкафе.
6. Для завершения процесса щелкните команду **Изменить пароль (Change Password)**.

Технология шифрования диска BitLocker

Технологии шифрования диска BitLocker и BitLocker To Go часто называют одним словом — BitLocker, — но это самостоятельные, хотя и схожие компоненты, входящие в состав изданий Windows 7 Ultimate и Enterprise. Технология шифрования диска BitLocker призвана защитить данные на утерянных, украденных или ненадлежащим образом списанных компьютерах и заключается в шифровании всего тома. Технология BitLocker To Go создана для защиты данных на флеш-накопителях и заключается в шифровании виртуального тома. Иными словами, стандартная технология BitLocker шифрует целый том, скрывая его при помощи защищенного шифрования. При использовании технологии BitLocker To Go на флеш-накопителе создается виртуальный том, который шифруется при помощи ключа, сохраненного на накопителе.

Знакомство с технологией BitLocker

Если компьютер не защищен технологией BitLocker, у пользователя, получившего физический доступ к компьютеру, есть множество способов получить полный контроль над ним, а затем и воспользоваться данными на компьютере, даже если они зашифрованы при помощи EFS. Например, пользователь может воспользоваться загрузочным диском, чтобы загрузить компьютер и изменить пароль администратора. Пользователь также может установить другую ОС, а затем загрузить компьютер с ее помощью и разблокировать ранее установленную ОС.

Технология шифрования диска BitLocker полностью скрывает диски при помощи шифрования и тем самым предотвращает любой доступ к ним всех пользователей, за исключением авторизованных. Если неавторизованный пользователь попытается получить доступ к диску, зашифрованному при помощи BitLocker, шифрование не позволит ему просматривать данные или каким-либо образом изменять их. При этом значительно снижается риск того, что неавторизованный сотрудник получит доступ к конфиденциальным данным, пока компьютер выключен.

Внимание! Технология BitLocker снижает производительность диска. Она предназначена для использования в тех случаях, когда компьютер физически находится в небезопасном месте и требует дополнительной защиты.

Технологию BitLocker можно использовать в сочетании с TPM, чтобы гарантировать целостность диспетчера загрузки и загрузочных файлов в момент запуска компьютера и проверять, не было ли попыток доступа к жесткому диску компьютера, пока ОС была выключена. Технология BitLocker также позволяет сохранять в TPM размеры ключевых файлов ОС.

Каждый раз при запуске компьютера Windows проверяет загрузочные файлы, файлы ОС и все зашифрованные тома, чтобы убедиться, что они не изменялись, пока ОС была отключена. Если файлы изменились, Windows информирует пользователя и отказывает в выдаче ключа, необходимого для доступа к ОС. Затем компьютер переходит в режим восстановления, предлагая пользователю предоставить ключ восстановления для получения доступа к загрузочному тому. Режим восстановления используется также, если дисковое устройство, зашифрованное при помощи BitLocker, переносится в другую систему.

Технология BitLocker может использоваться как на компьютерах, оснащенных TPM, так и на компьютерах, не оснащенных им. Если на компьютере есть модуль TPM, технология BitLocker использует его для обеспечения повышенной защиты данных и подтверждения целостности загрузочных файлов. Совместная работа этих компонентов позволяет предотвратить неавторизованный доступ к данным. Если на компьютере нет TPM или версия TPM несовместима с Windows, шифрование диска BitLocker все равно можно использовать для шифрования целых томов, защищая их от несанкционированного доступа.

На компьютерах с совместимым и инициализированным модулем TPM технология BitLocker может использоваться в одном из следующих режимов:

- **Только TPM** В этом режиме для проверки используется только TPM. При запуске компьютера TPM проверяет загрузочные файлы, файлы ОС и любые зашифрованные тома. Поскольку пользователю не приходится предъявлять дополнительный ключ запуска, этот режим для пользователя прозрачен, и сам процесс входа пользователя в систему не меняется. Если TPM отсутствует или изменялась целостность файлов или томов, BitLocker вводит режим восстановления и запрашивает ключ восстановления или пароль для получения доступа к загрузочному тому.

- **TPM и PIN** В этом режиме для проверки используется как TPM, так и вводимый пользователем цифровой код. При запуске компьютера для проверки загрузочных файлов, файлов ОС и любых зашифрованных томов используется TPM. Когда на экране появится соответствующее приглашение, пользователь должен ввести персональный идентификационный номер (PIN). Если у пользователя нет PIN-кода или он не может его корректно ввести, вместо загрузки ОС BitLocker переводит компьютер в режим восстановления. Как и в предыдущем случае, BitLocker также вводит режим восстановления, если TPM отсутствует или была нарушена целостность загрузочных файлов или зашифрованных томов.
- **TPM и ключ запуска** В этом режиме для проверки используется как TPM, так и ключ. При запуске компьютера TPM используется для проверки загрузочных файлов, файлов ОС и любых зашифрованных томов. Чтобы войти в компьютер под своим именем, пользователь должен предоставить флеш-накопитель с ключом запуска. Если у пользователя нет ключа запуска или он не может его корректно предоставить, BitLocker вводит режим восстановления. Как и в предыдущих случаях, этот режим вводится также, если TPM отсутствует или была нарушена целостность загрузочных файлов или шифрованных томов.
- **TPM и сертификат смарт-карты** В этом режиме для подтверждения используется как TPM, так и сертификат смарт-карты. При запуске компьютера TPM используется для проверки загрузочных файлов, файлов ОС и любых зашифрованных томов. Чтобы войти в компьютер под своим именем, пользователь должен иметь смарт-карту с действительным сертификатом. Если у пользователя нет такой карты или он не может ее предоставить, система BitLocker вводит режим восстановления. Этот режим, как и в предыдущих случаях, также вводится, если TPM отсутствует или была изменена целостность загрузочных файлов или шифрованных томов.

На компьютерах, не оснащенных TPM или оснащенных несовместимым TPM, в технологии BitLocker используются режимы только с ключом запуска или только с сертификатом смарт-карты. Для режима только с ключом запуска требуется USB-накопитель, содержащий ключ. Перед включением компьютера пользователь вставляет в него USB-накопитель. Ключ, сохраненный на накопителе, разблокирует компьютер.

Ближе к реальности Не исключено, что в одном из последующих обновлений Windows 7 появится возможность шифровать USB-накопитель с ключом запуска при помощи технологии BitLocker. Тем не менее, исходная версия Windows 7 не позволяет этого сделать. Поэтому не запускайте BitLocker на флеш-накопителе с ключом запуска.

Для режима с использованием только сертификата смарт-карты требуется карта с действительным сертификатом. Пользователь предъявляет карту-сертификат после включения компьютера, и сертификат разблокирует компьютер.

С момента внедрения технологии BitLocker в Windows Vista в нее были внесены некоторые изменения. На сегодняшний день в Windows 7 можно делать следующее:

- **Шифровать как тома FAT, так и тома NTFS** Раньше можно было шифровать только тома NTFS. Когда вы шифруете тома FAT, можете уточнить, каким образом следует разблокировать и просматривать зашифрованные тома на компьютерах, оснащенных Windows Vista, Windows XP или Windows Server 2008. Этот параметр настраивается через групповые политики и начинает работать, когда вы включаете BitLocker. В узле **Компоненты Windows\Шифрование диска BitLocker (Windows Components\BitLocker Drive Encryption)** административных шаблонов конфигурации компьютера предусмотрены отдельные правила для более ранних версий Windows, которые позволяют разблокировать и просматривать жесткие и съемные носители, форматированные в FAT.
- **Использовать агент восстановления данных совместно с BitLocker** Этот параметр также конфигурируется через групповую политику. Агент восстановления данных позволяет разблокировать и восстановить зашифрованный том при помощи персонального сертификата агента восстановления или 48-символьного пароля восстановления. При желании вы вольны сохранить данные о восстановлении в Active Directory. В административных шаблонах конфигурации компьютера имеются отдельные правила для томов ОС и других внутренних и съемных носителей.
- **Запретить запись информации на съемные носители, не защищенные BitLocker** Этот параметр также настраивается через групповую политику. Если вы включите этот параметр, доступ к незашифрованным съемным носителям у пользователей будут только для чтения. Чтение и запись можно будет проводить только на зашифрованных съемных носителях.

В домене агентами восстановления данных по умолчанию являются администраторы домена. В рабочих и домашних группах агента восстановления данных по умолчанию нет, но вы вольны его назначить. Пользователю, которого вы хотите назначить агентом восстановления данных, потребуется персональный сертификат шифрования. Чтобы сгенерировать сертификат, воспользуйтесь утилитой Cipher. Затем используйте сертификат для назначения агента восстановления данных в локальной политике безопасности, в узле **Политики открытого ключа\Шифрование диска BitLocker (Public Key Policies\BitLocker Drive Encryption)**.

Развертывание BitLocker

Применение на предприятии технологии BitLocker изменяет процесс работы администраторов и пользователей с компьютерами. Для запуска ОС на компьютере, оснащенном BitLocker, требуется вмешательство пользователя — он должен ввести PIN-код, вставить USB-накопитель с ключом запуска или использовать смарт-карту с сертификатом. После развертывания

шифрования диска BitLocker вы уже не можете быть уверены, что сможете осуществлять удаленное администрирование — ведь для него требуется перезагрузка компьютера в отсутствие физического доступа к компьютеру. Вам, возможно, потребуется помощь пользователя, который сможет ввести PIN-код, вставить USB-накопитель или использовать смарт-карту с действительным сертификатом.

Прежде чем начать использование шифрования диска BitLocker, необходимо провести тщательную оценку компьютерной базы организации и разработать планы мероприятий по следующим направлениям:

- оценить различные методы проверки подлинности в BitLocker и их применимость;
- определить, поддерживают ли компьютеры TPM, а затем определить, какие конфигурации BitLocker — с использованием TPM или без нее — вы будете использовать;
- разработать процедуру сохранения, применения и периодического изменения ключей шифрования, паролей и других механизмов проверки подлинности, используемых при работе с BitLocker.

Также необходимо продумать следующие аспекты:

- практика повседневных операций с носителями информации, зашифрованными при помощи BitLocker;
- обеспечение административной поддержки для носителей информации, зашифрованных при помощи BitLocker;
- восстановление работоспособности компьютеров, носители информации на которых зашифрованы средствами BitLocker.

Планируя эти процедуры, учитывайте особенности шифрования BitLocker и необходимость всегда иметь под рукой PIN-коды, ключи запуска, смарт-карты и ключи восстановления каждый раз, когда вам нужно иметь дело с компьютерами, зашифрованными при помощи BitLocker. Оценив компьютерную базу организации и разработав основные планы и процедуры, разработайте план внедрения шифрования диска BitLocker.

К вашим услугам несколько вариантов шифрования BitLocker: первоначальная версия, вышедшая вместе с Windows Vista, обновленная версия, вышедшая с Windows Server, и версия, выпущенная с Windows 7. Компьютеры по управлением Windows 7, Windows Server 2008 R2 и более поздних версий Windows способны работать с любой из этих версий. Кроме того, вполне возможно, что прежние версии Windows не смогут работать с самой последней версией BitLocker. Например, не исключено, что для открытия доступа к BitLocker из прежних версий Windows вам придется настроить групповую политику.

Для включения шифрования BitLocker на диске, содержащем ОС Windows, на этом диске должно быть, по крайней мере, два раздела:

- **Раздел для BitLocker** Это активный раздел, который содержит файлы, требуемые для запуска ОС. Он не шифруется.

- **Основной раздел для ОС и данных** Этот раздел шифруется, когда вы включаете BitLocker.

При внедрении BitLocker на системе, предшествующей Windows 7, для обеспечения совместимости вам придется определенным способом создать разделы. В Windows 7 этот недостаток уже устранен. Дополнительный раздел создается автоматически во время установки Windows 7. По умолчанию этот дополнительный раздел используется средой восстановления Windows (Windows RE). Однако, если вы включаете BitLocker на системном томе, Windows, как правило, переключает Windows RE на системный том, а затем использует дополнительный раздел для BitLocker.

Использование BitLocker на жестком диске не представляет трудностей. На компьютерах, оснащенных TPM, вы должны сначала инициализировать TPM, как описано ранее в разделе «Инициализация TPM при первом использовании», а затем запустить BitLocker. На компьютере без TPM достаточно запустить BitLocker на жестком диске.

Для управления конфигурацией TPM и BitLocker вы можете использовать локальную групповую политику и групповую политику на базе Active Directory. Настройки групповой политики для служб TPM расположены в административных шаблонах для конфигурации компьютера, в узле **Система\Службы доверенного платформенного модуля (System\Trusted Platform Module Services)**. Настройки групповой политики для BitLocker находятся в узле **Компоненты Windows\Шифрование диска BitLocker (Windows Components\BitLocker Drive Encryption)**. Имеются отдельные подпапки для жестких дисков, дисков ОС и съемных носителей.

Политики, на которые вам следует обратить внимание, таковы:

- Службы доверенного платформенного модуля (Trusted Platform Module Services):
  - Включить резервное копирование TPM в доменные службы Active Directory (Turn On TPM Backup To Active Directory Domain Services).
  - Настроить список заблокированных команд TPM (Configure The List Of Blocked TPM Commands).
  - Игнорировать список заблокированных команд TPM по умолчанию (Ignore The Default List Of Blocked TPM Commands).
  - Игнорировать локальный список заблокированных команд TPM (Ignore The Local List Of Blocked TPM Commands).
- Шифрование диска BitLocker (BitLocker Drive Encryption):
  - Выберите папку по умолчанию для пароля восстановления (Choose Default Folder For Recovery Password).
  - Выберите метод шифрования и стойкость шифра (Choose Drive Encryption Method And Cipher Strength).
  - Запретить перезапись памяти при перезагрузке (Prevent Memory Overwrite On Restart).

- Укажите уникальные идентификаторы для организации (Provide The Unique Identifiers For Your Organization).
- Проверить согласованность правил использования сертификатов смарт-карт (Validate Smart Card Certificate Usage Rule Compliance).

- Жесткие диски с данными (Fixed Drive):
  - Настроить использование смарт-карт на фиксированных дисках с данными (Configure Use Of Smart Cards On Fixed Data Drives).
  - Запретить запись на фиксированные диски, не защищенные BitLocker (Deny Write Access To Fixed Drives Not Protected By BitLocker).
  - Разрешить доступ к фиксированным дискам с данными, защищенными с помощью BitLocker, из более ранних версий Windows (Allow Access To BitLocker-Protected Fixed Data Drives From Earlier Versions Of Windows).
  - Настроить использование паролей для фиксированных дисков с данными (Configure Use Of Passwords For Fixed Data Drives).
  - Выбор методов восстановления жестких дисков, защищенных с помощью BitLocker (Choose How BitLocker-Protected Fixed Drives Can Be Recovered).
- Диски операционной системы (Operating System Drive):
  - Обязательная дополнительная проверка подлинности при запуске (Require Additional Authentication At Startup).
  - Разрешить использование улучшенных ПИН-кодов при запуске компьютера (Allow Enhanced PINs For Startup).
  - Установить минимальную длину ПИН-кода для запуска (Configure Minimum PIN Length For Startup).
  - Выбор методов восстановления дисков операционной системы, защищенных с помощью BitLocker (Choose How BitLocker-Protected Operating System Drives Can Be Recovered).
  - Настройка профиля проверки платформы TPM (Configure TPM Platform Validation Profile).
- Съемные диски с данными (Removable Data Drive):
  - Разрешить доступ к съемным дискам с данными, защищенными с помощью BitLocker, из более ранних версий Windows (Allow Access To BitLocker-Protected Removable Data Drives From Earlier Versions Of Windows).
  - Выбор методов восстановления съемных дисков, защищенных с помощью BitLocker (Choose How BitLocker-Protected Removable Drives Can Be Recovered).
  - Настроить использование паролей для съемных дисков с данными (Configure Use Of Passwords For Removable Data Drives).
  - Настроить использование смарт-карт для съемных дисков с данными (Configure Use Of Smart Cards On Removable Data Drives).

- Управление использованием BitLocker для съемных дисков (Control Use Of BitLocker On Removable Drives).
- Запретить запись на съемные диски, не защищенные BitLocker (Deny Write Access To Removable Drives Not Protected By BitLocker).

В Active Directory для объектов-компьютеров включены расширения восстановления для TPM и BitLocker. Для TPM в этих расширениях определено единственное свойство объекта-компьютера с именем ms-TPM-OwnerInformation. При инициализации TPM или изменении пароля владельца хеш пароля владельца TPM можно сохранить как значение атрибута ms-TPM-OwnerInformation соответствующего объекта-компьютера. Для BitLocker в этих расширениях определены объекты Recovery — дочерние объекты объекта-компьютера. Они используются для сохранения паролей восстановления и их связывания с конкретными томами, зашифрованными при помощи BitLocker.

Чтобы убедиться, что в вашем распоряжении есть вся информация TPM и BitLocker, необходимая для восстановления, настройте групповую политику для сохранения этой информации в Active Directory.

- Включите политику **Включить резервное копирование TPM в доменные службы Active Directory (Turn On TPM Backup To Active Directory Domain Services)** и установите флажок **Требовать резервного копирования TPM в AD DS (Require TPM Backup To AD DS)**.
- Включите политику **Выбор методов восстановления жестких дисков, защищенных с помощью BitLocker (Choose How BitLocker-Protected Fixed Drives Can Be Recovered)** и примите параметры по умолчанию, чтобы допустить работу агентов восстановления данных и сохранить информацию о восстановлении в Active Directory.
- Включите политику **Выбор методов восстановления дисков операционной системы, защищенных с помощью BitLocker (Choose How BitLocker-Protected Operating System Drives Can Be Recovered)** и примите параметры по умолчанию, чтобы допустить работу агентов восстановления данных и сохранить информацию о восстановлении в Active Directory.

Ближе к реальности Согласно требованиям стандарта FIPS (Federal Information Processing Standard), вы не можете создавать или сохранять пароли восстановления BitLocker. В этом случае вам необходимо настроить создание ключей восстановления в Windows. Параметры FIPS размещены в политике безопасности **Локальные политики\Параметры безопасности\Системная криптография: использовать FIPS-совместимые алгоритмы для шифрования, хеширования и подписывания (Local Policies\Security Options\System Cryptography: Use FIPS Compliant Algorithms For Encryption, Hashing, And Signing)**.

Чтобы настроить BitLocker на использование ключей восстановления, включите политику безопасности **Системная криптография: использовать FIPS-совместимые алгоритмы для шифрования, хеширования и подписывания (System Cryptography: Use FIPS Compliant Algorithms For Encryption, Hashing, And Signing)** в локальной групповой политике или в групповой политике Active Directory. Теперь пользователи смогут генерировать ключи восстановления.

Управление шифрованием диска BitLocker

В Windows 7 можно конфигурировать и запускать шифрование диска BitLocker как на системных томах, так и на томах данных. Если вы зашифруете системный том, в процессе загрузки вы должны будете разблокировать ПК, используя TPM, ключ запуска, PIN-код или какую-либо комбинацию трех этих элементов. Чтобы обеспечить максимально высокий уровень защиты, используйте все три способа проверки подлинности.

В текущей реализации BitLocker не требуется шифровать системный том компьютера перед шифрованием томов данных. Когда вы используете зашифрованные тома данных, ОС подключает тома BitLocker точно так же, как и любые другие тома. Но для доступа к ним требуется либо пароль, либо смарт-карта с действительным сертификатом.

Ключ шифрования для защищенного тома данных создается и хранится независимо от системного тома и любых других защищенных томов. Чтобы ОС могла подключать шифрованные тома, ключевая цепочка, защищающая том данных, сохраняется в шифрованном виде на томе ОС. Если операционная система входит в режим восстановления, разблокировать тома данных не удастся, пока ОС не выйдет из режима восстановления.

Для настройки шифрования диска BitLocker выполните следующие действия:

1. Разбейте жесткие диски компьютера на разделы и установите ОС (если настраиваете новый компьютер). Программа установки Windows разделит диски автоматически. Помните, что том, на котором сохранены данные BitLocker, должен быть активным системным томом.
2. Инициализируйте и настройте TPM (если будете ее использовать).
3. Включите функцию шифрование диска BitLocker (если будете ее использовать).
4. Проверьте в микропрограмме, что загрузка компьютера будет начинаться с диска, содержащего активный системный раздел, а не с носителя USB или дисков CD/DVD (это нужно, только если вы шифруете системные тома).
5. Настройте шифрование диска BitLocker.

Включив и настроив шифрование BitLocker, вы можете воспользоваться несколькими методами для его обслуживания и выполнения восстановления.

Подготовка к использованию шифрования диска BitLocker

Как уже говорилось, технологию BitLocker можно использоваться как в сочетании с TPM, так и без TPM. В обеих конфигурациях перед включением и настройкой BitLocker требуется определенная подготовка.

В Windows 7 Ultimate и Windows 7 Enterprise технология BitLocker устанавливается по умолчанию. Если этого не происходит, установите функцию

шифрования диска BitLocker, используя мастер Добавление компонентов (Add Features). Для завершения процесса установки нужно перезагрузить компьютер.

Чтобы определить готовность компьютера, откройте консоль **Шифрование диска BitLocker (BitLocker Drive Encryption)**. Щелкните команду **Пуск (Start)** и выберите команду **Панель управления (Control Panel)**. В окне панели управления выберите категорию **Система и безопасность (System And Security)** и щелкните ссылку **Шифрование диска BitLocker (BitLocker Drive Encryption)**. Если система не настроена должным образом, вы увидите сообщение об ошибке. Обратите внимание на следующее:

- Если в сообщении говорится об ошибке, связанной с TPM, и ваш компьютер оборудован совместимой TPM, прочитайте раздел «Запуск и использование TPM» этой главы, чтобы узнать о состояниях TPM и запуске TPM в микропрограмме.
- Если в сообщении говорится об ошибке, связанной с TPM, и на вашем компьютере нет совместимой TPM, измените настройки групповой политики компьютера так, чтобы шифрование диска BitLocker можно было включать без TPM.

Настройка параметров BitLocker осуществляется в локальной групповой политике или в групповой политике Active Directory. В локальной политике настройки применяются к объекту локальной политике компьютера. В домене настраивать нужно политики объекта GPO, применяемого к компьютеру. В процессе настройки доменной политики вы также можете уточнить требования для компьютеров с TPM.

Для настройки использования BitLocker с технологией TPM или без нее, выполните следующие действия:

1. Откройте соответствующий объект GPO для редактирования в редакторе управления групповой политикой.
2. В административных шаблонах конфигурации компьютера разверните узел **Компоненты Windows\Шифрование диска BitLocker\Диски операционной системы (Windows Components\BitLocker Drive Encryption\Operating System Drives)** и щелкните дважды политику **Обязательная дополнительная проверка подлинности при запуске (Require Additional Authentication At Startup)**.
3. В диалоговом окне **Обязательная дополнительная проверка подлинности при запуске (Require Additional Authentication At Startup),** показанном на рис. 11-4, включите политику, установив переключатель **Включить (Enabled)**.

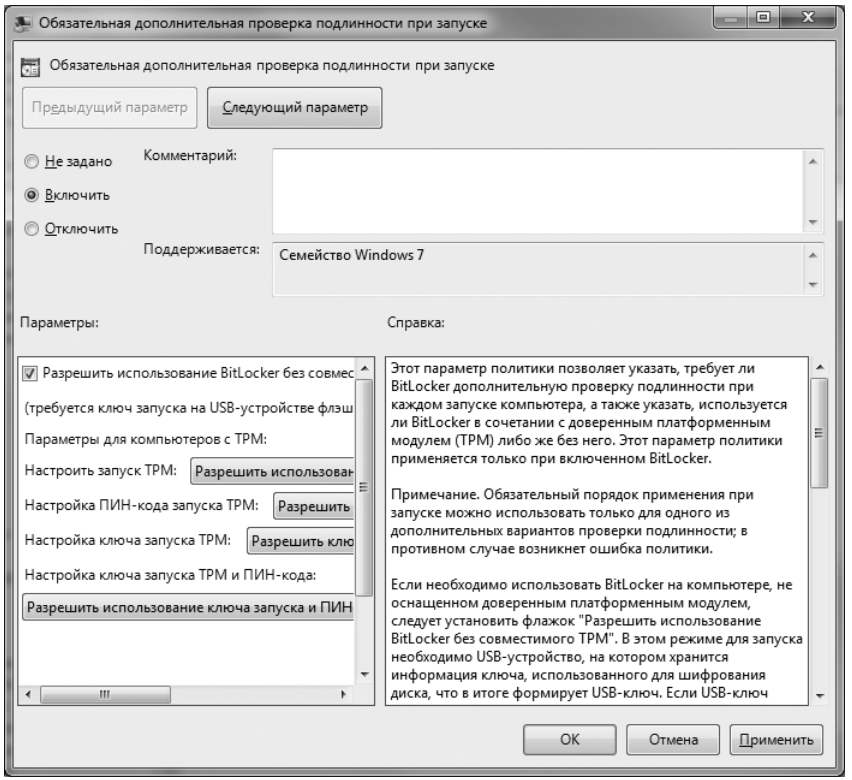

Рис. 11-4. Задайте отключение TPM

4. Выполните одно из следующих действий:
   - Чтобы использовать BitLocker без совместимого TPM, установите флажок **Разрешить использование BitLocker без совместимого TPM (Allow BitLocker Without A Compatible TPM)**. После этого вы сможете использовать шифрование BitLocker с ключом запуска на компьютере без TPM.
   - Чтобы использовать BitLocker с TPM, сбросьте флажок **Разрешить использование BitLocker без совместимого TPM (Allow BitLocker Without A Compatible TPM)**. После этого вы сможете использовать шифрование BitLocker на компьютере с TPM, используя PIN, ключ запуска или оба этих элемента.
5. На компьютере с совместимым TPM для повышенной защиты шифрованных данных при загрузке используются четыре типа проверки подлинности, которые могут быть допустимыми или обязательными. Табл. 11-2 поможет вам настроить использование TPM с имеющимися методами проверки подлинности.

Табл. 11-2. Типичные способы использования TPM с BitLocker

	Настройки			
При запуске компьютера	**Конфигурировать запуск TPM**	**Конфигурировать запуск TPM с PIN-кодом**	**Конфигурировать TPM с ключом запуска**	**Конфигурировать TPM с ключом запуска и PIN-кодом**
Разрешить использование TPM при запуске	Разрешить TPM	Не разрешать	Не разрешать	Не разрешать
Требовать использования TPM при запуске	Требовать TPM	Не разрешать	Не разрешать	Не разрешать
Использовать только TPM с ключом запуска	Разрешать или требовать TPM	Разрешать или требовать загрузочный PIN-код с TPM	Не разрешать	Не разрешать
Использовать только TPM с загрузочным PIN-кодом	Разрешать или требовать TPM	Не разрешать	Разрешать или требовать ключ запуска с TPM	Не разрешать
Использовать только TPM с ключом запуска и PIN-кодом	Разрешать или требовать TPM	Не разрешать	Не разрешать	Разрешать или требовать ключ запуска и PIN-код с TPM
Разрешить TPM с любым другим методом проверки подлинности	Разрешать или требовать TPM	Разрешать загрузочный PIN-код с TPM	Разрешать ключ запуска с TPM	Разрешать ключ запуска и PIN-код с TPM

6. Щелкните OK, чтобы сохранить изменения. Политика вступит в действие, когда вы в следующий раз обновите групповую политику.
7. Закройте редактор управления групповой политикой. Чтобы немедленно применить групповую политику к компьютеру, на который вы вошли под своим именем, щелкните кнопку **Пуск (Start)**, введите **gpupdate.exe /force** в поле поиска и нажмите Enter.

У компьютеров с ключом запуска или загрузочным PIN-кодом также имеется пароль или сертификат восстановления. Они требуются в следующих случаях:

- были внесены изменения в загрузочную информацию системы;
- зашифрованный носитель нужно перенести на другой компьютер;

- пользователь не может предоставить соответствующий ключ запуска или PIN-код.

Пароль или сертификат восстановления должны управляться и храниться отдельно от ключа запуска или PIN-кода. Доступ к ним должен быть только у администратора. Пароль или сертификат восстановления нужны администратору, чтобы разблокировать зашифрованные данные на томе, если BitLocker войдет в заблокированное состояние. В целом, если вы не используете общий агент восстановления данных, для каждого конкретного случая шифрования BitLocker пароль или сертификат восстановления уникальны. Это означает, что с его помощью вы не сможете восстановить зашифрованные данные из любого другого тома, зашифрованного при помощи BitLocker, даже на том же самом компьютере. Для большей безопасности храните ключи запуска и данные для восстановления отдельно от компьютера.

После установки BitLocker становится доступной консоль **Шифрование диска BitLocker (BitLocker Drive Encryption)**, входящая в состав панели управления. Параметры конфигурации BitLocker зависят от того, установлена ли на компьютере TPM, и от настроек групповой политики.

Запуск BitLocker на несистемных томах

Шифрование несистемного тома защищает данные, сохраненные на томе. Любой том, отформатированный в файловой системе FAT, FAT32 или NTFS, может быть зашифрован при помощи BitLocker. Длительность процесса шифрования носителя зависит от его объема, а также производительности и загруженности компьютера.

Прежде чем запустить BitLocker, настройте политики в узле **Жесткие диски с данными (Fixed Data Drive)** групповой политики, а затем дождитесь обновления групповой политики. Если этого не сделать и запустить BitLocker преждевременно, вам, возможно, придется отключить BitLocker, а затем снова подключить его, потому что при включении BitLocker устанавливаются флажки состояния и управления.

На компьютере с двумя ОС или при перемещении носителя с одного компьютера на другой включение политики **Разрешить доступ к фиксированным дискам с данными, защищенными с помощью BitLocker, из более ранних версий Windows (Allow Access To BitLocker-Protected Fixed Data Drives From Earlier Versions Of Windows)** гарантирует, что вы получите доступ к тому на других ОС и компьютерах. Разблокированные носители доступны только для чтения. Чтобы гарантировать возможность восстановления информации на зашифрованном томе, вы должны разрешить агентов восстановления данных и сохранить информацию о восстановлении в Active Directory.

Чтобы зашифровать несистемный том при помощи BitLocker, выполните следующие действия:

1. Щелкните кнопку **Пуск (Start)** и выберите команду **Компьютер (Computer)**. Правой кнопкой щелкните том данных и выберите команду **Включить BitLocker (Turn On BitLocker)**. Дождитесь окончания инициализации диска.

Внимание! Если BitLocker уже запущен, вместо команды **Включить BitLocker (Turn On BitLocker)** будет отображаться команда **Управление BitLocker (Manage BitLocker)**.

2. На странице **Выберите способы снятия блокировки диска (Choose How You Want To Unlock This Drive),** показанной на рис. 11-5, задайте один или несколько из перечисленных ниже параметров:
   - **Использовать пароль для снятия блокировки диска (Use A Password To Unlock The Drive)** Выберите этот параметр, если хотите, чтобы пользователь мог ввести пароль для разблокирования носителя. Пароль позволяет разблокировать носитель независимо от места его расположения, чтобы им могли пользоваться другие лица.
   - **Использовать смарт-карту для снятия блокировки диска (Use My Smart Card To Unlock The Drive)** Выберите этот параметр, если хотите, чтобы пользователь использовал для разблокирования носителя смарт-карту и вводил PIN-код. Поскольку для этой функции необходимо устройство для считывания смарт-карт**,** она обычно используется для разблокирования носителя на рабочем месте, а не для носителей, которые могут использоваться вне рабочего места.
   - **Автоматически снимать блокировку диска этого компьютера (Automatically Unlock This Drive On This Computer)** Установите этот флажок, чтобы разблокирование носителя происходило автоматически в момент запуска компьютера и загрузки ОС. Этот вариант доступен только после шифрования системного тома.

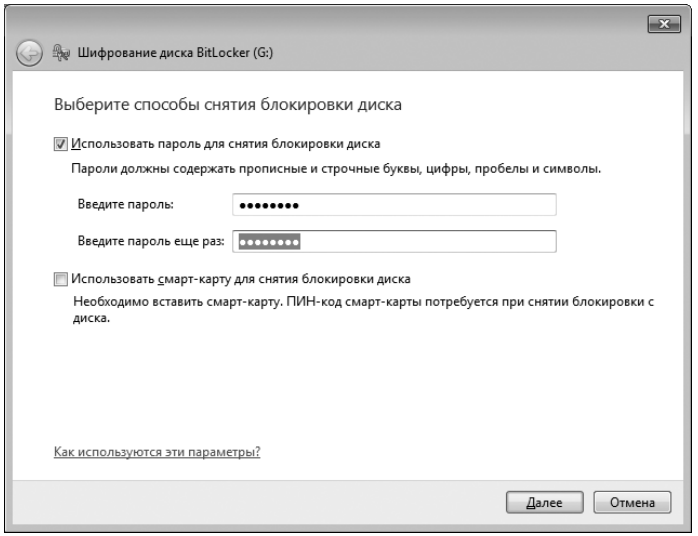

Рис. 11-5. Выберите способ разблокировки носителя

3. Щелкните **Далее (Next)**. На странице **Как сохранить ключ восстановления (How Do You Want To Store Your Recovery Key)** выберите команду **Сохранить ключ восстановления на флеш-накопителе USB (Save The Recovery Key To A USB Flash Drive)**.
4. В диалоговом окне **Сохранение ключа восстановления на USB-накопителе (Save a recovery key to a USB drive)** укажите размещение USB-носителя и выберите команду **Сохранить (Save)**. Не извлекайте USB-накопитель с ключом восстановления.
5. Теперь по своему выбору сохраните ключ восстановления в папку, распечатайте его или выберите оба варианта одновременно. Задайте нужные параметры и следуйте инструкциям мастера, чтобы выбрать место для сохранения или печати ключа восстановления. Закончив работу, щелкните **Далее (Next)**.
6. На странице **Зашифровать этот диск? (Are You Ready To Encrypt This Drive?)** щелкните кнопку **Начать шифрование (Start Encrypting)**. Длительность процесса шифрования зависит от объема носителя и других факторов.

Запуск BitLocker на USB-накопителе

Шифрование USB-накопителя защищает сохраненные на нем данные. Зашифровать при помощи технологии BitLocker можно любой флеш-накопитель, отформатированный в FAT, FAT32 или NTFS. Длительность шифрования носителя зависит его размера, производительности и загруженности компьютера.

Прежде чем запустить BitLocker, настройте политики в узле **Съемные диски с данными (Removable Data Drive)** групповой политики и дождитесь обновления групповой политики. Если этого не сделать и запустить BitLocker преждевременно, вам, возможно, придется отключить BitLocker, а затем снова его включить, поскольку при подключении BitLocker устанавливаются некоторые флажки состояния и управления.

Чтобы с гарантией иметь возможность восстановить зашифрованный том, разрешите агентов восстановления данных и сохраните информацию о восстановлении в Active Directory. Если будете использовать накопитель на компьютере с прежними версиями Windows, включение политики **Разрешить доступ к съемным дискам с данными, защищенными с помощью BitLocker, из более ранних версий Windows (Allow Access To BitLocker-Protected Removable Data Drives From Earlier Versions Of Windows)** обеспечит доступ к USB-накопителю на других ОС и компьютерах. Разблокированные носители доступны только для чтения.

Чтобы зашифровать USB-накопитель при помощи BitLocker, выполните следующие действия:

1. Вставьте USB-накопитель, щелкните кнопку **Пуск (Start)** и выберите команду **Компьютер (Computer)**.

2. Правой кнопкой мыши щелкните значок USB-накопителя и выберите команду **Включить BitLocker (Turn On BitLocker)**. BitLocker инициализирует носитель.
3. На странице **Выберите способы снятия блокировки диска (Choose How You Want To Unlock This Drive)** задайте один или несколько из следующих параметров:
   - **Использовать пароль для снятия блокировки диска (Use A Password To Unlock This Drive)** Установите этот флажок, если хотите, чтобы пользователь вводил пароль для разблокировки носителя. Пароль позволяет разблокировать носитель независимо от места его расположения.
   - **Использовать смарт-карту для снятия блокировки диска (Use My Smart Card To Unlock The Drive)** Выберите этот параметр, если хотите, чтобы для разблокирования носителя пользователь применял смарт-карту или вводил PIN-код. Поскольку для этой функции необходимо устройство для считывания смарт-карт, ее обычно применяют для разблокирования носителя на рабочем месте, а не для носителей, которые предполагается использоваться вне рабочего места.
4. Щелкните **Далее (Next)**. На странице **Как сохранить ключ восстановления (How Do You Want To Store Your Recovery Key)** щелкните команду **Сохранить ключ восстановления в файле (Save The Recovery Key To A File)**.
5. В диалоговом окне **Сохранить ключ восстановления BitLocker как (Save BitLocker Recovery Key As)** выберите место для сохранения ключа и затем выберите команду **Сохранить (Save)**.
6. При желании распечатайте ключ восстановления. Завершив печать, щелкните **Далее (Next)**.
7. На странице **Зашифровать этот диск? (Are You Ready To Encrypt This Drive)** щелкните кнопку **Начать шифрование (Start Encrypting)**. Не удаляйте USB-накопитель до полного завершения процесса шифрования. Длительность процесса зависит от объема носителя и других факторов.

   В процессе шифрования происходит следующее:

1. На USB-накопитель добавляется файл Autorun.inf, программа для чтения BitLocker To Go и файл Read Me.txt.
2. В оставшемся дисковом пространстве создается виртуальный том с полным содержимым носителя.
3. Виртуальный том шифруется. Полный процесс шифрования USB-накопителя занимает примерно от 6 до 10 минут на гигабайт. Процесс шифрования можно приостановить и возобновить при условии, что вы не удаляете носитель.

Когда вы вставляете носитель в компьютер с Windows 7 и включенным автозапуском, запускается программа для чтения BitLocker To Go, которая, в свою очередь, отображает диалоговое окно, показанное на рис. 11-6. Введите

пароль, PIN-код смарт-карты или выберите оба варианта, чтобы разблокировать носитель. Выберите параметр **В дальнейшем автоматически снимать блокировку с этого компьютера (Automatically Unlock On This Computer From Now On)**, чтобы сохранить пароль в зашифрованном файле на системном томе компьютера. Затем выберите команду **Разблокировать (Unlock)**, чтобы разблокировать том для дальнейшего использования.

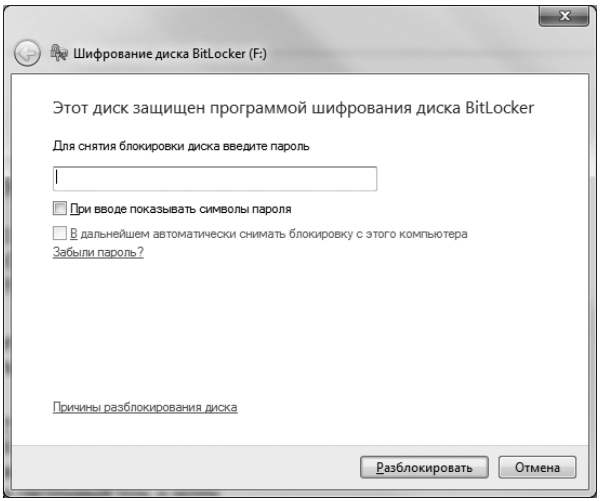

Рис. 11-6. Разблокирование зашифрованного носителя

Запуск BitLocker на системных томах

Прежде чем зашифровать системный том, следует удалить все загрузочные носители из CD/DVD-дисководов и из USB-разъемов. Затем запустите шифрование BitLocker на системном томе, выполнив следующие действия:

1. Щелкните кнопку **Пуск (Start)** и выберите команду **Компьютер (Computer)**. Правой кнопкой щелкните системный том и выберите команду **Включить BitLocker (Turn On BitLocker)**. Windows проверит, можно ли использовать технологию BitLocker с данным компьютером и носителем. Щелкните **Далее (Next)**.

Внимание! Если шифрование диска BitLocker уже запущено, вместо команды **Включить BitLocker (Turn On BitLocker)** будет отображаться команда **Управление BitLocker (Manage BitLocker)**.

2. На странице **Подготовка диска к шифрованию BitLocker (Preparing Your Drive For BitLocker)** щелкните **Сведения (Details)**, чтобы увидеть, как именно Windows будет готовить диск к шифрованию. Как правило, Windows использует для раздела BitLocker существующий диск или неразмеченное пространство на системном диске. Если в этом разделе находится Windows RE, Windows перемещает Windows RE на системный том, а затем использует дополнительный раздел для BitLocker.

3. Щелкните **Далее (Next)**, чтобы подготовить носитель для BitLocker. Когда процесс будет завершен, снова щелкните **Далее (Next)**.
4. Настройте параметры запуска BitLocker, как показано на рис. 11-7. Продолжение работы описано в следующих разделах.

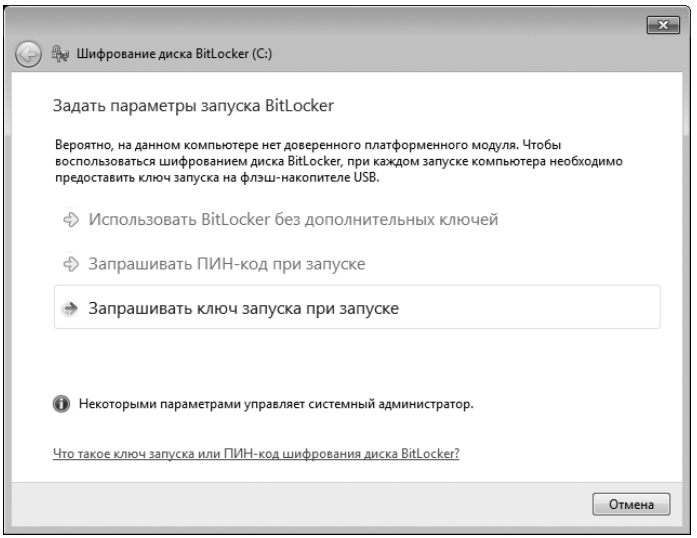

Рис. 11-7. Настройка параметров запуска BitLocker

Вы можете использовать BitLocker для обеспечения базовой защиты тома, без использования каких-либо дополнительных параметров. В этой конфигурации BitLocker защищает системный том посредством его шифрования, а также:

- открывает доступ к тому пользователям, которые могут войти в ОС со своими учетными данными;
- не позволяет злоумышленникам, получившим физический доступ к компьютеру, запустить его при помощи другой ОС, чтобы получить доступ к данным на томе;
- позволяет использовать компьютер как с технологией TPM, так и без нее;
- не требует ввода пароля или PIN-кода смарт-карты.

Чтобы использовать технологию BitLocker без дополнительных параметров, выполните следующие действия:

1. На странице **Задать параметры запуска BitLocker (Set BitLocker Startup Preferences)** выберите вариант **Использовать BitLocker без дополнительных ключей (Use BitLocker Without Additional Keys)**.
2. На странице **Как сохранить ключ восстановления? (How Do You Want To Store Your Recovery Key)** выберите вариант **Сохранить ключ восстановления на флеш-накопителе USB (Save The Recovery Key On A USB Flash Drive)**.

3. В диалоговом окне **Сохранение ключа восстановления на USB-накопителе (Save A Recovery Key To A USB Drive)** выберите USB-накопитель и щелкните кнопку **Сохранить (Save)**. Не используйте USB-накопитель, зашифрованный при помощи BitLocker.
4. По своему выбору сохраните ключ восстановления в папку, распечатайте или выберите оба варианта одновременно. Выберите нужный вариант и следуйте инструкциям мастера, чтобы выбрать место сохранения ключа или задать его печать. Затем щелкните **Далее (Next)**.
5. На странице **Зашифровать этот диск? (Encrypt The Drive)** щелкните кнопку **Начать шифрование (Start Encrypting)**. Длительность процесса шифрования зависит от размера носителя и других факторов.

Для большей безопасности используйте BitLocker с PIN-кодом или ключом запуска. Эта конфигурация:

- предоставляет доступ к тому только пользователям, которые предоставят действительный ключ;
- не дает злоумышленникам, получившим физический доступ к компьютеру, загружать его с альтернативной ОС, чтобы получить доступ к данным на томе;
- позволяет использовать компьютер как с TPM, так и без нее;
- требует пароля или смарт-карту с PIN-кодом.

Чтобы зашифровать том при помощи BitLocker с использованием ключа запуска, выполните следующие действия:

1. На странице **Задать параметры запуска BitLocker (Set BitLocker Startup Preferences)** выберите вариант **Запрашивать ключ запуска при запуске (Require A Startup Key At Every Startup)**.
2. Вставьте USB-накопитель в компьютер (если вы еще этого не сделали). Не используйте USB-накопитель, зашифрованный при помощи BitLocker.
3. На странице **Сохраните ключ запуска (Save Your Startup Key)** выберите USB-накопитель и щелкните кнопку **Сохранить (Save)**.
4. Сохраните ключ восстановления. Поскольку нельзя сохранять ключ восстановления и ключ запуска на одном и том же носителе, удалите USB-накопитель и вставьте другой.

Внимание! Ключ запуска отличается от ключа восстановления. Ключ запуска необходим для запуска компьютера. Ключ восстановления необходим, чтобы разблокировать компьютер, если BitLocker перейдет в режим восстановления. Это может произойти, если BitLocker заподозрит, что в компьютер осуществлялось вмешательство в то время, когда он находился в автономном режиме.

5. На странице **Как сохранить ключ восстановления? (How Do You Want To Store Your Recovery Key)** выберите команду **Сохранить ключ восстановления на флеш-накопителе USB (Save The Recovery Key To A USB Flash Drive)**.

6. В диалоговом окне **Сохранение ключа восстановления на USB-накопителе (Save A Recovery Key To A USB Drive)** найдите USB-накопитель и щелкните кнопку **Сохранить (Save)**. Не удаляйте USB-носитель с ключом восстановления.
7. По выбору сохраните ключ восстановления в папку, распечатайте ключ восстановления или выберите оба варианта одновременно. Выберите нужный параметр и выполните инструкции мастера, чтобы сохранить или распечатать ключ восстановления. Затем щелкните **Далее (Next)**.
8. На странице **Зашифровать этот диск? (Encrypt The Volume)** убедитесь, что установлен флажок **Запустить проверку системы BitLocker (Run BitLocker System Check)** и щелкните **Продолжить (Continue)**.
9. Подтвердите перезапуск компьютера, щелкнув **Перезагрузить сейчас (Restart Now)**. После перезапуска система убедится, что компьютер совместим с BitLocker и готов к шифрованию. Если компьютер не готов к шифрованию, вы увидите сообщение об ошибке. Прежде чем вы сможете закончить процедуру, ошибку придется устранить. Если компьютер готов к шифрованию, отображается строка состояния **Производится шифрование (Encryption In Progress)**. Чтобы отслеживать состояние шифрования тома, воспользуйтесь значком BitLocker в области сведений. Дважды щелкнув этот значок, вы откроете диалоговое окно **Шифрование (Encrypting)** и проследите за процессом шифрования более внимательно. Вы также можете приостановить процесс шифрования. На шифрование одного гигабайта тома требуется примерно одна минута.

Когда процедура закончена, том ОС зашифрован, и для него создан уникальный ключ восстановления. При следующем запуске компьютера USB-накопитель с ключом запуска должен быть вставлен в USB-порт компьютера. Если у вас нет USB-накопителя с ключом запуска, вам придется использовать режим восстановления, а затем предоставить ключ восстановления, чтобы получить доступ к данным.

Чтобы запустить шифрование BitLocker с использованием PIN-кода, выполните следующие действия:

1. На странице **Задать параметры запуска BitLocker (Set BitLocker Startup Preferences)** выберите вариант **Запрашивать ПИН-код при запуске (Require A PIN At Every Startup)**.
2. На странице **Введите ПИН-код (Type Your Startup PIN)** введите и подтвердите PIN-код — любое число длиной от 4 до 20 символов. Этот PIN-код хранится на вашем компьютере.
3. Вставьте USB-накопитель, на котором хотите сохранить ключ восстановления, а затем выберите **Задать ПИН-код (Set PIN)**. Не используйте USB-накопитель, зашифрованный при помощи технологии BitLocker.
4. Выполните шаги 5–9 предыдущей процедуры.

После завершения процесса шифрования том полностью зашифрован, и для него создан уникальный ключ восстановления. Если вы задали PIN-

код или ключ запуска, их придется использовать для запуска компьютера. Никаких других изменений в компьютере вы не заметите, пока не будет изменен TPM или пока не будет утрачен доступ к TPM, или кто-то попытается изменить диск при отключенной ОС. В этом случае компьютер войдет в режим восстановления, и вы должны будете ввести ключ восстановления, чтобы разблокировать компьютер.

Диагностика неисправностей BitLocker

Чтобы определить, используется ли на системном томе, томе данных или USB-накопителе технология BitLocker, щелкните кнопку **Пуск (Start)**, выберите команду **Панель управления (Control Panel)** и щелкните **Система и безопасность (System And Security)**. Дважды щелкните значок **Шифрование диска BitLocker (BitLocker Drive Encryption)**. Вы увидите состояние BitLocker для каждого тома, как показано на рис. 11-8.

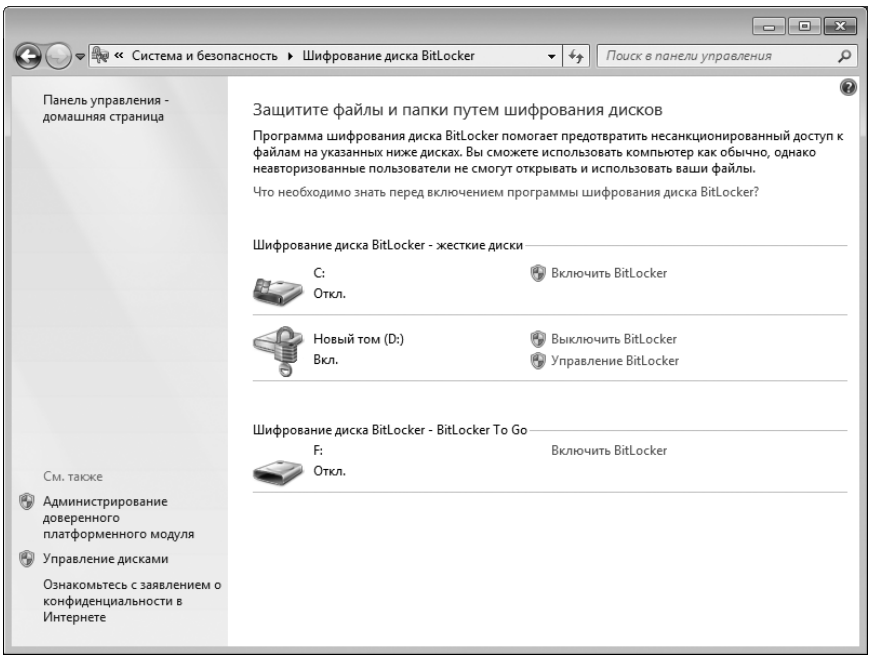

Рис. 11-8. Просмотр состояния BitLocker для тома

Для корректной работы технологии BitLocker необходимо запустить службу Шифрование диска BitLocker (BitLocker Drive Encryption). Как правило, для этой службы задан ручной запуск и работа от имени учетной записи Локальная система (LocalSystem).

Чтобы использовать в BitLocker смарт-карту, необходимо запустить службу Смарт-карта (Smart Card). Как правило, для нее настроен ручной запуск и работа от имени учетной записи Локальная система (LocalSystem).

Создав для компьютера ключ запуска или PIN-код и ключ восстановления, вы можете также создать их дубликаты. Щелкните кнопку **Пуск (Start)**

и выберите команду **Компьютер (Computer)**. Щелкните том правой кнопкой и выберите команду **Управление BitLocker (Manage BitLocker)**. Если BitLocker отключен, вместо нее будет показана команда **Включить BitLocker (Turn On BitLocker)**.

Параметры зависят от типа тома, с которым вы работаете, и настроек шифрования. Доступные варианты таковы:

- **Добавить пароль для снятия блокировки диска (Add A Password To Unlock The Drive)** Позволяет добавлять пароль шифрования. Выберите этот вариант, а затем введите и подтвердите новый пароль. Щелкните **Далее (Next)** и **OK**.
- **Изменить пароль для снятия блокировки диска (Change Password To Unlock The Drive)** Позволяет изменить пароль шифрования. Выберите этот вариант, затем введите и подтвердите новый пароль. Щелкните **Далее (Next)** и **OK**.
- **Удалить пароль для этого диска (Remove Password From This Drive)** Выберите этот вариант, чтобы отменить ввод пароля шифрования для разблокирования носителя.
- **Добавить смарт-карту для снятия блокировки диска (Add A Smart Card To Unlock The Drive)** Позволяет задать использование смарт-карты для разблокирования носителя. Выберите этот вариант и следуйте дальнейшим указаниям.
- **Удалить смарт-карту для этого диска (Remove Smart Card From This Drive)** Выберите этот вариант, чтобы отменить использование смарт-карты для разблокирования носителя.
- **Изменить смарт-карту для этого диска (Change Smart Card For This Drive)** Позволяет заменить используемую смарт-карту для разблокирования носителя. Выберите этот вариант и следуйте дальнейшим инструкциям.
- **Сохранить или напечатать ключ восстановления (Save Or Print Recovery Key Again)** Позволяет сохранить или распечатать ключ восстановления. Выберите этот вариант и следуйте дальнейшим инструкциям.
- **Автоматически снимать блокировку диска этого компьютера (Automatically Unlock This Drive On This Computer)** Выберите этот вариант, чтобы включить автоматическое разблокирование носителя.
- **Отключить автоматическое снятие блокировки для этого диска на этом компьютере (Turn Off Automatic Unlocking For This Drive On This Computer)** Выберите этот вариант, чтобы отключить автоматическое разблокирование носителя.

Восстановление данных, защищенных при помощи BitLocker

Если вы настроили шифрование диска BitLocker и компьютер вошел в режим восстановления, вам необходимо разблокировать компьютер. Чтобы

разблокировать компьютер с использованием ключа восстановления, сохраненного на USB-носителе, выполните следующие действия:

1. Включите компьютер. Если компьютер заблокирован, откроется консоль восстановления BitLocker.
2. Вставьте USB-накопитель с ключом восстановления и нажмите Enter.
3. Разблокирование и перезапуск компьютера произойдут автоматически. Вам не нужно вводить ключ восстановления вручную.

Если вы сохранили файл с ключом восстановления в папке на другом компьютере или съемном носителе, используйте другой компьютер, чтобы открыть и подтвердить файл с ключом восстановления. Чтобы найти нужный файл, найдите поле ИД пароля (Password ID) в окне консоли восстановления, открытой на заблокированном компьютере, и запишите номер. Этот идентификатор используется в качестве имени файла, содержащего ключ восстановления. Откройте этот файл и найдите ключ восстановления.

Чтобы разблокировать компьютер при помощи ключа восстановления, выполните следующие действия:

1. Включите компьютер. Если компьютер заблокирован, откроется консоль восстановления BitLocker.
2. Введите ключ восстановления и нажмите Enter. Разблокирование и перезагрузка компьютера произойдут автоматически.

Компьютер будет заблокирован, если пользователь введет неверный ключ. В восстановительной консоли вы можете дважды нажать Esc, чтобы выйти из подсказки о восстановлении и выключить компьютер. Компьютер также может заблокироваться, если произойдет ошибка, связанная с TPM, или будут модифицированы загрузочные данные. В этом случае процесс загрузки компьютера прервется рано, до начала работы ОС. В этом случае заблокированный компьютер не сможет принять стандартные цифры, вводимые с клавиатуры. В такой ситуации для ввода пароля восстановления используйте функциональные клавиши. Функциональные клавиши F1–F9 обозначают цифры от 1 до 9, а функциональная клавиша F10 обозначает 0.

Приостановка работы или выключение шифрования диска BitLocker

Если вам нужно внести изменения в TPM или в систему, необходимо временно отключить шифрование BitLocker на системном томе. Временно отключить шифрование BitLocker на томах данных нельзя; их можно только дешифровать.

Чтобы временно отключить шифрование BitLocker на системном томе, выполните следующие действия:

1. Щелкните кнопку **Пуск (Start)**, выберите команду **Панель управления (Control Panel)** и щелкните **Система и безопасность (System And Security)**. Затем дважды щелкните **Шифрование диска BitLocker (BitLocker Drive Encryption)**.

2. Для системного тома выберите команду **Приостановить защиту (Turn Off BitLocker Drive Encryption)**.

По завершению этой процедуры работа BitLocker на системном томе ОС будет временно приостановлена.

Чтобы отключить BitLocker Drive Encryption на томе данных и дешифровать его, выполните следующие действия:

1. Щелкните **Пуск (Start)**, выберите команду **Панель управления (Control Panel)**, щелкните **Система и безопасность (System And Security)**, а затем дважды щелкните **Шифрование диска BitLocker (BitLocker Drive Encryption)**.
2. Для нужного тома выберите команду **Выключить BitLocker (Turn Off BitLocker Drive Encryption)**.
3. В открывшемся диалоговом окне щелкните кнопку **Выполнить расшифровку диска (Decrypt The Volume)**.

Чтобы выключить BitLocker Drive Encryption и дешифровать USB-накопитель, выполните следующие действия:

1. Щелкните **Пуск (Start)**, выберите команду **Панель управления (Control Panel)**, щелкните **Система и безопасность (System And Security)**, а затем дважды щелкните **Шифрование диска BitLocker (BitLocker Drive Encryption)**.
2. Для USB-накопителя выберите команду **Выключить BitLocker (Turn Off BitLocker Drive Encryption)**.
3. В открывшемся диалоговом окне щелкните кнопку **Выполнить расшифровку диска (Decrypt The Volume)**.

Глава 12

Диски и файловые системы

На большинстве компьютеров используются накопители нескольких типов, включая встроенные и съемные. Главным устройством для хранения данных является, как правило, внутренний жесткий диск. В большинстве случаев первый установленный жесткий диск обозначается Disk 0. При добавлении новых жестких дисков, они обозначаются Disk 1, Disk 2 и т. д. Эта глава посвящена инструментальным средствам и приемам управления дисковыми накопителями и файловыми системами. Вы научитесь разбивать диски на разделы и форматировать их, а также преобразовывать диски из одного типа в другой. Мы также коснемся компонентов Windows 7, затрагивающих работу дисков, например Windows ReadyBoost, Windows ReadyDrive и Windows SuperFetch.

Общие сведения об управлении дисками

В Windows 7 физические диски определяются как основные и динамические.

- **Основной (basic) диск** Этот тип дисков характерен, главным образом, для прежних версий Windows. В Windows 7 основной диск можно разбить на один или несколько разделов. *Раздел* (partition) — это логическая часть диска, работающая так, словно является самостоятельным физическим диском. Чтобы использовать раздел, его необходимо отформатировать в одной из файловых систем (FAT, FAT32 или NTFS) и назначить ему *указатель* (designator). После этого отформатированный раздел называется *основным томом* (basic volume) — к нему можно обращаться, как к локальному диску компьютера. В Windows 7 на основных дисках поддерживаются основные и дополнительные разделы. Для запуска ОС используется *основной* (primary) раздел. Доступ к основному разделу осуществляется напрямую — по указателю тома. Основной раздел нельзя делить. В отличие от него, *дополнительный* (extended) раздел — это раздел непрямого доступа. После создания дополнительного раздела его необходимо разделить на один или более логических дисков. Обращаться к логическим дискам можно независимо друг от друга.

- **Динамический (dynamic) диск** Впервые появились в Windows 2000. Динамические диски позволяют решать большинство задач по обслуживанию дисков без перезагрузки компьютера. Подобно основному, динамический диск тоже можно разделить, только не на разделы, а на тома. Впрочем, том очень похож на раздел. Наиболее широко используются *простые тома* (simple volume). Простым называется том, который расположен на одном диске и предназначен для запуска ОС и хранения обычных данных. Применяются и другие типы томов, позволяющие, в частности, распространить один том на несколько дисков (составной том). Как и раздел или логический диск, том на динамическом диске нужно отформатировать и назначить ему указатель. Отформатированный том называется *динамическим*, и доступ к нему осуществляется так же, как и к локальному диску компьютера. Динамический том, объединяющий пространство нескольких физических дисков, отображается как один локальный диск с единым указателем.

Примечание В файловой системе FAT максимальный размер тома определяется разрядностью таблицы размещения файлов. В FAT16, или просто FAT, для определения таблицы размещения файлов требуется 16 бит. Размер томов, которые можно форматировать в FAT16, не превышает 4 Гб. Существует и 32-разрядная версия FAT — FAT32. В ней для таблицы размещения файлов используется 32 бита, а средства форматирования Windows позволяют создавать тома FAT32 размером до 32 Гб. Хотя в Windows есть возможность монтировать в FAT32 более объемные тома, созданные средствами сторонних производителей, в целом, тома, превышающие 32 Гб, следует форматировать в NTFS.

Вы вольны изменить тип накопителя с основного на динамический и с динамического в основной. При преобразовании основного диска в динамический разделы автоматически становятся томами соответствующего типа без потери данных. Преобразовать динамический диск в основной куда сложнее. Для этого нужно удалить тома на динамическом диске. При этом уничтожается вся содержащаяся в них информация, и единственный способ спасти данные — восстановить их из резервной копии.

Еще одной характеристикой диска является *стиль раздела* (partition style) — диск с основной загрузочной записью (MBR) или диск с таблицей разделов GUID (GPT). Разделы MBR и GPT поддерживаются как в 32-разрядных, так и в 64-разрядных версиях Windows 7, а вот в Windows XP и более ранних версиях стиль раздела GPT не распознается.

На диске MBR имеется таблица разделов, в которой описано расположение разделов на диске. В первом секторе диска хранится основная загрузочная запись и двоичный файл с основным загрузочным кодом (master boot code), использующимся для загрузки системы. Для обеспечения безопасности системы этот сектор не включен в разделы и скрыт от пользователей.

Диски MBR поддерживают тома объемом до 4 Тб. На них используются разделы двух типов — основные или дополнительные. На каждом MBR-диске может размещаться до четырех основных разделов или три основных

и один дополнительный раздел. Основные разделы — это области диска, к которым осуществляется прямой доступ для хранения файлов. Чтобы к основному разделу могли обращаться пользователи, на нем нужно создать файловую систему. В отличие от основных, дополнительные разделы — это разделы без прямого доступа. Они состоят из одного или нескольких логических дисков, используемых для хранения файлов. Возможность делить дополнительные разделы на логические диски позволяет разделить физический диск на более чем четыре раздела.

Раздел GPT изначально создавался для высокопроизводительных компьютеров на базе процессора Itanium. В системах на основе архитектуры x86 и x64 технологию GPT рекомендуется применять для дисков объемом более 2 Тб, а в системах на базе Itanium — для любых дисков. Ключевое различие разделов GPT и MBR заключается в способе хранения данных раздела. В GPT критические данные раздела хранятся в отдельных разделах, а избыточность данных в основной и резервной таблицах разделов укрепляет отказоустойчивость.

Несмотря на столь глубокие отличия между разделами GPT и MBR, большинство задач, связанных с дисками, выполняются в них одинаково. А это означает, что после установки и настройки дисков стиль раздела, GPT или MBR, как правило, не имеет большого значения. Но вместе с тем, помните о следующем:

- На основных MBR-дисках может содержаться не более четырех основных разделов, либо три основных и один дополнительный раздел с одним или несколькими логическими дисками. На динамических MBR-дисках может быть неограниченное количество томов.
- Количество разделов на GPT-дисках может достигать 128 объемом до 18 Эб. На компьютерах с дисками GPT есть два обязательных раздела и один или несколько необязательных — разделы изготовителя оборудования (OEM) или разделы с данными. К обязательным разделам относятся системный раздел EFI (EFI system partition, ESP) и резервный раздел Майкрософт (Microsoft Reserved, MSR). Хотя характер необязательных разделов зависит от конфигурации системы, чаще всего это основные разделы. Основные разделы GPT-дисков используются для хранения данных пользователей.
- На компьютерах на основе архитектуры x86 или x64 и BIOS стиль MBR применяется для загрузочных дисков и дисков с данными, а стиль GPT — только для дисков с данными. На компьютерах с процессором Itanium или x64 с системой EFI могут быть как GPT-диски, так и MBR-диски. Однако хотя бы один из них должен быть GPT-диском, на котором содержится раздел ESP, а также основной раздел или простой том, на котором записана загружаемая ОС.

В Windows 7 имеется несколько инструментов для работы с дисками. Об одном из них часто забывают — это консоль Компьютер (Computer). К другим

инструментам относятся консоль Управление дисками (Disk Management), а также утилиты FSUtil и DiskPart. Разделы и тома на дисках MBR и GPT форматируются в файловых системах FAT, FAT32 и NTFS. Создавая диск в утилите Управление дисками (Disk Management), вы можете отформатировать его, а также назначить ему букву или создать точку подключения. Хотя программа Управление дисками (Disk Management) позволяет форматировать разделы и тома на MBR-дисках в системах FAT, FAT32 и NTFS, для форматирования разделов и томов на GPT-дисках в ней доступна только система NTFS. Чтобы отформатировать GPT-диск в FAT или FAT32, нужно выполнить команду Format или DiskPart в командной строке.

Стиль таблицы разделов можно преобразовывать из MBR в GPT и наоборот. Изменение стиля таблицы разделов требуется при обмене дисками между компьютерами на базе x86 и Itanium или в случае, когда формат новых дисков не соответствует вашим потребностям. Преобразовать стиль таблицы разделов можно только на пустом диске, то есть, это должен быть новый или только что отформатированный диск.

Консоль Компьютер (Computer)

Чтобы открыть консоль Компьютер (Computer), последовательно щелкните кнопку **Пуск (Start)** и команду **Компьютер (Computer)**. В консоли Компьютер (Computer) можно быстро просмотреть все доступные на компьютере накопители (рис. 12-1):

- **Жесткие диски (Hard Disk Drives)** Локальные диски, установленные на компьютере. Щелкните диск правой кнопкой, чтобы просмотреть доступные возможности управления им, включая команду **Проводник (Explore)**, по которой диск открывается в Проводнике (Windows Explorer) с отображением представления Папки (Folders). Команда **Проводник (Explore)** более удобна, чем команда **Открыть (Open)**, при выборе которой диск открывается в Проводнике (Windows Explorer) без отображения представления Папки (Folders).
- **Устройства со съемными носителями (Devices With Removable Storage)** Здесь перечислены устройства со съемными носителями, включая дисководы CD и DVD, накопители USB и дисководы для гибких дисков. Щелкните устройство правой кнопкой, чтобы просмотреть доступные команды. Команда **Извлечь (Eject)** служит для извлечения текущего носителя и вставки следующего.

Совет На смену гибким дискам и прочим съемным носителям приходят флешнакопители с интерфейсом USB и FireWire. Наличие на компьютере порта USB или FireWire позволяет быстро подключать и отключать соответствующие диски. Перед отключением накопителя с интерфейсом USB или FireWire обеспечьте его безопасное извлечение. Один из способов — команда **Извлечь (Eject)**. В Проводнике (Windows Explorer) или в консоли Компьютер (Computer) щелкните правой кнопкой значок диска и выберите команду **Извлечь (Eject)**. Безопасно отсоединить диск можно только после того, как вы перестали им пользоваться.

- **Сетевое размещение (Network Location)** Все подключенные к компьютеру сетевые диски, предоставляющие доступ к общим папкам и дискам на других компьютерах. Чтобы подключить сетевой диск при помощи мастера Подключить сетевой диск (Map Network Drive Wizard), щелкните кнопку **Пуск (Start)**, затем щелкните правой кнопкой команду **Компьютер (Computer)** и выберите команду **Подключить сетевой диск (Map Network Drive)**. Для отключения сетевого диска щелкните кнопку **Пуск (Start)**, затем щелкните правой кнопкой команду **Компьютер (Computer)** и выберите команду **Отключить сетевой диск (Disconnect Network Drive)**.

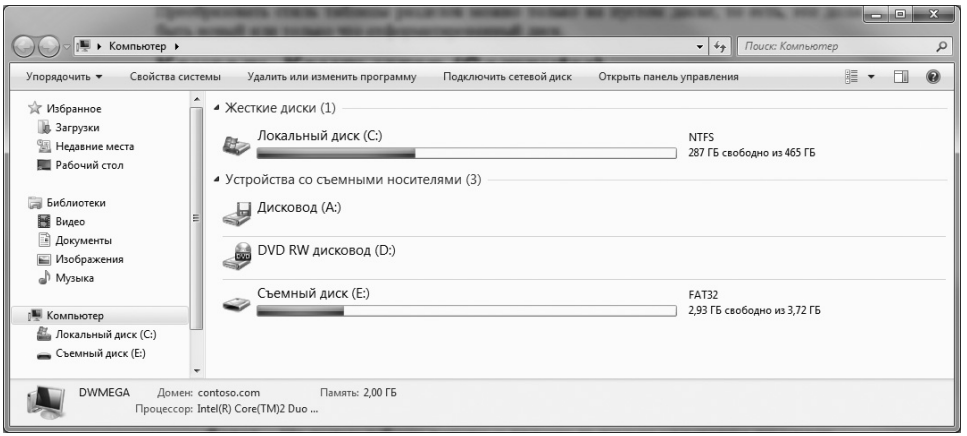

Рис. 12-1. Консоль Компьютер (Computer) — простой доступ к запоминающим устройствам компьютера

Консоль Управление дисками (Disk Management)

Консоль Управление дисками (Disk Management) как нельзя лучше подходит для настройки дисков. В ней есть средства для управления дисками, разделами, томами, логическими дисками и связанными с ними файловыми системами. Управление дисками (Disk Management) — это оснастка консоли MMC. Ее можно открыть в стандартной консоли, поставляемой с Windows, или добавить в пользовательскую консоль. Вот задачи, выполняемые в оснастке Управление дисками (Disk Management):

- определение объема, свободного места и других свойств дисков;
- создание разделов и логических дисков на основных дисках;
- создание томов на динамических дисках;
- расширение томов с целью увеличения их размера;
- форматирование томов в файловых системах FAT, FAT32 или NTFS;
- назначение букв диска и путей к томам;
- преобразование основных дисков в динамические и наоборот.

Оснастка Управление дисками (Disk Management), показанная на рис. 12-2, включена в консоль Управление компьютером (Computer Management). Чтобы открыть консоль Управление компьютером (Computer Management) введите **compmgmt.msc** в командной строке с повышенными полномочиями. Или щелкните кнопку **Пуск (Start)**, затем щелкните правой кнопкой команду **Компьютер (Computer)** и выберите команду **Управление (Manage)**. На левой панели консоли Управление компьютером (Computer Management) щелкните элемент **Управление дисками (Disk Management)**.

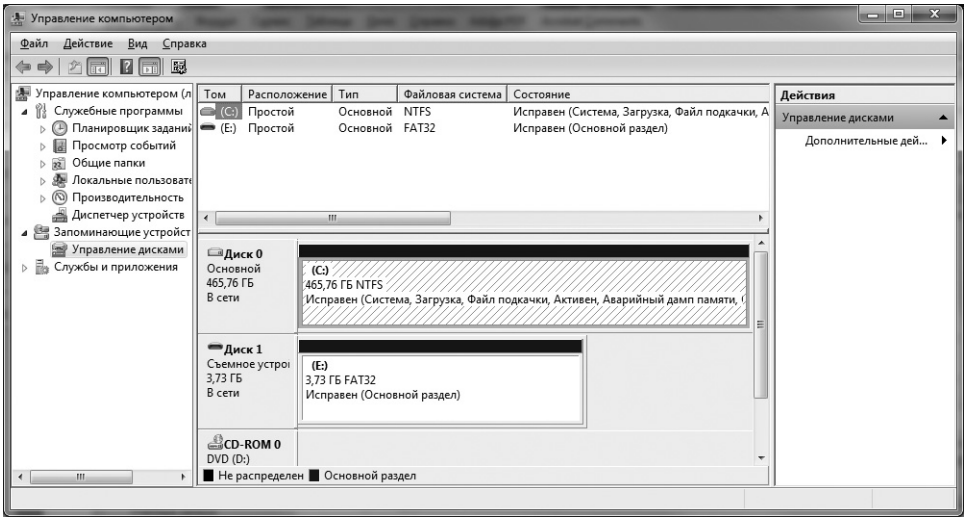

Рис. 12-2. Настройка дисков в программе Управление дисками (Disk Management)

После запуска консоль Управление компьютером (Computer Management) автоматически подключается к локальному компьютеру. Для просмотра дисков на другом компьютере щелкните правой кнопкой узел **Управление компьютером (Computer Management)** в дереве консоли и выберите в контекстном меню команду **Подключиться к другому компьютеру (Connect To Another Computer)**. Затем укажите систему, диски которой нужно просмотреть. Чтобы подключиться к другому компьютеру во время запуска консоли Управление компьютером (Computer Management) из командной строки, введите команду **compmgmt.msc/computer=*ИмяКомпьютера***, где *ИмяКомпьютера* — имя удаленного компьютера, к которому нужно подключиться.

В стандартной конфигурации консоли Управление дисками (Disk Management) в верхней панели отображен список томов, а в нижней показано их графическое представление. Одновременно отображаются только два представления из трех возможных:

- **Список томов (Volume List)** В этом представлении содержится подробная сводка информации об имеющихся на компьютере дисках. Щелкнув заголовок столбца, например **Расположение (Layout)** или **Состояние (Status)**, вы отсортируете сведения о дисках по данному столбцу.

- **Графическое представление (Graphical)** Наглядная информация о доступных физических и логических дисках. Для физических дисков указаны номер диска и тип устройства, например, основной, съемный или CD-ROM, а также объем диска и его состояние (активен или не активен). Для каждого логического диска на физическом диске предоставляются дополнительные сведения: буква диска и метка раздела или тома, тип файловой системы (FAT, FAT32 или NTFS), размер сектора диска (Мб) и состояние локального диска (исправен или неисправен).
- **Список дисков (Disk List)** В этом представлении содержится сводка сведений о физических дисках. Приводится номер диска и тип устройства, например основной, съемный или CD-ROM, объем диска, размер неразмеченной области на диске (если такая есть), состояние диска, например, в сети или нет носителя, и тип интерфейса устройства, например встроенный (IDE), SCSI, шина USB или FireWire (1394).

Чтобы сменить представления в верхней или нижней панели, воспользуйтесь меню **Вид (View)**. Чтобы изменить верхнее представление, в меню **Вид (View)** разверните подменю **Верх (Top)** и выберите нужное представление. Чтобы изменить нижнее представление, в меню **Вид (View)** разверните подменю **Низ (Bottom)** и щелкните нужное представление.

Как видите, имеющиеся представления представляют обзорные сведения о доступных дисках. Чтобы получить более подробную информацию о локальном диске, щелкните диск правой кнопкой в представлении **Список томов (Volume List)** и выберите команду **Свойства (Properties)**. Откроется диалоговое окно, пример которого показан на рис. 12-3. Это же окно можно открыть и в Проводнике (Windows Explorer), щелкнув правой кнопкой значок диска и выбрав команду **Свойства (Properties)**. Вкладка **Настройка (Customize)** предназначена для выбора шаблона, определяющего вид папки на панели просмотра содержимого в Проводнике (Windows Explorer).

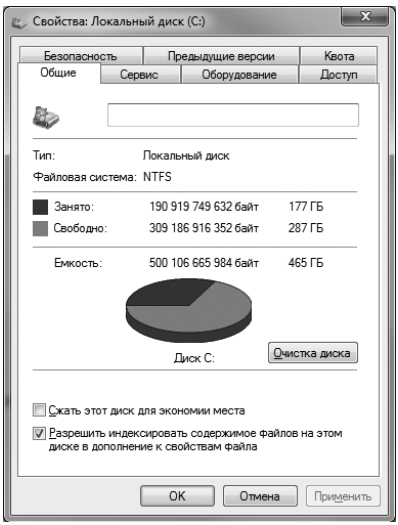

Рис. 12-3. Просмотр сведений о диске в диалоговом окне Свойства (Properties)

Утилиты FSUtil и DiskPart

В Windows 7 для работы с дисками предназначено несколько инструментов командной строки, включая следующие:

- **FSUtil** Утилита предназначена для профессионалов из службы поддержки для управления дисками на сравнительно низком уровне. С ее помощью вы сможете просматривать метаданные диска и работать с ними, а также просматривать другую относящуюся к дискам информацию, включая журналы изменений USN, точки повторной обработки и жесткие связи. Кроме того, здесь можно получить подробные сведения о секторах и кластерах, например количество свободных или зарезервированных секторов на диске. Для дальнейшего знакомства с программой FSUtil введите **fsutil** в командной строке с повышенными полномочиями.
- **DiskPart** Текстовый интерпретатор команд для управления дисками, разделами и томами из командной строки. Программа DiskPart не только дублирует функции консоли Управление дисками (Disk Management). Она также поддерживает сценарии, автоматизирующие процесс управления дисками. Чтобы открыть DiskPart, введите в командной строке с повышенными полномочиями команду **diskpart**. После этого откроется командная строка DISKPART>. Для вывода списка доступных команд с описанием введите команду help и нажмите Enter.

Примечание В отличие от консоли Управление дисками (Disk Management) с интуитивно понятным и простым интерфейсом, программы FSUtil и DiskPart довольно сложны и предназначены для опытных администраторов. Подробные сведения о работе с ними вы найдете в книге *Windows Command-Line Administrator's Pocket Consultant* (Microsoft Press 2008) [Командная строка Windows Vista® и Windows Server® 2008. Справочник администратора (Русская Редакция, БХВ-Петербург, 2008)]. Пример использования команды DiskPart приводится в разделе «Назначение раздела активным» этой главы.

Повышение производительности дисков

На работу с дисками влияет ряд компонентов Windows 7, в том числе:

- **Windows ReadyBoost** Повышает производительность системы за счет размещения кеша на флеш-накопителях.
- **Windows ReadyDrive** Повышает производительность переносных компьютеров, оснащенных гибридными дисками
- **Windows SuperFetch** Повышает производительность системы при помощи модифицированного алгоритма управления памятью.

Ниже мы подробнее рассмотрим эти компоненты.

Windows ReadyBoost

Дисковые накопители используются на компьютере не только для чтения и записи данных приложений и документов пользователей. Накопители нужны ОС для записи файлов подкачки и системного кеша. Чтение и запись на диск

выполняются значительно медленнее, чем чтение и запись в оперативную память, что может отрицательно сказаться на общей производительности.

Система Windows ReadyBoost призвана ускорить процесс чтения и записи системного кеша. Она ускоряет кеширование за счет использования флеш-накопителей, обладающих достаточно высоким быстродействием. Кеширование применяется ко всему содержимому диска, а не только к файлу подкачки или системным DLL. Как следствие, растет общая производительность компьютера — ведь скорость чтения с флеш-накопителей может до 10 раз превышать скорость чтения с физических дисков.

Реализовать Windows ReadyBoost можно на флеш-накопителях USB 2.0, картах Secure Digital (SD) и CompactFlash. Эти устройства должны обладать высоким быстродействием и объемом не менее 256 Мб. В целях повышения производительности рекомендуется приобретать флеш-накопители USB с высокоскоростной памятью. Если устройство обладает как быстрой, так и медленной памятью, для повышения производительности используется только высокоскоростная область памяти. Системой ReadyBoost резервируется от 230 до 4094 Мб флеш-памяти. Рекомендуемый объем памяти должен в 1–3 раза превышать объем доступной системной памяти.

Память флеш-накопителей USB используется, главным образом, для произвольного ввода-вывода, так как в части последовательного ввода-вывода большинство флеш-накопителей работают медленнее дисков. Благодаря Windows ReadyBoost наибольшая производительность достигается за счет автоматической передачи крупных последовательных запросов чтения для обработки на диск компьютера. Чтобы устройство USB можно было в любой момент извлечь, все операции записи данных выполняются сначала на жесткий диск, а затем копируются на флеш-память. Таким образом, все хранящиеся на съемном устройстве данные дублируются на жестком диске, и при извлечении устройства потери данных не происходит. В памяти съемного устройства может оказаться конфиденциальная информация, поэтому средствами Windows ReadyBoost выполняется шифрование данных, после чего данные можно использовать только на том компьютере, на котором они были изначально записаны.

Включение и настройка ReadyBoost

При подключении USB-устройства к порту USB 2.0 или более скоростному выполняется анализ быстродействия устройства. Если флеш-память устройства обладает достаточной скоростью, можно расширить физическую память компьютера на величину объема памяти устройства USB. Как правило, скорость флеш-памяти не ниже скорости шины компьютера.

Совет Windows иногда ошибочно оценивает устройство как не удовлетворяющее требованиям быстродействия. Если устройство не прошло начальный тест на быстродействие, оцените его еще раз на вкладке **ReadyBoost**. В Проводнике (Windows Explorer) щелкните устройство правой кнопкой и выберите команду **Свойства (Properties)**. В диалоговом окне **Свойства (Properties)** перейдите на вкладку **ReadyBoost** и щелкните **Протестировать устройство (Test Again)**.

Далее описано включение и настройка работы Windows ReadyBoost при первом подключении съемного устройства USB к компьютеру:

1. Подключите съемное устройство USB к порту USB версии 2.0 или более новой. Если вы не изменили стандартные параметры автозапуска в панели управления, окно **Автозапуск (AutoPlay)** откроется автоматически.
2. Щелкните вариант **Ускорить работу системы, используя Windows ReadyBoost** (**Speed Up My System Using Windows ReadyBoost**), чтобы открыть диалоговое окно **Свойства (Properties)**. Выполните одно из следующих действий на вкладке **ReadyBoost** (рис. 12-4) и щелкните **OK**:
   - Чтобы функция ReadyBoost автоматически резервировала как можно больше места на устройстве, установите переключатель **Предоставлять это устройство для технологии ReadyBoost (Dedicate This Device To ReadyBoost)**. Этот вариант не исключает запись файлов на устройство. Просто системе ReadyBoost будет отведено максимально возможное пространство.
   - Если вам не нужно использовать наибольший возможный объем, установите переключатель **Использовать это устройство (Use This Device)** и задайте объем пространства, отводимый для ReadyBoost, при помощи бегунка или в поле **Зарезервировать для ускорения работы системы (Space To Reserve For System Speed)**. Если зарезервировать объем меньше доступного, свободное пространство можно будет использовать для файлов и данных.

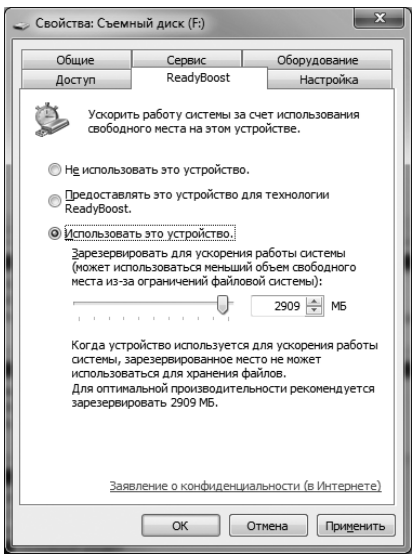

Рис. 12-4. Настройка параметров Windows ReadyBoost

Физическая память компьютера будет расширена на данное устройство. В стандартной конфигурации для повышения быстродействия системы Windows ReadyBoost резервирует все доступное на устройстве пространство.

Ближе к реальности Флеш-накопитель USB подходит для ReadyBoost, только если его пропускная способность не ниже 2,5 Мбит/с при произвольном чтении блоков по 4 Кб и 1,75 Мбит/с при произвольной записи блоков по 512 Кб. Реализуя ReadyBoost на устройстве, зашифрованном при помощи BitLocker To Go, имейте в виду, что процессы шифрования и дешифрования отрицательно сказываются на скорости чтения и записи. Если вы пользуетесь BitLocker To Go и ReadyBoost, рекомендуется при подключении автоматически разблокировать устройство. Иначе пользователю придется каждый раз дополнительно открывать устройство для доступа.

Чтобы реализовать технологию Windows ReadyBoost на специально выделенном для этого USB-устройстве, выполните следующие действия:

1. Щелкните кнопку **Пуск (Start)** и выберите команду **Компьютер (Computer)**.
2. В списке **Устройства со съемными носителями (Devices With Removable Storage)** щелкните правой кнопкой съемное устройство USB и выберите **Свойства (Properties)**.
3. На вкладке **ReadyBoost** настройте параметры, как описано в шаге 2 предыдущей процедуры. Щелкните **OK**.

Если устройство USB не поддерживает технологию ReadyBoost, использовать его не удастся. Съемное устройство USB с ReadyBoost можно извлечь в любой момент без потери данных и без причинения вреда системе. Однако после извлечения устройства производительность системы вернется к своему обычному уровню. Чтобы безопасно извлечь устройство, выполните следующие действия:

1. Откройте программу Проводник (Windows Explorer) или консоль Компьютер (Computer).
2. Щелкните устройство правой кнопкой и выберите команду **Извлечь (Eject)**. Если на устройстве есть открытые файлы или устройство открыто для просмотра в Проводнике (Windows Explorer), перед извлечением необходимо закрыть все файлы и окна Проводника.

Windows ReadyDrive

Технология Windows ReadyDrive предназначена для повышения быстродействия переносных компьютеров с гибридными дисками. Гибридным называется диск, в котором помимо жесткого накопителя существует еще и флеш-память. Флеш-память работает гораздо быстрее жесткого диска. Поэтому на компьютерах под управлением Windows 7 данные и изменения в данных сначала записываются во флеш-память, а потом периодически синхронизируются с диском. Благодаря этому снижается потребление энергии на вращение жесткого диска.

Флеш-память гибридных дисков используется для быстрого запуска и продолжения работы при выходе из спящего режима или гибернации. При этом перед переходом в режим сна или гибернации во флеш-память записывается информация, необходимая для запуска или возобновления ОС. Во время запуска или пробуждения компьютера информация считывается из флеш-памяти.

Включать функцию ReadyDrive не требуется — на переносных компьютерах с гибридными дисками она включается автоматически.

Windows SuperFetch

Для повышения производительности и сокращения времени отклика системы в Windows 7 скорректировано использование пользовательских и фоновых процессов. В Windows XP приоритет использования памяти пользовательскими и фоновыми процессами одинаков: и те, и другие загружаются в память при их использовании. Подобное отсутствие приоритета часто приводит к конфликтам при доступе к памяти, а также к снижению быстродействия, поскольку фоновые процессы после запуска остаются в памяти. В Windows 7 эта проблема решена: фоновые процессы выгружаются из памяти после выполнения, когда в память повторно загружаются данные пользовательских процессов.

В Windows XP у пользовательских и фоновых процессов одинаковый приоритет ввода-вывода. Часто это становится причиной конфликтов и низкой скорости чтения-записи. Для решения этой проблемы в Windows 7 реализованы очереди ввода-вывода с высоким и низким приоритетом. Пользовательские процессы используют для операций чтения и записи на физические диски ввод-вывод с высоким приоритетом. Фоновые процессы для операций чтения и записи на физические диски используют ввод-вывод с низким приоритетом.

Примечание В Windows 7 в качестве фоновых процессов выполняются многие службы и служебные задачи. В частности, в Windows 7 по расписанию запускается программа Дефрагментация диска (Disk Defragmenter). Она выполняется как фоновый процесс с низким приоритетом ввода-вывода.

Ключевой компонент в расстановке приоритетов использования памяти и ввода-вывода — служба Windows SuperFetch. В ней применен модифицированный алгоритм управления памятью, повышающий быстродействие системы. В отличие от алгоритма управления памятью из Windows XP и более ранних версий, в SuperFetch работа с памятью оптимизируется в зависимости от того, как использует компьютер текущий пользователь. Для этого компонент SuperFetch выполняет следующее:

- **Различает выполняющиеся на компьютере пользовательские приложения и фоновые службы** Процессы текущего пользователя имеют приоритет по сравнению с фоновыми задачами, что ускоряет реагирование компьютера на запросы пользователя. Вследствие расстановки приоритета процессов фоновые задачи не занимают все время процессора.
- **Оптимизирует память для пользователей после запуска фоновых задач** Для выполнения служебных задач в Windows 7, в отличие от предыдущих версий Windows, используется время простоя процессора. Именно тогда выполняется большинство системных и служебных задач, подобных дефрагментации диска и архивации. Во время бездействия

компьютера фоновые процессы выполняются как обычно, а после завершения фонового процесса память средствами SuperFetch возвращается к состоянию, предшествующему запуску фонового процесса. Тем самым память оптимизируется для пользовательских процессов, и компьютер способен отвечать на запросы пользователей.

- **Отслеживает часто используемые приложения и заранее готовится к действиям пользователей** Компонент SuperFetch выявляет приложения, которые запускаются чаще всего, а также определяет типичное время их использования. Эта информация используется для предварительной загрузки приложения ко времени его ожидаемого запуска.
- **Использует ввод-вывод с различным приоритетом** Наличие очередей ввода-вывода с высоким и низким приоритетом позволяет ускорить выполнение операций чтения-записи для пользовательских процессов и ускорить общий отклик компьютера Windows 7. Когда одновременно выполняется несколько процессов, процессы с высоким приоритетом получают больше времени на ввод-вывод, чем процессы с низким приоритетом. В результате процессы и приложения пользователя работают быстрее, и возникает меньше конфликтов при одновременном выполнении пользовательских и фоновых приложений.

Компонент SuperFetch поддерживается во всех версиях Windows 7. Администратор должен понимать, как работает SuperFetch и как его настраивать. Ниже приведены основные характеристики SuperFetch:

- Выполняется в качестве службы SuperFetch. Служба запускается автоматически при запуске системы от имени учетной записи LocalSystem.
- Использует исполняемый файл Svchost.exe и работает в режиме ограниченного сетевого доступа. Это означает, что компонент SuperFetch имеет доступ только к локальному компьютеру. У него нет выхода ни в одну из сетей, к которым подключен компьютер.
- Использует Диспетчер фильтров (Filter Manager), предоставляющий SuperFetch информацию о файлах и файловых системах. Компонент Диспетчер фильтров (Filter Manager) устанавливается автоматически вместе с ОС.
- Записывает данные предварительной выборки в папку %SystemRoot%\Prefetch. Эти данные нужны для быстрого запуска приложений. В папке Prefetch также находятся несколько файлов баз данных (БД) для наблюдения за использованием приложений и повышения быстродействия программ. Также записывается история сбоев приложений.

Примечание Обслуживание папки Prefetch выполняется автоматически. Ее не нужно удалять или очищать.

Иногда после внесения серьезных изменений в ОС, установки пакетов исправлений или обновлений, а также после установки или перенастройки приложений пользователи отмечают снижение скорости запуска. Степень

замедления зависит от масштаба изменений и от объема информации об использования памяти, перестраиваемой SuperFetch. Иногда, например после установки пакета исправлений, для нормализации скорости запуска требуется не одна перезагрузка.

Основные и динамические диски

Совсем недавно на всех компьютерах с предустановленной ОС Windows использовались только основные жесткие диски. Однако в наши дни растет спрос на более объемные и надежные носители, и потому все больше компьютеров поставляется с динамическими дисками. Вместо одного диска объемом 500 Гб на новых компьютерах нередко встречается составной логический диск объемом 1000 Гб, сформированный из двух физических дисков по 500 Гб каждый. Единственный способ реализовать это в Windows 7 — применять динамические диски.

Чем больше становится компьютеров с динамическими дисками, тем чаще будет вас посещать мысль о том, что вам стоит преобразовать основные диски на ваших компьютерах в динамические. В некоторых случаях такое решение продиктовано стремлением к стандартизации, когда все компьютеры, скажем, определенного отдела, должны иметь одну и ту же конфигурацию. Иногда инициатива исходит от ИТ-руководства, считающего преобразование основных дисков в динамические разновидностью обновления. Однако прежде чем принять решение о переходе с одного типа дисков на другой, подумайте о том, что поставлено на карту, какие функции поддерживаются и какие не поддерживаются.

Основной диск — это физический диск, содержащий один или несколько основных томов, которые могут быть настроены как основные разделы, а также необязательный дополнительный раздел, состоящий из логических дисков. Основной раздел — это область диска с возможностью прямого доступа для хранения файлов. На каждом физическом диске может размещаться до четырех основных разделов. Для доступа к основному разделу на нем нужно создать файловую систему. Вместо одного из четырех возможных основных разделов, вы можете создать дополнительный раздел (то есть на основном диске может быть до трех основных разделов и один дополнительный раздел). Отличие от основных разделов состоит в том, что к дополнительным разделам нет прямого доступа. Они состоят из одного или нескольких логических дисков и используются для хранения файлов. Деление дополнительных разделов на логические диски позволяет разделить физический диск более чем на четыре области. Можно, например, в одном дополнительном разделе создать логические диски F, G и H.

Динамическим называется физический диск с одним или несколькими динамическими томами. В отличие от основного диска, количество томов на динамическом диске не ограничено, и каждый из них может быть дополнительным или системным томом. Основные диски работают с любы-

ми выпусками ОС Windows, а динамические диски поддерживаются только в версиях не ранее Windows 2000. Например, если Disk 0 — динамический, его нельзя использовать в Windows 98.

Ранее ключевое преимущество динамических дисков заключалось в возможности объединять физические диски при помощи имеющихся в Windows функций составления, чередования или зеркалирования. Но в Windows 7 можно составлять, чередовать и зеркалировать и основные диски. При составлении или чередовании дисков создается один том, переходящий с одного диска на другой, в котором использует весь диск или только часть каждого диска в наборе. Различие между составлением и чередованием заключается в способе записи данных. В Windows 7 составные диски распознаются как один раздел, и операции записи на составной диск выполняются на всем разделе в случайном порядке. При чередовании данные по очереди записываются на каждый из дисков, составляющих том. В большинстве случаев чередование обеспечивает более быстрое выполнения чтения-записи, поскольку позволяет одновременно обращаться к нескольким дискам. Зеркалирование дисков заключается в создании одного отказоустойчивого тома из двух дисков. При отказе одного из томов набора остается доступным другой том, а сбойный том можно восстановить, не прерывая работы системы.

Внимание! С технической точки зрения диски с чередованием представляют собой избыточный массив независимых дисков (RAID) уровня 0 (RAID-0), а зеркальные диски — RAID уровня 1 (RAID-1). Зеркальные диски отказоустойчивы, чего нельзя сказать ни о чередующихся, ни о составных дисках, в которых ошибка на любом диске набора приводит к сбою всего тома.

В наши дни, когда для составления, чередования и создания зеркал подходят и основные диски, ключевое отличие динамических дисков от основных заключается в расширенных возможностях обнаружения и исправления ошибок, а также в возможности изменения дисков без перезагрузки компьютера. Другие доступные возможности зависят от файловой системы диска: FAT, FAT32 или NTFS.

В процессе форматирования диск разделяется на кластеры — логически объединенные группы секторов. В FAT, FAT32 и NTFS размер сектора постоянен и равен 512 байт, а размер кластера не регламентирован. Например, если размер кластера равен 4096 байт, то каждый кластер состоит из восьми секторов.

В табл. 12-1 приведена сводка стандартных размеров кластера для FAT16, FAT32, exFAT и NTFS. Создавая на диске файловую систему, вы вольны указать размер кластера или принять размер, предлагаемый по умолчанию. В любом случае, допустимые размеры кластера зависят от используемой файловой системы.

Ближе к реальности На платформах Windows применяется четыре файловые системы FAT: FAT12, FAT16, FAT32 и exFAT. Различие между FAT12, FAT16 и FAT32 заключается в количестве бит, используемых для записи в таблицах размещения фай-

лов, а именно 12, 16 или 32 бита. С точки зрения пользователя главное отличие файловых систем состоит в наибольшем допустимом объеме тома, который составляет 16 Мб для FAT12, 4 Гб для FAT16 и 2 Тб для FAT32. Если в обозначении FAT не указан номер, может подразумеваться как FAT16, так и FAT32. Новая версия FAT для съемных носителей называется Extended FAT, или exFAT. Она поддерживается в Windows Vista с Service Pack 1 и более поздними пакетами исправлений, Windows 7 и Windows Server 2008. В exFAT сохранена простота использования FAT32, но преодолен барьер в 4 Гб для размера файла и 32 Гб для тома. Поддерживаемый размер кластера в exFAT составляет до 32768 Кб. Особенность exFAT заключается в том, что ее можно легко использовать и перемещать между любыми совместимыми ОС. В этом exFAT превосходит FAT32.

Табл. 12-1. Стандартные размеры кластера для FAT16, FAT32, exFAT и NTFS

	Размер кластера			
Размер тома	**FAT16**	**FAT32**	**exFAT**	**NTFS**
7–16 Мб	512 байт	Не поддерживается	Не поддерживается	512 байт
7–32 Мб	512 байт	Не поддерживается	Не поддерживается	512 байт
33–64 Мб	1 Кб	512 байт	4 Кб	512 байт
65–128 Мб	2 Кб	1 Кб	4 Кб	512 байт
129–256 Мб	4 Кб	2 Кб	4 Кб	512 байт
257–512 Мб	8 Кб	4 Кб	32 Кб	512 байт
513–1024 Мб	16 Кб	4 Кб	32 Кб	1 Кб
1025 Мб – 2 Гб	32 Кб	4 Кб	32 Кб	2 Кб
2–4 Гб	64 Кб	4 Кб	32 Кб	4 Кб
4–8 Гб	Не поддерживается	4 Кб	32 Кб	4 Кб
8–16 Гб	Не поддерживается	8 Кб	32 Кб	4 Кб
16–32 Гб	Не поддерживается	16 Кб	32 Кб	4 Кб
32 Гб – 2 Тб	Не поддерживается	*	*	4 Кб

* Средства форматирования Windows имеют ограничение в 32 Гб. Создать тома большего размера можно при помощи инструментов сторонних производителей

Важно понимать, что кластеры являются минимальной единицей распределения дискового пространства. В одном кластере может находиться не более одного файла. Если вы создали файл размером 1 Кб, а размер кластера составляет 4 Кб, то в кластере останется 3 Кб свободного места, недоступного для других файлов. Если для размещения файла одного кластера

не хватило, остальные данные файла переходят в ближайший свободный кластер, затем в другой, пока файл не будет записан полностью. Например, в FAT в первом кластере файла есть указатель на второй кластер, а во втором кластере — указатель на следующий, и так далее до последнего занимаемого файлом кластера, в котором есть маркер конца файла (EOF).

Физической структурой дисков управляет дисковая подсистема ввода-вывода. Логической структурой дисков на уровне файловой системы управляет Windows. Под логической структурой понимаются основные и динамические тома, создаваемые на диске, и файловые системы, в которых они отформатированы. Как основные, так и динамические тома допускается форматировать в FAT или NTFS. У каждой файловой системы свои плюсы и минусы.

На одном компьютере основные и динамические диски могут сосуществовать, но диски, входящие в состав одного тома, должны быть однотипными. Например, если создать чередующийся том из дисков Disk 0 и Disk 1, которые были созданы в Windows NT 4.0, то их можно будет использовать в Windows 7. При изменении типа диска Disk 0 на динамический придется изменить также тип диска Disk 1. Преобразование основных дисков в динамические и обратно рассмотрено далее, в разделе «Преобразование основного диска в динамический и наоборот». Не забывайте, что преобразовать основной диск в динамический можно без потери данных, но при преобразовании динамического диска в основной придется удалить все разделы на динамическом диске. С удалением разделов теряются и все данные. Наконец, динамические диски невозможно создать на съемных носителях или накопителях портативных компьютеров. Диски ноутбуков, карманных ПК и пр. могут быть только основными.

Внимание! Работая с ноутбуками, будьте осторожны. Вид консоли Управление дисками (Disk Management) в некоторых из них создает впечатление, что основной диск можно преобразовать в динамический. Такое случается на компьютерах, не поддерживающих спецификации APM и ACPI. Может показаться, что на компьютере включена поддержка динамических дисков, но это не так. Попытка преобразовать основной диск в динамический на таком ноутбуке может привести к порче всего диска.

Примечание В динамические можно преобразовать некоторые внешние жесткие диски с интерфейсами FireWire, USB или eSATA. О том, как это сделать, написано в статье Базы знаний Microsoft 299598 «How To: Convert an IEEE 1394 Disk Drive to a Dynamic Disk Drive in Windows XP». Однако в этой статье недостаточно внимания уделяется мерам предосторожности. Внешний жесткий диск должен использоваться только на одном компьютере. Если в будущем может возникнуть необходимость подключить этот же диск к другому компьютеру, не выполняйте преобразование. Более того, прежде чем преобразовать любой внешний жесткий диск с интерфейсом FireWire или USB, создайте резервную копию данных. По возможности, сначала выполните преобразование на таком же диске, не содержащем важных данных, а затем проверьте работоспособность диска.

Применение основных и динамических дисков

В процессе использования основных и динамических дисков выполняется несколько типовых задач, например инициализация новых дисков, назначение диска активным или изменение типа диска. При этом, естественно, нужно понимать, что такое активный, загрузочный, системный диск и т. д.

Обозначения диска

Работая с основными и динамическими дисками, обращайте особое внимание на пять специальных типов разделов на дисках MBR.

- **Активен (Active)** Активный раздел или том — это раздел диска, служащий для запуска компьютеров на базе x86. Если на компьютере установлено несколько ОС, в активном разделе диска должны содержаться загрузочные файлы выбранной вами ОС, и он должен быть основным разделом на основном диске или простом томе динамического диска. Обычно в консоли Управление дисками (Disk Management) активный раздел никак особо не отмечен. В большинстве случаев это основной раздел или первый простой том на диске Disk 0. Метка Активен (Active) появляется при изменении стандартной конфигурации.

Внимание! Не путайте состояние Активен (Active) съемного носителя с меткой Активен (Active) активного раздела. Состояние Активен (Active) приписывается устройствам чтения карт памяти CompactFlash и пр., когда в них вставлен носитель. Иногда обозначение Disk 0 приписывается съемному носителю. В этом случае ищите активный раздел на первом по номеру физическом жестком диске. Например, если на компьютере установлены диски Disk 0, Disk 1, Disk 2, и первым физическим диском в последовательности является Disk 1, наиболее вероятно, что активный раздел находится на первом основном разделе или простом томе диска Disk 1.

- **Система (System)** На системном разделе или томе находятся файлы начальной загрузки для конкретного оборудования, которые нужны для загрузки ОС. Системный раздел или том может быть зеркальным, но не может быть частью составного или чередующегося тома. В консоли Управление дисками (Disk Management) метка системного раздела отображается в графическом представлении и в поле **Состояние (Status)** представления Список томов (Volume List).
- **Загрузка (Boot)** Загрузочный раздел или том, содержащий ОС и файлы для ее поддержки. Загрузочный раздел или том может быть зеркальным, но не может являться частью составного или чередующегося тома. В большинстве систем системный и загрузочный разделы (тома) совпадают. Как и активный, загрузочный раздел обычно особо не отмечен в утилите Управление дисками (Disk Management). В большинстве случаев, загрузочным является основной раздел или первый простой том диска Disk 0. Если ОС установлена в другом разделе или томе, метка Загрузка (Boot) отображается.

- **Файл подкачки (Page file)** Раздел или том, на котором содержится файл подкачки. В зависимости от конфигурации виртуальной памяти она может выгружаться на несколько дисков, а значит, на компьютере может быть несколько разделов и томов с файлом подкачки. Тем не менее, в зависимости от настроек сведения о файле подкачки могут отображаться только для основного тома. Подробнее об использовании и настройке файлов подкачки — в главе 6.
- **Аварийный дамп памяти (Crash dump)** Раздел или том, в который производится попытка записи файлов дампа в случае «падения» системы. Как отмечалось в главе 6, файлы дампа используются для диагностики причин сбоя системы. По умолчанию они записываются в папку %SystemRoot%, но их можно разместить в любом разделе или томе.

На каждом компьютере есть один активный, один системный, один загрузочный и один аварийный раздел или том. Причем, эти разделы и тома могут совпадать. Обозначение файла подкачки — единственное, которое может наличествовать на нескольких разделах или томах.

Установка и инициализация новых физических дисков

В Windows 7 существенно упростился процесс добавления на компьютер новых физических дисков. Установив диск согласно инструкции производителя, войдите в систему и откройте оснастку Управление дисками (Disk Management). Если новые диски уже были инициализированы, у них уже есть подписи дисков, которые позволяют выполнять чтение и запись. Для автоматического подключения дисков выберите в меню **Действие (Action)** команду **Повторить проверку дисков (Rescan Disks)**. Если вы установили новый диск, не прошедший инициализацию и не имеющий подписи, для обнаружения диска откроется мастер Инициализация дисков (Initialize And Convert Disk Wizard).

Для инициализации диска в мастере Инициализация дисков (Initialize And Convert Disk Wizard) выполните следующие действия:

1. На странице приветствия щелкните **Далее (Next)**. На странице **Выбор диска для инициализации (Select Disks To Initialize)** добавленные диски выбраны для инициализации автоматически. Если вы не хотите инициализировать тот или иной диск, сбросьте соответствующий флажок.
2. Щелкните **Далее (Next)**, чтобы перейти на страницу **Выбор дисков для преобразования (Select Disks To Convert)**. Здесь перечислены новые диски, а также все диски, не относящиеся к системе или загрузке, которые можно преобразовать. По умолчанию новые диски не выбраны. Чтобы преобразовать диски, выберите их и щелкните **Далее (Next)**.
3. На заключительной странице отображены заданные вами параметры, а также действия, которые будут выполнены для каждого из дисков. Если все указано правильно, щелкните **Далее (Next)**. После этого будут выполнены выбранные действия. При инициализации на диск будет запи-

сана подпись. Если выбрано также преобразование диска, после инициализации диск будет преобразован в динамический.

Можно, впрочем, обойтись и без мастера. Закройте мастер, оставаясь в оснастке Управление дисками (Disk Management). В представлении Список дисков (Disk List) новый диск отмечен красным значком с восклицательным знаком, а состояние диска отмечено словами **Не проинициализирован (Not Initialized)**. Щелкните правой кнопкой значок диска и выберите команду **Инициализировать диск (Initialize Disk)**. Подтвердите выбор (и добавьте другие диски, доступные для инициализации) и щелкните **OK**, чтобы начать инициализацию диска. Преобразование в динамический диск будет обсуждаться в разделе «Преобразование основного диска в динамический и наоборот».

Изменение таблицы разделов диска

Таблицу разделов можно преобразовать из MBR в GPT и наоборот. Такое изменение может понадобиться при перемещении дисков на компьютер с другой архитектурой процессора или при обновлении формата дисков. Преобразовать таблицу разделов можно только на пустом диске, либо новом, либо только что отформатированном. Разумеется, всегда можно очистить диск, удалив содержащиеся на нем разделы или тома.

Изменить вид таблицы разделов можно при помощи программ Управление дисками (Disk Management) и DiskPart. Чтобы сменить стиль раздела на пустом диске при помощи программы Управление дисками (Disk Management), щелкните значок диска в графическом представлении правой кнопкой и выберите нужную команду: **Преобразовать в GPT-диск (Convert To GPT Disk)** или **Преобразовать в MBR-диск (Convert To MBR Disk)**.

Чтобы изменить стиль раздела на пустом диске при помощи утилиты DiskPart, введите команду **diskpart**, а затем выберите диск, который нужно преобразовать. Например, чтобы преобразовать диск Disk 2, введите команду select disk 2. Затем выполните преобразование из MBR в GPT при помощи команды **convert gpt**. Чтобы преобразовать GPT-диск в MBR-диск, выполните **convert mbr**.

Назначение раздела активным

Как правило, изменять тип раздела не требуется. Если на компьютере установлена только Windows 7 или среди вариантов загрузки есть Windows 7 и другая версия ОС семейства Windows, смена активного раздела вам не понадобится. На компьютерах с архитектурой x86 активный раздел — это, как правило, основной раздел или первый простой том на диске Disk 0. Если на диске C установлена Windows 7, а на другом разделе, скажем, диске D — Windows 2000 или более поздняя версия, для загрузки Windows 7 и другой ОС менять активный раздел не нужно. Однако, чтобы обеспечить загрузку ОС, отличной от Windows, необходимо пометить раздел этой ОС как активный и перезагрузить компьютер.

Примечание Активным может быть только основной раздел. Логические диски нельзя сделать активными. Также нельзя сделать активными тома. При обновлении основного диска, содержащего активный раздел, до динамического, раздел становится простым томом, автоматически активным.

Чтобы сделать раздел активным, выполните следующие действия:

1. Убедитесь, что в основном разделе, который предполагается сделать активным, есть необходимые загрузочные файлы. Для Windows NT, Windows 2000 и Windows XP это файлы Boot.ini, Ntdetect.com, Ntldr и Bootsect.dos, а также, возможно, файл Ntbootdd.sys.
2. Откройте консоль Управление компьютером (Computer Management): в командной строке с повышенными полномочиями введите **diskmgmt.msc**.
3. Правой кнопкой щелкните основной раздел, который нужно сделать активным, и выберите команду **Сделать раздел активным (Mark Partition As Active)**.

Внимание! В программе Управление дисками (Disk Management) преобразование раздела или тома в активный может не удастся. В результате после перезапуска компьютера ОС может не загрузиться. Единственный найденный мною выход — использовать для внесения изменений утилиту DiskPart либо перед перезагрузкой, либо до применения средства Восстановление запуска (Startup Repair) после неудачного запуска.

В листинге 12-1 приведен пример создания активного раздела в утилите DiskPart. Как следует из листинга, после начального запуска DiskPart выводится имя и версия программы DiskPart, а также имя компьютера. Далее необходимо выбрать нужный диск и вывести список его разделов. В нашем примере это Disk 0. Мы выводим список его разделов, а затем выбираем для работы раздел Partition 1. Теперь, чтобы сделать раздел активным, достаточно ввести команду **Active**. Завершив работу, закройте DiskPart при помощи команды **Exit**.

Примечание В данном примере выбран диск Disk 0. В вашей системе этим диском может оказаться другой диск. Чтобы просмотреть список доступных дисков и выбрать из них нужный, выберите команду **List Disk**.

Листинг 12-1. Установка активного раздела в среде команды DiskPart

```
C:>diskpart

Microsoft DiskPart версии 6.1.7200
(C) Корпорация Майкрософт 1999-2008.
На компьютере: ENGPC85

DISKPART> select disk 0

Выбран диск 0.
DISKPART> list partition
```

```
  Раздел ###  Тип              Размер     Смещение
  ---------  ----------------  -------    -------
  Раздел 1    Основной           932 Gб   1024 Кб

DISKPART> select partition 1

Выбран раздел 2.

DISKPART> active

DiskPart: раздел помечен как активный.

DISKPART> exit
```

Преобразование основного диска в динамический и наоборот

Проще всего для преобразования основного диска в динамический и обратно использовать оснастку Управление дисками (Disk Management). После обновления до динамического диска разделы автоматически становятся томами соответствующего типа: основные разделы и логические диски дополнительного раздела становятся простыми томами. Неиспользуемое (свободное) пространство дополнительного раздела помечается как нераспределенное (Unallocated). А вот превратить тома обратно в разделы уже нельзя. Для этого потребуется удалить тома на динамическом диске и только после этого изменить тип диска обратно на основной. Удаление томов влечет за собой удаление всей информации на диске.

Перед преобразованием основного диска в динамический убедитесь, что вам не потребуется загружать компьютер при помощи предыдущих версий Windows. Кроме того, в конце диска необходимо оставить 1 Мб свободного места. При создании разделов и томов в оснастке Управление дисками (Disk Management) этот объем свободного пространства резервируется автоматически, но нет гарантии, что так же поступают инструменты для работы с дисками в других ОС. Это может стать причиной сбоя преобразования. Следует также знать о следующих ограничениях:

- Нельзя преобразовать в динамические диски съемные носители. Они могут быть только основными дисками с основными разделами.
- Допускается преобразование несистемных и незагрузочных разделов, которые являются частью составных или чередующихся томов. Такие тома становятся динамическими с сохранением типа. При этом необходимо преобразовывать все диски набора.

Чтобы преобразовать основной диск в динамический, выполните следующие действия:

1. В оснастке Управление дисками (Disk Management) в представлении **Список дисков (Disk List)** или на левой панели графического представления, щелкните правой кнопкой основной диск, который нужно пре-

образовать, и выберите команду **Преобразовать в динамический диск (Convert To Dynamic Disk)**.

2. В диалоговом окне **Преобразование в динамические диски (Convert To Dynamic Disk)** установите флажки для дисков, которые нужно преобразовать (рис. 12-5). При обновлении чередующегося тома, созданного в Windows NT, обязательно выберите все основные диски набора, так как набор необходимо преобразовывать одновременно.

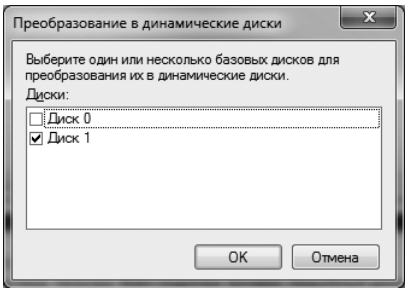

Рис. 12-5. Основной диск выбран для преобразования

3. Если на преобразуемом диске нет отформатированных томов, пропустите оставшиеся шаги, и щелкните **OK**, чтобы преобразовать диск. Если на преобразуемом диске есть отформатированные тома, щелкнув **OK**, вы откроете диалоговое окно **Диски для преобразования (Disks To Convert)**.
4. Подтвердите преобразование выбранных дисков. Обратите внимание на столбец **Будет преобразован (Will Convert)**. Если диск удовлетворяет условиям преобразования, в столбце должно стоять **Да (Yes)**. Просмотрите тома на выбранном диске, щелкнув **Сведения (Details)**. Для продолжения щелкните **OK** в диалоговом окне **Сведения о преобразовании (Convert Details)**.
5. Чтобы начать преобразование, щелкните **Преобразовать (Convert)**. На экране появится предупреждение о том, что после преобразования выбранного диска загрузить предыдущие версии Windows, содержащиеся в его томах, будет невозможно. Щелкните **Да (Yes)**.
6. На экране появится предупреждение о том, что файловая система преобразуемых дисков будет отключена, то есть они будут временно отключены и доступ к ним будет закрыт. Щелкните **Да (Yes)**. Если на выбранном диске есть загрузочный или системный раздел, либо раздел, используемый в данный момент, потребуется перезапустить компьютер.

Чтобы преобразовать динамический диск в основной, выполните следующие действия:

1. Чтобы сделать динамический диск основным, удалите все динамические тома на диске. Тем самым вы уничтожите все данные томов, поэтому сделайте их резервные копии.

2. Подготовившись к процессу преобразования, откройте оснастку Управление дисками (Disk Management), щелкните правой кнопкой преобразуемый диск и выберите команду **Преобразовать в основной диск (Convert To Basic Disk)**. Динамический диск будет преобразован в основной, где вы впоследствии сможете создать новые разделы и логические диски.

Диски, разделы и тома

Прежде чем хранить данные на физическом диске, его необходимо подготовить: задать тип диска, поделить на разделы, назначить указатель диска, отформатировать разделы и тома.

Создав на диске разделы, назначьте для всех разделов и томов указатель диска — букву или путь. Для доступа к файловым системам на разделах физических дисков используются буквы диска, как правило, от A до Z. Буква A обычно назначается дисководу для гибких дисков. Буква B обычно назначается второму дисководу, другому устройству со съемным носителем или остается неназначенной. Буква C обычно назначается первому разделу тома на диске Disk 0, а буква D — первому CD - или DVD-дисководу. Таким образом, в большинстве систем доступны буквы от E до Z. Если нужно создать больше томов, используют пути к дискам.

Путь к диску задается как расположение папки на существующем локальном диске. Вы, например, можете подключить дополнительные диски как папки C:\Docs1, C:\Docs2 и C:\Docs3. Пути к дискам используются как для основных, так и для динамических дисков. Единственное ограничение для путей к дискам состоит в том, что они подключаются только к пустым папкам, расположенным на локальных дисках, отформатированных в NTFS.

При форматировании раздела или тома определяется файловая система, и создаются необходимые структуры файлов. Как правило, вы форматируете раздел или том в системе FAT, FAT32 или NTFS. У каждой из этих систем есть ограничения и специфические требования.

Файловая система FAT, известная так же, как FAT16, — это 16-разрядная файловая система, предназначена для томов размером до 4 Гб. В FAT имеется загрузочный сектор, где хранится информация о типе диска, начальном и конечном секторах и активном разделе. Аббревиатурой FAT обозначена таблица размещения файлов (File Allocation Table), в которой хранятся расположения кластеров файлов и папок. Существуют основная и резервная таблицы. Резервная таблица нужна для восстановления основной в случае ее повреждения. В FAT есть возможность помечать кластеры как неиспользуемые, используемые, поврежденные или резервные. Благодаря этому файловая система FAT достаточно надежна. Лучше всего FAT подходит для томов размером до 2 Гб и накладывает ограничение на максимальный размер файла — также 2 Гб. Кроме того, FAT применяется на гибких и съемных дисках.

Файловая система FAT32 представляет собой 32-разрядную версию FAT, наделенную дополнительными функциями и возможностями. Как и в FAT16,

в FAT32 есть основная и резервная таблицы размещения файлов, а кластеры так же помечаются как неиспользуемые, используемые, поврежденные или зарезервированные. Она тоже применяется на гибких и съемных дисках. Минимальный размер тома в FAT32 составляет 33 Мб, а максимальный — 32 Гб, наибольший размер файла — 4 Гб. Отсюда следует, что FAT32 предназначена для значительно больших разделов и томов, чем FAT16.

Примечание Ограничение на размер файла и тома в FAT32 распространяются только на Windows 2000 и последующие версии Windows. В более ранних версиях Windows, а также в других ОС, при помощи FAT32 можно создавать и более объемные тома.

Файловая система NTFS сильно отличается от FAT16 и FAT32. В ней информация о файлах и папках хранится не в таблице размещения файлов, а в реляционной БД MFT (master file table). В ней хранятся записи обо всех файлах и папках тома, а также дополнительные сведения для обслуживания тома. В целом, именно благодаря MFT система NTFS гораздо более надежна, чем FAT16 и FAT32. При возникновении ошибок на диске NTFS восстанавливается быстрее, чем FAT16 и FAT32, и неисправностей на диске с NTFS случается, как правило, меньше.

Максимальный размер тома для NTFS составляет 2 Тб и даже больше (в зависимости от конфигурации тома), а наибольший размер файла ограничен только размером тома. На гибких дисках NTFS использовать нельзя, а вот на съемных дисках — можно. И еще, в отличие от FAT16 и FAT32, возможности которых по части безопасности ограничены (файлы помечаются как файлы только для чтения, скрытые или системные), NTFS обладает дополнительной системой безопасности, позволяющей управлять доступом к файлу или папке на основе разрешений. В NTFS также поддерживается много других возможностей, включая сжатие, шифрование и дисковые квоты.

Примечание Реализовано несколько версий NTFS. Система NTFS 4 увидела свет вместе с Windows NT, NTFS 5 — с Windows 2000, NTFS 5.1 — с Windows XP. Поскольку на современных компьютерах используется NTFS 5 и более поздние версии, за основу для этой книги взяты именно они. При модернизации системы со старой версией NTFS вам будет предложено обновить существующие тома до последней версии NTFS. В большинстве случаев это следует сделать, поскольку таким образом вы обеспечите поддержку новейших возможностей NTFS.

Создание и подготовка разделов

Основной инструмент для создания разделов на дисках и их подготовки к использованию — оснастка Управление дисками (Disk Management). Она позволяет делить диски на разделы, назначать указатели дисков, а также форматировать разделы и тома. Аналогичную функциональность в командной строке предоставляют утилита DiskPart, предназначенная для создания разделов и назначения указателя диска, и утилита Format, используемая при форматировании.

Создание разделов, логических дисков и простых томов

В Windows 7 интерфейс оснастки Управление дисками (Disk Management) упростился. В нем используется один набор диалоговых окон и мастеров как для разделов, так и для томов. Первые три тома основного диска автоматически создаются как основные разделы. При попытке создать на основном диске четвертый том оставшееся свободное пространство автоматически преобразуется в дополнительный раздел с логическим диском заданного вами размера. Все последующие тома автоматически создаются в дополнительных разделах и логических дисках.

Примечание Как известно, на MBR-диске может быть четыре основных раздела. Однако после создания четвертого основного раздела дальнейшее разделение диска станет невозможно, поэтому в Windows 7 автоматически создается дополнительный раздел. Дополнительный раздел позволяет создать несколько логических дисков.

В оснастке Управление дисками (Disk Management) разделы, логические диски и простые тома создаются следующим образом:

1. В графическом представлении оснастки Управление дисками (Disk Management) щелкните правой кнопкой неразмеченную область и выберите команду **Создать простой том (New Simple Volume)**. Откроется Мастер создания простого тома (New Simple Volume Wizard). Прочитав приветственную страницу, щелкните **Далее (Next)**.
2. На странице **Указание размера тома (Specify Volume Size)** приведены наименьший и наибольший размеры тома (Мб). Задайте размер тома в этих пределах (рис. 12-6), введя значение в поле **Размер простого тома (Simple Volume Size)**, и щелкните **Далее (Next)**.

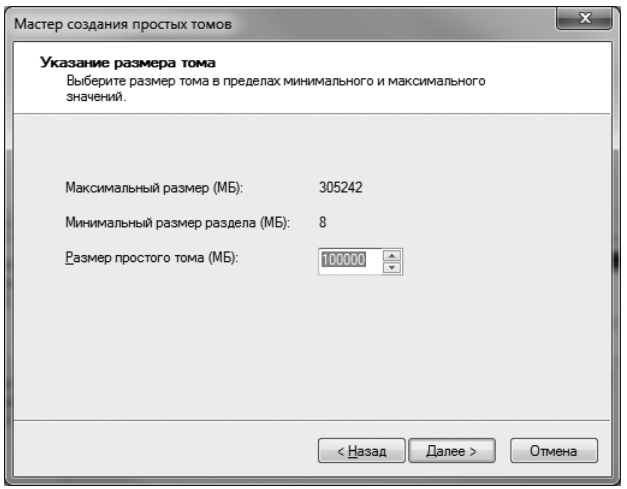

Рис. 12-6. Укажите размер тома

3. На странице **Назначение буквы диска или пути (Assign Drive Letter Or Path)**, показанной на рис. 12-7, укажите букву диска или путь и щелкните **Далее (Next)**. Возможны следующие варианты:

- **Назначить букву диска (Assign The Following Drive Letter)** Выберите в списке доступную букву. По умолчанию указана первая доступная буква диска. Исключены зарезервированные буквы, а также буквы, назначенные локальным и сетевым дискам.
- **Подключить том как пустую NTFS-папку (Mount In The Following Empty NTFS Folder)** Подключение тома как пустой NTFS-папки. Выбрав ее, введите путь к существующей папке или создайте папку, щелкнув кнопку **Обзор (Browse)**.
- **Не назначать буквы диска или пути диска (Do Not Assign A Drive Letter Or Drive Path)** Этот вариант выбирают, когда нужно создать раздел, не назначая буквы диска или пути. Это можно будет сделать позже.

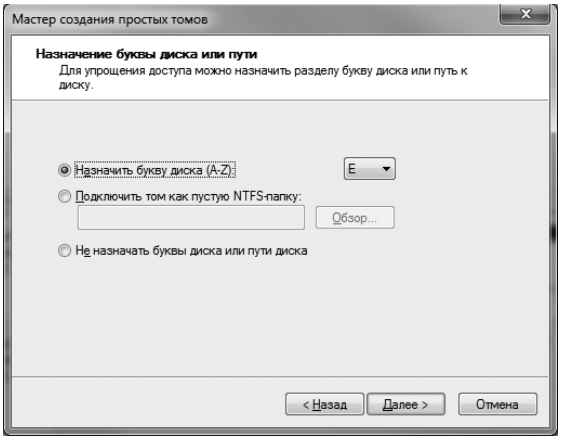

Рис. 12-7. Назначьте указатель диска сейчас или отложите это действие

Примечание Назначать букву диска или путь для тома совсем не обязательно. Том, не имеющий указателей, не подключен и, по сути, не используется. Позже вы сможете подключить отключенный том, назначив ему букву диска или путь, как описано далее в этой главе.

4. На странице **Форматирование раздела (Format Partition)** укажите, как форматировать том и нужно ли это делать (рис. 12-8). Чтобы отформатировать том, щелкните **Форматировать этот том следующим образом (Format This Volume With The Following Settings)**, а затем настройте следующие параметры:
   - **Файловая система (File System)** Указание типа файловой системы: FAT, FAT32 или NTFS. В большинстве случаев, по умолчанию выбрана NTFS. Отформатировав том в FAT или FAT32, позже вы сможете преобразовать файловую систему в NTFS при помощи утилиты Convert. Однако преобразовать раздел NTFS в FAT или FAT32 не удастся.
   - **Размер кластера (Allocation Unit Size)** Задание размера кластера файловой системы — основной единицы распределения дискового

пространства. Стандартное значение размера кластера зависит от размера тома и по умолчанию определяется динамически перед форматированием. Чтобы отменить такое поведение, задайте размер кластера вручную. Для небольших по размеру файлов лучше установить небольшой размер, например 512 или 1024. При этом небольшие файлы занимают меньше места.

- **Метка тома (Volume Label)** Текстовая метка тома, по умолчанию Новый том (New Volume). Изменить метку тома можно в любое время. Для этого в Проводнике (Windows Explorer) щелкните том правой кнопкой, выберите команду **Свойства (Propeties)** и введите новое значение в соответствующем поле на вкладке **Общие (General)**.
- **Быстрое форматирование (Perform A Quick Format)** Форматирование без проверки разделов на наличие ошибок. При работе с большими разделами это сэкономит вам несколько минут, но проверку все же лучше выполнить. При этом поврежденные сектора на диске помечаются и блокируются.
- **Применять сжатие файлов и папок (Enable File And Folder Compression)** Включение сжатия на диске. Встроенное сжатие доступно только в NTFS. Оно выполняется прозрачно для пользователей, и доступ к сжатым файлам не отличается от доступа к обычным файлам. При выборе данного параметра файлы и папки на данном диске сжимаются автоматически. Подробнее о сжатии дисков, файлов и папок читайте далее в разделе «Сжатие дисков и данных».

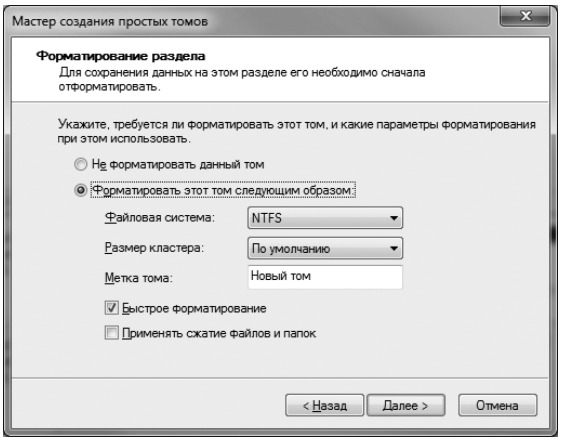

Рис. 12-8. Укажите параметры форматирования раздела

5. Щелкните **Далее (Next)**, проверьте значения параметров и щелкните **Готово (Finish)**.

Создание составных и чередующихся томов

Вы можете создать единый том, расположенный на нескольких дисках. При этом имейте в виду следующее:

- Для составного тома используется свободное пространство на нескольких однотипных дисках. Если вы располагаете свободным местом на двух или нескольких дисках одного типа, вы вольны объединить это пространство в составной том. Он не является отказоустойчивым и обладает умеренной скоростью чтения-записи. Файлы записываются на весь составной том в случайном порядке. В случае сбоя одного диска из строя выходит весь том с потерей всех данных.
- Для чередующегося тома используется свободное пространство на нескольких дисках с чередованием записи данных. Чередование обеспечивает более быстрый доступ для чтения-записи данных, так как чтение и запись данных выполняются на несколько дисков. Например, в чередующийся том, состоящий из трех дисков, данные из файла записываются сначала на диск 1, затем на диск 2, а затем на диск 3 блоками по 64 Кб. Как и составной том, чередующийся том не обладает отказоустойчивостью, поэтому при сбое любого из дисков выходит из строя весь том с потерей данных.

Примечание Если у вас в наличии только один диск, вам не удастся создать ни составной, ни чередующийся том. Размер простых и составных томов можно увеличить, расширив их. Чередующиеся тома расширить нельзя. Поэтому, создавая чередующийся том, хорошо запланируйте его размер, чтобы чередующийся том не пришлось удалять и создать заново.

Чтобы создать составной или чередующийся том в оснастке Управление дисками (Disk Management), выполните следующие действия:

1. В графическом представлении оснастки Управление дисками (Disk Management) щелкните правой кнопкой неразмеченную область и выберите команду **Создать составной том (New Spanned Volume)** или **Создать чередующийся том (New Striped Volume)**. После прочтения приветственной страницы щелкните **Далее (Next)**. В Windows 7 поддерживается составление и чередование основных дисков, но некоторые основные диски не подходят для объединения и чередования.
2. На странице **Выбор дисков (Select Disks)** отметьте диски, которые войдут в том, и укажите размер сегментов тома на этих дисках (рис. 12-9). Диски должны быть одного типа — основными или динамическими. Щелкните **Далее (Next)**.

   Доступные диски перечислены в списке **Доступны (Available)**. Выделите диск и щелкните **Добавить (Add)**, чтобы добавить диск в список **Выбраны (Selected)**. Чтобы убрать диск из списка **Выбраны (Selected)**, выделите его и щелкните **Удалить (Remove)**.

   Задайте пространство, которое следует использовать на каждом диске, выбирая диски в списке **Выбраны (Selected)** и указывая необходимый объем в поле **Выберите размер выделяемого пространства (Select The Amount Of Space In MB)**. В поле **Максимальное доступное пространство (Maximum)** отображена наибольшая свободная область на выбран-

ном диске, а в поле **Общий размер тома (Total Volume Size)** показано общее дисковое пространство, выделенное для диска в данный момент.

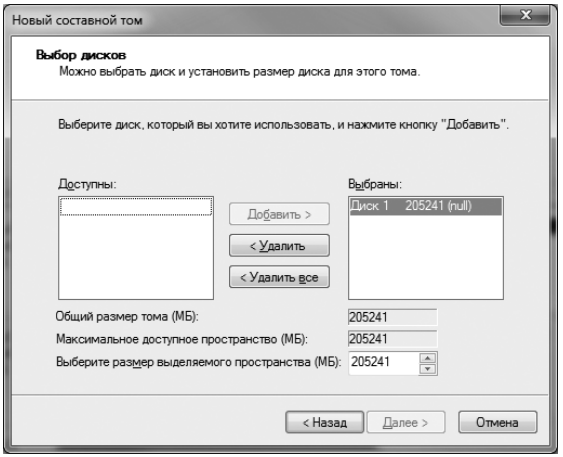

Рис. 12-9. Укажите объем, который следует использовать на каждом томе

Совет Есть способ быстро указать один и тот же объем для всех выбранных дисков. Выделите все диски: нажмите Shift и щелкните первый и последний диск в списке **Выбраны (Selected)**. Теперь укажите объем для всех выбранных дисков.

3. Выполните шаги 3–5 из предыдущего раздела.

Сжатие и расширение томов

Загрузка Windows 7 обходится без файлов Ntldr и Boot.ini. Вместо них применяется предзагрузочная среда, в которой управление запуском выбранного приложения загрузки осуществляется в Диспетчере загрузки Windows (Windows Boot Manager). Диспетчер загрузки — олицетворение независимости ОС Windows от MS-DOS — предоставляет новые способы использования дисков. В Windows 7 вы можете расширять и сжимать основные и динамические диски при помощи программ Управление дисками (Disk Management) и DiskPart. Сжимать и расширять чередующиеся тома невозможно.

При расширении тома происходит преобразование областей неразмеченного пространства и их добавление к существующему тому. Пространство для составных томов на динамических дисках можно взять на любом доступном динамическом диске, а не только на диске, на котором том был создан первоначально. Это позволяет объединять свободное пространство нескольких динамических дисков, увеличивая размер существующего тома.

Внимание! Приступая к расширению тома, помните о некоторых ограничениях. Первое: расширению подлежат только простые и сжатые тома, отформатированные в NTFS. Нельзя расширить чередующийся том, а также неформатированные тома или тома, отформатированные в FAT или FAT32. Кроме того, нельзя расширить системный или загрузочный том независимо от его конфигурации.

Чтобы сжать основной, простой или составной том, выполните следующие действия:

1. В оснастке Управление дисками (Disk Management) щелкните правой кнопкой диск, который нужно сжать, и выберите команду **Сжать том (Shrink Volume)**. Команда доступна, только если том удовлетворяет приведенным выше критериям.
2. Укажите объем сжатия в диалоговом окне **Сжать (Shrink)**, показанном на рис. 12-10. В этом диалоговом окне указана следующая информация:
   - **Общий размер до сжатия (Total Size Before Shrink)** Полный объем тома (Мб). Это форматированный размер тома.
   - **Доступное для сжатия пространство (Size Of Available Shrink Space)** Наибольший объем, на который можно сжать том. Параметр не отражает общего объема свободного места на томе. Это объем, который можно освободить, за исключением данных, зарезервированных для основной таблицы файлов, снимков тома, файлов подкачки и временных файлов.
   - **Размер сжимаемого пространства (Enter The Amount of Space To Shrink)** Общий объем, на который будет сжат том. Первоначальное значение, указанное по умолчанию, — это наибольший объем, на который можно сжать том. Для оптимальной производительности на томе после сжатия должно оставаться не менее 10% свободного пространства.
   - **Общий размер после сжатия (Total Size After Shrink)** Общий объем тома (Мб), который получится после сжатия. Это новый форматированный размер тома.

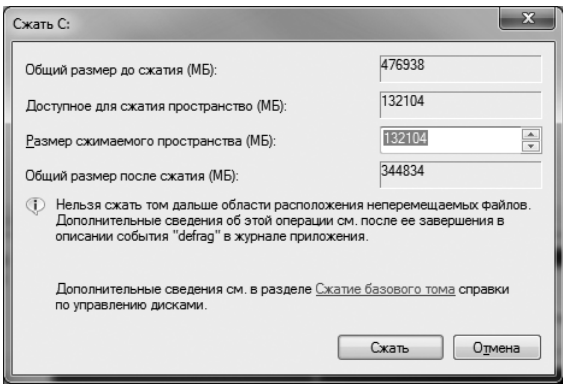

Рис. 12-10. Определите объем, на который нужно сжать том

3. Щелкните **Сжать (Shrink)**.

Чтобы расширить основной, простой или составной том, выполните следующие действия:

1. В оснастке Управление дисками (Disk Management) щелкните правой кнопкой диск, который нужно расширить, и выберите команду **Расши-**

рить том (Extend Volume). Команда доступна, если том удовлетворяет приведенным выше критериям и на одном или нескольких дисках есть свободное пространство.

2. Прочитайте вводное сообщение в Мастере расширения тома (Extend Volume Wizard) и щелкните **Далее (Next)**.
3. На странице **Выбор дисков (Select Disks)**, показанной ранее на рис. 12-9, выберите диск или диски, пространство которых хотите задействовать. Все диски, используемые томом в данный момент, будут выбраны автоматически. По умолчанию на этих дисках будет выбрано все свободное место.
4. Чтобы включить дополнительное пространство с других дисков, выполните следующие действия:
   - В списке **Доступны (Available)** выделите диск и щелкните **Добавить (Add)**, чтобы переместить диск в список **Выбраны (Selected)**.
   - В списке **Выбраны (Selected)**, выделяя каждый из дисков, укажите в поле **Выберите размер выделяемого пространства (Select The Amount Of Space)** объем неразмеченного пространства, который следует использовать.
5. Щелкните **Далее (Next)**, проверьте значения параметров и щелкните **Готово (Finish)**.

Форматирование разделов и томов

При форматировании раздела или тома создается файловая система, которую можно будет использовать для хранения данных. При этом существующие данные в соответствующем разделе физического диска удаляются без возможности восстановления. Создание файловой структуры называется *высокоуровневым форматированием*, а инициализация диска для использования — *низкоуровневым форматированием*. Чтобы отформатировать раздел или том, щелкните его правой кнопкой в оснастке Управление дисками (Disk Management) и выберите команду **Форматировать (Format)**. Откроется диалоговое окно **Форматирование (Format)**, показанное на рис. 12-11. Если сравнить рис. 12-11 и 12-8, нетрудно заметить, что поля окон, показанных на этих рисунках, совпадают.

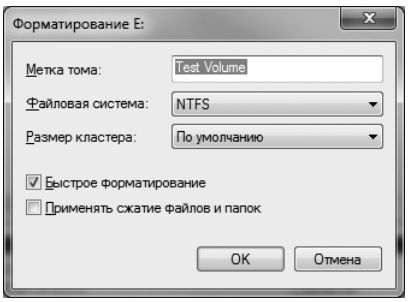

Рис. 12-11. Форматирование раздела или тома в диалоговом окне Форматирование (Format)

Задав нужные значения параметров, щелкните **OK**. При форматировании раздела все существующие данные будут удалены, поэтому вам предоставляется последний шанс остановить процедуру. Щелкните **OK**, чтобы начать форматирование. После этого произойдет изменение состояния диска, отражающее процесс форматирования, и будет показан ход выполнения процесса, если не установлен флажок **Быстрое форматирование (Perform A Quick Format)**. По завершению форматирования информация о состоянии диска будет соответственно обновлена.

Назначение, изменение и удаление букв дисков и путей

Каждому основному разделу, логическому диску или тому на компьютере назначается одна буква диска и один или несколько путей к диску, при условии что пути к дискам задаются для пустых NTFS-папок. Назначенная буква диска или путь остаются неизменными при каждом запуске компьютера. Назначенные буквы дисков и пути всегда можно изменить (за исключением системных или загрузочных разделов и томов). Кроме того, назначенную букву диска или путь к диску можно удалить (опять же за исключением системных или загрузочных разделов).

Примечание Чтобы изменить букву или путь системного или загрузочного тома, нужно отредактировать реестр. Эта процедура для Windows 2000 описана в статье 223188 Базы знаний Microsoft. В Windows 7 процедура точно такая же. Однако помните: если во время процедуры что-то пойдет не так, возможно, систему загрузить не удастся, и восстанавливать ее придется из резервной копии.

Для управления буквами дисков или путями откройте оснастку Управление дисками (Disk Management). В представлении Список томов (Volume List) или графическом представлении щелкните правой кнопкой нужный раздел или том и выберите команду **Изменить букву диска или путь к диску (Change Drive Letter And Paths)**. Откроется диалоговое окно, показанное на рис. 12-12. В нем вы можете выполнить следующие действия:

- **Добавить путь к диску** Щелкните **Добавить (Add)**, установите переключатель **Подключить том как пустую NTFS-папку (Mount In The Following Empty NTFS Folder)** и введите путь к существующей папке. Чтобы найти или создать папку, щелкните кнопку **Обзор (Browse)**.
- **Удалить путь к диску** Выберите путь к диску, который нужно удалить, щелкните **Удалить (Remove)** и **Да (Yes)**.
- **Назначить букву диска** Щелкните **Добавить (Add)**, установите переключатель **Назначить букву диска (Assign The Following Drive Letter)** и выберите доступную букву.
- **Изменить букву диска** Выделите текущую букву диска и щелкните **Изменить (Change)**. Щелкните **Назначить букву диска (Assign The Following Drive Letter)** и укажите для диска другую букву.
- **Удалить букву диска** Выделите текущую букву диска, щелкните **Удалить (Remove)** и **Да (Yes)**.

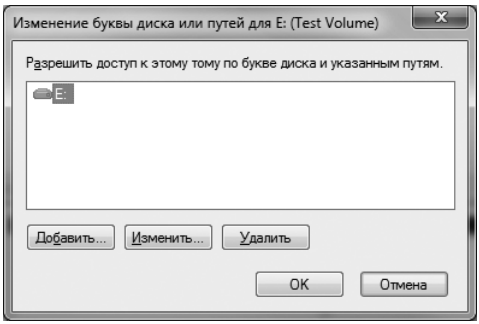

Рис. 12-12. Диалоговое окно для изменения и удаления буквы или пути диска

Примечание При попытке изменить букву диска, используемого в данный момент, вы получите предупреждение об этом. Закройте все программы, использующие диск, и повторите попытку или переименуйте диск принудительно, щелкнув **Да (Yes)**.

Ближе к реальности Если нужная буква диска недоступна, она уже используется или зарезервирована для другой цели. Иногда для достижения намеченной цели необходимо поменять буквы местами. Например, если буква D используется устройством CD-ROM, а буква E — локальным диском, буквы можно поменять, так что D будет соответствовать локальному диску, а E — устройству CD-ROM. Удалите букву диска, назначенную CD-ROM, освободив букву D. Затем назначьте букву D локальному диску, освободив букву E для CD-ROM. Не забывайте о последствиях, к которым может привести изменения буквы диска. Например, букву диска может содержать записанный в реестре путь к приложению. После изменения буквы этот путь станет недействительным. Также изменение буквы диска затронет ярлыки файлов и программ, которые придется создавать заново.

Назначение, изменение и удаление метки тома

Метка тома — это его краткое текстовое описание. Она отображается при обращении к диску из различных утилит Windows 7, например программ Проводник (Windows Explorer) и Компьютер (Computer), и предназначена для дополнительной характеристики содержимого диска.

Примечание В FAT и FAT32 метка тома не может быть длиннее 11 символов с пробелами. В NTFS длина метки тома ограничена 32 символами. В FAT и FAT32 нельзя использовать в метке тома некоторые специальные символы, включая * / \ [ ] : ; | = , . + " ? < >. В NTFS они допускаются.

Назначить, изменить или удалить метку тома можно в программе Управление дисками (Disk Management) или Проводник (Windows Explorer). Чтобы назначить, изменить или удалить метку в оснастке Управление дисками (Disk Management), выполните следующие действия:

1. Щелкните правой кнопкой нужный раздел или том и выберите **Свойства (Properties)**.
2. В диалоговом окне **Свойства (Properties)** на вкладке **Общие (General)** введите новую метку или удалите существующую. Щелкните **OK**.

Чтобы назначить, изменить или удалить метку в Проводнике (Windows Explorer), выполните следующие действия:

1. В меню **Пуск (Start)** выберите команду **Компьютер (Computer)**.
2. Щелкните правой кнопкой значок диска и выберите **Свойства (Properties)**.
3. В диалоговом окне **Свойства (Properties)** на вкладке **Общие (General)** введите новую метку или удалите существующую. Щелкните **OK**.

Удаление разделов, томов и логических дисков

Для изменения конфигурации полностью распределенного диска вам может потребоваться удаление имеющихся разделов, логических дисков или томов. Поскольку удаление выполняется безвозвратно, перед удалением раздела, логического диска или тома создайте резервные копии любых ценных файлов и папок. Соблюдайте осторожность при удалении томов на компьютере, где есть составные или чередующиеся диски. Удаление любого тома из набора означает потерю всего тома вместе со всеми данными.

Внимание! Удаление раздела, логического диска или тома — необратимое действие. При этом удаляется соответствующая файловая система, и все данные теряются.

Примечание Для защиты целостности системы запрещено удаление системного или загрузочного раздела. Однако в Windows 7 есть возможность удалить активный раздел, если он не назначен загрузочным или системным. Лишний раз убедитесь, что на удаляемом разделе или томе не содержится важных данных или файлов.

Чтобы удалить основной раздел, том или логический диск, выполните следующие действия:

1. В оснастке Управление дисками (Disk Management) щелкните правой кнопкой раздел, том или диск, который нужно удалить, и выберите команду **Проводник (Explore)**. В Проводнике (Windows Explorer) переместите все данные на другой том или убедитесь в наличии и целостности их резервной копии.
2. В оснастке Управление дисками (Disk Management) снова щелкните правой кнопкой раздел, том или диск и выберите команду **Удалить раздел (Delete Partition)**, **Удалить том (Delete Volume)** или **Удалить логический диск (Delete Logical Drive)**.
3. Подтвердите удаление выбранного элемента, щелкнув **Да (Yes)**.

Удаление дополнительного раздела несколько отличается от удаления основного раздела или логического диска. Чтобы удалить дополнительный раздел, сначала нужно удалить все логические диски раздела, следуя шагам из предыдущей процедуры. Затем нужно выбрать саму область дополнительного раздела и удалить ее.

Преобразование томов в NTFS

В Windows 7 есть утилита командной строки Convert для преобразования томов FAT или FAT32 в NTFS-тома. Она находится в папке %SystemRoot%\System32. В процессе преобразования тома при помощи этой утилиты структура файлов и папок сохраняется, и потери данных не происходит.

Внимание! В Windows 7 нет инструмента для преобразования NTFS в FAT или FAT32. Единственный способ преобразовать NTFS в FAT или FAT32 — удалить раздел, а затем создать на его месте новый раздел FAT или FAT32.

Чтобы преобразовать диск, выполните в командной строке с повышенными полномочиями следующие команды:

```
convert том /FS:NTFS
```

где *том* — буква диска с двоеточием (:), путь к диску или имя тома, например:

```
convert D: /FS:NTFS
```

Ниже приведен полный синтаксис команды Convert:

```
convert Том /FS:NTFS [/V] [/X] [/CvtArea:имя_файла] [/NoSecurity]
```

Значения параметров таковы:

- ***Том*** Том, который нужно преобразовать. В обозначении должен присутствовать полный указатель диска (буква диска с двоеточием в конце). Можете также указать точку подключения или имя тома.
- **/FS:NTFS** Целевая файловая система — NTFS. Другую файловую систему указать нельзя.
- **/V** Режим вывода подробной информации.
- **/X** Принудительное отключение тома (при необходимости) перед преобразованием.
- **/CvtArea:*имя_файла*** Указывает на имя непрерывного файла в корневой папке, который следует использовать как заполнитель для системных файлов NTFS, хранящихся в таблице MFT. Если не указать имя файла, будет использована стандартная конфигурация с резервированием 12,5% от объема раздела или тома. Это нужно, чтобы избежать фрагментации таблицы MFT.
- **/NoSecurity** Параметры безопасности NTFS для всех файлов и папок будут заданы таким образом, что доступ к ним получат все члены группы Все (Everyone). По сути, вы откроете доступ ко всей файловой системе всем пользователям, получившим локальный или удаленный доступ к системе.

До начала преобразования при помощи команды Convert проводится проверка, есть ли на диске достаточно свободного места для выполнения преобразования. В общем случае для преобразования при помощи утилиты Convert требуется около 25% от общего использованного пространства диска. Например, если на диске хранится 100 Мб данных, для работы Convert

потребуется около 25 Мб свободного места. При нехватке свободного места операция будет отменена, и вам будет предложено освободить место. Если свободного места достаточно, преобразование будет начато. Запаситесь терпением. Процесс преобразования занимает несколько минут (дольше для больших дисков). Во время преобразования не открывайте файлы или программы, хранящиеся на диске.

Примечание Перед работой с командой Convert перепроверьте, не используется ли раздел как активный загрузочный или системный раздел. В системах на базе Intel x86 допускается преобразование в NTFS активного загрузочного раздела, но для этого необходимо предоставить системе исключительный доступ к данному разделу, что возможно только во время запуска системы. Поэтому в Windows 7 при попытке преобразовать в NTFS активный загрузочный раздел выводится сообщение, в котором предлагается запланировать преобразование диска на следующий запуск системы. Чтобы перезагрузить систему и начать процесс преобразования, щелкните **Да (Yes)**. Часто для полного преобразования активного загрузочного раздела требуется несколько перезагрузок.

Ближе к реальности Параметр /CvtArea позволяет ускорить работу тома за счет резервирования места для таблицы MFT и помогает избежать фрагментации MFT. Как именно? Со временем таблица MFT вырастает из отведенного для нее пространства, и ее приходится расширять за счет других областей диска. Хотя в Windows 7 утилита Дефрагментация диска (Disk Defragmenter) способна дефрагментировать MFT, она не может переместить первый раздел MFT. При этом вероятность того, что после MFT останется свободное пространство, крайне мала, так как пространство будет заполнено данными файлов.

В некоторых случаях фрагментации можно избежать, зарезервировав для MFT больше места, чем предлагается по умолчанию (12,5% от размера раздела или тома). Увеличение размера MFT оправдано, если, например, на томе будет много небольших или средних по размеру файлов, а не один-два больших. Чтобы указать объем резервируемого пространства, при помощи утилиты FSUtil создайте файл-заполнитель, равный по размеру создаваемой таблице MFT. Затем преобразуйте том в NTFS, указав имя файла-заполнителя в параметре /CvtArea.

Далее приведен пример создания файла-заполнителя Temp.txt размером 1,5 Гб (1500000000 б) в утилите FSUtil:

```
fsutil file createnew c:\temp.txt 1500000000
```

Чтобы использовать файл-заполнитель для таблицы MFT во время преобразования диска C в NTFS, выполните команду:

```
convert c: /fs:ntfs /cvtarea:temp.txt
```

Обратите внимание, что файл-заполнитель создается в преобразуемом разделе или томе. В процессе преобразования файл перезаписывается метаданными NTFS, и все неиспользуемое в файле место резервируется для MFT на будущее.

Восстановление простого, составного или чередующегося тома после сбоя

Диагностика и восстановление основных разделов и простых томов довольно просты, если речь идет об одном диске. Составные и чередующие-

ся тома могут располагаться на нескольких дисках, сбой одного из которых приводит к выходу из строя всего тома. Диск при этом пребывает в состоянии Отсутствует (Missing), Неисправен (Failed), В сети (ошибки) (Online (Errors)), Не в сети (Offline) или Не читается (Unreadable).

Если диск отключен или выключен, ему соответствует состояние Отсутствует (Missing) или Не в сети (Offline). Если диски являются частью внешнего накопителя, проверьте подключение и питание накопителя. Возможно, для восстановления доступа к дискам достаточно повторно подключить устройство или включить его питание. Затем откройте оснастку Управление дисками (Disk Management) и выполните повторный поиск отсутствующего диска. Щелкните правой кнопкой отсутствующий диск и выберите команду **Повторить проверку дисков (Rescan Disks)**. По завершению проверки щелкните диск правой кнопкой и выберите **Реактивизировать диск (Reactivate Disk)**.

При возникновении на диске проблем ввода-вывода диск находит в состоянии Неисправен (Failed), В сети (ошибки) (Online (Errors)) и Не читается (Unreadable). Как и в предыдущем примере, попытайтесь повторно проверить и активировать диск. Если диск не удается вернуть в состояние Исправен (Healthy), замените диск.

Совет Иногда для подключения диска достаточно перезагрузить компьютер. Если это не помогло, поищите ошибки на диске, проверьте контроллер диска и кабели, а также питание и подключение диска.

Зеркальные диски

Зеркальные диски состоят из одинаковых по размеру томов на двух различных физических дисках и позволяют создать избыточный набор данных. На физических дисках записываются идентичные наборы информации, и в случае сбоя одного из дисков данные доступны на втором диске.

За отказоустойчивость зеркальных дисков приходится платить двукратным уменьшением места для хранения данных. Например, чтобы создать зеркало диска объемом 500 Гб, необходимо дополнительно 500 Гб. Таким образом, для хранения 500 Гб информации требуется 1000 Гб дискового пространства.

Создание зеркальных томов

Чтобы создать зеркальный том, выполните следующие действия:

1. В графическом представлении оснастки Управление дисками (Disk Management) щелкните правой кнопкой неразмеченную область и выберите команду **Создать зеркальный том (New Mirrored Volume)**. В окне Мастера создания образа (New Mirrored Volume Wizard) прочитайте приветственную страницу и щелкните **Далее (Next)**.
2. Создайте том, как описано ранее в разделе «Создание составных и чередующихся томов». Ключевое отличие заключается в том, что вам придет-

ся создать два одинаковых по размеру тома, расположенных на различных дисках. Вы не сможете продолжить работу, пока не выберете в окне **Выбор дисков (Selected Disks)** два диска.

Примечание Нормальное состояние зеркального тома — Исправен (Healthy). Во время создания зеркала в оснастке Управление дисками (Disk Management) состояние меняется на Ресинхронизация (Resynching).

Новый зеркальный набор можно создать и на основе существующего тома, добавив зеркало к основному разделу или простому тому. На втором диске должна быть область неразмеченного пространства по размеру идентичная или большая, чем существующий том.

Чтобы создать зеркало существующего тома в оснастке Управление дисками (Disk Management), выполните следующие действия:

1. Щелкните правой кнопкой основной раздел или простой том и выберите команду **Добавить зеркало (Add Mirror)**.
2. В открывшемся диалоговом окне **Добавить зеркальный том (Add Mirror)** выберите в списке **Диски (Disks)** расположение зеркала и щелкните **Добавить зеркальный том (Add Mirror)**. Диск, на котором создается зеркальный том, отмечен значком предупреждения.

Разбиение зеркального набора

Иногда нужно разбить зеркальный набор, например, чтобы освободить дисковое пространство для других целей. При выходе из строя одного из дисков зеркального набора зеркало продолжит работать, но рано или поздно его придется исправлять. А для этого зеркало необходимо разбить и потом создать снова. В ходе разбиения зеркала данные, хранящиеся в наборе, сохраняются. Тем не менее, перед этой процедурой необходимо выполнить резервное копирование. Это — гарантия восстановления данных на случай сбоя.

Чтобы разбить зеркало в оснастке Управление дисками (Disk Management), выполните следующие действия:

1. Правой кнопкой щелкните один из томов зеркального набора и выберите команду **Разделить зеркальный том (Break Mirrored Volume)**.
2. Подтвердите разбиение зеркала, щелкнув **Да (Yes)**. Если том используется, будет выведено еще одно предупреждение. Щелкните **Да (Yes)**, чтобы подтвердить действие.

   При разбиении зеркала создаются два независимых тома.

Удаление зеркального набора

Оснастка Управление дисками (Disk Management) позволяет удалять один из томов из зеркального набора. При этом на удаляемом зеркале теряются все данные, а занимаемое им место помечается как Не распределен (Unallocated).

Чтобы удалить зеркало, выполните следующие действия:

1. В оснастке Управление дисками (Disk Management) щелкните правой кнопкой один из томов зеркального набора и выберите команду **Удалить зеркало (Remove Mirror)**.
2. В открывшемся диалоговом окне выберите диск, на котором находится удаляемое зеркало.
3. Подтвердите удаление. Все данные удаленного зеркала будут утеряны.

Перемещение динамического диска в другую систему

Немаловажное преимущество динамических дисков по сравнению с основными заключается в том, что динамические диски можно легко перемещать из одного компьютера в другой. Допустим, вы решили, что в одном из ваших компьютеров дополнительный жесткий диск ни к чему. Переместите его на другой компьютер, где он нужнее. Перед перемещением дисков нужно выполнить следующие действия:

1. Откройте оснастку Управление дисками (Disk Management) на компьютере, где в данный момент находятся динамические диски, и проверьте их состояние. Допустимое состояние — Исправен (Healthy). Если это не так, устраните все неисправности до перемещения.

Внимание! Этот способ не позволяет перемещать диски, зашифрованные при помощи технологии шифрования дисков BitLocker Drive Encryption, включенной в издания Windows 7 Enterprise и Ultimate. Если с диском в отключенном состоянии производились любые несанкционированные действия, он становится недоступным, пока администратор не разблокирует его. Подробнее о технологии BitLocker Drive Encryption — в главе 11.

2. Проверьте подсистемы жесткого диска на исходном и целевом компьютерах. На обоих компьютерах они должны быть одинаковыми. В противном случае, идентификатор Plug and Play на системном диске с исходного компьютера не совпадет с ожидаемым идентификатором на целевом компьютере. В результате на целевом компьютере не будут загружены нужные драйверы, что может привести к сбою загрузки.
3. Проверьте, не являются ли перемещаемые динамические диски частью составных, расширенных или чередующихся наборов. Если это так, выясните, какие диски и в состав каких наборов входят, и перемещайте все диски набора вместе. Перемещение только части дисков из набора неизбежно приведет к неприятным последствиям. При перемещении только части составного, расширенного или чередующегося тома, соответствующий том становится непригодным для использования как на текущем компьютере, так и на компьютере, на который планируется переместить диски.

Подготовившись к перемещению дисков, выполните следующие действия:

1. На исходном компьютере откройте консоль Управление компьютером (Computer Management). На левой панели щелкните элемент **Диспетчер**

устройств (Device Manager). В списке устройств разверните узел **Дисковые устройства (Disk Drives)**. В открывшемся списке физических дисков компьютера последовательно щелкните правой кнопкой все перемещаемые диски и выберите команду **Удалить (Disk Drives)**. Если вы не уверены, какие диски следует отключить, щелкните правой кнопкой диск, в отношении которого сомневаетесь, и выберите **Свойства (Properties)**. В диалоговом окне **Свойства (Properties)** перейдите на вкладку **Тома (Volumes)** и щелкните **Заполнить (Populate)**. При этом будут выведены сведения об имеющихся на выбранном диске томах.

2. Затем на исходном компьютере в консоли Управление компьютером (Computer Management) щелкните узел **Управление дисками (Disk Management)**. Щелкая правой кнопкой все перемещаемые диски, выбирайте команду **Удалить диск (Remove Disk)**.
3. Переместите динамические диски. Если они поддерживают функцию горячей замены и данная функция поддерживается на обоих компьютерах, извлеките диски с исходного компьютера и установите на целевой. В противном случае, выключите оба компьютера, извлеките диски из исходного компьютера и установите их целевой компьютер. Затем снова включите компьютеры.
4. На целевом компьютере откройте оснастку Управление дисками (Disk Management) и в меню **Действие (Action)** выберите команду **Повторить проверку дисков (Rescan Disks)**. После проведения проверки дисков, щелкните правой кнопкой все диски с меткой Инородный (Foreign) и выберите команду **Импортировать (Import)**. Так вы получите доступ к дискам и их томам на целевом компьютере.

Примечание Тома на динамических дисках сохраняют буквы дисков, назначенные им на исходном компьютере. Если на целевом компьютере буква диска уже используется, том получит ближайшую свободную букву. Если у динамического диска ранее не было буквы, при перемещении на другой компьютер буква диска ему не назначается. Если отключена функция автоматического подключения, подключать тома и назначать им буквы вам придется вручную.

Типичные неисправности дисков

В ходе запуска и работы Windows 7 на диски ложится немалая нагрузка. Оптимизация дисков зачастую значительно увеличивает производительность ОС и приложений. Особое внимание следует уделять использованию дискового пространства, ошибкам на диске и фрагментации. Кроме того, вы можете сжать данные, чтобы уменьшить пространство, занимаемое файлами, освободив его для других целей.

Примечание В программах Очистка диска (Disk Cleanup), Проверка диска (Check Disk) и Дефрагментация диска (Disk Defragmenter) используются возможности Windows 7 по определению приоритета ресурсов, как было описано в разделе «Windows SuperFetch». Это позволяет перечисленным инструментам работать в фоновом ре-

жиме, используя время простоя системы. В результате быстродействие приложений пользователей остается высоким, несмотря на выполнение в фоновом режиме служебных задач.

Вы обязаны внимательно следить за использованием пространства на всех дисках системы. По мере заполнения дисков производительность дисков и в целом ОС может снижаться, особенно если не хватает пространства для виртуальной памяти или временных файлов. Инструмент Очистка диска (Disk Cleanup) предназначен для оптимизации использования дискового пространства и сжатия старых файлов. Подробнее о работе с ним написано в главе 6. Чтобы пользователи не забывали запускать программу Очистка диска (Disk Cleanup), запланируйте ее регулярное выполнение, как описано в главе 17.

Оснастка Управление дисками (Disk Management) позволяет определить состояние дисков и содержащиеся на них тома. Состояние диска указано под номером диска в графическом представлении и в поле **Состояние (Status)** представления Список дисков (Disk List). Состояние тома отображено в области сведений о томе в графическом представлении и в столбце Состояние (Status) представления Список томов (Volume List).

В табл. 12-2 приведены сообщения о состоянии дисков, а также возможные причины и рекомендуемые действия по исправлению.

Табл. 12-2. Типичные состояния дисков

Состояние	Описание	Решение
В сети (Online)	Нормальное состояние диска. Свидетельствует о наличии доступа к диску и отсутствии неисправностей	На диске нет известных проблем. Корректирующие действия не нужны
В сети (ошибки) (Online (Errors))	На диске обнаружены ошибки ввода-вывода	Попытайтесь исправить случайные ошибки, щелкнув диск правой кнопкой и выбрав команду **Реактивизировать диск (Reactivate Disk)**. Если это не помогло, возможно, на диске есть физический дефект. Запустите полную проверку диска
Не в сети (Offline)	Диск не читается, возможно, поврежден или временно недоступен. Изменение состояния диска на Отсутствует (Missing) говорит о том, что диск отсутствует в системе или не идентифицируется	Проверьте накопитель, контроллер и кабели. Проверьте питание и подключение диска. Для возврата диска в оперативное состояние (если это возможно) используйте команду **Реактивизировать диск (Reactivate Disk)**

Табл. 12-2. (*продолжение*)

Состояние	Описание	Решение
Инородный (Foreign)	Диск был перемещен на компьютер, но импорт диска не произведен. В этом же состоянии иногда может находиться сбойный диск, возвращенный в оперативный режим	Чтобы добавить диск в систему, щелкните его правой кнопкой мыши и выберите команду **Импорт чужих дисков (Import Foreign Disks)**
Не читается (Unreadable)	В данный момент к диску отсутствует доступ. Такое может случиться во время повторной проверки дисков	Данное состояние характерно для устройств чтения карт памяти с интерфейсом FireWire/USB, когда карта не отформатирована или отформатирована неправильно. Оно также встречается после извлечения карты из устройства. В случае обычного диска это состояние означает, что диск, возможно, поврежден или имеет ошибки ввода-вывода (если в данный момент не проводится проверка дисков). Щелкните диск правой кнопкой и выберите команду **Повторить проверку дисков (Rescan Disks)**. Кроме того, попробуйте перезапустить систему
Неопознан (Unrecognized)	Диск неизвестного типа и непригодный для использования в системе. Такое состояние может отображаться для дисков из систем, отличных от Windows	Если диск из другой ОС, ничего не делайте. Вы не сможете использовать данный диск на компьютере, поэтому попробуйте подключить другой диск
Не проинициализирован (Not Initialized)	Отсутствует действительная подпись диска. Такое состояние могут возвращать диски из систем, отличных от Windows	Если диск перенесен из другой ОС, ничего не делайте. Вы не сможете использовать данный диск на компьютере, поэтому попробуйте подключить другой диск. Чтобы подготовить диск для использования в Windows 7, щелкните его правой кнопкой и выберите команду **Инициализировать диск (Initialize Disk)**

Табл. 12-2. (*окончание*)

Состояние	Описание	Решение
Нет носителя (No Media)	В CD-ROM-дисковод или съемный диск не вставлен носитель, или носитель извлечен. Данное состояние характерно только для устройств CD-ROM и съемных дисков	Чтобы включить диск, вставьте компакт-диск, дискету или съемный диск. В устройствах чтения карт памяти с интерфейсом FireWire/USB такое состояние обычно (но не всегда) отображается после извлечения карты

В табл. 12-3 приведены сообщения о состоянии томов, а также возможные причины и действия по их устранению.

Табл. 12-3. Определение и решение проблем состояния томов

Состояние	Описание	Решение
Данные неполны (Data Incomplete)	Составные тома на внешнем диске не укомплектованы. Возможно, вы добавили не все диски составного набора	Добавьте оставшиеся диски составного тома, затем импортируйте все диски одновременно
Нет избыточности данных (Data Not Redundant)	Не укомплектованы отказоустойчивые тома на внешнем диске. Возможно, вы добавили не все диски зеркального набора	Добавьте оставшиеся диски, затем импортируйте все диски одновременно
Неисправен (Failed)	На диске ошибка. Нет доступа к диску или диск поврежден	Убедитесь, что диск подключен, при необходимости щелкните его правой кнопкой и выберите команду **Реактивизировать диск (Reactivate Disk)**. Затем щелкните правой кнопкой том и выберите команду **Реактивизировать том (Reactivate Volume)**
Форматирование (Formatting)	Временное состояние, отражающее форматирование тома	Ход форматирования отображается в процентах, если не задан параметр **Быстрое форматирование (Perform A Quick Format)**
Исправен (Healthy)	Рабочее состояние тома	На томе нет известных проблем. Корректирующие действия не нужны

Табл. 12-3. (*окончание*)

Состояние	Описание	Решение
Исправен (под угрозой (Healthy (At Risk))	Возникли проблемы при чтении-записи на физический диск, на котором расположен том. Данное состояние отображается при наличии ошибок	Щелкните диск правой кнопкой и выберите команду **Реактивизировать диск (Reactivate Disk)**. Если диск остался в прежнем состоянии или периодически в него возвращается, возможно, диск выходит из строя — поспешите с архивацией хранящихся на нем данных
Исправен (неизвестный раздел) (Healthy (Unknown Partition))	Раздел не распознается Windows. Такое случается, когда раздел принадлежит другой ОС или создан производителем для хранения системных файлов	Исправление не требуется
Инициализация (Initializing)	Временное состояние, отражающее инициализацию диска	Состояние диска изменится через несколько секунд
Ресинхронизация (Resynching)	Временное состояние, отражающее повторную синхронизацию зеркала	Ход выполнения отображен в процентах. Том должен вернуться в состояние Исправен (Healthy)
Устаревшие данные (Stale Data)	Не синхронизированы данные на чужих отказоустойчивых дисках	Выполните повторную проверку дисков или перезапустите компьютер, а затем проверьте состояние. Том может перейти в состояние Отказавшая избыточность (Failed Redundancy)
Неизвестный (Unknown)	Нет доступа к тому. Возможно, поврежден загрузочный сектор	Причиной может быть вирус в загрузочном секторе. Проверьте его обновленной антивирусной программой. Если вирус не обнаружен, восстановите основную загрузочную запись: загрузите Windows 7 с CD-ROM и в Консоли восстановления (Recovery Console) выполните команду Fixmbr

Исправление ошибок и рассогласований на диске

Целый ряд функциональных усовершенствований Windows 7 позволяет сократить долю ручного труда в обслуживании дисков. Наибольшее влияние на работу с дисками оказали следующие технологии:

- транзакционная NTFS (Transactional NTFS);
- самовосстановление NTFS (Self-healing NTFS).

Транзакционная файловая система NTFS позволяет выполнять операции с файлами на NTFS-томе в режиме транзакций: программы формируют наборы из операций с файлами и реестром, и успехом завершаются все операции или ни одна из них. Пока транзакция активна, изменения за пределами транзакции не видны. Фиксация и полная запись изменений на диск происходит только после завершения транзакции. Если во время транзакции произошла ошибка или транзакция не завершилась, транзакция откатывается, чтобы восстановить файловую систему до состояния, предшествующего транзакции.

Транзакции, охватывающие несколько томов, координирует диспетчер транзакций ядра (Kernel Transaction Manager, KTM), поддерживающий независимое восстановление томов в случае сбоя транзакции. Диспетчер локальных ресурсов тома обслуживает журнал транзакций и отвечает за обработку потоков транзакций отдельно от потоков работ с файлами.

Традиционно для исправления ошибок и непоследовательностей в NTFS-томах применялся инструмент Проверка диска (Check Disk). Однако его работа может нарушить доступность компьютеров с Windows, поэтому в Windows 7 для защиты файловой системы используется самовосстановление NTFS — технология, позволяющая устранять неполадки без специализированных средств. Большая часть самовосстановления выполняется автоматически, поэтому ручное обслуживание тома понадобится вам только в случае, если вы получите уведомление ОС о невозможности автоматического решения проблемы. При этом вам также будут предложены возможные решения.

Самовосстановление NTFS обладает многими преимуществами по сравнению с программой Проверка дисков (Check Disk):

- Программе Проверка дисков (Check Disk) необходим исключительный доступ к томам, поэтому проверку системных и загрузочных томов можно выполнять только при запуске ОС. В самовосстанавливающейся NTFS файловая система всегда доступна и в большинстве случаев не нуждается в отключении для корректировки.
- При самовосстановлении NTFS в случае повреждения производится попытка сохранить как можно больше данных. Во время перезапуска функция самовосстановления NTFS немедленно исправляет том, чтобы том можно было подключать.
- В ходе исправления NTFS сообщает о внесенных в том изменениях посредством существующего механизма программы Chkdsk.exe, уведомлений каталога и записей USN (Update Sequence Number). Полномочные пользователи и администраторы могут наблюдать за ходом исправлений при помощи сообщений Verification, Waiting For Repair Completion и Progress Status.
- При помощи функции самовосстановления NTFS можно восстановить том, если он не опознан, но на нем читается загрузочный сектор. В этом

случае необходимо отключить том и запустить средство восстановления загрузочного сектора, после чего NTFS начнет самостоятельное восстановление.

Хотя самовосстановление NTFS — это существенное усовершенствование, время от времени вам придется проверять целостность диска вручную. В этом случае для проверки и исправления сбоев на томах FAT, FAT32 и NTFS применяется программа Проверка дисков (Check Disk, Chkdsk.exe), способная найти и исправить многие типы ошибок и уделяющая основное внимание непоследовательностям в файловой системе и связанных метаданных. Но на этом функциональность программы заканчивается. В частности, Chkdsk.exe бесполезна при восстановлении поврежденных данных в файлах, структура которых кажется целостной.

Поиск ошибок на диске

Целостность дисков следует периодически проверять. Многие типичные ошибки на дисках FAT16, FAT32 и NTFS позволяет исправить программа Проверка дисков (Check Disk). Для ее запуска могут применяться как графический интерфейс, так и командная строка.

Запуск программы Проверка дисков (Check Disk) из командной строки

Вы можете запустить программу в командной строке с повышенными полномочиями или из других программ. Чтобы проверить целостность диска C в командной строке с повышенными полномочиями, введите команду:

```
chkdsk C:
```

После этого будет произведен анализ диска с выводом сообщения, в котором отражаются все найденные неисправности. Если вы не укажете дополнительные параметры, исправление ошибок выполняться не будет. Следующая команда служит для поиска и устранения ошибок на диске C:

```
chkdsk /f C:
```

В ходе выполнения этой команды производится анализ диска с последующим исправлением всех найденных ошибок, при условии что диск не используется. Если диск используется, вам будет предложено запланировать его проверку при следующем запуске системы. Если вас это устраивает, щелкните **Да (Yes)**.

Полный синтаксис утилиты Проверка дисков (Check Disk) таков:

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

Далее перечислены параметры утилиты Проверка дисков (Check Disk):

- **Том** Проверяемый том.
- **Путь/имя файла** Файлы, которые следует проверить на фрагментацию (только для FAT16 и FAT32).
- **/F** Исправление ошибок на диске.

- **/V** Для FAT16 и FAT32: вывод полного пути и имени всех файлов на диске; для NTFS вывод возможных сообщений об очистке.
- **/R** Поиск поврежденных секторов и восстановление читаемой информации (требуется параметр /F).
- **/X** Предварительное принудительное отключение тома при необходимости (требуется параметр /F).
- **/I** Быстрая проверка элементов индекса (только NTFS).
- **/C** Пропуск проверки циклов внутри структуры папок (только NTFS).
- **/L:размер** Размер файла журнала (только NTFS).
- **/B** Повторная оценка поврежденных секторов на диске (только NTFS; требуется параметр /R).

Интерактивный запуск программы Проверка дисков (Check Disk)

Утилиту Проверка дисков (Check Disk) можно открыть интерактивно. Чтобы проверить диски локального компьютера в Проводнике (Windows Explorer), выполните следующие действия:

1. Выберите в меню **Пуск (Start)** команду **Компьютер (Computer)**. В области **Жесткие диски (Hard Disk Drives)** щелкните нужный диск и выберите **Свойства (Properties)**.
2. На вкладке **Сервис (Tools)** щелкните **Выполнить проверку (Check Now)**. Открывшееся диалоговое окно **Проверить диск (Check Disk)** показано на рис. 12-13.

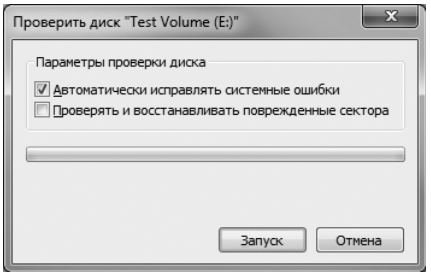

Рис. 12-13. Окно Проверить диск (Check Disk) для поиска и исправления ошибок на диске

3. Для простого поиска ошибок на диске без их исправления щелкните **Запуск (Start)**, не устанавливая ни один флажок.
4. Для поиска ошибок и их исправления установите один или оба флажка и щелкните **Запуск (Start)**:
   - **Автоматически исправлять системные ошибки (Automatically Fix File System Errors)** Исправление найденных ошибок файловой системы.
   - **Проверять и восстанавливать поврежденные сектора (Scan For And Attempt Recovery Of Bad Sectors)** Поиск поврежденных секторов и попытка восстановления читаемой информации.

5. Если диск используется, вам будет предложено запланировать его проверку при следующем запуске системы. Щелкните **Да (Yes)**.
6. По завершению анализа и исправления ошибок щелкните **OK**.

Дефрагментация диска

Каждое добавление или удаление файлов чревато фрагментацией данных на диске. На фрагментированном диске большие файлы невозможно записать в одну последовательную область. В результате файл записывается в несколько областей диска меньшего размера, а это означает, что для его чтения с диска потребуется больше времени. Чтобы уменьшить фрагментацию, в Windows 7 предусмотрена возможность регулярно автоматически или вручную дефрагментировать диски в утилите Дефрагментация диска (Disk Defragmenter). Чем чаще обновляются данные на дисках, тем чаще следует использовать этот инструмент.

Чтобы выполнить дефрагментацию вручную, выполните следующие действия:

1. В консоли Управление компьютером (Computer Management) разверните узел **Запоминающие устройства (Storage)** и щелкните элемент **Управление дисками (Disk Management)**. Щелкните правой кнопкой нужный диск и выберите **Свойства (Properties)**.
2. На вкладке **Сервис (Tools)** щелкните кнопку **Выполнить дефрагментацию (Defragment Now)**. Открывшееся диалоговое окно **Дефрагментация диска (Disk Defragmenter)** показано на рис. 12-14.

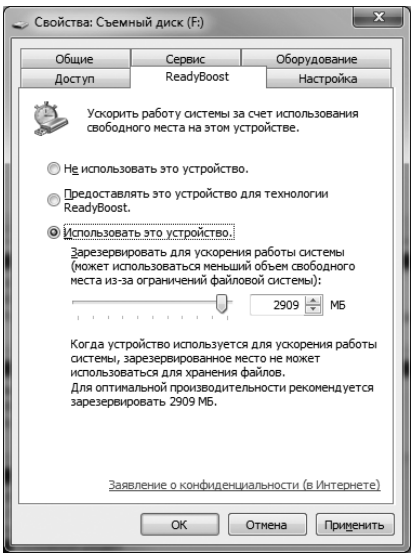

Рис. 12-14. Анализ и дефрагментация дисков в программе Дефрагментация диска (Disk Defragmenter)

3. В диалоговом окне **Дефрагментация диска (Disk Defragmenter)** выберите дефрагментируемые диски и щелкните **Дефрагментация диска (Defragment Now)**.

Примечание На большом диске дефрагментация может занять несколько часов. Для прекращения дефрагментации щелкните кнопку **Остановить дефрагментацию (Cancel Defragmentation)**.

По умолчанию автоматическая дефрагментация, если вы ее включите, выполняется каждую среду в 01.00, конечно, если компьютер включен в это время. Чтобы настроить автоматическую дефрагментацию, выполните следующие действия:

1. В консоли Управление компьютером (Computer Management) разверните узел **Запоминающие устройства (Storage)** и щелкните **Управление дисками (Disk Management)**. Щелкните правой кнопкой нужный диск и выберите **Свойства (Properties)**.
2. На вкладке **Сервис (Tools)** щелкните **Выполнить дефрагментацию (Defragment Now)**.
3. Для изменения расписания дефрагментации щелкните кнопку **Настроить расписание (Configure Schedule)**. Чтобы отменить автоматическую дефрагментацию, в открывшемся диалоговом окне **Настройка расписания (Modify Schedule)**, показанном на рис. 12-15, сбросьте флажок **Выполнять по расписанию (Run On A Schedule)**, щелкните **OK**, **Закрыть (Close)** и пропустите оставшиеся шаги. Чтобы включить автоматическую дефрагментацию, установите флажок **Выполнять по расписанию (Run On A Schedule)**. В окне отображается стандартное расписание или расписание, установленное в последний раз.

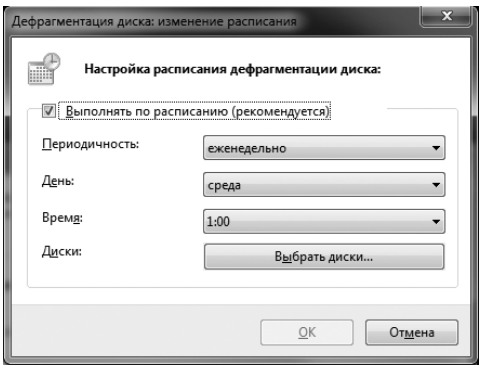

Рис. 12-15. Расписание автоматической дефрагментации

4. В списке **Периодичность (Frequency)** выберите вариант **Ежедневно (Daily)**, **Еженедельно (Weekly)** или **Ежемесячно (Monthly)**. Задав еженедельную или ежемесячную дефрагментацию, выберите в списке **День (Day)** день недели или месяца. Наконец, в списке **Время (Time)** задайте время, в которое следует выполнять автоматическую дефрагментацию.

Дефрагментация диска не выполняется, если компьютер в назначенное время выключен.

5. Для выбора дефрагментируемых дисков щелкните кнопку **Выбрать диски (Select Disks)**. Укажите дефрагментируемые тома в диалоговом окне **Выберите диски для включения в расписание (Select Disks For Schedule)**. По умолчанию дефрагментации подлежат все установленные или подключенные к компьютеру диски, а также все новые диски. В списке **Диски, включаемые в расписание (Disks To Include In Schedule)** установите флажки дисков, которые нужно дефрагментировать автоматически, и сбросьте флажки дисков, для которых этого делать не нужно.
6. Щелкните **OK**, чтобы сохранить параметры, а затем щелкните **Закрыть (Close)**.

Примечание В Windows Vista SP1 и более поздних версиях, а также в Windows 7 автоматически выполняется циклический перезапуск дефрагментации: в случае остановки дефрагментации, выполняющейся по расписанию, при повторном включении автоматически будет продолжена дефрагментация первого незавершенного тома.

Повторная синхронизация и восстановление зеркального набора

В Windows 7 синхронизация зеркальных томов на дисках выполняется автоматически. Тем не менее, данные на зеркальных дисках могут утратить синхронность. Например, при отключении одного из дисков данные записываются только на диск, оставшийся включенным.

Зеркальные наборы можно повторно синхронизировать и исправлять, но для перестроения набора подойдут только диски с идентичными разделами — MBR или GPT. При возникновении ошибки на одном из дисков набора он переходит в состояние Отказавшая избыточность (Failed Redundancy). Способ исправления зависит от состояния сбойного тома:

- Если том находится в состоянии Отсутствует (Missing) или Не в сети (Offline), проверьте питание и соединение. Затем в оснастке Управление дисками (Disk Management) щелкните том правой кнопкой и выберите команду **Реактивизировать том (Reactivate Volume)**. Сначала состояние тома изменится на Регенерация (Regenerating), а затем — на Исправен (Healthy). Если том не переходит в состояние Исправен (Healthy), щелкните его правой кнопкой и выберите команду **Ресинхронизировать зеркало (Resynchronize Mirror)**.
- Если том находится в состоянии В сети (ошибки) (Online (Errors)), щелкните правой кнопкой сбойный том и выберите команду **Реактивизировать том (Reactivate Volume)**. Сначала состояние тома изменится на Регенерация (Regenerating), а затем — на Исправен (Healthy). При отсутствии состояния Исправен (Healthy), щелкните правой кнопкой том и выберите команду **Ресинхронизировать зеркало (Resynchronize Mirror)**.
- Если один из дисков находится в состоянии Не читается (Unreadable), попробуйте повторно проверить диски в оснастке Управление дисками

(Disk Management): в меню **Действие (Action)** выберите команду **Повторить проверку дисков (Rescan Disks)**. Перезагрузите компьютер, если состояние тома не изменилось.

- Если после этого один из дисков по-прежнему не подключен, щелкните правой кнопкой сбойный том и выберите команду **Удалить зеркало (Remove Mirror)**. Затем щелкните правой кнопкой оставшийся том и выберите команду **Добавить зеркало (Add Mirror)**. Теперь нужно создать зеркало тома в неразмеченной области отдельного диска. Если на нем или на другом диске нет неразмеченной области, ее необходимо создать, удалив другие тома или заменив отказавший том.

Восстановление зеркального системного тома

Сбой зеркального диска может стать причиной отказа загрузки системы. Обычно это происходит при использовании зеркала системного и (или) загрузочного тома, когда первичное зеркало выходит из строя.

Во время зеркалирования системного тома в системный диспетчер загрузки добавляется запись, позволяющая производить загрузку со вторичного зеркала. Присутствие этой записи в файле диспетчера загрузки значительно упрощает восстановление первичного зеркала, поскольку от вас требуется всего лишь выбрать вариант загрузки со вторичного зеркала. Если при создании зеркала загрузочного тома запись вторичного зеркала в диспетчере загрузки не создана, создайте при помощи утилиты BCD Editor.

Если систему не удается загрузить с первичного системного тома, перезагрузите систему и выберите загрузку с вторичного зеркала. Система загрузится обычным образом, и вы при желании сможете запланировать необходимые процедуры по перестроению зеркала, выполнив следующие действия:

1. Завершите работу системы, замените сбойный том или добавьте новый жесткий диск, а затем запустите систему.
2. Разделите зеркальный набор и создайте зеркало на замененном диске. Скорее всего, это Disk 0. Щелкните правой кнопкой оставшийся от первоначального зеркала том и выберите команду **Добавить зеркало (Add Mirror)**.
3. В открывшемся диалоговом окне **Добавить зеркальный том (Add Mirror)** укажите расположение зеркала в списке **Диски (Disks)** и щелкните **Добавить зеркальный том (Add Mirror)**. В начале создания зеркала состояние обоих томов в оснастке Управление дисками (Disk Management) изменится на Ресинхронизация (Resynching). Диск, на котором создается зеркальный том, отмечен значком предупреждения.
4. Чтобы первичное зеркало находилось на добавленном (или замененном) диске, еще раз разделите зеркало в оснастке Управление дисками (Disk Management). Буква первичного диска в первоначальном наборе зеркал должна совпадать с буквой, ранее назначенной всему зеркалу. Если это не так, назначьте соответствующую букву диска.

5. Щелкните правой кнопкой первоначальный системный том и выберите команду **Добавить зеркало (Add Mirror)**. Теперь создайте зеркало заново.
6. Проверьте конфигурацию загрузки, убедившись, что во время загрузки используется первоначальный системный том. Для этого может потребоваться изменить конфигурацию загрузки.

Съемные запоминающие устройства

Внешние накопители не устанавливаются внутри компьютера, а подключаются к нему извне. Благодаря этому внешние накопители в сравнении с большинством фиксированных дисков проще и быстрее устанавливаются. Как правило, внешние накопители поставляются с интерфейсом USB или FireWire. Форматирование съемных запоминающих устройств выполняется в файловых системах NTFS, FAT, FAT32 и exFAT. При этом скорость передачи и общая производительность устройства зависят, в основном, от поддерживаемой версии интерфейса.

В настоящий момент используется несколько версий USB и FireWire: USB 1.0, USB 1.1, USB 2.0, FireWire 400 и FireWire 800. Стандарт USB 2.0 поддерживает передачу с максимальной скоростью 480 Мбит/с при средней скорости от 10 до 30 Мбит/с. Фактическая скорость передачи зависит от многих факторов, например типа устройства, передаваемых данных и быстродействия компьютера. На компьютере у каждого USB-контроллера есть фиксированная полоса пропускания, которая делится между всеми подключенными к контроллеру устройствами. Скорость передачи данных будет значительно ниже, если USB-порт компьютера имеет более раннюю версию, чем используемое устройство. Например, при подключении устройства USB 2.0 к порту USB 1.0 или наоборот скорость будет ограничена стандартом USB 1.0.

Выглядят порты USB 1.0, 1.1 и 2.0 одинаково. Для определения типа установленных на компьютере USB-портов проще всего обратиться к документации компьютера. В новых ЖК-мониторах также есть порты USB 2.0 для подключения различных устройств. При подключении USB-устройства к монитору он выступает в роли USB-концентратора. Как и в случае других USB-концентраторов, все подключенные устройства делят общую полосу пропускания, причем доступная ширина полосы определяется скоростью входного устройства USB на компьютере, к которому подключен концентратор.

Высокоскоростной стандарт FireWire (IEEE 1394) основан на одноранговой архитектуре, в которой периферийные устройства разрешают конфликты доступа к шине, определяя устройство, которое будет осуществлять передачу данных. Сейчас применяется несколько версий FireWire, включая FireWire 400 (IEEE 1394a) и FireWire 800 (IEEE 1394b). В первом максимальная поддерживаемая скорость передачи составляет 400 Мбит/с, во втором — 800 Мбит/с. Как и в случае USB, при подключении устройства FireWire 800 к порту FireWire 400 или наоборот, скорость устройства ограничивается возможностями стандарта FireWire 400.

Порты FireWire 400 и FireWire 800 имеют различную форму, что упрощает их распознавание, если конечно, вы знаете, что искать. Порты и кабели стандарта FireWire 400 выглядят так же, как порты и кабели предыдущих версий FireWire, которые были реализованы еще до окончательного формирования спецификаций IEEE 1394a и IEEE 1394b. Кабели и порты FireWire с четырьмя контактами не имеют питания от шины. У кабелей и портов FireWire 400 — шесть контактов, у кабелей и портов FireWire 800 — девять контактов.

Приобретая внешнее устройство для компьютера, подумайте, какие интерфейсы поддерживаются компьютером и какие используются устройством. Встречаются устройства с двойным интерфейсом, поддерживающие USB 2.0 и FireWire 400, и даже с тройным — USB 2.0, FireWire 400 и FireWire 800. Двойной и тройной интерфейс более функционален.

Для работы со съемным носителем щелкните его правой кнопкой в консоли Компьютер (Computer) или оснастке Управление дисками (Disk Management). Доступны следующие команды:

- **Открыть (Open)** или **Проводник (Explore)** Просмотр содержимого диска в Проводнике (Windows Explorer).
- **Форматировать (Format)** Форматирование съемного диска. Обычно на съемных носителях форматируют единственный раздел.
- **Свойства (Properties)** Просмотр свойств носителя.

Чтобы настроить представление дисков и папок для съемных носителей, щелкните диск или папку правой кнопкой, выберите **Свойства (Properties)** и перейдите на вкладку **Настройка (Customize)**. Затем задайте вид папки по умолчанию. Для папки, в частности, доступны стандартные представления Документы (Documents), Изображения (Pictures) и Видео (Videos). Здесь также можно задать изображения и значки для папок.

Съемные диски поддерживают сетевой общий доступ к файлам и папкам. Он настраивается так же, как и обычный общий доступ к файлам: вы назначаете разрешения, настраиваете параметры кеша для автономной работы с файлами и ограничиваете число одновременных обращений. Можно открыть общий доступ ко всему съемному диску или к отдельным его папкам. Кроме того, можно создавать несколько экземпляров общего ресурса.

Общий доступ к съемным носителям отличается от обычного общего доступа NTFS отсутствием архитектуры безопасности. В exFAT, FAT или FAT32 у папок и файлов нет разрешений доступа, помимо основных атрибутов — только для чтения или скрытый.

Компакт-диски и DVD-диски

Часто образы компакт-дисков и DVD хранятся в виде ISO-файлов. Встроенные возможности Windows 7 позволяют распознавать образы ISO и записывать их на CD- или DVD-диски, а также создавать CD- и DVD-диски «с нуля». При записи данных на компакт-диски и DVD-диски вам пригодятся сведения о типах дисков и доступных файловых системах.

Основы записи на компакт-диск

По умолчанию, когда вы вставляете в CD- или DVD-дисковод пустой диск, на панели инструментов Проводника (Windows Explorer) появляется кнопка **Записать на оптический диск (Burn)**. Щелкните ее, чтобы открыть мастер Записать диск (Burn A Disc), предназначенный для записи дисков с данными. Помните, что компьютерные дисководы CD и DVD отличаются от домашних и автомобильных проигрывателей. Дисковод CD/DVD, установленный на компьютере, как правило, предназначен для чтения как CD-ROM и DVD-ROM, записанных промышленным способом, так и компакт-дисков и DVD, записанных на компьютере в особых форматах. Домашний или автомобильный проигрыватель CD/DVD может не распознать CD или DVD-диски, созданные на компьютере.

В большинстве пишущих дисководов поддерживаются диски нескольких типов. В Windows 7 изначально поддерживается запись данных на диски CD-R, CD+R и CD-RW, а также DVD-R, DVD-RW, DVD+R, DVD+RW и DVD-RAM. Диски DVD делятся на односторонние однослойные и односторонние двухслойные. Кроме того, в Windows 7 изначально поддерживается Blu-ray. Если на компьютере есть проигрыватель Blu-ray, вы сможете записывать диски Blu-ray.

В Windows 7 поддерживается два способа записи дисков:

- запись в формате «Mastered»;
- запись в работающей (live) файловой системе.

В большинстве программ для Windows диски с данными создаются в формате «Mastered» и автоматически записываются в нужном формате. При записи в формате «Mastered» наборы файлов, которые нужно скопировать на диск, записываются одновременно. Это удобно при записи больших наборов файлов, кроме того данные совместимы с любым компьютером или устройством, поддерживающим используемый тип диска.

Запись файлов на диски с данными в формате «Mastered» осуществляется в режиме сеанса. В большинстве программ для записи CD/DVD имеется возможность оставлять сеанс открытым, чтобы добавлять файлы на диск в несколько приемов. Поместив на диск все файлы, вы закрываете сеанс, после чего диск формируется окончательно и может быть прочтен на других компьютерах и устройствах. Пока сеанс не закрыт, диск читается только на совместимом компьютере.

Диски с работающей файловой системой используются, как любой съемный накопитель — «флешка» или внешний диск. Файлы на диск добавляются простым копированием/вставкой или перетаскиванием — никакой записи. Если диск предназначен для многократной перезаписи, файлы можно удалять. Диск можно извлечь из дисковода, а потом снова вставить его и снова использовать в качестве съемного носителя.

Диски с файловой системой записываются в универсальном формате UDF (Universal Disk Format), а не в обычной файловой системе CDFS (CD

File System). Читаются диски в формате UDF, в основном, только на компьютерах. В Windows 7 поддерживается запись компакт-дисков в нескольких версиях UDF:

- **UDF 1.5** Формат, совместимый с Windows 2000 и последующими версиями Windows. Может не читаться на компьютерах под управлением Windows 98 или Apple.
- **UDF 2.0** Формат, совместимый с Windows XP и последующими версиями Windows. Может не читаться на компьютерах под управлением Windows 98, Windows 2000 или Apple.
- **UDF 2.01** Формат, используемый по умолчанию, содержит много полезных обновлений. Совместим с Windows XP и последующими версиями Windows. Может не читаться на компьютерах под управлением Windows 98, Windows 2000 или Apple.
- **UDF 2.5** Оптимизированный формат для Windows Vista и последующих версий. Может не читаться на компьютерах под управлением предыдущих версий Windows или Apple.

Запись образа ISO на диск

Для записи на диск образа ISO выполните следующие действия:

1. Вставьте чистый диск в пишущий CD/DVD-дисковод компьютера. Если откроется окно **Автозапуск (AutoPlay)**, закройте его.
2. В программе Проводник (Windows Explorer) дважды щелкните ISO-файл, на основе которого нужно создать CD или DVD с данными.
3. В диалоговом окне **Средство записи образов дисков Windows (Windows Disc Image Burner)**, показанном на рис. 12-16, выберите устройство для записи в списке **Устройство записи на диск (Disc Burner)** и щелкните **Записать (Burn)**.

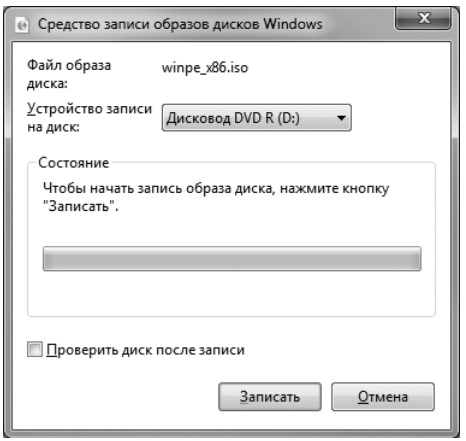

Рис. 12-16. Запись образа ISO на диск

Запись диска в формате «Mastered»

Для записи диска в формате «Mastered» выполните следующие действия:

1. Вставьте чистый диск в пишущий CD/DVD-дисковод компьютера. Выполните одно из следующих действий:
   - В диалоговом окне **Автозапуск (AutoPlay)** щелкните **Записать файлы на диск, используя Проводник (Burn Files To Disc Using Windows Explorer)**.
   - Если окно **Автозапуск (AutoPlay)** не открылось, щелкните кнопку **Пуск (Start)** и выберите команду **Компьютер (Computer)**. В окне Компьютер (Computer) щелкните правой кнопкой устройство записи CD/DVD и выберите команду **Открыть автозапуск (Open AutoPlay)**. В диалоговом окне **Автозапуск (AutoPlay)** щелкните **Записать файлы на диск, используя Проводник (Burn Files To Disc Using Windows Explorer)**.
2. В окне мастера Записать диск (Burn A Disc) введите название диска (рис. 12-17). Чтобы создать диск в формате в формате «Mastered», установите переключатель **С проигрывателем CD/DVD (With A CD/DVD Player)**. Щелкните **Далее (Next)**. Диск с данными откроется в Проводнике (Windows Explorer). Не закрывайте открывшееся окно.
3. При помощи Проводника (Windows Explorer) копируйте файлы в окно диска. Реально файлы копируются из начального расположения во временную папку в личном профиле пользователя. Копии файлов нужны, чтобы перед началом записи собрать все файлы в одном месте, гарантирующем наличие у пользователя необходимых разрешений.
4. Скомпоновав набор файлов, щелкните кнопку **Запись на компакт-диск (Burn To Disc)**. Название диска вы указали ранее. Обратите внимание, что задана наибольшая скорость записи, поддерживаемая CD/DVD-дисководом.

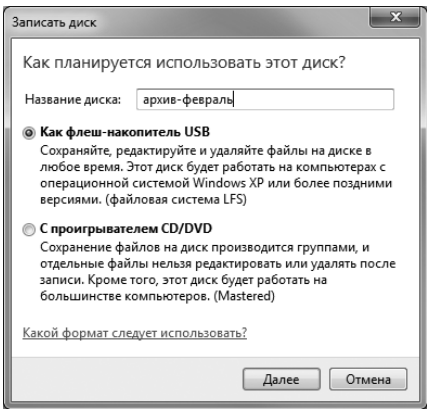

Рис. 12-17. Подготовка к записи данных на диск

5. Щелкните **Далее (Next)**. Выбранные вами файлы будут добавлены к образу, а затем записаны на диск с данными. По умолчанию после записи диск будет автоматически извлечен, а временные файлы — удалены. Щелкните **Готово (Finish)**, чтобы закрыть мастер. Для записи тех же файлов на другой диск, прежде чем щелкнуть **Готово (Finish)**, установите флажок **Да, записать эти же файлы на другой диск (Yes, Burn These Files To Another Disc)**.

Если во время записи возникает ошибка, вы увидите сообщение о ней. В этом случае вы можете записать файлы на другой диск, удалить не записанные временные файлы или сохранить временные файлы, отложив запись. Если вы решите попытаться записать файлы еще раз, установите более низкую скорость записи. Даже если CD/DVD-дисковод поддерживает высокую скорость записи, сам диск может быть не рассчитан на нее.

Обычно при возникновении ошибки записи на диск записывается только часть файлов. Если сеанс записи все еще открыт, попытайтесь записать диск снова. Иногда для этого может понадобиться еще один диск.

Запись дисков в файловой системе

Для записи диска в файловой системе выполните следующие действия:

1. Вставьте чистый диск в пишущий CD/DVD-дисковод. Выполните одно из следующих действий:
   - В диалоговом окне **Автозапуск (AutoPlay)** щелкните **Записать файлы на диск, используя Проводник (Burn Files To Disc Using Windows Explorer).**
   - Если окно **Автозапуск (AutoPlay)** не открылось, щелкните кнопку **Пуск (Start)** и выберите **команду Компьютер (Computer)**. В окне **Компьютер (Computer)** щелкните правой кнопкой устройство записи CD/DVD и выберите команду **Открыть автозапуск (Open AutoPlay)**. В диалоговом окне **Автозапуск (AutoPlay)** щелкните **Записать файлы на диск, используя Проводник (Burn Files To Disc Using Windows Explorer)**.
2. В окне мастера Записать диск (Burn A Disc) введите название диска. Чтобы создать диск с файловой системой, щелкните **Как флеш-накопитель USB (Like A USB Flash Drive)**. Когда вы щелкнете **Далее (Next)**, на диске будет создана файловая система и диск откроется в Проводнике (Windows Explorer).
3. Добавляйте файл на диск и удаляйте их как на любом другом накопителе. На перезаписываемых дисках на место удаленных файлов можно записывать другие. На обычных записываемых дисках файлы помечаются как удаленные, но на самом деле остаются на диске. Поэтому занимаемое ими пространство по-прежнему распределено и не может использоваться для других файлов.

4. Пока диск находится в дисководе, продолжается открытый сеанс записи на диск. При извлечении диска сеанс записи закрывается, чтобы диск можно было использовать на других компьютерах. Когда вы снова вставите диск, то снова сможете добавлять и удалять файлы в Проводнике (Windows Explorer). При каждом изменении содержимого диска открывается новый сеанс записи. Чтобы закрыть сеанс, как и прежде, извлеките диск. Для закрытия сеанса также можно щелкнуть правой кнопкой CD/DVD-дисковод в окне **Компьютер (Computer)** и выбрать команду **Закрыть сеанс (Close Session)**.

Изменение параметров записи по умолчанию

Чтобы изменить параметры записи, применяемые по умолчанию, выполните следующие действия:

1. Щелкните кнопку **Пуск (Start)** и выберите команду **Компьютер (Computer)**. В окне **Компьютер (Computer)** щелкните правой кнопкой CD/DVD-дисковод и выберите **Свойства (Properties)**.
2. На вкладке **Запись (Recording)** в списке **Запись на диск (Disc Burning)** задайте устройство, используемое для записи по умолчанию (на компьютере с несколькими пишущими дисководами).
3. Укажите место хранения временных файлов.
4. Чтобы диски в формате «Mastered» не извлекались автоматически после записи, сбросьте соответствующий флажок.
5. По умолчанию при извлечении диска с файловой системой он закрывается. Чтобы изменить это поведение, щелкните кнопку **Общие параметры (Global Settings)**. В диалоговом окне **Общие параметры (Global Settings)** укажите, следует ли закрывать сеансы и если да, то какие. Затем щелкните **OK**.
6. Щелкните **OK**, чтобы сохранить параметры.

Сжатие дисков и шифрование файлов

При форматировании диска в NTFS у вас есть возможность включить функции сжатия и шифрования файлов. Сжатие используется для уменьшения дискового пространства, занятого файлами, а шифрование представляет собой дополнительный уровень защиты данных. Сжатие данных на диске и шифрование — взаимоисключающие функции. Однако их можно использовать совместно с функцией BitLocker Drive Encryption.

Сжатие дисков и данных

Если включено сжатие, все файлы и каталоги на диске автоматически сжимаются в момент их создания. Сжатие прозрачно для пользователей, и доступ к сжатым файлам не отличается от доступа к обычным файлам. Различие в том, что сжатый диск вмещает больше информации, чем несжатый.

Ближе к реальности Хотя сжатие, безусловно, полезно для экономии дискового пространства, сжатые данные нельзя шифровать. Сжатие и шифрование — две взаимоисключающие характеристики NTFS-томов. Применить сразу обе технологии нельзя. Дополнительные сведения о шифровании вы найдете далее в разделе «Шифрование дисков и данных». При попытке сжатия зашифрованных данных данные автоматически расшифровываются, а затем сжимаются. Аналогично, при шифровании сжатых данных данные распаковываются, а затем шифруются.

Сжатие дисков

Чтобы сжать диск и все его содержимое, выполните следующие действия:

- В Проводнике (Windows Explorer) или оснастке Управление дисками (Disk Management), щелкните правой кнопкой диск, который нужно сжать, и выберите **Свойства (Properties)**.
- Установите флажок **Сжать этот диск для экономии места (Compress Drive To Save Disk Space)** и щелкните **OK**.

Сжатие каталогов и файлов

Если вы не хотите сжимать диск целиком, папки и файлы можно сжимать выборочно. Чтобы сжать файл или папку, выполните следующие действия:

1. В Проводнике (Windows Explorer) щелкните правой кнопкой файл или папку, которые нужно сжать, и выберите **Свойства (Properties)**.
2. На вкладке **Общие (General)** диалогового окна свойств щелкните **Другие (Advanced)**. В диалоговом окне **Дополнительные атрибуты (Advanced Attributes)** установите флажок **Сжимать содержимое для экономии места на диске (Compress Contents To Save Disk Space)**, как показано на рис. 12-18. Дважды щелкните **OK**.

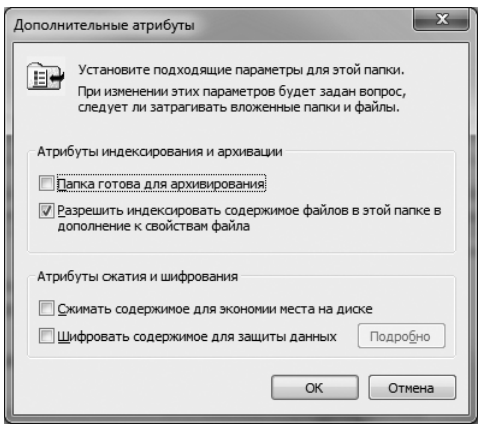

Рис. 12-18. Сжатие отдельного файла или папки

При сжатии отдельного файла он сначала помечается как сжатый, после чего выполняется его сжатие. При сжатии папки она помечается как сжатая, а затем сжимаются все находящиеся в ней файлы. Если в папке есть вложенные папки, выводится диалоговое окно, в котором можно задать сжатие всех

подпапок. Выберите переключатель **К данной папке и ко всем вложенным папкам и файлам (Apply Changes To This Folder, Subfolders, And Files)** и щелкните **OK**. После сжатия папки любые файлы, добавляемые или копируемые в нее, сжимаются автоматически.

Примечание При перемещении несжатого файла с другого диска файл будет автоматически сжат. Если переместить несжатый файл в сжатую папку, находящуюся на том же NTFS-томе, файл сжат не будет.

Распаковка сжатых дисков

Чтобы отменить сжатие диска, выполните следующие действия:

1. В Проводнике (Windows Explorer) или оснастке Управление дисками (Disk Management), щелкните правой кнопкой диск с данными, который нужно распаковать, и выберите **Свойства (Properties)**.
2. Сбросьте флажок **Сжать этот диск для экономии места (Compress Drive To Save Disk Space)** и щелкните **OK**.

Совет Перед распаковкой сжатых данных выполняется проверка на наличие свободного пространства. Если объем занятого пространства превышает объем свободного пространства, распаковка может не получиться. Например, если сжатый диск занимает 150 Гб и еще 70 Гб свободно, свободного места для распаковки диска не хватит.

Распаковка сжатых папок и файлов

Чтобы отменить сжатие файла или папки, выполните следующие действия:

1. В Проводнике (Windows Explorer) щелкните правой кнопкой файл или папку и выберите **Свойства (Properties)**.
2. На вкладке **Общие (General)** диалогового окна свойств щелкните **Другие (Advanced)**. Сбросьте флажок **Сжимать содержимое для экономии места на диске (Compress Contents To Save Disk Space)** и щелкните **OK**. Еще два раза щелкните **OK**.

При отмене сжатия файла он распаковывается. При отмене сжатия папки распаковываются все файлы в ней. Если в папке есть вложенные папки, вам будет предложено отменить и их сжатие. Установите переключатель **К данной папке и ко всем вложенным папкам и файлам (Apply Changes To This Folder, Subfolders, And Files)** и щелкните **OK**.

Совет В Windows 7 для сжатия и распаковки данных используются также утилиты командной строки. Утилита сжатия называется Compact (Compact.exe), а утилита распаковки — Expand (Expand.exe).

Шифрование дисков и данных

Система NTFS обладает многими преимуществами по сравнению с другими доступными в Windows 7 файловыми системами. Одно из основных преимуществ заключается в способности автоматически шифровать и дешифровать данные в шифрованной файловой системе (Encrypting File System, EFS). Шифрование — это дополнительный уровень защиты данных, заслон, отделя-

ющий других пользователей от содержимого шифрованных файлов, так что доступ к данным есть только у одного пользователя. Это преимущество таит в себе и недостаток: чтобы авторизованные пользователи смогли получить доступ к данным, означенный пользователь должен отменить шифрование.

Примечание Мы уже говорили о том, что шифрованные файлы нельзя сжать. Шифрование и сжатие — две взаимоисключающие возможности NTFS. Можно включить одну или другую функцию, но не обе сразу.

Общие сведения о сжатии и шифрованной файловой системе

Сжатие файлов поддерживается на уровне папки и уровне файла. Любой файл, помещаемый в зашифрованную папку, автоматически шифруется. Файлы в шифрованном формате может прочесть только пользователь, зашифровавший файл. Чтобы файл могли прочитать другие пользователи, его нужно дешифровать.

У каждого шифрованного файла есть уникальный ключ шифрования. Это означает, что шифрованные файлы, как и все остальные, можно копировать, перемещать и переименовывать. В большинстве случаев эти действия не влияют на шифрование данных (см. раздел «Работа с шифрованными файлами и папками».) У пользователя, зашифровавшего файл, доступ к файлу есть всегда, при условии что на компьютере имеется сертификат открытого ключа пользователя. Для этого пользователя процесс шифрования и дешифрования выполняется автоматически и прозрачно.

За шифрование и дешифрование файлов отвечает файловая система EFS. Ее стандартная настройка позволяет пользователям шифровать файлы без специального разрешения. Шифрование файлов выполняется на основе открытого и закрытого ключа, автоматически генерируемого для пользователя.

Сертификаты шифрования хранятся вместе с данными в профиле пользователя. Чтобы пользователь, работающий на нескольких компьютерах, мог воспользоваться шифрованием, администратор должен настроить для него перемещаемый профиль. Он обеспечит доступ к данным профиля и сертификатам открытого ключа с других компьютеров. Без этого пользователь не сможет открыть свои шифрованные файлы на другом компьютере.

Совет По умолчанию для шифрования применяется алгоритм AES-128-CBC. Для усиления защиты в Windows 7 поддерживается алгоритм шифрования Triple DES (шифрование трафика TSL, алгоритм открытого ключа RSA для обмена ключами TSL и проверки подлинности, а также хеширование SHA-1 для всех потребностей хеширования TLS). Чтобы воспользоваться шифрованием Triple DES, включите в групповой политике параметр **Системная криптография: Использовать FIPS-совместимые алгоритмы для шифрования (System Cryptography: Use FIPS Compliant Algorithms For Encryption)**. Он находится в узле **Конфигурация компьютера\Политики\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности (Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options)**. Независимо от выбранного алгоритма шифрования, администраторы, назначенные агентами восстановления, могут при необходимости дешифровать данные. Если включено шифрование Triple DES, в Internet Explorer для SSL будет использоваться только протокол TLS, который поддерживается не всеми веб-сайтами.

Шифрование дисков BitLocker и EFS — разные функции, но обе они имеют встроенную систему восстановления данных. Она обеспечивает восстановление шифрованных данных в случае потери или удаления сертификата открытого ключа пользователя. Типичный пример: когда пользователь увольняется и его учетная запись удалена, руководителю все равно необходим доступ к данным пользователя для сохранения нужных файлов. Если учетная запись пользователя удалена, для доступа к шифрованным томам и файлам необходимо снять шифрование или переместить файлы на тома FAT или FAT32, для которых не включено шифрование BitLocker (шифрование EFS на таких томах не поддерживается).

Для доступа к шифрованным файлам после удаления учетной записи пользователя нужен агент восстановления. Он обладает доступом к ключу шифрования файлов, необходимому для их разблокирования. При этом у агентов восстановления нет доступа к закрытому ключу пользователя и к любой информации об этом ключе.

В Windows 7 можно шифровать тома без назначения агентов восстановления BitLocker, но без назначения агентов восстановления EFS файлы шифровать не получится. Агенты восстановления EFS назначаются автоматически, необходимые сертификаты восстановления также генерируются автоматически. Таким образом, шифрованные файлы всегда можно восстановить.

Есть два уровня агентов восстановления:

- **Домен** Агент восстановления для домена настраивается автоматически при установке первого контроллера домена. По умолчанию агентом восстановления является администратор домена. Он волен назначить дополнительных агентов восстановления в групповой политике. Администраторы домена могут также делегировать полномочия агента восстановления назначенным администраторам безопасности.
- **Локальный компьютер** Если компьютер входит в рабочую группу или работает в изоляции, агентом восстановления по умолчанию является администратор локального компьютера. Можно назначать дополнительных агентов восстановления. Если вы даже в домене хотите использовать локальных агентов восстановления, удалите политику восстановления из групповой политики домена.

Если агенты восстановления не нужны, удалите их. Однако помните, что при удалении всех агентов восстановления EFS шифрование файлов выполняться не будет.

Шифрование папок и файлов

В NTFS-томах есть возможность выборочного шифрования файлов и папок. При шифровании файла его данные преобразуются в шифрованный формат, доступный только пользователю, выполнившему шифрование файла. Пользователи могут шифровать файлы только при наличии соответствующего разрешения. При шифровании папки она помечается как шифрованная, но в действительности шифрование применяется только к файлам вну-

три нее. Все созданные в папке или добавленные в нее файлы помечаются как шифрованные и автоматически шифруются.

Чтобы применить шифрование к файлу или папке, выполните следующие действия:

1. Щелкните правой кнопкой файл или папку, которые нужно зашифровать, и выберите **Свойства (Properties)**.
2. На вкладке **Общие (General)** диалогового окна свойств щелкните кнопку **Другие (Advanced)**. Установите флажок **Шифровать содержимое для защиты данных (Encrypt Contents To Secure Data)**. Дважды щелкните **OK**.

Примечание Нельзя шифровать сжатые, системные файлы и файлы, доступные только для чтения. При попытке зашифровать сжатые файлы они автоматически распаковываются, а затем шифруются. При попытке шифрования системных файлов возникает ошибка.

При шифровании отдельного файла он помечается как шифрованный, после чего выполняется шифрование. При шифровании папки она помечается как шифрованная, а затем выполняется шифрование всех находящихся в ней файлов. Если в папке есть вложенные папки, выводится диалоговое окно, в котором предлагается зашифровать все подпапки. Установите переключатель **К данной папке и ко всем вложенным папкам и файлам (Apply Changes To This Folder, Subfolders, And Files)** и щелкните **OK**.

Примечание На томах NTFS при перемещении, копировании и переименовании файлы остаются шифрованными. Если переместить шифрованный файл на диск FAT, FAT32 или exFAT перед копированием или перемещением он автоматически дешифруется. Это означает, что для копирования и перемещения файла нужны соответствующие разрешения.

Работа с шифрованными файлами и папками

Как уже отмечалось, шифрованные файлы и папки можно копировать, перемещать и переименовывать как любые другие файлы. Это действительно так, но с одной оговоркой — в большинстве случаев. При работе с шифрованными файлами на NTFS-томах одного компьютера проблем у вас не возникнет. Трудности могут появиться при работе с другими файловыми системами или на других компьютерах. Вот наиболее распространенные сценарии:

- **Копирование между томами одного компьютера** При копировании или перемещении шифрованного файла или папки из одного NTFS-тома в другой NTFS-том одного компьютера шифрование с файла не снимается. Однако при копировании или перемещении шифрованного файла на том FAT, FAT32 или exFAT перед перемещением шифрование с файла снимается, и он перемещается как обычный файл. Файловые системы FAT, FAT32 и exFAT не поддерживают шифрование.
- **Копирование между томами на разных компьютерах** При копировании или перемещении шифрованного файла или папки на NTFS-том другого компьютера файл остается зашифрованным, при условии что на

целевом компьютере у вас есть разрешение на шифрование файлов, и удаленный компьютер является доверенным для делегирования. В противном случае шифрование снимается, и файл перемещается как обычный файл. То же самое происходит при копировании или перемещении шифрованных файлов на тома FAT, FAT32 или exFAT на другом компьютере.

Переместив важный шифрованный файл, обязательно проверьте, что шифрование не снято. Щелкните файл правой кнопкой и выберите **Свойства (Properties)**. На вкладке **Общие (General)** диалогового окна свойств щелкните **Другие (Advanced)**. Флажок **Шифровать содержимое для защиты данных (Encrypt Contents To Secure Data)** должен быть установлен.

Настройка политики восстановления

В домене для контроллеров домена и рядовых компьютеров политики восстановления EFS и BitLocker настраиваются автоматически. Агентами восстановления EFS и BitLocker для всех компьютеров домена по умолчанию назначаются администраторы домена. В рабочих и домашних группах агентом восстановления EFS на изолированной рабочей станции назначается локальный администратор. Агенты восстановления BitLocker в домашних и рабочих группах по умолчанию не назначаются.

Просмотреть, назначить и удалить агентов восстановления можно в консоли Групповая политика (Group Policy). Выполните следующие действия:

1. В оснастке Редактор управления групповыми политиками (Group Policy Management Editor) откройте для редактирования объект GPO.
2. Разверните узел **Конфигурация компьютера\Политики\Конфигурация Windows\Параметры безопасности\Политики открытого ключа (Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies)** Далее разверните узел в соответствии с нужным типом агента восстановления — **Шифрующая файловая система (EFS) (Encrypting File System)** или **Шифрование диска BitLocker (BitLocker Drive Encryption)**. В групповой политике откройте узел **Агенты восстановления шифрованных данных (Encrypted Data Recovery Agents)**.

   На правой панели перечислены текущие сертификаты восстановления, упорядоченные по выдавшему центру, владельцу, сроку действия, назначению и другим свойствам.
3. Чтобы назначить дополнительного агента восстановления, щелкните правой кнопкой узел **Шифрующая файловая система EFS (Encrypting File System)** или **Шифрование диска BitLocker (BitLocker Drive Encryption),** и выберите команду **Добавить агент восстановления данных (Add Data Recovery Agent)**. В открывшемся Мастере добавления агента восстановления (Add Recovery Agent Wizard) выберите ранее созданный сертификат, который был назначен пользователю, и отметьте его как сертификат восстановления. Щелкните **Далее (Next)**.

4. На странице **Выбор агентов восстановления (Select Recovery Agents)** щелкните **Обзор каталога (Browse Directory)**. В диалоговом окне **Поиск: пользователи, контакты и группы (Find Users, Contacts, And Groups)** выберите нужного пользователя.

Примечание Чтобы назначить дополнительных агентов восстановления, в домене должен иметься корневой центр сертификации (ЦС). В оснастке диспетчера сертификатов создайте личный сертификат по шаблону Агент восстановления EFS (EFS Recovery Agent). Для использования сертификата запрос на сертификат должен быть утвержден в корневом ЦС.

5. Чтобы удалить агент восстановления, выделите соответствующий сертификат на правой панели и нажмите клавишу Delete. Щелкните **Да (Yes)**, чтобы подтвердить удаление сертификата. Если политика восстановления EFS пуста (поскольку другие агенты восстановления не назначены), функция EFS будет отключена и шифрование файлов станет недоступно.

Общий доступ к дешифрованным файлам

По умолчанию шифрованные файлы может просматривать только их владелец. Чтобы открыть доступ к шифрованному файлу для других пользователей, его необходимо дешифровать или предоставить особый доступ к файлу, выполнив следующие действия:

1. В Проводнике (Windows Explorer) щелкните правой кнопкой файл или папку и выберите **Свойства (Properties)**.
2. На вкладке **Общие (General)** диалогового окна свойств щелкните **Другие (Advanced)**. В диалоговом окне **Дополнительные атрибуты (Advanced Attributes)** щелкните **Подробно (Details)**.

   В открывшемся диалоговом окне **Пользовательский доступ к (User Access To)** перечислены пользователи, имеющие доступ к шифрованному файлу.
3. Чтобы разрешить доступ к файлу другому пользователю, щелкните **Добавить (Add)**.
4. Если у пользователя, которому предполагается предоставить доступ, есть сертификат, выберите имя пользователя из списка и щелкните **OK**. В противном случае найдите пользователя, щелкнув **Найти пользователя (Find User)**.

Дешифрование файлов и папок

Чтобы дешифровать файл или папку, выполните следующие действия:

1. В Проводнике (Windows Explorer) щелкните правой кнопкой файл или папку и выберите **Свойства (Properties)**.
2. На вкладке **Общие (General)** диалогового окна свойств щелкните **Другие (Advanced)**. Сбросьте флажок **Шифровать содержимое для защиты данных (Encrypt Contents To Secure Data)**. Дважды щелкните **OK**.

Файлы будут дешифрованы и возвращены в исходное состояние. В папках дешифруются все файлы. Если в папке есть вложенные папки, вам будет предложено снять шифрование и с них. Установите переключатель **К данной папке и ко всем вложенным папкам и файлам (Apply Changes To This Folder, Subfolders, And Files)** и щелкните **OK**.

Совет В Windows 7 есть утилита командной строки для шифрования и дешифрования данных — это Cipher (Cipher.exe). Если ввести в командной строке команду cipher без дополнительных параметров, будет выведено состояние шифрования всех папок в текущей папке.

Глава 13

Защита файлов и общий доступ к ресурсам

В домене ли, в рабочей или домашней группе мало найдется аспектов работы операционной системы, которые были бы более важны, чем безопасность файлов и их совместное использование. При этом защита и общий доступ к файлам настолько взаимосвязаны, что трудно обсуждать один аспект, не упоминая другой. Защита файлов предполагает обеспечение безопасности данных на ваших компьютерах за счет ограничения доступа, а совместное использование файлов, напротив, позволяет делиться данными, предоставляя доступ к ним другим пользователям.

Методы защиты и совместного использования файлов

На компьютерах Windows 7 реализация защиты и совместного использования файлов определяется двумя факторами: форматом диска и настройками компьютера. От формата локального диска зависит набор функций, обеспечивающих безопасность файлов. Локальные диски могут быть отформатированы в файловых системах FAT (FAT16, FAT32) или NTFS. Параметры безопасности для томов FAT и NTFS значительно различаются:

- В FAT возможности по управлению доступом к файлам весьма ограничены. Файлы можно сделать доступными только для чтения, скрытыми или системными, но отменить эти настройки может любой пользователь, имеющий доступ к тому FAT. Это означает, что защиты против доступа к файлу или его удаления, по сути, не существует. Любой пользователь может удалить любой файл без каких-либо ограничений.
- В NTFS вы полностью управляете доступом к файлам и папкам, назначая пользователям разрешения, которые будут избирательно отказывать в доступе, разрешать полный доступ или ограничивать его. Разрешения можно задавать как для индивидуальных пользователей, так и для групп. Тем самым осуществляется детальный контроль над доступом к информации. Например, вы можете открыть пользователям группы Sales Managers полный доступ к конкретной папке и ее файлам, тогда как у пользователей группы Sales Reps не будет возможности даже просматривать ее содержимое.

Настройки компьютера определяют, каким образом может осуществляться общий доступ к файлам. В Windows 7 поддерживаются две модели общего доступа:

- **Стандартный общий доступ** Позволяет совместно пользоваться файлами в любой папке на компьютере. Чтобы определить, кто имеет доступ к общим папкам, вы применяете два вида разрешений: разрешения NTFS (описаны в разделе «Управление доступом к файлам и папкам средствами NTFS» этой главы) и разрешения общего доступа (описаны в разделе «Общий доступ к файлам и папкам в сети»). В совокупности разрешения NTFS и сетевые разрешения позволяют указывать, кто имеет доступ к общим папкам, а также задавать уровень доступа. Вам нет необходимости перемещать файлы, к которым вы открываете общий доступ, в какое-то особое расположение.
- **Общий доступ к специальной папке** Позволяет открывать общий доступ к файлам, которые находятся в папке %SystemDrive%\Users\Public. Пользователи и группы получают доступ к общим файлам на основании разрешений общей папки. Когда вы копируете или перемещаете файлы в общую папку, их разрешения на доступ заменяются разрешениями общей папки. К ним также добавляются некоторые дополнительные разрешения. Подробнее — в разделе «Использование общей папки и настройка доступа к ней» далее в этой главе.

Примечание При использовании стандартного общего доступа локальные пользователи не получают автоматически доступ к любым данным, сохраненным на компьютере. Локальный доступ к файлам и папкам полностью управляется настройками безопасности на локальном диске. Если локальный диск отформатирован в файловой системе FAT, вы можете защищать файлы и папки, делая их доступными только для чтения, системными или скрытыми, но это не позволит ограничить доступ. Если локальный диск отформатирован в файловой системе NTFS, вы полностью контролируете доступ, разрешая или запрещая его отдельным пользователям или группам.

При совместном пользовании специальной общей папкой скопированные или перемещенные в нее файлы доступны любому пользователю, локально вошедшему в систему, независимо от типа его учетной записи (обычная учетная запись или учетная запись администратора). Доступ к общей папке может также предоставляться через сеть. При этом общая папка и ее содержимое открыты любому пользователю, имеющему доступ к компьютеру через сеть.

В отличие от Windows XP, где в данный момент может использоваться только одна модель общего доступа, в Windows 7 допускается использование одновременно обеих моделей. Ключевое преимущество стандартного общего доступа состоит в том, что пользователи могут предоставлять в совместное использование любую папку на компьютере, при этом не перемещая файлы и папки. С другой стороны, общие папки — зона риска. Открыв общий доступ к одной из папок компьютера, вы можете раскрыть больше информации, чем предполагаете.

В Проводнике Windows 7 есть несколько новых команд для управления папками.

- **Добавить в библиотеку (Include In Library)** Создает ссылку на папку и ее содержимое в библиотеке Документы (Documents), Музыка (Music), Изображения (Pictures), Видео (Video) и др. Это позволяет пользователю просматривать содержимое папки и работать с нею как с частью библиотеки. Пользователь, работая с файлом в папке библиотеки, фактически работает с файлом в его первоначальном расположении.
- **Общий доступ (Share With)** Открывает общий доступ к папке. В домашней группе папку можно предоставить в общее пользование всем членам домашней группы, делая ее доступной только для чтения или для чтения и записи. В рабочей группе или домене имеется возможность предоставления доступа к папке только конкретным пользователям. В любой конфигурации пользователи могут также выбрать вариант **Никому из пользователей (Nobody)**, который, по сути, прекращает совместное пользование.

Конфигурация общего доступа по умолчанию на компьютере зависит от того, является ли он членом домашней группы, рабочей группы или домена. Создавая домашнюю группу, вы указываете, какие типы файлов следует предоставить в общее пользование, а также нужно открывать ли общий доступ к принтерам. После этого на компьютерах одной домашней группы автоматически открывается общий доступ к изображениям, музыке, видео, документам и принтерам.

Организовать общий доступ к папкам в пределах домашней группы довольно просто. Выполните следующие действия:

1. Выберите папку в Проводнике Windows.
2. Щелкните кнопку **Общий доступ (Share With)** на панели инструментов и выберите команду **Домашняя группа (Чтение) (Homegroup (Read))** или **Домашняя группа (Чтение и запись) (Homegroup (Read/Write))**.

Такой простой подход к общему доступу может показаться привлекательным и для применения в рабочих группах. Тем не менее, он предоставляет слишком широкий доступ к данным пользователя и, как правило, не рекомендуется для использования на рабочем месте. Именно поэтому стоит рекомендовать даже пользователям домашних групп предоставлять общий доступ только конкретным людям, а не всем пользователям. Общий доступ для конкретных пользователей — единственный метод, который применяется в рабочих группах и доменах.

Чтобы включить общий доступ для конкретных пользователей, выполните следующие действия:

1. Выберите папку в Проводнике Windows.
2. Щелкните кнопку **Общий доступ (Share With)** на панели инструментов и выберите команду **Конкретные пользователи (Specific People)**. Запустится мастер Общий доступ к файлам (File Sharing). По умолчанию владельцем общего ресурса становится локальная группа Администраторы (Administrators). Пользователю, в данный момент работающему в системе, предоставляется доступ для чтения и записи.

3. Используйте параметры мастера Общий доступ к файлам (File Sharing), чтобы выбрать пользователей, которым будет предоставлен доступ к общим файлам. Например, чтобы включить всех пользователей с локальными учетными записями, введите в поле **Пользователи (Users)** и щелкните кнопку **Добавить (Add)**. Помните, что группа Пользователи (Users) отличается от группы Все (Everyone). Первая включает в себя только пользователей домена или локальных пользователей, а вторая — всех пользователей, имеющих разрешение к компьютеру.
4. По умолчанию добавленному пользователю предоставляется доступ только для чтения. Чтобы изменить уровень доступа для пользователя или группы, щелкните имя пользователя или группы и выберите вариант **Чтение (Read)** или **Чтение и запись (Read/Write)**.
5. Щелкните кнопку **Общий доступ (Share)**, чтобы сделать папку общей, а затем щелкните кнопку **Готово (Done)**.

Чтобы отменить общий доступ к папке, выполните следующие действия:

1. Выберите папку в Проводнике Windows.
2. На панели инструментов щелкните кнопку **Общий доступ (Share With)** и выберите команду **Никому из пользователей (Nobody)**.

Когда вы создаете на компьютере первую общую папку, Windows по умолчанию создает в брандмауэре Windows исключение Общий доступ к файлам и принтерам (File And Printer Sharing). Оно позволяет другим компьютерам сети направлять через брандмауэр входящий трафик SMB для получения доступа к общему ресурсу. При этом открываются следующие порты:

- **UDP 137** Разрешение имен NetBIOS.
- **UDP 138** Передача и прием датаграмм NetBIOS.
- **TCP 139** Используется службой сеанса NetBIOS.
- **Динамические порты для ICMPv4 и ICMPv6** Используются для запроса отклика, если он применим.

Таково краткое описание работы стандартного общего доступа. Далее в этой главе я подробнее расскажу об общем доступе для конкретных пользователей. Однако прежде чем кто угодно сможет использовать общий доступ к чему угодно, общий доступ необходимо включить.

Настройки общего доступа через сеть призваны обеспечить должный уровень безопасности для каждой категории сетей, к которым может подключаться компьютер. Поэтому в Windows поддерживается отдельный сетевой профиль для каждого типа сетей. Как правило, по умолчанию большинство настроек сетевого обнаружения и общего доступа отключено. Чтобы настроить параметры сетевого обнаружения и общего доступа, выполните следующие действия:

1. Щелкните кнопку **Пуск (Start)** и выберите команду **Панель управления (Control Panel)**. В категории **Сеть и Интернет (Network And Internet)** панели управления щелкните ссылку **Выбор параметров домашней группы и общего доступа к данным (Choose Homegroup And Sharing**

Options). Затем перейдите по ссылке **Изменение дополнительных параметров общего доступа (Change Advanced Sharing Settings)**.

2. Для каждого сетевого профиля имеется отдельная панель управления с параметрами конфигурации. Используйте кнопку со стрелкой, чтобы развернуть профиль, с которым хотите работать.
3. Сетевое обнаружение определяет, может ли данный компьютер находить другие компьютеры и устройства сети, и могут ли другие компьютеры сети обнаруживать этот компьютер. Включите или отключите сетевое обнаружение, установив соответствующий переключатель.
4. Общий доступ к файлам или принтерам означает, что компьютер может предоставлять файлы и принтеры для совместного пользования. Включите или отключите общий доступ к файлам и принтерам, выбрав соответствующий переключатель.
5. Доступ к общим папкам означает, что компьютер может предоставлять доступ к файлам в общих (public) папках. Включите или отключите доступ к общим папкам, выбрав соответствующий переключатель.
6. Потоковая передача мультимедиа (media streaming) позволяет пользователям делиться музыкой, видеофайлами, рисунками, а также получать доступ к музыке, видеофайлам и рисункам на других компьютерах. Включите потоковую передачу, щелкнув соответствующую кнопку, а потом настройте ее параметры. Разрешив другим пользователям слушать музыку, просматривать видео и рисунки со своего компьютера, вы рискуете снизить производительность компьютера. Подумайте, стоит ли включать эту функцию.
7. Для безопасной передачи данных, находящихся в общем доступе, Windows использует шифрование. По умолчанию в большинстве конфигураций применяется 128-разрядное шифрование. Убедитесь, что компьютеры и устройства, которые вы предоставляете для совместного использования, поддерживают этот уровень. При необходимости выберите более низкий уровень шифрования или обновите поддержку шифрования на устройствах и компьютерах.
8. В рабочих и домашних группах вы можете защитить общие данные паролем, чтобы доступ к ним получали только пользователи, у которых есть учетная запись и пароль на локальном компьютере. Включите или выключите защиту общих данных паролем, установив соответствующий переключатель.
9. Щелкните кнопку **Сохранить изменения (Save Changes)**, чтобы сохранить настройки.

Чтобы при помощи групповой политики запретить присоединение компьютеров к домашним группам, включите параметр **Запретить присоединение компьютера к домашней группе (Prevent The Computer From Joining A Homegroup)**. Он находится в папке **Административные шаблоны (Administrative Templates)** узла **Конфигурация компьютера (Computer**

Configuration), в узле **Компоненты Windows/Домашняя группа (Windows Components\Homegroup)**.

Групповая политика позволяет также ограничить действие общего доступа. Ключевое ограничение на общий доступ накладывается параметром **Запретить пользователям в их профиле предоставлять общий доступ к файлам (Prevent Users From Sharing Files Within Their Profiles)**. Он расположен в папке **Административные шаблоны (Administrative Templates)** узла **Конфигурация пользователя (User Configuration)**, в узле **Компоненты Windows/Общий сетевой доступ (Windows Components\Network Sharing)**. Этот параметр определяет, разрешен ли общий доступ к содержимому папок, связанных с профилями пользователей, главным образом, папки %SystemDrive%\Users. Настраивая политику **Запретить пользователям в их профиле предоставлять общий доступ к файлам (Prevent Users From Sharing Files Within Their Profiles)**, помните о следующем:

- Если эта политика не настроена (состояние по умолчанию), пользователям разрешено открывать общий доступ к файлам внутри своего профиля другим пользователям сети, при условии что администратор компьютера разрешил общий доступ к файлам. Чтобы разрешить общий доступ, администратору достаточно предоставить в общий доступ файл в своем профиле.
- Если эта политика включена, пользователи не могут открывать общий доступ к файлам в своем профиле с использованием мастера Общий доступ к файлам (File Sharing), а сам мастер Общий доступ к файлам (File Sharing) не будет создавать общие ресурсы в папке %SystemDrive%\Users.
- Если эта политика отключена, например, чтобы отменить наследуемую настройку, пользователям разрешено открывать общий доступ к файлам в своих профилях для других пользователей сети, при условии что администратор компьютера разрешил общий доступ к файлам.

Чтобы настроить политику **Запретить пользователям в их профиле предоставлять общий доступ к файлам (Prevent Users From Sharing Files Within Their Profiles)**, выполните следующие действия:

1. Откройте объект GPO для редактирования в редакторе управления групповой политикой. Разверните узлы **Конфигурация пользователя (User Configuration)**, **Административные шаблоны (Administrative Templates)**, **Компоненты Windows (Windows Components)** и **Общий сетевой доступ (Network Sharing)**.
2. Дважды щелкните политику **Запретить пользователям в их профиле предоставлять общий доступ к файлам (Prevent Users From Sharing Files Within Their Profiles)**.
3. Установите переключатель **Не задано (Not Configured)**, **Включить (Enabled)** или **Отключить (Disabled)**.
4. Щелкните **OK**.

Хотя использование папки общих документов может показаться заманчивым, в большинстве организаций — даже в небольших — следует отдавать предпочтение стандартному общему доступу к папкам. Такой доступ обеспечивает большую безопасность и лучшую защиту, поскольку позволяет не только открыть данные, но и надежно заблокировать их.

Разрешения общего доступа применяются только при попытке пользователя получить доступ к файлу или папке через сеть. А вот разрешения NTFS используются всегда — как при локальном входе в систему, так и при осуществлении доступа к файлу или папке через сеть. Если доступ к данным осуществляется удаленно, сначала применяются разрешения общего доступа, а затем — разрешения NTFS.

Во многих случаях это означает, что разрешения выступают в роли своего рода защитного слоя вокруг ваших данных. Первый слой — разрешения NTFS — защищает данные от несанкционированного локального доступа. Если пользователь входит в систему локально, разрешения NTFS открывают ему доступ к файлам и папкам или закрывают его. Второй слой — разрешения общего доступа — используются при удаленном доступе. Если пользователь хочет работать с информацией удаленно, на основании разрешений общего доступа определяется начальный доступ к данным. Но, поскольку данные защищены также разрешениями NTFS, пользователь должен успешно пройти и этот контроль, прежде чем начнет работать с файлами и папками.

Управление доступом к файлам и папкам средствами NTFS

При попытке доступа к файлу всегда производится оценка разрешений доступа файловой системы NTFS. Они довольно сложны, и для успешной работы с ними вам необходимо разобраться в следующих аспектах:

- базовые разрешения доступа;
- специальные разрешения доступа;
- владением файлом;
- наследование свойств;
- действующие разрешения.

Базовые разрешения

В Windows 7 владелец файла или папки имеет право разрешить доступ к этому ресурсу или запретить его так же, как могут сделать это члены группы администраторов. Разрешение можно предоставить (доступ пользователю или группе разрешен) или отозвать (доступ пользователю или группе запрещен). Помните, что запрет доступа имеет более высокий приоритет, чем его разрешение. Если пользователь является членом двух групп, одной из которых доступ разрешен, а другой — запрещен, пользователю будет отказано в доступе.

Чтобы просмотреть назначенные в настоящее время базовые разрешения в Проводнике Windows, щелкните файл или папку правой кнопкой мыши, выберите команду **Свойства (Properties)** и в открывшемся диалоговом окне перейдите на вкладку **Безопасность (Security)**.

Как показано на рис. 13-1, в список **Группы или пользователи (Group Or User Names)** включены пользователи и группы с разрешениями, заданными для этого ресурса. Выделите пользователя или группу, и его разрешения отобразятся в списке **Разрешения для (Permissions For)**. Если разрешения затенены (недоступны), значит, они унаследованы у родительской папки. Наследование подробно описано в разделе «Наследование разрешений» да-

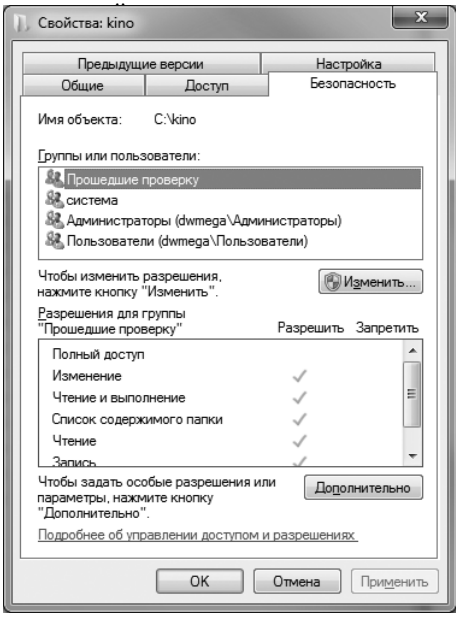

Рис. 13-1. На вкладке Безопасность (Security) показаны текущие разрешения

Работа с базовыми разрешениями и их назначение

Все разрешения хранятся в файловой системе как часть списка управления доступом (Access Control List, ACL), назначенного файлу или папке. Как показано в табл. 13-1, для папок используются шесть базовых разрешений, для файлов — пять. Некоторые разрешения наследуются у родительской папки, но все они обязательно явным образом определяются на том или ином уровне иерархии файловой системы.

Табл. 13-1. Базовые разрешения на доступ к файлам и папкам

Разрешение	Описание
Полный доступ (Full Control)	Предоставляет пользователю или группе полный доступ к выбранному файлу или папке. Разрешает чтение, запись, внесение изменений и удаление файлов и подпапок. Пользователь с полным доступом к файлу или папке имеет также право изменять разрешения и становиться владельцем папки или файла. Пользователь с полным доступом к папке может удалять файлы в ней независимо от уровня доступа к этим файлам. При выборе этого разрешения остальные разрешения предоставляются автоматически
Изменение (Modify)	Позволяет пользователю или группе читать, записывать, изменять и удалять файлы. Пользователь с этим разрешением также может создавать файлы и подпапки, но не может становиться их владельцем. Выбирая это разрешение, вы также предоставляете все разрешения, перечисленные ниже
Чтение и выполнение (Read & Execute)	Позволяет просматривать и составлять список файлов и подпапок, а также запускать исполняемые файлы. Если это разрешение применено к папке, оно наследуется всеми ее файлами и подпапками. При выборе этого разрешения предоставляются также разрешения Список содержимого папки (List Folder Contents) и Чтение (Read)
Список содержимого папки (List Folder Contents)	Аналогично разрешению Чтение и выполнение (Read & Execute), но применяется только к папкам. Позволяет просматривать и составлять список файлов и подпапок, а также запускать исполняемые файлы. В отличие от разрешения Чтение и выполнение (Read & Execute) это разрешение наследуется только подпапками, но не файлами внутри самой папки или ее подпапок
Чтение (Read)	Позволяет пользователю или группе посматривать список содержимого папки. Пользователь с этим разрешением может просматривать атрибуты файла, просматривать разрешения и синхронизировать файлы. Чтение (Read) — единственное разрешение, необходимое для запуска сценариев. Оно также требуется для доступа к ярлыку и его целевому объекту
Запись (Write)	Позволяет пользователю или группе создавать новые файлы и записывать данные в существующие файлы. Пользователь с этим разрешением может также просматривать атрибуты файла, читать разрешения и синхронизировать файлы. У пользователя нет права удалять файлы и папки, но есть право удалять их содержимое

Важно не только продумывать набор базовых разрешений, но выбирать пользователей и группы, которым вы присваиваете эти разрешения. Если

пользователь или группа, разрешения для которых вы хотите настроить, уже присутствуют в списке **Группы или пользователи (Group Or User Names)** на вкладке **Безопасность (Security)**, для изменения разрешений щелкните кнопку **Разрешить (Edit)** и расставьте флажки в столбцах **Разрешить (Allow)** и **Запретить (Deny)**. Закончив настройку, щелкните **OK**.

Чтобы полностью отказать пользователю или группе в конкретном разрешении, установите соответствующие флажки в столбце **Запретить (Deny)**. Поскольку отказ в разрешении имеет приоритет над его предоставлении, флажки **Запретить (Deny)** полезны в двух следующих сценариях:

- Пользователь является членом группы, которой разрешение предоставлено. Вас устраивает, что это разрешение есть у группы, но вы не хотите, чтобы оно имелось у этого конкретного пользователя. Отмените наследуемое разрешение, отозвав его у этого конкретного пользователя.
- Разрешение унаследовано от родительской папки, но вы не хотите, чтобы оно имелось у конкретного пользователя или группы. Отмените наследуемое разрешение, отозвав его у этого пользователя или группы.

Если пользователя или группы, разрешения которых вы хотите настроить, нет в списке **Группы или пользователи (Group Or User Names)** на вкладке **Безопасность (Security)**, добавьте их, выполнив следующие действия:

1. На вкладке **Безопасность (Security)** щелкните кнопку **Изменить (Edit)**. Откроется диалоговое окно **Разрешения для (Permissions For)**.
2. Щелкните кнопку **Добавить (Add)**, чтобы открыть диалоговое окно **Выбор: «Пользователи» или «Группы» (Select Users, Computers, Service Accounts, Or Groups)**, показанное на рис. 13-2.

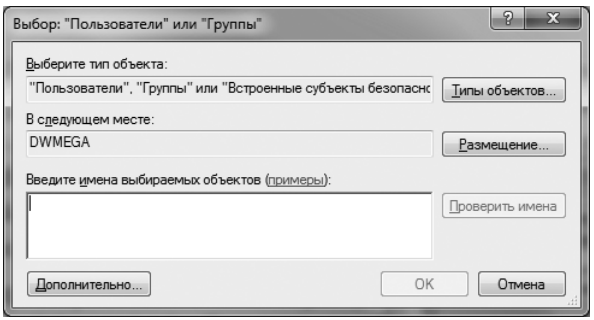

Рис. 13-2. Укажите пользователей или группы, разрешения для которых хотите настроить

Совет Всегда проверяйте значение поля **В следующем месте (From This Location)**. В рабочей группе вам доступны только локальные учетные записи и группы. В доменах значение в этом поле можно изменить. По умолчанию в нем значится домен, с учетной записью которого вы вошли в систему. Если для выбора учетных записей вы хотите использовать другое расположение, щелкните кнопку **Размещение (Locations)**. На экран будет выведен список расположений, в которых вы можете проводить поиск, включая текущий домен, доверенный домен и другие ресурсы, к которым у вас есть доступ.

3. Введите имя учетной записи пользователя или группы. Будьте внимательны: здесь нужно имя учетной записи, а не полное имя пользователя. При вводе нескольких имен разделяйте их точками с запятой.
4. Щелкните кнопку **Проверить имена (Check Names)**. Если для каждого введенного имени найдется одно соответствие, диалоговое окно автоматически обновится, а введенные имена будут подчеркнуты. Если соответствий будет несколько, вы увидите дополнительное диалоговое окно. Если никаких соответствий не найдено, вы некорректно ввели имя или вы работаете с неправильным расположением. Отредактируйте имя в диалоговом окне **Имя не найдено (Name Not Found)** и повторите попытку или щелкните кнопку **Размещение (Locations)**, чтобы задать новое место поиска. При обнаружении нескольких соответствий выберите имя или имена в диалоговом окне **Найдено несколько имен (Multiple Names Found)** и щелкните **OK**. Имена будут добавлены в список **Группы или пользователи (Group Or User Names)**.
5. Настройте разрешения для всех добавленных пользователей и групп, выделяя их имена и устанавливая и сбрасывая соответствующие флажки.

Специальные идентификаторы и оптимальные способы назначения разрешений

В Windows имеются специальные идентификаторы, облегчающие назначение разрешения. Чаще других применяются идентификаторы Создатель-владелец (Creator Owner) и Пользователи (Users), но иногда используются и другие, перечисленные в табл. 13-2. Специальные идентификаторы автоматически являются членам некоторых групп. Чтобы настроить разрешения для специального идентификатора, введите его имя, как вы вводите имя любого другого пользователя или группы.

Табл. 13-2. Специальные идентификаторы, используемые при назначении разрешений

Специальный идентификатор	Описание
Анонимный вход (Anonymous Logon)	Любые входы в сеть, при которых не предоставлялись учетные данные. Этот идентификатор используется для разрешения анонимного доступа к ресурсам, например к ресурсам веб-сервера
Все (Everyone)	Все интерактивные, удаленные и прошедшие проверку пользователи. Эта группа включает в себя гостей, но не включает анонимных пользователей
Интерактивные (Interactive)	Любой пользователь, вошедший в систему локально или при помощи подключения удаленного рабочего стола
Пользователи (Users)	Пользователи, прошедшие проверку, и пользователи домена. В Windows 7 рекомендуется использовать группу Пользователи (Users) вместо группы Все (Everyone)

Табл. 13-2. (*окончание*)

Специальный идентификатор	Описание
Прошедшие проверку (Authenticated Users)	Пользователи и компьютеры, подключающиеся к системе с именем пользователя и паролем; не включает пользователей, вошедших в систему с гостевой учетной записью, даже если ей назначен пароль
Сеть (Network)	Любой пользователь, вошедший в систему через сеть. Этот идентификатор используется, чтобы предоставить удаленным пользователям доступ к ресурсу. Сюда не входят пользователи, вошедшие в систему при помощи подключения удаленного рабочего стола
Создатель-владелец (Creator Owner)	Учетная запись, от имени которой создан файл или папка. В Windows 7 этот идентификатор обозначает учетную запись, имеющую полный контроль над файлом или папкой
Удаленный доступ (Dialup)	Пользователь, подключившийся к компьютеру при помощи соединения удаленного доступа. Этот идентификатор используется, чтобы отличать пользователей удаленного доступа от пользователей других типов

Разобравшись в специальных идентификаторах, вы сможете эффективнее использовать разрешения на томах файловой системы NTFS. Кроме того, при работе с разрешениями вы должны помнить о следующем:

- **Следуйте иерархии файловой системы** В назначении разрешений большую роль играет наследование. По умолчанию разрешения папки применяются ко всем ее файлам и подпапкам. Поэтому всегда начинайте настройку разрешений с корневой папки локального диска или с папки профиля пользователя (обе выступают как папки высшего уровня).
- **Разработайте план** Не настраивайте разрешения, не имея четкого плана. Если вы запутались в разрешениях папки и хотите повторить процедуру настройки «с нуля», настройте должным образом разрешения родительской папки, а затем сбросьте разрешения всех ее подпапок и файлов, как описано в разделе «Восстановление наследуемых разрешений» этой главы.
- **Предоставляйте доступ строго в пределах необходимости** Важным свойством разрешений на доступ к файлам NTFS, является то, что все они назначаются явным образом. Если вы не выдаете пользователю некоторое разрешение и он не является членом группы, у которой есть это разрешение, соответствующее действие пользователю запрещено. Назначая разрешения, помните об этом правиле. Всегда велик соблазн разрешить пользователям полный доступ вместо назначения только тех разрешений, которые им действительно необходимы. Не поддавайтесь ему, строго следуя *принципу минимальных полномочий*.
- **Используйте группы для эффективного управления разрешениями** По возможности делайте пользователей членами соответствующих

групп, а затем присваивайте разрешения группам, а не отдельным пользователям. При этом для определения полномочий нового пользователя его достаточно будет сделать членом соответствующей группы. Если пользователь переходит в другой отдел, вы легко измените его разрешения, соответствующим образом изменив его членство в группе. Допустим, Сара поступила на работу в отдел продаж, и вы добавили ее в группы SalesUS и SalesCan, чтобы предоставить ей доступ к общим данным групп. Затем она переходит в отдел маркетинга, и вы удаляете ее из групп SalesUS и SalesCan и добавляете в группы MarketingUS и MarketingCan. Такой подход гораздо более эффективен, чем редактирование свойств каждой папки, доступ к которой может потребоваться Саре.

Назначение специальных разрешений

Для более детального управления доступом в Windows 7 применяются специальные разрешения пользователей и групп. На самом деле, даже когда вы работаете с базовыми разрешениями, в реальности Windows 7 управляет набором соответствующих специальных разрешений, которые перечислены ниже:

- Чтение (Read):
  - Содержание папки / чтение данных (List Folder / Read Data).
  - Чтение атрибутов (Read Attributes).
  - Чтение дополнительных атрибутов (Read Extended Attributes).
  - Чтение разрешений (Read Permissions).
- Чтение и выполнение (Read) или Список содержимого папки (List Folder Contents):
  - Все специальные разрешения для разрешения Чтение (Read).
  - Траверс папок / выполнение файлов (Traverse Folder / Execute File).
- Запись (Write):
  - Создание файлов / запись данных (Create Files / Write Data).
  - Создание папок / дозапись данных (Create Folders / Append Data).
  - Запись атрибутов (Write Attributes).
  - Запись дополнительных атрибутов (Write Extended Attributes).
- Изменение (Modify):
  - Все специальные разрешения для разрешения Чтение (Read).
  - Все специальные разрешения для разрешения Запись (Write).
  - Удаление (Delete).
- Полный доступ (Full Control):
  - Все специальные разрешения, перечисленные выше.
  - Удаление подпапок и файлов (Delete Subfolders And Files).
  - Смена разрешений (Change Permissions).
  - Смена владельца (Take Ownership).

В табл. 13-3 описано, как в Windows 7 используются специальные разрешения.

Табл. 13-3. Специальные разрешения для файлов и папок

Специальное разрешение	Описание
Траверс папок / выполнение файлов (Traverse Folder / Execute File)	Специальное разрешение Траверс папки (Traverse Folder) позволяет переходить в подпапки, даже если у вас нет явного разрешения на чтение данных, содержащихся в папке. Специальное разрешение Выполнение файлов (Execute File) позволяет запускать исполняемый файл
Содержание папки / чтение данных (List Folder / Read Data)	Первое разрешение позволяет просматривать имена файлов и папок, второе — просматривать содержимое файла
Чтение атрибутов (Read Attributes)	Позволяет читать атрибуты файла или папки, помечающие их как доступные только для чтения, скрытые, системные и архивные
Чтение дополнительных атрибутов (Read Extended Attributes)	Позволяет просматривать расширенные атрибуты (именованные потоки данных), ассоциированные с файлом
Создание файлов / запись данных (Create Files / Write Data)	Первое разрешение позволяет добавлять в папку новые файлы. Второе разрешение позволяет перезаписывать существующие данные в файле, но не добавлять новые данные в существующий файл; для этого нужно разрешение Дозапись данных (Append Data))
Создание папок / дозапись данных (Create Folders / Append Data)	Первое разрешение позволяет создавать подпапки внутри папок. Второе разрешение позволяет добавлять данные в конец существующего файла, но не позволяет переписывать существующие данные; для этого нужно разрешение Запись данных (Write Data)
Запись атрибутов (Write Attributes)	Позволяет изменять атрибуты файла или папки, помечающие их как доступные только для чтения, скрытые, системные и архивные
Запись дополнительных атрибутов (Write Extended Attributes)	Позволяет изменять расширенные атрибуты (именованные потоки данных), ассоциированные с файлом
Удаление подпапок и файлов (Delete Subfolders And Files)	Позволяет удалять содержимое папки. Если у вас есть это разрешение, вы имеете право удалять подпапки и файлы в папке, даже если у вас нет разрешения Удаление (Delete) для этих подпапок или файлов
Удаление (Delete)	Позволяет удалить файл или папку. Если папка не пуста, и у вас нет разрешения Удаление (Delete) для одного или нескольких ее файлов и подпапок, вы не сможете ее удалить, если у вас нет разрешения Удаление подпапок и файлов (Delete Subfolders and Files)

Табл. 13-3. (*окончание*)

Специальное разрешение	Описание
Чтение разрешений (Read Permissions)	Позволяет читать все базовые и специальные разрешения, назначенные файлу или папке
Смена разрешений (Change Permissions)	Позволяет изменять базовые и специальные разрешения, назначенные файлу или папке
Смена владельца (Take Ownership)	Позволяет становиться владельцем файла или папки. По умолчанию администратор всегда может стать владельцем файла или папки, а также передать это разрешение другим
Синхронизация (Synchronize)	Позволяет синхронизировать файл или папку, находящиеся в автономном режиме

Чтобы просмотреть специальные разрешения файла или папки в Проводнике Windows, щелкните правой кнопкой нужный файл или папку и выберите команду **Свойства (Properties)**. В диалоговом окне **Свойства (Properties)** перейдите на вкладку **Безопасность (Security)** и щелкните кнопку **Дополнительно (Advanced)**, чтобы открыть диалоговое окно **Дополнительные параметры безопасности (Advanced Security Settings)**, показанное на рис. 13-3. В этом диалоговом окне разрешения представлены примерно так же, как на вкладке **Безопасность (Security)**, но здесь вы также видите, унаследованы ли текущие разрешения, если да, то откуда именно, а также к каким ресурсам применяются разрешения.

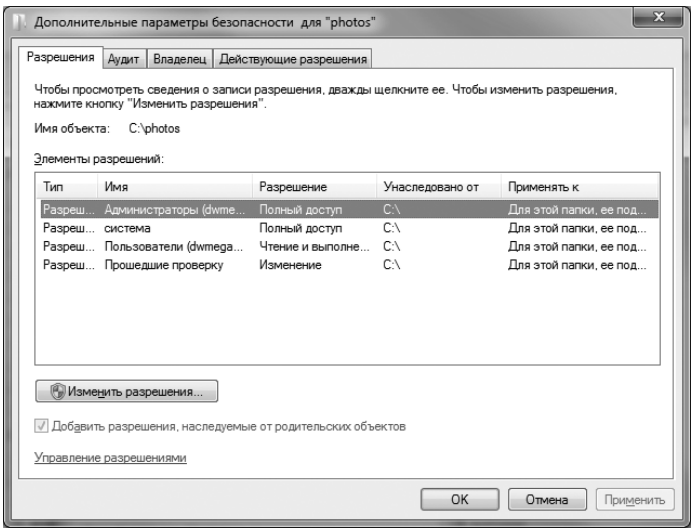

Рис. 13-3. Диалоговое окно Дополнительные параметры безопасности (Advanced Security Settings) для настройки специальных разрешений

Открыв диалоговое окно **Дополнительные параметры безопасности (Advanced Security Settings)**, щелкните кнопку **Изменить разрешения**

(Change Permissions). Откроется редактируемый вариант вкладки **Разрешения (Permissions)**, где вы сможете задать специальные разрешения, используя кнопки **Добавить (Add)**, **Изменить (Edit)** и **Удалить (Remove)**. Чтобы добавить в список пользователя или группу, а затем задать специальные разрешения, выполните следующие действия:

1. Щелкните кнопку **Добавить (Add)**, чтобы открыть диалоговое окно **Выбор: «Пользователь» или «Группа» (Select User, Computer, Service Account, Or Group)**.
2. Введите имя учетной записи пользователя или группы, которые входят в заданный домен или домен по умолчанию. Убедитесь, что вводите имя учетной записи пользователя, а не его собственное имя. За один раз можно ввести только одно имя.
3. Щелкните **OK**. Откроется диалоговое окно **Элемент разрешения для (Permission Entry For)**, показанное на рис. 13-4.

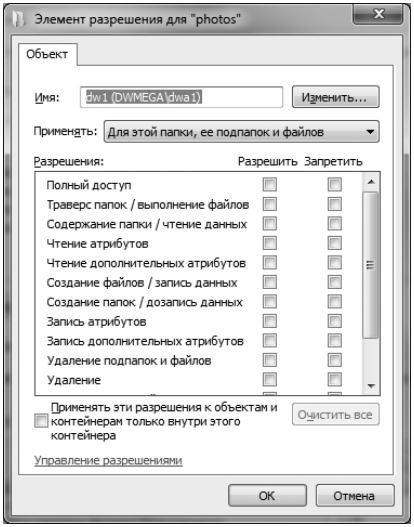

Рис. 13-4. Настройка специальных разрешений

4. Установите флажки **Разрешить (Allow)** или **Запретить (Deny)** у специальных разрешений, которые вы хотите настроить. Если какие-либо разрешения затенены, значит, они унаследованы от родительской папки. При необходимости вы можете перекрыть наследуемое разрешение, выбрав противоположное разрешение, например Запретить (Deny) вместо Разрешить (Allow).
5. Выберите в списке **Применять (Apply To)** способ наследования разрешений. Доступны следующие варианты:
   - **Только для этой папки (This Folder Only)** Разрешения применяются только к текущей папке.

- **Для этой папки, ее подпапок и файлов (This Folder, Subfolders and Files)** Разрешения применяются к самой папке, любым ее подпапкам и любым файлам в любой из этих папок.
- **Для этой папки и ее подпапок (This Folder and Subfolders)** Разрешения применяются к самой папке и любым ее подпапкам. Разрешения не применяются к файлам в любой из этих папок.
- **Для этой папки и ее файлов (This Folder and Files)** Разрешения применяются к самой папке и любым файлам в ней. Разрешения не применяются к подпапкам этой папки.
- **Только для подпапок и файлов (Subfolder and Files Only)** Разрешения применяются к любым подпапкам этой папки и любым файлам в любой из этих папок. Разрешения не применяются к самой папке.
- **Только для подпапок (Subfolder Only)** Разрешения применяются к любым подпапкам этой папки, но не к самой папке и не к файлам в любой из этих папок.
- **Только для файлов (Files Only)** Разрешения применяются к любым файлам в этой папке и к любым файлам в подпапках этой папки. Разрешения не применяются к самой папке или к ее подпапкам.

6. Закончив настройку разрешений, щелкните **OK**.

Владение файлами и назначение разрешений

Владелец файла или папки имеет право разрешить доступ к ресурсу или запретить его. Фактически, он имеет право полностью заблокировать ресурс для пользователей-неадминистраторов. После этого единственный способ восстановить доступ к этому ресурсу состоит в том, чтобы права владельца взял на себя член группы администраторов или Операторов восстановления (Restore Operators). Иными словами, статус владельца файла или папки особенно важен в контексте назначения разрешений.

По умолчанию владельцем файла или папки является создавший их пользователь. Есть также несколько способов передачи права владения. Текущий владелец файла или папки может передать права владения другому пользователю или группе. Член группы администраторов может сделать себя владельцем файла или папки, а также передать права владельца другому пользователю или группе — даже если набор разрешений блокирует администраторам доступ к ресурсу. Стать владельцем файла или папки может любой пользователь с разрешением Смена владельца (Take Ownership), а также член группы Операторы архива (Backup Operators) или любой другой пользователь, которому присвоено право Восстановление файлов и каталогов (Restore Files And Directories).

Принятие прав владельца файла или папки

Если вы являетесь администратором, авторизованным пользователем или оператором архива, то можете принять права владельца файла или папки, выполнив следующие действия:

1. В Проводнике Windows щелкните правой кнопкой мыши нужный файл или папку и выберите команду **Свойства (Properties)**.
2. На вкладке **Безопасность (Security)** щелкните кнопку **Дополнительно (Advanced)**, чтобы открыть диалоговое окно **Дополнительные параметры безопасности (Advanced Security Settings)**.
3. На вкладке **Владелец (Owner)** щелкните кнопку **Изменить (Edit)**. Откроется редактируемое диалоговое окно **Дополнительные параметры безопасности (Advanced Security Settings)**, показанное на рис. 13-5.
4. В списке **Изменить владельца на (Change Owner To)** выберите свою учетную запись. Чтобы стать владельцем не только папки, но и всех ее подпапок и файлов, установите флажок **Заменить владельца подконтейнеров и объектов (Replace Owner On Subcontainers And Objects)**.
5. Дважды щелкните **ОК**.

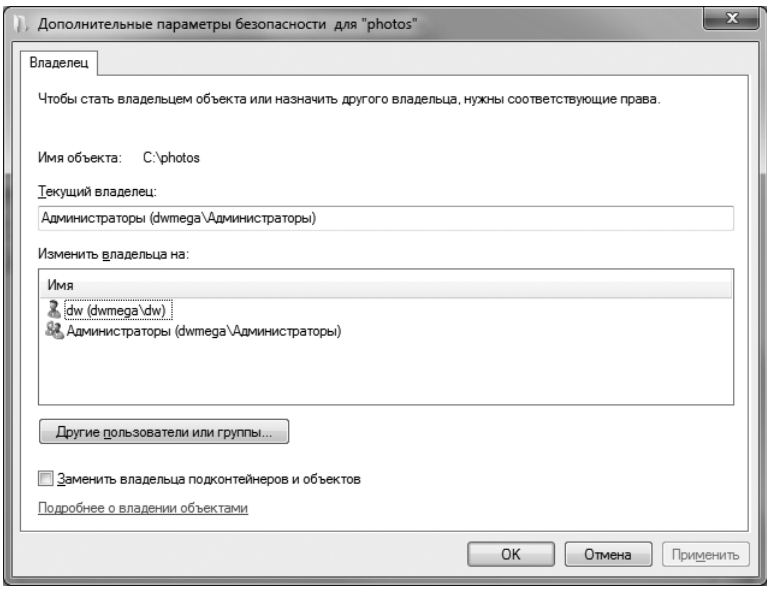

Рис. 13-5. Используйте вкладку Владелец (Owner), чтобы изменить владельца файла или папки

Присваивание прав владельца

Если вы являетесь администратором или текущим владельцем файла или папки, то можете сделать их владельцем другого пользователя или группу, выполнив следующие действия:

1. В Проводнике Windows щелкните правой кнопкой мыши нужный файл или папку и выберите команду **Свойства (Properties)**.
2. На вкладке **Безопасность (Security)** щелкните кнопку **Дополнительно (Advanced)**, чтобы открыть диалоговое окно **Дополнительные параметры безопасности (Advanced Security Settings)**.

3. На вкладке **Владелец (Owner)** щелкните кнопку **Изменить (Edit)**. Откроется редактируемое диалоговое окно **Дополнительные параметры безопасности (Advanced Security Settings)**.
4. Щелкните кнопку **Другие пользователи или группы (Other Users Or Groups)**, чтобы открыть диалоговое окно **Выбор: «Пользователь» или «Группа» (Select User Or Group)**.
5. Введите имя пользователя или группы и щелкните кнопку **Проверить имена (Check Names)**. Если введенному значению соответствует несколько имен, вы увидите их список и сможете выбрать то, которое хотите использовать. В противном случае имя будет введено автоматически и вам нужно будет щелкнуть **OK**, чтобы закрыть диалоговое окно **Выбор: «Пользователь» или «Группа» (Select User Or Group)**.
6. В списке **Изменить владельца на (Change Owner To)** выберите нового владельца. Чтобы распространить права владельца на все подпапки и файлы, установите флажок **Заменить владельца подконтейнеров и объектов (Replace Owner On Subcontainers And Objects)**.
7. Дважды щелкните **OK**.

Наследование разрешений

В иерархии файлов и папок Windows 7 корневая папка локального диска и папка %UserProfile% по умолчанию являются родительскими для всех файлов и папок, которые они содержат. Добавляемый в них ресурс наследует разрешения корневой папки локального диска или папки профиля пользователя. Если это вас не устраивает, отредактируйте настройки наследования, чтобы папка более не наследовала разрешения от родительской папки.

Основы наследования

Наследование происходит автоматически, и наследуемые разрешения присваиваются в момент создания файла или папки. Если вы не хотите, чтобы файл или папка наследовали разрешения родительской папки, у вас есть несколько способов действия:

- Прекратить наследование разрешений родительской папки, а затем скопировать или удалить существующие разрешения согласно своим потребностям.
- Сохранив наследование, отредактировать разрешения родительской папки.
- Попробуйте перекрыть наследуемое разрешение, выбрав противоположное разрешение. В большинстве случаев, разрешение Запретить (Deny) имеет более высокий приоритет, чем разрешение Разрешить (Allow).

На вкладке **Безопасность (Security)** диалогового окна свойств файла или папки наследуемые разрешения затенены (недоступны). Когда вы назначаете родительской папке новые разрешения, они распространяются на содержащиеся в ней подпапки и файлы, дополняя или заменяя существующие разрешения.

Чтобы полнее разобраться в наследовании, рассмотрим следующие примеры:

- На диске C: вы создаете папку Data, а в ней — подпапку CurrentProjects. По умолчанию папка Data наследует разрешения папки C:\, а эти разрешения в свою очередь будут унаследованы папкой CurrentProjects. Любые файлы, которые вы добавите в папки C:\, C:\Data и C:\Data\CurrentProjects, будут иметь одни и те же разрешения — унаследованные от папки C:\.
- На диске C: вы создаете папку Docs, а в ней — подпапку Working. Затем вы прекращаете наследование для папки Working и удаляете разрешения, унаследованные от родительской папки C:\. Теперь любые файлы, добавляемые в папку C:\Docs\Working, будут наследовать исключительно разрешения папки C:\Docs.
- На диске C: вы создаете папку Backup, а в ней — подпапку Sales. Затем вы назначаете подпапке Sales разрешения, которые дают доступ к ней членам группы Sales. Любые файлы, добавляемые в папку C:\Backup\Sales, будут наследовать разрешения папки C:\, а также иметь дополнительные разрешения для членов группы Sales.

Ближе к реальности Администраторы-новички часто интересуются, в чем именно состоят преимущества наследования и почему оно используется. Действительно, иногда кажется, что наследование скорее усложняет жизнь, чем упрощает ее, однако оно позволяет очень эффективно управлять разрешениями. Без наследования вам пришлось бы индивидуально настраивать разрешения для каждого создаваемого файла или папки. Если бы в дальнейшем вы захотели изменить разрешения, вам пришлось бы снова работать со всеми файлами и папками. Благодаря наследованию файлы и папки получают набор разрешений автоматически. Если вам необходимо изменить разрешения, вы можете редактировать их в папке более высокого уровня или в родительской папке, и эти изменения будут автоматически применены ко всем вложенным подпапкам и файлам. Иными словами, вы вольны применить единое разрешение ко множеству файлов и папок без необходимости настраивать безопасность отдельных файлов и папок.

Просмотр унаследованных разрешений

Чтобы просмотреть унаследованные разрешения к файлу или папке, правой кнопкой щелкните файл или папку в Проводнике Windows и выберите команду **Свойства (Properties)**. На вкладке **Безопасность (Security)** щелкните кнопку **Дополнительно (Advanced)**, чтобы открыть диалоговое окно **Дополнительные параметры безопасности (Advanced Security Settings)**, показанное выше на рис. 13-3. В столбце **Разрешение (Permission)** перечислены текущие разрешения, присвоенные ресурсу. Если разрешение унаследовано, в столбце **Унаследовано от (Inherited From)** будет указана родительская папка. Если разрешение наследуется другими ресурсами, в столбце **Применять к (Apply To)** будут показаны ресурсы, наследующие это разрешение.

Прекращение наследования

Чтобы прекратить наследование разрешений от родительской папки для файла или папки, выполните следующие действия:

1. В Проводнике Windows правой кнопкой щелкните нужный файл или папку и выберите команду **Свойства (Properties)**. На вкладке **Безопасность (Security)** щелкните кнопку **Дополнительно (Advanced)**.
2. На вкладке **Разрешения (Permissions)** щелкните кнопку **Изменить разрешения (Change Permissions)**. Откроется редактируемое диалоговое окно **Дополнительные параметры безопасности (Advanced Security Settings)**.
3. Сбросьте флажок **Добавить разрешения, наследуемые от родительских объектов (Include Inheritable Permissions From This Object's Parent)**.
4. В окне, показанном на рис. 13-6, щелкните кнопку **Добавить (Add)**, чтобы добавить унаследованные разрешения в качестве явных разрешений, или кнопку **Удалить (Remove)**, чтобы удалить унаследованные разрешения.

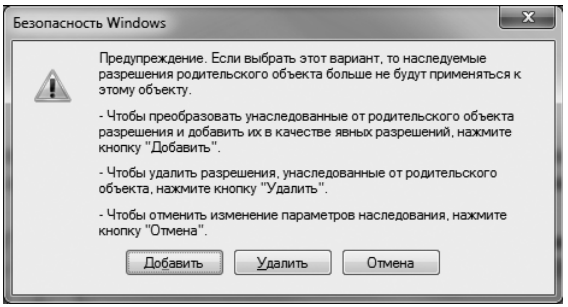

Рис. 13-6. Копирование или удаление унаследованных разрешений

Совет Если вы удаляете наследуемые разрешения и не присваиваете никаких других разрешений, в доступе к ресурсу будет отказано всем, кроме его владельца. Доступ не сможет получить даже администратор, однако за ним сохраняется право сделать себя владельцем ресурса независимо от назначенных ресурсу разрешений. Таким образом, если для администратора файл или папка заблокированы, а ему необходимо работать с ними, он может стать владельцем файла или папки и получить неограниченный доступ к ним.

Восстановление наследуемых разрешений

Со временем разрешения файлов и подпапок могут настолько далеко уйти от разрешений родительской папки, что эффективно управлять доступом станет практически невозможно. Чтобы облегчить управление, вам, возможно, придется решиться на восстановление наследуемых разрешений ресурсов родительской папки. При этом подпапки и файлы унаследуют все разрешения от родительской папки, а все разрешения, определенные явным образом для отдельных подпапок и файлов, будут удалены.

Чтобы восстановить наследование разрешений, выполните следующие действия:

1. В Проводнике Windows правой кнопкой щелкните папку и выберите команду **Свойства (Properties)**. На вкладке **Безопасность (Security)** щелкните кнопку **Дополнительно (Advanced)**.
2. На вкладке **Разрешения (Permissions)** щелкните кнопку **Изменить разрешения (Change Permissions)**. Откроется редактируемое диалоговое окно **Дополнительные параметры безопасности (Advanced Security Settings)**.
3. Установите флажок **Заменить все разрешения дочернего объекта на разрешения, наследуемые от этого объекта (Replace All Child Object Permissions With Inheritable Permissions From This Object)**. Затем щелкните **OK**.
4. На экране появится предупреждение, показанное на рис. 13-7. Щелкните **Да (Yes)**.

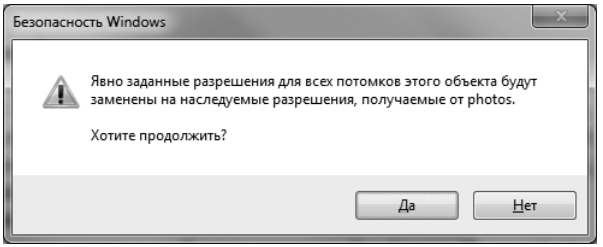

Рис. 13-7. Подтвердите замену существующих разрешений

Чтобы файл или папка включали в себя наследуемые разрешения родительской папки, выполните следующие действия:

1. В Проводнике Windows правой кнопкой щелкните папку или файл, которые должны включать в себя наследуемые разрешения, а затем выберите **Свойства (Properties)**. На вкладке **Безопасность (Security)** щелкните кнопку **Дополнительно (Advanced)**.
2. На вкладке **Разрешения (Permissions)** щелкните кнопку **Изменить разрешения (Change Permissions)**. Откроется редактируемое диалоговое окно **Дополнительные параметры безопасности (Advanced Security Settings)**.
3. Установите флажок **Добавить разрешения, наследуемые от родительских объектов (Include Inheritable Permissions From This Object's Parent)** и щелкните **OK**.

Определение действующих разрешений и поиск неисправностей

Разрешения файловой системы NTFS довольно сложны, и ими бывает трудно управлять. Иногда даже очень незначительное изменение приводит к непредсказуемым последствиям. Пользователь может неожиданно потерять доступ к файлам, с которым он раньше без проблем работал, или, напротив, получить доступ к файлам, которые раньше были для него закрыта. Любая

подобная ситуация означает, что существует какая-то проблема с разрешениями и что ее необходимо устранить.

Процесс диагностики проблем с разрешениями следует начинать с определения действующих разрешений для файлов и папок, права доступа к которым оказались не такими, как ожидалось. Как следует из названия, действующие разрешения указывают, какие именно разрешения действуют для конкретного пользователя или группы.

Набор действующих разрешений пользователя сочетает все разрешения, которые были ему даны или в которых ему было отказано как явным образом, так и в составе разрешений групп, членом которых является пользователь. Например, если JimB является членом групп Пользователи (Users), Sales, Marketing, SpecTeam и Managers, то действующим набором разрешений для файла или папки будет совокупный набор разрешений, которые были присвоены JimB явным образом, и разрешений, которые были присвоены группам Пользователи (Users), Sales, Marketing, SpecTeam и Managers. Если JimB является членом группы, которой явным образом было отказано в разрешении, то ему также будет отказано в разрешении, даже если другой его группе это разрешение предоставлено. Это происходит потому, что запрет имеет приоритет перед разрешением.

Чтобы определить действующие разрешения пользователя или группы в отношении того или иного файла или папки, выполните следующие действия:

1. В Проводнике Windows правой кнопкой щелкните файл или папку, с которой хотите работать, и выберите команду **Свойства (Properties)**. В диалоговом окне **Свойства (Properties)** перейдите на вкладку **Безопасность (Security)** и щелкните кнопку **Дополнительно (Advanced)**, чтобы открыть диалоговое окно **Дополнительные параметры безопасности (Advanced Security Settings)**.
2. Перейдите на вкладку **Действующие разрешения (Effective Permissions)**, щелкните кнопку **Выбрать (Select)**, введите имя пользователя или группы и щелкните **OK**.
3. Действующие разрешения для пользователя или группы отображаются в виде специальных разрешений. Если у пользователя есть полный доступ к ресурсу, ему будут предоставлены все разрешения, как показано на рис. 13-8. В противном случае назначено лишь некоторое подмножество разрешений. Используйте табл. 13-3, чтобы определить совокупность прав пользователя.

Примечание Для просмотра действующих разрешений пользователя или группы вам необходимы соответствующие разрешения. Также помните, что нельзя просматривать действующие разрешения для неявных групп или специальных идентификаторов, например групп Прошедшие проверку (Authenticated Users) или Все (Everyone). В действующих разрешениях не учитываются разрешения, предоставленные пользователю как владельцу ресурса.

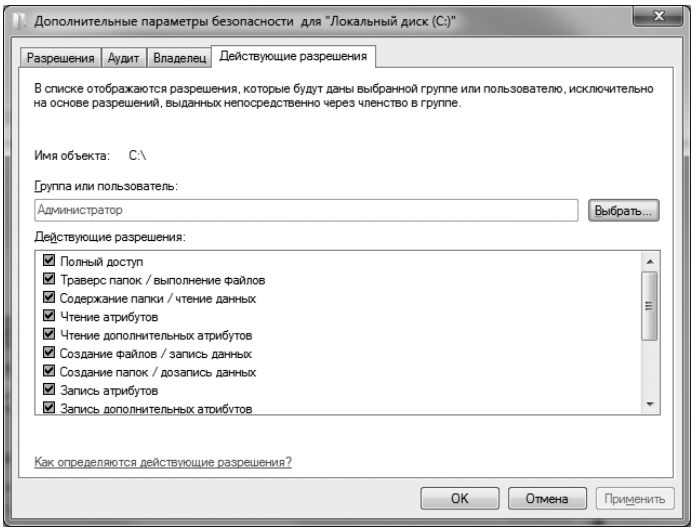

Рис. 13-8. Пользователю с полным доступом предоставлены все разрешения

Общий доступ к файлам и папкам в сети

В Windows 7 поддерживается два способа общего доступа к файлам: использование папки Общие (Public) и общий доступ к обычным папкам. В рабочих группах и доменах может использоваться как один из этих способов, так и оба одновременно. При этом общий доступ к обычным папкам предпочтительнее, поскольку он более безопасен, чем использование папки Общие (Public). В первом случае к вашим услугам весь стандартный набор разрешений, открывающий или закрывающий доступ к файлам и папкам через сеть на базовом уровне. Настройки общего доступа к папкам включаются или выключаются индивидуально для каждого компьютера. Чтобы включить или отключить общий доступ, выполните следующие действия:

1. Щелкните кнопку **Пуск (Start)** и выберите команду **Панель управления (Control Panel)**. В панели управления щелкните ссылку **Выбор параметров домашней группы и общего доступа к данным (Choose Homegroup And Sharing Options)** в категории **Сеть и Интернет (Network And Internet)**. Затем щелкните ссылку **Изменение дополнительных параметров общего доступа (Change Advanced Sharing Settings)**.
2. Каждому сетевому профилю соответствует отдельная панель управления с параметрами настройки. Используйте кнопки со стрелками, чтобы открыть нужный профиль.
3. Чтобы включить общий доступ к файлам и принтерам, установите переключатель **Включить общий доступ к файлам и принтерам (Turn On File And Printer Sharing)**. Чтобы отключить общий доступ к файлам и принтерам, установите переключатель **Отключить общий доступ к файлам и**

принтерам (Turn Off File And Printer Sharing). Щелкните кнопку **Сохранить изменения (Save Changes)**.

Управление доступом к общим сетевым ресурсам

Уровень сетевого доступа пользователя к файлу или папке определяется двумя наборами разрешений, которые в совокупности определяют действия, которые пользователь может производить с конкретными общими файлами или папками. Первый уровень — это разрешения, назначенные самому общему ресурсу. Они определяют наивысший достижимый уровень доступа. Пользователь или группа не могут иметь больше разрешений, чем предоставлено общим ресурсом. Второй уровень — это разрешения файлов или папок. Они служат для дальнейшего ограничения разрешенных действий.

Имеется три вида разрешений общего доступа:

- **Владелец (Owner)** Пользователю с полным доступом назначены разрешения Полный доступ (Full Control), Чтение (Read) и Изменение (Change), а также предоставлены возможности изменять разрешения файлов и папок и становиться их владельцем. Если вы владелец общего ресурса, у вас есть полный доступ к нему.
- **Чтение и запись (Read/Write)** У пользователя с этим разрешением есть разрешения Чтение (Read) и Изменение (Change), а также возможности создавать, изменять и удалять файлы и подпапки и изменять атрибуты файлов и подпапок. Становиться владельцем ресурса он не может.
- **Чтение (Read)** Пользователь с этим разрешением может просматривать имена файлов и подпапок, получать доступ к подпапкам общего ресурса, читать данные и атрибуты файлов и запускать программы.

Разрешения, назначаемые группам, работают следующим образом: если пользователь является членом одной группы, которой разрешен полный доступ к ресурсу, у пользователя также будет полный доступ к этому ресурсу. Если пользователь является членом нескольких групп, уровень доступа определяется совокупностью разрешений. Например, если у одной группы есть разрешение на чтение, а у другой — разрешение на чтение и запись, то у пользователя будет разрешение на чтение и запись. Если одна группа имеет разрешение на чтение, а другая названа владельцем ресурса, пользователь также будет считаться владельцем ресурса.

Чтобы перекрыть этот режим, отзовите конкретные разрешения. Отказ в разрешении имеет приоритет и отменяет назначенные разрешения. Например, если пользователь входит в группу, которая является владельцем общего ресурса, а вы хотите ограничить его возможности чтением и записью, укажите в настройках общего ресурса, чтобы пользователю отказано в разрешении Владелец (Owner).

Создание общего ресурса

Папки могут использоваться совместно как в рабочих группах, так и в доменах. Чтобы открыть общий доступ к первому ресурсу на компьютере, вы должны быть локальным администратором. Открыв общий доступ к первому ресурсу, вы тем самым разрешаете предоставление общего доступа к другим ресурсам. Причем делать это могут уже любые пользователи, являющиеся владельцами и (или) наделенные соответствующими разрешениями.

Общие ресурсы создаются несколькими инструментами, в том числе:

- **Проводник Windows (Windows Explorer)** Используйте Проводник Windows, чтобы открыть общий доступ к папке на компьютере, на который вы входите под своим именем.
- **Управление компьютером (Computer Management)** Используйте консоль Управление компьютером (Computer Management), чтобы открыть общий доступ к папке на любом компьютере, к которому вы можете подключиться.
- **Net Share** Используйте команду Net Share, чтобы предоставлять общий доступ к папкам в составе сценария. Введите **net share /?**, чтобы получить справку о синтаксисе команды.

Создание общего ресурса — многоэтапный процесс. Сначала вы открываете общий доступ к папке, затем задаете разрешения общего доступа. После этого вы должны проверить и необходимым образом изменить разрешения файловой системы. В этом разделе обсуждается общий доступ к ресурсу и назначение ему разрешений при помощи Проводника Windows и консоли Управление компьютером (Computer Management). Работа с разрешениями файловой системы подробно обсуждалась в начале этой главы.

Настройка общего доступа к ресурсу в Проводнике Windows

В Проводнике Windows поддерживается базовый общий доступ и расширенный общий доступ. В первом случае вы можете предоставить в совместное пользование любую папку за исключением корневой папки диска. Расширенный общий доступ подразумевает совместное использование и корневой папки диска, и любой другой папки. Корневые папки дисков автоматически становятся административными общими ресурсами.

Чтобы открыть обычный общий доступ к папке, выполните следующие действия:

1. В Проводнике Windows правой кнопкой щелкните папку, к которой хотите открыть общий доступ, разверните подменю **Общий доступ (Share With)** и выберите команду **Конкретные пользователи (Specific People)**. Откроется мастер Общий доступ к файлам (File Sharing), показанный на рис. 13-9.

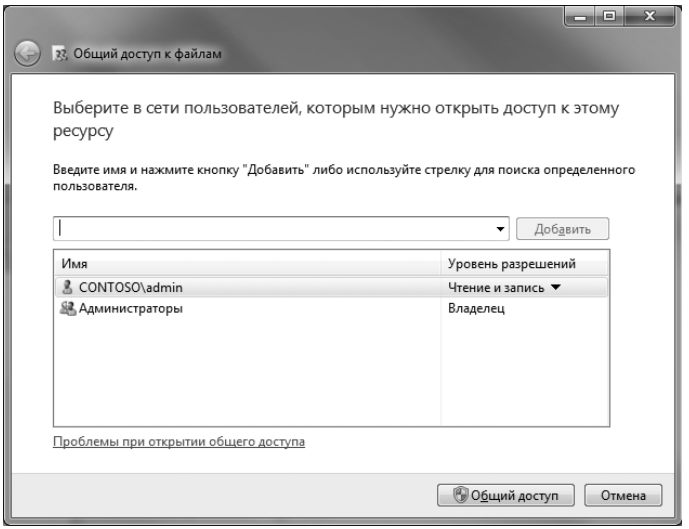

Рис. 13-9. Мастер Общий доступ к файлам (File Sharing) для настройки общего доступа

2. Введите имя пользователя и щелкните кнопку **Добавить (Add)** или найдите нужного пользователя в списке. В рабочей группе отображаются только локальные учетные записи и группы. В доменах вы увидите локальных пользователей и группы, а также сможете найти пользователей домена.
3. Когда вы щелкнете кнопку **Добавить (Add)**, выбранные пользователи и группы будут добавлены в список **Имя (Name)**. Настройте разрешения для каждого пользователя и группы, щелкнув имя учетной записи и выбрав нужный вариант в списке **Уровень разрешений (Permission Level)**. Вы можете разрешить только чтение или чтение и запись.
4. Щелкните кнопку **Общий доступ (Share)**, чтобы создать общий ресурс. Когда Windows 7 создаст общий ресурс и откроет доступ к нему, обратите внимание на имя ресурса. По этому имени пользователи сети будут получать доступ к ресурсу. Чтобы отправить адрес общего ресурса по электронной почте, щелкните ссылку **Отправить по электронной почте (E-mail)**. Чтобы скопировать адрес в буфер обмена, щелкните ссылку **Скопировать ссылки (Copy)**. Закончив работу, щелкните **Готово (Done)**.

Примечание Как правило, пользователи получают доступ к общему ресурсу, используя сокращенный UNC-путь. Например, если вы открыли общий доступ к папке C:\Data\Reports\Current как к ресурсу Reports на компьютере CorPC85, пользователи получат доступ к ней, используя UNC–путь \\CorPC85\Reports. Если же вы открыли общий доступ к папке внутри профиля пользователя, пользователи получают доступ к ней, указывая путь относительно папки Пользователи (Users). Например, если пользователь MollyH открыла общий доступ к папке Документы (Documents) из своего профиля на компьютере CustPC27, UNC-путь к общему ресурсу выглядит как \\CustPC27\Users\MollyH\Documents.

Чтобы открыть расширенный общий доступ к папке, выполните следующие действия:

1. В Проводнике Windows правой кнопкой щелкните нужную папку и выберите команду **Свойства (Properties)**. Откроется диалоговое окно свойств папки.
2. На вкладке **Доступ (Sharing)** щелкните кнопку **Расширенная настройка (Advanced Sharing)**. В диалоговом окне **Расширенная настройка общего доступа (Advanced Sharing)** установите флажок **Открыть общий доступ к этой папке (Share This Folder)**.
3. Имя общего ресурса Windows задает автоматически. Примите имя общего ресурса по умолчанию или введите другое имя.
4. Щелкните кнопку **Разрешения (Permissions)**. Используйте диалоговое окно **Разрешения для (Permissions For)**, чтобы настроить разрешения к общему ресурсу. Щелкните **OK**.
5. Щелкните кнопку **Кэширование (Caching)**. В диалоговом окне **Настройка автономного режима (Offline Settings)** задайте, могут ли данные быть помещены в кеш для использования в автономном режиме, и если да, то каким образом. Щелкните **OK**.
6. Щелкните **OK** и **Закрыть (Close)**.

Изменение или прекращение общего доступа

Если вы правой кнопкой щелкнете общую папку, развернете подменю **Общий доступ (Share With)** и выберете команду **Никому из пользователей (Nobody)**, общий доступ к папке прекратится, и все его настройки будут удалены. Чтобы изменить разрешения общего доступа, щелкните правой кнопкой общую папку, раскройте подменю **Общий доступ (Share With)** и выберите команду **Конкретные пользователи (Specific People)**. Далее вы сможете предоставить доступ новым пользователям и группам, как было описано выше. Чтобы остановить доступ для пользователя или группы, выделите соответствующее имя в списке **Имя (Name)** и выберите вариант **Удалить (Remove)**. Закончив внесение изменений, щелкните кнопку **Общий доступ (Share)**, чтобы сохранить измененные параметры общего доступа, а затем щелкните **Готово (Done)**.

При использовании расширенного общего доступа щелкните папку правой кнопкой мыши и выберите команду **Свойства (Properties)**. На вкладке **Доступ (Sharing)** щелкните кнопку **Расширенная настройка (Advanced Sharing)**. После этого вы сможете подключать и отключать альтернативные общие ресурсы и уточнять допустимые параметры соединений, а также конфигурировать разрешения и использование кеша.

Настройка общего доступа в консоли Управление компьютером (Computer Management)

Консоль Управление компьютером (Computer Management) позволяет предоставлять общий доступ к папкам любого компьютера, к которому у вас

есть доступ в качестве администратора. Подключаясь к компьютеру удаленно, вы обычно экономите время, поскольку можете настроить несколько систем, не покидая рабочего места, вместо того чтобы бегать по зданию. Чтобы открыть общий доступ к папке при помощи консоли Управление компьютером (Computer Management), выполните следующие действия:

1. Щелкните кнопку **Пуск (Start)**, правой кнопкой щелкните команду **Компьютер (Computer)** и выберите команду **Управление (Manage)**. По умолчанию консоль Управление компьютером (Computer Management) подключится к локальному компьютеру, а корневой узел дерева консоли будет назван **Управление компьютером (локальным) (Computer Management (Local))**.

Совет Чтобы открыть общий доступ к папке на локальном компьютере при помощи Мастера создания общих ресурсов (Create A Shared Folder Wizard), запустите мастер напрямую и пропустите шаги 1–4. Для запуска мастера введите **shrpubw** в командной строке с повышенными полномочиями и щелкните **Далее (Next)**.

2. Правой кнопкой щелкните **Управление компьютером (Computer Management)** в дереве консоли и выберите команду **Подключиться к другому компьютеру (Connect To Another Computer)**. В диалоговом окне **Выбор компьютера (Select Computer)** по умолчанию установлен переключатель **Другим компьютером (Another Computer)**. Введите полное имя домена компьютера, с которым хотите работать, например, **engpc08.microsoft.com**. Если вы не знаете имени компьютера, и у вас включено сетевое обнаружение, щелкните кнопку **Обзор (Browse)**, чтобы найти компьютер.
3. Разверните узел **Служебные программы\Общие папки (System Tools\Shared Folders)** и выделите элемент **Общие ресурсы (Shares)**, чтобы отобразить общие папки системы, на которой вы работаете, как показано на рис. 13-10.

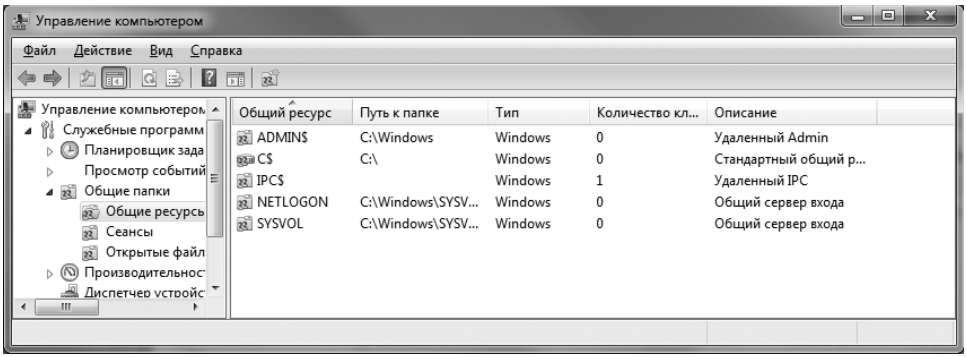

Рис. 13-10. Общие папки компьютера перечислены в узле Общие ресурсы (Shares)

4. Чтобы запустить Мастер создания общих ресурсов (Create A Shared Folder Wizard), правой кнопкой щелкните узел **Общие ресурсы (Shares)**

и выберите команду **Новый общий ресурс (New Share)**. Щелкните **Далее (Next)**, чтобы открыть страницу **Путь к папке (Folder Path)**.

5. В поле **Путь к папке (Folder Path)** введите полный путь к папке, которую хотите сделать общей, например **C:\Data**. Если вы не знаете полный путь, щелкните кнопку **Обзор (Browse)**, а затем используйте диалоговое окно **Обзор папок (Browse For Folder)**, чтобы найти папку. Диалоговое окно **Обзор папок (Browse For Folder)** также позволяет создать новую папку, к которой вы затем предоставите общий доступ. Щелкните **Далее (Next)**, чтобы открыть страницу **Имя, описание и параметры (Name, Description, And Settings)**.
6. В поле **Общий ресурс (Share Name)** введите имя общего ресурса. Имена общих ресурсов должны быть уникальными в пределах системы, могут быть до 80 символов в длину и содержать пробелы. Если вы хотите обеспечить поддержку доступа для Windows 98, Windows Me или Windows NT, ограничьте имя общего ресурса 12 символами.
7. Введите описание общего ресурса в поле **Описание (Share Description)**.

Совет По умолчанию для использования в автономном режиме доступны только файлы и программы, явно указанные пользователями. Щелкните кнопку **Изменить (Change)**, чтобы модифицировать настройки автономных файлов. Чтобы сделать доступными для автономного использования все файлы и программы, установите переключатель **Вне сети автоматически доступны все открывавшиеся пользователем файлы и программы (All Files And Programs That Users Open From The Shared Folder Are Automatically Available Offline)**. Чтобы сделать все файлы или программы недоступными для использования в автономном режиме, установите переключатель **Файлы и программы в этой общей папке недоступны вне сети (No Files Or Programs From The Shared Folder Are Available Offline)**. Затем щелкните **OK**.

8. Щелкните **Далее (Next)**, чтобы открыть страницу **Разрешения для общей папки (Shared Folder Permissions)**. Здесь доступны следующие варианты:
   - **У всех пользователей доступ только для чтения (All Users Have Read-Only Access)** Этот вариант выбран по умолчанию. Он предоставляет пользователям право просматривать файлы и читать данные, но не дает создавать, модифицировать или удалять файлы и папки.
   - **Администраторы имеют полный доступ, остальные — доступ только для чтения (Administrators Have Full Access; Other Users Have Read-Only Access)** Этот вариант дает полный доступ к общим ресурсам только администраторам; другие пользователи получают доступ только для чтения. Администраторы могут создавать, модифицировать и удалять файлы и папки. В файловой системе NTFS этот параметр также дает администраторам право изменять разрешения и становиться владельцем файлов и папок. Другие пользователи могут просматривать файлы и читать данные, но не могут создавать, модифицировать или удалять файлы и папки.

- **Администраторы имеют полный доступ, остальные не имеют доступа (Administrators Have Full Access; Other Users Have No Access)** Дает полный доступ к общему ресурсу только администраторам.
- **Настройка разрешений доступа (Customize Permissions)** Позволяет настраивать доступ для конкретных пользователей и групп. Как правило, это самый оптимальный способ. Установите переключатель **Настройка разрешений доступа (Customize Permissions)** и щелкните кнопку **Другой (Custom)**. Затем настройте нужные разрешения для общего ресурса.

9. Щелкните **Далее (Next)** и **Готово (Finish)**, чтобы сделать папку общей. Еще раз щелкните **Готово (Finish)**, чтобы выйти из мастера.

Если в дальнейшем вы решите прекратить общий доступ к папке, это также можно сделать в консоли Управление компьютером (Computer Management). Правой кнопкой щелкните общую папку и выберите команду **Прекратить общий доступ (Stop Sharing)**. Подтвердите действие, щелкнув **Да (Yes)**.

Создание общих папок и управление ими в групповой политике

Открывать общий доступ к папкам можно и при помощи предпочтений групповой политики. Я рекомендую использовать этот подход только в случае, когда для совместного пользования предоставляются данные со строго определенного набора компьютеров.

Чтобы создать элемент предпочтения для создания, обновления, замены или удаления общих папок, выполните следующие действия:

1. Откройте объект GPO для редактирования в редакторе управления групповой политикой. Разверните узел **Конфигурация компьютера\Настройка\Конфигурация Windows (Computer Configuration\Preferences\Windows Settings)**, а затем выделите узел **Сетевые общие ресурсы (Network Shares)**.
2. Правой кнопкой щелкните узел **Сетевые общие ресурсы (Network Shares)**, раскройте подменю **Создать (New)** и выберите команду **Сетевой ресурс (Network Share)**. Откроется диалоговое окно **Новые свойства общего сетевого ресурса (New Network Share Properties)**.
3. В диалоговом окне **Новые свойства общего сетевого ресурса (New Network Share Properties)** выберите в списке **Действие (Action)** вариант **Создать (Create)**, **Обновить (Update)**, **Заменить (Replace)** или **Удалить (Delete)**.
4. Введите имя общего ресурса в поле **Имя ресурса (Share Name)**. Имена общих ресурсов должны быть уникальны для каждой системы. Они могут быть до 80 символов в длину и содержать пробелы.
5. В поле **Путь к папке (Folder Path)** введите полный путь к папке, которую хотите сделать общей, например **C:\Data**. Если вы не знаете полный путь, щелкните кнопку с многоточием справа от поля и найдите папку в диалоговом окне **Обзор папок (Browse For Folder)**.

Ближе к реальности Если вы хотите использовать в пути к папке переменную среды, установите курсор в поле **Путь к папке (Folder Path)** и нажмите клавишу F3, чтобы отобразить список системных переменных. Выберите переменную, которую хотите использовать, например LogOnUser. По умолчанию значение переменной разрешается в групповой политике, перед ее применением на компьютере пользователя. Чтобы разрешать переменную, то есть заменять значением, только на компьютере пользователя, сбросьте флажок **Сопоставить переменную (Resolve Variable)** и щелкните кнопку **Выбрать (Select)**. В строку будет вставлено имя переменной, а не ее значение.

В предпочтениях групповой политики легко различить переменные, разрешаемые в групповой политике, и переменные, разрешаемые на компьютере пользователя. Первые имеют синтаксис %*ИмяПеременной*%, например %ProgramFiles%, вторые — %<*ИмяПеременной*>%, например %<ProgramFiles>%.

6. В поле **Комментарий (Comment)** введите описание общего ресурса.
7. Вы можете обновлять или удалять все общие ресурсы определенного типа, а не каждый общий ресурс отдельно. Для этого выполните одно или несколько следующих действий:
   - **Обновление или удаление всех обычных общих ресурсов** Чтобы обновить или удалить общие ресурсы, которые не являются скрытыми, административными или специальными, установите флажок **Обновить все обычные общие ресурсы (Update All Regular Shares)** или **Удалить все обычные общие ресурсы (Delete All Regular Shares)**.
   - **Обновление или удаление всех скрытых неадминистративных ресурсов** Чтобы обновить или удалить все скрытые ресурсы, кроме административных и специальных (ресурсов с именем диска, ADMIN$, FAX$, IPC$, и Print$), установите флажок **Обновить все скрытые неадминистративные общие ресурсы (Update All Hidden Non-Administrative Shares)** или **Удалить все скрытые неадминистративные общие ресурсы (Delete All Hidden Non-Administrative Shares)**.
   - **Обновление или удаление всех административных общих ресурсов** Чтобы обновить или удалить все общие ресурсы с именем диска, установите флажок **Обновить все административные общие ресурсы букв дисков (Update All Administrative Drive-Letter Shares)** или **Удалить все административные общие ресурсы букв дисков (Delete All Administrative Drive-Letter Shares)**.

Примечание Чтобы обновить специальные общие ресурсы, например ADMIN$, FAX$, IPC$ и Print$, или другие системные общие ресурсы, например SYSVOL и NETLOGON, создайте элемент предпочтения для общего ресурса и введите в поле **Имя ресурса (Share Name)** имя специального общего ресурса.

8. Задайте количество пользователей, которые могут подключаться к общему ресурсу. Установите переключатель **Максимально допустимое (Maximum Allowed)**, чтобы допустить максимальное количество пользователей, разрешенное ОС. Установите переключатель **Не более (Allow This Number Of Users)**, чтобы точно указать предел.

9. Укажите, нужно ли использовать списки управления доступом, чтобы определить видимость папок в этом общем ресурсе. Установите переключатель **Включить (Enable)**, чтобы папки внутри общего ресурса могли видеть только пользователи с разрешением Чтение (Read). Установите переключатель **Отключить (Disable)**, чтобы папки внутри общего ресурса могли видеть все пользователи.
10. На вкладке **Общие параметры (Common)** задайте способ применения предпочтений. Поскольку речь идет о доступе к данным, применять настройку следует при каждом обновлении групповой политики. Поэтому не устанавливайте флажок **Применить один раз и не применять повторно (Apply Once And Do Not Reapply)**.
11. Щелкните **OK**. При следующем обновлении групповой политики элемент будет применен в составе объекта групповой политики, в котором вы его определили.

Использование общих ресурсов и доступ к ним

Пользователи обращаются к общей папке как к сетевому ресурсу или подключаются к ней при помощи назначения буквы диска. Подключив к ресурсу сетевой диск, пользователи получат доступ к нему как к локальному диску своего компьютера.

Чтобы подключить сетевой диск к общему файлу или папке, выполните следующие действия:

1. Щелкните кнопку **Пуск (Start)** и выберите команду **Компьютер (Computer)**. Щелкните кнопку **Подключить сетевой диск (Map Network Drive)** на панели инструментов. Откроется одноименное диалоговое окно, показанное на рис. 13-11.

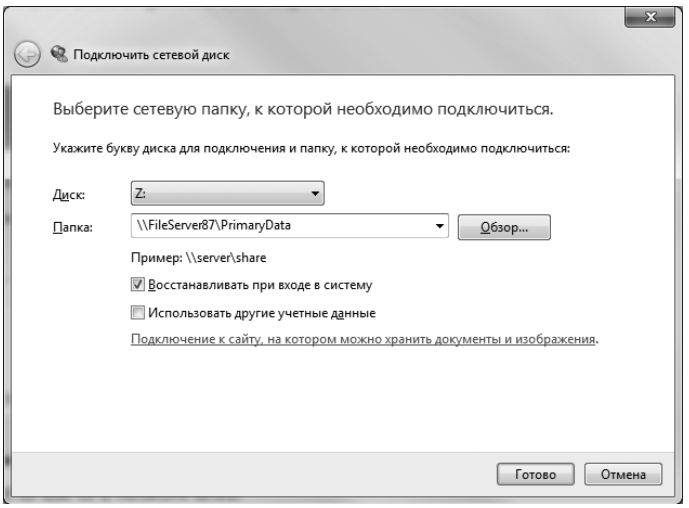

Рис. 13-11. Подключите нужный общий ресурс к сетевому диску

Совет Подключить или отключить сетевой диск можно в любом окне Проводника Windows при помощи команд меню **Сервис (Tools)**. Оно доступно при условии, что в Проводнике Windows отображаются классические меню. Если классические меню не показаны, нажмите клавишу F10 или щелкните кнопку **Упорядочить (Organize)**, раскройте подменю **Представление (Layout)** и выберите команду **Строка меню (Menu Bar)**.

2. Выберите в списке **Диск (Drive)** свободную букву и щелкните кнопку **Обзор (Browse)** справа от списка **Папка (Folder)**. В диалоговом окне **Обзор папок (Browse For Folder)** разверните сетевые папки, затем выберите имя рабочей группы или домена, с которым хотите работать.
3. Развернув имя компьютера в рабочей группе или домене, вы увидите список общих папок. Выберите нужную общую папку и щелкните **OK**.
4. Установите флажок **Восстанавливать при входе в систему (Reconnect At Logon)**, чтобы Windows 7 автоматически подключалась к общей папке в начале каждого сеанса.
5. Если у текущего пользователя нет разрешения на доступ к общему ресурсу, установите флажок **Использовать другие учетные данные (Connect Using Different Credentials)**. Затем щелкните **Готово (Finish)**. Введите имя пользователя и пароль учетной записи для подключения к общей папке. Имя пользователя вводите в формате *Домен\Имя пользователя*, например Cpandl\Williams.

Если впоследствии вы решите, что не хотите привязывать сетевой диск к папке, щелкните кнопку **Пуск (Start)** и выберите команду **Компьютер (Computer)**. В разделе **Сетевое размещение (Network Location)** щелкните правой кнопкой значок сетевого диска и выберите команду **Отключить (Disconnect)**.

Чтобы настроить сетевые диски на компьютерах по всему домену при помощи предпочтений групповой политики, выполните следующие действия:

1. Откройте объект GPO для редактирования в редакторе управления групповой политикой. Разверните узел **Конфигурация компьютера\Настройка\Конфигурация Windows (User Configuration\Preferences\Windows Settings)**. Выделите узел **Сопоставления дисков (Drive Maps)**.
2. Правой кнопкой щелкните узел **Сопоставления дисков (Drive Maps)**, разверните подменю **Создать (New)** и выберите команду **Сопоставленный диск (Mapped Drive)**. Откроется диалоговое окно **Новые свойства диска (New Drive Properties)**.
3. Выберите в списке **Действие (Action)** вариант **Создать (Create)**, **Обновить (Update)**, **Заменить (Replace)** или **Удалить (Delete)**.
4. В поле **Размещение (Location)** введите UNC-путь к сетевому общему ресурсу, например **CorpServer45\corpdatashare**, или щелкните кнопку с многоточием, чтобы найти расположение общего ресурса.
5. Установите флажок **Повторное подключение (Reconnect)**, чтобы Windows 7 автоматически подключалась к диску в начале каждого сеанса.

Ближе к реальности Если вы хотите использовать в пути к папке переменную среды, установите курсор в поле **Размещение (Location)** и нажмите клавишу F3, чтобы отобразить список системных переменных. Выберите переменную, которую хотите использовать, например LogOnUser. По умолчанию значение переменной разрешается в групповой политике, перед ее применением на компьютере пользователя. Чтобы разрешать переменную, то есть заменять значением, только на компьютере пользователя, сбросьте флажок **Сопоставить переменную (Resolve Variable)** и щелкните кнопку **Выбрать (Select)**. В строку будет вставлено имя переменной, а не ее значение.

В предпочтениях групповой политики легко различить переменные, разрешаемые в групповой политике, и переменные, разрешаемые на компьютере пользователя. Первые имеют синтаксис %*ИмяПеременной*%, например %ProgramFiles%, вторые — %<*ИмяПеременной*>%, например %<ProgramFiles>%.

6. Введите метку сетевого диска в поле **Подпись (Label As)**.
7. В разделе **Буква диска (Drive Letter)** уточните, каким образом должна присваиваться буква диска. Чтобы использовать первую доступную букву, начиная с заданной вами буквы, установите переключатель **Использовать первую доступную, начиная с (Use First Available, Starting At)** и введите первую допустимую букву. Чтобы всегда использовать конкретную букву, установите переключатель **Существующая (Use)**, а затем введите букву. Если вы точно не знаете, какие буквы свободны, используйте первый вариант.
8. При необходимости задайте учетные данные для подключения к общему ресурсу.
   - Если вы хотите подключать диск не от имени текущего пользователя, введите нужные учетные данные. Пароль шифруется и хранится в составе объекта групповой политики GPO на томе Sysvol контроллера домена.
   - Если вам нужно, чтобы пользователь вводил учетные данные при подключении, введите %<LogonUser>% в поле **Пользователь (User Name)** и оставьте незаполненными поля **Пароль (Password)** и **Подтверждение (Confirm Password)**.

Примечание Ввод учетных данных для подключения сетевого диска нежелателен с точки зрения безопасности и должен использоваться ограниченно. Если вы используете этот метод, обязательно периодически меняйте пароль учетной записи пользователя и обновляйте пароли в предпочтениях, которые используют эту учетную запись.

9. Можно задать дополнительные параметры сокрытия или показа одного диска или всех дисков. Задав отображение или сокрытие всех дисков, вы затрагиваете как сетевые, так и физические диски.
10. Используйте параметры вкладки **Общие параметры (Common)**, чтобы настроить применение предпочтений. Поскольку речь идет о безопасности, настройку следует применять при каждом обновлении групповой политики. Не устанавливайте флажок **Применить один раз и не применять повторно (Apply Once And Do Not Reapply)**.

11. Щелкните **OK**. Предпочтение будет применено при следующем обновлении объекта групповой политики, в котором оно определено.

Общие папки и администрирование

В Windows 7 некоторые специальные общие папки создаются автоматически и предназначены для использования администраторами или ОС. В конце имени большинства специальных общих папок имеется знак доллара ($), который скрывает эти общие папки от пользователей. Администратору иногда приходится создавать собственные скрытые общие папки или работать со стандартными специальными общими папками.

Создать скрытую общую папку довольно легко. Все что для этого нужно — добавить знак доллара ($) в конце имени общего ресурса. Например, если вы хотите сделать общей папку C:\Reports, но не хотите, чтобы она отображалась в обычном списке общих ресурсов, назовите ее Reports$, а не Reports. Но помните, что сокрытие папки не предотвращает доступ к ней. Доступ к общим папкам управляется посредством разрешений, независимо от того является общая папка видимой или скрытой.

Набор специальных общих папок зависит от конфигурации системы. Это означает, что на одних компьютерах может быть больше специальных общих папок, чем на других. Наиболее типичные специальные и административные общие папки перечислены в табл. 13-4.

Табл. 13-4. Специальные и административные общие ресурсы

Имя общего ресурса	Описание
C$, D$, E$, и другие общие ресурсы локальных дисков	Специальная общая папка для корневой папки локального диска или CD/DVD-диска. Эти общие ресурсы позволяют членам групп Администраторы (Administrators) и Операторы архива (Backup Operators) подключаться к корневой папке локального диска и выполнять административные задачи. Например, подключившись к ресурсу C$, вы получаете полный доступ к локальному диску C:\
ADMIN$	Административный общий ресурс для доступа к папке %SystemRoot%, в которой находятся файлы ОС. Предназначен для использования при удаленном администрировании, обеспечивая прямой доступ к файлам ОС
IPC$	Административный общий ресурс для поддержки именованных каналов (pipes). Поскольку именованные каналы могут перенаправляться по сети для подключения к локальным и удаленным системам, они также позволяют проводить удаленное администрирование
PRINT$	Поддерживает совместное использование принтера, предоставляя доступ к его драйверам. Когда вы открываете общий доступ к принтеру, система помещает в этот ресурс его драйверы, чтобы другие компьютеры могли при необходимости получить к ним доступ

Наиболее удобными инструментами для работы со специальными и другими скрытыми общими папками являются команда **Net Share** и консоль Управление компьютером (Computer Management). Чтобы просмотреть список всех общих папок на локальном компьютере, включая специальные административные общие папки, введите **net share** в командной строке. Чтобы отобразить список общих папок на другом компьютере сети, выполните следующие действия:

1. Щелкните кнопку **Пуск (Start)**, правой кнопкой щелкните команду **Компьютер (Computer)** и выберите команду **Управление (Manage)**, чтобы открыть консоль Управление компьютером (Computer Management). По умолчанию консоль подключается к локальному компьютеру, и корневой узел дерева консоли называется **Управление компьютером (локальным) (Computer Management (Local))**.
2. Правой кнопкой щелкните корневой узел консоли и выберите команду **Подключиться к другому компьютеру (Connect To Another Computer)**. В диалоговом окне **Выбор компьютера (Select Computer)** по умолчанию установлен переключатель **Другим компьютером (Another Computer)**. Введите имя хоста или полное имя компьютера, с которым хотите работать, например, **engpc08** или **engpc08.microsoft.com**. Если вы не знаете имя компьютера и обнаружение сети включено, щелкните кнопку **Обзор (Browse)**, чтобы найти компьютер, с которым хотите работать.
3. Разверните узлы **Служебные программы (System Tools)** и **Общие папки (Shared Folders)**, а затем выделите элемент **Общие ресурсы (Shares)**, чтобы отобразить список общих папок системы.

Иногда перед изменением параметров общих папок или файлов нужно убедиться, что к ним не подключены пользователи. Например, собираясь переместить файлы в новое расположение, сначала нужно проверить, что их никто не использует. Чтобы увидеть, кто работает с общими папками и их файлами, просмотрите сеансы пользователей и открытые файлы.

Каждый пользователь, подключаясь к общей папке, создает сеанс пользователя. Чтобы определить, кто из пользователей подключен в данный момент, выберите элемент **Сеансы (Sessions)** в узле **Общие папки (Shared Folders)** дерева консоли. Справа отобразится список текущих пользователей. Чтобы отключить пользователя и завершить его сеанс, правой кнопкой щелкните сеанс в правой панели, выберите команду **Закрыть сеанс (Close Session)** и щелкните **OK**, чтобы подтвердить действие. Чтобы отключить все сеансы, щелкните правой кнопкой элемент **Сеансы (Sessions)** в дереве консоли и выберите команду **Отключить все сеансы (Disconnect All Sessions)**. Щелкните **OK**, чтобы подтвердить действие.

Общий файл, к которому осуществляется доступ, считается открытым. Чтобы определить, какие файлы открыты, щелкните элемент **Открытые файлы (Open Files)** узла **Общие папки (Shared Folders)** в дереве консоли. Текущие открытые файлы перечислены в правой панели. Чтобы закрыть

открытый файл, правой кнопкой щелкните соответствующую запись, выберите команду **Закрыть открытый файл (Close Open File)** и щелкните **OK**, чтобы подтвердить действие. Чтобы закрыть все открытые файлы, щелкните правой кнопкой элемент **Открытые файлы (Open Files)** в дереве консоли и выберите команду **Отключить все открытые файлы (Disconnect All Open Files)**. Щелкните **OK**, чтобы подтвердить действие.

Диагностика неисправностей при общем доступе

Чтобы диагностировать и разрешить большинство проблем, связанных с общим доступом к файлам, выполните следующие действия:

- **Проверьте соединение с компьютером, на котором размещены общие ресурсы, и компьютером, с которого пользователь пытается получить к ним доступ** Оба компьютера должны быть подключены к сети. На обоих компьютерах должны быть правильно настроены параметры TCP/IP. В конфигурациях брандмауэров на обоих компьютерах должны быть разрешены входящие и исходящие соединения. На компьютере с общими ресурсами также должно быть настроено исключение Общий доступ к файлам и принтерам (File And Printer Sharing). Брандмауэр Windows поддерживает несколько активных профилей. Активный и применяемый профиль должны быть правильно настроены. Если вы используете брандмауэр другого поставщика, разрешите входящие соединения по UDP-портам 137 и 138, TCP-порту 139, и всех портах ICMPv4 и ICMPv6.
- **Проверьте учетные данные** Если оба компьютера являются членами домена, пользователь должен подключаться к общему ресурсу, используя доменные учетные данные. Если пользователь вошел в компьютер как локальный пользователь, а не пользователь домена, задайте для него подключение к общему ресурсу с другими учетными данными и введите в качестве этих данных учетные данные записи пользователя в соответствующем домене.
- **Проверьте настройки общего доступа в Центре управления сетями и общим доступом (Network And Sharing Center)** Чтобы пользователи могли получить доступ к файлам на компьютере Windows 7 через сеть, на нем необходимо включить Общий доступ к файлам и принтерам (File And Printer Sharing) для активного сетевого профиля. Убедитесь также, что не включена политика **Запретить пользователям в их профиле предоставлять общий доступ к файлам (Prevent Users From Sharing Files Within Their Profiles)**. Компьютер может подключаться к нескольким сетям одновременно. Убедитесь, что для каждой активной сети общий доступ правильно настроен в Центре управления сетями и общим доступом (Network And Sharing Center).
- **Проверьте тип активной сети** В Центре управления сетями и общим доступом (Network And Sharing Center) на обоих компьютерах должен быть установлен соответствующий тип сети. Если сеть настроена как Об-

щественная (Public), многие настройки общего доступа заблокированы и ограничены.

- **Проверьте разрешения общего доступа, разрешения файловой системы NTFS и атрибуты доступа к файлам** Убедитесь, что для пользователя правильно настроены разрешения общего доступа и разрешения файловой системы NTFS. Проверьте, что файл, к которому не удается получить доступ, не сделан доступным только для чтения, скрытым или системным.

Проводя более тщательную диагностику, взгляните на конфигурацию DNS обоих компьютеров, а также на их членство в доменах. В идеале оба компьютера должны находиться в одной сети или в сетях, соединенных при помощи быстрых Ethernet-соединений, а также быть членами одного домена или находиться в доверенных доменах.

Для предоставления общего доступа к файлам необходима служба Сервер (Server). Убедитесь, что она включена и правильно настроена. Как правило, для службы Сервер (Server) задается автоматический запуск от имени учетной записи Локальная система (LocalSystem). Служба Сервер (Server) зависит от доступного драйвера Server SMB. Эту зависимость вы можете проверить на вкладке **Зависимости (Dependencies)** в диалоговом окне свойств службы.

В групповой политике компьютера, файлы которого предоставляются в общий доступ, пользователю должно быть предоставлено право **Доступ к компьютеру из сети (Access This Computer From The Network)**. Оно задается в узле **Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя (Windows Settings\Security Settings\Local Policies\User Rights Assignment)** узла **Конфигурация компьютера (Computer Configuration)**. По умолчанию это право имеют все авторизованные пользователи.

Папка Общие (Public) и настройка доступа к ней

Папка Общие (Public) и ее подпапки обеспечивают локальным и сетевым пользователям возможность совместного использования данных из единого расположения, позволяя быстро настроить общие ресурсы и рассортировать общие файлы по типам. В этом разделе рассматривается использование папки Общие (Public) и способы ее настройки.

Общие ресурсы в папке Общие (Public)

Чтобы сделать файл или папку общими, вы можете скопировать или переместить их в папку %SystemDrive%\Users\Public. У папки Общие (Public) есть несколько подпапок, которые позволяют организовать общие файлы:

- **Общий рабочий стол (Public Desktop)** Используется для совместного использования элементов рабочего стола.
- **Общие документы (Public Documents), Общая музыка (Public Music), Общие изображения (Public Pictures), Общедоступные ТВ-записи**

(Public Recorded TV), Общие видео (Public Videos) Используется для совместного использования документов и медиафайлов.

- **Общие загруженные файлы (Public Downloads)** Используется для совместного использования загруженных материалов.

Любое содержимое, помещенное в эти подпапки, доступно всем пользователям, которые входят в компьютер локально, а также всем пользователям сети, если к папке Общие (Public) предоставлен сетевой доступ.

По умолчанию получить доступ к общим папкам может любой человек, имеющий на компьютере учетную запись пользователя и пароль. Когда вы копируете или перемещаете файлы в общую папку, их разрешения изменяются и становятся такими же, как разрешения общей папки. Кроме того, добавляются некоторые дополнительные разрешения.

Разрешения по умолчанию папки Общие (Public) позволяют пользователям локального компьютера читать, записывать, изменять и удалять любые файлы в ней. В папках Общая музыка (Public Music), Общие изображения (Public Pictures) и Общие видео (Public Videos) пользователи компьютера наделены разрешениями Чтение и выполнение (Read & Execute) и Чтение (Read).

Конфигурация по умолчанию для общей папки существует в двух основных вариантах:

- Вы можете разрешить сетевым пользователям просматривать и открывать общие файлы, но ограничить возможность их изменения, создания или удаления. При выборе этого варианта неявной группе Все (Everyone) даются разрешения Чтение и выполнение (Read & Execute) и Чтение (Read) в отношении общих файлов и разрешения Чтение и выполнение (Read & Execute), Список содержимого папки (List Folder Contents) и Читать (Read) в отношении общих папок.
- Вы можете разрешить сетевым пользователям просматривать общие файлы и управлять ими. Это позволяет открывать, изменять, создавать и удалять общие файлы. При выборе этого варианта неявной группе Все (Everyone) даются разрешения Полный доступ (Full Control) для общих файлов и общих папок.

Настройка папки Общие (Public)

Настройки использования папки Общие (Public) задаются индивидуально для каждого компьютера и применяются к самой папке и ко всем ее подпапкам. Чтобы настроить папку Общие (Public), выполните следующие действия:

1. Щелкните кнопку **Пуск (Start)** и выберите команду **Панель управления (Control Panel)**. В категории **Сеть и Интернет (Network And Internet)** щелкните ссылку **Выбор параметров домашней группы и общего доступа к данным (Choose Homegroup And Sharing Options)**. Затем перейдите по ссылке **Изменение дополнительных параметров общего доступа (Change Advanced Sharing Settings)**.

2. Разверните сетевой профиль, с которым хотите работать. В разделе **Доступ к общим папкам (Public Folder Sharing)** выберите нужный способ использования папки Общие (Public). Доступны следующие варианты:
   - **Включить общий доступ, чтобы сетевые пользователи могли читать и записывать файлы в общих папках (Turn On Sharing So Anyone With Network Access Can Read And Write Files In The Public Folders)** Выберите этот вариант, чтобы предоставить полный доступ к общим папкам и всем общим данным любому сетевому пользователю компьютера. Помните, что внешний доступ могут блокировать настройки брандмауэра Windows.
   - **Отключить общий доступ (Turn Off Public Folder Sharing)** Выберите этот вариант, чтобы отключить сетевой доступ к общим папкам и разрешить доступ к общим данным только пользователям, вошедшим в систему локально.
3. Щелкните кнопку **Сохранить изменения (Save Changes)**.

Аудит доступа к файлам и папкам

Разрешения помогают защитить данные, но не показывают, кто именно пытался неправомерно получить доступ к файлам и папкам, а также кто намеренно или случайно удалил важные файлы. Чтобы отследить, кто получал доступ к файлам и папкам и что он с ними делал, настройте аудит доступа. Сделав это и указав, какие файлы и папки подлежат аудиту, затем всю нужную информацию вы найдете в журнале безопасности.

Включение аудита файлов и папок

Для настройки аудита применяются групповая политика или локальная политика безопасности. Используйте групповую политику, чтобы настроить аудит по всему предприятию. Используйте локальную политику безопасности, чтобы настроить аудит на конкретном компьютере. Не забывайте, что локальная политика может быть перекрыта групповой политикой.

Чтобы включить аудит файлов и папок, выполните одно из следующих действий:

- Чтобы настроить локальную политику для конкретного компьютера, откройте консоль Локальная политика безопасности (Local Security Policy), щелкнув кнопку **Пуск (Start)** и выбрав команду **Все программы (All Programs)**, **Администрирование (Administrative Tools)** и **Локальная политика безопасности (Local Security Policy)**. Затем разверните узел **Локальные политики (Local Policies)** и выберите **Политика аудита (Audit Policy)**.
- Чтобы настроить политику предприятия, откройте объект GPO для редактирования в редакторе управления групповой политикой. Далее разверните узлы **Конфигурация компьютера (Computer Configuration)**, **Политики (Policies)**, **Административные шаблоны (Administrative Tem-**

plates), **Параметры безопасности (Security Settings)**, **Локальные политики (Local Policies)** и выберите узел **Политика аудита (Audit Policy)**.

Затем дважды щелкните параметр **Аудит доступа к объектам (Audit Object Access)**. Откроется диалоговое окно **Свойства: Аудит доступа к объектам (Audit Object Access Properties)**. В разделе **Вести аудит следующих попыток доступа (Audit These Attempts)** установите флажок **Успех (Success)**, чтобы регистрировались попытки успешного доступа, флажок **Отказ (Failure)**, чтобы регистрировались попытки неудачного доступа, или оба флажка, а затем щелкните **OK**. Аудит будет включен, но при этом не будет уточнено, какие именно файлы и папки подлежат аудиту.

Настройка аудита и отслеживание попыток доступа

Включив аудит доступа, вы можете настроить способ отслеживания файлов и папок, а также уровень аудита для отдельных папок и файлов. Помните, аудит доступен только на томах NTFS, к аудиту файлов и папок применяются правила наследования. Это позволяет задать аудит доступа ко всем файлам или папкам тома, настроив аудит только корневой папки тома.

Чтобы указать файлы и папки, подлежащие аудиту, выполните следующие действия:

1. В Проводнике Windows правой кнопкой щелкните файл или папку, аудит которой нужно провести, и выберите **команду Свойства (Properties)**.
2. В диалоговом окне **Свойства (Properties)** перейдите на вкладку **Безопасность (Security)**, затем щелкните **Дополнительно (Advanced)**.
3. В диалоговом окне **Дополнительные параметры безопасности (Advanced Security Settings)** щелкните кнопку **Изменить (Edit)** на вкладке **Аудит (Auditing)**. Откроется редактируемая версия вкладки **Аудит (Auditing)**, показанная на рис. 13-12.

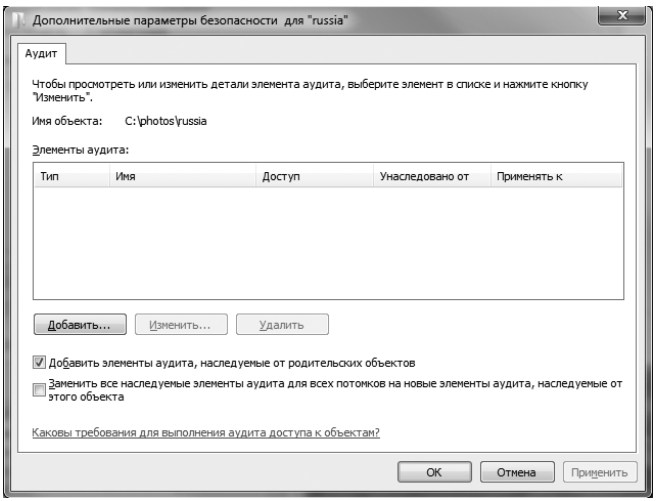

Рис. 13-12. Просмотр текущих настроек аудита и выбор новых настроек

4. Используйте список **Элементы аудита (Auditing Entries)**, чтобы выбрать пользователей, группы или компьютеры, аудит действий которых вы хотите проводить. Чтобы добавить конкретные учетные записи, щелкните кнопку **Добавить (Add)**, затем используйте диалоговое окно **Выбор: «Пользователь», «Компьютер», «Учетная запись службы» или «Группа» (Select User, Computer, Service Account, Or Group)**, чтобы выбрать имя добавляемой учетной записи. Чтобы проводить аудит действий всех пользователей, используйте специальную группу Все (Everyone). Или выберите конкретные группы и пользователей, например Пользователи домена (Domain Users). Щелкнув **OK**, вы увидите диалоговое окно **Элемент аудита для (Auditing Entry For)**, показанное на рис. 13-13.

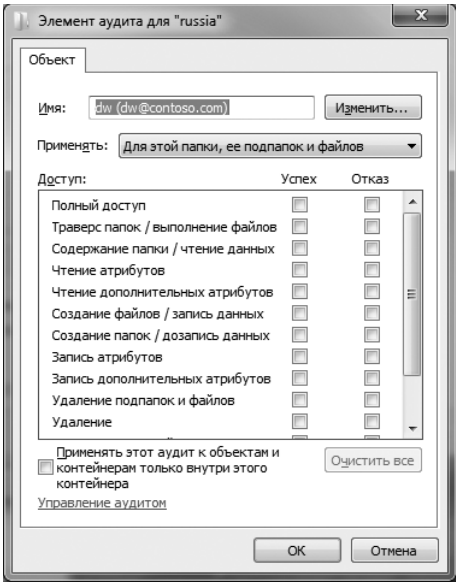

Рис. 13-13. Укажите действия пользователя, группы или компьютера, подлежащие аудиту

5. При помощи списка **Применять (Apply Onto)** укажите, как следует применять аудит.
6. Список **Доступ (Access)** позволяет указать, какие действия подлежат аудиту. Установите флажки **Успех (Successful)** или **Отказ (Failed)** для событий, аудит которых хотите проводить. Эти события совпадают со специальными разрешениями, перечисленным в Табл. 13-1 и 13-3, за исключением того что нельзя проводить аудит синхронизации автономных файлов и папок. Закончив настройку, щелкните **OK**. Чтобы провести аудит других пользователей, групп или компьютеров, повторите процесс сначала.
7. Прежде чем щелкнуть **OK** и закрыть диалоговое окно **Дополнительные параметры безопасности (Advanced Security Settings)**, настройте наследование. Для этого существуют те же два варианта наследования, о которых говорилось выше в этой главе:

- Чтобы параметры аудита наследовались от родительского объекта, установите флажок **Добавить элементы аудита, наследуемые от родительских объектов (Include Inheritable Auditing Entries From This Object's Parent)**.
- Чтобы дочерние объекты текущего объекта наследовали его настройки, установите флажок **Заменить все наследуемые элементы аудита… (Replace All Existing Inheritable Auditing Entries…)**.

Зачастую достаточно отслеживать только неудавшиеся действия. Таким образом вы узнаете, что кто-то пытался выполнить действие и потерпел неудачу. Конечно, неудавшаяся попытка не всегда означает, что кто-то пытался взломать файл или папку. Пользователь просто мог дважды щелкнуть папку или файл, к которым у него нет доступа. Кроме того, некоторые действия вызывают регистрацию многократных неудавшихся попыток, даже если пользователь выполнил действие всего один раз. Тем не менее, вы всегда должны проверять многократные неудавшиеся попытки доступа, поскольку есть вероятность, что кто-то пытается проникнуть в компьютер.

Попытки доступа к файлам или папкам, которые вы настроили для аудита, регистрируются в системном журнале безопасности, который вы можете открыть в консоли Просмотр событий (Event Viewer).

Глава 14

Обеспечение доступности данных

Обеспечение доступности данных — ключевая обязанность системного администратора. Помимо типовых задач по управлению файлами и папками, работа администратора охватывает настройку параметров Проводника Windows (Windows Explorer), управление автономными файлами, работу с дисковыми квотами и управление кешированием филиалов. Параметры автономных файлов определяют доступность файлов и папок во время автономной работы пользователя. Квоты нужны для ограничения доступного пользователю объема дискового пространства. При кешировании филиалов загружаемые документы и файлы сохраняются локально, чтобы их можно было быстро извлечь.

Настройка параметров Проводника Windows

Можно без малейшего преувеличения сказать, что большая часть работы на компьютере состоит в управлении файлами и папками. Вы создаете файлы и папки для хранения и упорядочения информации, перемещаете файлы и папки из одного расположения в другое, задаете свойства файлов и папок и т. д. На решение этих задач уходит уйма времени, между тем, есть ряд несложных приемов эффективного управления, которые сэкономят вам и время, и силы.

Настройка Проводника Windows

Программа Проводник Windows (Windows Explorer) — удобнейший инструмент для работы с файлами и папками. К сожалению, его стандартные параметры рассчитаны на максимально широкий круг пользователей, а не на опытных пользователей и администраторов. Допустим, вы как администратор часто обращаетесь к системным файлам, например к файлам DLL, или к сжатым и несжатым файлам. По умолчанию в Проводнике Windows скрытые файлы не отображаются, а сжатые файлы ничем не отличаются от несжатых.

Чтобы изменить начальные параметры, выполните следующие действия:

1. Откройте **Панель управления (Control Panel)** и щелкните **Оформление и персонализация (Appearance And Personalization)**.

2. В разделе **Параметры папок (Folder Options)** щелкните **Показ скрытых файлов и папок (Show Hidden Files And Folders)**. Как показано на рис. 14-1, диалоговое окно **Параметры папок (Folder Options)** откроется на вкладке **Вид (View)**.

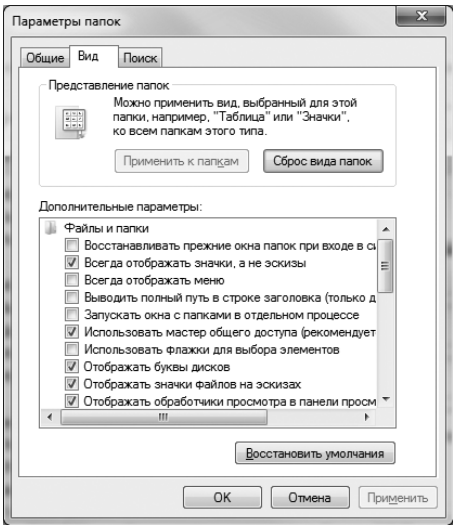

Рис. 14-1. Настройка параметров Проводника Windows в диалоговом окне Параметры папок (Folder Options)

3. Настройте следующие параметры Проводника Windows:
   - **Всегда отображать значки, а не эскизы (Always Show Icons, Never Thumbnails)** По умолчанию в Проводнике Windows отображаются крупные эскизы изображений и других типов файлов. При наличии папок с большим количеством изображений эта функция становится помехой, поскольку у Проводника много времени уходит на формирование эскиза каждого изображения. Установите этот флажок, чтобы отключить эскизы, за исключением случаев, когда в меню **Вид (View)** явно задан параметр **Эскизы (Thumbnails)**.
   - **Всегда отображать меню (Always Show Menus)** По умолчанию панель меню в Проводнике Windows скрыта. Чтобы отобразить ее, нужно щелкнуть **Упорядочить (Organize)**, развернуть подменю **Раскладка (Layout)** и выбрать **Строка меню (Menu Bar)**. Чтобы всегда отображать панель меню, установите этот флажок.
   - **Отображать значки файлов на эскизах (Display File Icon On Thumbnails)** По умолчанию в Проводнике Windows к отображаемым эскизам добавляются значки файлов. Чтобы эскизы отображались без значков, сбросьте этот флажок.
   - **Отображать сведения о размере файлов в подсказках папок (Display File Size Information In Folder Tips)** По умолчанию при наведении указателя мыши на имя или значок папки в Проводнике Windows вы-

водится подсказка, содержащая дату и время создания папки, размер папки и неполный список файлов. Чтобы выводить в подсказке только дату и время создания, сбросьте этот флажок.

- **Выводить полный путь в строке заголовка (Display The Full Path In The Title Bar)** По умолчанию, когда вы нажимаете на клавиши Alt+Tab, переходя в режим переключения между окнами, при наведении указателя мыши на окно Проводника Windows отображается имя открытой в нем папки. Чтобы вместо имени отображался полный путь к папке, установите этот флажок.
- **Скрытые файлы и папки (Hidden Files And Folders)** В Проводнике Windows по умолчанию скрытые файлы, папки или диски не отображаются. Чтобы они были видны, установите переключатель **Показывать скрытые файлы, папки и диски (Show Hidden Files, Folders, And Drives)**.
- **Скрыть пустые диски в папке «Компьютер» (Hide Empty Drives In The Computer Folder)** По умолчанию сведения о пустых дисках в окне Компьютер (Computer) не отображаются. Чтобы информация о пустых дисках отображалась всегда, сбросьте этот флажок.
- **Скрывать расширения для зарегистрированных типов файлов (Hide Extensions For Known File Types)** В Проводнике Windows расширения известных типов файлов по умолчанию не выводятся. Чтобы расширения выводились для всех типов файлов, сбросьте этот флажок.
- **Скрывать защищенные системные файлы (Hide Protected Operating System Files)** В Проводнике (Windows Explorer) файлы ОС по умолчанию не отображаются. Сбросьте флажок, чтобы видеть файлы ОС.
- **Запускать окна с папками в отдельном процессе (Launch Folder Windows In A Separate Process)** По умолчанию все экземпляры Проводника Windows запускаются в одном процессе. Это экономит память и, в общем случае, ускоряет процесс открытия новых окон. С другой стороны, все экземпляры Проводника зависят друг от друга. Сбой одного из экземпляров приводит к закрытию остальных, а из-за зависания или ожидания одного экземпляра все экземпляры могут оказаться заблокированными. Чтобы изменить такое поведение и запускать для каждого экземпляра Проводника новый процесс, установите этот флажок.
- **Отображать буквы дисков (Show Drive Letters)** По умолчанию в области сведений Проводника Windows отображаются буквы дисков. Если выводить их не нужно, сбросьте этот флажок.
- **Отображать сжатые или зашифрованные файлы NTFS другим цветом (Show Encrypted Or Compressed NTFS Files In Color)** По умолчанию зашифрованные и сжатые файлы в Проводнике (Windows Explorer) выделяются цветом: зашифрованные файлы отображаются

зеленым, а сжатые файлы — синим. Чтобы не использовать цветовое различие, сбросьте этот флажок.

- **Отображать описание для папок и элементов рабочего стола (Show Pop-Up Description For Folder And Desktop Items)** По умолчанию, если в Проводнике Windows навести указатель мыши на файл или папку, выводятся подсказки с дополнительными сведениями о них. Сбросьте флажок, чтобы отключить подсказки.
- **Отображать обработчики просмотра в панели просмотра (Show Preview Handlers In Preview Pane)** По умолчанию вы можете просматривать выделенные файлы и папки, если в Проводнике Windows включена область предварительного просмотра. Сбросьте этот флажок, чтобы отключить предварительный просмотр.
- **Использовать флажки для выбора элементов (Use Check Boxes To Select Items)** По умолчанию выбор файлов, папок и других элементов в Проводнике Windows осуществляется только стандартными способами выделения, например простым щелчком или щелчком при нажатой клавише Ctrl или Shift. Если установить этот флажок, выбирать файлы можно будет при помощи флажков.
- **Использовать мастер общего доступа (Use Sharing Wizard)** По умолчанию для настройки общего доступа к файлам в Проводнике Windows используется мастер, описанный в главе 13. Если вы предпочитаете самостоятельно настраивать параметры общего доступа, сбросьте флажок.
- **При вводе текста в режиме «Список» (When Typing Into List View)** По умолчанию при работе в режиме списка нажатие клавиши-буквы приводит к выделению первого файла или папки, начинающихся на эту букву. Если вам удобнее вводить текст в поле поиска, установите переключатель **Автоматически вводить текст в поле поиска (Automatically Type Into The Search Box)**.

Дополнительные параметры Проводника

На работу в программе Проводник Windows (Windows Explorer) и связанными представлениями, например консолью Компьютер (Computer), как пользователи, так и администраторы тратят массу времени, но решаемые администраторами задачи куда сложнее. Вот некоторые из этих задач:

- Развертывание компьютеров с блокировкой некоторых функций Проводника (Windows Explorer). Можно, например, блокировать доступ пользователей ко вкладке **Оборудование (Hardware)**, не давая им просматривать и изменять оборудование компьютера.
- Сокрытие локальных дисков или ограничение доступа к ним. Например, можно запретить пользователям доступ к дисководам для гибких дисков на развертываемых компьютерах.

Эти и другие дополнительные возможности настройки рассмотрены в этом разделе.

Настройка групповой политики для Проводника Windows и представлений папок

Параметры Проводника Windows, подобно параметрам других компонентов Windows 7, настраиваются в групповой политике. Мы подробно остановимся на этих параметрах, поскольку многие из них распространяются также на представления и параметры папок. В табл. 14-1 представлены применяемые в данном случае политики и сведения об их использовании. Эти политики находятся в узле **Конфигурация пользователя\Административные шаблоны\Компоненты Windows\Проводник Windows (User Configuration\Administrative Templates\Windows Components\Windows Explorer)**.

Табл. 14-1. Политики Проводника Windows (Windows Explorer)

Название политики	Описание политики
Запрашивать подтверждение при удалении файлов (Display Confirmation Dialog When Deleting Files)	При каждом удалении файлов или перемещении в Корзину (Recycle Bin) выводится диалоговое окно с запросом на подтверждение действия
Запретить вывод контекстного меню по умолчанию для проводника Windows (Remove Windows Explorer's Default Context Menu)	Запрещает отображение контекстных меню при правом щелчке рабочего стола и Проводника Windows
Запретить доступ к дискам через «Мой компьютер» (Prevent Access To Drives From My Computer)	Запрещает доступ пользователей к файлам на указанных дисках в представлениях Проводника Windows. Пользователи также не могут использовать для доступа к файлам команды **Выполнить (Run)** и **Подключить сетевой диск (Map Network Drive)**
Максимальная длина списка «Недавние документы» (Maximum Number Of Recent Documents)	Задает наибольшее число документов, отображаемых в списке **Недавние документы (Recent Items)**. Значение по умолчанию — 15. Для отображения списка установите флажок **Недавние документы (Recent Items)** в диалоговом окне **Настройка меню «Пуск» (Customize Start Menu)**
Отключить возможности библиотеки Windows, использующие данные индексированных файлов (Turn Off Library Features That Rely On Indexed File Data)	Отключает все представления упорядочивания, за исключением представления По папке (By Folder), а также все предлагаемые варианты фильтрования результатов поиска, кроме фильтрования по дате изменения и размеру. Также отключается возможность просмотра фрагментов содержимого файлов в режиме содержимого и возможность складывать объекты в стопку в контекстном меню

Табл. 14-1. (*продолжение*)

Название политики	Описание политики
Отключить кэширование эскизов изображений (Turn Off Caching Of Thumbnail Pictures)	Отключает кеширование эскизов
Отключить отображение эскизов и отображать только значки (Turn Off The Display Of Thumbnails And Only Display Icons)	Отключает возможность создания и отображения эскизов при доступе пользователей к папкам на локальном компьютере. В результате сокращается время ожидания при первом обращении пользователя к папке, однако теперь для выбора нужного файла пользователю придется просмотреть его содержимое
Отключить отображение эскизов и отображать только значки в сетевых папках (Turn Off The Display Of Thumbnails And Only Display Icons On Network Folders)	Отключает возможность создания и отображения эскизов при обращении пользователей к сетевым папкам. Тем самым сокращается время ожидания при первом обращении пользователя к папке, однако теперь для выбора нужного файла пользователю придется просмотреть его содержимое
Отображать строку меню в проводнике Windows (Display The Menu Bar In Windows Explorer)	Изменяет стандартную конфигурацию, возвращая в Проводник (Windows Explorer) классическую строку меню
Разрешить использование только пользовательских или зарегистрированных расширений (Allow Only Per User Or Approved Shell Extensions)	Расширения увеличивают функциональность Проводника Windows. Этот параметр разрешает запуск на компьютере только тех расширений, что были одобрены администратором или не влияют на других пользователей. Запись о разрешенных расширениях оболочки должна храниться в разделе HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Shell Extensions\Approved реестра
Скрыть выбранные диски из окна «Мой компьютер» (Hide These Specified Drives In My Computer)	Скрывает значки указанных жестких дисков из представлений Проводника Windows. Пользователи смогут получить доступ к этим дискам другими способами
Скрыть команду «Управление» из контекстного меню проводника Windows (Hides The Manage Item On The Windows Explorer Context Menu)	Удаляет из контекстных меню всех представлений Проводника Windows и меню **Пуск (Start)** команду **Управление (Manage)**. Эта команда используется для открытия консоли Управление компьютером (Computer Management)
Удалить вкладку «Безопасность» (Remove Security Tab)	Удаляет вкладку **Безопасность (Security)** из диалоговых окон свойств файлов, папок, ярлыков и дисков. Тем самым пользователям запрещается изменять или просматривать разрешения для соответствующего файла и папки

Табл. 14-1. (*окончание*)

Название политики	Описание политики
Удалить вкладку «Оборудование» (Remove Hardware Tab)	Удаляет из всех диалоговых окон вкладку **Оборудование (Hardware)** с запретом на просмотр, изменение и диагностику устройств пользователями
Удалить вкладку DFS (Remove DFS Tab)	Удаляет вкладку DFS из Проводника (Windows Explorer) и окон, основанных на Проводнике Windows. Пользователям запрещается работать с вкладкой для просмотра и изменения параметров распределенной файловой системы (DFS). Вкладка DFS доступна только, когда в домене или рабочей группе настроена DFS
Удалить возможности записи компакт-дисков (Remove CD Burning Features)	Запрещает создавать и изменять компакт-диски в Проводнике Windows. Пользователям разрешается применять другие программы записи компакт-дисков
Удалить команду «Свойства папки» из меню «Сервис» (Removes The Folder Options Menu Item From The Tools Menu)	Запрещает доступ пользователей к диалоговому окну **Свойства папки (Folder Options)**. В результате пользователи не могут изменять представления папки, типы файлов или параметры автономных файлов. Параметры папок для пользователей будут по-прежнему доступны в панели управления
Удалить команды «Подключить сетевой диск» и «Отключить сетевой диск» (Remove “Map Network Drive” And “Disconnect Network Drive”)	Запрещает подключение и отключение сетевых дисков в Проводнике Windows. Не запрещает использование других способов, например команд командной строки
Удалить меню «Файл» из проводника Windows (Remove File Menu From Windows Explorer)	Удаляет меню **Файл (File)** из представлений Проводника Windows. Выполнять задачи из этого меню другими способами пользователям не запрещено

Из табл. 14-1 видно, что многие политики Проводника Windows предназначены для управления доступностью параметров, например элементов меню и вкладок диалоговых окон. Чтобы настроить эти параметры для всех пользователей компьютера, выполните следующие действия:

1. Откройте объект GPO для редактирования в редакторе управления групповой политикой. Соответствующие политики находятся в узле **Конфигурация пользователя\Административные шаблоны\Компоненты Windows\Проводник Windows (User Configuration\Administrative Templates\Windows Components\Windows Explorer)**.
2. Дважды щелкните политику, которую нужно настроить. В открывшемся диалоговом окне выберите один из следующих переключателей:
   - **Не задано (Not Configured)** Для параметра политики не будет внесено никаких изменений в реестр.

- **Включить (Enabled)** Включение политики и обновление реестра.
- **Отключить (Disabled)** Отключение политики и обновление реестра.

3. Щелкните **OK**.

Примечание В последующих разделах вы найдете подробное описание некоторых из перечисленных политик. Особое внимание уделите разделу «Управление доступом к дискам в Проводнике Windows». В нем рассказано о сокрытии и запрещении доступа к дискам в Проводнике.

Работая с параметрами политик, относящихся к Проводнику Windows, имейте в виду, что следующие параметры неприменимы в Windows Vista и Windows 7:

- **Максимально допустимый размер «Корзины» (Maximum Allowed Re-cycle Bin Size)** Чтобы изменить параметры корзины для текущего пользователя, щелкните правой кнопкой значок **Корзина (Recycle Bin)** и выберите команду **Свойства (Properties)**. На вкладке **Общие (General)** укажите наибольший разрешенный размер, ее желаемое расположение, а затем щелкните **OK**.
- **Скрыть значок «Соседние компьютеры» в папке «Сеть» (No «Computers Near Me» In Network Locations)/Скрыть значок «Вся сеть» в папке «Сеть» (No «Entire Network» In Network Locations)** В Windows 7 возможность определения топологии сети встроена в Центр управления сетями и удаленным доступом (Network and Sharing Center). Функция Соседние пользователи (People Near Me), используемая в Windows Collaboration, нужна для идентификации людей, использующих компьютеры в одном и том же сегменте сети.
- **Удалить кнопку «Поиск» из проводника Windows (Remove Search Button From Windows explorer)** Функциональные возможности поиска более тесно интегрированы в Windows 7, поэтому они управляются иначе. Некоторые параметры находятся в узле **Конфигурация пользователя\Административные шаблоны\Компоненты Windows\Быстрый поиск (User Configuration\Administrative Templates\Windows Components\Instant Search)**. Параметры управления индексированием файлов и папок находятся в узле **Конфигурация пользователя\Административные шаблоны\Компоненты Windows\Найти (User Configuration\Administrative Templates\Windows Components\Search)**.

Управление доступом к дискам в Проводнике Windows

Иногда требуется заблокировать доступ к файлам, находящимся на тех или иных дисках, или даже скрыть целые диски. Сделать это можно в групповой политике. При этом используются политики **Скрыть выбранные диски из окна «Мой компьютер» (Hide These Specified Drives In My Computer)** и **Запретить доступ к дискам через «Мой компьютер» (Prevent Access To Drives From My Computer)**.

К скрытым дискам пользователи не могут обращаться из представлений Проводника (Windows Explorer), но могут получить доступ к ним другими способами. Если же доступ к дискам запрещен, пользователям не удастся получить доступ к любым находящимся на них файлам, что означает запрет на доступ из программы Проводник (Windows Explorer) или при помощи команд **Выполнить (Run)** и **Подключить сетевой диск (Map Network Drive)**. При этом в Проводнике Windows остаются видимыми значки дисков и структура папок.

Чтобы скрыть выбранные диски или закрыть доступ к файлам на выбранных дисках, выполните следующие действия:

1. Откройте объект GPO для редактирования в редакторе управления групповой политикой. Соответствующие политики находятся в узле **Конфигурация пользователя\Административные шаблоны\Компоненты Windows\Проводник Windows (User Configuration\Administrative Templates\Windows Components\Windows Explorer)**.
2. Чтобы скрыть диски, дважды щелкните параметр **Скрыть выбранные диски из окна «Мой компьютер» (Hide These Specified Drives In My Computer)** и установите переключатель **Включить (Enabled)**. Укажите диски, которые нужно скрыть, и щелкните **OK**. Вот основные возможности:
   - Чтобы ограничить доступ ко всем встроенным жестким дискам и дисководам для гибких дисков, выберите в списке вариант **Ограничить доступ ко всем дискам (Restrict All Drives)**.
   - Чтобы ограничить доступ только к дисководам для гибких дисков, выберите вариант **Ограничить доступ к дискам A и B (Restrict A And B Drives Only)**.
   - Чтобы ограничить доступ к дисководам для гибких дисков и диску C, выберите вариант **Ограничить доступ к дискам A, B и C (Restrict A, B And C Drives Only)**.
   - Чтобы снять ограничения, выберите вариант **Не ограничивать доступ к дискам (Do Not Restrict Drives)**.
3. Чтобы запретить доступ к файлам, находящимся на заданных дисках, дважды щелкните параметр **Запретить доступ к дискам через «Мой компьютер» (Prevent Access To Drives From My Computer)** и установите переключатель **Включить (Enabled)**. Затем выберите диски, доступ к которым нужно ограничить, и щелкните **OK**.

Примечание Возможностью просматривать файлы в папке управляет разрешение Список содержимого папки (List Folder Contents). Чтобы пользователи гарантированно не могли просматривать даже имена папок на дисках, скройте диски.

Управление автономными файлами

Настройка автономных файлов производится в несколько этапов. Начинается он с настройки параметров групповой политики и параметров спе-

циальных автономных папок, а заканчивается настройкой параметров автономной работы пользователя. Хотя автономно работают, главным образом, пользователи ноутбуков, которые увозят их домой или в командировку, настройка автономных файлов может оказаться полезной и другим пользователям. Настройка автономных файлов в групповой политике описана в главе 3. В этом разделе мы подробнее остановимся на автономных файлах и действиях по их настройке.

Основы автономных файлов

Автономные файлы позволяют осуществлять доступ к сетевым файлам в тот момент, когда компьютер отключен от сети или в сети произошел сбой. После настройки автономных файлов в Windows 7 эти файлы всегда используются автоматически при недоступности сетевых файлов, поэтому в случае сбоя в сети пользователь может не прерывать работу. После восстановления сетевого подключения файлы на компьютере пользователя синхронизируются с файлами, находящимися в сетевой папке.

Способ применения изменений зависит от того, как они были сделаны. Если в один и тот же автономный файл внесли изменения несколько пользователей, функция разрешения конфликтов поможет им сохранить свою версию файла, перезаписав существующую версию, сохранить существующую версию или сохранить в сети обе версии. При удалении пользователем автономного файла из сети файл также удаляется, если, конечно, сетевой файл не был к этому моменту изменен другим пользователем. В этом случае файл удаляется с компьютера пользователя, но не из сети. Если пользователи изменил автономный файл, который был удален из сети, ему будет представлена возможность сохранить свою версию в сети или удалить ее со своего компьютера.

В Windows 7 в способ применения автономных файлов внесено два ключевых изменения:

- **Синхронизация только изменений** Быстрая синхронизация, в ходе которой в Windows 7 синхронизируются, то есть записываются на сервер, только измененные блоки файлов.
- **Несинхронизированные копии недоступных файлов и папок** Если в автономном режиме доступна лишь часть содержимого папки, для сохранения оперативного контекста в Windows 7 создаются несинхронизированные записи остальных файлов и папок. Если вы не подключены к удаленному расположению, наряду с обычными записями автономных объектов вы увидите несинхронизированные записи оперативных объектов.

Время синхронизации автономных файлов могут задавать как пользователи, так и администраторы. Автоматическую синхронизацию можно назначить на время входа и выхода пользователя из системы, а также на время перехода компьютера в режим сна или гибернации. Значения параметров автоматической синхронизации зависят от параметров групповой политики

и параметров пользователя. Подробно о настройке параметров автономных файлов в групповой политике рассказано в главе 3.

Ручная синхронизация выполняется в Центре синхронизации (Sync Center). Чтобы открыть Центр синхронизации (Sync Center), последовательно щелкните **Пуск (Start)**, **Все программы (All Programs)**, **Стандартные (Accessories)** и **Центр синхронизации (Sync Center)**.

Организация автономного доступа к файлам и папкам

Общие сетевые папки можно сделать доступными для автономного использования. По умолчанию в автономном режиме доступны также все вложенные папки и файлы общих папок, но при необходимости доступность отдельных файлов и папок в автономном режиме можно изменить. Имейте в виду, что новые файлы, добавляемые в общую папку, предназначенную для автономной работы, пользователям, работающим автономно, автоматически не передаются. Чтобы получить обновления, автономную папку необходимо синхронизировать.

Настройка автономных файлов выполняется в Проводнике (Windows Explorer) или в консоли Управление компьютером (Computer Management). Консоль Управление компьютером (Computer Management) позволяет управлять автономными файлами на любом компьютере сети, что делает ее более предпочтительным средством. Чтобы сделать файлы и папки доступными автономно, нужно выполнить три действия: сначала открыть общий доступ к папке, затем сделать ее доступной автономно и, наконец, указать конкретные файлы и папки для автономной работы.

Шаг 1: предоставление общего доступа к папке

Чтобы открыть общий доступ к папке в консоли Управление компьютером (Computer Management), выполните следующие действия:

1. В дереве консоли щелкните правой кнопкой узел **Управление компьютером (Computer Management)** и выберите команду **Подключиться к другому компьютеру (Connect To Another Computer)**. В диалоговом окне **Выбор компьютера (Select Computer)** найдите нужный компьютер.
2. В дереве консоли последовательно разверните узлы **Служебные программы (System Tools)** и **Общие папки (Shared Folders)**, затем выберите **Общие ресурсы (Shares)**. В области сведений отображены текущие общие ресурсы системы.
3. Щелкните правой кнопкой узел **Общие ресурсы (Shares)** и выберите команду **Новый общий ресурс (New Share)**. Открытие общего доступа к папке при помощи мастера описано в главе 13.

Шаг 2: открытие автономного доступа к файлам и папкам

Чтобы сделать общую папку доступной для автономного использования в консоли Управление компьютером (Computer Management), выполните следующие действия:

1. В дереве консоли щелкните правой кнопкой узел **Управление компьютером (Computer Management)** и выберите команду **Подключиться к другому компьютеру (Connect To Another Computer)**. В диалоговом окне **Выбор компьютера (Select Computer)** найдите нужный компьютер.
2. В дереве консоли последовательно разверните узлы **Служебные программы (System Tools)** и **Общие папки (Shared Folders)**, затем выберите **Общие ресурсы (Shares)**.
3. Дважды щелкните общий ресурс, который нужно сделать доступным для автономного использования. На вкладке **Общие (General)** щелкните кнопку **Настройка (Offline Settings)**.
4. В диалоговом окне **Настройка автономного режима (Offline Settings)**, показанном на рис. 14-2, выберите один из переключателей:
   - **Вне сети доступны только указанные пользователем файлы и программы (Only The Files And Programs That Users Specify Are Available Offline Use)** Этот вариант применяется, когда пользователи должны сами указать файлы, с которыми они будут работать в автономном режиме. Он установлен по умолчанию и лучше всего подходит в ситуации, когда несколько пользователей намерены изменять одни и те же файлы. После настройки ручного кеширования файлов они автоматически загружаются и делаются доступными для автономного использования. Если раньше в кеш была записана более старая версия документа, она будет удалена. При работе с файлом в оперативном режиме в его серверной версии всегда присутствует информация о том, что файл используется.
   - **Вне сети автоматически доступны все открывавшиеся пользователем файлы и программы (All Files And Programs That Users Open From The Shared Folder Are Automatically Available Offline)** Этот вариант применяется для папок, в которых содержатся пользовательские данные и программы. Открытые файлы и программы загружаются и делаются доступными для автономного использования автоматически. Если раньше в кеш была записана более старая версия документа, она будет удалена. При работе с файлом в оперативном режиме в его серверной версии всегда присутствует информация о том, что файл используется. При возникновении конфликтов версий выводятся сообщения об этом.

     Для этого варианта доступен флажок **Оптимизировать производительность (Optimize For Performance)**, включающий расширенное кеширование программ. При этом программы, доступные в сети, кешируются и запускаются локально, что повышает производительность.
5. Дважды щелкните **OK**.

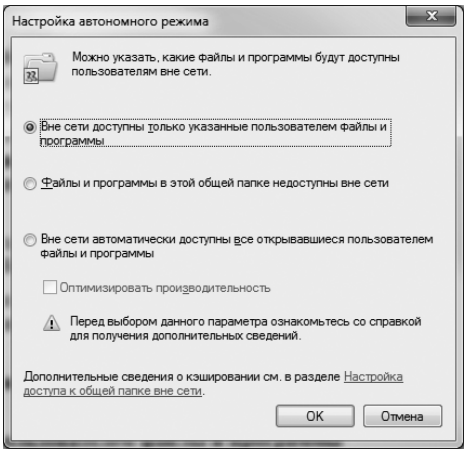

Рис. 14-2. Настройка параметров записи в кеш автономных файлов

Шаг 3: указание используемых автономных файлов и папок

Создав общие ресурсы и настроив их автономное использование, укажите используемые автономно файлы и папки, выполнив следующие действия:

1. Подключите к общему файлу или папке сетевой диск, как описано в главе 13.
2. В меню **Пуск (Start)** выберите команду **Компьютер (Computer)**.
3. Создайте кеш автономных файлов одним из следующих способов:
   - Чтобы скопировать содержимое общей папки на компьютер пользователя и сделать его доступным для автономного использования, в разделе **Сетевое размещение (Network Location)** щелкните правой кнопкой нужное размещение и выберите команду **Всегда доступны автономно (Always Available Offline)**.
   - Чтобы скопировать на компьютер пользователя и сделать доступными для автономного использования только выбранную папку (и ее содержимое) или выбранный файл, найдите сетевой файл или папку в консоли Компьютер (Computer), щелкните его правой кнопкой и выберите команду **Всегда доступны автономно (Always Available Offline)**.

При открытии автономного файла или папки на компьютере пользователя создается локальный кеш содержимого этого файла и папки. Между локальным и удаленным компьютерами устанавливается связь синхронизации (или расширяется за счет включения в нее новых общих файлов и папок). Об управлении связями синхронизации читайте в разделе «Управление синхронизацией файлов в автономном режиме».

Автономная работа

Всякий раз, когда компьютер не подключен к локальной сети, вы работаете автономно. Признаком автономной работы является красный крестик

в разделе Сетевые размещения (Network Locations) консоли Компьютер (Computer) или на значке **Сеть (Network)** области уведомлений панели задач. В автономном режиме работа с сетевыми файлами не отличается от работы в оперативном режиме. При этом во время автономной работы сохраняются все разрешения. Если у вас есть доступ к файлу только для чтения, когда вы подключены к сети, изменить файл в автономном режиме вам не удастся.

Выбрать работу в автономном режиме можно и при наличии активного сетевого подключения, выполнив следующие действия:

1. В программе Проводник (Windows Explorer) откройте сетевую папку с файлами, с которыми хотите работать в автономном режиме, и щелкните кнопку **Режим работы вне сети (Work Offline)** на панели инструментов.
2. Для возврата в оперативный режим снова щелкните кнопку **Работать в сети (Work Online)** на панели инструментов. При этом будет произведена синхронизация всех изменений, внесенных в сетевые файлы в автономном режиме.

Управление синхронизацией файлов в автономном режиме

Программа Центр синхронизации (Sync Center) облегчает управление кешированными автономными файлами и папками (рис. 14-3). В центре синхронизации для каждой общей папки, содержание которой записывается в локальный кеш, устанавливается связь синхронизации, свойства которой позволяют задавать, когда и как проводится синхронизация.

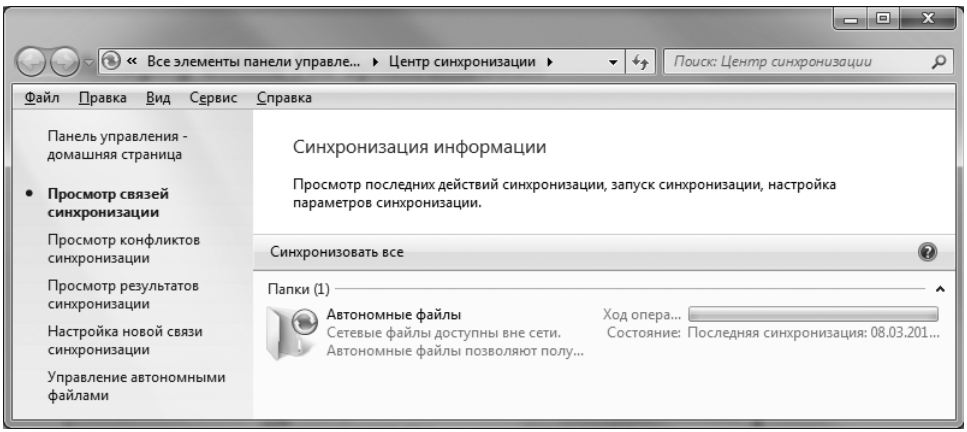

Рис. 14-3. Управление синхронизацией осуществляется в Центре синхронизации (Sync Center)

Просмотр текущих связей синхронизации

Для просмотра текущих связей синхронизации в программе Центр синхронизации (Sync Center) выполните следующие действия:

1. Чтобы открыть Центр синхронизации (Sync Center), щелкните **Пуск**

(Start), **Все программы (All Programs)**, **Стандартные (Accessories)** и **Центр синхронизации (Sync Center)**.

2. Просмотрите связи синхронизации. Для них указаны имена, состояние, процесс выполнения, счетчик конфликтов, счетчик ошибок и категория.

Программа Центр синхронизации (Sync Center) позволяет легко выявлять проблемы синхронизации, а также запускать, останавливать или настраивать синхронизацию.

Ручная синхронизация автономных файлов

Вы можете выполнить синхронизацию автономных файлов вручную одним из следующих способов:

- **Синхронизация всех автономных файлов и папок** При наличии нескольких связей для синхронизации всех автономных файлов и папок откройте Центр синхронизации (Sync Center) и щелкните **Синхронизировать все (Sync All)**. Кнопка **Синхронизировать все (Sync All)** доступна только тогда, когда не выбрана ни одна из связей синхронизации.
- **Синхронизация отдельного сетевого ресурса** Для синхронизации автономных файлов и папок в конкретной общей сетевой папке откройте Центр синхронизации (Sync Center), щелкните нужную связь синхронизации, а затем щелкните кнопку **Синхронизация (Sync)**.

Автоматическая синхронизация автономных файлов

Синхронизация автономных файлов определяется параметрами групповой политики. Обычно она выполняется автоматически при возвращении пользователя в сеть. Синхронизация также может выполняться в одном из следующих случаев:

- в запланированное время;
- при входе пользователя в систему;
- во время бездействия компьютера;
- когда пользователь блокирует или разблокирует Windows.

Синхронизация по расписанию

Чтобы настроить синхронизацию по расписанию, выполните следующие действия:

1. В Центре синхронизации (Sync Center) щелкните правой кнопкой нужную связь синхронизации и выберите команду **Расписание для (Schedule For Offline Files)**.
2. Если для данного ресурса ранее была настроена синхронизация по расписанию, вы можете выполнить следующие действия:
   - Щелкните **Создать новое расписание синхронизации (Create A New Sync Schedule)** и выполните шаги 3-7, чтобы создать новое расписание.
   - Щелкните **Просмотреть или изменить существующее расписание синхронизации (View Or Edit An Existing Sync Schedule)**, щелкните

Далее (Next) и выполните шаги 3-7, чтобы изменить существующее расписание.

- Щелкните **Удалить существующее расписание синхронизации (Delete An Existing Sync Schedule)**, выделите удаляемое расписание и щелкните **Удалить (Delete)**, чтобы удалить расписание. Щелкните **OK** и пропустите остальные шаги.

3. Просмотрите настраиваемые элементы и сбросьте флажки элементов, настраивать которые не следует. Щелкните **Далее (Next)**, а затем **В указанное по расписанию время (At A Scheduled Time)**.
4. Параметры **Запуск (Start On)** и **В (At)** настроены так, что запланированная синхронизация начнется немедленно (рис. 14-4). Если синхронизацию по расписанию нужно начать в другое время, измените дату и время запуска.
5. Интервал синхронизации определяется значение параметра **Повторять каждые (Repeat Every)**. Стандартный интервал равен одному дню. Значение интервала можно задать в минутах, часах, днях, неделях или месяцах. Синхронизируются только изменения, поэтому частая синхронизация, в отличие от Windows XP, не повредит быстродействию компьютера. Например, важные файлы можно синхронизировать каждые 3-4 часа.
6. Щелкните **Далее (Next)**.
7. Введите имя для синхронизации по расписанию и щелкните **Сохранить расписание (Save Schedule)**.

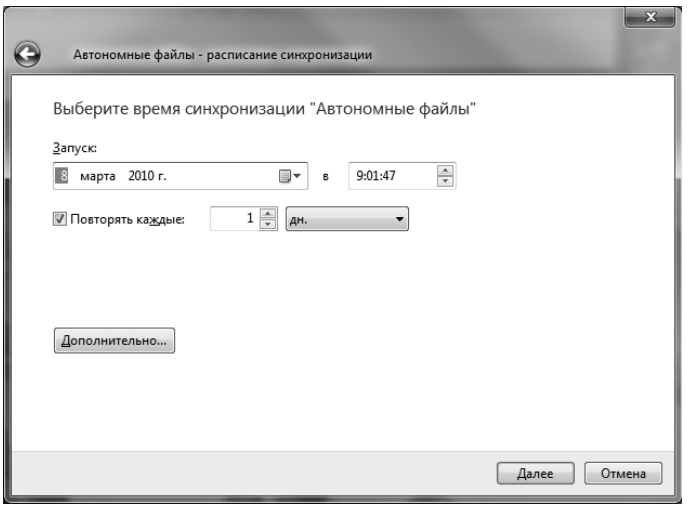

Рис. 14-4. Создание расписания синхронизации

Синхронизация по событию или действию

Чтобы управлять синхронизацией на основе событий или действий, выполните следующие действия:

1. В Центре синхронизации (Sync Center) выделите нужную связь синхронизации и щелкните **Расписание (Schedule)**.
2. Если для данного ресурса ранее была настроена синхронизация по расписанию, вы можете выполнить следующие действия:
   - Щелкните **Создать новое расписание синхронизации (Create A New Sync Schedule)** и выполните шаги 3-6, чтобы создать новое расписание.
   - Щелкните **Просмотреть или изменить существующее расписание синхронизации (View Or Edit An Existing Sync Schedule)**, щелкните **Далее (Next)** и выполните шаги 3-6, чтобы изменить существующее расписание.
   - Щелкните **Удалить существующее расписание синхронизации (Delete An Existing Sync Schedule)**, выделите удаляемое расписание и щелкните **Удалить (Delete)**, чтобы удалить расписание. Щелкните **OK** и пропустите остальные шаги.
3. Просмотрите настраиваемые элементы, сбросьте флажки элементов, настраивать которые не следует, и щелкните **Далее (Next)**. Щелкните **Когда происходит определенное событие (When An Event Occurs)**.
4. Флажками отметьте события и действия, при наступлении которых следует начать автоматическую синхронизацию (рис. 14-5).
5. Щелкните **Далее (Next)**.
6. Введите имя синхронизации и щелкните **Сохранить расписание (Save Schedule)**.

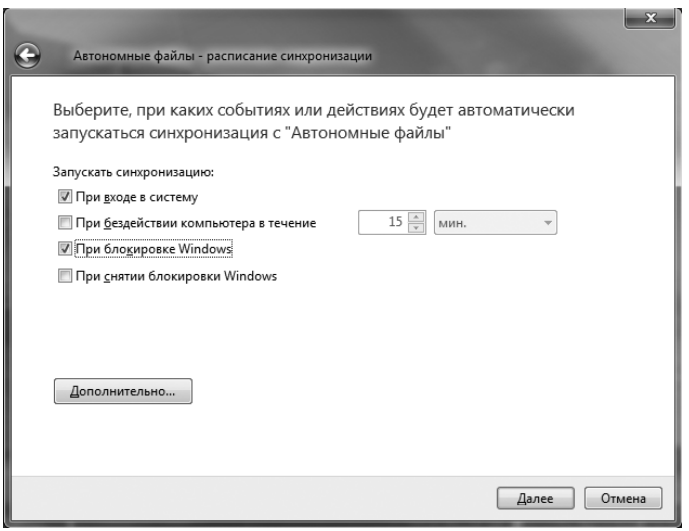

Рис. 14-5. Синхронизация, основанная на событиях и действиях

Просмотр сведений, ошибок и предупреждений синхронизации

В результатах синхронизации содержатся сведения о ней, ошибки и предупреждения. Чтобы просмотреть результаты синхронизации, откройте Центр синхронизации (Sync Center) и щелкните ссылку **Просмотр результатов синхронизации (View Sync Results)**. На экран будут выведены сведения о времени начала, остановки или завершения синхронизации. Информация об ошибках и предупреждения помогут найти возможные сбои в конфигурации синхронизации.

Разрешение конфликтов синхронизации

Конфликты синхронизации возникают при изменении пользователем автономного файла, который был обновлен в сети другим пользователем. Чтобы просмотреть и разрешить конфликты синхронизации, выполните следующие действия:

1. В Центре синхронизации (Sync Center) щелкните **Просмотр конфликтов синхронизации (View Sync Conflicts).**
2. Просмотрите информацию о конфликтах на открывшейся панели (рис. 14-6).

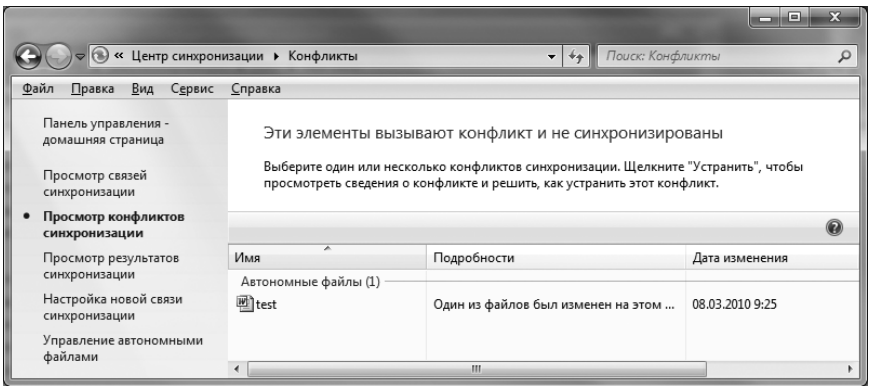

Рис. 14-6. На этой панели показана информация о конфликтах

3. Дважды щелкните конфликт, чтобы открыть диалоговое окно **Устранить конфликт (Resolve Conflict)**, показанное на рис. 14-7.

4. Выполните одно из следующих действий:
   - Щелкните версию, которую нужно сохранить. Если вы хотите сохранить локальную версию и перезаписать версию, имеющуюся в сети, щелкните версию с комментарием **На этом компьютере (On This Computer)**. Если нужно сохранить сетевую версию и перезаписать локальную версию, щелкните версию, расположенную в общем сетевом расположении.
   - Чтобы записать локальную версию в общее сетевое расположение под новым именем, щелкните **Сохранить обе версии (Keep Both Versions)**.

Новое имя будет совпадать со старым, с добавлением идентификатора версии. Если вы не уверены, какой из версий отдать предпочтение, сохраните обе версии, а потом сравните их, применяя одни и отменяя другие изменения.

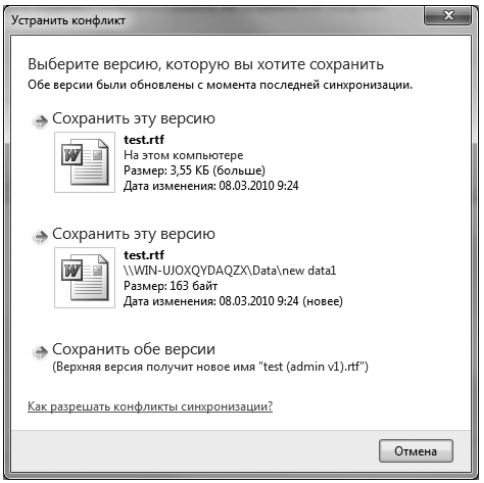

Рис. 14-7. Разрешение конфликтов синхронизации в диалоговом окне Устранить конфликт (Resolve Conflict)

Настройка использование диска автономными файлами

Программа Центр синхронизации (Sync Center) позволяет управлять объемом дискового пространства, доступного для автономных файлов. По умолчанию автономные файлы могут занимать определенную долю объема диска, на котором хранятся профили пользователя. Чтобы настроить ограничения по использованию диска для автономных файлов, выполните следующие действия:

1. В Центре синхронизации (Sync Center) щелкните ссылку **Управление автономными файлами (Manage Offline Files)**.
2. В открывшемся диалоговом окне **Автономные файлы (Offline Files)** на вкладке **Использование диска (Disk Usage)** выведен полный объем пространства, занимаемый всеми автономными и временными файлами (рис. 14-8). Временные файлы создаются в процессе работы пользователей с автономными файлами на компьютере.
3. Обратите внимание на ограничение для автономных и временных файлов. Оно указано в мега- или гигабайтах, а также в процентах от размера диска, на котором хранятся профили пользователя.
4. Щелкните кнопку **Изменить ограничения (Change Limits)**. В диалоговом окне **Ограничения места на диске для автономных файлов (Offline Files Disk Usage Limits)** задайте ограничения для автономных и временных файлов, а затем щелкните **OK**.

5. Чтобы удалить неиспользуемые временные файлы, щелкните **Удалить временные файлы (Delete Temporary Files)**. Удаление временных файлов не влияет на сохраненные локальные копии сетевых файлов.
6. Щелкните **OK**.

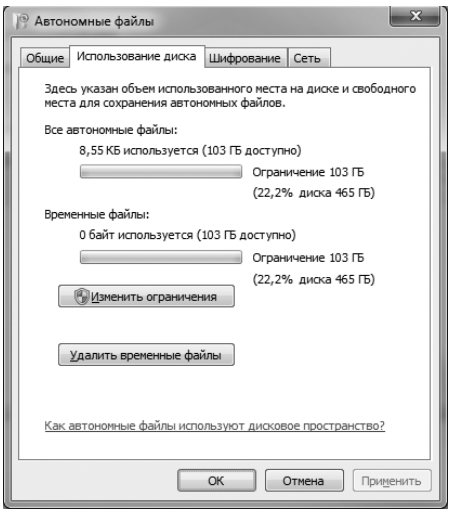

Рис. 14-8. Настройка ограничений на использование диска автономными файлами

Шифрование автономных файлов

Для повышения безопасности данных вы вольны использовать шифрование автономных файлов. При этом шифроваться будут только те файлы, которые хранятся на вашем компьютере, но не в сети. Для работы с шифрованными файлами пользователям не требуется их расшифровывать. Расшифровка выполняется автоматически средствами ОС. Чтобы включить шифрование автономных файлов, выполните следующие действия:

1. В Центре синхронизации (Sync Center) щелкните **Управление автономными файлами (Manage Offline Files)**.
2. На вкладке **Шифрование (Encryption)** щелкните кнопку **Зашифровать (Encrypt)**, чтобы включить шифрование автономных файлов. Щелкните **OK**.
3. Если позже вам потребуется снять шифрование, повторите процедуру, щелкнув кнопку **Расшифровать (Unencrypt)**.

Отмена доступа к автономным файлам

Администратор вправе указать файлы, которые не должны использоваться автономно. Обычно так делают, когда некоторые файлы из общей папки пользователю копировать не следует. Чтобы сделать файл недоступным для автономной работы, нужно задать политику исключений, как описано в разделе «Административное управление автономными файлами и папками» главы 3.

Чтобы сделать общую папку недоступной для автономного использования в консоли Управление компьютером (Computer Management), выполните следующие действия:

1. В дереве консоли щелкните правой кнопкой узел **Управление компьютером (Computer Management)** и выберите команду **Подключиться к другому компьютеру (Connect To Another Computer)**. В диалоговом окне **Выбор компьютера (Select Computer)** найдите нужный компьютера.
2. В дереве консоли разверните узлы **Служебные программы (System Tools)** и **Общие папки (Shared Folders)**, а затем выберите **Общие ресурсы (Shares)**.
3. Дважды щелкните общий ресурс, который нужно настроить. На вкладке **Общие (General)** щелкните **Настройка (Offline Settings)**.
4. В диалоговом окне **Настройка автономного режима (Offline Settings)** установите переключатель **Файлы и программы в этой общей папке недоступны вне сети (No Files Or Programs From The Shared Folder Are Available Offline)**.
5. Щелкните **OK**.

Чтобы полностью отменить возможность использования автономных файлов, выполните следующие действия:

1. В Центре синхронизации (Sync Center) щелкните **Управление автономными файлами (Manage Offline Files)**.
2. В открывшемся диалоговом окне **Автономные файлы (Offline Files)** на вкладке **Общие (General)** щелкните кнопку **Отключить автономные файлы (Disable Offline Files)**, а затем щелкните **OK**.

Если позже вам потребуется включить автономные файлы, повторите процедуру, на этот раз щелкнув кнопку **Включить автономные файлы (Enable Offline Files)**.

Дисковые квоты

В следующих разделах мы поговорим об использовании и настройке дисковых квот. Дисковые квоты позволяют управлять дисковым пространством и настраиваются на уровне тома. Квоты доступны только для томов с файловой системой NTFS — их нельзя создать для томов FAT16 или FAT32. Первым шагом в настройке дисковой квоты является включение политик дисковых квот, как описано в разделе «Политики дисковых квот» главы 3. После настройки политик приступайте к установке квот для томов.

Применение дисковых квот

Администраторы применяют дисковые квоты для регулирования использования дискового пространства критически важных томов, например, томов, на которых содержатся корпоративные или пользовательские общие ресурсы. Включив квоты на диске, вы задаете предел дисковой квоты, а также

порог предупреждения дисковой квоты. Предел определяет наибольшее доступное пространство (не давая пользователям записывать на том дополнительную информацию) и (или) запись события превышения пользователем ограничения. Уровень предупреждений дисковой квоты предназначен для оповещения пользователей и записи предупреждений, когда пользователи приближаются к ограничениям дисковой квоты.

Ближе к реальности Большинство администраторов настраивает принудительные квоты, но вы вольны настроить и дисковые квоты без принудительного применения. Вы спросите — зачем? Иногда достаточно просто отследить использование диска пользователями и выяснить, когда пользователь превысил заданный предел. Вместо отказа в предоставлении пользователю дополнительного пространства на диске вы можете отметить превышение, записав событие в журнал приложений.

Дисковые квоты применимы только к обычным пользователям, но не к администраторам. Администратору нельзя отказать в использовании дискового пространства, даже если он вышел за предел принудительного ограничения дисковой квоты. Ограничения и предупреждения дисковых квот задаются в килобайтах (Кб), мегабайтах (Мб), терабайтах (Тб) и пр. В обычной среде используются мегабайты и гигабайты. Так, на корпоративном общем ресурсе с данными одного отдела можно ограничить использование дискового пространства в пределах 20–100 Гб. Гораздо меньший уровень в 5–20 Гб устанавливают для общего ресурса пользователя, не давая ему создавать больше объемы личных данных. Пороги предупреждения дисковой квоты задаются в процентном отношении к пределу дисковой квоты. Например, порог предупреждения может составлять 90–95% от предела дисковой квоты.

Наблюдение за дисковыми квотами ведется для тома или для пользователя, поэтому использование диска одним пользователем никак не влияет на дисковые квоты других пользователей. Если один пользователь превысил предел, применяемые к нему ограничения не распространяются на других пользователей. Допустим, пользователь превысил предел дисковой квоты в 5 Гб, и параметры тома запрещают запись при превышении предела. Пользователь не сможет записывать данные на том, но сможет удалить файлы и папки из тома, переместить файлы и папки в сжатую область тома или сжать файлы, чтобы освободить пространство. Перемещение файлов в другое расположение в пределах тома не влияет на ограничение квоты. Объем занимаемого файлами пространства останется прежним, если, конечно, несжатые файлы не перемещаются в сжатую папку. В любом случае, ограничение одного пользователя не повлияет на возможность других пользователей производить запись на том (если на томе есть свободное пространство).

Дисковые квоты можно включить на локальных и на удаленных томах. Для управления дисковыми квотами на локальном томе нужно работать непосредственно с диском. Для управления дисковыми квотам на удаленных томах необходимо открыть общий доступ к корневому каталогу тома, а затем установить для тома дисковую квоту. Имейте в виду, что при включенных дисковых квотах на локальном томе файлы ОС и приложений не учи-

тываются в объеме дискового пространства для установившего их пользователя. Как правило, владельцем системных файлов является учетная запись TrustedInstaller, а файлов программ — системная учетная запись.

Настраивать дисковые квоты имеют право только члены групп администраторов домена и локальных администраторов. Локальная групповая политика позволяет включить дисковые квоты для отдельного компьютера. Дисковые квоты для групп пользователей и компьютеров включаются при помощи политик сайта, домена или подразделения. Соблюдение дисковых квот приводит к некоторым издержкам, зависящим от количества применяемых квот, общего размера томов и их данных, а также количества пользователей, к которым применены квоты.

Хотя внешне наблюдение за дисковыми квотами выполняется для конкретных пользователей, реально в Windows 7 управление квотами выполняется при помощи идентификаторов безопасности (SID). Это позволяет изменять имена пользователей, не затрагивая конфигурацию дисковой квоты. Правда, использование SID приводит к дополнительным издержкам при просмотре статистики дисковой квоты для пользователей. Это связано с необходимостью привязки SID к именам учетных записей, для чего необходима связь со службой диспетчера локальных пользователей или контроллером домена. После первичного просмотра имен они кешируются в локальный файл, чтобы обеспечить быстрый доступ к ним при следующем обращении. Кеш-память запросов обновляется редко, поэтому при обнаружении несоответствия между отображаемыми и настроенными сведениями обновите информацию. Обычно для этого достаточно щелкнуть **Обновить (Refresh)** в текущем окне или нажать клавишу F5.

Включение дисковых квот на томах NTFS

Дисковые квоты создаются для тома и только на NTFS-томах. Лучше всего настраивать дисковые квоты в групповой политике, как описано в главе 3. После настройки соответствующих политик вы сможете создать записи дисковых квот для управления квотами на основе пользователей и групп.

Если вам проще настраивать квоты на каждом компьютере, включите дисковые квоты для NTFS-тома, выполнив следующие действия:

1. Откройте консоль Управление компьютером (Computer Management). По умолчанию вы подключены к локальному компьютеру. Для настройки дисковых квот на удаленном компьютере правой кнопкой щелкните узел **Управление компьютером (Computer Management)** и выберите команду **Подключиться к другому компьютеру (Connect To Another Computer)**. В диалоговом окне **Выбор компьютера (Select Computer)** выберите нужный компьютер.
2. В дереве консоли разверните узел **Запоминающие устройства (Storage)** и щелкните **Управление дисками (Disk Management)**. Настроенные на выбранном компьютере тома отображены в области сведений.

3. В графическом представлении или в списке томов щелкните правой кнопкой нужный том и выберите **Свойства (Properties)**.
4. Перейдите на вкладку **Квота (Quota)**, показанную на рис. 14-9. Установите флажок **Включить управление квотами (Enable Quota Management)**.

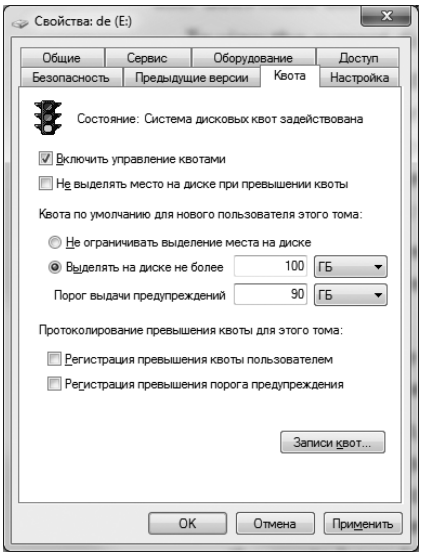

Рис. 14-9. Включите управление квотами и настройте предел и порог предупреждения квоты

5. Чтобы задать стандартный предел дисковой квоты, применяемый к каждому пользователю, установите переключатель **Выделять на диске не более (Limit Disk Space To)** и задайте значение предела в соответствующих полях. В поле **Порог выдачи предупреждений (Set Warning Level To)** задайте стандартный порог предупреждения. Порог предупреждения дисковой квоты, как правило, делают равным 90–95% от предела дисковой квоты.

Совет Стандартные пределы и пороги предупреждения применяются ко всем пользователям, но вы вольны настроить для пользователей индивидуальные пределы в диалоговом окне **Записи квот (Quota Entries)**. Чтобы не создавать повторно записи квоты на томе с точно такими же характеристиками и нагрузкой, вы можете экспортировать записи квоты и импортировать их на другом томе.

6. Чтобы принудительно применить предел дисковой квоты и запретить пользователям превышать его, установите флажок **Не выделять место на диске при превышении квоты (Deny Disk Space To Users Exceeding Quota Limit)**. Имейте в виду, что физическое ограничение при этом создается для пользователей, но не для администраторов.
7. Для регистрации превышения пользователями порога предупреждений или предела дисковой квоты установите флажки в разделе протоколирования.
8. Если система квот в данный момент не включена, вам будет предложено включить ее. По щелчку **OK**, будет выполнена повторная проверка тома и обновление статистики использования диска. В отношении пользователей,

превысивших текущий предел или порог предупреждения, будут приняты меры, включающие запрет на запись, уведомление пользователя при следующем обращении к тому и регистрация событий в журнале приложений.

Просмотр записей дисковой квоты

Наблюдение за использованием дискового пространства ведется для конкретного пользователя. При включенных дисковых квотах каждому пользователю, хранящему на диске данные, соответствует запись в файле дисковой квоты. Она периодически обновляется и отображает текущее использование дискового пространства, применимый предел квоты, применимый порог предупреждения и процент использования разрешенного пространства. Администратор имеет право изменять записи дисковой квоты, устанавливать различные пределы и пороги предупреждения для отдельных пользователей. Вы также вольны создать записи дисковой квоты для пользователей, которые еще не сохраняли данные на диске.

Чтобы просмотреть текущие записи дисковой квоты для тома, выполните следующие действия:

1. Откройте консоль Управление компьютером (Computer Management). По умолчанию вы подключены к локальному компьютеру. Для просмотра дисковых квот на удаленном компьютере, правой кнопкой щелкните узел **Управление компьютером (Computer Management)** и выберите команду **Подключиться к другому компьютеру (Connect To Another Computer)**. В диалоговом окне **Выбор компьютера (Select Computer)** выберите нужный компьютер.
2. В дереве консоли разверните узел **Запоминающие устройства (Storage)** и выберите **Управление дисками (Disk Management)**. Настроенные на выбранном компьютере тома отображены в области сведений.
3. В графическом представлении или в списке томов щелкните правой кнопкой нужный том и выберите **Свойства (Properties)**.
4. На вкладке **Квота (Quota)** щелкните кнопку **Записи квот (Quota Entries)**. В открывшемся диалоговом окне **Записи квот (Quota Entries)**, показанном на рис. 14-10, записи квоты упорядочены по состоянию. Состояние **OK** означает, что пользователь работает в пределах квоты. Любое другое состояние обычно означает, что пользователь достиг уровня предупреждения или предела квоты.

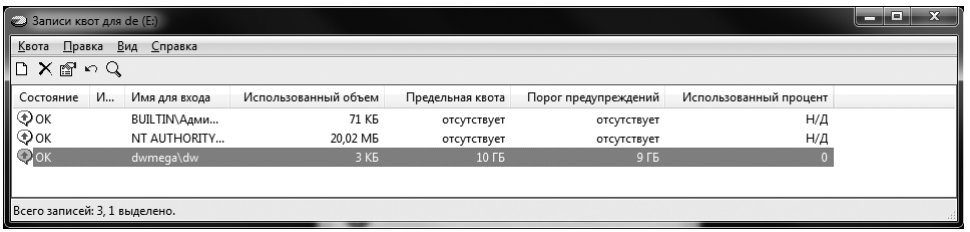

Рис.14-10. В записях дисковых квот содержатся сведения об использовании дискового пространства

Создание записей дисковой квоты

Записи дисковых квот можно создавать как для пользователей, которые еще не сохранили данные на томе, так и для пользователей, которые уже сохранили на томе данные. Это позволяет при необходимости задать для любого пользователя нестандартные пределы и пороги выдачи предупреждений. Обычно это нужно, если один пользователь часто сохраняет больше информации, чем другие. Графическому дизайнеру требуется куда больше места для хранения данных, чем, например, специалисту по работе с клиентами. Важно, что у вас есть возможность экспортировать пользовательские записи квот на другие тома, применив один и тот же набор правил к нескольким томам.

Чтобы создать запись квоты тома, выполните следующие действия:

1. В консоли Управление компьютером (Computer Management) разверните узел **Запоминающие устройства (Storage)** и выберите **Управление дисками (Disk Management)**. В графическом представлении или в списке томов щелкните правой кнопкой нужный том и выберите **Свойства (Properties)**.
2. На вкладке **Квота (Quota)** щелкните **Записи квот (Quota Entries)**. Чтобы обновить список записей квоты для всех пользователей, нажмите клавишу F5 или в меню **Вид (View)** выберите команду **Обновить (Refresh)**.
3. Если на томе нет записи нужного пользователя, создайте ее, выбрав в меню **Квота (Quota)** команду **Создать запись квоты (New Quota Entry)**.
4. В открывшемся диалоговом окне **Выбор: «Пользователи» (Select Users)** в поле **Введите имена выбираемых объектов (Enter The Object Names To Select)** введите имя пользователя и щелкните **Проверить имена (Check Names)**. При нескольких совпадениях выберите нужную учетную запись и щелкните **OK**. Если совпадения не найдены, попробуйте ввести имя заново и повторите поиск. При необходимости повторите этот шаг, затем щелкните **OK**.
5. После выбора имени выводится диалоговое окно **Добавление новой квоты (Add New Quota Entry)**. Дальше у вас есть несколько вариантов дальнейших действий. Чтобы удалить все ограничения для данного пользователя, установите переключатель **Не ограничивать выделение места на диске (Do Not Limit Disk Usage)**. Вы также вольны задать определенный предел и порог выдачи предупреждений, установив переключатель **Выделять на диске не более (Limit Disk Space To)** и заполнив соответствующие поля.
6. Щелкните **OK**. Закройте диалоговое окно **Записи квот (Quota Entries)**, а затем щелкните **OK** в диалоговом окне **Свойства (Properties)**.

Обновление и настройка записей дисковых квот

Чтобы изменить параметры записей дисковых квот для отдельных пользователей, выполните следующие действия:

1. В консоли Управление компьютером (Computer Management) разверните узел **Запоминающие устройства (Storage)** и выберите **Управление дисками (Disk Management)**. В графическом представлении или в списке томов щелкните правой кнопкой нужный том и выберите **Свойства (Properties)**.
2. На вкладке **Квота (Quota)** щелкните **Записи квот (Quota Entries)**.
3. Дважды щелкните запись квоты пользователя. Откроется диалоговое окно **Параметры квоты для (Quota Settings For)**.
4. Чтобы снять все ограничения для данного пользователя, установите переключатель **Не ограничивать выделение места на диске (Do Not Limit Disk Usage)**.
5. Чтобы изменить текущий предел и порог предупреждений, щелкните **Выделять на диске не более (Limit Disk Space To)** и введите нужные значения в соответствующие поля.
6. Щелкните **OK**.

Удаление записей дисковой квоты

Если пользователь больше не использует том, на котором для него создана запись квоты, эту запись можно удалить. При этом на экран будет выведен список всех файлов, которыми владеет пользователь. Вы можете удалить эти файлы, стать их владельцем или переместить файлы в папку на другом томе.

Для удаления записи дисковой квоты пользователя выполните следующие действия:

1. В консоли Управление компьютером (Computer Management) разверните узел **Запоминающие устройства (Storage)** и выберите **Управление дисками (Disk Management)**. В графическом представлении или в списке томов щелкните правой кнопкой нужный том и выберите **Свойства (Properties)**.
2. На вкладке **Квота (Quota)** щелкните **Записи квот (Quota Entries)**.
3. Выделите удаляемую запись квоты и нажмите клавишу Delete или выберите команду **Удалить запись квоты (Delete Quota Entry)** в меню **Квота (Quota)**. Вы можете выбрать несколько записей при помощи клавиш Ctrl или Shift.
4. Подтвердите удаление, щелкнув **Да (Yes)**. Откроется диалоговое окно **Дисковая квота (Disk Quota)** со списком файлов, владельцем которых является пользователь.
5. Просмотрите файлы пользователя, запись дисковой квоты которого вы намерены удалить, и укажите, как следует с ними поступить. Нужное действие можно выбрать для каждого файла в отдельности или для нескольких файлов, выделяя их при помощи клавиш Ctrl или Shift. Существуют такие возможности:

- **Отображать только папки (Show Folders Only)** Установите этот флажок, чтобы показать только папки, в которых находятся файлы пользователя. Это позволит удалить, переместить или стать владельцем всех файлов пользователя в папке.
- **Отображать только файлы (Show Files Only)** Установите этот флажок, чтобы показать файлы, которыми владеет пользователь.
- **Безвозвратно удалить файлы (Permanently Delete Files)** Выделите удаляемые файлы и щелкните **Удалить (Delete)**. Подтвердите действие, щелкнув **Да (Yes)**.
- **Стать владельцем файлов (Take Ownership Of Files)** Выделите файлы, владельцем которых хотите стать, и щелкните кнопку **Сменить владельца (Take Ownership)**.
- **Переместить в (Move Files To)** Выделите перемещаемые файлы, а затем введите в соответствующее поле путь к папке, расположенной на другом томе. Если вы не знаете точный путь, щелкните **Обзор (Browse)** для вывода диалогового окна **Обзор папок (Browse For Folder)**. Найдя папку, щелкните **Переместить (Move)**.

6. Завершив работу с файлами, щелкните **Закрыть (Close)**. Записи дисковых квот удаляются при условии выбора действия для всех файлов пользователя.

Экспорт и импорт параметров дисковых квот

Чтобы не создавать записи дисковых квот на нескольких идентичных томах, настройте параметры на одном томе, а затем экспортируйте их и импортируйте на другом томе. Оба тома должны быть отформатированы в формате NTFS. Для экспорта и импорта записей дисковых квот выполните следующие действия:

1. Откройте консоль Управление компьютером (Computer Management). По умолчанию вы подключены к локальному компьютеру. Для работы с дисковыми квотами на удаленном компьютере правой кнопкой щелкните узел **Управление компьютером (Computer Management)** и выберите команду **Подключиться к другому компьютеру (Connect To Another Computer)**. В диалоговом окне **Выбор компьютера (Select Computer)** выберите нужный компьютер.
2. В дереве консоли разверните узел **Запоминающие устройства (Storage)** и щелкните **Управление дисками (Disk Management)**. Настроенные на выбранном компьютере тома отображены в области сведений.
3. В графическом представлении или в списке томов щелкните правой кнопкой исходный том и выберите **Свойства (Properties)**.
4. На вкладке **Квота (Quota)** щелкните **Записи квот (Quota Entries)**.
5. В открывшемся диалоговом окне **Записи квот (Quota Entries)** выберите в меню **Квота (Quota)** команду **Экспорт (Export)**. В открывшемся диа-

логовом окне **Параметры экспорта квоты (Export Quota Settings)** выберите расположение, в котором нужно сохранить файл с параметрами квот. Введите имя файла в поле **Имя файла (File Name)** и щелкните **Сохранить (Save)**.

Совет Сразу сохранив файл параметров на диске, где их предполагается импортировать, вы сэкономите время. Файлы квот, как правило, довольно малы, поэтому расходом дискового пространства здесь можно пренебречь.

6. Выберите в меню **Квота (Quota)** команду **Закрыть (Close)**. Щелкните **OK**, чтобы закрыть диалоговое окно **Свойства (Properties)**.
7. В дереве консоли щелкните правой кнопкой узел **Управление компьютером (Computer Management)**. В контекстном меню выберите команду **Подключиться к другому компьютеру (Connect To Another Computer)**. В диалоговом окне **Выбор компьютера (Select Computer)** выберите компьютер, к тому которого нужно применить экспортируемые параметры.
8. Разверните узел **Запоминающие устройства (Storage)** и выберите **Управление дисками (Disk Management)**. В графическом представлении или в списке томов щелкните правой кнопкой целевой том и выберите **Свойства (Properties)**.
9. Перейдите на вкладку **Квота (Quota)** и убедитесь, что параметр **Включить управление квотами (Enable Quota Management)** включен. Затем щелкните **Записи квот (Quota Entries)**.
10. В открывшемся диалоговом окне **Записи квот (Quota Entries)** для целевого тома выберите в меню **Квота (Quota)** команду **Импорт (Import)**. В диалоговом окне **Параметры импорта квоты (Import Quota Settings)** выделите ранее сохраненный файл параметров квоты. Щелкните **Открыть (Open)**.
11. Если на томе есть записи квот, созданные ранее, вы можете заменить существующие записи или сохранить их. Щелкните **Да (Yes)**, чтобы заменить существующую запись, или **Нет (No)**, чтобы оставить существующую запись. Прежде чем щелкнуть **Да (Yes)** или **Нет (No)**, установите флажок **Применить ко всем записям квот (Do This For All Quota Entries)**, если хотите заменить или сохранить все существующие записи.

Отключение дисковых квот

Отключать квоты можно как для отдельных пользователей, так и для всех пользователей тома. При отключении квот для отдельного пользователя он перестает быть объектом регулирования квот, но наблюдение за дисковыми квотами для других пользователей продолжается. При отключении квот для тома наблюдение за квотами прекращается полностью. Отключение квоты для отдельного пользователя описано ранее в разделе «Обновление и настройка записей дисковых квот». Чтобы отключить квоты для тома, выполните следующие действия:

1. Откройте консоль Управление компьютером (Computer Management). Для отключения дисковых квот на удаленном компьютере правой кнопкой щелкните узел **Управление компьютером (Computer Management)** и выберите команду **Подключиться к другому компьютеру (Connect To Another Computer)**. В диалоговом окне **Выбор компьютера (Select Computer)** выберите нужный компьютер.
2. В дереве консоли разверните узел **Запоминающие устройства (Storage)** и щелкните **Управление дисками (Disk Management)**. Тома, настроенные на выбранном компьютере, отображены в области сведений.
3. В графическом представлении или в списке томов щелкните правой кнопкой том и выберите **Свойства (Properties)**.
4. На вкладке **Квота (Quota)** сбросьте флажок **Включить управление квотами (Enable Quota Management)**. Щелкните **OK**. Подтвердите действие, щелкнув **OK**.

Кеширование филиалов

Функция Windows BranchCache предназначена для кеширования файлов и работает в паре с фоновой интеллектуальной службой передачи (BITS). Включив функцию кеширования филиалов в доменной среде, администраторы удаленного офиса дают компьютерам под управлением Windows 7 или последующих версий возможность извлекать документы и другие файлы из локального кеша, а не с удаленных серверов.

Функция кеширования филиалов работает с файлами, переданными по протоколам HTTP и SMB. Это означает, что в кеш записываются файлы, переданные как с веб-серверов интрасети, так и с внутренних файл-серверов. Кеширование значительно сокращает время отклика и время передачи документов, веб-страниц и данных мультимедиа.

Включить кеширование филиалов можно во всех удаленных офисах компании. В целом, работа данной функции определяется границами локальной вычислительной сети (ЛВС). Если ЛВС подключена к центральному офису через соединение, в котором время задержки превышает 80 мс, клиенты ЛВС по возможности будут использовать локальный кеш. Отметим, что несколько локальных сетей, подключенных друг к другу через быстрое соединение, также могут использовать единый локальный кеш.

После включения функции кеширования филиалов при первом обращении к файлу на веб-узле интрасети или сетевом файловом сервере файл передается с сервера-источника и записывается в локальный кеш удаленного офиса. При последующем обращении к файлу того же или другого пользователя удаленного офиса поиск файла проводится в локальном кеше. Если файл найден, на сервер-источник посылается запрос с целью выяснить, был ли файл изменен со времени записи в кеш. Если файл не изменялся, он извлекается из локального кеша, без использования сетевого соединения. Если файл был изменен, он извлекается с сервера-источника, а копия файла, находящаяся в кеше, обновляется.

Существует два режима кеширования филиалов:

- **Распределенный кеш (Distributed cache)** В этом режиме кешированные файлы хранятся на компьютерах пользователей под управлением Windows 7 или более поздних версий. При этом сервер в удаленном офисе не нужен, поскольку кешировать и рассылать файлы способен каждый локальный компьютер.
- **Размещенный кеш (Host cache)** В этом режиме локальный файловый кеш находится на сервере под управлением Windows Server 2008 R2 (или более поздней версии), установленном в удаленном офисе. Файлы записываются в кеш на сервере и отсылаются клиентам, расположенным в локальном офисе.

Безусловно, у обоих режимов работы кеша имеются свои преимущества и недостатки. В режиме распределенного кеша не требуется устанавливать в филиале сервер. Вместе с тем, возрастает нагрузка на компьютеры пользователей, которые должны обслуживать кеш и распределять файлы, что может отрицательно сказаться на производительности. В режиме размещенного кеша вы должны установить в удаленном офисе сервер. Зато после его установки обслуживание кеша будет выполняться на сервере без дополнительной нагрузки на компьютеры пользователей.

Помните о следующем:

- Функция кеширования филиалов не мешает пользователям сохранять файлы локально. Она работает с запросами на чтение, например, когда пользователь запрашивает файл на файловом сервере.
- Кеширование филиалов способно работать совместно с функцией шифрования и технологиями безопасной передачи, подобными подписыванию SMB (SMB Signing) и IPSec.
- По умолчанию сетевые файлы кешируются в удаленном офисе, только если время задержки сети превышает 80 мс.
- Кеширование филиалов не нужно специально включать в центральном офисе. Оно целиком управляется из филиала.

Чтобы включить кеширование филиалов, выполните следующие действия:

1. В редакторе групповой политики откройте для редактирования нужный объект GPO. Разверните узел **Конфигурация компьютера\Административные шаблоны\Сеть\BranchCache (Computer Configuration\Administrative Templates\Network\BranchCache)**.
2. Дважды щелкните параметр **Включить BranchCache (Turn On BranchCache)**. В диалоговом окне **Свойства (Properties)** установите переключатель **Включить (Enabled)** и щелкните **OK**.
3. Выполните одно из следующих действий:
   - Для включения распределенного кеширования филиалов дважды щелкните параметр **Включить режим распределенного кэша BranchCache (Set BranchCache Distributed Cache Mode)**. В диалоговом

окне **Свойства (Properties)** установите переключатель **Включить (Enabled)** и щелкните **OK**.

- Для включения размещенного кеширования филиалов дважды щелкните параметр **Включить режим размещенного кэша BranchCache (Set BranchCache Hosted Cache Mode)**. В диалоговом окне **Свойства (Properties)** установите переключатель **Включить (Enabled)**, введите в соответствующее поле хост-имя сервера кеша и щелкните **OK**.

4. Если вы хотите задать собственное значение задержки сети, при котором включается кеширование, дважды щелкните параметр **Настройка BranchCache для сетевых файлов (Configure BranchCache For Network Files)**. В диалоговом окне **Свойства (Properties)** установите переключатель **Включить (Enabled)**. В соответствующее поле введите время задержки сети, при превышении которого сетевые файлы должны записываться в кеш. Значение указывается в миллисекундах. При значении 0 файлы кешируются всегда.
5. Если вы включили размещенное кеширование филиалов, дважды щелкните параметр **Установить процент дискового пространства, используемого для кэша клиентского компьютера (Set percentage of disk space used for client computer cache)**. В диалоговом окне **Свойства (Properties)** установите переключатель **Включить (Enabled)**. В соответствующее поле введите процент от общего дискового пространства клиентских компьютеров, которое следует выделять для работы BranchCache. Щелкните **OK**. По умолчанию наибольший размер кеша составляет 5% от общего дискового пространства.

Оптимизировать кеширование филиалов позволяют две политики:

- **Запретить клиенту BITS использование кэша филиалов Windows (Do Not Allow The BITS Client To Use Windows BranchCache)** Политика находится в узле **Конфигурация компьютера\Административные шаблоны\Сеть\Фоновая интеллектуальная служба передачи (Computer Configuration\Administrative Templates\Network\Background Intelligent Transfer Service)**. В ней определена возможность использования функции кеширования филиалов клиентом BITS для фоновой передачи. В большинстве случаев следует разрешить клиенту BITS записывать и извлекать файлы из кеша. Но среди этих файлов будут файлы ОС и других типов, передаваемые посредством BITS, что может привести к росту кеша и дополнительной нагрузке на компьютеры.
- **Публикация хэша для службы BranchCache (Hash Publication For BranchCache)** Политика находится в узле **Конфигурация компьютера\Административные шаблоны\Сеть\Сервер Lanman (Computer Configuration\Administrative Templates\Network\Lanman Server)**. В ней задаются возможность и способ создания функцией BranchCache цифрового хеша для кешируемых файлов. По умолчанию цифровой хеш создается, позволяя клиентам быстро определять соответствие кешированного файла файлу на сервере.

Глава 15

Настройка и диагностика сетей TCP/IP

В этой главе мы обратимся к управлению сетевыми проводными и беспроводными подключениями. Для правильной работы сети вы должны установить сетевые компоненты и настроить сетевое взаимодействие с использованием протоколов DHCP, DNS и WINS. Протокол DHCP предназначен для динамической настройки IP-адреса и других параметров подключения к сети. Протоколы DNS и WINS нужны для разрешения имен, причем предпочтительным является использование DNS, а WINS поддерживается для обеспечения обратной совместимости с ранними выпусками ОС Windows.

Обзор сетевых возможностей Windows 7

По своим сетевым возможностям Windows 7 отличается от Windows XP и предыдущих версий Windows. Обновленный набор сетевых средств Windows 7 включает:

- **Сетевой проводник (Network Explorer)** Централизованная консоль для обзора компьютеров и устройств сети.
- **Центр управления сетями и общим доступом (Network And Sharing Center)** Централизованная консоль для просмотра и управления конфигурацией сетевых подключений и параметрами общего доступа компьютера.
- **Карта сети (Network Map)** Карта сети, отображающая способы подключения компьютеров и устройств.
- **Диагностика сетей (Network Diagnostics)** Автоматизированный инструмент для диагностики, помогающий при устранении сетевых неполадок.

Прежде чем перейти к обсуждению работы с перечисленными сетевыми инструментами, отметим компоненты Windows 7, которые применяются в этих инструментах:

- **Сетевое обнаружение (Network discovery)** Возможность видеть другие компьютеры и устройства сети.
- **Служба сведений о подключенных сетях (Network awareness)** Создание отчетов об изменениях в сети.

Сетевое обнаружение и категории сетей

Компьютеры и устройства, доступные для просмотра в сетевых инструментах Windows 7, определяются параметрами сетевого обнаружения вашего компьютера. Эти параметры вкупе с параметрами брандмауэра Windows (Windows Firewall) призваны заблокировать или разрешить следующие действия:

- обнаружение компьютеров и устройств в сети;
- обнаружение вашего компьютера другими компьютерами.

Параметры сетевого обнаружения обеспечивают надлежащий уровень безопасности для каждого типа сети, к которой подключен компьютер. Сети делятся на следующие категории:

- **Доменная (Domain)** Сеть, в которой компьютеры являются членами корпоративного домена.
- **Рабочая (Work)** Сети, компьютеры которой являются членами рабочей группы.
- **Домашняя (Home)** Сеть, компьютеры которой являются членами домашней группы и не имеют прямого выхода в Интернет.
- **Общественная (Public)** Сеть в общественном месте, например в кафе или аэропорту.

Примечание По умолчанию функции сетевого обнаружения и общего доступа к файлам отключены, но их можно включить в доменных, рабочих и домашних сетях. Включение выполняется в консоли Центре управления сетями и общим доступом (Network And Sharing Center), в окне **Сеть (Network)** или **Дополнительные параметры общего доступа (Advanced Sharing Settings)**. При этом вы сократите число ограничений и позволите компьютерам сети обнаруживать другие компьютеры и устройства в этой сети, а также совместно использовать файлы. В общественных сетях обнаружение и общий доступ к файлам заблокированы. Запрет на обнаружение других компьютеров и устройств укрепляет безопасность. При отключенном сетевом обнаружении и общем доступе блокируется доступ из сети к файлам и принтерам. Кроме того, к сети не смогут подключиться некоторые программы.

На компьютере настройки для каждой категории сетей хранятся отдельно. Поэтому для каждой категории параметры блокировки и разрешения сетевого трафика могут быть разными. При первом подключении компьютера к конкретной сети открывается диалоговое окно, в котором вы можете указать свое местонахождение — дома, на работе или в общественном месте. От вашего выбора зависит определение категории сети. При изменении сетевого подключения или подключении к другой сети предпринимается попытка автоматического определения категории сети. Если средствами Windows 7 категорию сети определить не удается, сеть считается общественной. После присоединения компьютера к домену сеть, к которой подключен компьютер, считается рабочей.

В зависимости от категории сети сетевое обнаружение либо включается, либо отключается. Включенное сетевое обнаружение означает, что компью-

тер может обнаруживать другие компьютеры и устройства сети и что другие устройства и компьютеры в сети могут обнаруживать этот компьютер. Отключение сетевого обнаружения означает, что компьютер не может обнаруживать другие компьютеры и устройства в сети, а другие устройства и компьютеры в сети не могут обнаруживать этот компьютер.

Сетевой проводник (Network Explorer)

В программе Сетевой проводник (Network Explorer) отображается список обнаруженных в сети компьютеров и устройств. Чтобы открыть Сетевой проводник (Network Explorer), выберите в меню **Пуск (Start)** команду **Сеть (Network)**. Если вы не добавили команду **Сеть (Network)** в меню **Пуск (Start)**, откройте **Сетевой проводник (Network Explorer)** при помощи панели управления. Откройте панель управления и щелкните категорию **Сеть и Интернет (Network And Internet)**. Затем щелкните ссылку **Просмотр сетевых компьютеров и устройств (View Network Computers And Devices)**.

Список отображаемых в сетевом проводнике компьютеров и устройств определяется параметрами сетевого обнаружения компьютера. Если обнаружение включено, вы увидите другие компьютеры сети (рис. 15-1). Если обнаружение отключено, в области уведомлений программы Сетевой проводник (Network Explorer) появится предупреждение об этом, как показано на рис. 15-2. Чтобы включить сетевое обнаружение, щелкните это предупреждение и выберите команду **Включить сетевое обнаружение (Turn On Network Discovery)**. При этом будут открыты соответствующие порты брандмауэра Windows (Windows Firewall). Если в отношении сетевого обнаружения больше не предпринимать никаких шагов, компьютер сможет только обнаруживать другие компьютеры. Общий доступ к принтерам, файлам и мультимедиа придется настраивать вручную, как описано в главе 13.

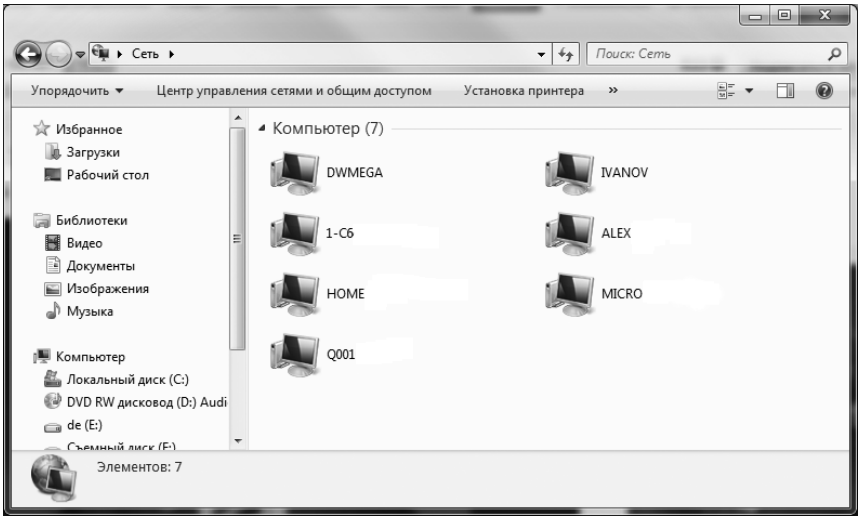

Рис. 15-1. Сетевой проводник (Network Explorer): сетевое обнаружение включено

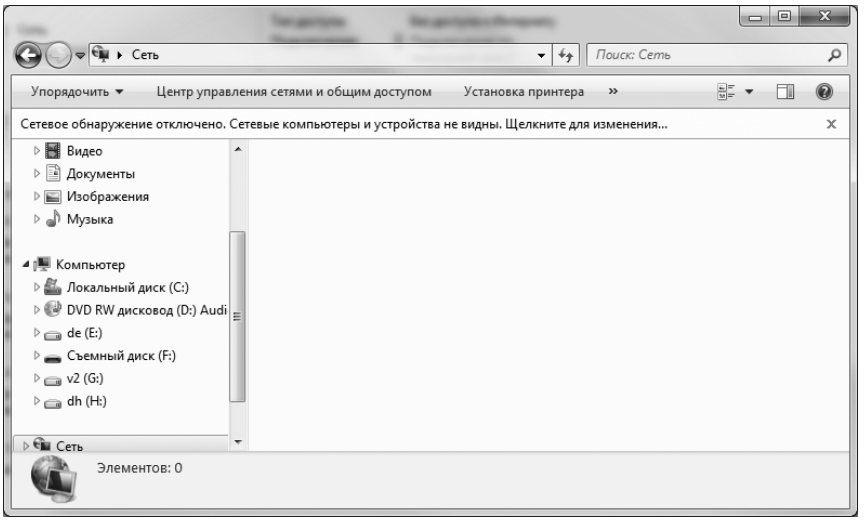

Рис. 15-2. Если сетевое обнаружение выключено, для просмотра других компьютеров и устройств потребуется ее включить

Если у вас есть соответствующие разрешения, вы сможете найти любой компьютер или устройство из списка сетевого проводника. Чтобы открыть общие ресурсы компьютера, дважды щелкните его значок. Для управления интерфейсом и ресурсами устройства дважды щелкните значок устройства.

На панели инструментов Сетевого проводника (Network Explorer) имеются следующие кнопки:

- **Центр управления сетями и общим доступом (Network And Sharing Center)** Щелкните эту кнопку, чтобы просмотреть состояние сети или управлять ее параметрами. Подробнее — в следующем разделе.
- **Установка принтера (Add A Printer)** Запуск мастера Установка принтера (Add Printer), который поможет добавить локальный, сетевой, беспроводной принтеры или принтер Bluetooth.
- **Добавить беспроводное устройство (Add A Wireless Device)** Запуск Мастера добавления устройства (Add A Device), который позволяет добавить обнаруженные, но не настроенные беспроводные устройства.

Центр управления сетями и общим доступом

В окне Центр управления сетями и общим доступом (Network And Sharing Center) вы найдете сведения о текущем состоянии сети, а также обзор текущей конфигурации сети (рис.15-3). Чтобы открыть Центр управления сетями и общим доступом (Network And Sharing Center), откройте панель управления, щелкните категорию **Сеть и Интернет (Network And Internet)**, а затем щелкните **Центр управления сетями и общим доступом (Network And Sharing Center)**.

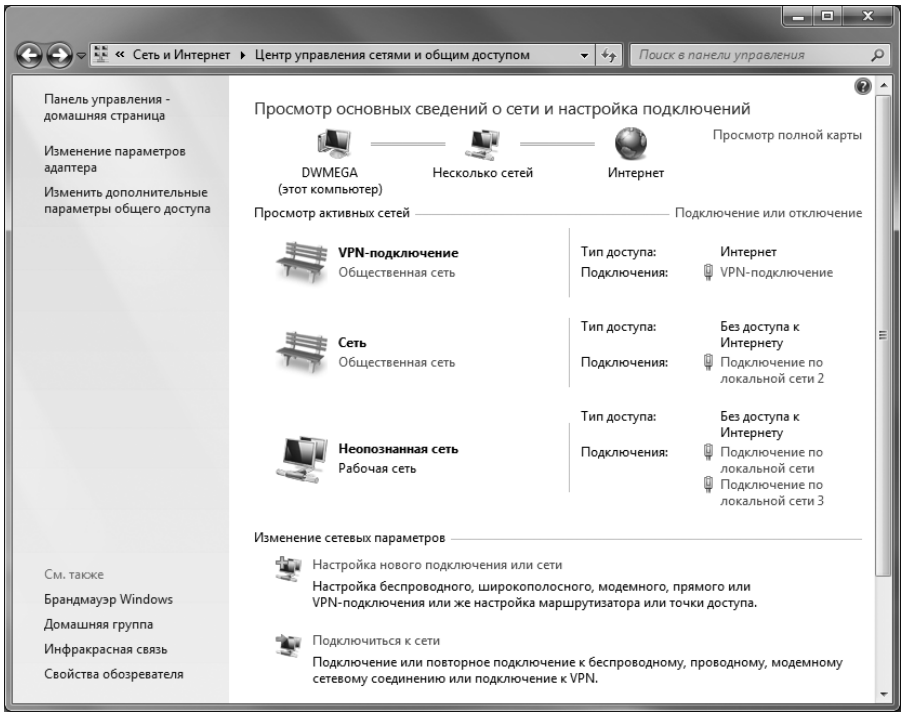

Рис. 15-3. Просмотр состояния и конфигурации сети

Центр управления сетями и общим доступом (Network And Sharing Center) разделен на четыре основные области:

- **Карта сети** Графическое отображение конфигурации сети и сетевых подключений. Нормальному состоянию соответствует линия, соединяющая различные сегменты сети. Любые проблемы с конфигурацией сети или подключениями отображаются значками предупреждения. Желтый значок указывает на возможную неполадку конфигурации. Красный крестик свидетельствует об отсутствии подключения к отдельному сегменту сети. На рис. 15-3 компьютер подключен к сети и Интернету. Если перейти по ссылке **Просмотр полной карты (See Full Map)**, откроется окно **Карта сети (Network Map)** с расширенным представлением сети, описанным далее.
- **Активные сети** Список имен текущих активных сетей. Имена сетей выделены жирным шрифтом справа от значка сети. Если дважды щелкнуть значок сети, можно задать ее имя и изменить значок. Ссылка под значком сети обозначает ее категорию: Рабочая сеть (Work Network), Домашняя сеть (Home Network) или Общественная сеть (Public Network). Перейдя по ссылке, можно изменить тип сетевого расположения.
- **Тип доступа** Способ и описание подключения компьютера к текущей сети. Если компьютер не имеет выхода в Интернет, в качестве типа доступа указанной **Без доступа к Интернету (No Internet Access)**. В поле

Подключения (Connections) показаны имена подключений, используемых для подключения к активным сетям. Если щелкнуть подключение, откроется диалоговое окно с информацией о его состоянии.

- **Параметры сети** Инструменты для настройки сетевых параметров компьютера. Чтобы настроить общий доступ, щелкните ссылку **Изменить дополнительные параметры общего доступа (Change Advanced Sharing Settings)**. В окне **Дополнительные параметры общего доступа (Advanced Sharing Settings)** для включения или отключения сетевого обнаружения щелкните переключатель **Включить сетевое обнаружение (Turn On Network Discovery)** или **Отключить сетевое обнаружение (Turn Off Network Discovery)**. Затем щелкните **Сохранить изменения (Save Changes)**.

В Центре управления сетями и общим доступом (Network And Sharing Center) можно попытаться установить причину вывода предупреждения. Откройте инструмент Диагностика сетей Windows (Windows Network Diagnostics), щелкнув значок предупреждения. После этого будет предпринята попытка определить причину сбоя и предложено возможное решение.

Карта сети

Если отображение сети разрешено групповой политикой и включено, карта сети (рис.15-4) представляет собой расширенное графическое отображение сетевой конфигурации и подключений. Чтобы открыть окно **Карта сети (Network Map)**, выполните следующие действия:

1. В окне панели управления последовательно щелкните **Сеть и Интернет (Network And Internet)** и **Центр управления сетями и общим доступом (Network And Sharing Center)**.

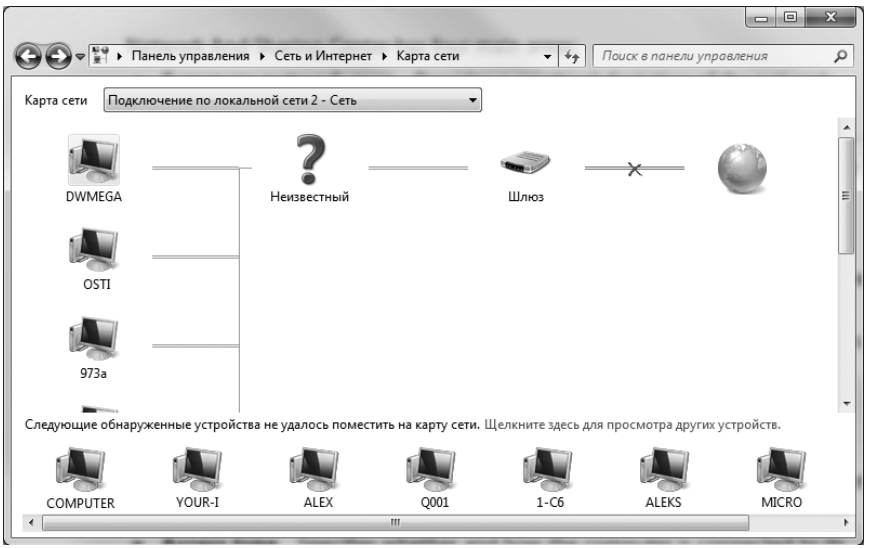

Рис. 15-4. Карта сети (Network Map) — расширенное представление сети

2. В Центре управления сетями и общим доступом (Network And Sharing Center) щелкните ссылку **Просмотр полной карты (See Full Map)**.

Примечание На компьютерах под управлением Windows 7 в стандартной конфигурации создается краткая карта сети, как и в Центре управления сетями и общим доступом (Network And Sharing Center). Более подробная карта доступна при условии, что включено сетевое обнаружение и вывод карты сети разрешен в групповой политике.

Компьютеры и устройства, которые обнаружены и могут быть нанесены на карту, соединены линиями, изображающими подключения. Компьютеры и устройства, которые обнаружены, но не могут быть нанесены на карту, перечислены внизу страницы.

Все проблемы с конфигурацией сети или подключениями отображены на сетевой карте значками предупреждений. Желтый значок указывает на возможную неполадку конфигурации. Красный крестик свидетельствует об отсутствии подключения к отдельному сегменту сети. Щелкнув значок, вы запустите инструмент Диагностика сетей Windows (Windows Network Diagnostics), который попытается определить причину сетевой неполадки и предложит возможное решение.

Ближе к реальности В некоторых ситуациях карта сети весьма полезна. Но для ее создания вы должны разрешить обнаружение во внутренней сети организации. Это фактор риска, поэтому сетевое сопоставление в групповой политике по умолчанию отключено. Параметры групповой политики, в которых определяется сетевое сопоставление, находятся в узле **Конфигурация компьютера\Административные шаблоны\Сеть\Обнаружение топологии связи (Link-Layer) (Computer Configuration\ Administrative Templates\Network\Link-Layer Topology Discovery)**. Чтобы компьютер мог обнаруживать другие компьютеры и отображать их на карте, в примененном к компьютеру объекте GPO должен быть включен параметр **Включает драйвер отображения ввода-вывода (Turn On Mapper I/O (LLTDIO) Driver)**. Чтобы компьютер мог обнаруживаться другими компьютерами, в примененном к компьютеру объекте GPO должен быть включен параметр **Включить драйвер «Ответчика» (Turn On Responder (RSPNDR) Driver)**.

Включив любой или оба из этих параметров, уточните их работу. В большинстве случаев параметры настраивают так, чтобы разрешить действие в домене и запретить действие при подключении к частной сети. В публичной сети действие разрешают только в исключительных случаях — для конкретного компьютера, который необходимо отобразить на карте.

Установка сетевых компонентов

Чтобы настроить сетевое подключение, необходимо установить сетевой адаптер и задать параметры TCP/IP. В Windows 7 протокол TCP/IP используется в качестве стандартного протокола сетей WAN. Компоненты сети обычно устанавливаются во время установки Windows 7. Кроме того, TCP/IP-сеть можно настроить посредством свойств подключения по локальной сети.

TCP/IP и двойной стек IP

Протоколы TCP и IP позволяют компьютерам, находящимся в разных сетях и в Интернете, взаимодействовать при помощи сетевых адаптеров: подключаемых через USB-порт, адаптеров на базе PC Card, внутренних плат или встроенных адаптеров на материнской плате. В Windows 7 применена двойная архитектура IP, в которой реализованы обе версии протокола — версия 4 (IPv4) и версия 6 (IPv6), — использующие общие транспортный и канальный уровни.

Различия между IPv4 и IPv6 весьма значительны. Протокол IPv4 с 32-разрядной адресацией и по сей день является основным протоколом IP, применяющимся в большинстве сетей, включая Интернет. Протокол IPv6 со 128-разрядной адресацией представляет собой следующее поколение протоколов IP.

Обычно 32-разрядные адреса IPv4 выражаются четырьмя отдельными десятичными значениями, например 127.0.0.1 или 192.168.1.20. Четыре десятичных значения называются *октетами*, так как каждый из них представляет 8 бит 32-разрядного числа. В стандартных IPv4-адресах для одноадресной рассылки часть IP-адреса представляет собой идентификатор сети, а другая часть — идентификатор узла. Размеры двух частей могут меняться. Связи между IPv4-адресом узла и MAC-адресом его сетевого адаптера не существует.

Адреса IPv6 состоят из 128 разрядов и разделены на 16-разрядные блоки, отделяемые двоеточием. Каждый 16-разрядный блок выражен в шестнадцатеричной форме. В стандартных IPv6-адресах одноадресной рассылки первые 64 бита представляют идентификатор сети, а последние 64 бита — сетевой интерфейс. Вот пример IPv6-адреса:

```
FEC0:0:0:02BC:FF:BECB:FE4F:961D
```

Поскольку многие блоки IPv6-адреса имеют значение 0, для сокращения записи последовательный набор нулевых блоков обозначают двойным двоеточием «::». Применение этой формы записи к предыдущему адресу дает следующий вариант:

```
FEC0::02BC:FF:BECB:FE4F:961D
```

Если встречается три или более нулевых блоков, они сокращаются точно так же. Например адрес FFE8:0:0:0:0:0:0:1 сокращается до FFE8::1.

Во время установки ОС при обнаружении сетевого оборудования по умолчанию включаются оба протокола (IPv4 и IPv6), и устанавливать отдельный компонент для поддержки IPv6 не нужно. Модифицированная архитектура IP в Windows 7 называется *стеком TCP/IP следующего поколения* (Next Generation TCP/IP stack). В табл. 15-1 приведены ключевые усовершенствования TCP/IP, реализованные в стеке TCP/IP следующего поколения. В табл. 15-2 содержатся ключевые усовершенствования TCP/IP, присущие IPv6.

Табл. 15-1. Ключевые изменения TCP/IP, реализованные в стеке TCP/IP следующего поколения

Поддерживаемая функция	Описание
Автоматическое обнаружение маршрутизаторов типа «черная дыра»	Препятствует закрытию подключения TCP, когда промежуточные маршрутизаторы без объяснения отбрасывают крупные TCP-сегменты, повторные передачи и сообщения об ошибках
Автоматический повторный вызов неработающего шлюза	Периодическая проверка недоступного шлюза на предмет его доступности
Алгоритм контроля перегрузки (Compound TCP)	Оптимизация передач TCP с узла-отправителя путем увеличения объема отправляемых данных, при условии что это не мешает другим TCP-подключениям
Расширенные выборочные подтверждения	Более широкое применение выборочных подтверждений (Selective Acknowledgment, SACK), позволяющее получателю указывать до четырех непоследовательных блоков принятых данных и информировать о повторяющихся пакетах. Благодаря этому получатель выявляет ошибочную повторную передачу сегмента и корректирует поведение для предотвращения повторной передачи в будущем
Модернизированный алгоритм быстрого восстановления	Повышение пропускной способности за счет изменения отправителем способа повышения скорости отправки при потере нескольких сегментов в окне данных, когда отправителю сообщается, что успешно получена была только часть данных
Обнаружение недоступности соседнего узла для IPv4	Когда соседние узлы становятся недоступными, это состояние обнаруживается и создается отчет
Инфраструктура диагностики сети	Расширяемая инфраструктура для диагностики неполадок сетевых подключений и их восстановления
Автоматическая настройка окна приема	Оптимизация передачи TCP для узла, принимающего данные, путем автоматического управления размером буфера памяти (принимающего окна), используемого для хранения входящих данных, в зависимости от текущих условий в сети
Сегменты маршрутизации	Предотвращение нежелательной пересылки трафика между интерфейсами путем привязки интерфейса или набора интерфейсов к сеансу входа в систему с собственными таблицами маршрутизации
Восстановление потерь на основе выборочных подтверждений	Использование выборочных подтверждений для восстановления потерь при получении повторяющегося подтверждения, а также для быстрого восстановления в случаях, когда приемник не получил несколько сегментов

Табл. 15-1. (*окончание*)

Поддерживаемая функция	Описание
Обнаружение фиктивного таймаута повторной отправки	Исправление внезапного временного увеличения таймаута при повторной отправке и предотвращение ненужной повторной отправки сегментов
Расширенная статистика TCP	Помогает установить причину снижения производительности подключения: отправляющее приложение, получающее приложение или сеть
Платформа фильтрации Windows	Интерфейсы API для расширения архитектуры фильтрации TCP/IP и поддержки новых функциональных возможностей

Табл. 15-2. Ключевые усовершенствования TCP/IP для IPv6

Поддерживаемая функция	Описание
Клиент DHCP, совместимый с DHCPv6	Расширение DHCP-клиента с поддержкой IPv6. Предназначено для автоматического конфигурирования адреса с DHCPv6-сервером в режиме с сохранением информации о состоянии
IP-безопасность	Позволяет использовать обмен ключам в Интернете (In-ternet Key Exchange, IKE) и шифрование данных для IPv6
IPv6 поверх PPP (PPPv6)	Разрешение пересылки собственного трафика IPv6 через PPP-подключения, что, в свою очередь, позволяет клиентам удаленного доступа подключаться к поставщикам Интернета, работающим по протоколу IPv6, через подключение удаленного доступа или PPPoE
Локальное разрешение группового имени (LLMNR)	Узлы IPv6, находящиеся в одной подсети без DNS-сервера, способны разрешать имена друг друга
Обнаружение многоадресного прослушивателя версия 2 (MLDv2)	Поддержка многоадресного трафика, зависящего от источника. Эквивалент протокола IGMPv3 для IPv4
Случайный идентификатор интерфейса	Предотвращает сканирование IPv6-адресов по известным идентификаторам производителей сетевых адаптеров для компании. По умолчанию для постоянных автоматически назначаемых IPv6-адресов, включая публичные и локальные адреса, в Windows 7 создаются случайные идентификаторы интерфейсов
Симметричные трансляторы сетевых адресов	Сопоставление внутреннего (частного) адреса и номера порта нескольким внешним (публичным) адресам и портам в зависимости от внешнего адреса получателя

Установка сетевого адаптера

Сетевой адаптер — это устройство для передачи и приема данных по сети. Для установки и настройки сетевого адаптера выполните следующие действия:

1. Выполните инструкции производителя по установке. Например, при установке может понадобиться запуск ПО производителя, чтобы изменить параметры прерывания и порта адаптера.
2. При установке внутренней сетевой платы выключите компьютер, отсоедините питание и установите плату адаптера в соответствующий слот. По завершению подключите питание и включите компьютер.
3. Во время запуска Windows 7 новый адаптер, как правило, обнаруживается автоматически. Если у вас есть диск с драйверами для адаптера, вставьте его в дисковод.
4. Если адаптер не обнаружен автоматически, следуйте инструкции по установке устройств (см. главу 8).
5. Если в системе не установлены сетевые службы, установите их, как описано в следующем разделе.

Установка сетевых служб TCP/IP

Если установка стека протоколов TCP/IP выполняется после установки Windows 7, войдите на компьютер с учетной записью администратора и выполните следующие действия:

1. В панели управления последовательно щелкните **Сеть и Интернет (Network And Internet)** и **Центр управления сетями и общим доступом (Network And Sharing Center)**.
2. В Центре управления сетями и общим доступом (Network And Sharing Center) в разделе **Просмотр активных сетей (View Your Active Networks)** перейдите по ссылке, соответствующей нужному сетевому подключению.

Совет Если нужное подключение неактивно, щелкните ссылку **Подключиться к сети (Connect To A Network)**. В окне сетевых подключений щелкните правой кнопкой нужное подключение и выберите **Свойства (Properties)**.

3. В диалоговом окне **Состояние (Status)** щелкните **Свойства (Properties)**. На рис. 15-5 показано диалоговое окно свойств подключения, открывшееся на вкладке **Сеть (Networking)**.
4. Если в списке установленных компонентов отсутствуют записи **Протокол Интернета версии 6 (Internet Protocol Version 6)** или **Протокол Интернета версии 4 (Internet Protocol Version 4)**, их нужно установить вручную. Последовательно щелкните кнопку **Установить (Install)**, элемент **Протокол (Protocol)** и кнопку **Добавить (Add)**. В диалоговом окне **Выбор сетевого протокола (Select Network Protocol)** выделите устанавливаемый протокол и щелкните **OK**. Для установки обоих протоколов (TCP/IPv6 и TCP/IPv4) повторите эти действия.

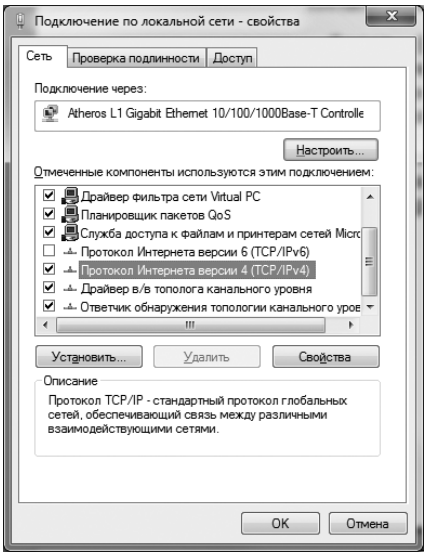

Рис. 15-5. Настройка параметров TCP/IP

5. В диалоговом окне свойств подключения установите флажок нужного протокола, если он еще не установлен. Щелкните **OK**.
6. При необходимости настройте подключение по локальной сети, как описано в следующем разделе.

Настройка подключения по локальной сети

Подключение по локальной сети создается автоматически, если на компьютере установлен сетевой адаптер и компьютер подключен к сети. Если на компьютере установлено несколько сетевых адаптеров и компьютер подключен к сети, подключение по локальной сети создается для каждого адаптера. Если сетевое подключение недоступно, следует подключить компьютер к сети или создать подключения другого типа, как описано в разделе «Управление локальными сетевыми подключениями» далее в этой главе.

Для связи между компьютерами по протоколам TCP/IP используются IP-адреса. В Windows 7 имеются следующие способы настройки IP-адресов:

- **Ручная настройка** IP-адреса, назначаемые вручную, называются *статическими* (static). Статические IP-адреса фиксированы и не изменяются, пока вы специально не измените их. Обычно статические IP-адреса назначаются серверам Windows. При этом, чтобы сервер мог просматривать объекты сети, нужно настроить дополнительные параметры.
- **Динамическая настройка** *Динамические* (dynamic) IP-адреса назначаются DHCP-сервером (если он установлен в сети) во время запуска компьютера. Со временем адреса могут меняться. Динамическая IP-адресация является стандартной конфигурацией.

- **Альтернативно (только IPv4)** Если компьютер с Windows 7 настроен на использование DHCPv4-сервера, но он недоступен, компьютеру автоматически назначается альтернативный закрытый IP-адрес. По умолчанию он выделяется из диапазона от 169.254.0.1 до 169.254.255.254 с маской подсети 255.255.0.0. Вы также можете указать пользовательский альтернативный IPv4-адрес, что особенно удобно для пользователей ноутбуков.

Настройка статических IP-адресов

Настройка статического IP-адреса состоит в назначении компьютеру собственно IP-адреса, маски подсети для данного IP-адреса и, при необходимости, адреса основного шлюза, используемого для межсетевого взаимодействия. IP-адрес представляет собой числовой идентификатор компьютера. Схема IP-адресации зависит от конфигурации сети, но, как правило, IP-адреса назначаются для отдельных сетевых сегментов.

Как уже говорилось, IPv6-адреса сильно отличаются от IPv4-адресов. В IPv6-адресах первые 64 бита идентифицируют сеть, а оставшиеся 64 бита — сетевой интерфейс. В IPv4 некоторое количество начальных битов обозначает сеть, а оставшиеся биты идентифицируют узел. Например, в IPv4-адресе компьютера, находящегося в сегменте сети 10.0.10.0 с маской подсети 255.255.255.0, три первых октета указывают на сеть с уникальным идентификатором 10.0.10.0. Адреса можно назначать в диапазоне от 10.0.10.1 до 10.0.10.254. Адрес 10.0.10.255 зарезервирован для широковещательных рассылок.

Если вы находитесь в частной сети, не имеющей прямого подключения к Интернету, следует использовать частные IPv4-адреса. В табл. 15-3 содержится список IPv4-адресов для частной сети.

Табл. 15-3. Адресация IPv4 в частной сети

Идентификатор сети	Маска подсети	Диапазон допустимых IP-адресов	Широковещательный адрес
10.0.0.0	255.0.0.0	10.0.0.0–10.255.255.254	10.255.255.255
172.16.0.0	255.240.0.0	172.16.0.0–172.31.255.254	172.31.255.255
192.168.0.0	255.255.0.0	192.168.0.0–192.168.255.254	192.168.255.255

Все остальные IPv4-адреса являются открытыми, сдаются в аренду или приобретаются. Если сеть имеет прямое подключение к Интернету и вам выделен диапазон IPv4-адресов от поставщика услуг Интернета, вы можете использовать эти IPv4-адреса для компьютеров своей сети.

Проверка адреса при помощи команды PING

Назначая статический IP-адрес, необходимо убедиться, что этот адрес уже не используется и не зарезервирован для DHCP. Для проверки возможного использования адреса применяется команда ping. Откройте командную

строку и введите ping, а затем IP-адрес, который вы проверяете. Например, проверки IPv4-адреса 10.0.10.12 следует ввести команду:

```
ping 10.0.10.12
```

Синтаксис команды для проверки IPv6-адреса FEC0::02BC:FF:BECB:FE4F:961D таков:

```
ping FEC0::02BC:FF:BECB:FE4F:961D
```

Если при тестировании с помощью ping вы получили положительный отклик, данный IP-адрес используется, и вам следует выбрать другой адрес. Если же во время всех четырех попыток превышен интервал ожидания, IP-адрес в данный момент неактивен и, возможно, не используется. Однако не исключено, что ваш запрос был заблокирован брандмауэром. С гарантией подтвердить незанятость IP-адреса может только администратор сети.

Настройка статического IPv4- или IPv6-адреса

Каждый установленный сетевой адаптер может быть подключен к одной локальной сети. Эти подключения создаются автоматически. Чтобы настроить статический IP-адрес для конкретного подключения, выполните следующие действия:

1. В панели управления последовательно щелкните **Сеть и Интернет (Network And Internet)** и **Центр управления сетями и общим доступом (Network And Sharing Center)**.
2. В Центре управления сетями и общим доступом (Network And Sharing Center) в разделе **Просмотр активных сетей (View Your Active Networks)** перейдите по ссылке, соответствующей сетевому подключению.
3. В диалоговом окне состояния подключения щелкните кнопку **Свойства (Properties)**.
4. В открывшемся окне свойств подключения дважды щелкните запись **Протокол Интернета версии 6 (Internet Protocol Version 6)** или **Протокол Интернета версии 4 (Internet Protocol Version 4)**, в зависимости от типа настраиваемого IP-адреса.
5. Для настройки IPv6-адреса выполните следующие действия:
   а) Щелкните **Использовать следующий IPv6-адрес (Use The Following IPv6 Address)** и введите IPv6-адрес в текстовое поле **IPv6-адрес (IPv6 Address)**. Назначенный вами IPv6-адрес не должен использоваться нигде в сети.
   б) Нажмите Tab. Информация в поле **Длина префикса подсети (Subnet Prefix Length)** служит для обеспечения правильного взаимодействия компьютера в сети. Для префикса подсети будет введено стандартное значение. Если в сети не используются маски подсети переменной длины, стандартного значения достаточно. Если в сети используются маски подсети переменной длины, измените это значение в соответствии с конфигурацией вашей сети.

6. Для настройки IPv4-адреса выполните следующие действия:
   а) Щелкните **Использовать следующий IP-адрес (Use The Following IP Address)** и введите IPv4-адрес в поле **IP-адрес (IP Address)**. Назначенный вами IPv4-адрес не должен использоваться нигде в сети.
   б) Нажмите Tab. Информация в поле **Маска подсети (Subnet Mask)** служит для обеспечения правильного взаимодействия компьютера в сети. Для маски подсети будет введено стандартное значение. Если в сети не применяются маски подсети переменной длины, стандартного значения достаточно, но если маски подсети переменной длины используются, измените данное значение в соответствии с конфигурацией вашей сети.
7. Укажите в поле **Основной шлюз (Default Gateway)** IP-адрес основного шлюза для доступа компьютера к другим TCP/IP-сетям, Интернету или другим подсетям. Введите IP-адрес маршрутизатора, используемого в сети по умолчанию.
8. Для разрешения доменных имен необходим адрес DNS-сервера. Введите адреса предпочитаемого и альтернативного DNS-серверов в соответствующих полях.
9. Завершив настройку, дважды щелкните **OK**. Затем щелкните **Закрыть (Close)**. Повторите процедуру для настройки других сетевых адаптеров и IP-протоколов.
10. При необходимости настройте WINS, как описано далее в разделе «Настройка WINS».

Настройка динамических IP-адресов и альтернативной IP-адресации

В настоящее время на большинстве рабочих станций используется динамическая и (или) альтернативная IP-адресация. Чтобы настроить динамическую и альтернативную адресацию, выполните следующие действия:

1. В панели управления последовательно щелкните **Сеть и Интернет (Network And Internet)** и **Центр управления сетями и общим доступом (Network And Sharing Center)**.
2. В Центре управления сетями и общим доступом (Network And Sharing Center) в разделе **Просмотр активных сетей (View Your Active Networks)** перейдите по ссылке, соответствующей сетевому подключению.
3. В диалоговом окне состояния подключения щелкните **Свойства (Properties)**. Откроется диалоговое окно свойств подключения, показанное на рис. 15-5.

Примечание Подключения создаются автоматически для каждого адаптера. Если у установленного адаптера нет подключения, проверьте его драйвер. Возможно, он установлен неправильно.

4. Дважды щелкните запись **Протокол Интернета версии 6 (Internet Protocol Version 6)** или **Протокол Интернета версии 4 (Internet Protocol Version 4)**, в зависимости от типа настраиваемого IP-адреса.
5. Щелкните переключатель **Получить IPv6-адрес автоматически (Obtain An IPv6 Address Automatically)** или **Получить IP-адрес автоматически (Obtain An IP Address Automatically)**, в зависимости от типа настраиваемого IP-адреса. При необходимости установите переключатель **Получить адрес DNS-сервера автоматически (Obtain DNS Server Address Automatically)** или **Использовать следующие адреса DNS-серверов (Use The Following DNS Server Addresses)**. Затем введите адреса предпочитаемого и альтернативного DNS-серверов в соответствующие поля.
6. Используя динамическую IPv4-адресацию на настольном компьютере, настройте автоматический альтернативный адрес. Убедитесь, что на вкладке **Альтернативная конфигурация (Alternate Configuration)** установлен переключатель **Автоматический частный IP-адрес (Automatic Private IP Address)**. Дважды щелкните **OK**, **Закрыть (Close)** и пропустите остальные шаги.
7. Используя динамическую IPv4-адресацию на переносном компьютере, настройте альтернативный адрес вручную. На вкладке **Альтернативная конфигурация (Alternate Configuration)** установите переключатель **Настраиваемый пользователем (User Configured)**. Затем введите нужный IP-адрес в поле **IP-адрес (IP Address)**. Это должен быть частный IP-адрес (см. табл. 15-3), который более нигде не используется.
8. Введите маску подсети, основной шлюз и параметры DNS и WINS. Завершив настройку, дважды щелкните **OK**. Затем щелкните **Закрыть (Close)**.

Примечание Подробнее о настройке портативных компьютеров — в главе 16.

Настройка нескольких шлюзов

Для обеспечения отказоустойчивости при выходе маршрутизатора из строя компьютеры под управлением Windows 7 можно настроить на использование нескольких шлюзов. При этом для выбора используемого шлюза и времени его использования применяется метрика шлюза, значение которой указывает на затратность использования шлюза. Шлюз с наименьшей ценой или метрикой используется первым. Если компьютер не способен взаимодействовать с данным шлюзом, предпринимается попытка использовать следующий шлюз с наименьшей метрикой и т. д.

Выбор способа настройки нескольких шлюзов зависит от конфигурации сети. Если на компьютерах используется DHCP, дополнительные шлюзы можно настроить при помощи параметров на DHCP-сервере. Если используются статические IP-адреса или требуется указать шлюзы вручную, выполните следующие действия:

1. В панели управления последовательно щелкните **Сеть и Интернет (Network And Internet)** и **Центр управления сетями и общим доступом (Network And Sharing Center)**.
2. В Центре управления сетями и общим доступом (Network And Sharing Center) в разделе **Просмотр активных сетей (View Your Active Networks)** перейдите по ссылке, соответствующей сетевому подключению.
3. В диалоговом окне состояния подключения щелкните **Свойства (Properties)**.
4. В открывшемся окне свойств подключения дважды щелкните запись **Протокол Интернета версии 6 (Internet Protocol Version 6)** или **Протокол Интернета версии 4 (Internet Protocol Version 4)**, в зависимости от типа настраиваемого IP-адреса.
5. Щелкните **Дополнительно (Advanced)** для перехода в диалоговое окно **Дополнительные параметры TCP/IP (Advanced TCP/IP Settings)**, показанное на рис. 15-6.

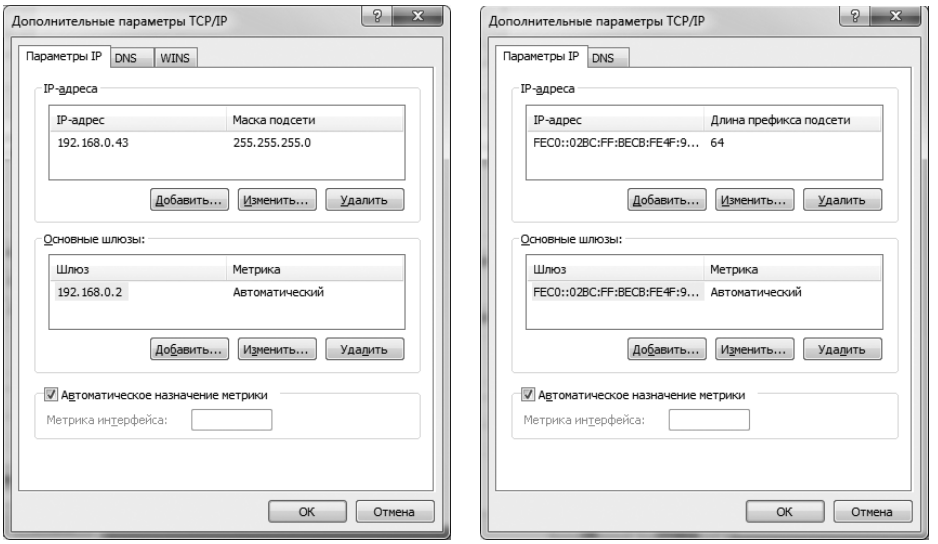

Рис. 15-6. Настройка нескольких IP-аресов и шлюзов (слева для IPv4, справа для IPv4)

6. В разделе **Основные шлюзы (Default Gateways)** показаны текущие шлюзы, настроенные вручную. При необходимости щелкните кнопку **Добавить (Add)** и введите адрес шлюза в поле **Шлюз (Gateway)**.
7. По умолчанию метрика шлюза в Windows 7 назначается автоматически, но ее также можно ввести вручную. Сбросьте флажок **Автоматическое назначение метрики (Automatic Metric)** и введите значение метрики в соответствующее поле.
8. Чтобы ввести адреса дополнительных шлюзов, еще раз щелкните **Добавить (Add)** и введите адрес и метрику.
9. Три раза щелкните **OK**, а затем щелкните **Закрыть (Close)**.

Настройка DNS

Служба разрешения имен DNS позволяет найти IP-адрес компьютера по имени хоста. Благодаря этому пользователи работают с понятными хост-именами, например http://www.msn.com или http://www.microsoft.com, а не с IP-адресами, наподобие 192.168.5.102 или 192.168.12.68. Служба DNS является основной службой имен в Windows 7 и в Интернете.

Выбор способа настройки DNS зависит от конфигурации сети. Если используется DHCP, DNS можно настроить при помощи DHCP-сервера. Если используются статические IP-адреса или требуется индивидуально настроить DNS для пользователя или системы, следует настроить DNS вручную.

Основные параметры DNS

Чтобы настроить основные параметры DNS, выполните следующие действия:

1. В панели управления последовательно щелкните **Сеть и Интернет (Network And Internet)** и **Центр управления сетями и общим доступом (Network And Sharing Center)**.
2. В Центре управления сетями и общим доступом (Network And Sharing Center) в разделе **Просмотр активных сетей (View Your Active Networks)** перейдите по ссылке, соответствующей сетевому подключению.
3. В диалоговом окне состояния подключения щелкните **Свойства (Properties)**.
4. В открывшемся окне свойств подключения дважды щелкните запись **Протокол Интернета версии 6 (Internet Protocol Version 6)** или **Протокол Интернета версии 4 (Internet Protocol Version 4)**, в зависимости от типа настраиваемого IP-адреса.
5. Если вы хотите, чтобы адрес DNS-сервера предоставлялся DHCP-сервером, установите переключатель **Получить адрес DNS-сервера автоматически (Obtain DNS Server Address Automatically)**. В противном случае установите переключатель **Использовать следующие адреса DNS-серверов (Use The Following DNS Server Addresses)** и введите адреса основного и альтернативного DNS-серверов в соответствующие поля.
6. Дважды щелкните **OK**, а затем щелкните **Закрыть (Close)**.

Дополнительные параметры DNS

Дополнительные параметры DNS находятся на вкладке **DNS** диалогового окна **Дополнительные параметры TCP/IP (Advanced TCP/IP Settings)**, показанной на рис. 15-7. Назначение полей на вкладке **DNS** таково:

- **Адреса DNS-серверов, в порядке использования (DNS Server Addresses, In Order Of Use)** Укажите здесь IP-адреса всех DNS-серверов, используемых для разрешения доменных имен. Чтобы добавить IP-адрес сервера в список, щелкните **Добавить (Add)**. Щелкните **Удалить (Remove)** для удаления адреса сервера из списка. Для изменения выде-

ленного элемента щелкните **Изменить (Edit)**. Можно указать для разрешения DNS несколько серверов. Их приоритет определяется расположением в списке. Если первый сервер не может ответить на запрос разрешения имен, запрос посылается на следующий DNS-сервер из списка и т. д. Чтобы изменить положение сервера в списке, выделите сервер, а затем воспользуйтесь кнопками со стрелками вверх и вниз.

- **Дописывать основной DNS-суффикс и суффикс подключения (Append Primary And Connection Specific DNS Suffixes)** Этот переключатель по умолчанию включен. Он применяется для разрешения неизвестных имен узлов в основном домене. Если, например, имя компьютера Gandolf, а имя родительского домена microsoft.com, имя компьютера будет разрешено как gandolf.microsoft.com. Если в родительском домене нет такого FQDN-имени, произойдет сбой запроса. Имя родительского домена указано в диалоговом окне **Свойства системы (System Properties)** на вкладке **Имя компьютера (Computer Name)**.
- **Дописывать родительские суффиксы основного DNS-суффикса (Append Parent Suffixes Of The Primary DNS Suffix)** Этот флажок по умолчанию установлен. Он применяется для разрешения имен неизвестных узлов при помощи структуры домена «родитель-потомок». В случае сбоя запроса в ближайшем родительском домене при следующей попытке разрешить запрос используется родительский суффикс для родительского домена. Это продолжается до тех пор, пока не будет достигнута вершина доменной структуры DNS. Если, например, компьютер с именем Gandolf используется в домене dev.microsoft.com, будет проведена попытка разрешить имя компьютера как gandolf.dev.microsoft.com. В случае неудачи будет проведена попытка разрешить имя компьютера как gandolf.microsoft.com.
- **Дописывать следующие DNS-суффиксы (по порядку) (Append These DNS Suffixes (In Order))** Установите этот переключатель, чтобы задать DNS-суффиксы, которые следует использовать для разрешения имен вместо суффикса родительского домена. Чтобы добавить доменный суффикс в список, щелкните **Добавить (Add)**. Щелкните **Удалить (Remove)** для удаления суффикса из списка. Для изменения выделенного элемента щелкните **Изменить (Edit)**. Если указать несколько суффиксов, они будут использоваться в порядке расположения в списке. Если при помощи первого суффикса разрешение невозможно, служба DNS попытается использовать следующий по списку суффикс. Для изменения порядка в списке выделите суффикс и измените его положение стрелками вверх и вниз.
- **DNS-суффикс подключения (DNS Suffix For This Connection)** В этом поле задается специальный DNS-суффикс подключения, который перекрывает DNS-имена, уже настроенные для данного подключения. Чтобы задать DNS-имя домена, нужно в панели управления последовательно щелкнуть **Система и безопасность (System And Security), Система (System)** и **Изменить параметры (Change Settings)**. Щелкните кнопку

Изменить (Change) на вкладке **Имя компьютера (Computer Name)** диалогового окна **Свойства системы (System Properties)**, а затем щелкните **Дополнительно (More)**. Введите основной DNS-суффикс для компьютера в соответствующее поле. Чтобы сохранить изменения, три раза щелкните **OK**.

- **Зарегистрировать адреса этого подключения в DNS (Register This Connection's Addresses In DNS)** Этот флажок по умолчанию установлен и используется для регистрации всех IP-адресов данного подключения в DNS с полным доменным именем компьютера. По умолчанию параметр включен.

  Динамические обновления DNS совместно с DHCP позволяют клиенту в случае изменения IP-адреса обновить запись A (адрес узла), а DHCP-серверу предоставляют возможность обновить PTR-запись (указатель) клиента на DNS-сервере. Кроме того, DHCP-серверы можно настроить на одновременное обновление A- и PTR-записей от имени клиента. Динамические обновления DNS поддерживаются только в BIND 5.1 или более поздних версиях DNS-сервера, а также в Windows 2000 Server, Windows Server 2003 и последующих версиях Windows. Эта возможность не поддерживается в Windows NT Server 4.
- **Использовать DNS-суффикс подключения при регистрации в DNS (Use This Connection's DNS Suffix In DNS Registration)** Установите этот флажок, чтобы все IP-адреса данного подключения регистрировались в DNS под родительским доменом.

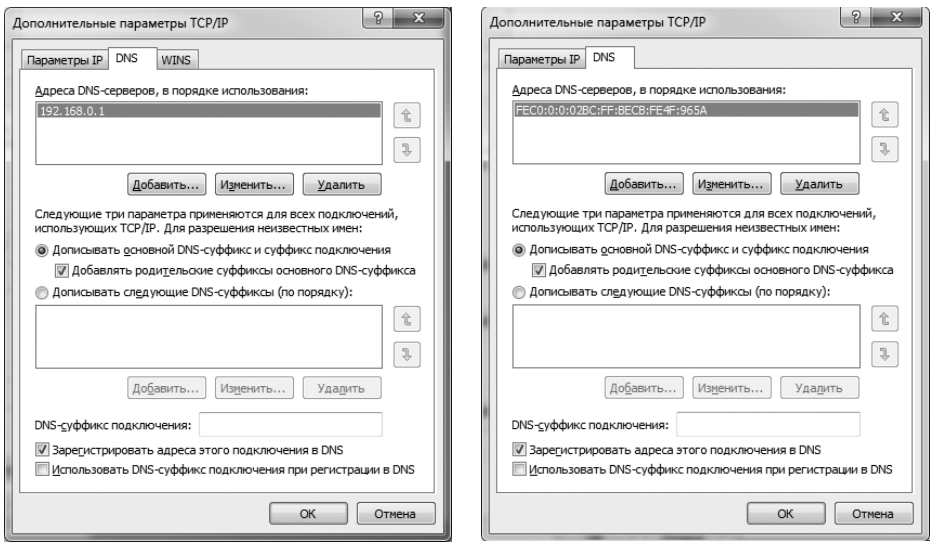

Рис. 15-7. Настройка дополнительных параметров DNS (слева для IPv4, справа для IPv6)

Настройка WINS

Служба WINS предназначена для разрешения имен NetBIOS в IPv4-адреса. Она позволяет компьютерам сети определять адреса других компьютеров. Если в сети установлен WINS-сервер, можно разрешать имена компьютеров с его помощью. Хотя WINS поддерживается во всех версиях Windows, в Windows 7 эта служба используется, главным образом, для обеспечения обратной совместимости.

На компьютерах под управлением Windows 7 для разрешения NetBIOS-имен можно использовать локальный файл LMHOSTS. Однако обращение к нему происходит только в случае сбоя разрешения имен обычными методами. В правильно настроенной сети эти файлы почти не используются. Таким образом, предпочтительным методом разрешения NetBIOS-имен компьютеров остается служба WINS в сочетании с WINS-сервером.

Выбор способа настройки WINS зависит от конфигурации сети. Если в сети используется DHCP, WINS можно настроить при помощи параметров на DHCP-сервере. Если используются статические IPv4-адреса или требуется отдельно настроить WINS для пользователя или системы, выполните следующие действия:

1. Откройте диалоговое окно **Дополнительные параметры TCP/IP (Advanced TCP/IP Settings)** на вкладке **WINS**, показанной на рис. 15-8.

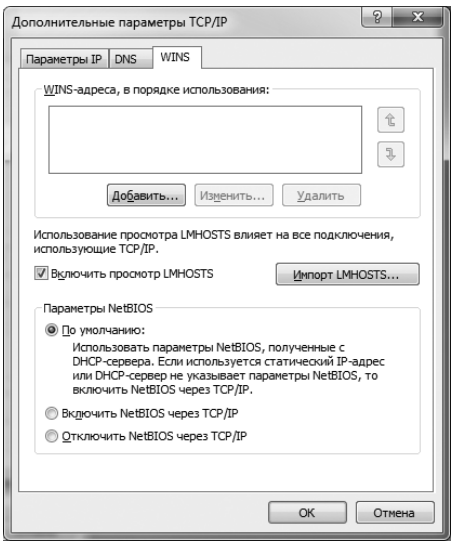

Рис. 15-8. Настройка разрешения WINS для NetBIOS-имен

2. В области **WINS-адреса, в порядке использования (WINS Addresses, In Order Of Use)** укажите IPv4-адреса WINS-серверов, применяемых для разрешения NetBIOS-имен. Чтобы добавить IPv4-адрес сервера в список, щелкните **Добавить (Add)**. Щелкните **Удалить (Remove)** для удаления выделенного сервера из списка. Для изменения выделенного элемента щелкните **Изменить (Edit)**.

3. Если в списке указано несколько серверов, при разрешении WINS они используются в порядке следования. Если первый сервер не отвечает на запрос разрешения NetBIOS-имени, запрос посылается на следующий WINS-сервер из списка и т. д. Чтобы изменить положение сервера в списке, выделите сервер, а затем воспользуйтесь кнопками со стрелками вверх и вниз.
4. При необходимости установите флажок **Включить просмотр LMHOSTS (Enable LMHOSTS Lookup)**. Для использования существующего файла LMHOSTS щелкните **Импорт LMHOSTS (Импорт LMHOSTS)**. Файл LMHOSTS, как правило, используется при сбое всех остальных методов разрешения.
5. Чтобы настроить разрешение имен WINS при помощи NetBIOS, выберите один из следующих параметров:
   - Если используется DHCP и динамическая адресация, назначайте параметры NetBIOS при помощи DHCP-сервера. Установите переключатель **По умолчанию: Использовать параметры NetBIOS, полученные с DHCP-сервера (Default: Use NetBIOS Setting From The DHCP Server)**.
   - Если используется статический IP-адрес или на DHCP-сервере нет параметров NetBIOS, установите переключатель **Включить NetBIOS через TCP/IP (Enable NetBIOS Over TCP/IP)**.
   - Если в сети не используются WINS и NetBIOS, установите переключатель **Отключить NetBIOS через TCP/IP (Enable NetBIOS Over TCP/IP)**. Тем самым вы прекратите рассылку компьютером широковещательных пакетов NetBIOS.
6. Три раза щелкните **OK**, а затем щелкните **Закрыть (Close)**. При необходимости повторите процесс для других сетевых адаптеров.

Совет Файлы LMHOSTS поддерживаются индивидуально на каждом компьютере, из-за чего со временем сведения в них могут стать недостоверными. Поэтому не полагайтесь на LMHOSTS, а обеспечьте правильность конфигурации и доступность DNS- и WINS-серверов для централизованного администрирования служб разрешения имен.

Управление локальными сетевыми подключениями

Подключения по локальной сети открывают компьютеру доступ к ресурсам сети и Интернета. Для каждого установленного на компьютере сетевого адаптера автоматически создается одно локальное сетевое подключение. Этот раздел посвящен методам управления сетевыми подключениями.

Включение и отключение подключений по локальной сети

Подключения по локальной сети создаются и включаются автоматически. Чтобы отключить и не использовать подключение, выполните следующие действия:

1. В панели управления последовательно щелкните **Сеть и Интернет (Network And Internet)** и **Центр управления сетями и общим доступом (Network And Sharing Center)**.
2. В Центре управления сетями и общим доступом (Network And Sharing Center) на левой панели щелкните **Изменение параметров адаптера (Change Adapter Settings)**.
3. В окне **Сетевые подключения (Network Connections)** щелкните правой кнопкой нужное подключение и выберите команду **Отключить (Disable)**.
4. Если позже вам понадобится включить подключение, щелкните его правой кнопкой и выберите команду **Включить (Enable)**.

Чтобы отключиться от сети или подключиться к ней, выполните следующие действия:

1. В панели управления последовательно щелкните **Сеть и Интернет (Network And Internet)** и **Центр управления сетями и общим доступом (Network And Sharing Center)**.
2. В Центре управления сетями и общим доступом (Network And Sharing Center) на левой панели щелкните **Изменение параметров адаптера (Change Adapter Settings)**.
3. В окне **Сетевые подключения (Network Connections)** щелкните правой кнопкой нужное подключение и выберите команду **Отключить (Disconnect)**. Обычно она есть только в меню подключений удаленного доступа.
4. Если вы хотите активировать подключение, в окне **Сетевые подключения (Network Connections)** щелкните правой кнопкой нужное подключение и выберите команду **Подключить (Connect)**.

Проверка состояния, скорости и активности локального подключения

Чтобы проверить состояние локального сетевого подключения, выполните следующие действия:

1. В панели управления последовательно щелкните **Сеть и Интернет (Network And Internet)** и **Центр управления сетями и общим доступом (Network And Sharing Center)**.
2. В Центре управления сетями и общим доступом (Network And Sharing Center) в разделе **Просмотр активных сетей (View Your Active Networks)** перейдите по ссылке, соответствующей нужному подключению.
3. Откроется диалоговое окно состояния сетевого подключения. Если оно не открылось, подключение или носитель отключены. Включите подключение или присоедините сетевой кабель, а потом снова попытайтесь открыть диалоговое окно **Состояние (Status)**.
4. На вкладке **Общие (General)** диалогового окна состояния (рис. 15-9) просмотрите следующие сведения:

- **IPv4-подключение (IPv4 Connectivity)** Состояние и вид текущего IPv4-подключения: работоспособность, наличие или отсутствие доступа в Интернет.
- **IPv6-подключение (IPv6 Connectivity)** Состояние и вид текущего IPv6-подключения: работоспособность, наличие или отсутствие доступа в Интернет.
- **Состояние среды (Media State)** Поскольку диалоговое окно **Состояние (Status)** открывается только при активном подключении, в этом поле, как правило, стоит состояние **Подключено (Enabled)**.
- **Длительность (Duration)** Время, прошедшее с момента установки подключения. Небольшая длительность подключения свидетельствует, что пользователь недавно подключился к сети или подключение было восстановлено.
- **Скорость (Speed)** Скорость подключения. Возможные значения: 10.0 Мбит/с, 100.0 Мбит/с и 1.0 Гбит/с. Неправильно заданная скорость может снизить быстродействие компьютера.
- **Байт (Bytes)** Количество отправленных и принятых за время подключения байт. На текущую отправку и прием пакетов указывает мигание значков компьютеров.

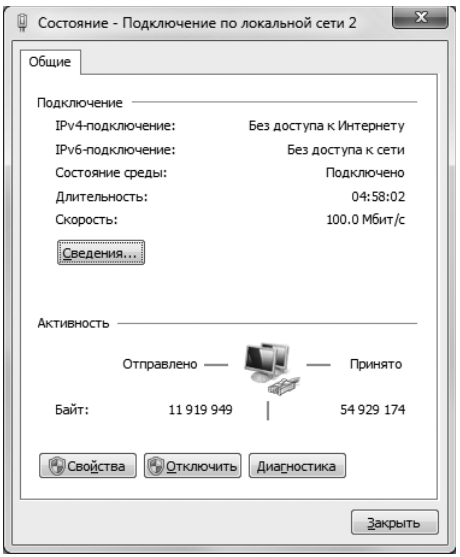

Рис. 15-9. Вкладка Общие (General) диалогового окна состояния подключения

Просмотр сведений о конфигурации сети

В Windows 7 есть несколько способов просмотра текущей конфигурации сетевых адаптеров. Для просмотра параметров конфигурации в диалоговом окне **Состояние (Status)**, выполните следующие действия:

1. В панели управления последовательно щелкните **Сеть и Интернет (Network And Internet)** и **Центр управления сетями и общим доступом (Network And Sharing Center)**.
2. В Центре управления сетями и общим доступом (Network And Sharing Center) щелкните **Изменение параметров адаптера (Change Adapter Settings)** на левой панели.
3. В окне **Сетевые подключения (Network Connections)** дважды щелкните нужное подключение. Откроется диалоговое окно состояния подключения.
4. Щелкните кнопку **Сведения (Details)** для просмотра подробных сведений об IP-конфигурации, включая следующие сведения:
   - **Физический адрес (Physical Address)** MAC-адрес сетевого адаптера, уникальный для каждого адаптера.
   - **IPv4-адрес (IPv4 Address)** Адрес для IPv4-подключения.
   - **Маска подсети IPv4 (IPv4 Subnet Mask)** Маска подсети, используемая для IPv4-подключения.
   - **Шлюз по умолчанию IPv4 (IPv4 Default Gateways)** Адреса основных шлюзов для IPv4-подключения.
   - **DNS-сервер IPv4 (IPv4 DNS Servers)** IP-адреса DNS-серверов, используемых для IPv4-подключения.
   - **WINS-сервер IPv4 (IPv4 WINS Servers)** IP-адреса WINS-серверов, используемых для IPv4-подключения.
   - **DHCP-сервер IPv4 (IPv4 DHCP Server)** IP-адрес DHCPv4-сервера, у которого была получена текущая аренда (только для DHCPv4).
   - **Аренда получена (Lease Obtained)** Отметка времени и даты получения аренды DHCPv4 (только для DHCPv4).
   - **Аренда истекает (Lease Expires)** Отметка времени и даты истечения срока аренды DHCPv4 (только для DHCPv4).

Чтобы просмотреть дополнительные параметры конфигурации, воспользуйтесь командой Ipconfig. Выполните следующие действия:

1. Щелкните кнопку **Пуск (Start)** и введите cmd в поле поиска.
2. Нажмите Enter.
3. Чтобы просмотреть подробные сведения о конфигурации всех сетевых адаптеров, настроенных на компьютере, в командной строке введите **ipconfig /all**.

Примечание Командную строку откройте в режиме обычного пользователя, без повышенных полномочий.

Переименование подключения по локальной сети

Первоначально в Windows 7 подключениям по локальной сети присваиваются стандартные имена. Для переименования подключения в окне **Сетевые**

подключения (Network Connections) щелкните его правой кнопкой, выберите команду **Переименовать (Rename)** и введите новое имя. Если на компьютере есть несколько подключений по локальной сети, подходящее имя поможет вам и другим пользователям ориентироваться в подключениях.

Диагностика и тестирование параметров сети

В Windows 7 имеется ряд средств диагностики и тестирования TCP/IP-подключений. Далее мы обратимся к автоматизированным средствам диагностики, основным тестам, которые следует проводить после каждой установки или изменения сетевых параметров компьютера, и способам разрешения проблем подключения, связанных с DHCP и DNS. В последнем разделе рассказано о том, как проводить подробное диагностическое исследование сети.

Диагностика и разрешение проблем подключения по локальной сети

Иногда подключение перестает работать из-за случайного отсоединения кабеля или сбоя сетевого адаптера. После присоединения кабеля или устранения неисправности адаптера подключение должно восстанавливаться автоматически. Чтобы провести диагностику локального сетевого подключения, щелкните правой кнопкой значок **Сеть (Network)** на панели задач и выберите команду **Диагностика неполадок (Troubleshoot Problems)**.

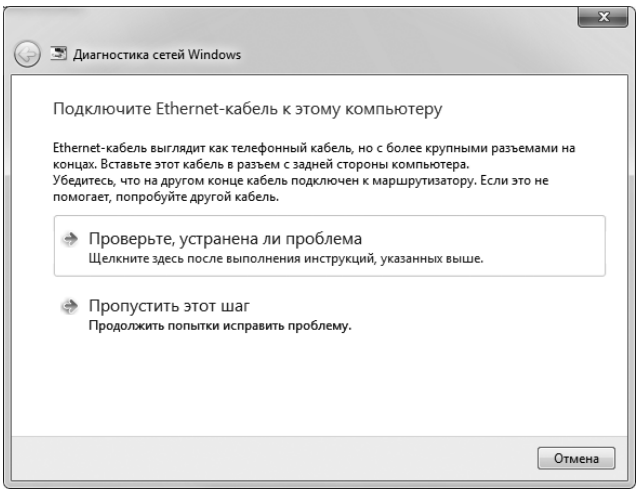

Рис. 15-10. Устранение неисправности сети по рекомендациям системы

Инструмент Диагностика сетей Windows (Windows Network Diagnostics) выполняет поиск неисправности. Как показано на рис. 15-10, при обнаружении известных проблем выводится список возможных решений. Некоторые решения сопровождаются ссылками на автоматизированные инструменты устранения неисправностей, для вызова которых достаточно щелкнуть соответствующую ссылку. В других решениях предполагается устранить непо-

ладки вручную, например, сбросить сетевой маршрутизатор или широкополосный модем. Если действия не привели к желаемому результату, обратитесь к другим рекомендациям.

Диагностика и устранение неполадок подключения к Интернету

Поиск причин неисправности сети может оказаться непростой задачей из-за запутанных взаимозависимостей служб, протоколов и параметров конфигурации. К счастью, ОС Windows 7 оснащена действенным инструментом для диагностики сети, позволяющим обнаруживать сбои в следующих областях:

- общие проблемы с подключением;
- параметры служб Интернета для электронной почты, групп новостей и прокси-серверов;
- параметры модемов, сетевых клиентов и сетевых адаптеров;
- конфигурация DNS, DHCP и WINS;
- основные шлюзы и IP-адреса.

Для диагностики подключения к Интернету в Центре управления сетями и общим доступом (Network And Sharing Center), щелкните красный крестик на карте сети. Инструмент Диагностика сетей Windows (Windows Network Diagnostics) начнет поиск неисправности. При обнаружении известных проблем будет выведен список возможных решений.

Базовое тестирование сети

После настройки сети на новом компьютере или после внесения изменений в сетевые параметры следует протестировать конфигурацию. Самое простое тестирование подключения компьютера к сети TCP/IP выполняется при помощи команды Ping. Введите в командной строке **ping *<узел>***, где *<узел>* — имя компьютера или IP-адрес узла, к которому вы пытаетесь подключиться.

В Windows 7 команда Ping может применяться для проверки следующих аспектов конфигурации:

- **Проверка наличия связи с IP-адресами** Если компьютер настроен правильно и узел, к которому вы пытаетесь подключиться, доступен, запуск команды Ping приведет к получению отклика, при условии что передача эхо-пакетов разрешена брандмауэром компьютера. Если при помощи команды Ping найти узел не удается или передача заблокирована брандмауэром, выполнение команды Ping будет завершено по истечению срока действия.
- **Проверка работы WINS по NetBIOS-именам компьютеров** Если при помощи команды Ping удается правильно разрешить NetBIOS-имя компьютера, значит параметры WINS настроены правильно.

- **Проверка работы DNS по именам узлов в DNS-доменах** Если с помощью команды Ping удается правильно разрешить полные DNS-имена узлов, разрешение имен DNS настроено правильно.

Кроме того, можно проверить возможность просмотра сети. Если компьютер входит в домен Windows 7 и в домене включена возможность просмотра компьютеров, выполните вход на компьютер и просмотрите другие компьютеры домена в Проводнике Windows (Windows Explorer) или Сетевом проводнике (Network Explorer). Затем выполните вход на другой компьютер домена и попытайтесь найти настраиваемый вами компьютер. Эти тесты направлены на проверку правильности разрешения имен DNS в локальной среде. Если просмотр не удался, проверьте конфигурацию служб и протоколов DNS.

Ближе к реальности Возможность доступа к ресурсам сети в Сетевом проводнике (Network Explorer) зависит от состояния службы Обозреватель компьютеров (Computer Browser) и параметров сетевого обнаружения. Служба Обозреватель компьютеров (Computer Browser) отвечает за составление списка компьютеров, находящихся в сети. В случае останова или неправильной работы этой службы доступные ресурсы в Сетевом проводнике (Network Explorer) отображены не будут. Проверить состояние службы Обозреватель компьютеров (Computer Browser) можно в консоли **Управление компьютером (Computer Management)**. Разверните узел **Службы и приложения (Services And Applications)**, затем на левой панели выберите узел **Службы (Services)**. Служба Обозреватель компьютеров (Computer Browser) должна находиться в состоянии Работает (Started). Если поле состояния этой службы пусто, служба не выполняется и ее нужно запустить.

В некоторых случаях, служба Обозреватель компьютеров (Computer Browser) работает нормально, но обновленный список ресурсов в Сетевом проводнике (Network Explorer) все-таки отсутствует. Такое случается, когда вместо постоянной проверки обновлений список ресурсов обновляется лишь периодически. Если нужный вам ресурс отсутствует в списке, дождитесь его появления (на что, как правило, уходит не более 15 минут) или подключитесь к ресурсу напрямую при помощи UNC-имени или IP-адреса, как описано в главе 13.

В некоторых случаях возможность обнаружения блокирована параметрами обнаружения и общего доступа. Чтобы разрешить обнаружение, выполните следующие действия:

- В панели управления последовательно щелкните **Сеть и Интернет (Network And Internet)** и **Центр управления сетями и общим доступом (Network And Sharing Center)**.
- В Центре управления сетями и общим доступом (Network And Sharing Center) на левой панели щелкните **Изменить дополнительные параметры общего доступа (Change Advanced Sharing Settings)**.
- Если сетевое обнаружение отключено, щелкните **Включить сетевое обнаружение (Turn On Network Discovery)**.

Устранение неполадок IP-адресации

Просмотр текущих параметров IP описан ранее в разделе «Просмотр сведений о конфигурации сети». Если компьютер не способен получить доступ к сетевым ресурсам или у него нет связи с другими компьютерами, виновата, скорее всего, IP-адресация. Проверьте текущий IP-адрес компьютера и другие параметры IP. Далее приведены сведения, которые пригодятся вам при диагностике:

- Если назначенный в данный момент IPv4-адрес находится в диапазоне от 169.254.0.1 до 169.254.255.254, компьютер использует автоматическое назначение частных IP-адресов. При использовании DHCP это означает, что клиент DHCP не может подключиться к DHCP-серверу. При использовании автоматического частного адреса Windows 7 периодически проверяет доступность DHCP-сервера. Если даже по прошествии некоторого времени компьютер не получает динамический IP-адрес, скорее всего, у вас проблемы с сетевым подключением. Проверьте целостность сетевого кабеля до хаба или коммутатора.
- Если IPv4-адрес и маска подсети компьютера в данный момент равны 0.0.0.0, сеть отключена или кто-то пытался использовать статический IP-адрес, совпадающий с другим уже задействованным в сети IP-адресом. Откройте окно **Сетевые подключения (Network Connections)** и проверьте состояние подключения. Если подключение отключено или выключено, щелкните его правой кнопкой и выберите команду **Подключить (Enable)** или **Восстановить (Repair)**. Если подключение уже включено, необходимо изменить параметры IP-адреса подключения.
- Если IP-адрес назначается динамически, убедитесь, что в сети нет другого компьютера, использующего этот же IP-адрес. Сделать это можно, отсоединив сетевой кабель настраиваемого компьютера и проверив проблемный IP-адрес при помощи команды Ping. Получение отклика Ping означает, что данный IP-адрес используется на другом компьютере. Настраиваемому компьютеру, скорее всего, присвоен неправильный статический IP-адрес или неправильно настроено резервирование адресов.
- Если IP-адрес назначен правильно, проверьте маску подсети, шлюз, DNS и WINS, сравнив сетевые параметры диагностируемого компьютера с параметрами компьютера, правильность сетевой конфигурации которого не вызывает сомнений. Одна из основных причин сбоев — неверно настроенная маска сети. Когда применяется разбиение на подсети, маска подсети одной области может быть очень похожа на маску подсети другой области. Например, в одной области IPv4 маска сети может быть 255.255.255.240, а в другой области — 255.255.255.248.

Освобождение и обновление параметров DHCP

Серверы DHCP способны автоматически назначать многие параметры сетевой конфигурации, в том числе IP-адрес, адреса основных шлюзов, основ-

ного и дополнительного DNS-серверов, основного и дополнительного WINS-серверов и др. При динамической адресации конкретный IP-адрес выделяется компьютеру в аренду. Аренда выдается на определенный промежуток времени и должна периодически обновляться. Когда аренду нужно обновить, компьютер вызывает выдавший аренду DHCP-сервер. Если сервер доступен, аренда обновляется с предоставлением нового срока действия. Кроме того, аренду на отдельных компьютерах можно обновлять вручную при помощи самого DHCP-сервера.

Сбои, нарушающие сетевое взаимодействие, возникают во время назначения аренды и в процессе обновления. Если сервер недоступен и до окончания срока аренды к нему не удалось подключиться, IP-адрес может оказаться недействительным. В этом случае компьютер переходит на альтернативный IP-адрес, который зачастую не позволяет полноценно работать в сети. Для решения проблемы необходимо освободить, а затем обновить аренду DHCP.

Еще одна причина сбоев — перемещение пользователей по офисам и подсетям организации. При временном перемещении в другое место компьютер может получить параметры DHCP с «неправильного» сервера. По возвращению в исходный офис компьютер может работать медленно или с ошибками, из-за того что параметры назначены ему DHCP-сервером, находящимся в другом расположении. В этом случае также нужно сначала освободить, а затем обновить аренду DHCP.

Чтобы освободить и обновить аренду DHCP, выполните следующие действия:

1. В Центре управления сетями и общим доступом (Network And Sharing Center) на левой панели щелкните **Изменение параметров адаптера (Change Adapter Settings)**.
2. В окне сетевых подключений щелкните правой кнопкой нужное подключение и выберите **Диагностика (Diagnose)**.
3. Инструмент Диагностика сетей Windows (Windows Network Diagnostics) выведет список возможных решений. Если компьютеру назначен один или несколько динамических IP-адресов, среди решений должен быть вариант **Автоматически получить новые параметры IP (Automatically Get New IP Settings)**. Щелкните это решение.

Чтобы освободить и обновить параметры при помощи команды Ipconfig, выполните следующие действия:

1. Откройте командную строку с повышенными полномочиями.
2. Чтобы освободить текущие параметры для всех сетевых адаптеров, введите в командной строке **ipconfig /release**. Затем обновите аренду, выполнив команду **ipconfig /renew**.
3. Чтобы только обновить аренду DHCP для всех сетевых адаптеров, введите в командной строке **ipconfig /renew**.
4. Чтобы проверить обновленные параметры, введите в командной строке **ipconfig /all**.

Ближе к реальности Если вы перед попыткой обновления не освободите старые параметры DHCP, запрос на обновление будет направлен в сеть, к которой компьютер был подключен в последнее время. При «переезде» в другую сеть попытка подключиться к серверу, ранее назначавшему параметры DHCP, может оказаться неудачной.

Если на компьютере установлено несколько сетевых адаптеров, то для работы только с одним или с выбранными адаптерами нужно после команды ipconfig /renew или ipconfig /release указать полное или частичное имя подключения. В качестве символа подстановки для любых знаков используются звездочка (*). Например, для обновления аренды всех подключений с именами, начинающимися на Loc, достаточно ввести команду ipconfig /renew Loc*. Для освобождения параметров всех подключений со словом Network, введите команду ipconfig /release *Network*.

Регистрация и очистка DNS

Кеш распознавателя DNS обслуживает историю просмотров DNS, выполненных во время обращения пользователя к сетевым ресурсам при помощи TCP/IP. В кеше содержатся как прямые просмотры, разрешающие имя узла в IP-адрес, так и обратные просмотры, то есть разрешение IP-адреса в имя узла. После попадания элемента DNS для конкретного узла в кеш распознавателя на локальном компьютере отпадает необходимость в запросе информации DNS об этом узле, хранящейся на внешних серверах. Это позволяет разрешать запросы DNS локально и ускоряет отклик.

Время, в течение которого элементы хранятся в кеше распознавателя, зависит от значения параметра TTL (Time to Live), заданного для записи на исходном сервере. Для просмотра текущих записей и остатка TTL для каждой записи, введите в командной строке с повышенными полномочиями команду **ipconfig /displaydns**. В отображенных значениях приведено количество секунд, в течение которых запись остается в кеше перед истечением срока ее действия. Когда значение TTL в результате обратного отсчета достигает 0, срок действия записи истекает и она удаляется из кеша.

Иногда кеш распознавателя нужно очищать принудительно, удаляя старые записи. Это позволит компьютеру проверить обновления DNS до истечения срока действия и очистки. Обычно это нужно при изменении IP-адресов серверов, когда текущие записи кеша распознавателя указывают на их старые адреса. Иногда сам кеш распознавателя рассинхронизируется, особенно после неправильной настройки DHCP.

Ближе к реальности Опытные администраторы за несколько недель до изменения DNS-записей начинают снижать значения TTL с нескольких дней (недель) до нескольких часов. Это позволяет быстрее распространять изменения на компьютеры, в кешах которых сохранены соответствующие DNS-записи. После применения изменений администратор восстанавливает исходные значения TTL, чтобы сократить количество запросов на обновление.

В большинстве случаев устранить проблему с кешем распознавателя DNS помогает очистка или повторная регистрация DNS. При сбросе кеша из него удаляются все DNS-записи, а новые не создаются до очередного про-

смотра конкретного узла и IP-адреса. В ходе повторной регистрации DNS в Windows 7, производится попытка обновления всей текущей аренды DHCP, после чего выполняется просмотр каждой DNS-записи в кеше распознавателя. При повторном просмотре каждого узла или IP-адреса происходит обновление и повторная регистрация записей кеша распознавателя. Как правило, выполняют полную очистку кеша, после чего компьютер по мере надобности выполняет просмотры. Перерегистрация DNS нужна только тогда, когда есть подозрение на сбои в DHCP и кеше распознавателя.

Чтобы сбросить и повторно зарегистрировать записи в кеше распознавателя DNS при помощи команды Ipconfig, выполните следующие действия:

1. Откройте командную строку с повышенными полномочиями.
2. Для очистки кеша распознавателя введите в командной строке **ipconfig /flushdns**.
3. Чтобы обновить аренду DHCP и повторно зарегистрировать DNS-записи, введите в командной строке **ipconfig /registerdns**.
4. По завершению проверьте результат, введя в командной строке **ipconfig /displaydns**.

Глава 16

Управление мобильными сетями и удаленным доступом

Довольно часто пользователю бывает нужно подключиться к сети своей организации с компьютера, находящегося вне рабочего места. Для этого необходимо подключение удаленного доступа, широкополосное соединение, подключение через виртуальную частную сеть (VPN) или подключение прямого доступа (DirectAccess). Удаленный доступ позволяет подключить компьютер к сети организации, используя модем и стандартную телефонную линию. Широкополосное соединение позволяет подключаться к сети организации, используя маршрутизаторы DSL или кабельные модемы. Соединения VPN и DirectAccess при помощи шифрования обеспечивают безопасное соединение через существующее подключение, которое может быть подключением по локальной сети, подключением удаленного доступа или широкополосным соединением.

В настоящее время постоянно растет число используемых беспроводных подключений. При беспроводном соединении компьютеры устанавливают связь друг с другом и другими беспроводными устройствами при помощи сетевого адаптера с антенной.

Настройка сети для ноутбуков

Большинству ноутбуков требуется несколько сетевых конфигураций: одна для офиса, одна для дома и, возможно, еще одна для использования в поездках. В офисе ноутбук использует динамический IP-адрес и настройки сети, присваиваемые DHCP-сервером. Дома ноутбуку назначен статический IP-адрес и другие сетевые параметры, позволяющие получить доступ к общему принтеру и широкополосному подключению к Интернету. В некоторых случаях необходимо настроить на ноутбуке беспроводное подключение со статической IP-конфигурацией для случаев, когда пользователь находится не на рабочем месте, и с конфигурацией DHCP для случаев, когда ноутбук физически подключен к сети (или наоборот). Если система получает основные настройки сети от DHCP, вы вольны конфигурировать альтернативные параметры для случаев, когда DHCP-сервер недоступен, например, когда пользо-

ватель находится в поездке или дома. Альтернативная конфигурация может задействоваться как автоматически, так и по указанию пользователя. При работе в конференц-залах или в поездке пользователям ноутбуков часто требуется подключение к проектору. С этой задачей вам поможет справиться мастер Подключение к сетевому проектору (Connect To A Network Projector).

Работа с центром мобильности Windows

В Центре мобильности Windows (Windows Mobility Center) сосредоточены элементы для управления настройками мобильного ПК. Он состоит из набора панелей, обеспечивающих быстрый доступ к основным параметрам мобильного ПК. На ноутбуке или планшетном ПК для получения доступа к Центру мобильности Windows нужно щелкнуть правой кнопкой значок **Питание (Power)** в области уведомлений на панели задач и затем выбрать **Центр мобильности (Mobility Center)**. Можно также последовательно щелкнуть кнопку **Пуск (Start)** и команды **Панель управления (Control Panel)**, **Оборудование и звук (Hardware And Sound)**, **Центр мобильности Windows (Windows Mobility Center)**.

Панели Центра мобильности Windows позволяют регулировать самые разнообразные настройки мобильного ПК: при помощи бегунка настраивать яркость дисплея, выбирать в списке план электропитания при помощи кнопки включать и выключать настройки презентации. Набор доступных вкладок зависит от типа мобильного ПК и производителя, но наиболее распространены следующие вкладки:

- **Состояние батареи (Battery Status)** Показывает состояние аккумулятора компьютера. Выберите в списке нужную схему питания. Если вы создали собственный план управления питанием, он также будет включен в этот список.
- **Яркость (Brightness)** Позволяет управлять яркостью дисплея. Если яркость поддается настройке, используйте бегунок для ее регулировки.
- **Внешний дисплей (External Display)** Позволяет подключать дополнительный дисплей, который может потребоваться для проведения презентации. Щелкните кнопку **Подключить дисплей (Connect Display)**, чтобы подключиться к дополнительному дисплею, подключенному к компьютеру при помощи кабеля.
- **Параметры презентации (Presentation Settings)** Позволяет вам включать и отключать режим презентации. В режиме презентации дисплей и жесткий диск мобильного ПК не переходят в спящий режим, когда компьютер неактивен. Щелкните кнопку **Включить (Turn On)**, чтобы войти в режим презентации.
- **Центр синхронизации (Sync Center)** Позволяет просматривать состояние синхронизации файла и инициировать синхронизацию. Щелкните кнопку **Параметры синхронизации (Sync)**, чтобы начать новую синхронизацию с использованием центра синхронизации.

- **Громкость (Volume)** Позволяет управлять текущей настройкой громкости. Если на компьютере допускается регулировка звука, используйте для его регулировки бегунок.
- **Беспроводное подключение (Wireless Network)** Позволяет просматривать состояние беспроводного сетевого подключения и управлять им. Щелкните кнопку **Включить беспроводную связь (Turn Wireless On)**, чтобы активировать беспроводное подключение.

Большинство производителей ноутбуков и планшетных ПК дополняют Центр мобильности Windows своими контрольными окнами для того, чтобы расширить общие опции. Например, в некоторых ноутбуках HP имеется панель **HP Wireless Assistant**, которая применяется для настройки встроенного беспроводного устройства.

Настройка динамических IP-адресов

DHCP позволяет централизовано управлять IP-адресами и настройками TCP/IP. Если в сети имеется DHCP-сервер, вы можете назначить динамический IP-адрес любому сетевому адаптеру компьютера. После этого основную информацию, необходимую для работы в сетях TCP/IP, вы будете получать от DHCP-сервера. Настройка DHCP для адресов IPv4 и IPv6 осуществляется раздельно.

Чтобы настроить динамическую IP-адресацию, выполните следующие действия:

1. В панели управления щелкните категорию **Сеть и Интернет (Network And Internet)**, а затем щелкните **Центр управления сетями и общим доступом (Network And Sharing Center)**.
2. В левой панели Центра управления сетями и общим доступом (Network And Sharing Center) щелкните ссылку **Изменение параметров адаптера (Change Adapter Settings)**.
3. В окне **Сетевые подключения (Network Connections)** показаны все сетевые подключения, настроенные на компьютере. Правой кнопкой щелкните подключение, которое хотите настроить, и выберите команду **Свойства (Properties)**.
4. Дважды щелкните элемент **Протокол Интернета версии 4 (TCP/IPv4) (Internet Protocol Version 4 (TCP/IPv4))**. Откроется диалоговое окно свойств протокола, показанное на рис. 16-1.
5. Установите переключатель **Получить IP-адрес автоматически (Obtain An IP Address Automatically)**. При необходимости установите переключатель **Получить адрес DNS-сервера автоматически (Obtain DNS Server Address Automatically)** или введите адрес основного и альтернативного DNS-серверов в соответствующие поля.
6. Щелкните **OK**.
7. Если в вашей сети используется протокол IPv6, дважды щелкните элемент **Протокол Интернета версии 6 (TCP/IPv6) (Internet Protocol Ver-**

sion 6 (TCP/IPv6)). Установите переключатель **Получить IPv6-адрес автоматически (Obtain An IPv6 Address Automatically)**. При необходимости установите переключатель **Получить адрес DNS-сервера автоматически (Obtain DNS Server Address Automatically)** или введите адрес основного и альтернативного DNS-серверов в соответствующие поля. Затем щелкните **OK**.

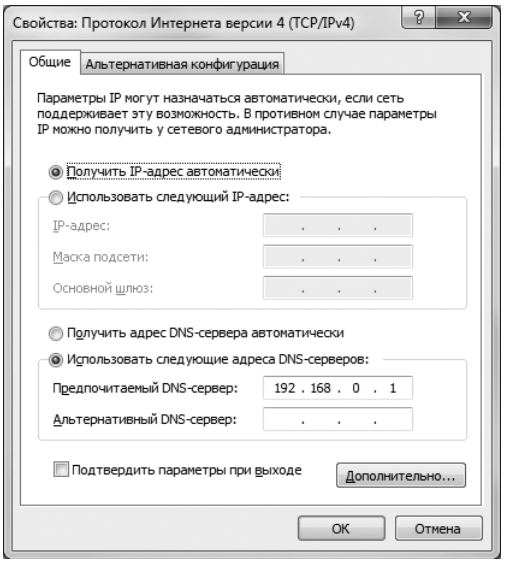

Рис. 16-1. Настройте компьютер на автоматическое получение IP-адреса

8. Настройте альтернативные IP-адреса, как описано в следующем разделе.

Настройка альтернативного частного IP-адреса

Альтернативные конфигурации применяются только в подключениях по протоколу IPv4. При использовании DHCP для подключения IPv4 компьютеру присваивается автоматический частный IP-адрес, если к DHCP-серверу нет доступа во время загрузки или если истек срок аренды текущего IP-адреса. Автоматический частный IP-адрес находится в диапазоне от 169.254.0.1 до 169.254.255.254 с маской подсети 255.255.0.0. Поскольку в конфигурацию автоматического частного IP-адреса не входят адреса основного шлюза, DNS-сервера и WINS-сервера, компьютер, использующий альтернативное назначение IP-адресов, изолирован в отдельном сегменте сети в указанном диапазоне.

Если вы хотите, чтобы при отсутствии доступа к DHCP-серверам на компьютере использовался конкретный IP-адрес и параметры сети, настройте альтернативную конфигурацию. Одним из ключевых вариантов использования альтернативной конфигурации является обслуживание пользователей ноутбуков, которые берут компьютеры домой. В этом случае ноутбук пользователя может быть настроен на использование динамического IP-адреса

на работе и альтернативного IP-адреса дома. Перед началом настройки уточните у пользователя параметры его домашней сети, включая IP-адрес, шлюз и адрес DNS-сервера, предоставленные Интернет-провайдером.

Для настройки альтернативного частного IP-адреса выполните следующие действия:

1. В панели управления щелкните категорию **Сеть и Интернет (Network And Internet)**, а затем щелкните **Центр управления сетями и общим доступом (Network And Sharing Center)**.
2. В левой панели Центра управления сетями и общим доступом (Network And Sharing Center) щелкните ссылку **Изменение параметров адаптера (Change Adapter Settings)**.
3. В окне **Сетевые подключения (Network Connections)** щелкните правой кнопкой нужное подключение и выберите команду **Свойства (Properties)**.
4. Дважды щелкните элемент **Протокол Интернета версии 4 (TCP/IPv4) (Internet Protocol Version 4 (TCP/IPv4))**, чтобы открыть диалоговое окно свойств протокола.
5. Перейдите на вкладку **Альтернативная конфигурация (Alternate Configuration)**, показанную на рис. 16-2.

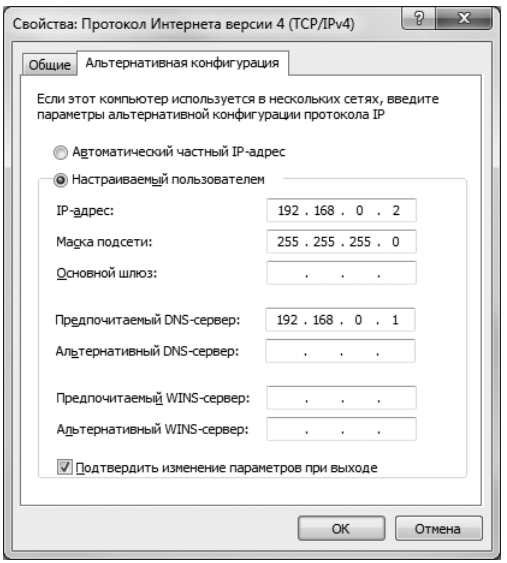

Рис. 16-2. Настройка альтернативной конфигурации IP

6. Установите переключатель **Настраиваемый пользователем (User Configured)**. Затем введите в поле **IP-адрес (IP Address)** нужный адрес. Это должен быть частный IP-адрес, который в момент применения настроек нигде более не используется. Как правило, частные IP-адреса находятся в диапазоне от 10.0.0.1 до 10.255.255.254, от 172.16.0.1 до 172.31.255.254

или от 192.168.0.1 до 192.168.255.254 (за исключением IP-адресов, зарезервированных для идентификаторов сети и широковещательных рассылок).

7. Чтобы компьютер должным образом работал в сети, в поле **Маска подсети (Subnet Mask)** должно стоять правильное значение. В Windows 7 значение маски подсети подставляется автоматически. Если в сети не используются подсети, значения по умолчанию будет вполне достаточно. Если же в сети используются подсети, вам необходимо изменить это значение соответственно требованиям сети.
8. Если компьютеру нужен доступ к другим сетям TCP/IP, Интернету или другим подсетям, укажите адрес основного шлюза в поле **Основной шлюз (Default Gateway)**.
9. Укажите адреса основного и альтернативного DNS-серверов.
10. Если для совместимости с предыдущими версиями Windows в сети используется WINS, укажите адреса основного и альтернативного WINS-серверов.
11. Закончив настройку, дважды щелкните **OK**, затем щелкните кнопку **Закрыть (Close)**.

Подключение к сетевому проектору

Во многих конференц-залах и комнатах для переговоров имеются сетевые проекторы, используемые для проведения презентаций. Чтобы использовать подобный проектор, вы должны подключить компьютер к локальной сети, а затем получить доступ к проектору по сети, используя мастер Подключение к сетевому проектору (Connect To A Network Projector). Мастер произведет поиск проекторов и установит подключение.

Чтобы запустить мастер Подключение к сетевому проектору (Connect To A Network Projector), выполните следующие действия:

1. Щелкните кнопку **Пуск (Start)** и выберите команды **Все программы (All Programs)**, **Стандартные (Accessories)** и **Подключение к сетевому проектору (Connect To A Network Projector)**.
2. Если ранее вы не подключались к сетевым проекторам и у вас включен брандмауэр Windows, выберите команду **Разрешить сетевому проектору обмениваться данными с моим компьютером (Allow The Network Projector To Communicate With My Computer)**. Это позволит сетевому проектору подключаться к компьютеру через брандмауэр Windows.
3. Если вы хотите выбрать один из проекторов, обнаруженных в локальной сети, то выберите команду **Выполнить поиск проектора (Search For A Projector)**. Мастер произведет поиск проекторов в сети и выведет их список, а также список проекторов, которые вы недавно использовали. Выберите нужный проектор, который при необходимости введите пароль доступа к проектору и щелкните **Далее (Next)**.

4. Если вы знаете сетевой адрес проектора, щелкните команду **Введите сетевой адрес проектора (Enter The Projector Network Address)**. На одноименной странице введите адрес проектора, например **http://intranet.cpandl.local/projectors/confb-proj1**. Введите пароль доступа и щелкните кнопку **Подключить (Connect)**.
5. Установив подключение к проектору, щелкните кнопку **Готово (Finish)**, чтобы выйти из мастера и начать работу с проектором.

Мобильные сети и удаленный доступ

Подключения удаленного доступа, широкополосные подключения, подключения VPN и DirectAccess позволяют пользователям получать доступ к сети организации извне. При этом технологии, лежащие в основе этих способов, фундаментально различаются. В обычной конфигурации подключения удаленного доступа пользователи, находящиеся вне организации, при помощи модема и обычной телефонной линии подключаются к пулу модемов, размещенному в офисе. Сервер Windows, управляющий модемным пулом, на котором запущена служба Маршрутизация и удаленный доступ (Routing And Remote Access), проверяет имя входа и пароль и разрешает пользователю подключиться к внутренней сети. После этого пользователь получит доступ к сетевым ресурсам, как если бы находился на рабочем месте.

На рис. 16-3 проиллюстрировано подключение удаленного доступа с использованием модемных пулов. Аналоговый модем посредством выделенной телефонной линии подключает пользователя к внутренней сети на скорости до 33,6 килобит в секунду (кбит/сек) на линию. Цифровые модемы по каналам T1 подключают пользователя к внутренней сети на скорости до 56 кбит/сек на линию. В стандартной конфигурации в модемный пул может входить 8, 12 или 16 модемов с собственной линией (или каналом) у каждого. Как правило, у модемного пула есть ведущий номер, на который могут звонить пользователи. Этот номер осуществляет подключение к первому модему пула. Если ведущий номер занят, линия переходит на следующий номер и т. д., что позволяет пользователю набирать один номер для получения доступа ко всем модемам пула.

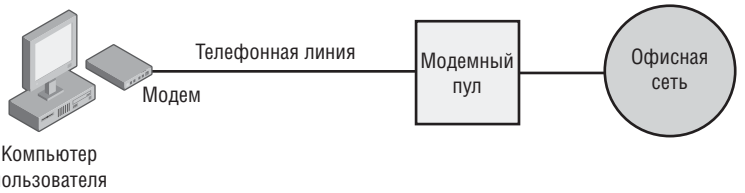

Рис. 16-3. Использование удаленного доступа для подключения к офисной сети через модемный пул

В отличие от подключений с прямым набором номера, которые производятся напрямую к офисной сети, широкополосные подключения произво-

дятся через сеть Интернет-провайдера. DSL-маршрутизатор пользователя, кабельный модем или сотовый модем устанавливают соединение с провайдером, который в свою очередь подключает пользователя к Интернету. Для подключения к офисной сети пользователь с широкополосным соединением должен установить подключение VPN или DirectAccess между своим компьютером и офисной сетью. На рис.16-4 показан принцип работы сетей VPN и DirectAccess.

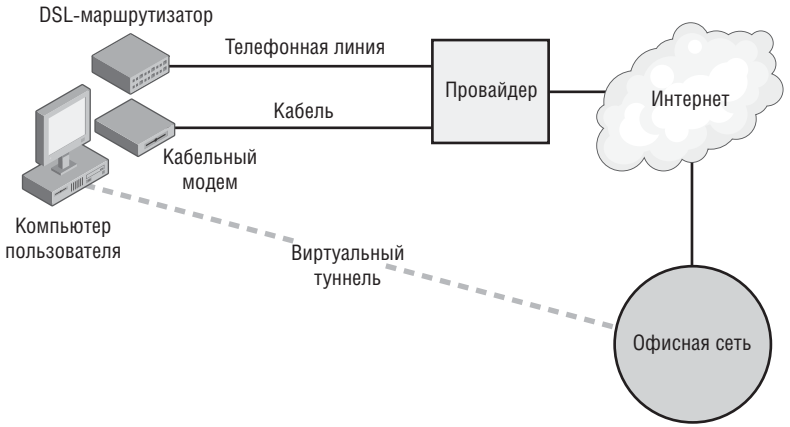

Рис. 16-4. Использование виртуальных туннелей для получения доступа к офисной сети

Виртуальная частная сеть VPN — это расширение закрытой сети по каналам Интернета. После подключения пользователь напрямую подключен к офисной сети и может получать доступ к сетевым ресурсам, как если бы находился на своем рабочем месте. Такое «гладкое» подключение возможно благодаря созданию виртуального туннеля между компьютером пользователя и офисной сетью. Технология VPN обеспечивает маршрутизацию информации через Интернет. Как правило, используется одна из двух технологий VPN — протокол PPTP (Point-to-Point Tunneling Protocol) или протокол L2TP (Layer 2 Tunneling Protocol).

Оба протокола обеспечивают шифрование и защиту от атак, но в протоколе L2TP для расширенного шифрования используется технология IPSec, что делает его более безопасным. К сожалению, L2TP сложнее настраивать. При использовании L2TP необходимо использовать службы сертификации Майкрософт или сервер сертификатов сторонних производителей для выдачи индивидуального сертификата каждой системе, которая будет подключаться к сети.

Сети VPN можно использовать не только с широкополосным подключением, но и с подключением удаленного доступа. В этой конфигурации, как показано на рис. 16-4, пользователи подключаются к Интернету через своего провайдера, а затем устанавливают частное подключение к офисной сети. Когда эта конфигурация станет стандартной практикой для пользователей, пользующихся подключением удаленного доступа, у вашей организации не

будет необходимости в выделенных частных линиях, наподобие тех, что зарезервированы для модемного пула.

Технология DirectAccess — это новый подход к виртуальному туннелированию. Хотя он фундаментально отличается от VPN, основной принцип тот же самый: подключение через DirectAccess — это продолжение частной сети через Интернет. После подключения (оно происходит автоматически после активирования функции) пользователь видит, что он напрямую подключен к офисной сети, и получает доступ к сетевым ресурсам, как если бы находился на своем рабочем месте.

Клиент-серверной технологии DirectAccess необходимы протоколы IPv6 и IPSec. При этом клиентский компьютер должен работать на Windows 7 Enterprise или выше, а серверный компьютер — на Windows Server 2008 Release 2 или выше. Чтобы использовать DirectAccess, вы должны установить и настроить IPv6-адресацию как на клиентских, так и на серверных компьютерах предприятия, включая DNSv6 и DHCPv6.

Для управления работой DirectAccess применяется политика **Маршрутизировать весь трафик через внутреннюю сеть (Route All Traffic Through The Internal Network)**, расположенная в узле **Сеть\Сетевые подключения (Network\Network Connections)** из папки **Административные шаблоны (Administrative Templates)** узла **Конфигурация компьютера (Computer Configuration)**. Когда пользователь подключен к сети на рабочем месте, его компьютер по умолчанию производит доступ к Интернет-ресурсам напрямую, а не через сеть на рабочем месте. Если вы актировали политику маршрутизации, компьютер пользователя получит доступ к Интернету через сеть на рабочем месте.

Очевидно, что у обоих подходов есть свои преимущества и недостатки. Если вы не маршрутизируете Интернет-трафик через внутреннюю сеть, то сокращаете трафик через внутреннюю сеть, но теряете дополнительную защиту, имеющуюся во внутренней сети. Если вы маршрутизируете Интернет-трафик через внутреннюю сеть, вы интенсифицируете трафик в сети на рабочем месте и, возможно, существенно увеличиваете время отклика при работе пользователя с Интернет-ресурсами, но зато с гарантией принимаете все дополнительные меры безопасности для защиты внутренней сети.

Создание подключения удаленного доступа

Как уже говорилось, для удаленного доступа к сети можно использовать как телефонное, так и широкополосное подключение. Если вам необходима дополнительная безопасность, настройте использование VPN. После включения функции DirectAccess работа в сети не требует от пользователя дополнительных усилий. Ему достаточно установить подключение к Интернету.

В Windows 7 имеется мастер для создания подобных подключений. В большинстве случаев доступ к нему получают через Центр управления сетями и общим доступом (Network And Sharing Center). Щелкните команду

Настройка нового подключения или сети (Set Up A New Connection Or Network). После этого вы сможете создать телефонное, широкополосное или VPN-подключение.

Ближе к реальности Если вы собираетесь использовать одни и те же настройки подключения на нескольких компьютерах, создайте телефонное подключение или VPN-подключение при помощи предпочтений групповой политики. Вы также можете импортировать настройки в групповую политику. В обоих случаях подключения становятся доступными для всех компьютеров, охваченных соответствующим объектом групповой политики. Вы можете использовать этот метод для развертывания новых конфигураций, редактирования существующих конфигураций и для удаления существующих конфигураций и их замены на новые.

Создание телефонного подключения

В Windows 7 есть две возможности создания телефонных подключений: телефонное подключение к провайдеру или к своему рабочему месту. Хотя подключения двух этих видов создаются с использованием несколько различающихся технологий, настройки подключения используются те же самые за следующими исключениями:

- При телефонном подключении к Интернет-провайдеру *не используется* компонент Клиент для сетей Майкрософт (Client For Microsoft Networks), а в случае сброса линии повторный набор осуществляется по умолчанию.
- При телефонном подключении к рабочему месту *используется* компонент Клиент для сетей Майкрософт (Client For Microsoft Networks), а в случае сброса линии повторный набор по умолчанию *не* осуществляется.

Сетевой компонент Клиент для сетей Майкрософт (Client For Microsoft Networks) позволяет системам Windows 7 взаимодействовать в домене Windows или в рабочей группе. Поскольку домены Windows или рабочие группы используются в большинстве офисных сетей, но лишь изредка используются Интернет-провайдерами, этот компонент конфигурируется для рабочей среды, а не для Интернет-провайдера.

Создание телефонного подключения — двусторонний процесс. Перед созданием подключения проверьте текущие параметры телефона и модема, отвечающие за режим набора. Настроив правила набора номера, вы сможете создать телефонное подключение.

Работа с правилами набора и расположениями

Правила набора используются модемами для определения процесса доступа к телефонной линии, телефонного кода абонента и дополнительных параметров, которые необходимы при подключении по телефону. Сочетания правил набора сохраняются в виде расположений в инструменте **Телефон и модем (Phone And Modem)**.

Просмотр и установка расположения по умолчанию

Чтобы посмотреть или настроить расположение по умолчанию, выполните следующие действия:

1. В панели управления выберите в списке **Просмотр (View By)** вариант **Крупные значки (Large Icons)** или **Мелкие значки (Small Icons)**.
2. Щелкните команду **Телефон и модем (Phone And Modem)**. При первом использовании этого инструмента откроется диалоговое окно **Сведения о расположении (Location Information)**, показанное на рис. 16-5.

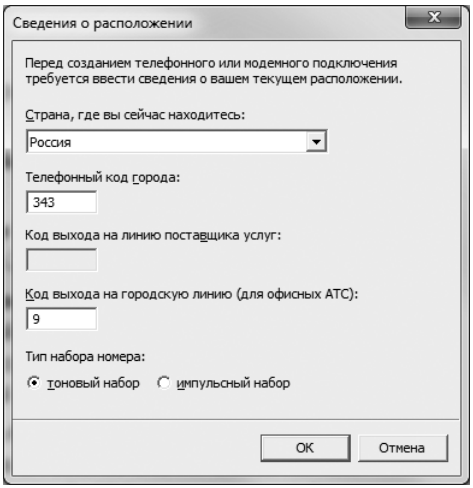

Рис. 16-5. Задайте параметры расположения

3. Задайте следующие параметры:
   - **Страна, где вы сейчас находитесь (What Country/region are You in Now?)** Выберите страну или регион, в котором находитесь, например **Россия**.
   - **Телефонный код города (What area Code (Or City Code) are You in Now?)** Введите код города или области, например 343.
   - **Код выхода на линию поставщика услуг (If You Need to Specify a Carrier Code, What is it?)** Укажите код, используемый при наборе и создании подключений. Он может понадобиться, если вы совершаете междугородний или международный звонок.
   - **Код выхода на городскую линию ()для офисных АТС (If You Dial a Number to access an Outside Line, What is it?)** Введите номер для получения доступа к внешней линии, если таковой имеется. Он может понадобиться, чтобы пройти коммутатор компании или при наборе номера из отеля.
4. Установите переключатель **Тип набора номера (The Phone System At This Location Uses)** в положение **Тоновый набор (Tone Dialing)** или **Импульсный набор (Pulse Dialing)**.
5. Настроив расположение, щелкните **OK**. Откроется диалоговое окно **Телефон и модем (Phone And Modem)**, изображенное на рис. 16-6.

   После этого вам уже не нужно будет настраивать начальное расположение.

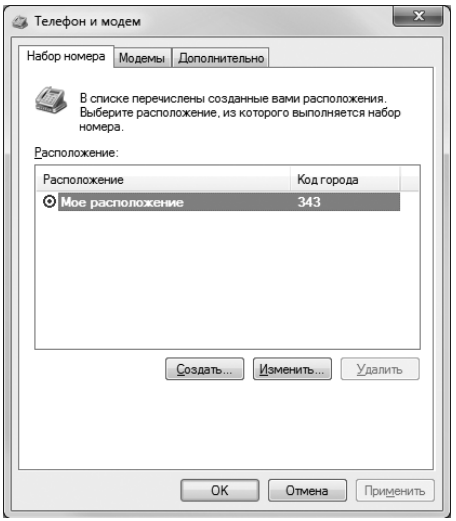

Рис. 16-6. В зависимости от расположения выбираются правила набора номера

Для настроенных расположений в списке **Расположение (Locations)** указаны имена и коды городов. Расположение, используемое в данный момент, выделяется полужирным шрифтом.

6. Исходное расположение по умолчанию называется **Мое расположение (My Location)**. Сделать текущим расположением или расположением по умолчанию можно любое другое расположение. Измените имя расположения по умолчанию так, чтобы оно включало в себя название города и расположение офиса. Для просмотра параметров выбранного расположения щелкните кнопку **Изменить (Edit)**. Чтобы переименовать расположение, введите новое имя в поле **Имя расположения (Location Name)** на вкладке **Общие (General)** и щелкните **OK**.

Примечание Из всех параметров набора чаще всего вам предстоит иметь дело с кодом региона. Часто бывает так, что код региона по умолчанию не совпадает с кодом, который необходим пользователю для осуществления звонка из дома.

Создание расположения

Расположения создаются, чтобы задать уникальные правила набора номера для каждого региона, из которого пользователь производит телефонные подключения. Чтобы создать расположение, выполните следующие действия:

1. В панели управления выберите в списке **Просмотр (View By)** вариант **Крупные значки (Large Icons)** или **Мелкие значки (Small Icons)**.
2. Щелкните категорию **Телефон и модем (Phone And Modem)**. В одноименном диалоговом окне на вкладке **Набор номера (Dialing Rules)** щелкните кнопку **Создать (New)**. Откроется диалоговое окно **Новое расположение (New Location)**.
3. Введите параметры на трех вкладках:

- **Общие (General)** Имя расположения, страна (регион) и код города. На этой вкладке также задаются номера доступа к внешним линиям для местных и междугородних звонков, удержание вызова и режим набора (тоновый или импульсный). Выберите для расположения понятное имя. Как правило, это имя города или района, откуда пользователь производит набор номера.
- **Код города (Area Code Rules)** Правила набора телефонных номеров из расположения в регионы с другими кодами и внутри расположения. Эти правила полезны, когда в одном и том же расположении используется несколько кодов.
- **Телефонная карточка (Calling Card)** Телефонная карточка, используемая при наборе из этого расположения. На этой вкладке уже есть информация для большинства поставщиков, но вы вольны создавать и собственные записи по использованию телефонной карты.

4. Создав расположение, при необходимости сделайте его расположением по умолчанию. Щелкните **OK**.

Удаление расположения

Для удаления телефонного подключения выполните следующие действия:

1. В панели управления выберите в списке **Просмотр (View By)** вариант **Крупные значки (Large Icons)** или **Мелкие значки (Small Icons)**. Щелкните категорию **Телефон и модем (Phone And Modem)**.
2. В одноименном диалоговом окне выберите расположение, которое хотите удалить, и щелкните кнопку **Удалить (Delete)**. Подтвердите действие, щелкнув **Да (Yes)**.
3. Выберите новое расположение по умолчанию и щелкните **OK**.

Создание телефонного подключения к провайдеру Интернета

Создать телефонное подключение можно следующими способами:

- У некоторых Интернет-провайдеров точки доступа имеются в различных городах, поэтому можно настроить правила набора для конкретного расположения. Например, вы можете создать расположение «Екатеринбург» и телефонное подключение **Подключить к Интернет-провайдеру в Екатеринбурге**, указав телефонный код Екатеринбурга, а также местный номер доступа к Интернет-провайдеру. Покажите пользователям, как изменять текущее расположение для случаев, когда они переезжают из одного места в другое.
- Если пользователи набирают номер с кодом 800 или междугородным кодом, чтобы получить доступ к офисному модемному пулу или Интернет-провайдеру, вам нужно настроить отдельные подключения, а не отдельные расположения. В этом случае можно создать подключение для междугородных звонков и подключение, которое будет использоваться, когда пользователь находится в местной зоне. При этом вам потребуется только одно расположение.

Чтобы создать телефонное подключение к Интернету, выполните следующие действия:

1. Проверьте текущие параметры телефона и модема, как описано в разделе ранее в этой главе.

Примечание Если для подключения вы используете правила набора, а затем задаете коды страны и региона, для подключения будут использоваться междугородные вызовы, которые зачастую обходятся недешево. Если вас это не устраивает, попробуйте подобрать другой вариант подключения.

2. В Центре управления сетями и общим доступом (Network And Sharing Center) выберите команду **Настройка нового подключения или сети (Set Up A New Connection Or Network)**. Будет запущен мастер Установка подключения или сети (Set Up A Connection Or Network).
3. Выберите команду **Настройка телефонного подключения (Set Up A Dial-Up Connection)** и щелкните **Далее (Next)**.
4. В поле **Набираемый номер (Dial-Up Phone Number)** введите телефонный номер, набираемый для этого подключения.
5. Введите информацию об учетной записи для подключения: имя пользователя и пароль. Чтобы не вводить пароль в будущем, установите флажок **Запомнить этот пароль(Remember This Password)**. Помните, что это существенно снижает уровень безопасности, поскольку использовать подключение сможет любой пользователь, получивший доступ к компьютеру.
6. В поле **Имя подключения (Connection Name)** введите имя подключения, например **Поставщик услуг**. Помните, что имя должно быть коротким (не более 50 символов), но ясным.
7. Чтобы подключение было доступно всем пользователям компьютера, установите флажок **Разрешить использовать это подключение другим пользователям (Allow Other People To Use This Connection)**. Это удобно, если вы планируете предоставлять подключение через групповую политику и не ввели учетные данные пользователя для входа в систему.
8. Щелкните кнопку **Создать (Create)** для создания телефонного подключения. Чтобы протестировать параметры соединения, выполните действия, описанные в разделе «Установка подключения» далее в этой главе.

Ближе к реальности В большинстве организаций используются цифровые телефонные системы, которые не позволяют создавать аналоговое подключение ко внешней линии. В этом случае перед тестированием подключения вам необходимо будет получить доступ к аналоговой линии. Некоторые цифровые телефоны оборудованы цифроаналоговыми преобразователями, которые можно использовать для тестирования телефонных подключений. В некоторых случаях эти преобразователи используются для селекторных телефонов и факсов. В других случаях селекторные телефоны и факсы сами подключены к аналоговым телефонным линиям.

Создание телефонного подключения к рабочему месту

Создание телефонного подключения к рабочему месту аналогично созданию телефонного подключения к Интернету. Выполните следующие действия:

1. В Центре управления сетями и общим доступом (Network And Sharing Center) выберите команду **Настройка нового подключения или сети (Set Up A New Connection Or Network)**. Будет запущен мастер Установка подключения или сети (Set Up A Connection Or Network).
2. Выберите команду **Подключение к рабочему месту (Connect To A Workplace)** и щелкните **Далее (Next)**.
3. На странице **Как выполнить подключение (How Do You Want To Connect)** выберите команду **Использовать прямой набор номера (Dial Directly)**.
4. Укажите номер телефона, который нужно набирать для этого подключения, в поле **Номер телефона (Telephone Number)**. В поле **Имя местоназначения (Destination Name)** введите имя подключения, например **Основной офис**. Помните, что имя должно быть коротким (не более 50 символов), но ясным.
5. Если вы хотите, чтобы подключение было доступно всем пользователям компьютера, установите флажок **Разрешить использовать это подключение другим пользователям (Allow Other People To Use This Connection)**. Это удобно, если вы планируете предоставлять подключение через групповую политику и не ввели учетные данные пользователя для входа в систему.
6. Если вы хотите использовать для соединения смарт-карту, установите флажок **Использовать смарт-карту (Use A Smart Card)**.
7. Щелкните **Далее (Next)**. Введите имя пользователя и пароль для подключения. Чтобы сохранить пароль в памяти, установите флажок **Запомнить этот пароль (Remember This Password)**, но это существенно снижает безопасность, поскольку использовать это соединение сможет любой пользователь, получивший доступ к компьютеру.
8. Если вы подключаетесь к домену, укажите его имя в поле **Домен (Domain)**.
9. Щелкните кнопку **Подключить (Connect)**, чтобы создать подключение и подключить его. Скорее всего, попытка подключения закончится сбоем, поскольку вы устанавливаете его для альтернативного расположения, например, для домашнего подключения пользователя к Интернету, и в сети организации эти настройки работать не будут. Щелкните кнопки **Пропустить (Skip)** и **Закрыть (Close)**.

Чтобы создавать, редактировать и удалять телефонные подключения в групповой политике, выполните следующие действия:

1. Откройте объект групповой политики для редактирования. Чтобы настроить предпочтения для компьютера, разверните узел **Конфигурация компьютера\Настройка\Параметры панели управления (Computer Configuration\Preferences\Control Panel Settings)** и выделите элемент **Сетевые параметры (Network Options)**. Чтобы настроить предпочтения для пользователя, разверните узел **Конфигурация пользователя\На-**

стройка\Параметры панели управления (User Configuration\Preferences\Control Panel Settings) и выделите элемент **Сетевые параметры (Network Options)**.

2. Щелкните узел **Сетевые параметры (Network Options)** правой кнопкой, разверните подменю **Создать (New)** и выберите команду **Подключение удаленного доступа (Dial-Up Connection)**.
3. В списке **Действие (Action)** выберите вариант **Создать (Create)**, **Обновить (Update)** или **Заменить (Replace)**.
4. Чтобы подключение было доступно всем пользователям компьютера, установите переключатель **Подключения всех пользователей (Allow Users Connection)**. Установите переключатель **Подключение пользователя (User Connection)**, чтобы применять подключение только для того пользователя, для которого обрабатывается политика.
5. Введите имя подключения и телефонный номер.
6. На вкладке **Общие параметры (Common)** задайте способ применения предпочтений. Как правило, достаточно применить эту политику только один раз, поэтому установите флажок **Применить один раз и не применять повторно (Apply Once And Do Not Reapply)**.
7. Щелкните **OK**. При следующем обновлении групповой политики предпочтение будет применено в составе объекта групповой политики, в котором оно определено.

Создание широкополосного подключения к Интернету

Настройка широкополосного подключения во многом проще, чем настройка телефонных подключений. Вам не нужно устанавливать правила набора и расположение, не нужно беспокоиться о телефонных картах, номерах доступа к Интернет-провайдеру или параметрах повторного набора. Именно поэтому с широкополосным соединением легче работать.

Большинство поставщиков широкополосного подключения предоставляют пользователю DSL-маршрутизатор или модем. Пользователю также необходим сетевой адаптер на компьютере, подключенный к DSL-маршрутизатору или кабельному модему. В этой конфигурации необходимое соединение устанавливается через локальную сеть, а не через конкретное широкополосное подключение. Поэтому, чтобы получить доступ к Интернету, необходимо правильно настроить локальное подключение. Создавать отдельное широкополосное подключение нет необходимости.

Тем не менее, если нужно, вы вольны создать конкретное широкополосное подключение. В некоторых случаях это приходится делать, чтобы задать конкретные параметры, например безопасную проверку подлинности, или указать имя пользователя и пароль, запрашиваемые провайдером соединения.

Чтобы создать широкополосное подключение к Интернету, выполните следующие действия:

1. В Центре управления сетями и общим доступом (Network And Sharing Center) выберите команду Настройка нового подключения или сети (Set Up A New Connection Or Network). Будет запущен мастер Установка подключения или сети (Set Up A Connection Or Network).
2. Выберите команду **Подключение к Интернету (Connect To The Internet)** и щелкните **Далее (Next)**.
3. На странице **Как выполнить подключение (How Do You Want To Connect)** выберите вариант **Высокоскоростное (PPPoE) (Broadband (PPPoE))**.
4. Выполните следующие действия, а затем щелкните **Далее (Next)**:
   - Введите имя пользователя и пароль для подключения. Чтобы сохранить пароль в памяти, установите флажок **Запомнить этот пароль (Remember This Password)**, но это существенно снижает безопасность, поскольку использовать это подключение сможет любой пользователь, получивший доступ к компьютеру.
   - В поле **Имя подключения (Connection Name)** введите имя подключения, например **Защищенное подключение к офису**. Помните, что имя должно быть коротким (не более 50 символов), но ясным.
   - Чтобы подключение было доступно всем пользователям компьютера, установите флажок **Разрешить использовать это подключение другим пользователям (Allow Other People To Use This Connection)**. Это удобно, если вы планируете предоставлять подключение через групповую политику и не ввели учетные данные пользователя для входа в систему.
5. Выберите команду **Подключить (Connect)**, чтобы создать подключение и подключить его. В большинстве случае сделать это не удастся, поскольку вы настраиваете подключение для альтернативного расположения, например, удаленного офиса, и в сети организации эти настройки не будут работать. Щелкните **Пропустить (Skip)** и **Закрыть (Close)**.

Совет Для тестирования широкополосного подключения вам потребуется DSL-маршрутизатор или кабельный модем. Убедитесь, что настроили все параметры, запрашиваемые Интернет-провайдером, как описано в разделе «Настройка свойств подключения» далее в этой главе.

Создание VPN-подключения

Соединения VPN используются для создания безопасных каналов связи по существующим телефонным или широкополосным подключениям. Вы должны знать IP-адрес или полное доменное имя сервера удаленного доступа, к которому подключаетесь. Если необходимое соединение доступно и вы располагаете данными главного компьютера, вы можете создать подключение, выполнив следующие действия:

1. В Центре управления сетями и общим доступом (Network And Sharing Center) щелкните **Настройка нового подключения или сети (Set Up A New Connection Or Network)**. Будет запущен мастер Установка подключения или сети (Set Up A Connection Or Network).

2. Выберите команду **Подключение к рабочему месту (Connect To A Workplace)** и щелкните **Далее (Next)**. Помните, что пользователю необходимо установить телефонное или широкополосное подключение к Интернету, прежде чем использовать VPN.
3. Выберите команду **Использовать мое подключение к Интернету (VPN) (Use My Internet Connection (VPN))**.
4. Введите адрес IPv4 или IPv6 или полное доменное имя компьютера, к которому вы подключаетесь, например **157.54.0.1** или **external.microsoft.com**. В большинстве случаев это адрес сервера удаленного доступа, настроенного в офисной сети.
5. Введите имя подключения в поле **Имя местоназначения (Destination Name)**. Если на компьютере настроена проверка подлинности при помощи смарт-карты, установите флажок **Использовать смарт-карту (Use A Smart Card)**.
6. Чтобы подключение было доступно всем пользователям компьютера, установите флажок **Разрешить использовать это подключение другим пользователям (Allow Other People To Use This Connection)**. Это удобно, если вы планируете предоставлять подключение через групповую политику и не ввели учетные данные пользователя для входа в систему.
7. Щелкните **Далее (Next)**. Когда пользователь производит подключение, ему по умолчанию предлагается ввести имя и пароль. Если вы создаете подключение для конкретного пользователя и хотите, чтобы ему не нужно было вводить свои данные для входа в систему, введите здесь имя пользователя и пароль. В противном случае введите только имя пользователя, а поле пароля оставьте незаполненным.
8. Чтобы сохранить пароль в памяти, установите флажок **Запомнить этот пароль (Remember This Password)**, однако это существенно снижает уровень безопасности, поскольку использовать подключение сможет любой пользователь, получивший доступ к компьютеру.
9. Укажите домен, поверяющий подлинность пользователя, в поле **Домен (Domain)** и щелкните кнопку **Подключить (Connect)**. Чтобы подключиться к VPN-подключению, вы сначала должны осуществить телефонное или широкополосное соединение, как описано выше. В большинстве случаев подключение будет безуспешным, поскольку вы устанавливаете VPN-подключение для альтернативного расположения, например, домашнего соединения пользователя, и эти настройки не будут работать в сети организации. Щелкните **Пропустить (Skip)** и **Закрыть (Close)**.

Для настройки VPN-подключения в групповой политике выполните следующие действия:

1. Откройте объект групповой политики (GPO) для редактирования. Чтобы настроить предпочтения для компьютера, разверните узел **Конфигурация компьютера\Настройка\Параметры панели управления (Computer Configuration\Preferences\Control Panel Settings)** и выделите

элемент **Сетевые параметры (Network Options)**. Чтобы настроить предпочтения для пользователя, разверните узел **Конфигурация пользователя\Настройка\Параметры панели управления (User Configuration\Preferences\Control Panel Settings)** и выделите элемент **Сетевые параметры (Network Options)**.

2. Правой кнопкой щелкните узел **Сетевые параметры (Network Options)**, разверните подменю **Создать (New)** и выберите команду **VPN-подключение (VPN Connection)**.
3. В списке **Действие (Action)** выберите вариант **Создать (Create)**, **Обновить (Update)** или **Заменить (Replace)**.
4. Чтобы подключение было доступно всем пользователям компьютера, установите переключатель **Подключение всех пользователей (Allow Users Connection)**. Установите переключатель **Подключение пользователя (User Connection)**, чтобы применить подключение только для пользователя, для которого обрабатывается политика.
5. Введите имя подключения и IP-адрес сервера или установите флажок **Использовать DNS-имя (Use DNS Name)** и введите полное доменное имя сервера.
6. На вкладке **Безопасность (Security)** установите переключатель **Дополнительные (Advanced)**. При помощи списка **Шифрование данных (Data Encryption)** укажите, будет ли использоваться шифрование, и если да, то каким именно образом. В большинстве случаев шифрование необходимо. Задайте нужные параметры в разделе **Безопасный вход (Logon Security)**.
7. На вкладке **Общие параметры (Common)** задайте способ применения предпочтений. Как правило, достаточно применить эту политику только один раз, поэтому установите флажок **Применить один раз и не применять повторно (Apply Once And Do Not Reapply)**.
8. Щелкните **OK**. При следующем обновлении групповой политики предпочтение будет применено в составе объекта групповой политики, в котором оно определено.

Настройка свойств подключения

Настройка любого подключения включает в себя задание его дополнительных свойств. В этой главе описаны ключевые параметры, с которыми вам предстоит иметь дело.

Примечание Помните, что для VPN используются существующие подключения, каждое из которых может иметь собственную конфигурацию. При работе с VPN сначала устанавливается исходное подключение с использованием параметров, назначенных этому подключению, а затем производится VPN-подключение с использованием параметров уже VPN-подключения. Сначала настройте исходное подключение, а затем подключение VPN. Эту последовательность можно изменять только при диагностике неисправностей VPN. В этом случае начните с параметров VPN и лишь затем переходите к настройкам исходного подключения.

Автоматическое и ручное подключение

Windows 7 можно настроить на автоматическое установление телефонного, широкополосного или VPN-подключения, когда пользователь запускает программы, например веб-браузер, требующие подключения к Интернету. Работа автоматических подключений зависит от настроек в окне Свойства обозревателя (Internet Options). Доступны следующие варианты:

- **Никогда не использовать коммутируемые подключения (Never Dial A Connection)** Пользователи должны устанавливать подключение вручную.
- **Использовать при отсутствии подключения к сети (Dial Whenever A Network Connection Is Not Present)** Подключение устанавливается автоматически, но только в тех случаях, когда отсутствует локальное подключение.
- **Всегда использовать принятое по умолчанию подключение (Always Dial My Default Connection)** Подключение по умолчанию устанавливается всегда, когда необходимо подключение к Интернету (даже если уже установлены другие подключения).

Совет Способ использования автоматических подключений зависит от потребностей организации. Вопреки сложившемуся у администраторов мнению, пользователи ноутбуков зачастую предпочитают, чтобы автоматическое подключение было у них отключено. Например, находясь вне офиса, пользователь может все равно не иметь доступа к этому подключению, при этом попытки компьютера установить подключение на встрече с клиентами или во время презентации могут быть нежелательны. А вот пользователи стационарных компьютеров в удаленном офисе или дома, вероятно, захотят пользоваться автоматическими подключениями.

Чтобы настроить ручное подключение компьютера, выполните следующие действия:

1. В панели управления выберите категорию **Сеть и Интернет (Network And Internet)**. Затем щелкните **Свойства обозревателя (Internet Options)**. В одноименном диалоговом окне перейдите на вкладку **Подключения (Connections)**, показанную на рис. 16-7.
2. Установите переключатель **Никогда не использовать коммутируемые подключения (Never Dial A Connection)** и щелкните **OK**.

Чтобы настроить автоматическое подключение, выполните следующие действия:

1. В панели управления выберите категорию **Сеть и Интернет (Network And Internet)**. Затем щелкните **Свойства обозревателя (Internet Options)**. В одноименном диалоговом окне перейдите на вкладку **Подключения (Connections)**.
2. Установите переключатель **Использовать при отсутствии подключения к сети (Dial Whenever A Network Connection Is Not Present)**, чтобы автоматически установить подключение, если локальное подключение не работает. Установите переключатель **Всегда использовать принятое по**

умолчанию подключение (Always Dial My Default Connection), чтобы всегда использовать данное подключение.

3. В списке **Настройка коммутируемого соединения и виртуальных частных сетей (Dial-Up And Virtual Private Network Settings)** отображаются телефонные, широкополосные и VPN-подключения, конфигурация которых доступна в данный момент. Выберите подключение, которое хотите использовать по умолчанию, и щелкните кнопку **Умолчание (Set Default)**.
4. Щелкните **OK**.

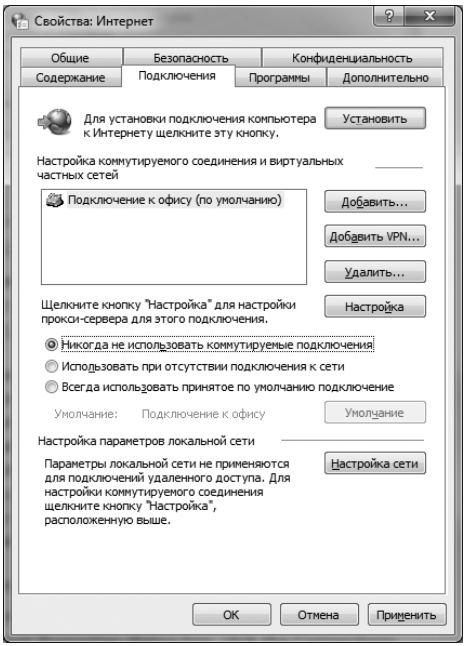

Рис. 16-7. Настройка подключений вручную и автоматически

Настройка прокси-сервера для мобильных подключений

Параметры прокси-сервера, как и сами подключения, могут устанавливаться вручную и автоматически. При настройке вручную вам придется настраивать каждое свойство. При автоматическом конфигурировании компьютер пытается обнаружить настройки прокси-сервера и затем задать соответствующие параметры или запускает конфигурационный сценарий.

Примечание Настройки прокси-сервера для нескольких систем можно задавать через групповую политику. Если вы предпочитаете настраивать прокси-серверы отдельно для каждого подключения, воспользуйтесь описанными в этом разделе способами.

Сценарии конфигурации могут храниться в файле локального компьютера или по Интернет-адресу. Использование сценариев экономит время, осо-

бенно если каждое создаваемое вами подключение настраивается отдельно. Поскольку VPN-подключения устанавливаются поверх существующего подключения, настройки прокси-сервера для VPN могут отличаться от настроек для исходного подключения.

Чтобы воспользоваться автоматической конфигурацией прокси-сервера, выполните следующие действия:

1. В панели управления выберите категорию **Сеть и Интернет (Network And Internet)**. Затем щелкните **Свойства обозревателя (Internet Options)**. В одноименном диалоговом окне перейдите на вкладку **Подключения (Connections)**.
2. В списке **Настройка коммутируемого соединения и виртуальных частных сетей (Dial-Up And Virtual Private Network Settings)** выберите подключение, которое хотите настроить, и щелкните кнопку **Настройка (Settings)**. Откроется диалоговое окно, показанное на рис. 16-8.

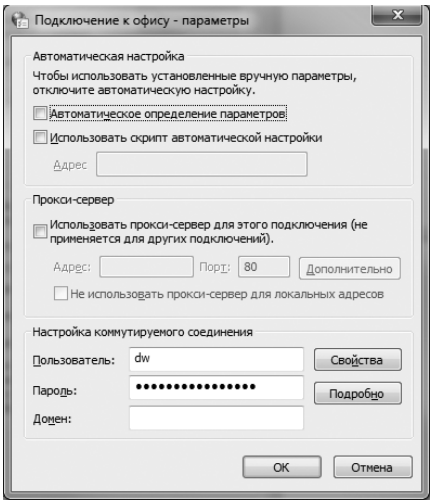

Рис. 16-8. Настройки прокси-сервера могут задаваться автоматически или при помощи сценария

3. Для автоматического обнаружения настроек прокси-сервера при установке подключения установите флажок **Автоматическое определение параметров (Automatically Detect Settings)**.
4. Для использования сценария конфигурации установите переключатель **Использовать скрипт автоматической настройки (Use Automatic Configuration Script)** и введите путь к файлу или URL сценария. Указывая путь к файлу, вы можете использовать переменные среды, например %UserProfile%\PROXY.VBS.
5. Чтобы с гарантией использовать только автоматические настройки, сбросьте флажок **Использовать прокси-сервер для этого подключения (Use A Proxy Server For This Connection)**.
6. Дважды щелкните **OK**.

Чтобы настроить прокси-сервер вручную, выполните следующие действия:

1. В панели управления выберите категорию **Сеть и Интернет (Network And Internet)**. Затем щелкните **Свойства обозревателя (Internet Options)**. В одноименном диалоговом окне перейдите на вкладку **Подключения (Connections)**.
2. В списке **Настройка коммутируемого соединения и виртуальных частных сетей (Dial-Up And Virtual Private Network Settings)** выберите подключение, которое хотите настроить, и щелкните кнопку **Настройка (Settings)**.
3. Сбросьте флажки **Автоматическое определение параметров (Automatically Detect Settings)** и **Использовать скрипт автоматической настройки (Use Automatic Configuration Script)**, если они установлены.
4. Установите флажок **Использовать прокси-сервер для этого подключения (Use A Proxy Server For This Connection)**. Флажок **Не использовать прокси-сервер для локальных адресов (Bypass Proxy Server For Local Addresses)** по умолчанию не установлен. Но в большинстве случаев вы предпочтете не использовать прокси-сервер для запросов в том же сетевом сегменте. Важно понимать, что при сброшенном флажке **Не использовать прокси-сервер для локальных адресов (Bypass Proxy Server For Local Addresses)** для получения доступа к ресурсам интрасети через прокси-сервер пользователям могут понадобиться дополнительные разрешения.
5. Щелкните кнопку **Дополнительно (Advanced)**, чтобы открыть диалоговое окно **Параметры прокси-сервера (Proxy Settings)**, показанное на рис. 16-9.

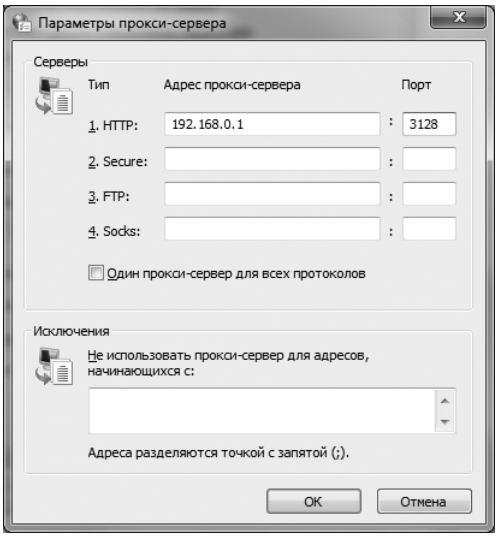

Рис. 16-9. Один и тот же прокси-сервер можно использовать для всех протоколов

6. Введите IP-адрес прокси-сервера в поля области **Серверы (Servers)**. Здесь есть два столбца:
   - **Адрес прокси-сервера (Proxy Address To Use)** IP-адрес прокси-сервера. Его можно задать индивидуально для каждого протокола. Если для конкретного протокола настраивается несколько прокси-серверов, введите их IP-адреса в том порядке, в котором веб-клиент должен пытаться их использовать. Адреса разделяются точками с запятой. Если для конкретного протокола не предполагается использование прокси-сервера, не заполняйте соответствующее поле.
   - **Порт (Port)** Введите номер порта, по которому прокси-сервер отвечает на запросы. Большинство прокси-серверов отвечают на запросы по порту 80. Стандартными портами являются порт 80 для HTTP, порт 443 для SSL, порт 21 для FTP и порт 1081 для Socks. Сверьте правильность настроек с веб-администратором.
7. Установите флажок **Один прокси-сервер для всех протоколов (Use The Same Proxy Server For All Protocols)**, чтобы использовать один и тот же IP-адрес и настройки порта для протоколов HTTP, SSL, FTP и Socks.
8. Если ваша сеть состоит из нескольких сегментов или имеются конкретные серверы, которые не должны использовать прокси-серверы, введите соответствующие IP-адреса или диапазоны IP-адресов в список **Исключения (Exceptions)**. Отделяйте вводимые записи точками с запятой. Символ * можно использовать для указания диапазона адресов от 0 до 255, например 192.*.*.*, 192.168.*.* или 192.168.10.*.
9. Трижды щелкните **ОК**.

Настройка учетных данных подключения

У каждого создаваемого вами подключения есть индивидуальные учетные данные для входа в систему. Чтобы задать имя пользователя, пароль и домен, выполните следующие действия:

1. В панели управления выберите категорию **Сеть и Интернет (Network And Internet)**. Затем щелкните **Свойства обозревателя (Internet Options)**. В одноименном диалоговом окне перейдите на вкладку **Подключения (Connections)**.
2. В списке **Настройка коммутируемого соединения и виртуальных частных сетей (Dial-Up And Virtual Private Network Settings)** выберите подключение, которое хотите настроить, и щелкните кнопку **Настройка (Settings)**.
3. Введите имя пользователя и пароль в поля **Пользователь (User Name)** и **Пароль (Password)**.
4. При необходимости введите имя домена в поле **Домен (Domain)**.
5. Дважды щелкните **ОК**.

Задание учетных данных для входа в систему — не последний шаг настройки. Вы также можете задать параметры, указывающие, будет ли поль-

зователь получать приглашение на ввод учетных данных или телефонного номера. Если для подключения требуется домен, поверяющий подлинность учетных данных, убедитесь, что его имя включено в учетные данные. По умолчанию имя домена не включается.

Чтобы настроить дополнительные параметры, выполните следующие действия:

1. В панели управления выберите категорию **Сеть и Интернет (Network And Internet)**. Затем щелкните **Свойства обозревателя (Internet Options)**. В одноименном диалоговом окне перейдите на вкладку **Подключения (Connections)**.
2. В списке **Настройка коммутируемого соединения и виртуальных частных сетей (Dial-Up And Virtual Private Network Settings)** выберите подключение, которое хотите настроить, и щелкните кнопку **Настройка (Settings)**.
3. Щелкните кнопку **Свойства (Properties)**.
4. В диалоговом окне свойств перейдите на вкладку **Параметры (Options)**. Настройте следующие параметры:
   - Чтобы отображать сообщения о ходе подключения, установите флажок **Отображать ход подключения (Display Progress While Connecting)**.
   - Чтобы пользователю выдавалось приглашение на ввод учетных данных, установите флажок **Запрашивать имя, пароль, сертификат и т. д. (Prompt For Name And Password, Certificate, Etc)**.
   - Чтобы включить домен в учетные данные, установите флажок **Включать домен входа в Windows (Include Windows Logon Domain)**.
   - Чтобы иметь возможность ввести номер телефона, установите флажок **Запрашивать номер телефона (Prompt For Phone Number)**.
5. Трижды щелкните **OK**.

Параметры повторного звонка и автоматического отключения

При использовании коммутируемых подключений можно задать автоматический повторный набор номера, если линия занята или подключение было прервано. Выполните следующие действия:

1. В панели управления выберите категорию **Сеть и Интернет (Network And Internet)**. Затем щелкните **Свойства обозревателя (Internet Options)**. В одноименном диалоговом окне перейдите на вкладку **Подключения (Connections)**.
2. В списке **Настройка коммутируемого соединения и виртуальных частных сетей (Dial-Up And Virtual Private Network Settings)** выберите подключение, которое хотите настроить, и щелкните кнопку **Настройка (Settings)**.
3. Щелкните кнопку **Свойства (Properties)**.

4. В диалоговом окне свойств перейдите на вкладку **Параметры (Options)**. Задайте следующие параметры в области **Параметры повторного звонка (Redialing Options)** и щелкните **OK**:
   - **Число попыток набора номера (Redial Attempts)** Количество попыток автоматического повторного набора телефонного номера. Для отключения повторного набора введите 0 в это поле.
   - **Интервал между попытками (Time Between Redial Attempts)** Время ожидания перед началом повторного набора. Возможные значения: 1 секунда, 3 секунды, 5 секунд, 10 секунд, 30 секунд, 1 минута, 2 минуты, 5 минут и 10 минут.
   - **Время простоя до разъединения (Idle Time Before Hanging Up)** Отключение от телефонной линии, если соединение активно не использовалось на протяжении определенного интервала времени. Возможные значения: никогда, 1 минута, 5 минут, 10 минут, 20 минут (по умолчанию), 30 минут, 1 час, 2 часа, 4 часа, 8 часов и 24 часа.
   - **Перезвонить при разрыве связи (Redial If Line Is Dropped)** Устанавливает, предпринимать ли попытки повторного набора номера, если подключение было разорвано. При подключениях к рабочему месту этот флажок обычно сброшен. Тем не менее, в большинстве случаев его следует установить.
5. В диалоговом окне параметров подключения щелкните кнопку **Подробно (Advanced)**. Установите или сбросьте флажок **Отсоединяться, когда не требуется подключение к Интернету (Disconnect When Connection May No Longer Be Needed)**, чтобы указать, нужно ли отключаться при выходе пользователя из всех программ, работающих с Интернетом.
6. Трижды щелкните **OK**.

Совет Если пользователи жалуются на неожиданные разрывы подключения, проверьте состояние флажка **Отсоединяться, когда не требуется подключение к Интернету (Disconnect When Connection May No Longer Be Needed)**. Уточните у пользователей, как они пользуются Интернетом. Возможно, вам придется изменить состояние этого флажка. Другой причиной отключения может быть флажок **Время простоя до разъединения (Idle Time Before Hanging Up)**.

Установка правил набора для подключения

Телефонные подключения могут использоваться как с применением правил набора, так и без них. Если вы не используете правила набора для подключения, во всех случаях будет набираться присвоенный подключению семизначный телефонный номер. Если вы задали применение правил набора, текущее расположение определяет, будет ли подключение выполняться как местный или как междугородный телефонный звонок.

Чтобы просмотреть правила набора для подключения, выполните следующие действия:

1. В панели управления выберите категорию **Сеть и Интернет (Network And Internet)**. Затем щелкните **Свойства обозревателя (Internet Options)**. В одноименном диалоговом окне перейдите на вкладку **Подключения (Connections)**.
2. В списке **Настройка коммутируемого соединения и виртуальных частных сетей (Dial-Up And Virtual Private Network Settings)** выберите подключение, которое хотите настроить, и щелкните кнопку **Настройка (Settings)**.
3. Щелкните кнопку **Свойства (Properties)**. Откроется диалоговое окно свойств подключения.
4. Чтобы в подключении с гарантией использовались корректные правила набора, на вкладке **Общие (General)** установите флажок **Использовать правила набора номера (Use Dialing Rules)**, а затем введите код города и код страны или региона.
5. Если вы не хотите использовать правила набора, сбросьте флажок **Использовать правила набора номера (Use Dialing Rules)**.
6. Трижды щелкните **OK**.

Настройка основных и дополнительных телефонных номеров

Для телефонного подключения можно настроить телефонные номера двух видов: основной, который будет набираться при попытке соединения, и альтернативный для случаев, когда не удастся произвести набор по основному номеру. Для настройки телефонных номеров выполните следующие действия:

1. В панели управления выберите категорию **Сеть и Интернет (Network And Internet)**. Затем щелкните **Свойства обозревателя (Internet Options)**. В одноименном диалоговом окне перейдите на вкладку **Подключения (Connections)**.
2. В списке **Настройка коммутируемого соединения и виртуальных частных сетей (Dial-Up And Virtual Private Network Settings)** выберите подключение, которое хотите настроить, и щелкните кнопку **Настройка (Settings)**.
3. Щелкните кнопку **Свойства (Properties)**. Откроется диалоговое окно свойств подключения.
4. Основной телефонный номер указан в поле **Номер телефона (Phone Number)**. При необходимости введите другой номер.
5. Щелкните кнопку **Другие (Alternates)**. Откроется диалоговое окно **Дополнительные номера телефонов (Alternate Phone Numbers)**. Задайте параметры основного и альтернативных телефонных номеров:
   - Чтобы добавить телефонный номер, щелкните **Добавить (Add)**. Откроется диалоговое окно **Добавить дополнительный номер телефона (Add Alternate Phone Number)**. Введите семизначный номер в поле **Номер телефона (Phone Number)**, при желании включив в него

дефис, например **555-1234**. Чтобы использовать правила набора, установите флажок **Использовать правила набора номера (Use Dialing Rules)**, введите код города и код страны или региона и щелкните **OK**.

- Для изменения порядка набора номеров выделите номер, а затем используйте стрелки вверх и вниз, чтобы изменить его положение в списке **Номера телефонов (Phone Numbers)**. Первый номер в списке становится основным.
- Чтобы отредактировать телефонный номер, выделите его в списке **Номера телефонов (Phone Numbers)** и щелкните кнопку **Изменить (Edit)**. Затем в диалоговом окне **Изменение дополнительного номера телефона (Edit Alternate Phone Number)** измените номер и щелкните **OK**.
- Для удаления номера выберите его в списке **Номера телефонов (Phone Numbers)** и щелкните **Удалить (Delete)**.

6. Чтобы использовать дополнительные номера автоматически, установите флажок **При отказе пытаться соединиться по следующему номеру (If A Number Fails, Try The Next Number)**. Если вы хотите автоматически делать основным успешно набранный дополнительный номер, установите флажок **Переносить успешно набранный номер в начало списка (Move Successful Numbers To Top Of The List)**.
7. Щелкните **OK** четыре раза.

Настройка проверки подлинности

Тщательная проверка подлинности важна для обеспечения безопасности сети. В случаях, когда пользователи пользуются телефонным подключением к офису, необходимо, чтобы проверка учетных данных проходила безопасно, но для стандартных телефонных подключений безопасная проверка подлинности по умолчанию не задана. Это означает, что учетные данные пользователя передаются по соединению в виде незашифрованного текста. Если вы запретите использование незашифрованных паролей, Windows 7 будет пытаться передать учетных данных с использованием безопасного метода, например, MS-CHAP Version 2 или CHAP. Вы можете также настроить использование протокола EAP (Extensible Authentication Protocol).

В телефонных и широкополосных подключениях вы можете использовать любой из этих вариантов. VPN-подключения допускают применение только безопасных методов. Если вы требуете защищенного пароля, то можете также автоматически передавать имя входа, пароль и домен Windows, указанные в конфигурации. Автоматическая передача учетных данных Windows полезна, когда пользователи подключаются к офису и должны пройти проверку подлинности в домене Windows. В обоих случаях вы можете потребовать шифрования данных и принудительно отключать соединение, если шифрование не может быть использовано. При использовании проверки подлинности Windows шифрование автоматически используется как для защищенных паролей, так и для смарт-карт.

Чтобы настроить проверку подлинности учетных данных, выполните следующие действия:

1. В панели управления выберите категорию **Сеть и Интернет (Network And Internet)**. Затем щелкните **Свойства обозревателя (Internet Options)**. В одноименном диалоговом окне перейдите на вкладку **Подключения (Connections)**.
2. В списке **Настройка коммутируемого соединения и виртуальных частных сетей (Dial-Up And Virtual Private Network Settings)** выберите подключение, которое хотите настроить, и щелкните кнопку **Настройка (Settings)**.
3. Щелкните кнопку **Свойства (Properties)**. Откроется диалоговое окно свойств подключения.
4. Перейдите на вкладку **Безопасность (Security)**. Для VPN-подключения вы можете указать используемый протокол или использовать автоматическое обнаружение. Можно также задать автоматический вход в систему и потребовать шифрования данных. Оба варианта полезны при входе в домен Windows. Помните, что заданные вами параметры должны поддерживаться системой. Если они не поддерживаются, пользователи не смогут подтвердить подлинность своих учетных данных и подключение не будет выполнено.

   Если вы используете смарт-карты, то также должны потребовать шифрования данных. Оно гарантирует безопасность обмена данными между исходным компьютером и авторизующим компьютером. Если вы выберете вариант **Обязательное (Require Encryption)**, а подключение не защищено при помощи шифрования, клиентский компьютер разорвет подключение.
5. Укажите разрешенные протоколы проверки подлинности и щелкните **OK**.

Настройка сетевых протоколов и компонентов

Способ настройки сетевых протоколов и компонентов зависит от типа подключения. Как показано в табл. 16-1, в телефонных подключениях в качестве протокола применяются протоколы PPP или SLIP, в широкополосных подключениях — протокол PPPoE, в VPN-подключениях — протоколы PPTP или L2TP.

Табл. 16-1. Протоколы для подключений различных типов

Тип подключения	Протокол	Описание
Телефонное	PPP	Используется для установления коммутируемого подключения к серверам Windows
Телефонное	SLIP	Используется для установления коммутируемого подключения к серверам UNIX; доступно, если вы установили ПО независимых разработчиков

Табл. 16-1. (*окончание*)

Тип подключения	Протокол	Описание
Широкополосное	PPPoE	Используется для установления подключения через Ethernet
VPN	Автоматический	Используется для автоматического обнаружения доступного протокола VPN и создания виртуального туннеля с использованием этого протокола
VPN	PPTP VPN	Расширение PPP для VPN
VPN	L2TP IPSec VPN	Протокол для VPN, в котором для повышения безопасности используется IPSec
DirectAccess	IPv6 через IPSec	Используется для создания безопасного туннеля к рабочему месту через существующее подключение

При работе с мобильными сетями используются три сетевых компонента: протокол TCP/IP, Служба доступа к файлам и принтерам сетей Microsoft (File And Printer Sharing For Microsoft Networks) и Клиент для сетей Microsoft (Client For Microsoft Networks). Как показано в табл. 16-2, настройка этих компонентов по умолчанию зависит от исходного типа подключения. Вы вольны изменить эти настройки нужным образом, а также при необходимости установить дополнительные сетевые компоненты.

Табл. 16-2. Конфигурация компонентов по умолчанию по типам подключения

Сетевой компонент	Описание	Широкополосное	Стандартное телефонное	Телефонное в офис	VPN
TCP/IP	Требуется для сетевых коммуникаций. По умолчанию для подключений используется DHCP, если не указано иное	Да	Да	Да	Да
Служба доступа к файлам и принтерам сетей Microsoft (File And Printer Sharing For Microsoft Networks)	Активирует совместное использование принтеров и файлов через сетевое подключение; разрешает привязку принтеров и дисков	Нет	Нет	Нет	Да

Табл. 16-2. (*окончание*)

Сетевой компонент	Описание	Широкополосное	Стандартное телефонное	Телефонное в офис	VPN
Клиент для сетей Microsoft (Client For Microsoft Networks)	Активирует проверку подлинности Windows в доменах Windows; активирует работу компьютера в качестве члена домена	Нет	Нет	Да	Да

Чтобы просмотреть или изменить сетевые параметры подключения, выполните следующие действия:

1. В панели управления выберите категорию **Сеть и Интернет (Network And Internet)**. Затем щелкните **Свойства обозревателя (Internet Options)**. В одноименном диалоговом окне перейдите на вкладку **Подключения (Connections)**.
2. В списке **Настройка коммутируемого соединения и виртуальных частных сетей (Dial-Up And Virtual Private Network Settings)** выберите подключение, которое хотите настроить, и щелкните кнопку **Настройка (Settings)**.
3. Щелкните кнопку **Свойства (Properties)**. Откроется диалоговое окно свойств подключения.
4. Перейдите на вкладку **Сеть (Networking)** и выполните одно из следующих действий:
   - Активируйте сетевые компоненты, установив соответствующие флажки в списке **Компоненты, используемые этим подключением (This Connection Uses The Following Items)**.
   - Отключите сетевые компоненты, сбросив соответствующие флажки в списке **Компоненты, используемые этим подключением (This Connection Uses The Following Items)**.

Совет Если какой-либо сетевой компонент из табл. 16-2, необходимый для подключения, отсутствует, установите его, щелкнув кнопку **Установить (Install)** на вкладке **Сеть (Networking)**. Затем укажите тип компонента, щелкните **Добавить (Add)** и выберите компонент в списке.

5. По умолчанию подключения используют DHCP для конфигурации сетевых параметров, в том числе IP-адреса, маски подсети, основного шлюза, DNS-сервера и WINS-сервера. Чтобы назначить подключению статический IP-адрес или изменить другие параметры, выберите элемент **Протокол Интернета версии 4 (TCP/IPv4) (Internet Protocol Version 4 (TCP/IPv4))** или **Протокол Интернета версии 6 (TCP/IPv6) (Internet Protocol Version 6 (TCP/IPv6))** и щелкните **Свойства (Properties)**. Затем настройте параметры, как было описано ранее в этой главе.
6. Трижды щелкните **OK**.

Включение и отключение брандмауэра Windows для сетевых подключений

Брандмауэр Windows обеспечивает компьютеру дополнительную защиту от нападения при телефонных, широкополосных и VPN-подключениях. Он защищает Windows 7, ограничивая типы передаваемой информации. Задав соответствующие ограничения, вы снижаете вероятность проникновения злоумышленников в систему. Это чрезвычайно важно в тех случаях, когда пользователи получают доступ к сети организации извне, не будучи защищенными штатными брандмауэрами и прокси-серверами.

Брандмауэр Windows активируется по умолчанию для всех подключений и может быть включен или выключен для каждого типа сети, к которой подключается пользователь. Чтобы активировать или отключить брандмауэр Windows для того или иного подключения, выполните следующие действия:

1. В панели управления щелкните категорию **Система и безопасность (System And Security)**.
2. Щелкните **Брандмауэр Windows (Windows Firewall)**. В левой панели щелкните команду **Включение и отключение брандмауэра Windows (Turn Windows Firewall On Or Off)**.
3. На странице **Настроить параметры (Customize Settings)** перечислены настройки брандмауэра для каждого типа сети. Установите переключатель **Включение брандмауэра Windows (Turn On Windows Firewall)** или **Отключить брандмауэр Windows (Turn Off Windows Firewall)** для каждого типа сети.
4. Щелкните **OK**.

Установка подключения

Как уже говорилось в этой главе, телефонные, широкополосные и VPN-подключения могут устанавливаться как вручную, так и автоматически. Ручное подключение позволяет пользователю самому выбирать момент подключения. Автоматическое подключение происходит, когда пользователь запускает программу, которой требуется доступ к сети, например веб-браузер.

Телефонное подключение

При телефонном подключении соединение между двумя модемами осуществляется по телефонной линии. Для установки телефонного подключения выполните следующие действия:

1. Щелкните значок сети на панели задач, выберите телефонное подключение, которое хотите использовать, и щелкните кнопку **Подключение (Connect)**.
2. Проверьте корректность имени пользователя и введите пароль учетной записи, если он не появился.

3. Чтобы использовать эти имя пользователя и пароль каждый раз, когда вы предпринимаете попытку установить данное подключение, установите флажок **Сохранять имя пользователя и пароль (Save This User Name And Password For The Following Users)**, а затем установите переключатель **Только для меня (Me Only)**.
4. Чтобы использовать эти имя пользователя и пароль каждый раз, когда любой пользователь предпринимает попытку установить данное подключение, установите флажок **Сохранять имя пользователя и пароль (Save This User Name And Password For The Following Users)**, а затем установите переключатель **Для любого пользователя (Anyone Who Uses This Computer)**. Не используйте этот вариант, если планируете настраивать подключение через групповую политику.
5. В раскрывающемся списке **Набрать (Dial)** отображен набираемый номер телефона. По умолчанию это основной номер. Для выбора дополнительного номера раскройте список и выберите номер, который хотите использовать.
6. Щелкните кнопку **Вызов (Dial)**. После подключения модема к Интернет-провайдеру или офисной сети вы увидите скорость подключения. Она варьируется для каждого вызова и зависит от максимальной скорости обоих модемов, а также от качества подключения и используемых алгоритмов сжатия.

Если у вас возникли проблемы при телефонном подключении, используйте следующие рекомендации:

- **Проблема** Модем набирает номер, звонок поступает на другой модем, но подключения не происходит. Модем издает характерные звуки подключения до полной отмены операции.

  Решение Обычно проблема кроется в телефонных линиях. Неудачные попытки подключения провоцируются электростатическими помехами и шумами. Проверьте соединение между модемом и телефонной розеткой. Свяжитесь с телефонной компанией, чтобы они протестировали линию и устранили неисправность.
- **Проблема** Модем набирает номер и начинает устанавливать подключение с провайдером или офисной сетью, но оно внезапно обрывается. Успешного подключения не происходит.

  Решение Проверьте параметры сетевых протоколов и установленные компоненты. Если с ними все в порядке, проверьте, передаете ли вы учетные данные Windows, поскольку они могут требоваться. Подробнее — в разделе «Настройка учетных данных подключения».
- **Проблема** Пользователь не может получить доступ к ресурсам домена Windows.

  Решение Для получения доступа к ресурсам офисной сети может потребоваться Клиент для сетей Microsoft (Client For Microsoft Networks). Активируйте этот компонент и убедитесь, что при подключении должным образом передается информация о домене.

- **Проблема** Пользователь не может дозвониться до номера. Создается впечатление, что модем неверно набирает номер: вы слышите, что набирается слишком много или слишком мало цифр.

  Решение Проверьте правила набора для данного подключения, а также текущее расположение. Убедитесь, что они настроены правильно.
- **Проблема** Отображается сообщение об отсутствии сигнала, хотя модем установлен корректно и находится в рабочем состоянии.

  Решение Проверьте телефонный кабель и убедитесь, что он правильно подключен. У некоторых модемов есть два гнезда: одно подписано Phone/In, другое — Line/Out. Телефонный кабель от стенной розетки должен подключаться в гнездо Line/Out. Некоторые телефонные разъемы предназначены только для передачи данных по высокоскоростной линии, а не для телефона или модема. Попробуйте подключиться к другому гнезду.
- **Проблема** Компьютер «зависает», когда пользователь пытается использовать модем.

  Решение Скорее всего, проблема вызвана конфликтом устройств. Диагностика неисправностей устройств описана в главе 8.
- **Проблема** Некоторые службы «зависают» или не работают.

  Решение Проверьте настройки прокси-сервера и брандмауэра. Они могут ограничивать доступные службы.

Широкополосное подключение

Широкополосные соединения устанавливаются при помощи кабельного модема и кабельной линии или DSL-маршрутизатора и телефонной линии. Для установки широкополосного соединения выполните следующие действия:

1. Щелкните значок сети на панели задач. Выберите широкополосное подключение, которое хотите использовать, и щелкните кнопку **Подключение (Connect)**.
2. Проверьте имя пользователя и введите пароль учетной записи, если он не появился.
3. Чтобы использовать эти имя пользователя и пароль каждый раз, когда вы предпринимаете попытку установить данное подключение, установите флажок **Сохранять имя пользователя и пароль (Save This User Name And Password For The Following Users)**, а затем установите переключатель **Только для меня (Me Only)**.
4. Чтобы использовать эти имя пользователя и пароль каждый раз,, когда любой пользователь предпринимает попытку установить данное подключение, установите флажок **Сохранять имя пользователя и пароль (Save This User Name And Password For The Following Users)**, а затем установите переключатель **Для любого пользователя (Anyone Who Uses This Computer)**.
5. Щелкните кнопку **Подключение (Connect)**.

Если при широкополосном подключении у вас возникли проблемы, используйте следующие рекомендации:

- **Проблемы** Вы не можете подключиться. Подключение не работает.

  Решение Проверьте сетевые подключения. Убедитесь, что линии, соединяющие DSL-маршрутизатор или кабельный модем и компьютер, правильно подключены к гнездам.
- **Проблема** Подключение неожиданно прерывается. Не происходит успешного подключения.

  Решение Проверьте параметры сетевых протоколов и установленные компоненты. Если с ними все в порядке, проверьте, передаете ли вы учетные данные Windows, поскольку они могут требоваться. Подробнее — в разделе «Настройка учетных данных подключения».
- **Проблема** Некоторые службы «зависают» или не работают.

  Решение Проверьте настройки прокси-сервера и брандмауэра. Они могут ограничивать доступные службы.
- **Проблема** Пользователь не может получить доступ к ресурсам домена Windows.

  Решение Для получения доступа к ресурсам офисной сети может потребоваться Клиент для сетей Microsoft (Client For Microsoft Networks). Активируйте этот компонент и убедитесь, что при подключении должным образом передается информация о домене.

Подключение VPN

VPN-подключение производится при существующем локальном сетевом, телефонном или широкополосном подключении.

VPN-подключения отображаются отдельно от телефонных, широкополосных или локальных сетевых подключений. Для установки VPN-подключения выполните следующие действия:

1. Щелкните значок сети на панели задач. Выберите широкополосное подключение, которое хотите использовать, и щелкните кнопку **Подключение (Connect)**.
2. Если подключение настроено так, что сначала происходит набор номера для подключения другого типа, Windows 7 сначала попытается установить это подключение. Подтвердите это действие, щелкнув **Да (Yes)**, а затем установите телефонное или широкополосное подключение, как описано выше.
3. Когда необходимое подключение установлено, откроется диалоговое окно **Подключение (Connect)**. Проверьте имя пользователя, введите пароль учетной записи, если он не появился, и щелкните **Подключение (Connect)**.

Если в ходе подключения возникли проблемы, используйте следующие рекомендации:

- **Проблема** Вы не можете подключиться. Подключение не работает.

  Решение Проверьте сетевые подключения. Убедитесь, что линии, соединяющие DSL-маршрутизатор или кабельный модем и компьютер, подключены к гнездам должным образом.
- **Проблема** Появляется сообщение об ошибке в имени хост-системы.

  Решение Возможно, имя хост-системы указано некорректно. Проверьте настройки и убедитесь, что имя задано полностью, например external01.microsoft.com, а не просто external01. Также причина может быть в некорректной работе DNS. Попробуйте ввести IP-адрес хост-системы, а не ее имя.
- **Проблема** Появляется сообщение об ошибке из-за некорректного IP-адреса.

  Решение Проверьте или повторно введите IP-адрес. Если IP-адрес введен корректно, возможно, неверно настроены параметры TCP/IP. Проверьте сетевые протоколы и компоненты. Возможно, вам потребуется вручную задать для подключения основной шлюз и статический IP-адрес.
- **Проблема** Появляется сообщение о том, что протокол не поддерживается; успешного подключения не происходит.

  Решение Задайте вместо PPTP или L2TP автоматический выбор протокола. Проверьте параметры безопасного входа в систему. В них может быть задан ввод безопасного пароля вместо смарт-карты или наоборот. Если настройки в порядке, проверьте, передаете ли вы учетные данные Windows, поскольку они могут требоваться. Подробнее — в разделе «Настройка учетных данных подключения».
- **Проблема** Не удается подключить сетевые диски или получить доступ к принтерам.

  Решение Для доступа к дискам и принтерам требуется Служба доступа к файлам и принтерам сетей Microsoft (File And Printer Sharing For Microsoft Networks). Активируйте ее, как описано в разделе «Настройка сетевых протоколов и компонентов».
- **Проблема** Некоторые службы «зависают» или не работают.

  Решение Проверьте настройки прокси-сервера и брандмауэра. Они могут ограничивать доступные службы.

Беспроводные сети

Чтобы облегчить пользователям использование ноутбуков на переговорах и в других подразделениях офиса, многие организации внедряют беспроводные сети. Они могут использоваться во многих различных конфигурациях. В этом разделе описаны наиболее распространенные конфигурации.

Беспроводные сетевые устройства и технологии

При работе с беспроводными сетями вам чаще всего будут встречаться термины *беспроводной сетевой адаптер* (wireless network adapter) и *точка беспроводного доступа* (wireless access point). Беспроводные адаптеры выпускаются

в виде PC-плат для ноутбуков, плат PCI для настольных компьютеров и USB-устройств, которые могут использоваться как с ноутбуками, так и с настольными компьютерами. Многие современные ноутбуки оборудованы встроенными беспроводными адаптерами. Антенна беспроводного адаптера используется для связи с точкой доступа. Как правило, точка доступа напрямую подключена к физической сети организации, а также может функционировать как сетевой коммутатор или концентратор, то есть оборудована физическими портами, которые позволяют создавать как проводные, так и беспроводные подключения. Точки доступа также известны как *беспроводные базовые станции* (wireless base station) и *беспроводные шлюзы* (wireless gateway).

Наиболее широко распространены беспроводные адаптеры и точки доступа на основе спецификации IEEE 802.11. Беспроводные устройства, разработанные на основе этой спецификации, могут иметь сертификацию Wi-Fi, гарантирующую, что их производительность и совместимость тщательно протестированы. В табл. 16-3 приведены сравнительные характеристики наиболее распространенных беспроводных технологий на основе спецификации IEEE 802.11. Как видно из таблицы, существует четыре стандарта, каждый из которых имеет свои преимущества и недостатки. Беспроводные устройства спецификации 802.11a не способны взаимодействовать с устройствами спецификации 802.11b or 802.11g. При этом диапазон 5 ГГц используется в небольшом количестве устройств, что снижает вероятность возникновения помех для беспроводных устройств других типов (большинство из которых использует диапазон 2,4 ГГц).

Табл. 16-3. Беспроводные сетевые технологии

Беспроводной стандарт	**802.11a**	**802.11b**	**802.11g**	**802.11n**
Скорость	До 54 Мбит/сек	До 11 Мбит/сек	До 54 Мбит/сек	До 540 Мбит/сек
Частота передачи	5 ГГц	2,4 ГГц	2,4 ГГц	2,4 ГГц, 5 ГГц или обе
Диапазон действия в помещении	Приблизительно от 7 до 25 м	Приблизительно от 30 до 50 м	Приблизительно от 30 до 50 м	Приблизительно от 60 м до 100 м
Совместимость	Несовместимо с устройствами 802.11b и 802.11g	Может работать с устройствами 802.11g (на скорости 11 Мбит/сек); беспроводные адаптеры 802.11g могут работать с точками доступа 802.11b (на скорости 11 Мбит/сек)	Может работать с устройствами 802.11b (на скорости 11 Мбит/сек)	Может работать с устройствами 802.11b (на скорости 11 Мбит/сек) и устройствами 802.11g (на скорости 54 Мбит/сек)

В число более новых спецификаций передачи 802.11 входит спецификация 802.11n, предоставляющая скорости до 540 мегабит в секунду (Мбит/сек) и способная взаимодействовать с устройствами стандарта 802.11b и 802.11g. Чтобы добиться высоких скоростей передачи, в 802.11n можно использовать несколько передатчиков и приемников. Каждый передатчик может передавать один или несколько потоков данных. Чем больше потоков данных используется устройством, тем выше пропускная способность. Многие устройства стандарта 802.11n с несколькими передатчиками и приемниками объединяют сильные, слабые и отраженные сигналы в один поток данных, чтобы расширить диапазон.

Для дополнительной безопасности введен стандарт IEEE 802.11i. В отличие от стандартов 802.11a, 802.11b, 802.11g и 802.11n стандарт 802.11i связан не со скоростями и частотами передачи. Это стандарт безопасности, который добавляется к существующим стандартам. Говоря конкретнее, он добавляет к спецификациям 802.11a, 802.11b и 802.11g функции защиты данных. Это означает, что сетевые адаптеры и точки доступа стандарта 802.11a (а также 802.11b и 802.11g) могут включать в себя функциональность 802.11i.

Примечание Помните, что в некоторые компьютеры (особенно, ноутбуки) встроены чипсеты, поддерживающие несколько беспроводных сетевых технологий. Альянсом Wi-Fi одобрена реализация 802.11i в виде спецификации WPA2. В нее включены все обязательные элементы стандарта 802.11i.

Ближе к реальности Перед развертыванием устройств, основанных не на стандарте IEEE 802.11, обратите особое внимание на вопросы совместимости. Постепенно быстродействие устройств будет возрастать. В некоторых из этих устройств повышение скорости достигается в рамках IEEE 802.11 за счет сжатия и других аналогичных методов. В других могут использоваться собственные сетевые технологии, предполагающие, что вы используете для улучшения качестве передачи беспроводные адаптеры и точки доступа именно этого производителя. Чтобы получить более подробную информацию о беспроводных стандартах и сертифицированных устройствах, обратитесь к сайту *www.wi-fi.org*.

Безопасность беспроводных подключений

Обеспечение безопасности в беспроводной сети существенно отличается от обеспечения безопасности в проводной сети. В проводной сети пользователь должен использовать кабель, чтобы физически подключиться к сети и получить доступ к одному из внутренних коммутаторов или концентраторов. Если компьютер к сети подключает неавторизованный пользователь, это довольно легко определить и найти физический кабель, ведущий к данному компьютеру.

Когда вы устанавливаете беспроводную сеть, доступ к вашей сети получает любой пользователь в радиусе действия одной из ваших точек доступа. Он способен не только перехватывать передаваемые беспроводные сигналы, но и проникать в сеть. При этом расположение взломщика трудно отследить, поскольку отсутствуют физические провода, по которым к нему можно было бы добраться. Хуже того, если взломщик получил доступ к беспро-

водной точке доступа, это, как правило, означает, что он находится внутри брандмауэра организации. Чтобы защитить сеть, вам необходимо настроить для нее брандмауэр и настроить беспроводные устройства на шифрование всех беспроводных передач.

Самой распространенной схемой беспроводного шифрования является технология WEP (Wireless Equivalency Protection). Она позволяет шифровать данные с использованием 40-разрядного, 128-разрядного, 152-разрядного (или выше) шифрования с закрытым ключом. Все данные шифруются при помощи симметричного ключа, выводимого из ключа или пароля WEP перед передачей. Любой компьютер, на котором нужно прочитать данные, должен обладать способностью дешифровать их с использованием ключа. В типичной проводной среде для защиты данных достаточно шифрования при помощи общего ключа. В беспроводной среде с высокой интенсивностью трафика вполне возможно, что кто-либо сможет взломать общий ключ. И, поскольку общий ключ не меняется автоматически с течением времени, взломщик сможет получить доступ к внутренней сети организации.

WEP обеспечивает лишь самый базовый уровень безопасности, поэтому его применение не рекомендуется, за исключением случаев, когда нет другой альтернативы. Предпочтительными альтернативами для WEP являются WPA (Wi-Fi Protected Access) и WPA2 (Wi-Fi Protected Access Version 2). Стандарт WPA был принят альянсом Wi-Fi Alliance как промежуточный стандарт перед утверждением 802.11i. WPA2 основан на официальном стандарте 802.11i и полностью обратно совместим с WPA.

Для повышения безопасности WPA и WPA2 способны чередовать ключи и изменять способы вывода ключей. Ротация ключи шифрования и отсутствие строго определенного способа их вывода в WPA и WPA2 значительно повышает безопасность. Устройства, совместимые с WPA и WPA2, могут работать как в режиме предприятия, так и в режиме небольшого или домашнего офиса, как описано ниже:

- **Режим предприятия с проверкой подлинности на базе IEEE 802.1X и EAP** В режиме предприятия у беспроводных устройств имеется два комплекта ключей: сеансовые ключи и групповые ключи. Сеансовые ключи уникальны для каждой связи между точкой доступа и беспроводным клиентом. Они используются, чтобы создать частный виртуальный порт между точкой доступа и клиентом. Групповые ключи распределяются между всеми клиентами, подключенными к одной и той же точке доступа. Оба комплекта ключей порождаются динамически и чередуются, чтобы сохранить целостность ключей с течением времени.
- **Персональный режим с проверкой подлинности на базе предварительного ключа или пароля** В персональной конфигурации вместо меняющегося ключа шифрования WPA использует предварительный ключ шифрования. Пользователь вводит основной (групповой) ключ в точку доступа, а затем настраивает все беспроводные устройства на использование этого основного ключа. Беспроводное устройство на базе основно-

го ключа математически генерирует сеансовый ключ. Сеансовый ключ регулярно меняется, чтобы один и тот же ключ никогда не использовался дважды. Поскольку чередование ключа осуществляется автоматически, управление ключами обрабатывается в фоновом режиме.

WPA и WPA2 полностью совместимы со стандартами 802.11a, 802.11b, 802.11g и 802.11n. Совместимость с WPA и WPA2 для многих старых беспроводных устройств обеспечивается посредством обновления ПО. При использовании WPA никаких дополнительных модификаций не требуется. Но это не всегда справедливо для WPA2. Для некоторых беспроводных устройств может потребоваться обновление процессора или другого оборудования, чтобы они справлялись с шифрованием стандарта AES (Advanced Encryption Standard), требующим большого объема вычислений.

При работе с WPA и WPA2 помните о следующем:

- Все продукты, сертифицированные для WPA2, способны взаимодействовать с продуктами, сертифицированными для WPA.
- Как WPA, так и WPA2 работают в персональном режиме и режиме предприятия.
- И в WPA, и в WPA2 для проверки подлинности используются 802.1X и EAP.
- WPA обеспечивает надежное шифрование данных при помощи протокола TKIP (Temporal Key Integrity Protocol).
- WPA2 обеспечивает улучшенное шифрование данных посредством AES, благодаря чему соответствует требованиям стандарта FIPS 140-2 для правительственных учреждений.

Примечание Стандарты WPA и WPA2 обеспечивают высокий уровень безопасности для сохранности личных данных и ограничения доступа к беспроводным сетям только для авторизованных пользователей. Надежное шифрование посредством AES (что требуется для некоторых корпоративных и правительственных пользователей) обеспечивает только WPA2.

Есть еще одна современная технология беспроводной безопасности, поддерживаемая устройствами стандарта 802.11i, — RSN (Robust Security Network), которая позволяет беспроводным устройствам динамически согласовывать алгоритмы проверки подлинности и шифрования. Это означает, что алгоритмы шифрования и проверки подлинности, используемые RSN-совместимыми устройствами, могут быть изменены. При возникновении новых проблем безопасности в этот стандарт могут добавляться новые методы и алгоритмы проверки подлинности. RSN основан на EAP и AES.

Установка и настройка беспроводного адаптера

Помимо ноутбуков со встроенными беспроводными адаптерами, вам чаще всего придется иметь дело с PC-платами для ноутбуков и платами для настольных компьютеров. Эти адаптеры наиболее просты в настройке и, как подсказывает мой опыт, наиболее надежны. Имеются также беспроводные

адаптеры, которые подключаются к ноутбуку или настольному компьютеру при помощи USB-кабеля. Используя беспроводные устройства с USB, помните, что существуют две спецификации USB: оригинальная спецификация USB 1.0 и более новая и быстрая спецификация USB 2.0. Беспроводное устройство, совместимое с USB 2.0, должно подключаться к порту USB 2.0, чтобы оно функционировало с той скоростью, которую вы ожидаете.

Примечание Беспроводные технологии изменяются так быстро, что большинство беспроводных устройств в Windows 7 не распознаются. Это затруднит установку, поскольку вы, как правило, уже не можете рассчитывать на Plug and Play. Для большинства современных беспроводных адаптеров приходится запускать установочный компакт-диск. Особенно это касается USB-устройств. Обязательно внимательно прочитайте документацию.

Установочное ПО поможет вам настроить беспроводное устройство. В ходе установки вы сможете уточнить имя беспроводной сети, к которой хотите подключиться, и режим, в котором будет запускаться беспроводное устройство. Беспроводные адаптеры работают в одном из двух режимов:

- **Режим «ad hoc»** В этом режиме вы конфигурируете беспроводной адаптер на прямое подключение к другим компьютерам с беспроводными адаптерами.
- **Инфраструктура** В режиме инфраструктуры вы настраиваете беспроводной адаптер на работу в беспроводной сети. Предполагается, что адаптер будет подключаться к точке доступа, а не напрямую к компьютеру.

Указав режим работы адаптера, вы, возможно, должны будете указать ключ шифрования. Если в вашей организации применяется WEP, в большинстве случаев вам нужно будет ввести ключ шифрования. В конфигурациях с безопасностью WPA/WPA2 для предоставления ключа шифрования чаще всего применяются сертификаты или смарт-карты.

Работа с беспроводными сетями и подключениями

В случае успешной установки устройства вы сможете подключиться к беспроводной сети. Как обычному сетевому адаптеру соответствует локальное подключение, беспроводному сетевому адаптеру соответствует беспроводное сетевое подключение. Оно подключено к сети, которая может быть общественной, частной или доменной. Если на компьютере установлены адаптеры обоих типов, он может иметь два активных подключения: одно для проводной сети и одно для беспроводной.

Для беспроводных сетевых подключений отображаются следующие дополнительные данные:

- Имя беспроводной сети в скобках после идентификатора типа подключения.
- Текущее качество сигнала. Одно деление означает низкое качество сигнала; пять делений — превосходное качество.
- Команда для отключения беспроводного соединения.

Окно состояния беспроводного подключения показано на рис. 16-10. С его помощью вы проверите состояние подключения и скорость соединения. Как и у локальных подключений, у беспроводных подключений есть настраиваемые свойства. Приводившееся выше описание настройки свойств локального подключения применимо также и к беспроводным подключениям. Вы можете сделать следующее:

- Устанавливать и отменять установку сетевых функций для клиентов, служб и протоколов. В диалоговом окне **Состояние — Беспроводное сетевое соединение (Wireless Network Connection Status)** щелкните кнопку **Свойства (Properties)**, и щелкните кнопку **Установить (Install)** или выделите элемент и щелкните кнопку **Удалить (Uninstall)**.
- Задать параметры протоколов TCP/IPv6 и TCP/IPv4 — использование DHCP, статический и дополнительный IP-адреса. В диалоговом окне **Состояние — Беспроводное сетевое соединение (Wireless Network Connection Status)** щелкните кнопку **Свойства (Properties)**, а затем дважды щелкните элемент **Протокол Интернета версии 6 (TCP/IPv6) (Internet Protocol Version 6 (TCP/IPv6))** или **Протокол Интернета версии 4 (TCP/IPv4) (Internet Protocol Version 4 (TCP/IPv4))**.
- Отключить беспроводное подключение или провести его диагностику. В диалоговом окне **Состояние — Беспроводное сетевое соединение (Wireless Network Connection Status)** щелкните кнопки **Отключить (Disable)** или **Диагностика (Diagnose)**.

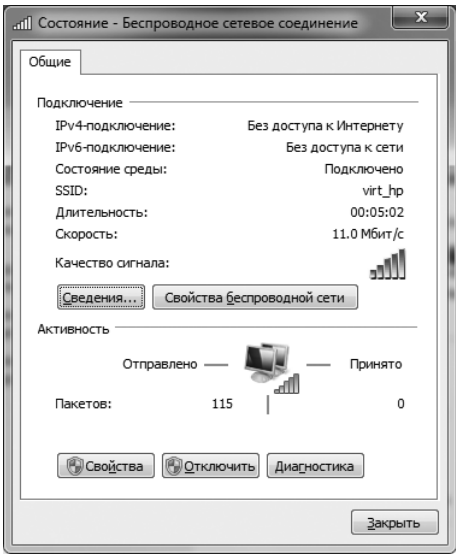

Рис. 16-10. Состояние и мощность сигнала беспроводного сетевого подключения

Если у вас возникли проблемы при установке беспроводного подключения или автоматизированная диагностика неспособна устранить проблему, используйте следующие рекомендации:

- **Проблема** Ограниченное подключение к беспроводной сети или его отсутствие.

  Решение Проверьте качество сигнала. Если его мощность низка, переместитесь ближе к точке доступа или перенаправьте антенну. Если вы используете встроенную антенну, измените положение ноутбука относительно точки доступа. Проблема может заключаться в том, что сеть не подключена должным образом или не произведена настройка сетевых адресов. Проверьте состояние подключения, щелкнув соответствующую ссылку в Центре управления сетями и общим доступом (Network And Sharing Center). Если в поле состояния среды стоит значение, отличное от **Подключено (Enable)**, щелкните кнопку **Диагностика (Diagnose)**, чтобы попытаться устранить проблему с использованием автоматической диагностики.

- **Проблема** Отсутствие или невозможность подключения к беспроводной сети.

  Решение Если вы находитесь вне зоны передачи, ваш компьютер не сможет подключиться к беспроводной сети. Дважды щелкните подключение. Вы увидите сообщение о том, что доступные беспроводные сети не найдены. Если вы считаете это сообщение ошибочным, щелкните кнопку обновления. Если сообщение верно, попытайтесь переместиться ближе к точке доступа или измените положение антенны или компьютера относительно нее. Возможно также, что компьютер не настроен должным образом для установки беспроводного подключения к этой сети.

Совет Скорость подключения достигнет максимально возможного значения, только если у вас будет мощный сигнал. Если качество сигнала невысоко, скорость подключения значительно снизится. Для повышения мощности сигнала переместите антенну или постарайтесь изменить положение компьютера относительно точки доступа.

Подключение к беспроводной сети

Компьютеру с беспроводным адаптером должна быть доступна любая беспроводная точка доступа, осуществляющая вещание внутри соответствующего диапазона. По умолчанию Windows 7 автоматически определяет соответствующие настройки. Если для подключения требуется пароль или другие данные, при попытке подключения к беспроводной сети вы получите приглашение на их ввод. Вы также можете предварительно настроить беспроводные соединения для пользователей. Это позволит должным образом настроить различные параметры проверки подлинности, шифрования и обмена данными.

Чтобы предварительно настроить подключение к беспроводной сети, выполните следующие действия:

1. В Центре управления сетями и общим доступом (Network And Sharing Center) щелкните ссылку **Настройка нового подключения или сети (Set Up A New Connection Or Network)**. Будет запущен мастер Установка подключения или сети (Set Up A Connection Or Network).

2. Выберите команду **Подключение к беспроводной сети вручную (Manually Connect To A Wireless Network)** и щелкните **Далее (Next)**.
   Теперь вам необходимо ввести информацию о беспроводном подключении, к которому вы хотите подключиться. Вы получите ее у сетевого администратора.
3. В поле **Имя сети (Network Name)** введите имя сети (сетевой идентификатор безопасности или SSID).
4. В списке **Тип безопасности (Security Type)** выберите используемый тип безопасности. Поле с типом шифрования будет заполнено автоматически.
5. При использовании типов безопасности WEP и WPA-Personal введите ключ безопасности или пароль в поле **Ключ безопасности (Security Key)**. Как правило, ключом WEP могут быть:
   - 5 символов разного регистра;
   - 13 символов разного регистра;
   - 10 шестнадцатеричных цифр;
   - 26 шестнадцатеричных цифр.
6. По умолчанию запуск подключения происходит автоматически при входе пользователя в систему. Чтобы компьютер подключался к сети, даже если она недостижима, например, когда компьютер находится вне диапазона беспроводной передачи, установите флажок **Подключаться, даже если сеть не производит широковещательную передачу (Connect Even If The Network Is Not Broadcasting)**.
7. Щелкните **Далее (Next)** и **Закрыть (Close)**.

Как правило, при нахождении в пределах диапазона вещания беспроводной сети нет необходимости заранее настраивать подключение. Вы можете подключиться напрямую, позволив Windows определить корректные настройки. Для подключения к беспроводной сети выполните следующие действия:

1. В Центре управления сетями и общим доступом (Network And Sharing Center) щелкните **Подключиться к сети (Connect To A Network)**. По умолчанию в открывшемся окне перечислены все имеющиеся сети. Если сеть должна быть доступна, но ее нет в списке, щелкните кнопку обновления.
2. Поместив указатель над именем сети, вы увидите всплывающее окно с именем сети, мощностью сигнала, типом безопасности, поддерживаемым беспроводным стандартом и идентификатором безопасности.
3. Подключитесь к беспроводной сети или отключитесь от нее, выбрав сеть и щелкнув, соответственно, кнопку **Подключение (Connect)** или **Отключение (Disconnect)**.

Управление и диагностика беспроводных сетей

Для управления беспроводными сетями в Центре управления сетями и общим доступом (Network And Sharing Center) щелкните ссылку **Управление**

беспроводными сетями (Manage Wireless Networks). В этом окне перечислены беспроводные сети в том порядке, в котором компьютер должен их использовать. Первой предпринимается попытка подключения к сети, стоящей в верхней строке списка. Если компьютеру не удается установить подключение к этой сети, он использует следующую сеть по списку и т. д.

Чтобы изменить порядок выбора сетей, щелкните одну из сетей и переместите в нужное положение при помощи кнопок **Переместить вверх (Move Up)** или **Переместить вниз (Move Down)**. Щелкните **Добавить (Add)**, чтобы создать новое беспроводное соединение. Чтобы удалить сеть, выделите ее и щелкните **Удалить (Remove)**.

В Windows 7 включено множество инструментов для диагностики неисправностей и подключения к сети. Методы диагностики и разрешения проблем, возникающих при работе с сетью, описаны в главе 15. В беспроводных сетях вы можете столкнуться с аналогичными проблемами. Помимо этих методов диагностики вы также можете сделать следующее:

- Просмотрите настройки безопасности для беспроводной сети и проверьте их корректность. Повторно введите ключ безопасности или пароль.
- Убедитесь, что беспроводное устройство правильно размещено и находится в зоне действия точки беспроводного доступа. Попробуйте переместить компьютер ближе к точке доступа.
- Убедитесь в отсутствии помех от других устройств, использующих тот же диапазон передачи создающих магнитные поля. Попробуйте переместить или отключить устройства, вызывающие помехи.

Глава 17

Обслуживание и техническая поддержка

На протяжении всей этой книги я говорил о методиках технической поддержки и диагностики, применяемых в администрировании Windows 7. В этой главе мы обратимся к дальнейшему совершенствованию поддержки независимо от расположения компьютеров и к их восстановлению после некоторых типов сбоев. Начнем с автоматического обновления, после чего обсудим, как при помощи компонента Удаленный помощник (Remote Assistance) устранять неполадки дистанционно. Также не забывайте об инструменте Средство записи действий по воспроизведению неполадок (Problem Steps Recorder, Psr.exe). Как уже говорилось в главе 5, он позволяет получить сведения о конкретной проблеме на компьютере пользователя без непосредственного доступа к этому компьютеру.

Автоматическое обновление

Стандартный компонент автоматического обновления Windows 7 называется Центр обновления Windows (Windows Update). Это доработанная версия аналогичного компонента из предыдущих версий Windows. Центр обновления Windows позволяет обновлять как саму ОС, так и поставляемые с ней программы и драйверы устройств. В следующих разделах мы поговорим о том, как работает Центр обновления Windows и как правильно выполнять обновления компьютера.

Центр обновления Windows

Центр обновления Windows (Windows Update) — это клиентский компонент, периодически подключающийся к заданному серверу и проверяющий наличие обновлений. Его можно настроить на автоматическую загрузку и установку доступных обновлений или на уведомление пользователя и администратора о наличии обновлений. Центр обновления Windows устанавливает соединение либо с веб-узлом центра обновления Windows на сервере Майкрософт (http://windowsupdate.microsoft.com/), либо с сервером служб обновления Windows (Windows Update Services) вашей организации.

В отличие от компонентов автоматического обновления из предыдущих версий Windows, предназначенных только для распространения и установ-

ки критических обновлений, Центр обновления Windows поддерживает распространение и установку следующих компонентов:

- **Критические обновления** Обновления, критически важные для стабильной работы и защиты компьютера.
- **Обновления безопасности** Обновления, повышающие защищенность системы.
- **Накопительные обновления** Обновления, включающие в себя комплекты обновлений.
- **Пакеты обновлений** Комплексные обновления ОС и ее компонентов, как правило, включающие критические обновления, обновления безопасности и накопительные обновления.
- **Необязательные обновления** Обновления, которые просто могут оказаться полезными, включая обновления драйверов.

Ключевая особенность Центра обновления Windows заключается в расстановке приоритетов загрузки, что позволяет применять обновления в соответствии с их важностью: самые важные обновления загружаются и устанавливаются в первую очередь. Также вы можете управлять способом поиска и установки обновлений. По умолчанию интервал запрашивания обновлений составляет 22 часа, но его можно изменить в групповой политике. По умолчанию установка загруженных обновлений выполняется ежедневно в 3.00 по местному времени. Вы вольны потребовать вывода уведомления о доступности обновлений или изменить время установки.

В ходе установки обновлений Windows 7 перезагружать компьютер нужно не так часто. Новая версия обновляемого файла будет установлена, даже если старая версия в данный момент используется приложением или компонентом системы. При этом используемый файл помечается, и его замена выполняется автоматически при следующем запуске приложения. При обновлении некоторых приложений и компонентов в Windows 7 выполняется сохранение данных приложения, само приложение закрывается, а затем выполняется обновление файла, и приложение открывается вновь. В итоге, процесс обновления меньше затрагивает работу пользователей.

Ближе к реальности Во время автоматического обновления для передачи файлов используется Фоновая интеллектуальная служба передачи (Background Intelligent Transfer Service, BITS). Служба BITS выполняет передачу файлов в фоновом режиме и позволяет перезапускать прерванные передачи. В версии BITS 3.5, включенной в Windows 7, усовершенствован механизм передачи: полоса пропускания используется более эффективно, следовательно, данных передается меньше, и передача происходит быстрее. В групповой политике BITS можно настроить таким образом, чтобы обновления загружались только в специально указанные промежутки времени с ограничением использования полосы пропускания. Эти и другие параметры настраиваются в политике **Ограничить максимальную пропускную способность сети, используемую службой BITS для фоновой передачи, с помощью расписания работы (Set Up A Work Schedule To Limit The Maximum Network Bandwidth Used For BITS Background Transfers)**. Политика находится в узле **Конфигурация компьютера\Административные шаблоны\Сеть\Фоновая интеллектуальная служба переда-**

чи (BITS) (Computer Configuration\Administrative Templates\Network\Background Intelligent Transfer Service). Кроме того, благодаря BITS 3.5 в Windows 7 можно получать обновления от доверенных узлов локальной сети, а также напрямую с сервера обновлений Майкрософт. Если копия обновления имеется на компьютере локальной сети, другие компьютеры сети способны автоматически обнаруживать и загружать обновление непосредственно с этого компьютера. При этом передача обновления по внешнему каналу выполняется всего один раз, а не десятки или сотни раз.

Имеется несколько вариантов реализации автоматического обновления. Доступны следующие параметры:

- **Устанавливать обновления автоматически (Install Updates Automatically)** Все обновления извлекаются с заданным интервалом (по умолчанию 22 ч), после чего устанавливаются в заданное время, по умолчанию ежедневно в 3.00. Действие данного параметра отличается от аналогичного параметра Windows XP. Отличие состоит в том, что от пользователя не требуется подтверждать установку обновлений. Обновления загружаются автоматически, а затем устанавливаются в соответствии с расписанием: ежедневно в заданное время или еженедельно в назначенный день и час.
- **Загружать обновления, но решение об установке принимается мной (Download Updates But Let Me Choose Whether To Install Them)** Это значение установлено по умолчанию. Обновления извлекаются по мере их поступления, после чего пользователь получает уведомление о готовности обновлений к установке. Он волен подтвердить или отменить установку обновлений. Принятые обновления устанавливаются. Отклоненные обновления не устанавливаются, но остаются в системе и могут быть установлены позже.
- **Искать обновления, но решение о загрузке и установке принимается мной (Check For Updates But Let Me Choose Whether To Download And Install Them)** Перед извлечением любых обновлений пользователь получит уведомление. Даже если пользователь принимает решение загрузить обновления, за ним сохраняется право одобрить или отклонить их установку. Принятые обновления устанавливаются. Отклоненные обновления не устанавливаются, но остаются в системе и могут быть установлены позже.
- **Не проверять наличие обновлений (Never Check For Updates)** Если возможность автоматического обновления отключена, пользователи не получают уведомлений о наличии обновлений. Тем не менее, они вольны загружать обновления вручную с веб-узла Центра обновления Windows.

Если параметры Центра обновления Windows (Windows Update) настроены на автоматическую загрузку и установку обновлений, пользователи получают наименьшее количество уведомлений. Для получения дополнительных сведений об обновлении щелкните значок уведомления на панели задач.

Настройка автоматического обновления

В Windows 7 разделяются следующие категории обновлений:

- **Важные обновления (Important updates)** Критические обновления, обновления безопасности, накопительные обновления и пакеты обновлений для ОС и поставляемых с ней программ.
- **Рекомендуемые обновления (Recommended updates)** Обновления для драйверов, поставляемых с ОС, и дополнительные обновления, рекомендуемые для установки.
- **Обновления для других продуктов Microsoft (Microsoft product updates)** Обновления для остальных продуктов Майкрософт, установленных на компьютере, а также нового дополнительного ПО Майкрософт.
- **Драйверы указания и печати (Point and print drivers)** Обновления для автоматически устанавливаемых драйверов печати.

Примечание По умолчанию средствами Центра обновления Windows обновляются списки веб-узлов, отображаемых в режиме совместимости. Настройка этой возможности выполняется в узле **Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Internet Explorer\Представление совместимости (Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Compatibility View)**.

Ближе к реальности Если компьютеру под управлением Windows 7 Home, Ultimate и Professional не удается найти совместимые драйверы указания и печати на самом компьютере, их поиск продолжается в Центре обновления Windows (Windows Update) на сайте Майкрософт. Если соответствующий драйвер не найден, предпринимается попытка создать подключение при помощи любого доступного драйвера, поддерживающего данное оборудование. Чтобы аналогичный поиск выполнялся в Windows 7 Enterprise, включите политику **Расширить подключения указания и печати для поиска обновлений Windows (Extend Point And Print Connection To Search Windows Update)**. Она находится в узле **Конфигурация компьютера\Административные шаблоны\Принтеры (Computer Configuration\Administrative Templates\Printers)**.

Важные обновления в Windows 7 по умолчанию устанавливаются автоматически. Для настройки параметров автоматического обновления на конкретном компьютере выполните следующие действия:

1. На панели управления щелкните категорию **Система и безопасность (System And Security)**. Затем щелкните **Центр обновления Windows (Windows Update)**.
2. На левой панели страницы **Центр обновления Windows (Windows Update)** перейдите по ссылке **Настройка параметров (Change Settings)**.
3. Задайте способ поиска и установки обновлений.
4. Если вы включили установку обновлений и хотите также устанавливать обновления для драйверов и дополнительные обновления, установите флажок **Получать рекомендуемые обновления таким же образом, как и важные обновления (Give Me Recommended Updates The Same Way I Receive Important Updates)**.

5. Чтобы разрешить установку обновлений обычным пользователям, щелкните **Разрешить всем пользователям устанавливать обновления на этот компьютер (Allow All Users To Install Updates On This Computer)**.
6. Чтобы получать обновления для продуктов и дополнительного ПО Майкрософт, установите флажок **При обновлении Windows предоставить обновления для продуктов Майкрософт и проверить наличие нового необязательного программного обеспечения Майкрософт (Give Me Updates For Microsoft Products And Check For New Optional Microsoft Software When I Update Windows)**.
7. Щелкните **OK**.

Централизованная настройка и управление автоматическим обновлением в домене Active Directory выполняются при помощи политик, находящихся в подузле **Компоненты Windows\Центр обновления Windows (Windows Components\Windows Update)** узла **Административные шаблоны (Administrative Templates)** для конфигурации компьютера и конфигурации пользователя. Ключевые политики приведены в табл. 17-1.

Табл. 17-1. Политики, управляющие автоматическим обновлением

Политика	Назначение
Включить рекомендуемые обновления через автоматическое обновление (Turn On Recommended Updates Via Automatic Updates)	Если эта политика включена, рекомендуемые обновления, включая обновления драйверов и прочие дополнительные обновления, устанавливаются вместе с другими обновлениями
Задержка перезагрузки при запланированных установках (Delay Restart For Scheduled Installations)	По умолчанию, если после выполнения автоматического обновления требуется перезагрузка, компьютер перезагружается с задержкой в 15–20 мин. Чтобы изменить время задержки, включите политику и установите время задержки
Запретить использование любых средств Центра обновления Windows (Remove Access To Use All Windows Update Features)	Включение этой политики означает удаление всех компонентов Центра обновления Windows. Доступ пользователей к Центру обновления Windows блокируется, автоматическое обновление полностью отключается
Настройка автоматического обновления (Configure Automatic Updates)	Включение этой политики позволяет настроить работу автоматического обновления при помощи параметров, описанных далее в этой главе. Здесь также можно задать расписание установки
Не выполнять автоматическую перезагрузку при автоматической установке обновлений, если в системе работают пользователи (No Auto-Restart With Logged On Users For Scheduled Automatic Updates Installations	Если эта политика включена, после установки обновлений, требующих перезапуска, компьютер не будет автоматически перезагружен, если в данный момент в системе находится пользователь. Пользователь получит уведомление о необходимости перезагрузки

Табл. 17-1. (*продолжение*)

Политика	Назначение
Перенос запланированных автоматических установок обновлений (Reschedule Automatic Updates Scheduled Installations)	Если эта политика включена, в ней задается интервал между запуском системы и продолжением запланированной установки, которая не состоялась ранее
Повторный запрос для перезагрузки при запланированных установках (Re-Prompt For Restart With Scheduled Installations)	Если эта политика включена и установка обновлений выполняется по расписанию, пользователь, находящийся в системе, с заданным интервалом получает повторное напоминание об отложенной перезагрузке. Если параметр отключен или не настроен, используется стандартный интервал запроса — 10 мин
Разрешить клиенту присоединение к целевой группе (Enable Client-Side Targeting)	Если эта политика включена, администраторам разрешено определять целевую группу для текущего объекта GPO. Присоединение к целевой группе позволяет администратору регулировать установку обновлений на заданной группе компьютеров. Перед развертыванием обновление должно быть авторизовано для конкретной целевой группы
Разрешить немедленную установку автоматических обновлений (Allow Automatic Updates Immediate Installation)	Если эта политика включена, обновления, не препятствующие работе служб Windows и не требующие перезагрузки компьютера, будут устанавливаться автоматически немедленно после загрузки
Разрешить пользователям, не являющимся администраторами, получать уведомления об обновлениях (Allow Non-Administrators To Receive Update Notifications)	Если эта политика включена, уведомления о наличии обновлений в соответствии с конфигурацией автоматического обновления будет получать любой пользователь, выполнивший вход на компьютер. Если эта политика отключена или не настроена, уведомления о наличии обновлений получают только администраторы
Разрешить прием обновлений с подписью из службы обновления Майкрософт в интрасети (Specify Intranet Microsoft Update Service Location)	Если эта политика включена, вы можете указать полные доменные имена сервера службы обновления Microsoft, находящегося в вашей организации, и связанного с ним сервера статистики. Обе службы могут выполняться на одном сервере
Разрешить управлению электропитанием Центра обновления Windows выводить систему из спящего режима для установки запланированных обновлений (Enabling Windows Update Power Management To Automatically Wake Up The System To Install Scheduled Updates)	Если эта политика включена и компьютер настроен на автоматическую установку обновлений по расписанию, в назначенное время средствами управления электропитанием компьютер выводится из режима гибернации для установки обновлений. Вывод из спящего режима для установки обновлений при работе компьютера от батареи не выполняется

Табл. 17-1. (*окончание*)

Политика	Назначение
Частота поиска автоматических обновлений (Automatic Updates Detection Frequency)	Если эта политика включена, она определяет интервал поиска обновлений. По умолчанию поиск обновлений проводится примерно каждые 22 ч. Включив эту политику, можно установить новый интервал. При этом реальный интервал может отличаться от заданного значения на 20%. Это означает, что при установке интервала 10 ч, действительный интервал составит от 8 до 12 ч

Поиск обновлений

На главной странице Центра обновления Windows вы найдете сведения о том, когда в последний раз компьютер или пользователь выполняли поиск обновлений, когда в последний раз устанавливались обновления, а также о текущей конфигурации автоматического обновления. Чтобы настроить Центр обновления Windows или провести поиск обновлений вручную, выполните следующие действия:

1. На панели управления щелкните категорию **Система и безопасность (System And Security)**. Затем щелкните **Центр обновления Windows (Windows Update)**. В окне показаны время последнего поиска обновлений, последней установки обновлений и текущая конфигурация обновлений.
2. Чтобы выполнить поиск обновлений вручную, щелкните **Проверка обновлений (Check For Updates)**.
3. Для установки необязательных обновлений перейдите по ссылке, указывающей на количество доступных необязательных обновлений.
4. На странице **Выбор обновлений для установки (Select Updates To Install)** укажите обновления, которые следует установить, и щелкните **OK**.

Просмотр истории обновления и установленных обновлений

Успешные и неудачные попытки установки обновлений отслеживаются диспетчером загрузки обновлений и фиксируются в журнале обновлений. Для просмотра журнала выполните следующие действия:

1. На панели управления щелкните категорию **Система и безопасность (System And Security)**. Затем щелкните **Центр обновления Windows (Windows Update)**.
2. На левой панели щелкните **Просмотр журнала обновлений (View Update History)**.
3. На открывшейся странице **Просмотр журнала обновлений (View Update History)** указано состояние загрузки и установки обновлений — **Успех (Successful)** или **Отказ (Unsuccessful)**. Состояние **Отказ (Unsuc-**

cessful) означает, что обновление было загружено, но не было установлено. Чтобы удалить обновление, щелкните ссылку **Установленные обновления (Installed Updates)** на странице **Просмотр журнала обновлений (View Update History)**. На странице **Установленные обновления (Installed Updates)** щелкните правой кнопкой обновление, которое нужно удалить, и выберите команду **Удалить (Remove)**.

Удаление автоматически установленного проблемного обновления

Если автоматическое обновление стало причиной неполадок в системе, его можно удалить так же, как и любую другую программу. Выполните следующие действия:

1. На панели управления щелкните категорию **Система и безопасность (System And Security)**. Затем щелкните **Центр обновления Windows (Windows Update)**.
1. Щелкните **Просмотр журнала обновлений (View Update History)** и перейдите по ссылке **Установленные обновления (Installed Updates)**.
2. Выделите обновление в списке и щелкните **Удалить (Uninstall)**.

Сокрытие доступных обновлений

Со временем растет число обновлений, которые вы решили не устанавливать, но они по-прежнему присутствуют в списке доступных для установки. Если вы совершенно уверены, что не будете их устанавливать, скройте эти обновления, выполнив следующие действия:

1. На панели управления щелкните категорию **Система и безопасность (System And Security)**. Затем щелкните **Центр обновления Windows (Windows Update)**.
2. Перейдите по ссылке, указывающей на количество доступных обновлений.
3. На странице **Выбор обновлений для установки (Select Updates To Install)** щелкните правой кнопкой обновление, которое не собираетесь устанавливать, и выберите команду **Скрыть обновление (Hide Update)**.

Восстановление отклоненных обновлений

Скрытое обновление, от установки которого вы в свое время отказались, можно снова сделать видимым и доступным для установки. Выполните следующие действия:

1. На панели управления щелкните категорию **Система и безопасность (System And Security)**. Затем щелкните **Центр обновления Windows (Windows Update)**.
2. Щелкните ссылку **Восстановить скрытые обновления (Restore Hidden Updates)**.

3. На странице **Восстановить скрытые обновления (Restore Hidden Updates)** выделите обновление, которое нужно восстановить, и щелкните **Восстановить (Restore)**.Обновление будет восстановлено и станет доступно для установки обычным порядком.

Работа с удаленным помощником

Компонент Удаленный помощник (Remote Assistance) позволяет персоналу из службы техподдержки наблюдать за компьютером пользователя и временно принимать управление компьютером на себя, чтобы устранить неполадку или помочь пользователю в решении сложной задачи. Для работы с Удаленным помощником (Remote Assistance) его необходимо настроить локально (см. главу 5) или в групповой политике (см. главу 3).

Основные сведения об удаленном помощнике

Компонент Удаленный помощник (Remote Assistance) имеется в Windows XP и более поздних версиях Windows. Только в этих ОС пользователи могут открывать сеансы удаленной помощи и отвечать на приглашения удаленной помощи. На предприятии простой способ работы с Удаленным помощником (Remote Assistance) обеспечивается соблюдением следующих правил:

- Вы должны работать с учетной записью, входящей в локальную группу Группа удаленных помощников (Offer Remote Assistance Helpers).
- В Брандмауэре Windows (Windows Firewall) нужно создать исключения для исполняемых файлов Msra.exe и Raserver.exe и открыть TCP-порт 135 для DCOM. Обычно эти параметры по умолчанию настраиваются в групповой политике.
- Проверьте конфигурацию удаленного компьютера: она должна допускать подключение удаленного помощника. Затем подключитесь к нему, используя имя компьютера или IP-адрес.

Чтобы предоставить удаленную помощь на предприятии, выполните следующие действия:

1. Щелкните кнопку **Пуск (Start)**, введите **msra** в поле поиска и нажмите Enter.
2. В мастере Удаленный помощник Windows (Windows Remote Assistance) выберите вариант **Помочь тому, кто вас пригласил (Help Someone Who Has Invited You)**.
3. Введите имя или IP-адрес компьютера, на котором нужна помощь, и щелкните **Далее (Next)**.

Для запуска сеанса пользователь должен создать запрос на получение помощи. Служба техподдержки запускает сеанс, предлагая пользователю помощь. После открытия сеанса помощники могут общаться с пользователями, просматривать содержимое их экранов и, если это будет разрешено, управлять компьютерами пользователей.

Существуют следующие способы создания приглашений Удаленного помощника (Remote Assistance):

- **Приглашение, по электронной почте** Направляется адресату в сообщении электронной почты. Для открытия сеанса Удаленного помощника (Remote Assistance) используется вложение, содержащееся в сообщении. Чтоб упростить работу, можно создать для получения службой поддержки приглашений пользователей стандартный адрес электронной почты, например *RemoteAssist@your_company_name.com*. Сделайте этот адрес в Microsoft Exchange Server адресом списка распространения для доставки приглашений сотрудникам службы поддержки или дополнительным почтовым ящиком для отдельных сотрудников. Это поможет при обработке запросов в службе поддержки и упростит процедуру запроса помощи.
- **Файл приглашения** Файлы приглашения сохраняются в формате файлов происшествий Microsoft Remote Control (Microsoft Remote Control Incident) с расширением .MsRcIncident. Чтобы открыть сеанс Удаленного помощника (Remote Assistance), нужно дважды щелкнуть имя файла. Файлы приглашения удобны, если для работы с почтой используется веб-интерфейс, и вложение нужно прикреплять отдельно. Кроме того, можно настроить общую папку, которая у пользователя подключена как сетевой диск и доступна персоналу службы поддержки. Ее имя должно соответствовать назначению папки, например HelpDeskRequest или AssistanceInvitations.
- **Приглашение с использованием Easy Connect** Для отправки приглашения Удаленного помощника (Remote Assistance) через Интернет может применяться протокол разрешения имен PNRP (Peer Name Resolution Protocol). При использовании технологии Easy Connect пароль для доступа генерируется автоматически. Это позволяет помощнику подключиться напрямую к компьютеру. Контактная информация помощника сохраняется, чтобы в будущем к ней можно было обращаться без пароля. Этот способ доступен, если компьютеры помощника и пользователя работают под управлением Windows 7 или более поздних выпусков.

В Windows 7 создаваемые приглашения обязательно защищаются паролем — в отличие от предыдущих выпусков Windows. Пароль обеспечивает дополнительный уровень безопасности Удаленного помощника за счет проверки подлинности пользователей, предоставляющих удаленную помощь. В организации должно быть официальное правило, требующее применения паролей для приглашений. Чтобы упростить процесс приглашения, придумайте определенные пароли, регулярно меняйте их, назначайте разные пароли для разных групп организации.

В своей работе компонент Удаленный помощник (Remote Assistance) опирается на сетевое подключение между компьютерами пользователя и помощника. Для связи используются протоколы UPnP, SSDP, PNRP и Teredo. В большинстве брандмауэров подключения с использованием этих прото-

колов по умолчанию запрещены, и потому брандмауэр, находящийся между двумя компьютерами, как правило, препятствует сеансу предоставления удаленной помощи. Для работы необходимо создать исключение для исходящих подключений от компьютера помощника к компьютеру пользователя. Чтобы настроить исключение для Удаленного помощника (Remote Assistance) в Брандмауэре Windows (Windows Firewall), выполните следующие действия:

1. На панели управления щелкните категорию **Система и безопасность (System And Security)**. В разделе **Брандмауэр Windows (Windows Firewall)** щелкните **Разрешение запуска программы через Брандмауэр Windows (Allow A Program Through Windows Firewall)**.
2. В окне **Разрешенные программы (Allows Programs)** пролистайте список вниз до элемента Удаленный помощник (Remote Assistance). Убедитесь, что флажок **Удаленный помощник (Remote Assistance)** установлен.
3. Выберите типы сетей, для которых нужно разрешить использование Удаленного помощника (Remote Assistance), и щелкните **OK**.

Компонент Удаленный помощник (Remote Assistance) может работать через брандмауэры NAT. В нем доступны встроенные средства диагностики. К компьютеру для объединения усилий одновременно могут подключаться два помощника. Наконец, вам не придется заново подключаться к удаленному компьютеру, если в процессе разрешения проблемы возникнет необходимость его перезагрузки. Сеанс Удаленного помощника (Remote Assistance) после перезагрузки возобновляется автоматически.

Создание приглашения удаленной помощи

Чтобы создать приглашение удаленной помощи по электронной почте, выполните следующие действия:

1. В окне панели управления перейдите по ссылке **Поиск и исправление проблем (Find And Fix Problems)** в разделе **Система и безопасность (System And Security)**. В левой панели окна **Устранение неполадок (Troubleshooting)** щелкните **Обратиться за помощью к другу (Get Help From A Friend)**.
2. На странице **Удаленный помощник (Remote Assistance)** щелкните **Пригласите кого-нибудь для оказания помощи (Invite Someone To Help You)**, затем щелкните **Пригласить по электронной почте (Use E-Mail To Send An Invitation)**.
3. На предложение системы дважды введите надежный пароль для подключения к компьютеру. Пароль предназначен для приглашенного вами лица и действителен только для сеанса Удаленного помощника (Remote Assistance).
4. Щелкните кнопку **Далее (Next)**. Будет открыта почтовая программа по умолчанию, и создано сообщение с приглашением. В поле **Кому (To)** введите адрес электронной почты приглашаемого пользователя, а затем щелкните **Отправить (Send)**.

Чтобы создать приглашение удаленной помощи и сохранить его в файл, выполните следующие действия:

1. В окне панели управления перейдите по ссылке **Поиск и исправление проблем (Find And Fix Problems)** в разделе **Система и безопасность (System And Security)**. В левой панели окна **Устранение неполадок (Troubleshooting)** щелкните **Обратиться за помощью к другу (Get Help From A Friend)**.
2. На странице **Удаленный помощник (Remote Assistance)** щелкните **Пригласите кого-нибудь для оказания помощи (Invite Someone To Help You)**, затем щелкните **Сохранить приглашение как файл (Save This Invitation As A File)**.
3. Введите путь и имя файла приглашения. Если указан путь к сетевой папке, приглашение сможет получить администратор, имеющий доступ к этой папке.
4. Предоставьте предполагаемому помощнику файл приглашения и автоматически созданный пароль. Пароль предназначен для приглашенного помощника и действителен только для сеанса Удаленного помощника (Remote Assistance).

Чтобы создать приглашение удаленной помощи с использованием технологии Easy Connect, выполните следующие действия:

1. В окне панели управления перейдите по ссылке **Поиск и исправление проблем (Find And Fix Problems)** в разделе **Система и безопасность (System And Security)**. В левой панели окна **Устранение неполадок (Troubleshooting)** щелкните **Обратиться за помощью к другу (Get Help From A Friend)**.
2. На странице **Удаленный помощник (Remote Assistance)** щелкните **Пригласите кого-нибудь для оказания помощи (Invite Someone To Help You)**, затем щелкните **Используйте Easy Connect (Use Easy Connect)**.

   Передайте помощнику пароль для работы с Easy Connect. Пароль генерируется автоматически и действителен только для данного сеанса Удаленного помощника (Remote Assistance).

Приглашения Удаленного помощника (Remote Assistance) по умолчанию действительны не более шести часов и позволяют службе поддержки управлять компьютером дистанционно. В разделе «Настройка удаленного помощника» главы 5 рассказано, как изменить эти параметры в диалоговом окне **Свойства системы (System Properties)**. Когда вы отправите приглашение по электронной почте или создадите файл приглашения, на экране появится диалоговое окно **Удаленный помощник Windows (Windows Remote Assistance)**, показанное на рис. 17-1. В нем имеются следующие параметры:

- **Отмена (Cancel)** Фактически, это отмена запроса удаленной помощи путем запрета на использование приглашения для подключения к компьютеру.

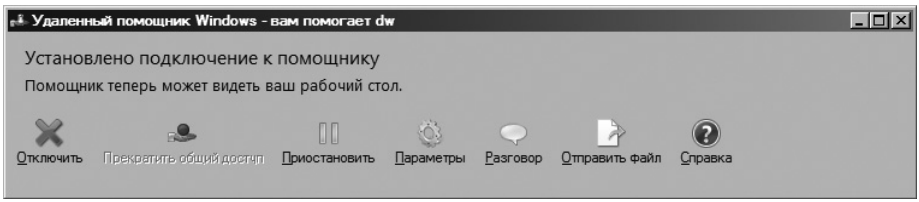

Рис. 17-1. Управление сеансом Удаленного помощника (Remote Assistance)

- **Запросить управление/Прекратить удаленное управление (Request Control/Stop Sharing)** Запрос на доступ к управлению компьютером или прекращение такого доступа. Помощник, которому не разрешено управление компьютером, может наблюдать за его работой на своем экране в качестве зрителя.
- **По размеру экрана (Fit To Screen)** Изменение размера экрана на компьютере помощника в соответствии с размером вашего окна.
- **Отключить (Disconnect)** Завершение сеанса помощника.
- **Параметры (Settings)** Настройка параметров сеанса. Набор параметров зависит от типа компьютера, которому оказывается помощь. По умолчанию заданы следующие параметры: после нажатия клавиши Esc удаленное управление компьютером прекращается, ведется журнал сеанса удаленного помощника, запрещено перетаскивание окон с содержимым, фон рабочего стола отключен. Чтобы задать параметры для быстрых и медленных подключений, воспользуйтесь бегунком **Уровень использования пропускной способности (Bandwidth Usage)**.

Примечание Журнал удаленного помощника по умолчанию создается в папке *%UserProfile%\Documents\Remote Assistance Logs* на компьютере пользователя, запросившего удаленную помощь.

- **Разговор (Chat)** Открытие окна для обмена сообщениями между помощником и текущим пользователем компьютера.
- **Отправить файл (Send File)** Отправка файла на другой компьютер.

Предложение удаленной помощи или отклик на приглашение удаленного помощника

Зная, что пользователь испытывает затруднения, выполните следующие действия, чтобы предложить удаленную помощь, не дожидаясь, пока он пришлет вам приглашение или пароль для Easy Connect:

1. Щелкните **Пуск (Start)**, введите **msra** в поле поиска и нажмите Enter.
2. В мастере Удаленный помощник Windows (Windows Remote Assistance) выберите **Помочь тому, кто вас пригласил (Help Someone Who Has Invited You)**.
3. Перейдите по ссылке **Вариант расширенного подключения для службы поддержки (Advanced Connection Option For Help Desk)**.

4. Введите имя или IP-адрес компьютера, пользователю которого нужна помощь, и щелкните **Далее (Next)**, чтобы подключиться к компьютеру.

Если кто-либо уже создал приглашение, вы можете на него ответить, дважды щелкнув соответствующее вложение или файл. Вы также можете откликнуться на сохраненное в файле приглашение, выполнив следующие действия:

1. Щелкните **Пуск (Start)**, введите **msra** в поле поиска и нажмите Enter.
2. В мастере Удаленный помощник Windows (Windows Remote Assistance) выберите команду **Помочь тому, кто вас пригласил (Help Someone Who Has Invited You)**.
3. Щелкните **Используйте файл приглашения (Use An Invitation File)**, найдите приглашение в диалоговом окне **Открыть (Open)** и щелкните **Открыть (Open).**
4. Введите пароль приглашения.
5. Щелкните **Готово (Finish)**. Соединение между вашим компьютером и компьютером нуждающегося в помощи пользователя будет установлено, при условии что пользователь не отменил приглашение, срок действия приглашения не истек и удаленная помощь разрешена.

Если кто-либо направил вам приглашение при помощи Easy Connect, ответить на приглашение можно так:

1. Щелкните **Пуск (Start)**, введите **msra** в поле поиска и нажмите Enter.
2. В мастере Удаленный помощник Windows (Windows Remote Assistance) выберите **Помочь тому, кто вас пригласил (Help Someone Who Has Invited You)**.
3. Щелкните **Используйте Easy Connect (Use Easy Connect)**. Введите пароль приглашения.
4. Щелкните **OK**.

Поиск и устранение ошибок Windows 7

На каждом компьютере насчитываются десятки, а иногда и сотни различных компонентов, служб и программ. Вы должны следить за тем, чтобы все эти компоненты работали корректно, и вам помогут в этом встроенные средства диагностики, способные обнаруживать общие сбои и найти пути для их устранения. В главе 8 отмечалось, что сведения об известных проблемах собраны в консоли Отчеты о проблемах (Problem Reports And Solutions). Однако не все проблемы могут быть обнаружены и разрешены автоматически. В подобных ситуациях важную роль играют ошибки, возвращаемые компонентами Windows, приложениями, службами и устройствами.

Регистрация ошибок и диагностика при помощи журналов событий

Ошибки, генерируемые процессами, службами, приложениями и устройствами хранятся в файлах журнала. Наиболее распространены файлы журналов двух типов:

- **Журналы Windows** Используются для записи основных системных событий, связанных с приложениями, безопасностью, установкой и компонентами системы.
- **Журналы приложений и служб** Используются отдельными приложениями или службами для записи событий этих приложений или служб.

Записи журнала содержат как сведения об ошибках, так и просто информационные сообщения о произошедших событиях. Существуют следующие уровни записей:

- **Информация (Information)** Информационное событие, связанное, как правило, с успехом действия.
- **Аудит успехов (Audit Success)** Событие, связанное с успешным выполнением действия.
- **Аудит неудач (Audit Failure)** Событие, связанное с неудачным выполнением действия.
- **Предупреждение (Warning)** Предупреждение, подробные сведения из которого часто используются для предотвращения системных сбоев в дальнейшем.
- **Ошибка (Error)** Ошибка, например, неудачный запуск службы.

Кроме типа, даты и времени, в записи о событии вы найдете следующие сведения:

- **Источник (Source)** Приложение, служба или компонент, для которого создана запись.
- **Код события (Event ID)** Идентификатор события.
- **Категория задачи (Task Category)** Категория события, которая иногда применяется для более подробного описания соответствующего действия.
- **Пользователь (User)** Учетная запись пользователя, с которой был выполнен вход в момент наступления события. Если событие запущено системным процессом или службой, в качестве имени пользователя будет указан специальный идентификатор.
- **Компьютер (Computer)** Имя компьютера, на котором произошло событие.
- **Подробности (Details)** Подробное текстовое описание события и связанные с ним данные.

Просмотр журналов событий и управление ими

Для просмотра журналов событий откройте узел **Просмотр событий (Event Viewer)** консоли Управление компьютером (Computer Management). Чтобы открыть консоль Управление компьютером (Computer Management), последовательно щелкните **Пуск (Start)**, **Все программы (All Programs)**, **Администрирование (Administrative Tools)** и **Управление компьютером (Computer Management)**. Можно также щелкнуть кнопку **Пуск (Start)** и

выбрать команду **Панель управления (Control Panel)**. На панели управления последовательно щелкните **Система и безопасность (System And Security)**, **Администрирование (Administrative Tools)** и **Управление компьютером (Computer Management)**.

Чтобы открыть журналы событий, выполните следующие действия:

1. Откройте консоль **Управление компьютером (Computer Management)**. По умолчанию вы подключены к локальному компьютеру. Для просмотра журналов на удаленном компьютере правой кнопкой щелкните элемент **Управление компьютером (Computer Management)** в дереве консоли (левая панель) и выберите команду **Подключиться к другому компьютеру (Connect To Another Computer)**. В диалоговом окне **Выбор компьютера (Select Computer)** введите имя нужного компьютера и щелкните **OK**.
2. Разверните узел **Просмотр событий (Event Viewer)**, а затем разверните узел **Журналы Windows (Windows Logs)**, узел **Журналы приложений и служб (Application And Services Logs)** или оба этих узла для просмотра доступных журналов.
3. Выделите журнал, который нужно просмотреть (рис.17-2).

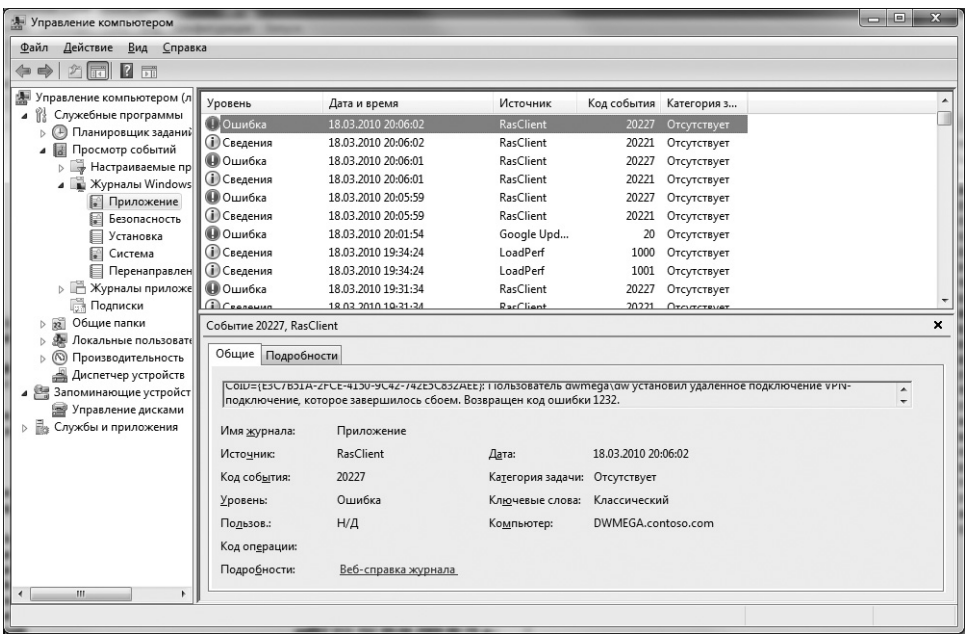

Рис. 17-2. События одного из журналов в оснастке Просмотр событий (Event Viewer)

Основные типы событий — это предупреждения и ошибки. Для выяснения причины события дважды щелкните соответствующую запись и просмотрите подробное описание события. Выясните происхождение ошибки и попытайтесь решить проблему способами, рассмотренными в этой книге. Чтобы найти дополнительные сведения об ошибке и действиях по ее устра-

нению, перейдите по ссылке **Веб-справка журнала (Event Log Online)** или проведите в базе знаний Майкрософт поиск по коду события или выдержке из описания ошибки.

Выполнение заданий по расписанию

В процессе управления настольными компьютерами и ноутбуками повседневные задачи обслуживания нередко требуется решать повторно, в том числе, периодически. Автоматизировать выполнение одноразовых или повторяющихся задач позволяет служба Планировщик заданий (Task Scheduler). Для автоматизации используются сценарии командной оболочки, WSH-сценарии или приложения, выполняющие необходимые команды. В отличие от предыдущих версий Windows 7 поставляется с обширной библиотекой готовых заданий на все случаи жизни: от удаления устройства Bluetooth до дефрагментации дисков и проверки компьютера Защитником Windows (Windows Defender).

Зачем планировать задания?

Для создания запланированных заданий в Windows 7 применяются Планировщик заданий (Task Scheduler) и инструмент командной строки Schtasks. Оба инструмента способны автоматизировать выполнение действий как на локальной, так и на удаленной системе. Планировщик заданий (Task Scheduler) включает в себя несколько мастеров с интерактивным интерфейсом для назначения заданий.

Оба планировщика следят за показаниями системных часов и запускают запланированные задания при помощи службы Планировщик заданий (Task Scheduler). Она по умолчанию выполняется от имени учетной записи Локальная система (LocalSystem). Обычно у этой учетной записи недостаточно полномочий для выполнения административных задач. Чтобы преодолеть это ограничение, запуск каждого задания выполняется от имени конкретного пользователя, учетные данные которого предоставляются во время создания задания. Убедитесь, что для выполнения запланированного задания выбираете учетную запись с надлежащими полномочиями.

Примечание Этот раздел посвящен программе Планировщик заданий (Task Scheduler) — основному инструменту для создания запланированных заданий в Windows 7. Чтобы более подробно узнать об утилите Schtasks, введите в командной строке **schtasks /?** или посмотрите информацию об этой утилите в главе 9 книги *Windows Command-Line Administrator's Pocket Consultant, Second Edition (Microsoft Press, 2008)*.

В Windows 7 применяются запланированные задания двух основных типов:

- **Стандартные задания** Применяются для автоматизации обычных задач и задач обслуживания. Они видимы для пользователей, и при необходимости их можно изменить.
- **Скрытые задания** Применяются для автоматизации специальных системных задач. По умолчанию они скрыты от пользователей, и изменять

их в большинстве случаев не следует. Некоторые скрытые задания создаются и управляются конкретными программами, например Защитником Windows (Windows Defender).

В Windows 7 процесс создания и управления заданиями заметно усложнился. Для каждого задания можно задать следующие настройки:

- Выполнять, если пользователь зарегистрирован в системе, или независимо от входа пользователя.
- Выполнять с обычными пользовательскими полномочиями или с наивысшими требуемыми полномочиями (включая административные).

Задания, созданные в Windows 7, несовместимы с предыдущими версиями ОС, поэтому, скопировав задание Windows 7 на компьютер под управлением прежней версии Windows, не ждите его выполнения. Правда, в процессе создания задания вы можете указать, что оно должно быть совместимо с предыдущими версиями Windows.

Ниже перечислены основные свойства заданий:

- **Триггеры (Triggers)** Триггеры определяют условия начала и завершения задания. Условием запуска может быть расписание, вход пользователя в систему, запуск компьютера или бездействие процессора, событие, подключение или отключение пользователя от сеанса сервера терминалов, блокирование или разблокирование пользователем рабочей станции. Наиболее интересны задания, инициируемые событиями, поскольку они позволяют автоматизировать обработку ошибок и предупреждений.
- **Действия (Actions)** Действия, выполняемые заданием: запуск программ, отправка сообщений электронной почты или вывод сообщений.
- **Условия (Conditions)** Дополнительные условия запуска и остановки назначенного задания. Условия можно применять, чтобы для выполнения задания вывести компьютер из состояния сна или запускать компьютер только при наличии определенного сетевого подключения. Условия применяются также для запуска, остановки и перезапуска задания на основе загруженности процессора. Например, можно задать запуск задания, при условии что компьютер простаивает не менее 10 минут, остановку задания, если компьютер более не простаивает, повторный запуск при следующем простое компьютера. Кроме того, условия позволяют запускать задания при наличии питания от сети и останавливать при переходе на питание от батареи.

Просмотр и управление заданиями локальной и удаленной системы

Текущие настроенные задания перечислены в узле **Планировщик заданий (Task Scheduler)** консоли Управление компьютером (Computer Management). Для просмотра и управления запланированными заданиями выполните следующие действия:

1. Откройте консоль **Управление компьютером (Computer Management)**. По умолчанию вы подключены к локальному компьютеру. Для просмотра заданий на удаленном компьютере правой кнопкой щелкните элемент **Управление компьютером (Computer Management)** в дереве консоли и выберите команду **Подключиться к другому компьютеру (Connect To Another Computer)**. В диалоговом окне **Выбор компьютера (Select Computer)** введите имя нужного компьютера и щелкните **OK**.
2. Для просмотра настроенных заданий разверните узел **Планировщик заданий (Task Scheduler)**, затем узел **Библиотека планировщика заданий (Task Scheduler Library)** и при необходимости следующие узлы.

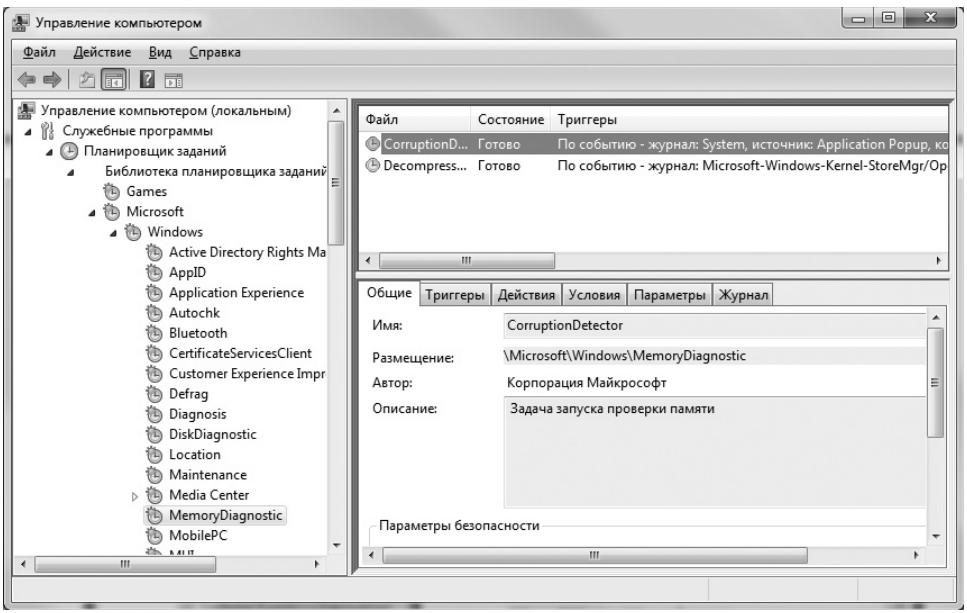

Рис. 17-3. Управление запланированными заданиями

3. Выделите задание, чтобы просмотреть его свойства (рис. 17-3). Для управления заданием щелкните его правой кнопкой и выполните одно из следующих действий:
   - Щелкните **Удалить (Delete)**, чтобы удалить задание.
   - Щелкните **Отключить (Disable)**, чтобы отключить задание.
   - Щелкните **Свойства (Properties)** для редактирования свойств задания. В диалоговом окне **Свойства (Properties)** внесите необходимые изменения и щелкните **OK**.
   - Щелкните **Экспортировать (Export)**, чтобы экспортировать задание в файл для импорта на другой компьютер. После экспорта задания подключитесь к другому компьютеру в консоли **Управление компьютером (Computer Management)**, правой кнопкой щелкните узел **Библиотека планировщика заданий (Task Scheduler Library)** и вы-

берите команду **Импортировать задачу (Import Task)**. Затем найдите и откройте задание на другом компьютере при помощи диалогового окна **Открыть (Open)**.

- Щелкните **Выполнить (Run)** для запуска задания.
- Если задание выполняется, щелкните **Завершить (End)**, чтобы завершить его.

Примечание Вы можете изменять и удалять пользовательские задания, но большинство заданий, созданных ОС, изменить или удалить нельзя. Если задания ОС не отображаются, для их просмотра выберите в меню **Вид (View)** команду **Отобразить скрытые задачи (Show Hidden Tasks)**. Обратите внимание на список **Настроить для (Configure For)** в свойствах задания. В нем можно выбрать ОС, в которых может использоваться задание.

Чтобы просмотреть задания, выполняемые на компьютере в данный момент, выполните следующие действия:

1. Откройте консоль **Управление компьютером (Computer Management)** и подключитесь к нужному компьютеру.
2. Выделите узел **Планировщик заданий (Task Scheduler)**. Щелкните его правой кнопкой и выберите команду **Отображать все выполняемые задачи (Display All Running Tasks).**

Создание запланированного задания

Чтобы создать запланированное задание, выполните следующие действия:

1. Откройте консоль **Управление компьютером (Computer Management)** и подключитесь к нужному компьютеру.
2. Выделите узел **Планировщик заданий (Task Scheduler)** и щелкните его правой кнопкой. Выберите команду **Создать задачу (Create Task)**.
3. На вкладке **Общие (General)** открывшегося окна **Создание задачи (Create Task)** введите имя задания и задайте параметры безопасности для его запуска:
   - Если задание должно выполняться не от имени текущего пользователя, щелкните кнопку **Изменить (Change User Or Group)**. В диалоговом окне **Выбор: «Пользователь» или «Группа» (Select User Or Group)** укажите пользователя или группу, от имени которой следует выполнять задание, и предоставьте необходимые учетные данные.
   - При необходимости задайте другие параметры запуска. По умолчанию задание запускается только тогда, когда пользователь зарегистрирован в системе. Если задание должно быть выполнено независимо от входа пользователя в систему, установите переключатель **Выполнять вне зависимости от регистрации пользователя (Run Whether User Is Logged On Or Not)**. Также можно задать выполнение задания с наивысшими полномочиями и настроить его для более ранних версий Windows.

4. На вкладке **Триггеры (Triggers)** щелкните кнопку **Создать (New)**, настройте параметры запуска задания и щелкните **OK**.
5. На вкладке **Действия (Actions)** задаются действия, выполняемые в рамках задания. Щелкните кнопку **Создать (New)**, настройте параметры действия и щелкните **OK**.
6. На вкладке **Условия (Conditions)** укажите ограничения запуска или остановки задания.
7. На вкладке **Параметры (Settings)** установите дополнительные параметры задания.
8. Щелкните **OK**, чтобы создать задание.

Диагностика запланированных заданий

При настройке заданий вы можете столкнуться с различными проблемами. Некоторые задания не запускаются в положенное время, другие запускаются, но не могут остановиться. Для проверки состояния задания выделите его в оснастке Планировщик заданий (Task Scheduler) и просмотрите состояние, время и результат последнего запуска. Если задание находится в состоянии **В очереди (Queued)**, оно ожидает запуска в назначенное время. Задание в состоянии **Готово (Ready)** готово к очередному запуску. Если для задания, выполняемого автоматически, в качестве состояния указано **Никогда (Never)**, проверьте свойства задания и установите причину. Если результатом последнего запуска стала ошибка, устраните проблему.

Чтобы проверить свойства задания, щелкните соответствующий элемент в оснастке Планировщик заданий (Task Scheduler). На вкладке **Журнал (History)** представлены подробные сведения о задании, начиная с создания и до последнего запуска. Эти сведения помогут вам в устранении неполадок.

Состояние задания **Работает (Running)** может говорить не только о работе, но и о зависании задания. Посмотрите на время запуска задания в столбце **Время прошлого запуска (Last Run Time)**. Если задание выполняется вторые сутки, скорее всего, произошел сбой. Сценарий может ожидать ввода, в задании могли возникнуть проблемы с чтением и записью файлов, наконец, задание могло просто зависнуть. Чтобы остановить задание, щелкните его правой кнопкой в оснастке Планировщик заданий (Task Scheduler) и выберите команду **Завершить (End)**.

Резервное копирование и восстановление компьютера

В качестве централизованной консоли для резервного копирования и восстановления компьютера в Windows 7 используется Центр архивации и восстановления (Backup And Restore Center). Чтобы открыть его, щелкните кнопку **Пуск (Start)** и выберите команду **Панель управления (Control Panel)**. Затем в разделе **Система и безопасность (System And Security)** щелкните ссылку **Архивирование данных компьютера (Back Up Your Computer)**. К другим средствам архивации и восстановления данных отно-

сятся компонент Предыдущие версии (Previous Versions), а также инструменты Восстановление запуска (Startup Repair), Загрузчик возобновления Windows (Windows Resume Loader), Восстановление системы (System Restore) и Архивация (Backup). Все эти инструменты рассмотрены ниже.

Восстановление предыдущей версии

Компонент Предыдущие версии (Previous Versions), его настройка и применение описаны в главе 6. Хотя он и не заменит полную резервную копию системы, с его помощью можно создавать автоматические резервные копии изменяемых файлов и папок на наблюдаемых дисках. Если наблюдаемый файл или папка был случайно удален или изменен, его можно восстановить до предыдущей версии, как описано в главе 6.

Восстановление после неудачного возобновления работы компьютера

При переходе компьютера под управлением Windows 7 в спящий режим или режим гибернации создается снимок его текущего состояния. При переходе в спящий режим снимок сохраняется в памяти, а при переходе в режим гибернации записывается на диск. Запись и чтение снимка выполняются Загрузчиком возобновления Windows (Windows Resume Loader).

Существует множество причин возникновения проблем с возобновлением работы компьютера, включая ошибки снимка, ошибки в памяти и ошибки на диске. Если во время пробуждения компьютера возник сбой, вы получите от загрузчика возобновления Windows предупреждение примерно следующего содержания:

```
Загрузчик возобновления Windows

Предыдущая попытка перезапуска системы из прежнего источника не удалась.
Хотите повторить попытку?

Продолжение перезапуска системы
Удалить данные восстановления и перейти к меню загрузки системы

Enter=Выбор
```

Чтобы повторить попытку возобновления состояния системы, выберите вариант **Продолжение перезапуска системы (Continue with system restart)**. Чтобы удалить сохраненное состояние компьютера и перезапустить компьютер, выберите вариант **Удалить данные восстановления и перейти к меню загрузки системы (Delete restoration data and proceed to system boot)**. Вариант с полным перезапуском, как правило, устраняет сбой, но он чреват потерей данных, если перед переходом в режим сна или гибернации работа на компьютере не была сохранена.

Исправление ошибок запуска

Для запуска компьютеру под управлением Windows 7 требуется доступ к определенным системным файлам. Если компьютер не запускается из-за повреждения или отсутствия определенного системного файла, воспользуйтесь инструментом Восстановление запуска (Startup Repair). Восстановление поврежденного или отсутствующего файла не всегда решает проблему, и для устранения более серьезной неисправности вам может потребоваться более глубокая диагностика.

Как правило, прочие проблемы запуска связаны с внесением изменений в систему, например с неправильной установкой устройства или из-за неправильного обновления конфигурации системы или реестра, приведшего к конфликту. Часто для устранения неполадок при запуске используется безопасный режим, когда в систему загружаются только основные файлы, службы и драйверы мыши, монитора, клавиатуры, запоминающих устройств и видео. Драйвер монитора обеспечивает работу монитора с базовыми параметрами и режимами; базовый драйвер видео задает общие параметры для графической платы. Сетевые службы и драйверы не запускаются, если при загрузке компьютера явно не выбран вариант Безопасный режим с загрузкой сетевых драйверов (Safe Mode With Networking). В безопасном режиме загружается ограниченный набор сведений о конфигурации, что помогает в поиске и устранении неисправностей.

Чтобы перезапустить систему в безопасном режиме, выполните следующие действия:

1. Щелкните кнопку **Пуск (Start)**, щелкните кнопку **Завершение работы (Shut Down)** и выберите вариант **Перезагрузка (Restart)**.
2. Во время загрузки нажмите клавишу F8, чтобы открыть экран Дополнительные варианты загрузки (Advanced Boot Options). Если на компьютере установлено несколько ОС или установлена Консоль восстановления (Recovery Console), на экране появится окно диспетчера загрузки Windows. В качестве загружаемой ОС выберите Windows 7 и нажмите F8.
3. Клавишами-стрелками выберите тип безопасного режима и нажмите Enter. Подходящий тип безопасного режима зависит от типа неисправности. Основные варианты таковы:
   - **Восстановление системы (Repair Your Computer)** Загрузка инструмента Восстановление запуска (Startup Repair), о котором будет рассказано далее в разделе «Восстановление компьютера».
   - **Безопасный режим (Safe Mode)** В ходе инициализации системы загружаются только основные файлы, службы и драйверы: мыши, монитора, клавиатуры, запоминающих устройств и базового видео. Сетевые службы и драйверы не загружаются.
   - **Безопасный режим с загрузкой сетевых драйверов (Safe Mode With Networking)** Загрузка основных файлов, служб и драйверов, а также служб и драйверов, необходимых для работы в сети.

- **Безопасный режим с поддержкой командной строки (Safe Mode With Command Prompt)** Загрузка основных файлов, служб и драйверов. Вместо графического интерфейса Windows 7 открывается командная строка. Сетевые службы и драйверы не запускаются.

Совет В безопасном режиме с поддержкой командной строки вы также вольны запустить оболочку Проводника (Explorer). Откройте Диспетчер задач (Task Manager), нажав на Ctrl+Shift+Esc. В меню **Файл (File)** выберите команду **Новая задача (New Task)**. В окне **Новая задача (New Task)** введите **explorer.exe** и щелкните **OK**.

- **Ведение журнала загрузки (Enable Boot Logging)** Запись всех событий запуска в журнал загрузки.
- **Включение видеорежима с низким разрешением (Enable low-resolution video)** Запуск системы в режиме с низким разрешением монитора (640 × 480). Это полезно, если системный дисплей настроен на работу в режиме, который не поддерживается текущим монитором.
- **Последняя удачная конфигурация (Last Known Good Configuration)** Запуск компьютера в безопасном режиме с использованием информации реестра, сохраненной при последнем завершении работы. Загружается только раздел HKEY_CURRENT_CONFIG (HKCC). В нем хранятся сведения о конфигурации оборудования, с которой компьютер ранее был успешно запущен.
- **Отключить автоматическую перезагрузку при отказе системы (Disable Automatic Restart On System Failure)** Запрет на перезапуск Windows после сбоя. Многократная перезагрузка Windows может привести к проблеме с конфигурацией микропрограммы, описанной в главе 10.
- **Отключение обязательной проверки подписи драйверов (Disable Driver Signature Enforcement)** Запуск компьютера в безопасном режиме без применения политики использования цифровых подписей драйверов. Если причиной сбоя стал драйвер с неверной или несуществующей цифровой подписью, вы временно устраните проблему, сможете запустить компьютер и устранить неполадку путем установки нового драйвера или изменения параметров проверки подписи драйверов.

4. Если после запуска в безопасном режиме неполадка не обнаружена, можно исключить из списка возможных причин стандартные параметры и драйверы основных устройств. Если проблема вызвана недавно установленным устройством или обновленным драйвером, работая в безопасном режиме, удалите устройство, откатите обновление или установите другую версию драйвера.
5. Если во время обычного запуска системы по-прежнему возникают проблемы и вы подозреваете наличие неполадок с оборудованием, ПО или параметрами, снова перезагрузитесь в безопасном режиме и попробуй-

те отменить изменения в программе Восстановление системы (System Restore), как описано далее в этой главе.

6. Если программа Восстановление системы (System Restore) не помогла, попробуйте изменить параметры запуска, как описано в разделе «Управление конфигурацией, запуском и загрузкой системы» главы 6.

Компонент Восстановление системы (System Restore)

Компонент Восстановление системы (System Restore) представлен в разделе «Вкладка Защита системы (System Protection)» главы 6. При помощи точек восстановления можно восстановить систему, в которой неполадки возникли после обновления, установки ПО, установки оборудования и других изменений. Следующие разделы посвящены созданию точек восстановления вручную и восстановлению системы с их помощью. В большинстве случаев операция по восстановлению является обратимой.

Основные сведения о точках восстановления

Компонент Восстановление системы (System Restore) отслеживает изменения в ОС и ежедневно перед внесением изменений создает точку восстановления, то есть снимок системной конфигурации компьютера, и записывает ее на диск с возможностью последующего восстановления системы до сохраненного состояния. Важная деталь: компонент Восстановление системы (System Restore) не затрагивает личные данные. Система восстанавливается из точки восстановления с сохранением пользовательских данных приложений, файлов кеша и документов пользователя. Никакой информации в папку Документы (Documents) компонент Восстановление системы (System Restore) не записывает.

Сведения о конфигурации записываются отдельно для каждого диска компьютера. Это означает, что на каждом диске компонент Восстановление системы (System Restore) занимает некоторое пространство. Наблюдение за конкретными дисками можно отключить. Если за диском ведется наблюдение, при сбое вы сможете отменить внесенные изменения. Если за диском не ведется наблюдение, изменения конфигурации не отслеживаются, и вносимые изменения отменить нельзя. В большинстве систем Восстановление системы (System Restore) включают на системном диске, где хранятся файлы ОС, и на всех дисках с критически важными приложениями.

Восстановление из точки восстановления выполняется одним из трех способов: по контрольной точке, по дате или по событию. Отдельные снимки, время создания которых определяется ОС, называются системными контрольными точками. Первый снимок состояния (начальная системная контрольная точка) создается автоматически во время установки Windows 7. Остальные системные контрольные точки создаются примерно каждые 24 часа. Если в момент создания ежедневной контрольной точки компьютер выключен, она будет создана при следующем запуске компьютера.

Некоторые снимки создаются автоматически при наступлении событий, генерируемых ОС при внесении изменений или установке приложений. Для простоты я называю все эти точки *установочными точками восстановления*. Но на самом деле их много, и у каждой — свое назначение. Снимки создаются при следующих событиях:

- **Установка программы** Контрольная точка создается перед установкой программы с использованием совместимого установщика. Такие точки восстановления применяются для отслеживания установки приложения и восстановления компьютера до состояния, предшествующего установке. Восстановление состояния компьютера состоит в удалении всех файлов и параметров реестра установленной программы. Кроме того, к исходному состоянию восстанавливаются программы и системные файлы, измененные в процессе установки. После восстановления установленная программа работать не будет, и для дальнейшей работы с ней программу придется переустановить.

Внимание! В процессе восстановления из этой точки файлы установленного приложения не удаляются. Удаляются лишь файлы и параметры реестра, влияющие на работу компьютера. Чтобы полностью удалить программу, используйте утилиту Программы (Programs) из панели управления.

- **Автоматическое обновление** Точка восстановления создается перед применением автоматического обновления. Если после автоматического обновления на компьютере возникли неполадки, при помощи этой точки вы восстановите компьютер до прежнего состояния. Для удаления автоматического обновления годится также утилита Программы (Programs) из панели управления.
- **Операция восстановления** Точки восстановления этого типа создаются перед восстановлением компьютера. Если потом окажется, что точка восстановления выбрана неверно или неработоспособна, при помощи этих точек восстановления можно отменить операцию восстановления и вернуть компьютер к состоянию, предшествовавшему отмене предыдущих параметров.
- **Неподписанный драйвер устройства** Точка восстановления создается перед установкой на компьютер неподписанного или не прошедшего сертификацию драйвера. Если после установки такого драйвера на компьютере возникли неполадки, эта точка восстановления поможет восстановить компьютер к состоянию, предшествующему установке драйвера. Если драйвер имеет подпись и сертификат, для возврата к ранее используемому драйверу используется обычная процедура отката.
- **Восстановление в программе Архивация (Backup)** Контрольные точки, создаваемые перед восстановлением файлов или системных данных в программе Архивация (Backup). В случае сбоя восстановления или ненормальной работе компьютера после восстановления вы сможете отменить изменения, вернув компьютер в исходное состояние.

Пользователи вольны создавать снимки состояния вручную. Такие снимки называются *пользовательскими точками восстановления*. Порекомендуйте пользователям создавать снимки перед выполнением любой операции, способной отрицательно повлиять на систему.

Восстановление компьютеров выполняется в обычном или безопасном режиме. При этом контрольная точка восстановления создается перед восстановлением компьютера только в обычном режиме. Изменения, вносимые в безопасном режиме, не отслеживаются, и вы не сможете их отменить. Однако в безопасном режиме можно использовать любую из созданных ранее точек восстановления.

Создание пользовательской точки восстановления

Чтобы создать точку восстановления вручную, выполните следующие действия:

1. На панели управления щелкните категорию **Система и безопасность (System And Security)**. Затем щелкните команду **Система (System)**.
2. На левой панели щелкните команду **Защита системы (System Protection)**.
3. Выберите диск, для которого нужно создать точку восстановления, и щелкните **Создать (Create)**.
4. Введите описание точки восстановления, например **Обновление драйвера монитора**. Щелкните **Создать (Create)**.

   Когда точка восстановления будет создана, щелкните **OK**.

Восстановление при помощи точки восстановления

Чтобы восстановить компьютер из точки восстановления, выполните следующие действия:

1. На панели управления перейдите по ссылке **Архивирование данных компьютера (Back Up Your Computer)** в разделе **Система и безопасность (System And Security)**.
2. Перейдите по ссылке **Восстановить системные параметры или компьютер (Recover System Settings On Your Computer)**.
3. Щелкните **Запуск восстановления системы (Open System Restore).** Проверка доступных точек восстановления в программе Восстановление системы (System Restore) может занять несколько минут. После завершения проверки щелкните **Далее (Next)**.
4. Вам будет предложено несколько точек восстановления. В их описании содержится дата, время, описание и тип. Чтобы узнать, на какие программы повлияет операция восстановления, выделите точку восстановления и щелкните **Поиск затрагиваемых программ (Scan For Affected Programs)**.
5. Для просмотра других доступных точек восстановления установите флажок **Показать другие точки восстановления (Show More Restore Points)**.

6. Выделите нужную точку восстановления и щелкните **Далее (Next)**.
7. Щелкните **Готово (Finish)**. Подтвердите намерение восстановить системные файлы и параметры компьютера, щелкнув **Да (Yes)**.

В ходе восстановления компьютер будет перезагружен. По завершению восстановления Windows 7 будет загружена с параметрами, имевшимися на момент создания снимка. После перезапуска системы на экране вновь появится диалоговое окно **Восстановление системы (System Restore)**. Прочитайте сообщение и закройте окно. В случае ненормальной работы Windows 7 примените другую точку восстановления или отмените операцию восстановления, повторив вышеописанную процедуру и выбрав точку восстановления, которая была создана до применения текущего состояния системы.

Диагностика восстановления системы

Попытка восстановить систему в компоненте Восстановление системы (System Restore) не всегда заканчивается успехом. В случае неудачного восстановления компьютера к выбранному моменту времени повторите процедуру, чтобы попытаться восстановить компьютер из другой точки восстановления.

Работа с резервными копиями

В комплект профессиональной, корпоративной и максимальной версий Windows 7 входит Центр архивации и восстановления (Backup And Restore Center). Это средство предназначено для автоматического резервного копирования и создания полной резервной копии компьютера. Для выполнения архивации и восстановления файлов вы должны обладать соответствующими разрешениями.

Настройка резервного копирования

В Windows 7 имеется возможность автоматической архивации как личных данных, так и образа системы. Архивация личных данных предназначена для периодического сохранения изображений, музыки, видео, сообщений электронной почты, документов и ценных файлов. Цель архивации образа системы состоит в периодическом резервном копировании системного и других дисков, необходимых для работы Windows. Архивы с личными данными предназначены для восстановления пользовательских данных. Архивный образ системы применяется для восстановления компьютера.

Для выполнения автоматического резервного копирования в назначенное время компьютер должен быть включен. Архивы нельзя сохранять на системном диске, загрузочном диске или ленте. Архивы личных данных сохраняют на флеш-накопителях, CD/DVD-дисках и в сетевых папках независимо от способа их форматирования (FAT или NTFS). Архивные образы системы можно сохранять на встроенных дисках, флеш-накопителях, CD/DVD-дисках и в сетевых NTFS-папках.

По умолчанию архивация по расписанию выполняется каждое воскресение в 19.00. На рабочих местах, где компьютеры на выходные отключают, это расписание необходимо изменить.

Чтобы настроить автоматизированную архивацию, выполните следующие действия:

1. На панели управления перейдите по ссылке **Архивирование данных компьютера (Back Up Your Computer)** в разделе **Система и безопасность (System And Security)**. Откроется страница Архивация и восстановление файлов (Backup and Restore), показанная на рис. 17-4.

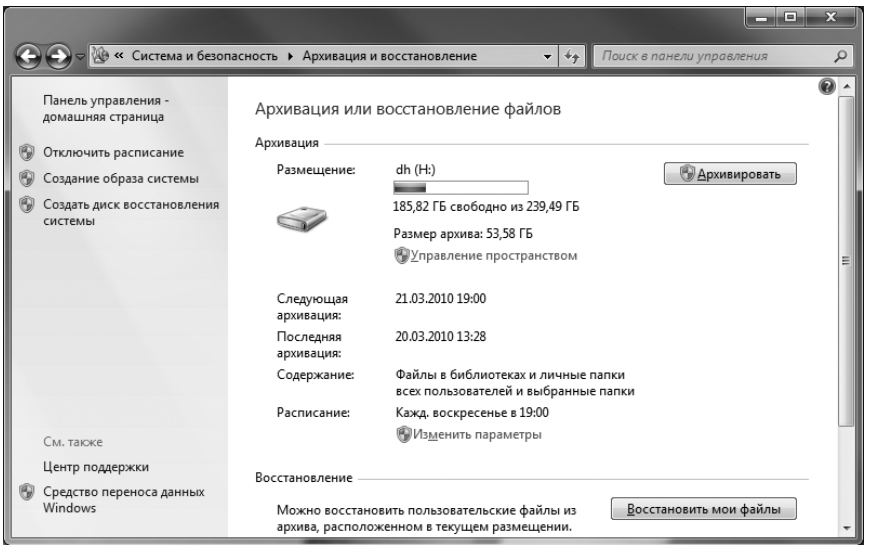

Рис. 17-4. Управление архивами в Центре архивации и восстановления (Backup And Restore Center)

2. Если автоматизированное резервное копирование еще не настроено, щелкните **Настроить резервное копирование (Set Up Backup)**. В противном случае щелкните **Изменить параметры (Change Settings)**.
3. На странице **Выберите, где следует хранить создаваемые архивы (Select Where You Want To Save Your Backup)** укажите расположение архива: локальный диск, CD/DVD-диск, флеш-накопитель или сетевой ресурс. Щелкните **Далее (Next)**. При архивации на CD/DVD будьте готовы вставить другой диск, если на один диск копия не поместится.
4. На странице **Что следует архивировать (What Do You Want To Back Up)** выберите один из следующих переключателей и щелкните **Далее (Next)**:
   - **Предоставить выбор Windows (Let Windows Choose)** Архивация всех личных данных в папках профиля пользователя и библиотеках, а также создание образа системы.
   - **Предоставить мне выбор (Let Me Choose)** Самостоятельный выбор архивируемых личных и системных данных.

5. Если вы выбрали вариант **Предоставить мне выбор (Let Me Choose)**, укажите личные данные, которые нужно архивировать. Можно выбрать отдельные папки и библиотеки, развернув узлы **Файлы данных (Data Files)** и **Компьютер (Computer)**. Флажок **Включить образ системы (Include A System Image)** установлен по умолчанию, обеспечивая создание архива системы (что чаще всего и нужно). Задав требуемые параметры, щелкните **Далее (Next)**.
6. На странице **Проверьте еще раз параметры архивации (Review Your Backup Settings)** щелкните **Изменить расписание (Change Schedule)**. В списке **Как часто (How Often)** задайте периодичность выполнения — **Ежедневно (Daily)**, **Еженедельно (Weekly)** или **Ежемесячно (Monthly)**. Выбрав еженедельное и ежемесячное архивирование, в списке **В какие дни (What Day)** укажите день недели или месяца. Наконец, в списке **В какое время (What Time)** установите время выполнения архивации. Щелкните **OK**.
7. Если это первая резервная копия, щелкните **Сохранить параметры и запустить архивацию (Save Settings And Run Backup)**, чтобы сохранить параметры и расписание архивации и создать первую резервную копию. Если это не первая резервная копия компьютера, у вас будет возможность **Сохранить параметры и выйти (Save Settings And Exit)**.

Настроив автоматизированную архивацию, вы в любое время сможете запускать ее и вручную с этими же параметрами. Откройте программу **Архивация и восстановление (Backup And Restore)** и щелкните **Архивировать (Back Up Now)**. Чтобы вручную создать архив системного образа, выполните следующие действия:

1. На панели управления перейдите по ссылке **Архивирование данных компьютера (Back Up Your Computer)** в разделе **Система и безопасность (System And Security)**. На левой панели щелкните **Создание образа системы (Create A System Image)**.
2. На странице **Где следует сохранять архив (Where Do You Want To Save The Backup)** укажите расположение архива. Щелкните **Далее (Next)**.
3. На странице **Какие диски нужно включить в архивацию (Which Drives Do You Want To Include In The Backup)** системный диск выбран по умолчанию. Его невозможно исключить, но в архив образа можно добавить другие диски, устанавливая соответствующие флажки. Для продолжения щелкните **Далее (Next)**.
4. Щелкните **Архивировать (Start Backup)**.

Резервные копии — управление и диагностика

Программа Архивация и восстановление (Backup And Restore) позволяет управлять и диагностировать архивы. В ее окне вы найдете основные сведения о об архивах, включая их расположение и размер. Для получения более подробных сведений об использовании диска программой Архивация

Windows (Windows Backup) щелкните ссылку **Управление пространством (Manage Space)**. В диалоговом окне **Управление дисковым пространством архивации данных (Manage Windows Backup Disk Space)** можно выполнить следующие действия (рис. 17-5):

- просмотреть отчет об использовании диска;
- найти расположение архива, щелкнув ссылку **Обзор (Browse)**;
- управлять файлами данных, щелкнув **Просмотреть архивы (View Backups)** и выделив удаляемый набор резервных копий;
- изменить параметры архивации образа системы для экономии дискового пространства.

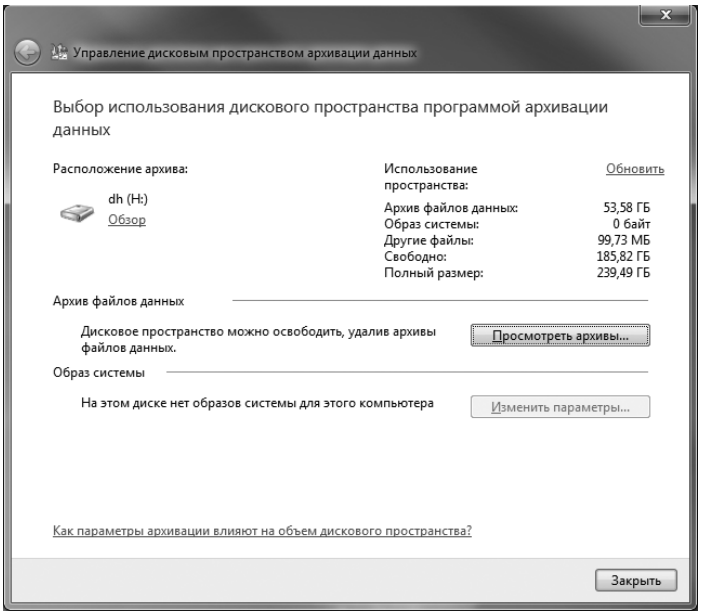

Рис. 17-5. Управление дисковым пространством архивов

Чтобы изменить расписание архивации, выполните следующие действия:

1. На панели управления перейдите по ссылке **Архивирование данных компьютера (Back Up Your Computer)** в разделе **Система и безопасность (System And Security)**.
2. В разделе **Расписание (Schedule)** щелкните **Изменить параметры (Change Settings)**, после чего выполните шаги 3–7 из процедуры настройки автоматизированной архивации.

Чтобы отключить автоматизированную архивацию, выполните следующие действия:

1. На панели управления перейдите по ссылке **Архивирование данных компьютера (Back Up Your Computer)** в разделе **Система и безопасность (System And Security)**.

2. В левой панели щелкните **Отключить расписание (Turn Off Schedule)**.

Если во время резервного копирования файлов в программе Архивация Windows (Windows Backup) возникнут неполадки, вы получите предупреждение или сообщение об ошибке со сведениями о проблеме.

Чтобы устранить неполадку, щелкните кнопку **Параметры (Options)**. На экране появится диалоговое окно **Архивация данных: варианты устранения неполадок (Windows Backup: Troubleshooting Options)**. Набор возможностей зависит от типа предупреждения или ошибки. В случае появления предупреждения вам будет предложено просмотреть пропущенные файлы и изменить параметры архивации. В случае ошибки вам будет предложено изменить параметры архивации и повторить ее.

Принимая решение, щелкните ссылку **Показать сведения (Show Details)** для получения информации о времени архивации и расположении архива. Если к моменту архивации компьютер пользователя или сервер, указанный в расположении архива, был выключен или находился не в сети, вы сможете выполнить архивацию еще раз. Если в расположении архива недостаточно свободного места, необходимо изменить параметры архивации, указав новое расположение.

Восстановление личных данных

Чтобы восстановить личные файлы данных из резервной копии, выполните следующие действия:

1. На панели управления перейдите по ссылке **Архивирование данных компьютера (Back Up Your Computer)** в разделе **Система и безопасность (System And Security)**.
2. Щелкните **Восстановить мои файлы (Restore My Files)**.

Если восстанавливаемые элементы находятся в текущем расположении архивов, отметьте нужные элементы в окне **Восстановление файлов (Restore Files)**, щелкните **Далее (Next)** и следуйте подсказкам. Ваши возможности при выборе элементов таковы:

- **Обзор файлов (Browse For Files)** Поиск в архиве файлов, которые нужно восстановить. Все файлы будут восстановлены до самой последней версии.
- **Обзор папок (Browse For Folders)** Поиск в архиве папок, которые нужно восстановить. Все папки и их содержимое будут восстановлены до последней версии.
- **Поиск (Search)** Поиск файлов и папок, которые нужно восстановить. Все выбранные файлы и папки будут восстановлены до последней версии.
- **Выбрать другую дату (Choose A Different Date)** Восстановление файлов из другого архива. В диалоговом окне **Восстановление файлов (Restore Files)** содержится список всех резервных копий по времени архивации. Выделите резервную копию, из которой следует восстановить файлы, после чего найдите нужные файлы.

Если восстанавливаемые файлы находятся в другом расположении, щелкните **Выбрать другую резервную копию для восстановления файлов (Select Another Backup To Restore Files From)**. В диалоговом окне **Восстановление файлов (для опытных) (Restore Files — Advanced)** содержится список всех резервных копий по времени архивации, компьютеру и расположению резервной копии. Выделите резервную копию, из которой следует восстановить файлы, после чего найдите нужные файлы.

Восстановление компьютера

Во время установки Windows 7 автоматически создается раздел среды восстановления Windows (Windows RE). Для восстановления компьютера при помощи Windows RE выполните следующие действия:

1. Если компьютер работает, но загружается с ошибками, щелкните **Пуск (Start)**. В меню **Пуск (Start)** щелкните кнопку **Завершение работы (Shut Down)** и выберите команду **Перезагрузка (Restart)**.
2. Во время запуска нажмите клавишу F8, чтобы открыть экран **Дополнительные варианты загрузки (Advanced Boot Options)**. Если на компьютере установлено несколько ОС, откроется окно диспетчера загрузки Windows. Нажмите F8.
3. При помощи клавиш-стрелок выберите в меню **Дополнительные варианты загрузки (Advanced Boot Options)** команду **Восстановление системы (Repair Your Computer)** и нажмите Enter.
4. На компьютер будет загружена среда Windows RE. В диалоговом окне **Параметры восстановления компьютера (System Recovery Options)** выберите язык и раскладку клавиатуры. Щелкните **Next (Далее)**.
5. Для доступа к параметрам восстановления нужно выполнить вход с учетной записью локального администратора. Выберите учетную запись локального администратора, введите ее пароль и щелкните **OK**.
6. В диалоговом окне **Параметры восстановления компьютера (System Recovery Options)** найдите расположение ОС, после чего выберите один из следующих вариантов восстановления:
   - **Восстановление запуска (Startup Repair)** Этот вариант подходит для разрешения проблем, препятствующих запуску Windows, включая неверные записи в хранилище данных конфигурации загрузки, повреждение системных файлов и повреждение диспетчеров загрузки. Обычно при обнаружении устранимой неполадки это средство запускается автоматически.
   - **Восстановление системы (System Restore)** Этот вариант предназначен для открытия программы Восстановление системы (System Restore), позволяющей восстановить ранее сохраненное состояние Windows. Если система не запускается из-за внесенных в конфигурацию изменений или после установки приложения, при наличии то-

чек восстановления вы сможете восстановить Windows до состояния, предшествующего внесению изменений.

- **Восстановление образа системы (System Image Recovery)** Полное восстановление компьютера при помощи заранее созданного образа системы. Если не удается восстановить компьютер при помощи восстановления запуска, восстановления системы и других средств, при наличии образа системы вы сможете восстановить компьютер из архива.
- **Средство диагностики памяти Windows (Windows Memory Diagnostics)** Выберите этот вариант, если у вас есть подозрения на наличие неполадок с памятью, обнаружить которые автоматически не удалось.
- **Командная строка (Command Prompt)** Доступ к командной строке для работы с командами и инструментами, доступными в среде восстановления.

Если восстановить Windows другими способами не удалось, последний выход — переустановка Windows 7. Прежде чем это сделать, попытайтесь восстановить компьютер в компонентах Восстановление запуска (Startup Repair) и Восстановление системы (System Restore). Если и это не поможет, попробуйте восстановить компьютер при помощи образа системы.

Устранение неполадок запуска и выключения

Администратору часто приходится устранять неполадки с запуском и выключением компьютера. В этом разделе мы рассмотрим способы разрешения типичных проблем.

Проблемы при перезапуске и выключении

Обычно для выключения или перезапуска Windows 7 используется кнопка **Завершение работы (Shut Down)** в меню **Пуск (Start)**. Но случается так, что нормально выключить или перезапустить Windows 7 не удается, и требуется предпринимать дополнительные меры. В этом случае выполните следующие действия:

1. Нажмите Ctrl+Alt+Del. В открывшемся окне щелкните **Запустить диспетчер задач (Start Task Manager)**.
2. На вкладке **Приложения (Applications)** попытайтесь найти приложение, которое не отвечает. Если выяснилось, что все программы работают нормально, перейдите к шагу 5.
3. Выделите неотвечающее приложение и щелкните **Снять задачу (End Task)**.
4. Если приложение не ответило на запрос, вам будет предложено завершить приложение или отменить запрос на снятие задачи. Щелкните **Завершить сейчас (End Now)**.

5. Попытайтесь выключить или перезапустить компьютер. Еще раз нажмите Ctrl+Alt+Del. Щелкните кнопку со стрелкой, расположенную справа от кнопки завершения работы и выберите команду **Перезагрузка (Restart)** или **Завершение работы (Shut Down)**.

В Windows 7 для отключения текущего пользователя и выключения компьютера можно также нажать на кнопку питания компьютера. Если некоторые программы не отвечают, вам будет предложено выйти из системы принудительно, или через несколько секунд принудительный выход из системы будет инициирован Windows.

Ближе к реальности В качестве крайней меры вам, возможно, придется выполнить некорректное выключение, нажав и удержав кнопку питания компьютера или отключив компьютер от сети. Скорее всего, после такого выключения при следующем запуске компьютера будет открыта программа Проверка диска (Check Disk). Это нужно, чтобы найти ошибки и неисправности, вызванные некорректным завершением работы. Если программа Проверка диска (Check Disk) не запустилась автоматически, ее следует запустить вручную.

Анализ STOP-ошибок

В разделе «Настройка загрузки и восстановления системы» главы 6 рассматривалась настройка записи отладочной информации в Windows 7. Если во время запуска Windows 7, установки программы или выполнения другой операции произошла серьезная ошибка, на экране появится сообщение о STOP-ошибке. Внимательно прочитайте сообщение и запишите следующие сведения:

- **Имя ошибки** Оно записано в третьей строке экрана ошибки заглавными буквами, например KERNEL_STACK_INPAGE_ERROR.
- **Рекомендации по устранению** За именем ошибки следуют рекомендации по ее устранению. Рекомендации опираются на тип ошибки и содержат общие советы по разрешению проблемы.
- **Номер ошибки** После рекомендаций следует техническая информация. В следующей строке под заголовком Technical Information вы увидите слово Stop, номер ошибки и список ее параметров. Следующий за словом Stop номер ошибки нужно записать, например STOP: 0X00000050.
- **Сведения о драйвере** Сразу за строкой, содержащей номер STOP-ошибки, следует строка с именем драйвера, связанного с ее возникновением. Эти сведения отображаются, только если удается отследить проблемный драйвер. Запишите имя драйвера.

Если в параметрах системы задана запись события в журнал событий при наступлении STOP-ошибки и если была возможность записать событие до полного прекращения работы системы, номер и параметры ошибки вы найдете в журнале **Система (System)** с источником события Save Dump. В событии также указано, был ли создан файл дампа и если да, то где он сохранен.

Ближе к реальности В Windows 7 имеется компонент Online Crash Analysis, позволяющий отправлять файл дампа в службу поддержки Майкрософт. Если у вас включено создание отчетов об ошибках, после перезапуска системы вам будет предложено отправить в Майкрософт отладочную информацию. Сделать это можно анонимно или при помощи учетной записи Microsoft Connect. Если вы отправите отладочную информацию от своего имени через службу Microsoft Connect, указав контактный телефон, с вами для получения более подробных сведений может связаться технический специалист. Он, возможно, даст вам рекомендации по устранению неисправности.

Собрав информацию о STOP-ошибке, перезагрузите систему в безопасном режиме, как описано ранее. Средства решения проблемы можно найти следующим образом:

- **Поиск STOP-ошибки в Базе знаний Майкрософт** Посетите страницу support.microsoft.com и выполните поиск в базе знаний Microsoft, используя номер ошибки в качестве ключевого слова. Если коду ошибки соответствует известная проблема, вы найдете в базе знаний нужную статью. Следуйте инструкциям по устранению неисправности.
- **Проверьте драйвер (если в сообщении были сведения о драйвере)** После перезагрузки проверьте драйвер на наличие цифровой подписи. Если драйвер был недавно обновлен, возможно, стоит вернуться к предыдущей версии. Наличие драйвера в сообщении об ошибке еще не значит, что драйвер поврежден. Причиной STOP-ошибки могут быть другие факторы.
- **Вспомните, что изменилось в последнее время** Причиной STOP-ошибки может быть как оборудование, так и ПО. Подробно рассмотрите все программы и оборудование, недавно установленные на компьютер. Если добавлено оборудование, проверьте правильность его установки и наличие новейших версий подписанных драйверов. Если добавлено ПО, проверьте, успешно ли завершилась установка. Также проверьте наличие обновлений и исправлений для ПО.
- **Проверьте ресурсы системы** Возникновение STOP-ошибки может быть обусловлено нехваткой памяти или дискового пространства. После запуска системы проверьте диски на наличие свободного места и при необходимости освободите место на диске при помощи утилиты Очистка диска (Disk Cleanup) или других средств. Откройте Диспетчер задач (Task Manager) и на вкладке **Быстродействие (Performance)** проверьте объем доступной физической и виртуальной памяти. При нехватке памяти определите, какие программы чрезмерно используют память и нет ли в системе вредоносных программ, например, рекламных или шпионских.
- **Восстановите системные файлы** Причиной STOP-ошибки может стать повреждение или несоответствие версии системных файлов. Если по вашему мнению причиной STOP-ошибки стал системный файл, следует восстановить или переустановить ОС, как описано выше.
- **Проверьте оборудование и микропрограммы** Причиной STOP-ошибки может стать сбойное оборудование. Если аварийное завершение работы компьютера происходит часто, внимательно изучите оборудование.

Проверьте драйверы оборудования — причина STOP-ошибки может заключаться именно в них. Проверьте само оборудование. Обратите особое внимание на жесткие диски, память, процессор и графические платы. Возможны дефекты в памяти, сбой жесткого диска, перегрев процессора, несовместимость графической платы с Windows 7. Исследуйте также и микропрограммы. Проверьте наличие у производителя обновлений для материнской платы.

Об авторе

Уильям Р. Станек (William R. Stanek) (*http://www.williamstanek.com*) обладает более чем двадцатилетним практическим опытом в области программирования и разработки. Он ведущий эксперт по компьютерным технологиям, блестящий преподаватель, автор более 100 книг, включая *Active Directory Administrator's Pocket Consultant*, *Windows Group Policy Administrator's Pocket Consultant*, *Windows PowerShell 2.0 Administrator's Pocket Consultant u Windows Server 2008 Inside Out*. На протяжении многих лет его практические советы помогают миллионам профессионалов во всем мире.

Уильям Станек участвует в коммерческом Интернет-сообществе с 1991 г. Основу его делового и технологического опыта составили 11 лет военной службы. Он также обладает значительным опытом в разработке серверных технологий, шифрования и решений Интернета. Им написано множество руководств и учебных курсов по самым разнообразным вопросам. Он часто выступает в роли эксперта и консультанта.

Уильям Станек с отличием защитил степень магистра информационных систем и степень бакалавра информатики. Он гордится тем, что во время войны в Персидском заливе принимал участие в боевых действиях в составе экипажа самолета радиоэлектронной борьбы. Он неоднократно совершал боевые вылеты в Ирак и награжден девятью медалями, включая одну из высочайших наград США — крест Air Force Distinguished Flying Cross. В настоящее время он живет на северо-западе США с женой и детьми.

Ищите Уильяма на Twitter — WilliamStanek.

Станек Уильям Р.

Windows 7.
Справочник администратора

Совместный проект издательства «Русская Редакция» и издательства «БХВ-Петербург».

РУССКАЯ РЕДАКЦИЯ bhv®

Подписано в печать 21.05.10. Формат 70×100 1/16.
Печать офсетная. Физ. печ. л. 45. Тираж 1500 экз. Заказ №

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

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

Windows® 7

Справочник администратора

В этой книге вы найдете ответы на вопросы, касающиеся повседневной работы администратора Windows 7. Пошаговые инструкции, многочисленные таблицы, списки важнейших параметров и иллюстрации помогут быстро и успешно решать любые проблемы.

В этой книге:

- управление конфигурацией системы, запуском и загрузкой;
- развертывание и настройка операционной системы;
- настройка параметров и предпочтений групповой политики;
- установка оборудования и драйверов;
- администрирование дисков, файловых систем и памяти;
- настройка и устранение неполадок сетей TCP/IP;
- настройка удаленного доступа, мобильных компьютеров и беспроводных сетей;
- управление доступом, безопасностью и доступностью общих ресурсов;
- использование удаленного управления и предоставление удаленной помощи;
- технологии TPM и BitLocker® Drive Encryption;
- устранение неполадок системы.

Каждая книга серии **Справочник администратора** (Administrator's Pocket Consultant) объединяет в себе руководство по эксплуатации и подробный справочник по основным функциям и параметрам системы.

Компактный справочник администратора — ваш идеальный помощник в повседневной работе!

Издательство
БХВ-Петербург
Санкт-Петербург,
Измайловский пр., 29
Тел.: (812) 251-4244
E-mail: mail@bhv.ru
Internet: www.bhv.ru

Издательство
Русская Редакция
Москва, Шелепихинская наб., 32
Тел.: (495) 638-5-638
Тел./факс: (495) 256-7145
E-mail: info@rusedit.com
Internet: www.rusedit.com

ISBN 978-5-7502-0399-4

bhv®

РУССКАЯ РЕДАКЦИЯ