

Ольга Кокорева

Реестр Windows 7

Санкт-Петербург

«БХВ-Петербург»

2010

УДК 681.3.06
ББК 32.973.26-018.2
К59

Кокорева О.

К59 Реестр Windows 7. — СПб.: БХВ-Петербург, 2010. — 704 с.: ил.
+ CD-ROM — (Мастер)

ISBN 978-5-9775-0485-0

Книга посвящена реестру операционной системы Windows 7, настройка и функционирование которой существенно зависит от него. Основное внимание уделено изменениям, внесенным в Windows 7, поскольку многие старые советы касательно редактирования реестра более ранних версий Windows в Windows 7 работать не будут. Обсуждаются методы резервного копирования и восстановления реестра, устранения неполадок в работе системы, вызванных его повреждением. Приводятся рекомендации по предотвращению сбоев системы и решению разнообразных проблем посредством редактирования реестра. Рассматривается работа с аппаратными средствами ПК, настройка и конфигурирование сети. Особое внимание уделяется вопросам безопасности и защиты реестра, а также управлению рабочими средами пользователей.

Прилагаемый компакт-диск содержит иллюстрации, фрагменты, не вошедшие в печатное издание книги, а также справочную информацию для углубленного изучения.

Для системных администраторов и опытных пользователей

УДК 681.3.06
ББК 32.973.26-018.2

Группа подготовки издания:

Главный редактор	<i>Екатерина Кондукова</i>
Зам. главного редактора	<i>Евгений Рыбаков</i>
Зав. редакцией	<i>Григорий Добин</i>
Компьютерная верстка	<i>Натали Каравасовой</i>
Корректор	<i>Виктория Пиотровская</i>
Дизайн серии	<i>Инны Тачиной</i>
Оформление обложки	<i>Елены Беляевой</i>
Зав. производством	<i>Николай Тверских</i>

Лицензия ИД № 02429 от 24.07.00. Подписано в печать 27.11.09.

Формат 70×100¹/₁₆. Печать офсетная. Усл. печ. л. 56,76.

Тираж 2000 экз. Заказ №

"БХВ-Петербург", 190005, Санкт-Петербург, Измайловский пр., 29.

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

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

ISBN 978-5-9775-0485-0

© Кокорева О., 2009
© Оформление, издательство "БХВ-Петербург", 2009

Оглавление

Введение.....	1
Цели этой книги	3
Глава 1. Обзорная информация о реестре Windows 7	11
Краткая историческая справка по реестру	12
Неудобства работы с INI-файлами	14
Введение реестра	15
Роль и место реестра в общесистемной архитектуре Windows 7.....	16
Цели и задачи реестра.....	18
Структура реестра	27
Хранение данных реестра.....	31
Атомарность и восстановление ульев реестра	37
Сброс данных.....	38
Усовершенствования реестра, появившиеся в Windows Vista и Windows 7	39
Когда следует браться за редактирование реестра	41
Альтернативы редактированию реестра.....	42
Изменение конфигурации в Панели управления	43
Другие инструментальные средства для изменения реестра	48
Заключение	48
Глава 2. Методы восстановления поврежденной системы	49
Подготовка к редактированию реестра	50
Средство восстановления системы	51
Точки восстановления	52
Создание точки восстановления	53
Восстановление состояния системы.....	56
Отмена операции восстановления	63
Восстановление предыдущих версий файлов	65
Ручное конфигурирование функции защиты системы	69
К вопросу об объеме свободного дискового пространства для средства восстановления системы	72
Конфигурирование средства восстановления системы из командной строки.....	73
Центр архивации и восстановления	75
О новых возможностях резервного копирования в Windows 7	78
Создание диска аварийного восстановления системы	78

Создание образа системы	81
Ограничения процедуры создания образа системы.....	84
Настройка и выполнение резервного копирования	85
Выполнение аварийного восстановления системы	85
Ручное резервное копирование и восстановление реестра Windows 7	87
Экспорт и импорт файлов реестра	87
Резервное копирование реестра с помощью утилит командной строки	90
Заключение	91

Глава 3. Методы редактирования реестра Windows 7..... 93

Использование Редактора реестра <i>Regedit.exe</i>	94
Исследование интерфейса Редактора реестра	97
Команды меню <i>Файл</i>	101
Команды меню <i>Правка</i>	110
Команды меню <i>Вид</i>	120
Меню <i>Избранное</i>	122
Управление безопасностью реестра	123
Установка прав доступа к ключам реестра	123
Установка специальных комбинаций прав доступа	126
Присвоение прав владельца ключа реестра	128
Аудит действий в отношении реестра	131
Работа с реестром с помощью утилит командной строки	136
Утилита <i>Reg.exe</i>	136
Команда <i>reg add</i>	138
Команда <i>reg delete</i>	139
Команды утилиты <i>reg.exe</i> для резервного копирования и восстановления реестра из командной строки	139
Команда <i>reg query</i>	140
Команда <i>reg compare</i>	141
Команда <i>reg flags</i>	142
Утилита <i>Regini.exe</i>	147
Синтаксис утилиты <i>Regini.exe</i>	147
Немного о типах прав доступа	148
Заклучение	149

Глава 4. Приступаем к редактированию реестра..... 151

Популярные постинсталляционные настройки	153
Настройки пользовательского интерфейса.....	154
Имитируем классическое меню <i>Пуск</i>	155
Активизируем и блокируем панель быстрого запуска в Windows 7	162
Настройка Панели задач — с помощью реестра и без него	163
Два рабочих совета по блокировке "миниатюр"	164

Пример совета, который не работает	164
Блокировка "миниатюр" в панели задач Windows 7 путем прямого редактирования реестра	165
Блокировка "миниатюр" в Windows 7 с помощью редактирования системных политик	166
Активизация Windows Aero	168
Через пользовательский интерфейс	169
Через реестр	171
Открытие "суперсекретной" администраторской учетной записи	172
Настройка контроля учетных записей пользователей.....	174
Через пользовательский интерфейс	176
Через групповые политики.....	179
Через реестр	183
Настройка активации Windows.....	187
Индивидуальная настройка процесса загрузки системы	191
Простейший способ редактирования процесса загрузки	192
Вводная информация о редактировании базы данных BCD.....	195
Решение проблемы с несовместимостью точек восстановления в системах с двойной загрузкой Windows XP и Windows Vista/7	204
Заключение	204
Глава 5. Реестр и аппаратные средства в Windows 7	205
Установка новых устройств в Windows 7.....	207
Установка в автоматическом режиме	207
Установка "вручную"	207
Подсистема Plug and Play и реестр.....	214
Краткая история Plug and Play	214
Поддержка Plug and Play в Windows 7	217
Уровни поддержки устройств и драйверов	222
Архитектура Plug and Play.....	223
Диспетчер Plug and Play в режиме ядра	224
Диспетчер электропитания и Диспетчер политики.....	224
Диспетчер ввода/вывода	224
Дерево устройств Plug and Play	225
Распознавание устройств Plug and Play	230
Откат драйвера.....	238
Аппаратные профили.....	239
Ключи реестра, используемые драйверами устройств	241
Ключ HKLM\SYSTEM\CurrentControlSet\Services	243
Ключ HKLM\SYSTEM\CurrentControlSet\Control	243
Ключ HKLM\SYSTEM\CurrentControlSet\Enum	245
Ключ HKLM\SYSTEM\CurrentControlSet\HardwareProfiles.....	245

Встроенные средства Windows 7 по управлению надежностью.....	246
Защита системных файлов Windows.....	249
Механизм защиты драйверов цифровой подписью.....	252
Другие средства защиты системных файлов Windows	254
Защита ресурсов Windows	254
Проверка системных файлов.....	255
Верификация цифровой подписи файлов.....	257
Заключение	259

Глава 6. Диагностика и устранение неполадок в работе с аппаратными средствами..... 261

Проблемы, связанные с установкой нового оборудования	262
Диагностика проблем с аппаратными средствами с помощью встроенных средств мониторинга	265
Устранение проблем с использованием энергосберегающих режимов	274
Энергосберегающие режимы — о чем речь?	274
Основные сведения о спецификации ACPI	275
Настройка планов энергопотребления системы	278
Редактирование планов электропитания с помощью групповых политик	288
Настройка поведения кнопок	290
Настройка поведения жесткого диска	291
Настройка параметров уведомления.....	292
Настройки режима сна	293
Настройки видеоподсистемы и дисплея.....	294
Редактирование с помощью реестра	295
Планы энергопотребления.....	295
Настройки энергопотребления системы.....	298
Модификация предпочтительного плана настройки параметров энергопотребления через реестр.....	299
Заключение	300

Глава 7. Процесс нормальной загрузки Windows 7 301

Нововведения в процессе загрузки Windows Vista/7	302
Последовательность загрузки Windows Vista и Windows 7.....	305
Процесс самотестирования при включении	305
Процесс инициализации при запуске	306
Процесс начальной загрузки на платформах x86	307
Процесс начальной загрузки на платформах Itanium.....	311
Файлы, необходимые для запуска системы.....	311
Работа Менеджера загрузки Windows Vista и Windows 7.....	314
Системное хранилище BCD.....	315
Редактирование BCD с помощью утилиты <i>BCDEdit</i>	319

Загрузочное меню Windows 7	321
Опции отладочного меню при загрузке Windows 7	322
Хранение информации о загрузочном меню в реестре.....	327
Работа загрузчика <i>Winload.exe</i>	329
Загрузка ядра	330
Инициализация ядра	334
Операции, осуществляемые на стадии инициализации ядра	335
Загрузка и инициализация драйверов устройств	336
Инициализация пользовательского режима	336
Параметр реестра <i>BootExecute</i>	337
Ключ <i>Memory Management</i>	337
Повышение производительности процесса загрузки в Windows Vista и Windows 7	338
Ключ <i>DOS Devices</i>	342
Ключ <i>SubSystems</i>	343
Регистрация в системе	346
Загрузка остальных сервисов и драйверов	350
Наборы управляющих параметров в реестре.....	351
Параметр <i>Start</i>	353
Параметр <i>ErrorControl</i>	354
Параметр <i>DelayedAutoStart</i>	354
Обеспечение запуска системы при любых обстоятельствах	356
Заключение	358
Глава 8. Параметры настройки сети в реестре.....	359
Установка сетевых компонентов с помощью утилит Панели управления	360
Сетевые параметры в реестре Windows Vista и Windows 7.....	368
Регистрационная информация сетевых адаптеров.....	372
Регистрационная информация сетевых компонентов	378
Краткий обзор нововведений в сетевых технологиях Windows Vista и Windows 7 и их взаимосвязи с реестром	379
Карта сети и поддерживаемые ее протоколы.....	379
Конфигурирование сервиса тополога канального уровня.....	382
Настройка параметров групповой политики в отношении LLTD через реестр	385
Взаимодействие Windows 7 с компьютерами, работающими под управлением Windows XP.....	387
Интеграция IPv4 и IPv6 в единый стек.....	387
Конфигурирование Teredo.....	390
Блокировка Teredo.....	390
Новинка Windows 7 — Домашняя группа	392

Настройка сетевых средств путем редактирования реестра.....	398
Автоматическое конфигурирование IP-адресов.....	398
Блокировка динамической регистрации DNS	401
Заключение	402
Глава 9. Защита реестра	403
Простейшие меры ограничения доступа к реестру	405
Дополнительные меры защиты Windows Vista/7	406
Запрет доступа к Редактору реестра через групповые политики	409
Запрет доступа к редактору реестра путем редактирования реестра.....	411
Ограничение доступа к редактору реестра путем редактирования прав доступа.....	411
Редактирование прав доступа к ключам реестра	419
Обзор стандартных прав доступа в Windows Vista/7	422
Изменения параметров безопасности Windows Vista/7 по сравнению с Windows XP.....	426
Изменения политики аудита	427
Изменения в назначении прав пользователя	428
Изменения в параметрах безопасности	435
Совместное использование файлов и полномочия доступа к ним в Windows Vista/7	450
Конфигурирование совместного доступа к файлам и папкам в Windows Vista и Windows 7	452
Указание имени рабочей группы	452
Настройка сетевого размещения	454
Предоставление папки в общий доступ.....	457
Получение доступа к общим папкам и возможные проблемы	462
Обязательный контроль целостности в Windows Vista и Windows 7	462
Защита реестра от несанкционированного удаленного доступа.....	465
Защита ульев SAM и Security	467
Как защитить улей SAM.....	467
Заклучение	470
Глава 10. Реестр и пользовательские профили	471
Базовая информация о пользовательских профилях	472
Параметры, хранящиеся в пользовательском профиле	472
Структура пользовательского профиля	473
Хранение пользовательских профилей	474
Отличия структуры пользовательских профилей в Windows Vista/7 и Windows XP.....	481
Файл <i>Ntuser.dat</i>	487
Папка <i>Общие</i> (Public)	488

Перемещение пользовательского профиля в другую папку.....	490
Совместимость с наследуемыми приложениями и профилями пользователей Windows 2000/XP	492
Совместимость с приложениями.....	492
Совместимость с пользовательскими профилями предыдущих версий операционной системы	494
Работа с перемещаемыми профилями в Windows Vista/7	494
Как выполнить перезапись профиля по умолчанию нужным вам пользовательским профилем	498
Политики пользовательских профилей.....	499
Новые политики Windows Vista и Windows 7 в отношении пользовательских профилей	500
Способ получения пользовательского профиля и перенаправление папок	503
Сценарии.....	505
Использование WSH для написания регистрационных сценариев	506
Общие сведения о системной политике	507
Системная политика в Windows NT/2000/XP.....	508
Групповая политика в Windows Vista/7	508
Формат ADMX.....	509
Хранение шаблонов ADMX	510
Устранение проблем с загрузкой пользовательских профилей	512
Сообщение о препятствиях для входа в систему	512
Заключение	515

Глава 11. Диагностика и устранение проблем с загрузкой системы с помощью реестра

517

Диагностика неудачной загрузки	520
Проблемы на начальной стадии загрузки и их устранение	522
Среда восстановления Windows	524
Шаг 1. Установка Windows Automated Installation Kit (WAIK).....	525
Шаг 2. Создание среды WinRE	526
Шаг 3. Настройка среды WinRE	529
Создание DVD для аварийного восстановления Windows 7	530
Создание USB-носителя для загрузки WinRE	530
Запуск среды восстановления Windows	531
Опции среды восстановления Windows	534
Опция <i>Восстановление запуска</i>	534
Опция <i>Восстановление системы</i>	535
Опция <i>Восстановление образа системы</i>	536
Опция <i>Диагностика памяти Windows</i>	536
Опция <i>Командная строка</i>	538

Восстановление поврежденной системы	
с помощью опции <i>Восстановление запуска</i>	539
Анализ файла журнала <i>SrtTrail.txt</i>	540
Основные причины сбоев при загрузке, отражаемые	
в файле журнала <i>SrtTrail.txt</i>	544
Восстановительные операции, выполняемые при выборе опции	
<i>Восстановление запуска</i>	547
Проблемы с мультизагрузочными конфигурациями	549
Проблемы с запуском, возникающие после загрузки ядра	551
Устранение неполадок, возникающих сразу же после входа в систему	552
Заключение	553
Глава 12. "Синий экран смерти"	555
Вы никогда не видели "синего экрана" и хотите на него посмотреть	560
Методы борьбы с "синим экраном смерти" в Windows Vista и Windows 7	560
Установка параметров запуска операционной системы	561
Наиболее распространенные ошибки <i>STOP</i>	
в Windows Vista и Windows 7	565
INACCESSIBLE_BOOT_DEVICE (STOP 0x0000007B)	567
PAGE_FAULT_IN_NONPAGED_AREA (STOP 0x00000050)	568
IRQL_NOT_LESS_OR_EQUAL (STOP 0x0000000A)	569
KERNEL_MODE_EXCEPTION_NOT_HANDLED	
(STOP 0x0000008E)	570
REGISTRY_ERROR (STOP 0x00000051)	570
PFN_LIST_CORRUPT (STOP 0x0000004E)	570
MACHINE_CHECK_EXCEPTION (0x0000009C)	570
MULTIPLE_IRP_COMPLETE_REQUESTS (0x00000044)	570
DRIVER_POWER_STATE_FAILURE (0x0000009F)	570
Другие распространенные ошибки <i>STOP</i>	571
Общие рекомендации по устранению ошибок BSOD	572
Заклучение	572
Глава 13. Настройка производительности системы	
с помощью реестра	573
Настройка производительности Windows 7	573
Оценка общей производительности аппаратной конфигурации	574
Интерпретация подуровней индекса производительности Windows	579
Подуровень индекса производительности процессора	580
Подуровень производительности по RAM	581
Подуровень производительности графической подсистемы	582
Подуровень графики для игр	583
Подуровень производительности основного жесткого диска	584

Инструмент WinSAT	584
Запуск WinSAT из командной строки	586
Как "подкрутить" индекс производительности в Windows 7	589
Настройка системы на оптимальную производительность	592
Диагностика проблемы нехватки памяти	593
Пошаговая процедура оптимизации Windows 7	594
Использование возможностей ReadyBoost и SuperFetch	600
Настройка файла подкачки	603
Очистка файла подкачки при выходе из системы	606
Заключение	608
Глава 14. Коллекция "твиков"	609
Настройка интерфейса	609
Изменение фонового изображения экрана регистрации в Windows 7 без применения сторонних инструментов	610
Дальнейшие модификации экрана регистрации в Windows 7	613
Модификация картинки пользователя	614
Модификация изображения кнопок, представляющих пользователей на экране регистрации	616
Старые рецепты по-прежнему работают	616
Добавляем часто используемые приложения в контекстное меню рабочего стола	621
Скрываем значки библиотек в навигационной панели Проводника	624
Помощь в устранении неполадок	627
Настройка программы архивации данных	628
Описание ключа <i>FilesNotToBackup</i>	630
Описание ключа <i>FilesNotToSnapshot</i>	632
Описание ключа <i>KeysNotToRestore</i>	633
Запуск регистрации работы Windows Installer	634
Запуск программ установки с повышенным уровнем привилегий	635
Конфликт гаджетов и UAC	636
Заклучение	637
Глава 15. Дополнительные утилиты	639
Утилиты для индивидуальной настройки и управления работой Windows	640
Утилиты для модификации регистрационного экрана Windows 7	640
Windows 7 Logon Background Changer	640
W7C Windows 7 UI Changer	642
Logon Changer for Windows 7	643
Универсальные утилиты: "твикеры" и не только!	643
EnhanceMySe7en	644
Little Tweaker	648

Ultimate Windows Tweaker	649
XdN Tweaker	651
Windows 7 Manager	652
TweakNow PowerPack 2009	654
Uniblue DriverScanner	656
Другие полезные программы для Windows 7	658
Утилита Process Monitor от Марка Руссиновича	658
Утилиты для взлома паролей	660
Заключение	662
 ПРИЛОЖЕНИЯ	 663
Приложение 1. Ресурсы Интернета	665
Заключение	669
Приложение 2. Список литературы	670
Книги о Windows Vista	670
Книги о Windows 7	671
Приложение 3. Описание компакт-диска	672
Предметный указатель	673

Введение

Буквально до последнего времени лучшей из всех операционных систем Microsoft по праву считалась Windows XP — она была быстрой, вполне надежной, в достаточной мере защищенной и заслуженно пользовалась популярностью. Тем не менее, технический прогресс не стоял на месте, и, несмотря на все свои достоинства, эта операционная система начала стремительно устаревать. Она уже не могла в полной мере поддерживать все новые устройства и технологии, за все время ее существования в этой ОС было обнаружено большое количество уязвимостей, с учетом которых появились и новые вирусы, рассчитанные специально на нее. Назрела настоятельная необходимость радикального обновления вместо выпуска бесчисленных сервисных пакетов (Service Packs). Именно по этим причинам в Microsoft и задумались о выпуске новой ОС из линейки Windows NT. Эта роль предназначалась, как все хорошо помнят, Windows Vista. Выпуская Windows Vista, Microsoft строила грандиозные планы и ожидала, что тысячи пользователей по всему миру сразу же поспешат перейти на новую операционную систему.

Однако этим надеждам не было суждено полностью сбыться. Конечно, часть пользователей именно так и поступила, но очень многие отнеслись к Vista если не отрицательно, то, по крайней мере, настороженно. Это подтверждается тем фактом, что когда Microsoft объявила о своих планах прекратить поставки Windows XP тридцатого января 2008 года, пользователи подняли волну протеста, вылившуюся в акцию "Save Windows XP" (<http://weblog.infoworld.com/save-xp/>). Эта волна оказалась настолько мощной, что корпорация Microsoft была просто вынуждена пойти навстречу пользователям и разрешить производителям ПК устанавливать Windows XP на ультрабюджетные настольные компьютеры до середины 2010 года. Поддержка же Windows XP будет продолжена до 2014 года. Поэтому пользователи, привыкшие к этой операционной системе, смогут продолжать работать с ней. Тем не менее, им удастся лишь затянуть переход на использование более новых операционных систем

из линейки Windows NT, но предотвратить его не в силах никто. Конечно, некоторые возмущенные пользователи перейдут на Linux, FreeBSD, OpenBSD, а кто-то присмотрится и к Mac OS X. Но сделают это не все. Большинству, пусть и нехотя, но все же придется привыкать к жизни с новыми версиями Windows.

Впрочем, широко разрекламированная Windows Vista действительно не оправдала ожиданий пользователей. Достаточно сказать, что она оказалась слишком громоздкой, неповоротливой, предъявляла завышенные (на момент ее выпуска в 2006 году) системные требования — в общем, она даже была признана "провалом года" и худшей операционной системой от Microsoft¹. И хотя к настоящему времени технический прогресс шагнул далеко вперед, и теперь системные требования Vista больше не кажутся завышенными, ожидаемой популярности она так и не приобрела. Многие пользователи испытывают к ней стойкое предубеждение, и даже стремятся "снести" ее предустановленную версию с новых компьютеров, установив "старую добрую XP" или другую операционную систему по своему выбору. Причем их не останавливают даже трудности, с которыми им неизбежно приходится бороться (чего стоят одни только поиски драйверов XP для нового оборудования)!

С учетом всего этого Microsoft хорошо поработала над ошибками, и в апреле 2009 года выпустила "релиз-кандидат" (RC) новой ОС, призванной прийти на смену так не понравившейся пользователям Vista — ею стала Windows 7. Уже 22 июля появилась окончательная версия (Release To Manufacturing, RTM)². По сравнению с Windows Vista, ее преемница встретила гораздо более теплый, благожелательный прием. Это и не удивительно — она не предъявляет завышенных требований ни к аппаратным средствам, ни к дисковому пространству, загружается и работает значительно быстрее, не только по сравнению с Windows Vista, но и по сравнению с Windows XP, да и в целом бьет все рекорды по производительности. Помимо прочего, в ней появились многие долгожданные функции и усовершенствования, а существующие — "доведены до ума". Иными словами, новая система имеет все шансы стать популярной и просто "обречена на успех", особенно с учетом того, что поддержка Windows XP медленно, но неуклонно "сходит на нет" (так, например, новые Service Pack для XP выпускаться уже не будут).

В целом, по моим личным впечатлениям — теперь именно Windows 7 станет "лучшей среди всех Windows", и по праву! Я тестировала ее, начиная с первых бета-версий, и должна заметить, что первое впечатление было — настоящий восторг! Например, меня очень удивила реакция системы на подключение

¹ См. http://ru.wikipedia.org/wiki/Windows_Vista, <http://www.point.ru/news/stories/19316/>.

² См. http://en.wikipedia.org/wiki/Development_of_Windows_7.

к порту USB моего старого Pocket PC (2002 года выпуска). Откровенно говоря, у меня были сомнения насчет совместимости ПО и драйверов, которые поставлялись производителем (Compaq) на прилагаемом к устройству CD, поэтому я приготовилась к проблемам. Однако ничего такого не произошло — Windows 7 сразу же узнала устройство (абсолютно правильно распознала, надо отметить), сама скачала из Интернета инсталлятор, и через пять минут все заработало, причем никакой компакт-диск производителя не понадобился. Немного озадачило только то, что система это сделала сама, даже "без спроса".

Впрочем, со временем восторги несколько поулеглись, а проблемы в работе появились. Так, со старым мобильным телефоном такой номер не прошел — Windows 7 его не узнала... Но общего приятного впечатления это не испортило. При этом есть надежда, что драйверы и софт для него все же появятся в ближайшем будущем. Немного напрягло отсутствие классического меню **Пуск** (Start) — но я быстро обнаружила, как его можно имитировать (этот совет далее в книге будет описан). В общем, проявившиеся проблемы не носили критического характера и, в основном, были связаны с отсутствием драйверов для некоторых старых устройств. Вероятнее всего, они вскоре будут успешно решены. Поэтому, в целом, я продолжаю считать, что Windows 7 — это намного лучше, чем Vista или даже XP. Впрочем, если вы опасаетесь такого рода проблем, то думаю, что вы не ошибетесь, если приобретете Windows 7 не сразу же, а через несколько месяцев после релиза. Но переходить на нее обязательно надо — она того стоит, и разочарованы вы не будете.

Цели этой книги

Эта моя книга, как и ее предшественницы, посвященные реестру Windows, традиционно выходит под названием "Реестр Windows 7". Но не могу не отметить, что в процессе работы у меня не раз возникал соблазн переименовать ее в "Windows 7 — о реестре и не только". С чем это связано? Трудно даже перечислить, сколько книг о реестре я прочла, сколько их перевела и сколько отредактировала! А некоторые даже сама написала. Я абсолютно серьезно считаю, что книги "только о реестре" не несут особой пользы, и вот почему: реестр не существует сам по себе и не висит в безвоздушном пространстве. Он служит вполне конкретной цели — поддерживает единую базу данных о конфигурации компьютера, всех установленных приложений, пользовательских настроек. Между ним и всеми остальными компонентами системы существуют десятки тысяч невидимых связей, и стоит порвать лишь одну, чтобы "на ровном месте" создать себе множество проблем и сложностей. Нельзя рассматривать только реестр как таковой, в отрыве от остальных

компонентов операционной системы! Вот нельзя, и точка. И меня страшно раздражают некоторые книги о реестре, где говорится только о том, что его (реестр) надо открыть, что-то там создать или удалить, чтобы получить "шикарный твик". Пользователь должен понимать, что он делает, зачем, и к каким эффектам это может привести. При этом надо отметить, что огромное количество советов, которые можно найти в таких книгах (да и в Интернете тоже), в новых версиях Windows — Vista и Windows 7 — просто не работают. Почему не работают? А они и не должны там работать, потому что относятся к Windows XP, но никак не к Vista и Windows 7. А это значит, что в книге надо обязательно описать изменения, внесенные в операционную систему, а потом и показать, как именно они взаимодействуют с реестром (и не стоит забывать, что они даже и реализованы на его основе). В общем, моя книга — это не сборник "секретов" (а кстати, что это за "секрет", если он опубликован в книге?). Нет, советы такие в книге тоже есть, но просто она не состоит из одних только советов.

Была и еще одна причина для переименования. Те пользователи, которые проигнорировали Windows Vista, начав работать с Windows 7, испытают своего рода "культурный шок". И в этом нет ничего удивительного, потому что если между Windows XP и Windows Vista лежит пропасть, то от Windows Vista до Windows 7 — всего лишь один (но очень важный) шаг. Хотите подтверждения? Посмотрите на то, как нумеровались версии ядра относительно новых операционных систем Microsoft ("древние" Windows NT 3.5, 3.51 и 4.0 мы в расчет не берем):

- 5.0 — Windows 2000 (1998 год) — кстати, очень хорошая система, получившая свою долю популярности (многие пользователи упорно сохраняли приверженность ей, не спеша переходить на Windows XP);
- 5.1 — Windows XP (2001 год) — заслуженная система-ветеран, долгие годы служившая верой и правдой тысячам пользователей по всему миру;
- 6.0 — Windows Vista (2006 год) — система-неудачница, которая, тем не менее, сыграла свою роль в качестве переходного звена эволюции Windows;
- 6.1 — Windows 7 (2009 год) — реальный претендент на звание "лучшей Windows" всех времен (пока не появится что-то еще лучше).

И если шаг сделать довольно просто, то пропасть может показаться непреодолимой. Поэтому пользователям, не познаковавшимся с Windows Vista, все будет казаться незнакомым и непривычным, у них будет возникать масса вопросов. На эти вопросы надо отвечать, а книг о Windows 7 пока что крайне мало. По мере возможности, я постаралась восполнить этот пробел, и в результате книга у меня получилась, действительно, "о реестре и не только".

Впрочем, поскольку задумывалась она все же, как книга о реестре, то и реестр занимает в ней почетное место. Реестр Windows 7, как и многие другие компоненты ОС, во многом похож на реестр Windows Vista и более ранних версий систем из линейки Windows NT. Но, наряду с этими сходными чертами, есть и отличия. Одни из них несущественны и настолько незаметны, что на них не сразу обращаешь внимание. Однако есть и весьма серьезные и радикальные изменения — чего стоят одни только новые ключи и ульи, впервые появившиеся в реестре Windows Vista и, безусловно, присутствующие в Windows 7. Поскольку реестр является централизованным хранилищем всей информации об аппаратных и программных компонентах, все новые функциональные возможности, появившиеся в Windows Vista/7, обязательно должны найти свое отражение в реестре. Я никак не могу согласиться с утверждениями некоторых авторов о том, что "по процентному содержанию ко всей базе данных реестра новые ключи составляют примерно 1–5%). По самым грубым подсчетам, в моей системе одни только новые ульи BCD и Components, впервые появившиеся в Windows Vista, составили не один и не пять процентов, а целых 18! А с учетом того, что улей Components отвечает за установку всех компонентов Windows и всех обновлений, он будет расти и дальше!

Основные отличия в реестре Windows Vista/7 главным образом предопределены усовершенствованиями ядра ОС. По ходу изложения я буду стараться подчеркнуть все отличия и обратить на них внимание читателя. Является ли эта книга максимально полным и подробным справочником, описывающим абсолютно все ключи реестра или справочником готовых решений на все случаи жизни? Нет, к сожалению. Я и сама мечтаю иметь такую книгу, но при этом отлично представляю себе, какой объем она будет иметь (если вообще возможно ее написать). Откровенно говоря, ее даже нельзя будет назвать "настойной", поскольку столы будут ломаться под ее тяжестью! Не ставила я перед собой и цели описать как можно больше "трюков" и "секретов" — напротив, основное внимание уделено объяснению того, почему тот или иной "трюк" может не только не работать, но и привести к плачевным результатам. Поэтому данная книга не конкурирует с книгами других авторов, написанными на эту же тему, а скорее дополняет их, рассматривая вопросы, которые не были рассмотрены вообще или рассматривались недостаточно подробно.

При написании этой книги задачи автора заключались в том, чтобы рассказать о наиболее важных компонентах реестра, подчеркнуть сходства и отличия реестров Windows Vista и Windows 7, описать различные методы резервного копирования и восстановления реестра, а также дать читателям необходимый минимум знаний по другим важным вопросам, связанным с реестром. Я надеюсь, что книга окажется полезной системным администраторам и пользователям, желающим систематизировать свои знания о реестре.

Среди части пользователей бытует негативное мнение, о том, что реестр Windows слишком непонятен, содержит массу избыточной информации и делает систему уязвимой. Если вы придерживаетесь того же мнения, я не стану вас переубеждать. Все-таки, большинство людей склонно несколько отрицательно относиться к тем явлениям, смысл которых им до конца не ясен. Я лишь отчасти соглашусь с этой точкой зрения — в том, что реестр является сложным для понимания, и в том, что он критично влияет на работоспособность системы и жизненно для нее необходим. Моя задача — помочь вам освоить реестр. Поэтому я не буду пытаться охватить все известные приемы, а сосредоточусь на общих принципах того, как и почему они действуют. Я считаю, что как только вы получите представление об архитектуре реестра, структуре и типах данных, вы сможете самостоятельно постигать все тонкости работы с ним.

Собственный опыт работы специалистом из группы технической поддержки, безусловно, наложил определенный отпечаток и на мои взгляды, и на методы работы вообще, и на всю эту книгу — в частности. Когда я начинаю работать с новой системой, первое, что меня интересует, — это обеспечение ее работоспособности в любых условиях, вопросы резервного копирования и восстановления ее основных компонентов (в данном случае — реестра), в том числе — редко используемые и нетрадиционные. Темам резервного копирования и восстановления, а также различным мерам по защите системы от сбоев в книге отведено почетное место. Я совершенно искренне считаю, что прежде чем переходить на использование новой операционной системы и начинать с ней экспериментировать, очень важно внимательно изучить все эти вопросы и даже отрепетировать свои действия в случае сбоя.

Материал книги структурно представлен так:

- ❑ *Глава 1* содержит обзорную информацию о реестре Windows Vista и Windows 7. В ней приведено краткое описание его структуры, типов данных реестра, определенных и применяющихся в системе. Здесь же анализируются методы хранения данных реестра.
- ❑ *Глава 2* полностью посвящена методам резервного копирования и восстановления реестра. Даже если вы опытный администратор, эту главу следует прочесть очень внимательно, поскольку в Windows Vista указанные операции претерпели целый ряд существенных изменений по сравнению с Windows XP, а в Windows 7 эти изменения зашли еще дальше.
- ❑ *Глава 3* обсуждает пользовательский интерфейс утилиты для редактирования реестра (Regedit.exe). Большинство пользователей помнят, что в составе Windows NT 4.0 и Windows 2000 есть две утилиты для редактирования реестра: Regedt32.exe, наиболее мощная утилита с расширенными возможно-

стями, но "старомодным" интерфейсом, и Regedit.exe — более новая утилита, с развитым пользовательским интерфейсом, однако отстающая от первой по своим возможностям. Начиная с Windows XP, в системе существует только один встроенный редактор реестра — Regedit.exe, объединивший в себе возможности своих предшественников. Начинаящие пользователи могут применять данную главу в качестве справочника по работе с Редактором реестра. Кроме того, в этой главе рассмотрены и утилиты командной строки, предназначенные для работы с реестром: Reg.exe и Regini.exe.

- Глава 4 рассматривает ряд несложных методов настройки и конфигурирования Windows 7 как путем редактирования реестра, так и с помощью административных утилит. Эта глава носит "разминочный" характер, но, в то же самое время, в ней приводится информация, которая очень пригодится при изучении материалов последующих глав этой книги — например, в Windows Vista и Windows 7 по соображениям безопасности многие операции необходимо выполнять от имени встроенной учетной записи **Администратор** (Administrator), а она от обычных пользователей не просто скрыта, но даже и заблокирована. Кроме того, в этой главе приводится ряд полезных настроек, которые позволят пользователям, "перескочившим" через Vista, привыкнуть к Windows 7, познакомиться с ее новшествами и создать себе удобную рабочую среду.
- Глава 5 посвящена хранению информации об аппаратных средствах в реестре. Приведены базовые сведения об архитектуре Plug and Play в системе Windows 2000/XP/Vista/7, подсистемах режима ядра — Plug and Play Manager и Power Manager, инициативе OnNow и спецификации ACPI. Особое внимание уделено тем усовершенствованиям, которые были реализованы в Windows Vista/7, в частности, Windows Resource Protection, System File Checker и File Signature Verification.
- Глава 6 рассматривает вопросы управления энергосберегающими режимами, что особенно актуально для пользователей портативных компьютеров. Детально рассматриваются такие усовершенствования, как планы электропитания, улучшенные средства управления режимами сна и гибернации, а также управление планами энергосберегающих режимов через групповые политики и реестр.
- Глава 7 рассматривает процесс загрузки Windows Vista/7, роль реестра в этом процессе, а также базовые методы предотвращения сбоев при загрузке. Особое внимание уделено усовершенствованиям загрузочной архитектуры Windows Vista и Windows 7, а также таким ее новым компонентам, как хранилище данных о загрузочной информации (BCD), менеджер загрузки Bootmgr, загрузчик Windows Winload.exe. Не обойдены вниманием

и средства повышения надежности Windows Vista/7, в том числе — улучшенные опции загрузки в безопасном режиме и среда восстановления Windows (WinRE).

- ❑ *Глава 8* рассматривает параметры настройки сети в реестре Windows 7, включая новшества, появившиеся в Windows Vista, а также новую возможность Windows 7 — домашнюю группу (HomeGroup).
- ❑ *Глава 9* занимает в книге особое место, потому что посвящена одной из самых важных тем — вопросам безопасности и защиты реестра.
- ❑ *Глава 10* освещает вопросы управления рабочими средами пользователей, включая пользовательские профили и групповую политику. В этой главе я отошла от правила, которого придерживалась на протяжении всей книги, — а именно от концентрации на реестре Windows 7. Пользовательские профили Windows 2000/XP тоже рассмотрены достаточно подробно и детально описана их эволюция. Это очень важно для системных администраторов, которые должны поддерживать сети с серверами и рабочими станциями, работающими под управлением различных версий Windows.
- ❑ *Глава 11* предлагает набор рекомендаций по настройке системы и решению разнообразных проблем путем редактирования реестра. Представляет особый интерес для системных администраторов и технического персонала.
- ❑ *Глава 12* рассматривает очень интересный вопрос — "Синий экран смерти" и методы борьбы с ним. Да, Windows 7 очень надежна, и при условии исправности всех аппаратных средств компьютера и грамотной работы пользователя вы вряд ли столкнетесь в ней с пресловутым "синим экраном". Но, на всякий случай — и эта информация приводится, с описанием наиболее часто встречающихся причин падения "семерки" в "синий экран".
- ❑ *Глава 13* посвящена вопросам настройки производительности Windows 7. Да-да, несмотря на то, что Windows 7 и так является самой быстрой из всех Windows, ее можно настроить так, чтобы она работала еще быстрее!
- ❑ *Глава 14* — это "россыпь" твиков", которые так любят многие пользователи. Внимание — все "рецепты" именно работающие, и именно в Windows 7. Они все неоднократно проверены и протестированы, ни одного нерабочего "твика" там нет.
- ❑ *Глава 15* — разумеется, еще не успела появиться Windows 7, как уже начали появляться и разнообразные утилиты для ее настройки, оптимизации, чистки реестра и т. д. Таких утилит уже много, но я отобрала лучшие из них, и, что немаловажно — не всякое старье, а именно то, что работает в Windows 7 и может оказаться реально полезным.

- *Приложение 1* предлагает список ресурсов Интернета. Если бы я задалась целью составить справочник по ресурсам глобальной сети, посвященным Windows Vista/7, то получилась бы целая книга! Не все эти ресурсы одинаково ценны, поэтому данное приложение содержит только те, которые с моей точки зрения являются наиболее информативными и действительно содержат ценную информацию и реально работающие советы.
- *Приложение 2* — список литературы, где в основном приведены ссылки на источники, в которых читатели смогут найти дополнительную информацию по темам, обсуждающимся в данной книге.
- *Приложение 3* — описание компакт-диска, прилагающегося к этой книге. Что на диске? А все, что не поместилось в книгу!

Глава 1



Обзорная информация о реестре Windows 7

Ну, вы-то сами знаете, что я имею в виду...

Е. М. Блейк

"Фантастический рассказ для телепатов"

Когда мы пытаемся вытащить что-нибудь одно, оказывается, что оно связано со всем остальным.

Закон Муира

Эта книга адресована системным администраторам, специалистам по технической поддержке и опытным пользователям Windows 7 — что такое реестр, большинство читателей этого круга очень хорошо знают. Как известно, прототип современного реестра существовал еще в Windows 3.1, и большинство программистов уже тогда понимали, что конкретно их собеседник имеет в виду, заводя разговор о реестре. Популярной тема реестра стала с выходом операционной системы Windows 95. В этом нет ничего удивительного, поскольку реестр — важнейший компонент любой современной операционной системы из семейства Windows. В этой главе приводится краткая обзорная информация о реестре Windows 7, описываются структура и типы данных реестра, а также анализируются методы хранения данных реестра Windows 7.

К сожалению, ограниченный объем книги не позволяет детально останавливаться на эволюции реестра и функциональных возможностях, унаследованных от Windows NT/2000/XP/Vista, — эта книга концентрируется на реестре Windows 7. Однако основные отличия между реестрами указанных операционных систем обязательно будут подчеркиваться по ходу изложения материала там, где это действительно необходимо.

Краткая историческая справка по реестру

Сама по себе концепция реестра не нова для Windows. Однако современный реестр — это гигантский шаг вперед в достижении управляемости всей системы в целом из единого источника — *регистрационной базы данных* (registry database). Эта база данных и является основным хранилищем всех сетевых, системных и пользовательских параметров настройки Windows.

Напомним, что в эру господства MS-DOS и ранних версий Windows (которые представляли собой просто надстройку над MS-DOS) все приложения хранили конфигурационную информацию в инициализационных файлах (INI-файлах). Ими служили обычные файлы формата ASCII, которые были доступны каждому и могли редактироваться любым текстовым редактором. Первой операционной системой из семейства Windows, получившей широкое распространение, стала Microsoft Windows 3.1¹. Именно в ней появился "зачаток" современного реестра — файл Reg.dat. Впрочем, в Windows 3.1 этот зачаточный реестр вполне мирно сосуществовал с традиционными конфигурационными файлами. Всего в Windows 3.1 применялись следующие три типа файлов конфигурации:

- *системные файлы инициализации* (system initialization files). При стандартном варианте установки Windows 3.1 таких файлов было шесть: Control.ini, Progman.ini, Protocol.ini, System.ini, Win.ini и Winfile.ini:
 - в файле Win.ini содержалась основная информация о программной конфигурации операционной системы, а также некоторые параметры, которые добавлялись прикладным программным обеспечением. Каждое вновь устанавливаемое приложение вносило свои параметры в файл Win.ini, поэтому при установке на компьютер большого количества прикладных программ объем этого файла очень быстро рос. Поскольку на его размеры было установлено ограничение (не более 64 Кбайт), то добавление новых записей в его состав часто создавало проблему. Суть этой проблемы заключалась в том, что система Windows 3.1 не информировала пользователя о том, что файл Win.ini достиг предельного размера, и все дальнейшие изменения, вносимые в последние разделы этого файла (за пределами инициализационной границы), благополучно игнорировались. Именно по этой причине корпорация Microsoft рекомендовала разработчикам программного обеспечения хранить информацию, необходимую приложениям, в отдельных файлах — так называемых *файлах инициализации приложений* (private INI files);

¹ Говоря о Microsoft Windows 3.1, мы не забываем, что в этой серии были выпущены две версии: Windows 3.1 и Windows for Workgroups 3.11, и имеем в виду обе эти системы.

- файл `System.ini` служил основным хранилищем системной информации, относящейся к аппаратным средствам компьютера. Если в файле `Win.ini` хранилась информация, влияющая в основном на поведение системы, то в файле `System.ini` содержалась информация, которая указывала операционной системе на установленные аппаратные средства, драйверы устройств, загружаемые оболочки и т. п.;
 - файл `Progman.ini` содержал инициализационные параметры Диспетчера программ (Windows Program Manager), а файл `Winfile.ini` — параметры инициализации Диспетчера файлов (Windows File Manager). Отсутствие этих файлов (в отличие от файлов `Win.ini` и `System.ini`) не мешало запуску Microsoft Windows, однако в этом случае Диспетчер программ и Диспетчер файлов запускались только в стандартной конфигурации, без каких бы то ни было индивидуальных настроек. Что касается файла `Control.ini`, то в нем содержались установки Панели управления (Control Panel);
 - файл `Protocol.ini` был добавлен в состав Windows for Workgroups 3.11. Его назначение состояло в хранении инициализационной информации для сетей Windows;
- *файлы инициализации приложений* (private initialization files) представляли собой INI-файлы, добавляемые приложениями, которые устанавливались в системе. Эти файлы содержали информацию о специфических параметрах настройки приложений, включая размеры и расположение окон, а также списки недавно использовавшихся файлов (они задавались параметром `MRUList`);
- ну, а уже упоминавшийся файл регистрационной базы данных Windows 3.1 — `Reg.dat` — стал непосредственным предшественником реестров Windows 95/98/ME, Windows NT/2000/XP/Vista и, наконец, Windows 7. Он представлял собой иерархическую базу данных, состоявшую из единственной корневой структуры-контейнера с именем `HKEY_CLASSES_ROOT` и ее вложенных структур, в которых хранилась информация, необходимая для поддержки технологии OLE (Object Linking and Embedding, связь и внедрение объектов), а также сопоставления приложений расширениям имен файлов. Благодаря регистрационной базе данных пользователи Windows 3.1 могли модифицировать поведение внедренных и связанных объектов, а также быстро просмотреть список приложений, на текущий момент зарегистрированных в среде Windows.

В отличие от INI-файлов, которые представляли собой просто текстовые файлы формата ASCII, доступные для редактирования в любом текстовом редакторе, файл `Reg.dat` имел двоичный формат, и для его редактирования

требовалось специальное приложение — Редактор реестра (Regedit.exe). Выполнив команду `Regedit.exe /v`, пользователь получал возможность просматривать файл `Reg.dat` в виде иерархической древовидной структуры, содержащей вложенные параметры. Тем не менее, файл `Reg.dat` по своему строению был гораздо проще структур реестра, которые можно найти в последующих версиях операционных систем Microsoft — как линейки Windows 9x/ME, так и линейки Windows NT/2000/XP/Vista/7.

Неудобства работы с INI-файлами

Одной из наиболее сложных проблем, связанных с INI-файлами, оказалось неудобство управления ими. Стандартный набор INI-файлов, формируемых при установке операционной системы Windows 3.1, сложностей в управлении не создавал, однако по мере установки и удаления приложений в системе появлялось все большее и большее количество INI-файлов. Такой подход имел ряд серьезных недостатков:

- ❑ ручное редактирование записей в INI-файлах и установка правильных значений параметров были, конечно, вполне по силам опытным пользователям, но даже они не всегда добивались нужного результата с первой попытки. Для новичков же эти задачи были не только сложными, но, порой, и непосильными;
- ❑ отсутствовали четкие правила хранения INI-файлов. Файлы инициализации приложений могли храниться в любом каталоге и не были защищены от изменений или случайного стирания. В результате нужный файл чаще всего приходилось долго искать;
- ❑ INI-файлы не обеспечивали поддержку многопользовательской среды, поэтому пользователи не могли устанавливать параметры индивидуальной настройки компьютера и приложений;
- ❑ INI-файлы не поддерживали множественных аппаратных конфигураций, по этой причине ОС Windows 3.1 не могла поддерживать технологию Plug and Play;
- ❑ различные программы записывали свои параметры настройки в разные INI-файлы. С одной стороны, именно в этом заключалась официальная рекомендация Microsoft, призванная обойти ограничение размера файла `Win.ini`, о котором говорилось ранее. Однако, с другой стороны, это ограничивало и возможности приложений по совместному использованию информации.

ПРИМЕЧАНИЕ

Одним из требований, которым должно удовлетворять приложение, совместимое с современными операционными системами из семейства Windows, является

обеспечение возможностей корректного удаления этого приложения из системы (uninstall capabilities). Автоматическое удаление приложений из системы не является новой идеей, но в ранних версиях Windows ее реализация была не так уж совершенна. Что касается современных версий Windows, где вся конфигурационная информация централизованно хранится в реестре, то для них автоматическое удаление приложений (так называемая *деинсталляция*) существенно упростилось (хотя и здесь тоже могут возникать проблемы).

Введение реестра

Системный реестр был впервые официально "введен в эксплуатацию" с выпуском Windows 95, а в виде, более или менее напоминающем его нынешнюю структуру, появился в Windows NT 3.5. Новый компонент операционной системы представлял собой централизованное хранилище конфигурационной информации и позволял существенно эффективнее управлять рабочей средой Windows. "Юный" реестр хорошо выполнял свои задачи по управлению системными настройками, а также установкой и настройкой приложений, и стал ключевым компонентом всех без исключения систем из семейства Windows. В то же самое время исходная модель реестра обладала и большим количеством слабых мест, наиболее критичными из которых были снижение общей производительности системы и нерешенные вопросы безопасности. Действительно, по мере того, как в системе устанавливались все новые и новые приложения, производительность ее неизбежно падала. Кроме того, файлы реестра как ключевого системного компонента были слабо защищены и оказались легкой мишенью для атак. По этим причинам реестр стал излюбленным объектом для критики. Ожесточенные споры между почитателями реестра и его ненавистниками продолжались без конца, и выход каждой новой версии Windows только подогревал их. Это могло продолжаться до бесконечности. Но когда очередная новинка от Microsoft — а это была Windows Vista — находилась на очень ранних стадиях разработки, стали распространяться слухи о том, что, начиная с этой ОС, Microsoft официально отходит от концепции реестра, отказываясь от него в пользу "манифестов приложений" (application manifests) — индивидуальных и защищенных файлов, в которых хранится конфигурационная информация². Критики реестра ликовали.

Однако дискуссия не прекращалась, поскольку множество вопросов все еще оставались без ответов. Пользователи живо интересовались тем, действительно ли Microsoft собралась освободиться от реестра? Ведь достичь этой цели без радикальной переработки — задача действительно нелегкая. Как быть с законными правами пользователей Windows XP, которые не захотят

² Подробнее об этом см. <http://msdn2.microsoft.com/ru-ru/windowsvista/aa904979.aspx> и <http://en.wikipedia.org/wiki/ClickOnce>.

мигрировать на новые версии? — ведь законы о защите прав потребителей никто не отменял. Впрочем, с выходом Windows Vista эти сомнения наконец-то разрешились — реестр в ней присутствовал и по-прежнему играл свою ключевую роль. Помимо прочего, его структура еще более разрослась. На практике также оказалось, что Windows Vista зависела от реестра ничуть не меньше, чем ее предшественницы, и то же самое можно сказать и об идущей ей на смену Windows 7. В следующем разделе данной главы я попытаюсь продемонстрировать это наглядным примером.

ПРИМЕЧАНИЕ

Я не пытаюсь заставить вас полюбить реестр, если вы его терпеть не можете. Просто, раз он по-прежнему существует и играет важную роль, грамотный пользователь должен знать о нем как можно больше. Таким образом, основная цель моей книги — помочь заинтересованным читателям лучше понять принципы работы реестра, использовать его для настройки системы и устранения неполадок, а также защитить его от возможных атак.

Итак, приступим к обсуждению роли и места реестра в архитектуре Windows 7, изменений, которые он претерпел по сравнению с Windows XP и Windows Vista, а также проанализируем тенденции его будущей эволюции.

Роль и место реестра в общесистемной архитектуре Windows 7

Вы когда-нибудь попадали в такую ситуацию, когда важную работу необходимо сделать срочно, но на экране появляются странные и пугающие сообщения, информирующие вас о невозможности загрузки операционной системы из-за того, что реестр поврежден? А ведь с такой проблемой время от времени сталкиваются все любящие эксперименты пользователи операционных систем из семейства Windows NT (подробное описание роли реестра в процессе загрузки Windows 7 будет дано в *главе 7*). Это было справедливо для Windows NT/2000/XP (рис. 1.1), и это осталось в силе как для Windows Vista, так и для Windows 7.

Как можно увидеть (рис. 1.2), в Windows Vista выводимые на экран сообщения стали несколько более информативными, и в Windows 7 эта тенденция была продолжена. И хотя Среда восстановления после сбоев (Windows Recovery Environment, WinRE) стала в последних версиях Windows существенно мощнее и удобнее, чем Консоль восстановления (Recovery Console), имевшаяся в Windows 2000/XP, но, тем не менее, примеры, показанные на рис. 1.2, четко демонстрируют, что даже единственная ошибка в системном реестре может повлиять на всю системную конфигурацию и запросто помешать загрузке.

Windows NT 4.0 не могла загружаться без реестра

```
OS Loader V 4.0
....
Windows NT could not start because the following file is missing or corrupt:
\WINNT\SYSTEM32\CONFIG\SYSTEM
You can attempt to repair this file by starting Windows NT Setup using the original Setup floppy disk or CD-ROM.
Select 'r' at the first screen to repair.
```



Windows 2000 и Windows XP также зависели от реестра

```
Windows XP could not start because the following file is missing
of corrupt:
\WINNT\SYSTEM32\CONFIG\SYSTEM
You can attempt to repair this file by starting Windows XP Setup using the original Setup floppy disk of CD-ROM.
Select 'r' at the first screen to repair.
```

Рис. 1.1. Единственная ошибка в системном реестре Windows NT/2000/XP могла повлиять на всю системную конфигурацию и даже помешать загрузке системы

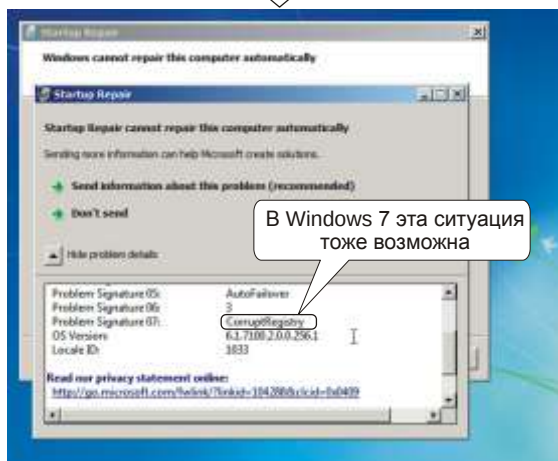
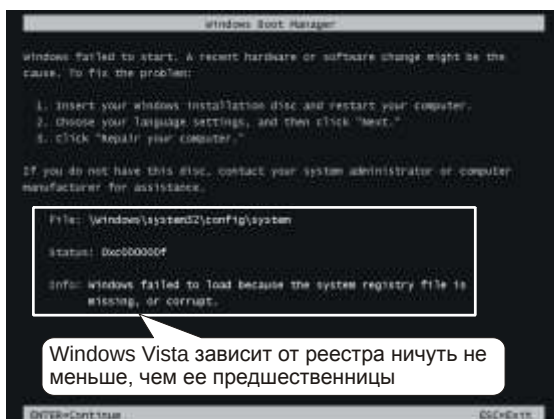


Рис. 1.2. Зависимость от реестра сохранилась как в Windows Vista, так и в Windows 7

Так же, как и в более ранних версиях Windows, в Windows 7 имеются приложения, настроить которые можно только путем конфигурирования системного реестра. Именно поэтому важно знание архитектуры реестра, его внутреннего устройства, а также наличие практических навыков работы с ним.

Цели и задачи реестра

Реестр сложен для понимания и расшифровки, однако он представляет собой важнейший компонент любой современной операционной системы из семейства Windows. Windows 7, как и любая другая операционная система из линейки Windows NT, работать без него не сможет. Что же он собой представляет? Реестр — это централизованная база данных, хранящая все настройки операционной системы и работающих в ней приложений. В этом смысле реестр аналогичен разнообразным INI-файлам, а также файлам Autoexec.bat и Config.sys, существовавшим в ранних версиях Windows. Реестр содержит информацию обо всех аппаратных устройствах, включая устройства Plug and Play (PnP), данные OLE, сведения о расширениях имен файлов, всех системных компонентах и работающих в системе приложениях, сетевые параметры, информацию безопасности и т. п.

Обобщенно говоря, если на компьютере имеется программный или аппаратный компонент, который так или иначе влияет на его работу, то информация о нем хранится и в реестре. Упрощенная схема, демонстрирующая системные компоненты и их взаимодействие с реестром, приведена на рис. 1.3.

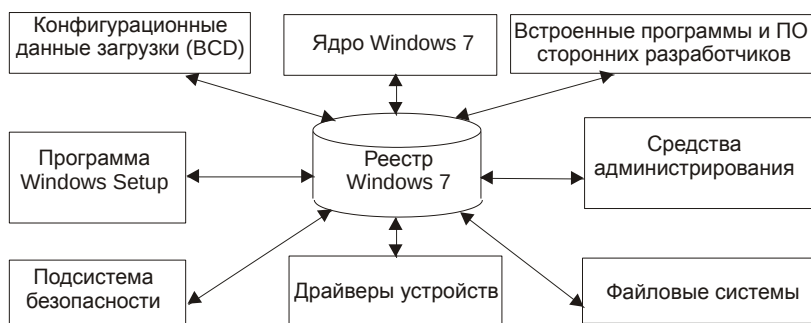


Рис. 1.3. Упрощенная схема, демонстрирующая взаимодействие системных компонентов с реестром Windows 7

На схеме в развернутом виде вы заметите, что практически все модули и функциональные возможности, впервые введенные в Windows Vista и при-

существующие в Windows 7, не только активно взаимодействуют с реестром, но и реализованы на его основе (рис. 1.4).

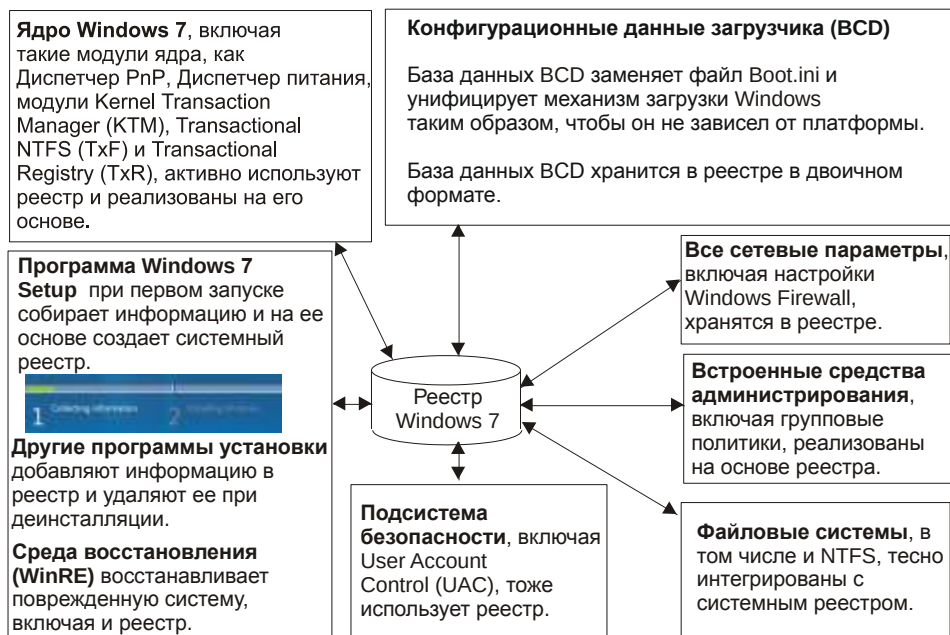


Рис. 1.4. Практически все новые функциональные возможности и усовершенствования, появляющиеся с выходом каждой новой версии Windows, активно взаимодействуют с реестром и реализованы на его основе

Итак, рассмотрим вкратце, как компоненты Windows 7 используют системный реестр. Более подробно все новые компоненты и механизмы их взаимодействия с реестром будут рассмотрены в последующих главах.

❑ **Программы установки** — программа Windows 7 Setup при первом запуске собирает информацию о системе и создает системный реестр на основе собранной информации. Другие программы-установщики, производящие установку драйверов или приложений, читают информацию из системного реестра и добавляют туда свою конфигурационную информацию. Если программа-установщик разработана корректно, то она читает информацию из системного реестра и определяет, присутствуют ли в системе компоненты, необходимые для успешного завершения процесса инсталляции. Благодаря наличию системного реестра как централизованной базы данных обо всех программных и аппаратных компонентах, все приложения могут совместно использовать эту информацию и более успешно

взаимодействовать друг с другом. Любое приложение, претендующее на статус Designed for Windows 7³, должно регистрировать свои конфигурационные данные в системном реестре (рис. 1.5) и предоставлять корректно работающую утилиту деинсталляции. Хранимая в реестре регистрационная информация приложений позволяет корректно выполнить процедуру деинсталляции, не удаляя совместно используемых компонентов (DLL, OCX и т. п.), которые могут быть необходимы для работы других приложений.



Рис. 1.5. Программа установки приложения, совместимого с Windows 7, записывает в реестр регистрационную информацию соответствующего приложения

- ❑ **Среда восстановления Windows** (Windows Recovery Environment, WinRE) — это набор средств (впервые введенных в состав Windows Vista и получивших дальнейшее развитие в Windows 7), предназначенных для диагностики поврежденной системы и восстановления ее после серьезных

³ Подробную информацию о программе Windows Logo v.3.0 можно найти по адресу <http://www.microsoft.com/whdc/winlogo/WLP30.msp>.

ошибок. Более подробную информацию о WinRE можно найти в *главах 2, 7 и 11*, здесь же отметим, что WinRE активно работает с реестром, и одна из выполняемых ею задач — это восстановление поврежденного реестра.

- **Менеджер загрузки Windows** (Windows Boot Manager, Bootmgr) — по сравнению с предшествующими версиями систем из семейства Windows NT последовательность загрузки Windows, начиная с Windows Vista, претерпела изменения. Более подробно эти вопросы будут рассматриваться в *главе 7*, пока же достаточно отметить, что Диспетчер загрузки (файл Bootmgr) получает доступ к базе данных BCD (Boot Configuration Data, см. рис. 1.4), которая, как уже говорилось, хранится в реестре. После чтения конфигурационных данных загрузки Менеджер загрузки передает управление Загрузчику Windows — файлу Winload.exe, который, в первую очередь, читает необходимые данные из реестра, а затем загружает в память ядро операционной системы (%system32%\ntoskrnl.exe) и уровень аппаратных абстракций (%system32%\hal.dll), а также все драйверы начальной загрузки и DLL режима ядра. Вот почему в случае отсутствия или повреждения файлов реестра операционная система просто не загрузится.

ПРИМЕЧАНИЕ

Следует отметить, что шпионская программа (spyware) PC Tattletale (клавиатурный шпион с возможностью сохранения экранных снимков), также содержит файл Winload.exe. Эта программа не имеет ничего общего с загрузчиком Windows Vista и Windows 7. Более подробную информацию об этом шпионе можно найти на сайте Symantec: http://www.symantec.com/security_response/writeup.jsp?docid=2005-062215-5127-99.

- **Диспетчер PnP** (PnP Manager) — компонент режима ядра, впервые появившийся в Windows 2000. Диспетчер PnP выполняет обнаружение устройств и их идентификацию по так называемому *идентификатору поставщика* (vendor ID, VID) и *идентификатору устройства* (device ID, DID). Комбинация этих двух чисел уникальным образом определяет устройство. Обнаружив уникальную комбинацию VID и DID, Диспетчер PnP запрашивает из реестра информацию о шине, на которой обнаружено устройство, и проверяет, установлен ли драйвер для этого устройства. Если драйвер устройства еще не установлен, то Диспетчер PnP информирует об этом подсистему PnP режима пользователя. Эта подсистема должна обнаружить подходящий INF-файл для инсталляции драйвера и начать его установку (рис. 1.6).

В данном примере устройство представляло собой КПК, впервые подключенный к компьютеру, работающему под управлением Windows 7. Опера-

ционная система правильно опознала устройство, начала установку его драйвера, после чего не прошло и минуты, как драйвер устройства был установлен, а само оно — готово к работе (рис. 1.7). После завершения установки драйвера сразу же было запущено приложение Windows Mobile Device Center (рис. 1.8), предлагающее начать работу с данным КПК — выполнить синхронизацию данных или начать обмен файлами без выполнения синхронизации. Таким образом, несмотря на то, что процесс установки нового оборудования при условии его совместимости с Windows 7 происходит автоматически, на самом деле системный реестр активно участвует в этом процессе. Более подробно все эти процессы будут описаны в главе 5.

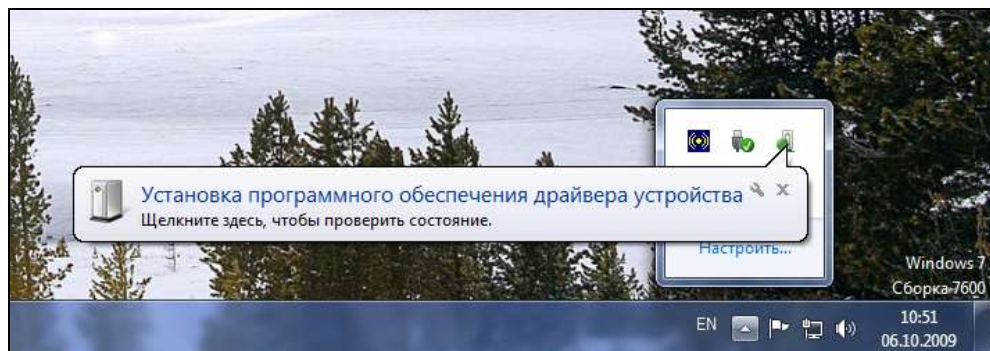


Рис. 1.6. Подсистема PnP режима пользователя в Windows 7 обнаружила подходящий INF-файл для инсталляции драйвера нового устройства и начала его установку

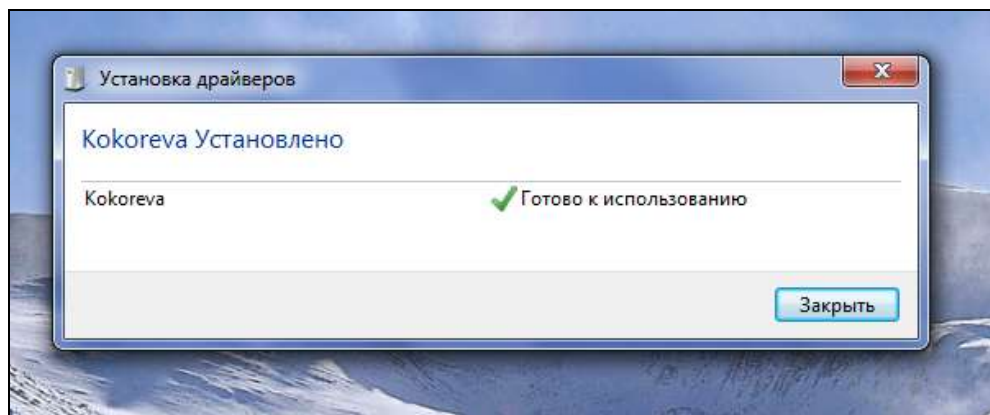


Рис. 1.7. Windows 7 правильно опознала устройство, установила драйвер, необходимый для данной модели, и теперь устройство полностью готово к работе

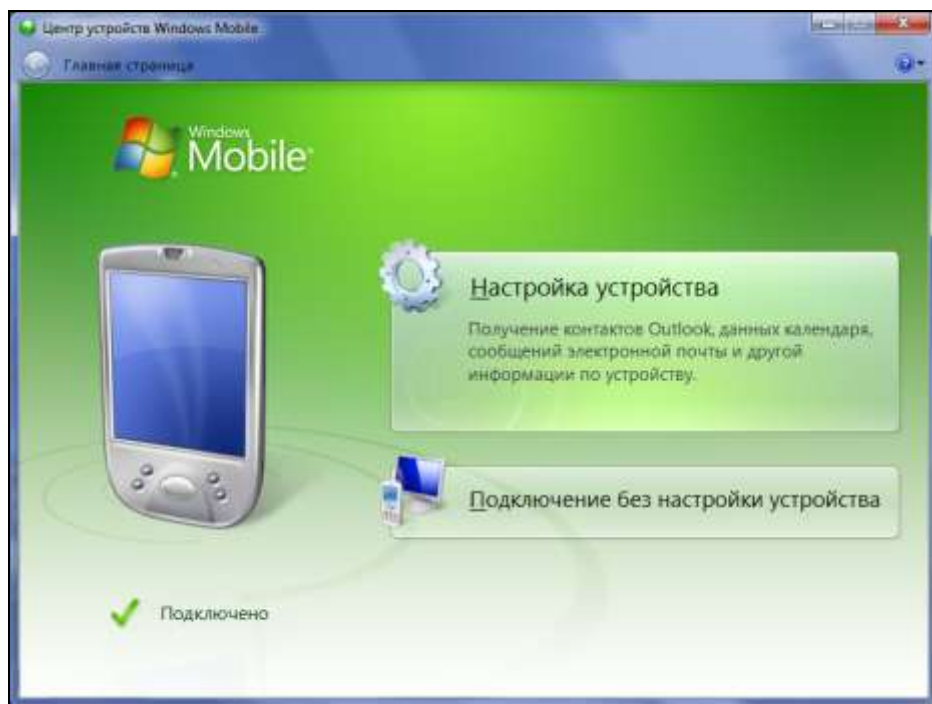
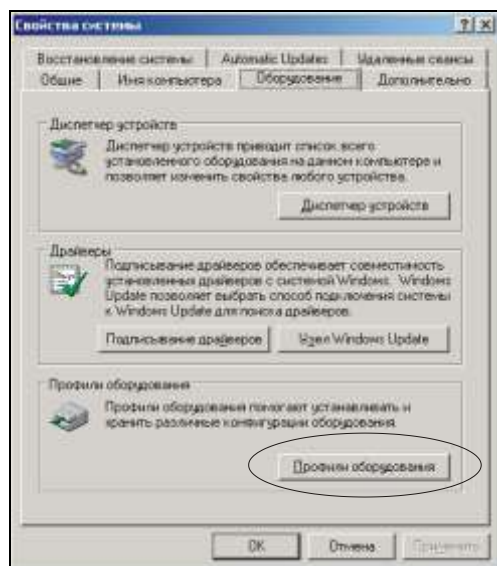


Рис. 1.8. Окно **Центр устройств Windows Mobile** (Windows Mobile Device Center)

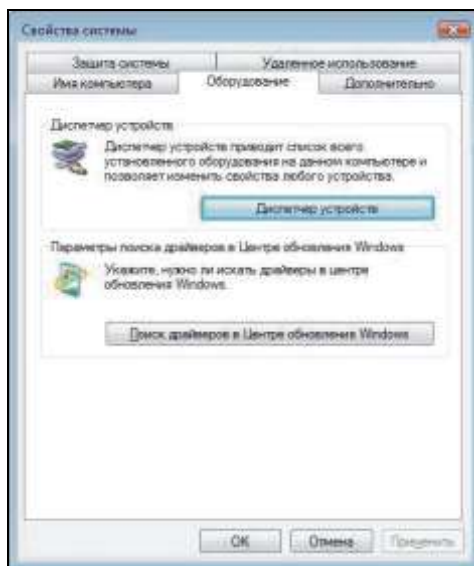
- ❑ **Диспетчер питания** (Power Manager) — включает множество усовершенствований, которые будут подробно рассмотрены в *главах 5 и 6*. Здесь же отметим, что он тесно взаимодействует с Диспетчером PnP, приложениями, поддерживает разнообразные схемы управления электропитанием и управляется групповыми политиками (Group Policies), а вся эта информация хранится в реестре.
- ❑ **Диспетчер транзакций ядра** (Kernel Transaction Manager, KTM) — новый модуль, впервые появившийся в Windows Vista и направленный на повышение надежности и отказоустойчивости. В более ранних версиях Windows часто возникали проблемы, вызванные необходимостью восстановления после некорректных модификаций файловой системы и ключей реестра. Новый модуль KTM координирует транзакции между приложениями и диспетчерами ресурсов, упрощая восстановление после ошибок. KTM реализует NTFS на базе транзакций (TxF) и реестр на базе транзакций (TxR).
- ❑ **Драйверы устройств** — обмениваются с реестром параметрами загрузки и конфигурационными данными. Эти данные аналогичны строкам `DEVICE=`,

которые можно найти в файле Config.sys для запуска компьютера под управлением MS-DOS. Драйвер устройства должен сообщить об используемых им системных ресурсах, включая аппаратные прерывания и каналы DMA, чтобы система могла включить эти данные в реестр. Приложения и драйверы устройств могут считывать эту информацию из реестра, предоставляя пользователям интеллектуальные средства установки и конфигурирования.

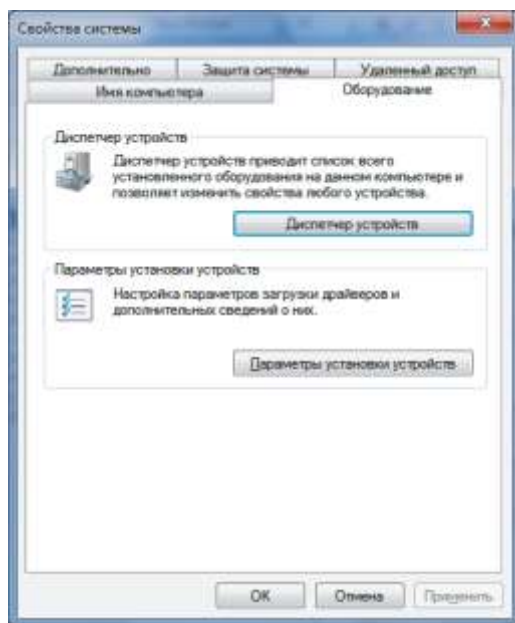
- ❑ **Административные средства** — административные средства Windows 7, в том числе утилиты из Панели управления (Control Panel) и программы из группы **Администрирование** (Administrative Tools) представляют собой наиболее удобные и безопасные средства модификации реестра. Редактор реестра, рассмотрению которого посвящена *глава 3*, также полезен для его просмотра и, время от времени, для внесения изменений в конфигурацию системы. Однако при работе с ним следует соблюдать внимательность и осторожность.
- ❑ **Пользовательские профили** (user profiles) — Windows 7 обеспечивает создание множества пользовательских профилей. Вся информация, относящаяся к конкретной учетной записи пользователя и ассоциированным с ней правам, хранится в реестре. Усовершенствованные групповые политики Windows 7 также хранятся в реестре и реализованы на его основе. Более подробная информация о пользовательских профилях и усовершенствованных групповых политиках Windows 7 будет приведена в *главе 10*, здесь же отметим, что пользовательский профиль определяет индивидуальные параметры настройки дисплея, параметры сетевых соединений, принтеры и многое другое. Пользовательские профили бывают следующих типов: *локальные* (local user profile), создаваемые автоматически при первой регистрации пользователя на локальном компьютере, *перемещаемые* (roaming user profile), создаваемые администратором и хранящиеся на сервере, и *обязательные* (mandatory user profile) — перемещаемые профили, обязательные для применения. Информация о пользовательских профилях также хранится в реестре.
- ❑ **Аппаратные профили** (hardware profiles) — реестр, в отличие от INI-файлов, позволяет хранить множественные аппаратные конфигурации. Так, например, можно создать профили для док-станций (что актуально для пользователей портативных компьютеров), а также для съемных устройств. Фактически аппаратный профиль представляет собой набор инструкций, с помощью которых можно указать операционной системе, драйверы каких устройств должны загружаться при запуске компьютера. Как вы, вероятно, помните, в Windows XP существовала возможность работы с аппаратными профилями через пользовательский интерфейс (рис. 1.9, *а*). Начиная с Windows Vista, этой возможности больше нет (рис. 1.9, *б* и *в*).



а) Windows XP



б) Windows Vista



в) Windows 7

Рис. 1.9. Вкладка **Оборудование** (Hardware) окна **Свойства системы** (System properties) — обратите внимание на исчезновение кнопки **Профили оборудования** (Hardware profiles), имевшейся в Windows XP

Возможность выбора аппаратного профиля при запуске системы присутствует в списке функций, официально удаленных из Windows Vista. Тем не менее, работать с аппаратными профилями как в Windows Vista, так и в Windows 7, все-таки можно, и в *главе 5* будет показано, как это делается.

- ❑ **Файловые системы** — начиная с Windows Vista как файловые системы, так и реестр основаны на *транзакциях* (transaction-based). На практике это означает, что если набор операций над файлами и реестром помечен как транзакция, то в случае неудачи хоть единственной из этих операций всю транзакцию можно "откатить" в исходное состояние. Кроме того, *шифрующая файловая система* (EFS), впервые введенная в Windows 2000, переработана и содержит ряд усовершенствований, включая повышение производительности, поддержку шифрования файла подкачки и хранение пользовательских ключей EFS на смарт-картах. Все эти новшества также реализованы через реестр.
- ❑ **Подсистема безопасности Windows 7** — подсистема безопасности со всеми ее функциональными возможностями, включая *контроль учетных записей пользователей* (User Account Control, UAC), также реализована на базе реестра и используется для его же защиты (рис. 1.10). UAC — это новая технология, впервые появившаяся в Windows Vista и направленная на повышение безопасности системы. Принцип действия UAC заключается в ограничении привилегий, предоставляемых запускаемым приложениям, уровнем привилегий обычного пользователя⁴. Иными словами, даже если пользователь, запускающий приложение, и обладает административными правами, запускаемые им приложения таких привилегий не имеют, если только пользователь явно не запускает их от имени администратора. Таким образом, с повышенным уровнем привилегий запускаются лишь приложения, которым пользователь доверяет. Более подробно вопросы безопасности Windows 7 и реестра как ее ключевого компонента будут рассмотрены в *главе 9*.
- ❑ **Сетевые компоненты Windows 7**, включая драйверы сетевых адаптеров, параметры настройки сетевых протоколов и сервисов, а также параметры сетевой безопасности и средства защиты сети от атак извне тоже хранятся в реестре. Например, база данных Брандмауэра Windows (Windows Firewall) находится в реестре. Многие брандмауэры сторонних производителей также создают в реестре свои ключи, и, следовательно, успешная атака на реестр открывает путь к вторжению извне. Эта проблема очень серьезна, и более подробно она будет рассмотрена в *главах 8 и 9*.

⁴ Эта функция очень похожа на технологию, реализованную в Linux.

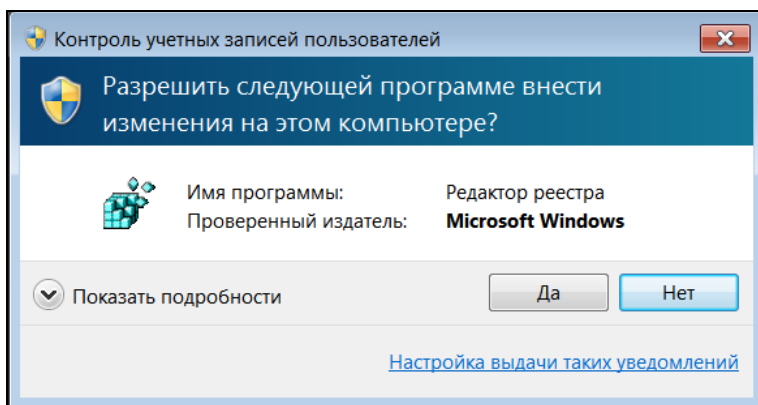


Рис. 1.10. Функция контроля учетных записей пользователей реализована на базе реестра и используется, в том числе, для его же защиты

Структура реестра

Для понимания логической структуры реестра проще всего провести аналогию со структурой файловой системы на диске. Реестр содержит *ключи* (keys), которые аналогичны каталогам, и *параметры* (values), которые можно сравнить с файлами, хранящимися на диске. Ключи реестра представляют собой контейнеры, в составе которых могут содержаться как *вложенные ключи* (subkeys), так и параметры. Параметры реестра (как и файлы) содержат данные. Ключи, находящиеся на верхнем уровне этой иерархической структуры, называются *корневыми ключами* (root keys). Схема именования ключей и параметров реестра также заимствуется от схемы именования путей к файлам и каталогам, принятой для файловой системы. Сравните, например, типичный путь к каталогу (WORK\BHV) и типичный путь к вложенному ключу реестра (HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet).

Реестр Windows 7, как и реестр Windows 2000/XP/Vista, содержит 5 корневых ключей: HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE, HKEY_USERS и HKEY_CURRENT_CONFIG. Рисунок 1.11 иллюстрирует иерархическую структуру реестра⁵.

⁵ В действительности, существует и еще один, шестой корневой ключ, который называется HKEY_PERFORMANCE_DATA. Как и следует из его названия, он содержит информацию о счетчиках производительности и используется ядром Windows для хранения информации о производительности системы. Редактор реестра этот ключ не отображает, следовательно, вы не можете его ни увидеть, ни изменить. Доступ к этому ключу возможен только программно, и поэтому в данной книге он рассматриваться не будет. Впрочем, заинтересованные читатели могут найти информацию об этом ключе по следующему адресу: <http://msdn.microsoft.com/en-us/library/microsoft.win32.registry.performancedata.aspx>.

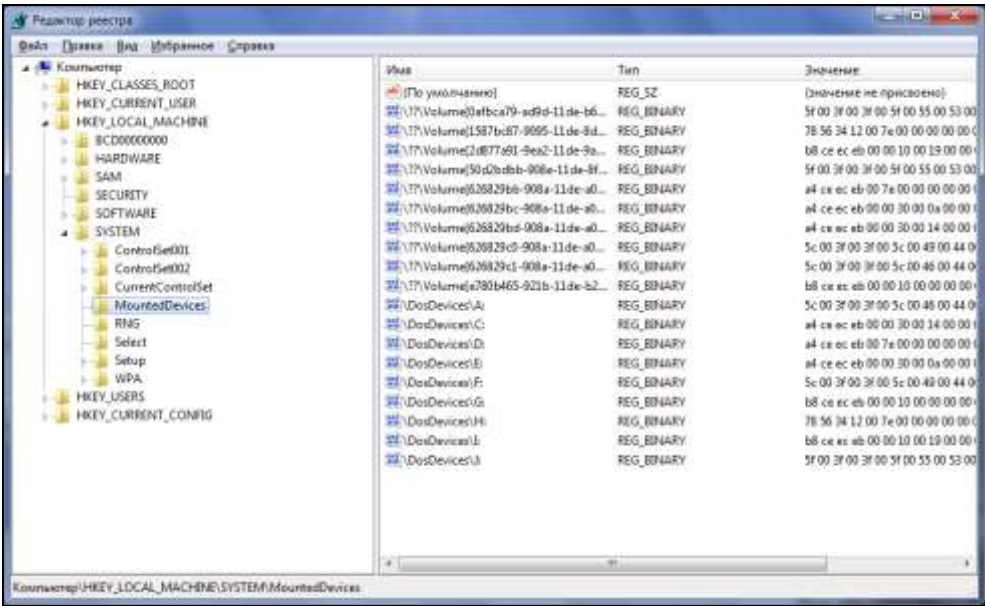


Рис. 1.11. Иерархическая структура реестра

Все имена корневых ключей начинаются со строки `HKEY_`, что указывает разработчикам программного обеспечения на то, что это — дескриптор, который может использоваться программой. *Дескриптор* (handle) — это значение, применяемое для уникального описания ресурса, к которому программа может получить доступ. Описания корневых ключей реестра Windows 7 приведены в табл. 1.1.

Таблица 1.1. Корневые ключи реестра

Имя корневого ключа	Описание
HKEY_LOCAL_MACHINE	Содержит глобальную информацию об аппаратных средствах и операционной системе, в том числе: тип шины, системная память, драйверы устройств и управляющие данные, используемые при запуске системы. Информация, содержащаяся в составе этого ключа, действует применительно ко всем пользователям, регистрирующимся в системе. На верхнем уровне иерархии реестра для этого ключа имеются три псевдонима: HKEY_CLASSES_ROOT, HKEY_CURRENT_CONFIG и HKEY_DYN_DATA

Таблица 1.1 (окончание)

Имя корневого ключа	Описание
HKEY_CLASSES_ROOT	Содержит ассоциации между приложениями и типами файлов (по расширению имени файла). Кроме того, этот ключ хранит информацию OLE, ассоциированную с объектами COM, а также данные по ассоциациям файлов и классов (эквивалент реестра ранних версий Windows, служивших настройкой над MS-DOS). Параметры этого ключа совпадают с параметрами, расположенными под ключом HKEY_LOCAL_MACHINE\Software\Classes. Подробную информацию о ключе HKEY_CLASSES_ROOT можно найти в руководстве "OLE Programmer's Reference", входящем в состав продукта Windows Platform Software Development Kit (SDK)
HKEY_CURRENT_CONFIG	Содержит конфигурационные данные для текущего аппаратного профиля. Аппаратные профили (Hardware profiles) представляют собой наборы изменений, внесенных в стандартную конфигурацию сервисов и устройств, установленную данными ключей Software и System корневого ключа HKEY_LOCAL_MACHINE. В ключе HKEY_CURRENT_CONFIG отражаются только изменения. Параметры этого ключа появляются также под ключом HKEY_LOCAL_MACHINE\System\CurrentControlSet\HardwareProfiles\Current
HKEY_CURRENT_USER	Содержит профиль пользователя, на данный момент зарегистрированного в системе, включая переменные окружения, настройку рабочего стола, параметры настройки сети, принтеров и приложений. Этот ключ представляет собой ссылку на ключ HKEY_USERS\user_SID, где user_SID — идентификатор безопасности (Security ID) пользователя, зарегистрированного в системе на текущий момент
HKEY_USERS	Содержит все активно загруженные пользовательские профили, включая HKEY_CURRENT_USER, а также пользовательский профиль по умолчанию (.DEFAULT). Пользователи, получающие удаленный доступ к серверу, не имеют профилей, содержащихся под этим ключом, — их профили загружаются в реестры на собственных компьютерах

Данные реестра поддерживаются в виде параметров, расположенных под ключами реестра. Каждый параметр характеризуется именем, типом данных

и собственно значением. Три части параметра реестра всегда располагаются в порядке, показанном на рис. 1.12.



Рис. 1.12. Три части параметра реестра

В табл. 1.2 перечислены типы данных, определенные и используемые в системе Windows 7.

Таблица 1.2. Типы данных для параметров реестра

Тип данных	Описание
REG_BINARY	Двоичные данные. Большинство аппаратных компонентов используют информацию, которая хранится в виде двоичных данных. Редакторы реестра отображают эту информацию в шестнадцатеричном формате
REG_DWORD	Данные представлены в виде значения, длина которого составляет 4 байта. Это — 32-битное беззнаковое целое число из диапазона от 0 до 4 294 967 295 ($2^{32} - 1$). Этот тип данных используют многие параметры драйверов устройств и сервисов. Редакторы реестра могут отображать такие данные в двоичном, шестнадцатеричном и десятичном формате
REG_EXPAND_SZ	Расширяемая строка данных. Она представляет собой текст, содержащий переменную, которая может быть заменена при вызове со стороны приложения
REG_MULTI_SZ	Многострочное поле. Значения, которые фактически представляют собой списки текстовых строк, обычно имеют этот тип данных. Строки разделены символом NULL
REG_SZ	Текстовая строка в формате, удобном для восприятия человеком. Значениям, представляющим собой описания компонентов, обычно присваивается именно этот тип данных
REG_DWORD_LITTLE_ENDIAN	32-разрядное число в формате "остроконечников" (little-endian). Представляет собой эквивалент типа REG_DWORD. При использовании метода "остроконечников" самый младший байт ("little end") хранится в памяти первым в числе. Например, шестнадцатеричное число A02Bh по методу "остроконечников" сохраняется как 2BA0. Метод "остроконечников" используется в микропроцессорах Intel

Таблица 1.2 (окончание)

Тип данных	Описание
REG_DWORD_BIG_ENDIAN	32-разрядное беззнаковое целое число из диапазона от 0 до 4 294 967 295 ($2^{32} - 1$) в формате "тупоконечников" (big endian). В противоположность методу "остроконечников" при использовании метода "тупоконечников" первым байтом числа оказывается самый старший байт ("big end")
REG_LINK	Символическая ссылка Unicode. Этот тип данных предназначен для внутреннего использования. Тип данных REG_LINK особенно интересен тем, что он позволяет одному элементу реестра ссылаться на другой ключ или параметр. Например, если элемент реестра \Root1\Link имеет параметр типа REG_LINK со значением \Root2\RegKey, а ключ RegKey содержит параметр RegValue, то этот параметр идентифицируется двумя путями: \Root1\Link\RegValue и \Root2\RegKey\RegValue. Операционные системы из семейства Windows NT, включая Windows 7, активно используют этот метод — некоторые из корневых ключей реестра, перечисленных в табл. 1.1, являются ссылками на вложенные ключи других корневых ключей
REG_NONE	Параметр не имеет определенного типа данных
REG_QWORD	64-разрядное значение
REG_QWORD_LITTLE_ENDIAN	64-разрядное число в формате "остроконечников". Эквивалент REG_QWORD
REG_RESOURCE_LIST	Список аппаратных ресурсов, применяется только в ветви HKEY_LOCAL_MACHINE\HARDWARE
REG_FULL_RESOURCE_DESCRIPTOR	Дескриптор (описатель) аппаратного ресурса. Применяется только в ветви HKEY_LOCAL_MACHINE\HARDWARE
REG_RESOURCE_REQUIREMENTS_LIST	Список необходимых аппаратных ресурсов. Применяется только в ветви HKEY_LOCAL_MACHINE\HARDWARE

Хранение данных реестра

В Windows 7, как и в Windows NT/2000/XP/Vista, элементы реестра хранятся в виде *атомарной структуры*. Реестр подразделяется на составные части, которые разработчики этой операционной системы называли *ульями* (hives), по аналогии с ячеистой структурой пчелиного улья.

ПРИМЕЧАНИЕ

В версиях Windows NT/2000/XP/Vista, локализованных на русский язык, эти компоненты были названы "кустами", что не совсем точно отражает их природу. В оригинальных версиях Windows NT/2000/XP/Vista/7 атомарные компоненты структуры реестра называются ульями (hives). Этот термин был введен разработчиками Microsoft с тем, чтобы подчеркнуть сходство структуры реестра с ячеистой структурой пчелиного улья. С точки зрения автора, этот термин является более удачным.

Улей представляет собой дискретную совокупность ключей, вложенных ключей и параметров, берущую начало в вершине иерархии реестра. Отличие ульев от других групп ключей состоит в том, что они являются постоянными компонентами реестра. Ульи не создаются динамически при загрузке операционной системы и не удаляются при ее остановке. Таким образом, ключ `HKEY_LOCAL_MACHINE\HARDWARE`, который строится динамически распознавателем аппаратных средств при запуске системы, улем не является.

ПРИМЕЧАНИЕ

Так же, как в Windows NT/2000/XP/Vista, реестр Windows 7 размещается на системном диске компьютера в виде набора именуемых ульями файлов, которые служат хранилищем данных о конфигурации системы. В Windows 7 программный код реестра переработан для обеспечения более высокой надежности и повышенной производительности. Далее в этой главе мы рассмотрим эти усовершенствования более подробно.

Данные ульев реестра, определяющие общесистемные параметры конфигурации, хранятся в файлах, которые размещаются в каталогах `%SystemDrive%\Boot\BCD` (новый улей реестра BCD, появившийся в Windows Vista и присутствующий в Windows 7) и `%SystemRoot%\System32\Config`. Ульи реестра, задающие пользовательскую конфигурационную информацию, в разных версиях операционных систем из семейства Windows NT хранятся в различных каталогах:

- ☐ `%SystemRoot%\Profiles\Username` — Windows NT 4.0;
- ☐ `%SystemRoot%\Documents and Settings\Username` — Windows 2000, Windows XP и Windows Server 2003;
- ☐ `%SystemRoot%\Users\Username` — Windows Vista, Windows Server 2008 и Windows 7.

Вот полный список всех ульев реестра, имеющих в системе Windows 7 по умолчанию:

- ☐ `%SystemDrive%\Boot\BCD`;
- ☐ `%SystemRoot%\System32\Config\RegBack\SECURITY`;
- ☐ `%SystemRoot%\System32\Config\RegBack\SOFTWARE`;

- ☐ %SystemRoot%\System32\Config\RegBack\DEFAULT;
- ☐ %SystemRoot%\System32\Config\RegBack\SAM;
- ☐ %SystemRoot%\System32\Config\RegBack\COMPONENTS;
- ☐ %SystemRoot%\System32\Config\RegBack\SYSTEM;
- ☐ %SystemRoot%\System32\Config\BCD-Template;
- ☐ %SystemRoot%\System32\Config\COMPONENTS;
- ☐ %SystemRoot%\System32\Config\DEFAULT;
- ☐ %SystemRoot%\System32\Config\SAM;
- ☐ %SystemRoot%\System32\Config\SECURITY;
- ☐ %SystemRoot%\System32\Config\SOFTWARE;
- ☐ %SystemRoot%\System32\Config\SYSTEM;
- ☐ %SystemDrive%\Users\Username \ntuser.dat;
- ☐ %SystemRoot%\winsxs\x86_microsoft-windows-b...bcdtemplate-client_31bf3856ad364e35_6.0.6000.16386_none_25edb26a062d63a9\BCD-Template.

ПРИМЕЧАНИЕ

Обратите внимание, что в Windows Vista и Windows 7, как и во всех предшествующих версиях, имеется папка, в которой хранятся резервные копии ульев реестра в том виде, который он имел на момент установки операционной системы. Только теперь эта папка, находящаяся в составе папки %SystemRoot%\System32\Config, называется REGBACK, а не REPAIR, как это было в Windows 2000/XP/2003.

ПРИМЕЧАНИЕ

В Windows 7 появилось и еще одно очень важное усовершенствование, нацеленное на повышение ее надежности и отказоустойчивости. Правда, оно имеет место только в том случае, если Windows 7 — это единственная операционная система, установленная на компьютер. Тогда при установке программа Windows 7 Setup во время разбиения диска на разделы создаст скрытый раздел, на который будут записаны все файлы, необходимые для начала процесса загрузки системы, — это Менеджер загрузки (bootmgr), улей реестра BCD и некоторые другие. Более подробно об этом будет рассказано в *главе 7*, посвященной процессу загрузки и роли реестра в этом процессе. Если же Windows 7 устанавливалась как вторая или даже третья операционная система, то все будет практически так же, как в Windows Vista. Впрочем, хотя этот скрытый раздел будет невидим пользователю, работающему с самой Windows 7, но при загрузке с Live-дистрибутивов или, например, даже с помощью древней утилиты ERD Commander от Wininternals, датирующей 2002 годом, этот раздел можно увидеть (рис. 1.13).

Каждый улей реестра Windows 7 ассоциирован с набором стандартных файлов. В табл. 1.3 перечислены стандартные ульи реестра и поддерживающие их файлы для Windows XP, а в табл. 1.4 — для Windows Vista и Windows 7.

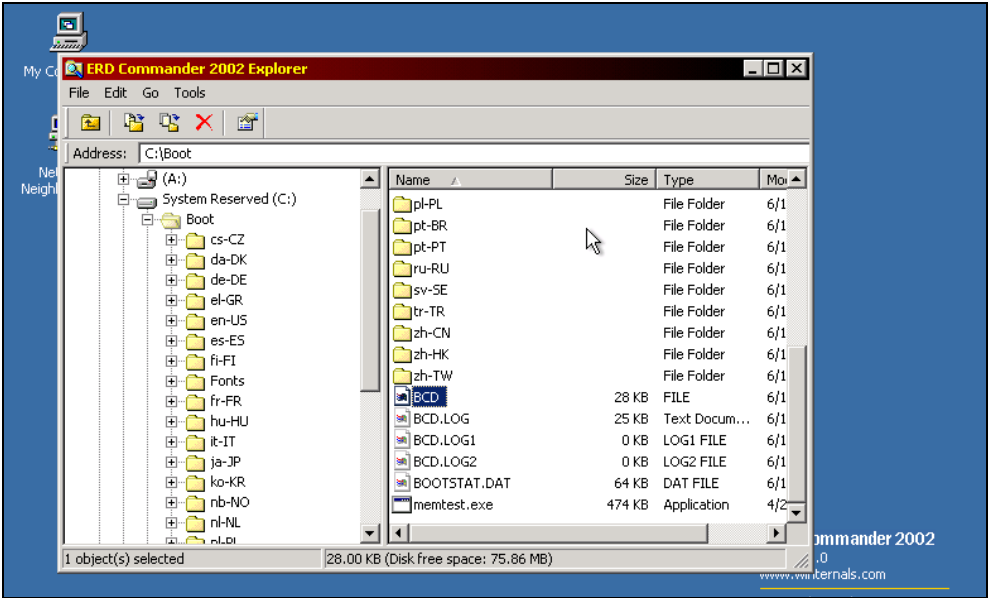


Рис. 1.13. Скрытый раздел, создаваемый Windows 7 для хранения базы данных загрузочной конфигурации и работающих с ней файлов, — он называется **System Reserved**

Таблица 1.3. Стандартные файлы, обеспечивающие поддержку ульеv реестра Windows XP

Улей реестра	Файлы поддержки
HKLM\SAM	Sam, Sam.log, Sam.sav
HKLM\Security	Security, Security.log, Security.sav
HKLM\Software	Software, Software.log, Software.sav
HKLM\System	System, System.log, System.sav
HKCC	System, System.log, System.sav
HKU\ .DEFAULT	Default, Default.log, Default.sav
Файлы, не ассоциированные ни с одним ключом	Userdiff, Userdiff.log, Userdifr, Userdifr.log
HKCU	Ntuser.dat, Ntuser.dat.log

**Таблица 1.4. Стандартные файлы, обеспечивающие поддержку
ульеv реестра Windows Vista и Windows 7**

Улей	Файлы
HKLM\BCD00000000	%SystemDrive%\BCD\BCD, %SystemDrive%\BCD\BCD.LOG, %SystemDrive%\BCD\BCD.LOG1, %SystemDrive%\BCD\BCD.LOG2, %SystemRoot%\System32\config\BCD-Template, %SystemRoot%\System32\config\BCD-Template.LOG
HKLM\COMPONENTS	%SystemRoot%\System32\config\COMPONENTS, %SystemRoot%\System32\config\COMPONENTS.SAV*, %SystemRoot%\System32\config\COMPONENTS.LOG, %SystemRoot%\System32\config\COMPONENTS.LOG1, %SystemRoot%\System32\config\COMPONENTS.LOG2
HKLM\SAM	%SystemRoot%\System32\config\SAM, %SystemRoot%\System32\config\SAM.SAV*, %SystemRoot%\System32\config\SAM.LOG, %SystemRoot%\System32\config\SAM.LOG1, %SystemRoot%\System32\config\SAM.LOG2
HKLM\SECURITY	%SystemRoot%\System32\config\SECURITY, %SystemRoot%\System32\config\SECURITY.SAV*, %SystemRoot%\System32\config\SECURITY.LOG, %SystemRoot%\System32\config\SECURITY.LOG1, %SystemRoot%\System32\config\SECURITY.LOG2
HKLM\SOFTWARE	%SystemRoot%\System32\config\SOFTWARE, %SystemRoot%\System32\config\SOFTWARE.SAV*, %SystemRoot%\System32\config\SOFTWARE.LOG, %SystemRoot%\System32\config\SOFTWARE.LOG1, %SystemRoot%\System32\config\SOFTWARE.LOG2
HKLM\SYSTEM	%SystemRoot%\System32\config\SYSTEM, %SystemRoot%\System32\config\SYSTEM.SAV*, %SystemRoot%\System32\config\SYSTEM.LOG, %SystemRoot%\System32\config\SYSTEM.LOG1, %SystemRoot%\System32\config\SYSTEM.LOG2
HKU\.\DEFAULT	%SystemRoot%\System32\config\DEFAULT, %SystemRoot%\System32\config\DEFAULT.SAV*, %SystemRoot%\System32\config\DEFAULT.LOG, %SystemRoot%\System32\config\DEFAULT.LOG1, %SystemRoot%\System32\config\DEFAULT.LOG2
HKCU	%SystemDrive%\Users\Username\Ntuser.dat, %SystemDrive%\Users\Username\Ntuser.dat.log

* Эти файлы присутствуют только в Windows Vista, а из Windows 7 они были исключены.

Большинство файлов ульев реестра находятся в подкаталоге %SystemRoot%\System32\Config. Исключение составляют ульи HKEY_LOCAL_MACHINE\BCD00000000 и HKEY_CURRENT_USER.

Поддержку улья HKEY_LOCAL_MACHINE\BCD00000000 осуществляют файлы BCD и BCD.LOG, расположенные в каталоге \Boot\BCD, и файлы BCD-Template, BCD-Template.log и BCD-Template.sav, расположенные в каталоге %SystemRoot%\System32\Config. Это новая база данных, впервые введенная в Windows Vista и выполняющая функции, ранее выполнявшиеся файлом boot.ini.

Поддержка улья HKEY_LOCAL_MACHINE\Components осуществляется файлами COMPONENTS, COMPONENTS.LOG, COMPONENTS.SAV, которые представляют собой хранилище данных о системных компонентах и всех обновлениях, установленных в Windows. Изменения в этот улей вносятся всякий раз, когда в системе производится установка обновлений, а также когда пользователь устанавливает или удаляет компоненты Windows.

Поддержку улья HKEY_CURRENT_USER выполняют файлы Ntuser.dat и Ntuser.dat.log. В файлах Ntuser.dat хранятся пользовательские профили. Файл Ntuser.dat.log отслеживает изменения, которые вносились в файл Ntuser.dat. В Windows NT 4.0 эти файлы располагаются во всех подкаталогах каталога %SystemRoot%\Profiles (за исключением подкаталога \All Users). Начиная с Windows 2000, упомянутые файлы находятся в каталогах %SystemDrive%\Documents and Settings\%Username%.

Файлы Ntuser и Userdiff были впервые введены в Windows NT 4.0:

- ❑ файл Ntuser.dat, в котором хранится пользовательский профиль, заменил собой файлы *usernamexxx* и *adminxxx* из предыдущих версий Windows NT;
- ❑ файл Ntuser.dat из каталога %SystemRoot%\Profiles\Default User заменил собой файл Userdef из предыдущих версий Windows NT. Этот профиль используется для построения улья HKEY_CURRENT_USER, когда новый пользователь впервые регистрируется в системе;
- ❑ файлы Userdiff, которые находятся только в каталоге %SystemRoot%\System32\Config, не ассоциируются ни с одним улем. Они служат для обновления существующих пользовательских профилей предыдущих версий Windows NT таким образом, чтобы эти профили могли использоваться в Windows NT/2000 и Windows XP.

С улями ассоциируются файлы четырех типов. Все эти типы файлов (с соответствующими расширениями имен файлов) перечислены в табл. 1.5.

Таблица 1.5. Типы файлов, ассоциированных с улями реестра
Windows NT 4.0/Windows 2000/Windows XP/Vista/7

Тип файла	Описание
Без расширения имени файла	Содержит копию улья
ALT (были исключены из Windows XP)	Содержит резервную копию жизненно важного улья <code>HKKEY_LOCAL_MACHINE\System</code> . Только ключ <code>\System</code> имеет соответствующий файл с расширением <code>alt</code> . Начиная с Windows XP, ALT-файлы ликвидированы, поскольку программный код реестра был переработан для реализации более совершенных алгоритмов, увеличивающих быстродействие при выполнении запросов, а также для повышения надежности и увеличения объема реестра
LOG1	Содержит журнал транзакций, в котором регистрируются все изменения, внесенные в ключи и значимые элементы улья
SAV (были исключены из Windows 7)	Содержит копии файлов улья в том виде, который они имели на момент завершения текстовой фазы процесса установки. Файлы с расширением <code>sav</code> имеются для ключей <code>\Software</code> , <code>\System</code> , <code>\SAM</code> , <code>\Security</code> и <code>\Default</code> . Windows NT/2000/XP/Vista выполняет резервное копирование содержимого ульев в процессе инсталляции. Процедура инсталляции состоит из двух стадий: стадии текстового режима и стадии графического режима. Когда установка в текстовом режиме завершается, выполняется копирование ульев в файлы с расширением <code>sav</code> . Это делается для того, чтобы защитить ульи от ошибок, которые могут произойти в случае сбоя на графической стадии установки. Если процедура установки даст сбой на графической стадии, то после перезагрузки компьютера будет производиться повтор только графической стадии установки. SAV-файлы используются для перестройки ульев реестра
LOG, LOG2	Эти файлы создаются в процессе установки Windows, но остаются неизменными в течение времени работы с системой

Атомарность и восстановление ульев реестра

Реестр гарантирует *атомарность* (atomicity) отдельных действий. Это означает, что любое изменение, выполненное по отношению к параметру реестра (установка, удаление или сохранение), либо работает, либо нет. За счет этого исключается возможность появления поврежденных комбинаций из старых и новых значений. Такое повреждение не произойдет, даже если в процессе внесения изменений в реестр система внезапно остановится вследствие прекращения подачи питания, аппаратного сбоя или проблем с программным

обеспечением. К примеру, если приложение устанавливает значение реестра, и в этот момент происходит остановка системы, то после перезагрузки реестр будет иметь либо прежнее значение, либо новое, но бессмысленная комбинация старого и нового значений не появится никогда. Кроме того, размер и временные данные для ключа, содержащего значение, в который вносились изменения, будут точными, вне зависимости от того, было изменено это значение или нет.

Сброс данных

Windows NT 4.0 и Windows 2000 записывают данные в реестр только после сброса (flush). Сброс же происходит после того, как измененные данные "постареют" на несколько секунд. К тому же, сброс может возникнуть и по прямому запросу приложения, которое намеренно сбросило данные на жесткий диск.

Для всех ульев (кроме \System) система выполняет следующую процедуру сброса:

1. Все измененные данные записываются в файл журнала (LOG-файл) соответствующего улья вместе с указанием их точного местоположения в улье. После этого выполняется сброс, и все измененные данные оказываются записанными в файл журнала.
2. Первый сектор файла улья помечается, что указывает на переходное состояние данного файла.
3. Измененные данные записываются в файл улья.
4. После этого файл улья помечается как файл, выполнение транзакции над которым завершилось.

ПРИМЕЧАНИЕ

Если в процессе выполнения описанной здесь процедуры сброса (между шагами 2 и 4) произойдет остановка системы, то при следующей загрузке улья при запуске системы (исключения составляют ульи профилей, которые загружаются при регистрации в системе) система увидит маркер, оставленный на шаге 2, и продолжит восстановление улья на основании измененных данных, которые содержатся в LOG-файле. Таким образом, если улей не находится в переходном состоянии, то при его загрузке LOG-файлы не используются. Если улей находится в переходном состоянии, он не может быть загружен без соответствующего LOG-файла.

Для улья \System используется другой процесс сброса, поскольку этот улей является жизненно важным элементом, данные которого считываются при запуске системы. Кроме того, при запуске системы его использование начинается гораздо раньше, чем других ульев, из-за того, что в его состав входит

ключ `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control`, содержащий параметры, необходимые при инициализации реестра в процессе загрузки. Так, параметры, расположенные в составе ключа `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\hivelist`, используются при поиске остальных файлов ульев реестра. Таким образом, если улей `\System` поврежден, то он не может быть восстановлен с помощью только что описанной процедуры.

Вследствие этого в операционных системах, предшествовавших Windows XP, процесс сброса осуществляется с использованием файла `System.alt`, содержащего копию данных файла `System`. Во время сброса данных изменения помечаются, записываются и затем помечаются как выполненные. После этого точно такой же процесс сброса выполняется для файла `System.alt`. Если на любой стадии процесса происходит отключение питания, аппаратный или программный сбой, то корректная информация может быть найдена либо в файле `System`, либо в файле `System.alt`. Файл `System.alt` в этой процедуре аналогичен LOG-файлу с тем исключением, что во время загрузки система вместо того, чтобы повторно вносить изменения, зарегистрированные в LOG-файле, просто переключается на использование файла `System.alt`. Если же файл `System` не находится в переходном состоянии, то файл `System.alt` не задействуется.

Начиная с Windows XP, эта проблема решается за счет перемещения реестра из нерезидентного пула (`paged pool`) в резидентный и использования менеджера кэша (`cache manager`) для выполнения оперативного управления реестром. Поэтому в Windows XP и последующих версиях Windows отпадает необходимость в использовании файла `System.alt`.

Усовершенствования реестра, появившиеся в Windows Vista и Windows 7

К изменениям, внесенным в реестр Windows, относятся следующие важные нововведения:

- *поддержка транзакций для всех операций над реестром* — позволяет реестру координировать свои обновления в случае групповых изменений, вносимых тем или иным приложением (например, программой-инсталлятором). К тому же, реестр может взаимодействовать с другими диспетчерами ресурсов, например, с расширением TxF (NTFS на базе транзакций). Оба расширения Диспетчера транзакций ядра (KTM, Kernel Transaction Manager) — и только что упомянутый TxF, и TxR (реестр на базе транзакций) — определяют новый набор интерфейсов файловой системы и реестров. Эти интерфейсы аналогичны существовавшим в более

ранних версиях Windows, за единственным исключением — они включают параметр транзакции. Сторонние разработчики тоже могут использовать KTM для разработки собственных диспетчеров ресурсов. Как TxF, так и TxR, основаны на функциях ведения журнала файловой системы, обеспечиваемых общей системой ведения файлов журналов (Common Log File System, CLFS). Сама система CLFS была впервые введена в Windows Server 2003 R2 и реализована драйвером %SystemRoot%\System32\Clfs.sys. Расширение TxR создает журнал CLFS, расположенный в папке %SystemRoot%\System32\Config\Journal, а также набор взаимосвязанных файлов журнала для отслеживания изменений реестра в каталоге %SystemRoot%\System32\Config\TxR (рис. 1.14);

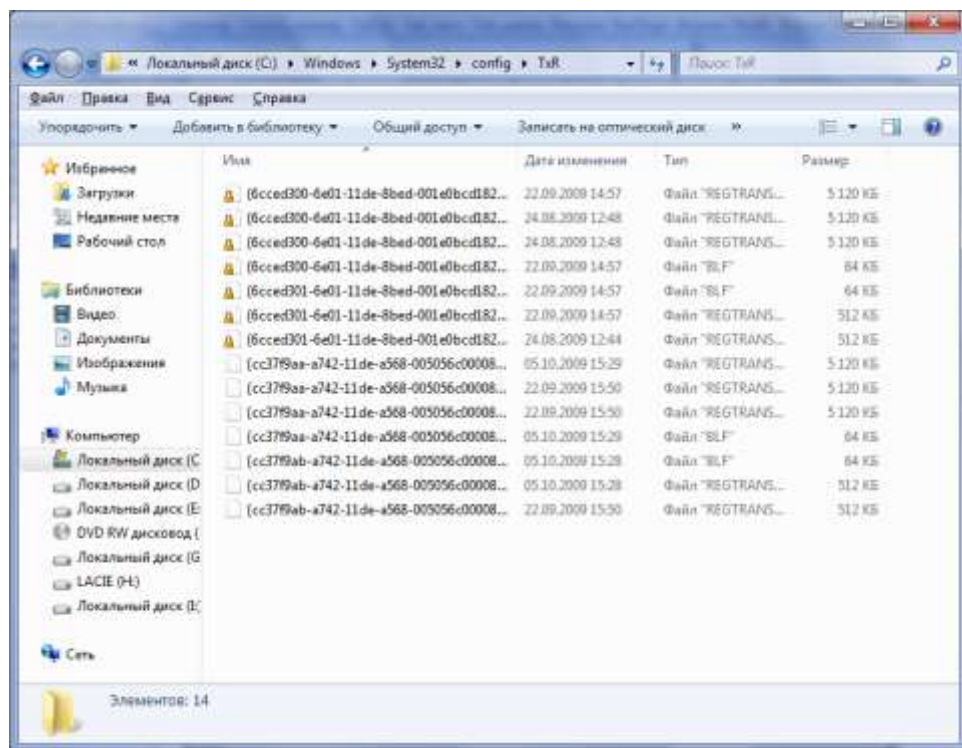


Рис. 1.14. Файлы журналов, ведущиеся расширением TxR для ульев реестра

- *минимизация риска повреждения реестра* — усовершенствованная поддержка при сбоях защищает страницы памяти от случайных повреждений, пометая их доступными только на запись. Когда реестр должен записывать данные на одну из таких страниц, права доступа меняются, делая

возможной записью. После завершения операции записи, права доступа к странице восстанавливаются в исходное состояние;

- *поддержка виртуализации реестра и уровней выполнения приложений* — виртуализация реестра (registry virtualization) позволяет наследуемым приложениям работать от лица учетных записей без административных прав. Виртуализация реестра изолирует операции записи, имеющие глобальное влияние на всю системную конфигурацию, перенаправляя операции записи в ключ `HKLM\Software` — в соответствующие подключи ключа `HKCU`. Все остальные ключи реестра виртуализацией не затрагиваются.

Для поддержки уровней выполнения и виртуализации все приложения в Windows теперь снабжаются специальным *маркером безопасности* (security token), который указывает уровень системных полномочий, необходимых для работы приложений. Приложения могут иметь маркер административный (administrator token) или стандартный (standard token):

- приложения с административными маркерами для запуска и выполнения основных задач требуют повышенного уровня привилегий. После запуска приложения с повышенным уровнем полномочий, оно сможет выполнять административные задачи, в том числе — и выполнять запись в защищенные разделы реестра и файловой системы;
- приложения со стандартным маркером безопасности для запуска и выполнения основных задач не требуют повышения уровня привилегий. Если приложение пытается выполнить административную задачу, оно должно запрашивать повышение уровня привилегий (в этом и заключается суть UAC).

Наследуемые приложения работают в специальном режиме совместимости. Когда такое приложение пытается выполнить запись в защищенный раздел реестра, Windows создает для него частную (private) копию параметра, которая сохраняется в пользовательском профиле. Впоследствии приложение будет работать именно с этой копией.

Когда следует браться за редактирование реестра

Наилучшим ответом на этот вопрос будет: только в крайнем случае. Не следует приобретать привычку думать о редактировании реестра каждый раз, как только у вас возникнет проблема. Разработчики старались не для того, чтобы пользователи решали незначительные, второстепенные проблемы путем модификации реестра. В самом деле, Microsoft приложила огромные

усилия для разработки мощных графических средств и информативных диалоговых окон, предназначенных для помощи пользователям при решении задач конфигурирования системы и устранения проблем. Пользователям настоятельно рекомендуется попытаться решить проблему с их помощью и только потом начинать копать в реестре — если все испробованные методы не помогают.

Однако, в конце концов, может наступить и такой момент, когда, сколько бы вы ни пытались изменить настройки в Панели управления (Control Panel) или переключать значения с помощью Диспетчера устройств (Device Manager), добиться правильной работы устройства или опции окажется невозможно. Именно на этот случай вы и должны знать, как обращаться с реестром и как его редактировать.

Множество рекомендаций, связанных с редактированием реестра, можно найти в Интернете. Как правило, все они содержат инструкции по изменению в реестре того или иного параметра. Настраивая реестр с использованием таких рекомендаций, обязательно выполните предварительное резервное копирование реестра. Методы резервного копирования и восстановления реестра будут детально рассмотрены в *главе 2*.

Альтернативы редактированию реестра

Непосредственное редактирование реестра, даже в тех случаях, когда оно необходимо, способно при условии неумелого выполнения привести к большим неприятностям. Например, оно может вызвать ошибки в загрузке драйверов устройств или не позволить пользователю зарегистрироваться в системе. Поэтому, если вы чувствуете себя неуверенно или просто не можете позволить себе затратить значительное время для проведения восстановительных работ, не ставьте смелых экспериментов над реестром своей операционной системы — вполне возможно, что единственная ошибка приведет к необходимости ее полной переустановки.

Когда вы поближе познакомитесь с реестром, вы можете поддаться соблазну отредактировать его, например, при установке новых аппаратных средств. Обсуждаемый в *главе 3* Редактор реестра (Registry Editor) представляет собой средство, с помощью которого можно с легкостью изменить и модифицировать параметры реестра. Однако не рекомендуется сразу начинать работать с Редактором реестра, не сделав сначала попытки выполнить эту же задачу при помощи административных утилит. Кроме того, многие из параметров реестра понять просто невозможно, поскольку они имеют смысловое значение только для использующего их физического устройства.

СОВЕТ

Использование административных утилит всегда предпочтительнее непосредственного редактирования реестра. Этот метод намного безопаснее, поскольку административные средства не позволяют сохранять в реестре некорректные значения. Если в процессе редактирования реестра с помощью Редактора реестра будет допущена ошибка, вы не получите никакого предупреждения, поскольку редактор реестра не распознает и не исправляет такие ошибки.

Так, не рекомендуется вручную редактировать реестр при установке новых устройств. Дело тут в способе работы устройств, соответствующих спецификации Plug and Play. Как будет показано в *главе 5*, устройства этих типов фактически не имеют установочных параметров, задаваемых по умолчанию. Напротив, они разработаны таким образом, что если некоторое устройство запрашивает ресурс, уже используемый другим устройством Plug and Play, то настройка устройства Plug and Play может измениться, чтобы исключить аппаратный конфликт с новым устройством. Изменяя в реестре параметры этих устройств вручную, вы тем самым задаете для них постоянные значения, которые Windows не сможет изменить, если другое устройство запросит тот же самый ресурс.

Изменение конфигурации в Панели управления

Большая часть полезных установок системы и аппаратного обеспечения может быть изменена в Панели управления (Control Panel). Для выполнения этих задач вам не нужно прибегать к редактированию реестра. К сожалению, ограниченный объем этой книги не позволяет подробно останавливаться на конфигурационных опциях, доступных через пользовательский интерфейс. Книг, посвященных этой тематике, вышло уже немало, и заинтересованный читатель может выбрать любую из них. Лично я рекомендовала бы книгу моего коллеги А. Н. Чекмарева "Microsoft Windows 7 — Это вам понравится".

Напомню только, что в Windows 7, как и в Windows 2000/XP/Vista, разработчики защищают от просмотра некоторые файлы операционной системы. Это так называемые *сверхскрытые* (super-hidden) файлы. По умолчанию Проводник (Explorer) не отображает файлы, которые имеют атрибуты **Скрытый** (Hidden) и **Системный** (System). Эти файлы операционная система считает необходимым защитить, чтобы обычный пользователь не только не мог внести в них изменения, но даже и увидеть их. Очевидно, что по умолчанию в список таких файлов входят все файлы, необходимые для запуска операционной системы.

Для получения возможности видеть скрытые файлы в Проводнике, запустите из Панели управления (Control Panel) утилиту **Свойства папки** (Folder Options) и перейдите на вкладку **Вид** (View) (рис. 1.15).

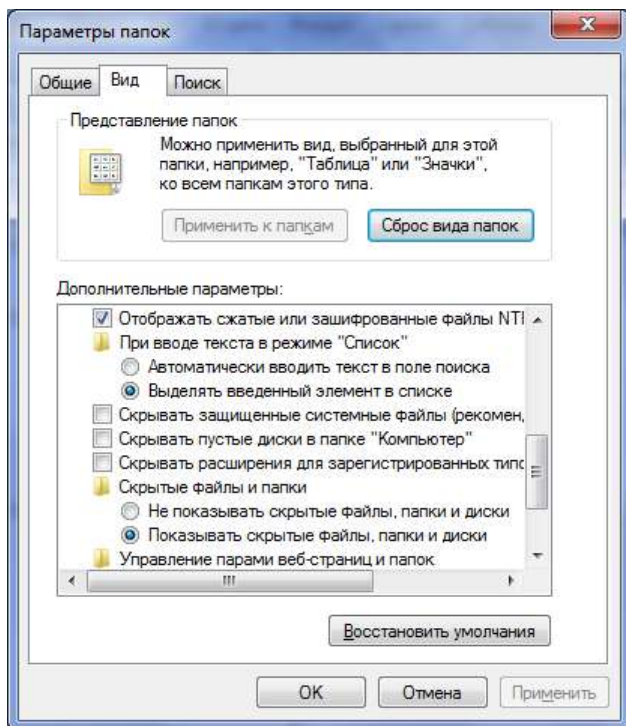


Рис. 1.15. Вкладка **Вид** (View) окна **Параметры папок** (Folder Options)

ПРИМЕЧАНИЕ

Существует и еще один метод доступа к окну **Свойства папки** — при просмотре любой папки через пользовательский интерфейс Windows выберите из меню **Упорядочить** (Organize) команду **Свойства папок и поиска** (Search and Folder Options), а затем перейдите на вкладку **Вид** (View).

Установите на вкладке **Вид** (View) переключатель **Показывать скрытые файлы, папки и диски** (Show hidden files, folders, and drivers) и сбросьте флажок **Скрывать защищенные системные файлы (рекомендуется)** (Hide protected operating system files (Recommended)) в списке **Дополнительные параметры** (Advanced settings). Теперь в Проводнике и папке **Компьютер** (Computer) будут показаны все файлы, включая также те, которые защищены операционной системой.

Перед выполнением указанных операций вам необходимо зарегистрироваться в локальной системе под именем пользователя **Администратор** (Administrator) или от лица пользователя с административными правами, в противном случае вы не получите желаемого результата.

ПРИМЕЧАНИЕ

В Windows Vista и Windows 7 есть секретная (!) учетная запись **Администратор** (Administrator), и она отличается от простой администраторской учетной записи. Эта секретная учетная запись не подпадает под действие UAC (User Account Control, контроль учетных записей пользователей), поэтому **Администратор** может производить в системе любые изменения и ни разу не увидит предупреждений UAC. По умолчанию эта учетная запись выключена и сделана скрытой. Более подробно об этой учетной записи, а также о том, как ее активизировать, будет рассказано в *главе 4*.

Чтобы увидеть все файлы, независимо от их атрибутов, можно также дать из *командной строки* команду `dir/a`. Командная строка пригодится вам и для выполнения многих других операций, но в Windows Vista и Windows 7 здесь существует один нюанс — в большинстве случаев, чтобы добиться нужного результата, вам потребуется не просто сеанс работы с командной строкой, а командная строка с административными правами. Поэтому, чуть забежав вперед, я расскажу, как это следует делать.

Проблема состоит в том, что, начиная с Windows Vista, Microsoft начала последовательно реализовывать поддержку так называемого *принципа минимальных полномочий* (Least Privileged User Account, LUA). В соответствии с этим принципом, пользователю или программе должны быть предоставлены только те полномочия, которые необходимы им для выполнения задания, не меньше, но и ни в коем случае — не больше. И в самом деле — вредоносные программы (malware) значительно опаснее, когда они выполняются в контексте безопасности учетной записи с широкими правами.

Пример, иллюстрирующий реализацию этого принципа в Windows 7, показан на рис. 1.16. В данном случае была сделана попытка выполнить привилегированную команду от лица пользователя, принадлежащего группе администраторов (Administrators), но не в контексте встроенной учетной записи **Администратор** (Administrator).

Результат выполнения тех же самых команд в контексте встроенной учетной записи администратора показан на рис. 1.17.

Запускать сеанс командной строки с правами администратора вам придется часто, поэтому остановимся на этом вопросе чуть подробнее. Как и во многих других случаях, в Windows Vista/7 эта задача может быть выполнена множеством различных способов. Вот только два из них, универсальных и надежно работающих в любом случае:

- из меню **Пуск** (Start) выберите опцию **Программы | Стандартные** (Programs | Accessories), щелкните правой кнопкой мыши на опции **Командная строка** (Command Prompt) и из контекстного меню выберите команду **Запуск от имени Администратора** (Run as Administrator);

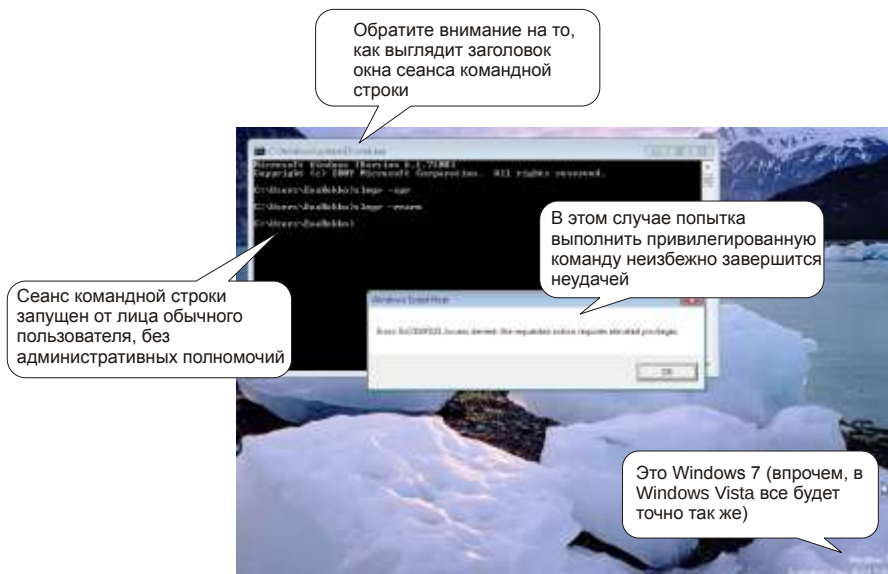


Рис. 1.16. Попытка выполнения привилегированной команды от лица непривилегированного пользователя неизбежно приводит к ошибке

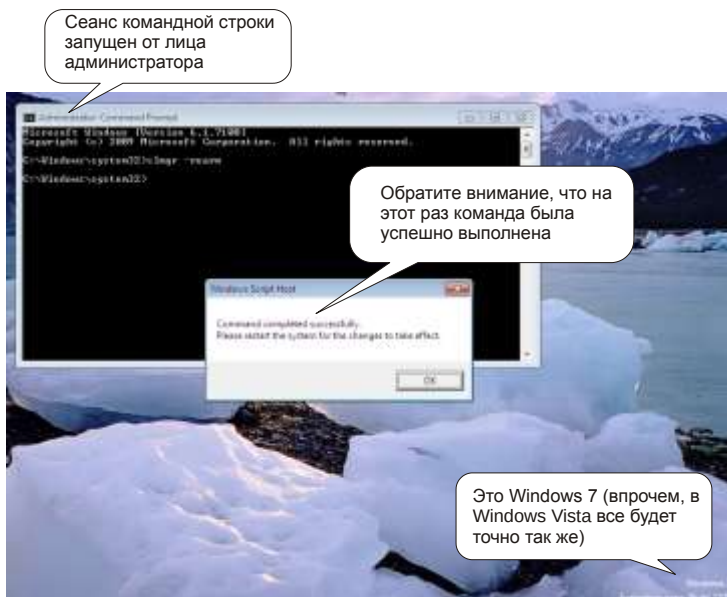


Рис. 1.17. Результат выполнения привилегированных команд из сеанса командной строки, запущенного в контексте встроенной учетной записи **Администратор** (Administrator)

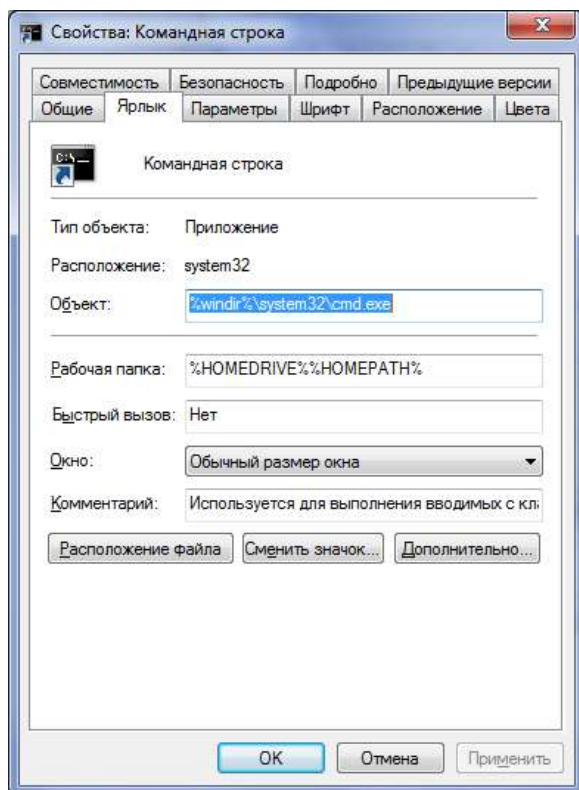
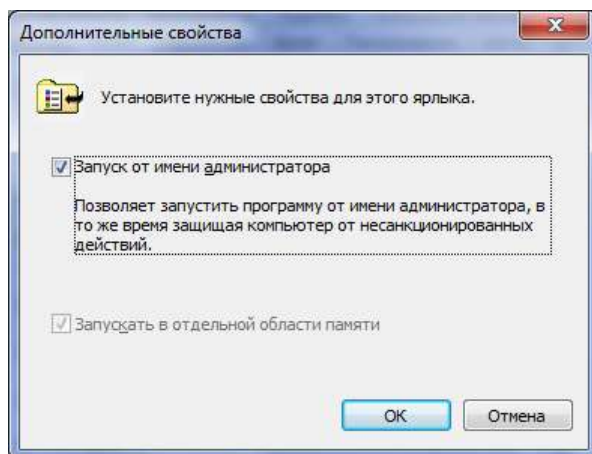
Рис. 1.18. Окно **Свойства: Командная строка**

Рис. 1.19. Окно дополнительных свойств командной строки позволяет запускать программу от имени администратора

- ❑ и более короткий вариант — создайте на рабочем столе ярлык для запуска командной строки (Command Prompt). Когда возникнет необходимость запуска сеанса командной строки от имени администратора, выполняйте щелчок правой кнопкой мыши на этом ярлыке и выбирайте из контекстного меню команду **Запуск от имени Администратора** (Run as Administrator). Чтобы дополнительно упростить эту процедуру, выполните щелчок правой кнопкой мыши на вновь созданном ярлыке и выберите из контекстного меню команду **Свойства** (Properties). Откроется окно **Свойства: Командная строка** (Command Line Properties), как на рис. 1.18. Нажмите в этом окне кнопку **Дополнительно** (Advanced) и в открывшемся на экране окне (рис. 1.19) установите флажок **Запуск от имени администратора** (Run as Administrator).

ПРИМЕЧАНИЕ

Если вы хотите поместить командную строку повышенного уровня в меню **Пуск** (Start), "перетащите" ярлык с рабочего стола на кнопку **Пуск**.

Другие инструментальные средства для изменения реестра

Кроме утилит панели управления и других инструментальных средств графического пользовательского интерфейса, предоставляемых Windows 7, существуют дополнительные инструментальные средства, предназначенные для изменения реестра:

- ❑ вы можете использовать диалоговые окна **Параметры** (Options), представленные в Windows-совместимых приложениях. Как мы уже упоминали, в каждом Windows-приложении должно быть предусмотрено хранение собственных установок и обеспечение пользователей графическими инструментальными средствами, позволяющими вносить изменения в эти установки реестра;
- ❑ установки реестра также могут быть изменены с помощью свободно распространяемых (freeware) или же условно-бесплатных (shareware) приложений (как Microsoft, так и других разработчиков). Более подробную информацию о наиболее популярных утилитах реестра можно найти в *главе 14*;
- ❑ можно изменять REG- и INF-файлы.

Заключение

В этой главе приведено общее описание реестра Windows 7, его истории, роли и возможностей, а также рассмотрено место реестра в общей архитектуре Windows.

Глава 2



Методы восстановления поврежденной системы

Если какая-нибудь неприятность может произойти, она случается.

Закон Мэрфи

Даже если неприятность не может случиться, она все равно случается.

Обобщение Шнэттерли

Если вы — системный администратор или специалист из группы технической поддержки, то наверняка можете привести множество примеров, когда пользователи обращались к вам за помощью, встретившись с ошибками реестра Windows. Иногда (к счастью, достаточно редко) бывает и так, что пользователи сталкиваются с проблемами поврежденного реестра даже прежде, чем могут в первый раз запустить операционную систему. Возникновение ошибок реестра особенно вероятно в тех случаях, когда пользователи часто модифицируют и редактируют реестр, пытаясь осуществить рискованные эксперименты. Не имея достаточного опыта, очень просто ввести в реестр неверное значение или ошибочно удалить необходимый ключ. В результате таких операций реестр может оказаться неработоспособным.

Прежде чем модифицировать реестр Windows 7, рекомендуется уделить время изучению альтернативных способов его редактирования, а также методов его резервного копирования и восстановления. Существует множество самых разнообразных альтернативных методов редактирования реестра Windows, с помощью которых можно решить проблему или установить системные параметры. В Интернете часто встречаются статьи, описывающие пути решения проблем с помощью сложных процедур редактирования реестра. Однако, хорошо зная базовые и дополнительные возможности Windows 7, можно найти гораздо более простые и элегантные решения с помощью опций из Панели управления (Control Panel) или других административных утилит.

СОВЕТ

Внеся в реестр некорректные изменения или случайно удалив некоторые из его элементов, можно полностью заблокировать работу системы. Поэтому всегда, если только возможно, вносите изменения в конфигурацию системы с помощью средств Панели управления (Control Panel) или других административных утилит. Редактор реестра (Registry Editor) следует применять только тогда, когда стандартные методы помочь не могут. Чтобы защитить конфигурацию системы, администраторы могут ограничить доступ пользователей к реестру. Подробная информация по данному вопросу будет приведена в *главе 9*.

Подготовка к редактированию реестра

Итак, у вас возникла потребность открыть реестр и путем его редактирования решить стоящие перед вами проблемы. Этому вопросу посвящена вся книга, поэтому предполагается, что читатель обязательно будет выполнять непосредственное редактирование реестра. Материал, изложенный в следующих главах, требует именно редактирования конкретных элементов реестра.

Однако прежде чем вы этим займетесь, следует выполнить резервное копирование реестра. Это первая мера, которую необходимо осуществить перед тем, как приступить к модификации реестра. Никогда не редактируйте реестр, не создав резервной копии! Как и всякий человек, вы не застрахованы от ошибок. Между тем, Редактор реестра, который будет подробно обсуждаться в *главе 3* данной книги, не обеспечивает надлежащей страховки, предоставляемой большинством других программ, — в частности, он не имеет даже команды **Отменить** (Undo). Не следует создавать себе лишних проблем (если, конечно, вы не являетесь поклонником этого вида искусства), ведь готовое решение уже есть, и заключается оно в резервном копировании реестра.

В официальной документации Microsoft и статьях из Microsoft Knowledge Base предупреждения о том, что утилиты редактирования реестра пользователи должны применять на свой страх и риск, встречаются постоянно. Microsoft не гарантирует непереносимости решения проблем, вызванных неправильным редактированием реестра. Вполне возможно, что если работоспособная резервная копия отсутствует, то единственным методом исправления ситуации может оказаться переустановка операционной системы. Помните, что на склеивание вазы уходит больше времени, чем на то, чтобы ее разбить.

Существует множество способов резервного копирования и восстановления реестра. В следующие за Windows XP версии Windows были введены суще-

ственно улучшенные средства защиты данных и системы, реализующие новые технологии резервного копирования, в том числе:

- ☐ восстановление системы (System Restore);
- ☐ теневое копирование;
- ☐ резервное копирование и восстановление файлов;
- ☐ средство полного резервного копирования и восстановления компьютера Windows (к сожалению, включенное только в Windows 7 Professional, Enterprise и Ultimate);
- ☐ улучшенная среда восстановления Windows (Windows Recovery Environment, WinRE).

Все эти технологии получили дальнейшее развитие и в Windows 7. Они взаимно дополняют друг друга, и в этой главе будет представлено подробное описание всех таких процедур для защиты и восстановления ваших данных. Практический опыт показывает, что в случае возникновения нестабильностей в работе системы лучше всего начать с использования функции восстановления системы, а к полному восстановлению компьютера лучше всего прибегать как к последнему средству и использовать его с осторожностью.

Средство восстановления системы

Восстановление системы (System Restore), реализованное в Windows 7, напоминает подобное же средство, имевшееся в Windows XP/Vista, однако в новой версии оно, как и следовало ожидать, было дополнено новыми возможностями. В первую очередь рассмотрим, что же представляет собой это средство. Как правило, опытным пользователям, которые хорошо знакомы с одной из предыдущих версий Windows (XP или Vista), уже известно, что использование System Restore позволяет произвести "откат" операционной системы к одной из стадий, на которой было зафиксировано состояние системы в тот момент, когда она была стабильной и работала правильно, — к так называемой *точке восстановления* (restore point).

Основные преимущества этого средства заключаются в его "дружественности" и в том, что оно позволяет быстро исправить все повреждения системы, не прибегая к выполнению утомительных процедур "ручного" восстановления системы или даже к ее переустановке. При этом восстановление системы (System Restore) не перезаписывает пользовательские файлы, такие как, например, созданные вами документы, сообщения электронной почты, архивы и т. п. Таким образом, эта функция должна стать для вас первой линией обороны.

В Windows XP средство восстановления системы использовало фильтр файловой системы для отслеживания произошедших в ней изменений. Начиная с Windows Vista, для этой же цели используется *теневое копирование томов* (Volume Shadow Copy), о котором будет рассказано чуть далее в этой главе. Отслеживание изменений при этом производится на уровне блоков в выбранных томах, что делает средство восстановления системы более надежным и позволяет поддерживать широкий спектр вариантов восстановления.

Кроме того, новое средство восстановления системы может применяться, даже если установленная копия Windows неработоспособна (например, прекратила загружаться). Это делается с помощью *среды восстановления* Windows WinRE (Windows Recovery Environment), позволяющей восстановить систему, даже если Windows не загружается.

Точки восстановления

Точки восстановления (restore points) представляют собой "моментальные снимки" состояния системы (включая, разумеется, и реестр), которые регулярно сохраняются на жестком диске.

Точки восстановления создаются автоматически или в соответствии с заданным расписанием, установленным с помощью *системного планировщика* (Task Scheduler). Кроме того, пользователи могут при необходимости создавать точки восстановления вручную. Такие точки восстановления будут иметь тип **Вручную** (Manual).

Автоматическое создание точек восстановления может быть вызвано определенными системными событиями, к числу которых относятся:

- ❑ установка в системе новых приложений/драйверов устройств либо их переконфигурирование/удаление — тип точки восстановления **Установка** (Install) или **Система** (System);
- ❑ установка в системе обновлений через Windows Update — тип точки восстановления **Критическое обновление** (Critical Update);
- ❑ выполнение операции восстановления — в этом случае создается точка восстановления типа **Отмена** (Undo). Создание точек восстановления этого типа обеспечивает обратимость операций восстановления системы.

Периодичность автоматического создания точек восстановления при отсутствии вызвавших их системных событий зависит от операционной системы. Напомним, что по умолчанию в Windows XP средство восстановления системы (System Restore) создает точку восстановления через каждые 24 часа непрерывной работы. В Windows Vista средство восстановления системы (System Restore) тоже автоматически создает точку восстановления каждые

24 часа непрерывной работы, но при условии, что в течение этих суток не было создано ни одной другой точки восстановления. Средство восстановления системы в Windows 7 автоматически создает точку восстановления в соответствии с расписанием, заданным системным планировщиком, но при условии, что в течение последних истекших 7 дней не было создано ни одной точки восстановления.

Кроме очевидных удобств, функция System Restore в Windows XP/Vista обладала целым рядом недостатков, в том числе:

- ❑ несмотря на свои простоту и удобство, делавшие ее "первой линией защиты", процесс восстановления системы, если точки восстановления долго не создавались, мог потребовать довольно значительного времени;
- ❑ файлы точек восстановления системы не позволяли пользователю "заглянуть внутрь" и узнать, какое влияние окажет на систему ее откат к выбранной точке восстановления;
- ❑ процедуру восстановления можно было выполнить лишь в полном объеме, а возможность восстановления отдельных файлов и папок отсутствовала;
- ❑ отсутствовала и возможность сохранения лишь части системных настроек — например, только системных файлов (System files) или только предшествующих версий файлов (теневого копии тома).

Начиная с Windows 7, средство System Restore свободно от перечисленных недостатков.

ПРИМЕЧАНИЕ

Использование средства восстановления системы (System Restore) в предшествующих версиях Windows достаточно полно и подробно описано в моих книгах "Реестр Windows XP", "Реестр Windows Vista" и "Windows Vista. Решение проблем", выпущенных издательством "БХВ-Петербург". Здесь же мы сосредоточимся на использовании новейшей и усовершенствованной версии этого средства, реализованной в Windows 7.

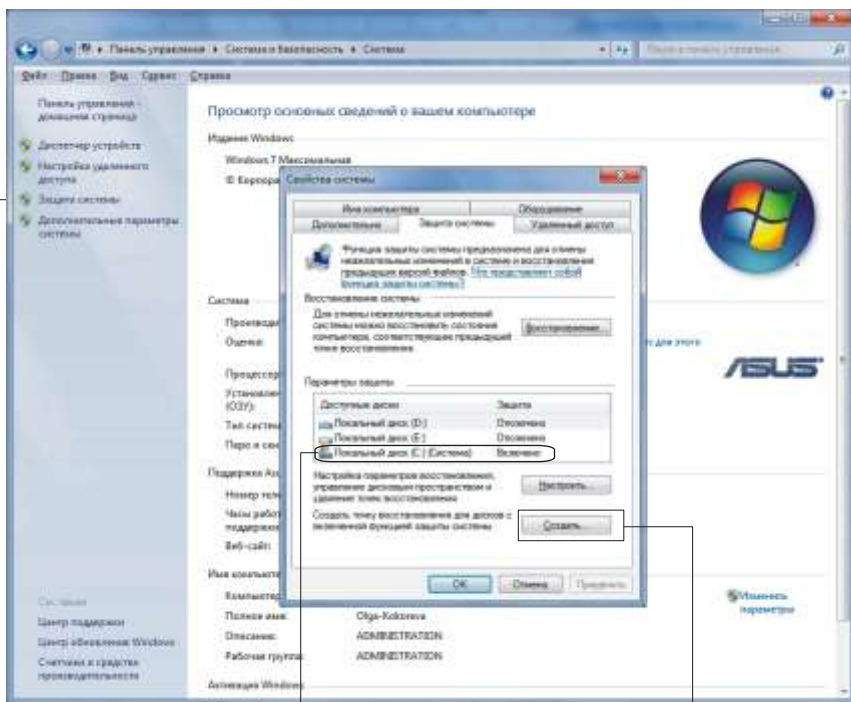
Создание точки восстановления

Как уже говорилось, по умолчанию Windows 7 создает точки восстановления перед важными системными событиями, а также по расписанию, заданному системным планировщиком (Task Scheduler), но при условии, что в течение последних истекших 7 дней не было создано ни одной точки восстановления. Разумеется, при желании вы можете создавать точки восстановления и вручную. Процесс ручного создания точек восстановления в Windows 7 очень

прост. Чтобы создать новую точку восстановления вручную, выполните следующие действия:

1. В меню **Пуск** (Start) выберите команду **Панель управления** (Control Panel), затем выберите опции **Система и безопасность** (System and Security) | **Система** (System), а затем щелкните по ссылке **Защита системы** (System Protection), и на экране появится окно **Свойства системы** (System Properties), раскрытое на вкладке **Защита системы** (System Protection), как показано на рис. 2.1. Именно в этом окне вы и можете вручную создать точку восстановления компьютера для средства восстановления системы (System Restore).

Работа средства System Restore основывается на функции System protection



Функция System Protection должна быть активна, как минимум, для раздела, на котором установлена система Windows 7

Чтобы создать точку восстановления, нажмите эту кнопку

Рис. 2.1. Вкладка **Защита системы** окна **Свойства системы**

Обратите внимание — для создания точки восстановления необходимо, чтобы в системе была активизирована функция защиты системы (System

Protection), на которую и опирается средство восстановления системы (System Restore). Впрочем, эта функция по умолчанию активизируется для того раздела жесткого диска, на котором установлена операционная система Windows 7 (разумеется, при условии, что на этом диске имеется достаточный объем дискового пространства, о чем мы поговорим чуть позже в этой главе). Если вы хотите активизировать функцию защиты системы и для других дисков и разделов, вы можете выполнить это в окне **Свойства системы** (System Properties) — см. рис. 2.1. Взгляните на это окно еще раз — в приведенном примере функция защиты системы (System Protection) защищает раздел, на котором установлена Windows 7, но не защищает других разделов — в столбце **Защита** (Protection) стоит значение **Отключено** (off).

Более подробно о конфигурировании функции System Protection будет рассказано чуть позже в этой главе, пока же вам достаточно убедиться в том, что, как минимум, для раздела, на котором установлена Windows 7, опция **Защита системы** (System Protection) активизирована.

- Итак, для создания точки восстановления на вкладке **Защита системы** (System Protection) диалогового окна **Свойства системы** (System Properties) (см. рис. 2.1) нажмите кнопку **Создать** (Create). В открывшемся диалоговом окне введите название вновь создаваемой точки восстановления (рис. 2.2) и нажмите кнопку **Создать** (Create).

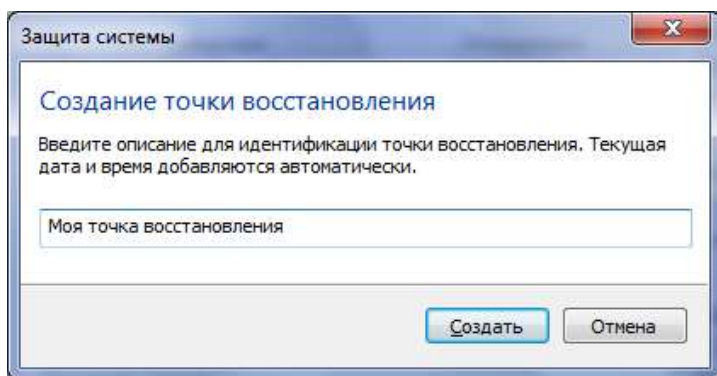


Рис. 2.2. Для создания новой точки восстановления вам потребуется вручную ввести ее имя

- На экране появится небольшое диалоговое окно с индикатором процесса, а затем, когда процесс завершится — диалоговое окно, сообщающее об успешном завершении операции (рис. 2.3).

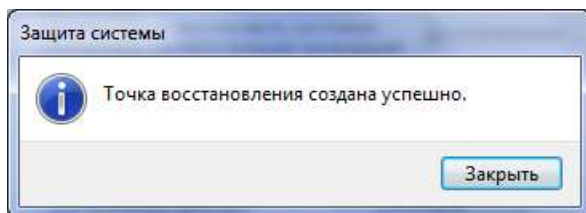


Рис. 2.3. Диалоговое окно, сообщающее об успешном создании точки восстановления

Восстановление состояния системы

Для восстановления системы с помощью одной из существующих точек восстановления, выполните следующие действия:

1. Нажмите кнопку **Восстановление системы** (System Restore) на вкладке **Защита системы** (System Protection) окна **Свойства системы** (System Properties) (см. рис. 2.1) или запустите утилиту **Восстановление системы** (System Restore) через меню **Пуск** (Start), как показано на рис. 2.4.

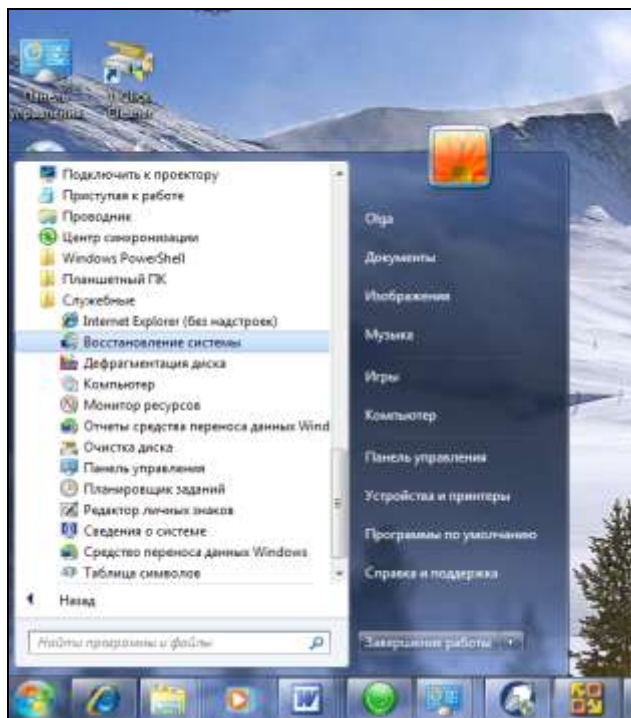
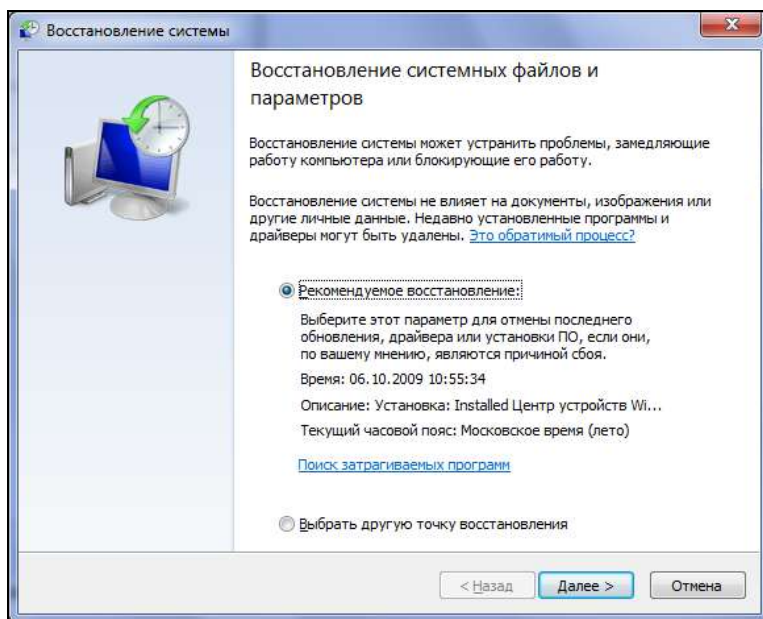
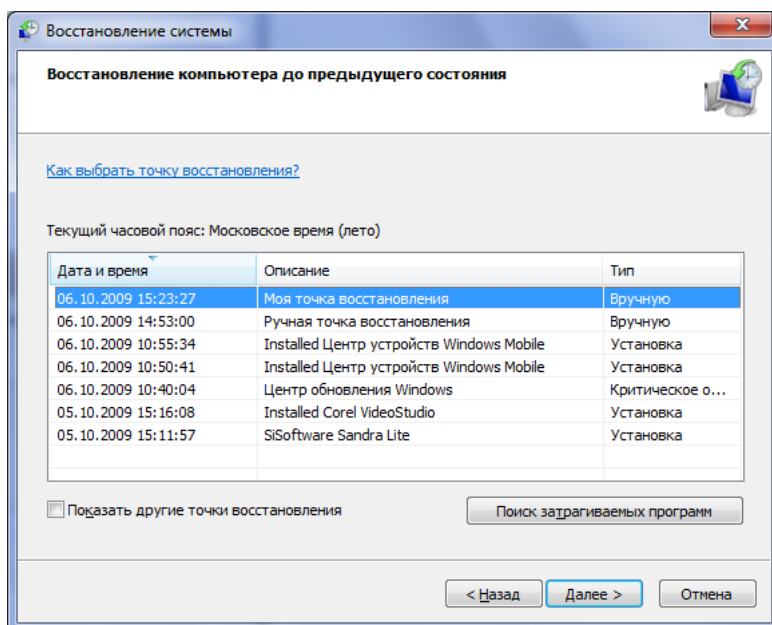


Рис. 2.4. Запуск утилиты System Restore через меню Пуск

Рис. 2.5. Окно утилиты **Восстановление системы** в Windows 7Рис. 2.6. Окно **Восстановление системы** (System Restore), предлагающее выбрать точку восстановления

2. Откроется окно утилиты **Восстановление системы** (System Restore), показанное на рис. 2.5. По умолчанию система предлагает вам выполнить откат к точке восстановления, которая была создана последней. Если вы хотите выбрать другую точку восстановления, отличную от рекомендованной, установите переключатель **Выбрать другую точку восстановления** (Select another restore point), нажмите в этом окне кнопку **Далее** (Next), и на экране откроется следующее окно (рис. 2.6), в котором вам будет предложено выбрать точку восстановления.

Если в вашей системе создано уже несколько точек восстановления, то в этом окне вы можете выбрать одну из них. Имейте также в виду, что если вы подолгу работаете на компьютере, то в некоторые дни будет создаваться несколько точек восстановления. С другой стороны, в те дни, когда вы не используете компьютер, точки восстановления создаваться не будут. Как показано на рис. 2.6, по умолчанию средство восстановления системы (System Restore) предложит вам точку восстановления, созданную последней.

СОВЕТ

Общая рекомендация по выбору точек восстановления заключается в том, чтобы выбирать те из них, которые были созданы накануне того момента, когда в системе начались проблемы — например, вы установили некую программу, а она не работает, или, допустим, установили или обновили драйвер устройства, и система после этого пришла в нестабильное состояние.

Заметьте также, что имена для точек восстановления, которые система создала автоматически, соответствуют имени системного события. Примерами таких системных событий являются, например, установка обновления средством Windows Update или установка/удаление программы или драйвера. Например, на рис. 2.7 выбрана точка восстановления, автоматически созданная системой перед установкой программы видеомонтажа Corel VideoStudio.

Наконец, самое главное — посмотрите: в Windows 7 появилась возможность не только выбрать точку сохранения, но и просмотреть, на какие приложения повлияет откат системы к состоянию, которое она имела на момент создания выбранной точки восстановления. Для этой цели нажмите кнопку **Поиск затрагиваемых программ** (Scan for affected programs) — см. рис. 2.6 или 2.7.

ПРИМЕЧАНИЕ

Окна, иллюстрирующие этот пример (рис. 2.6 и 2.7), очень показательны. Посмотрите — в списке присутствуют различные типы точек восстановления: созданные вручную (**Manual**), а также автоматически созданные системой при установке программы (**Install**) или обновления Windows (**Critical Update**).

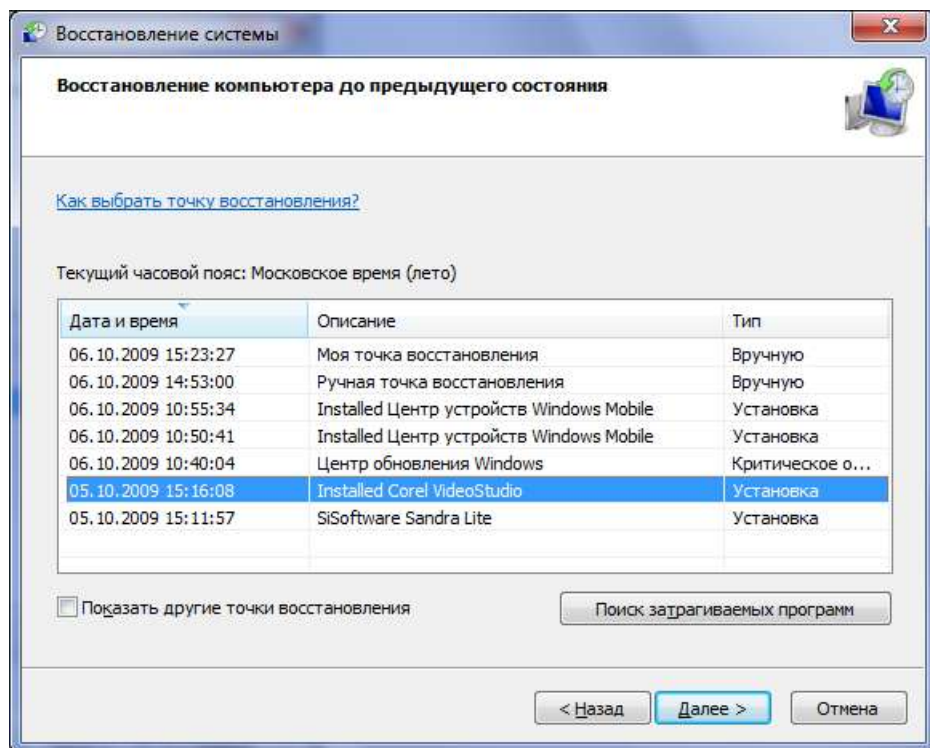


Рис. 2.7. Это окно предлагает выбрать одну из существующих точек восстановления — в данном примере выбрана точка **Installed Corel VideoStudio** (она была создана автоматически при установке соответствующей программы)

3. На экране сначала появится небольшое окно с индикатором прогресса, отражающим ход процесса сканирования, а затем откроется окно, показанное на рис. 2.8. Обратите внимание — в данном случае сначала была создана точка восстановления с именем **Installed Corel VideoStudio** (см. рис. 2.7), а вскоре после этого Центр обновления Windows (Windows Update Center) автоматически произвел установку критического обновления Windows. Затем было выполнено две попытки установки Центра устройств Windows Mobile (Windows Mobile Device Center), а после этого я вручную создала две точки восстановления. Теперь, если выполнить откат к точке восстановления с именем **Installed Corel VideoStudio**, то и эта программа, со всеми зависимыми от нее приложениями, а также все установленные после нее программы и драйверы (если они есть) будут удалены из системы. Согласитесь, что это очень удобно — сразу же получить информацию о том, какие программы и драйверы вам придется переустановить после отката (если, конечно, они вам нужны).

С другой стороны, если вы создали точку восстановления, а затем удалили одну из программ (один из драйверов), которые присутствовали в системе на момент создания точки восстановления, то эти программы появятся в списке в нижней части окна (рис. 2.8). Таким образом, Windows 7 предупреждает вас о том, что программы могут быть восстановлены, правда, работоспособность их после этой операции не гарантируется, и они все же могут потребовать переустановки.

Просмотрев списки программ, на которые может повлиять откат к выбранной точке восстановления, нажмите кнопку **Заккрыть** (Close), и вы вернетесь в окно, предлагающее выбрать одну из точек восстановления (см. рис. 2.6 или 2.7).

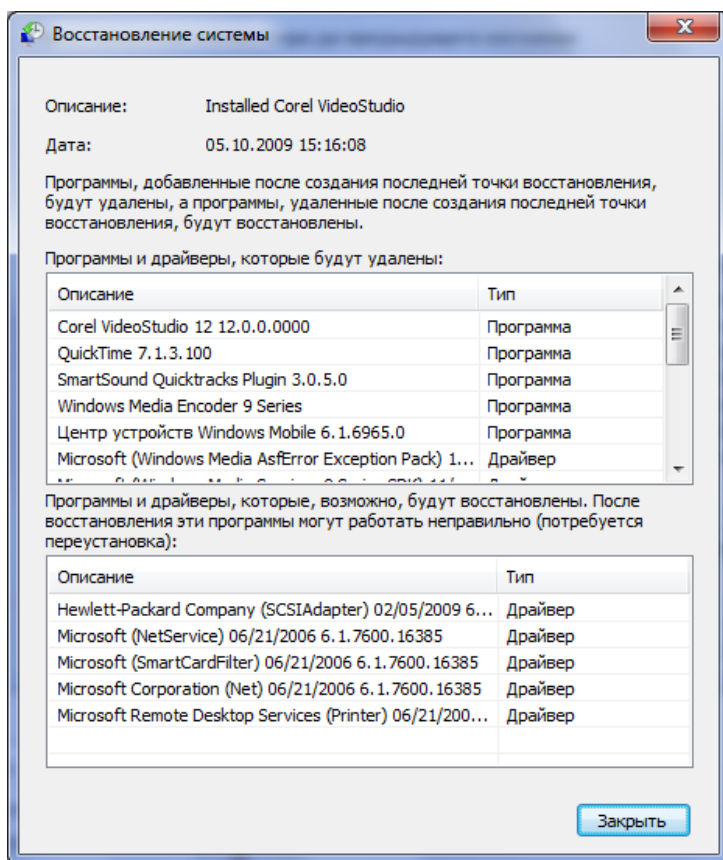


Рис. 2.8. Windows 7 отображает список программ и драйверов, установленных в системе после создания точки восстановления, — все эти программы и драйверы при откате будут удалены, а также список программ, которые при откате к точке восстановления могут быть восстановлены (правда, работоспособность их при этом не гарантируется)

4. Руководствуясь приведенными рекомендациями, выберите одну из точек восстановления и нажмите кнопку **Далее** (Next). На экране откроется следующее окно, предлагающее подтвердить выбранную точку восстановления (рис. 2.9). Обратите внимание — здесь вам еще раз будет дана возможность еще раз просканировать список программ, на которые может повлиять откат, а также создать диск, дающий возможность заменить пароль для входа в систему (это рекомендуется сделать в тех случаях, если вы его действительно меняли). Чтобы сделать это, пройдите по ссылке **Создание дискеты сброса пароля** (Create a password reset disk) и следуйте выводимым на экран инструкциям. Наконец, выполнив все проверки, нажмите кнопку **Готово** (Finish).

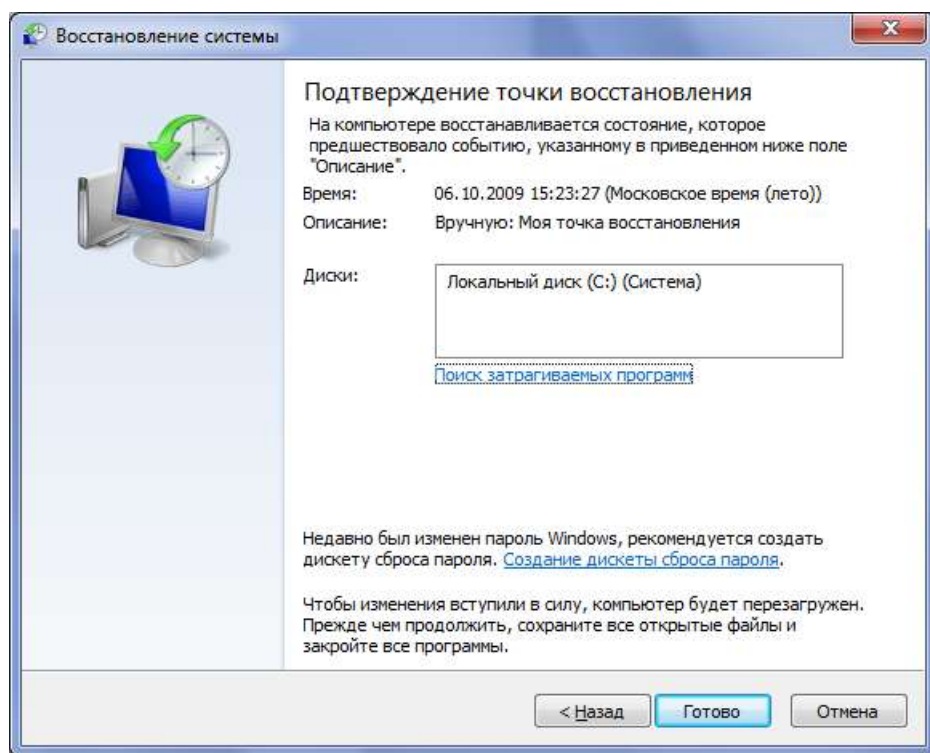


Рис. 2.9. Окно, предлагающее подтвердить выбранную точку восстановления

5. Сразу же после этого на экране появится окно с предупреждением (рис. 2.10). Так что имейте в виду — когда процесс восстановления начнется, он не может быть прерван. Кроме того, средство System Restore предупреждает вас и о том, что операции восстановления не всегда явля-

ются обратимыми — например, если операция была запущена при загрузке Windows в безопасном режиме или из меню **Устранение неполадок компьютера** (System Recovery Options) (об этом будет рассказано в *главах 7 и 11*). И окно предупреждения дает вам последнюю возможность отказаться от выполнения отката нажатием кнопки **Нет** (No).

6. Если же вы твердо решили выполнить операцию восстановления, нажмите кнопку **Да** (Yes), и процесс восстановления начнется. Средство восстановления системы (System Restore) выведет на экран целый ряд сообщений о том, какие операции оно выполняет: инициализируется, выполняет восстановление реестра (рис. 2.11), удаляет временные файлы и, наконец, перезагружает систему.

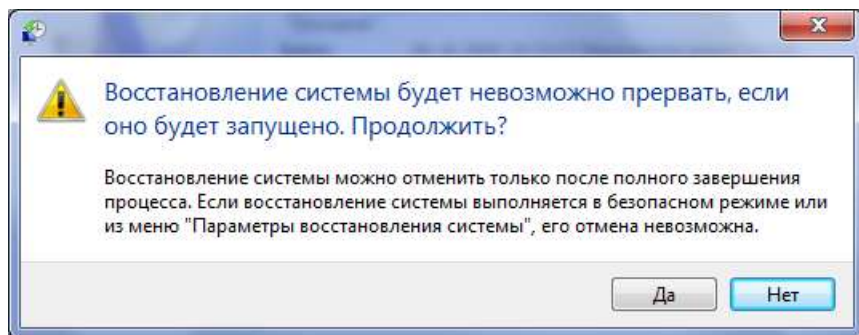


Рис. 2.10. Окно с предупреждением дает последнюю возможность отказаться от выполнения отката



Рис. 2.11. Обратите внимание, что в качестве одного из шагов средство восстановления системы выполняет восстановление реестра

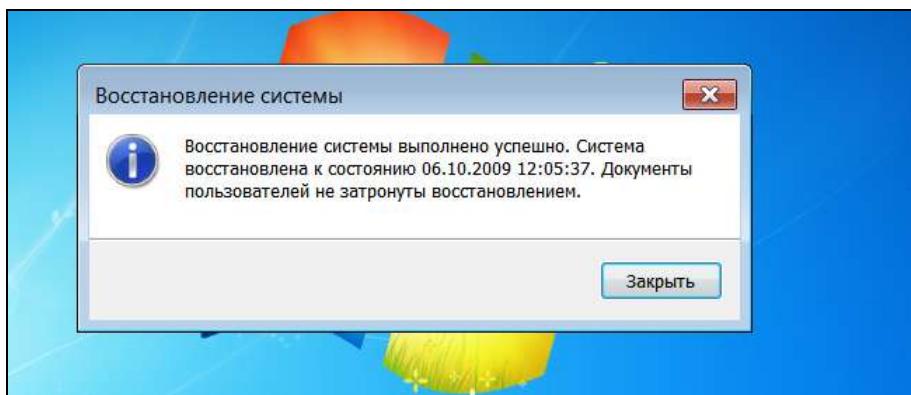


Рис. 2.12. Сообщение об успешном восстановлении системы к одному из предыдущих состояний

После перезагрузки (в случае успешного восстановления системы) вы увидите окно, показанное на рис. 2.12.

Кстати, если операция восстановления оказалась неудачной (бывает и так) или же вам просто не понравились ее результаты (например, несмотря на кажущийся успех, она не привела к устранению проблемы), то, как уже говорилось чуть ранее, эта операция обратима, за исключением тех случаев, когда вы запускали ее из безопасного режима загрузки Windows (Safe Mode) или из меню **Устранение неполадок компьютера** (System Recovery Options).

Отмена операции восстановления

Чтобы отменить операцию восстановления, запустите средство восстановления системы (System Restore) еще раз, и вы увидите окно, показанное на рис. 2.13. В этом окне вы можете как отменить только что выполненную операцию восстановления (эта опция предлагается по умолчанию), так и выбрать любую другую точку восстановления с помощью переключателя **Выбрать другую точку восстановления** (Choose a different Restore Point).

Если вы решили выбрать другую точку восстановления, вместо того, чтобы отменять только что выполненный откат, и воспользовались **Выбрать другую точку восстановления** (Choose a different Restore Point), на экране снова откроется диалоговое окно, предлагающее выбрать точку восстановления (рис. 2.14). Здесь вы снова получите возможность отменить только что выполненный откат — обратите внимание на точку отката с именем **Операция восстановления** (Restore Operation), имеющую тип **Отмена** (Undo), или же выбрать другую точку восстановления.

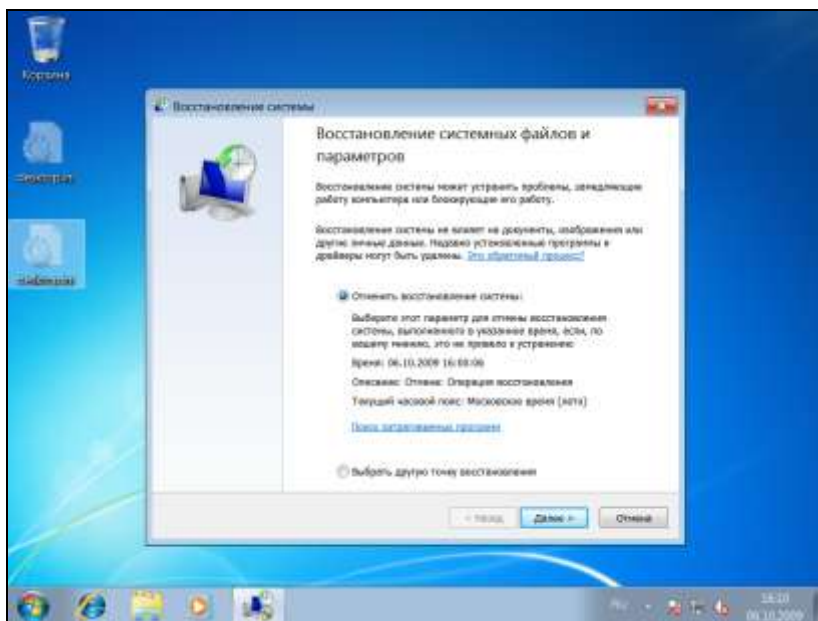


Рис. 2.13. В большинстве случаев, за исключением некоторых оговоренных, операция восстановления является обратной

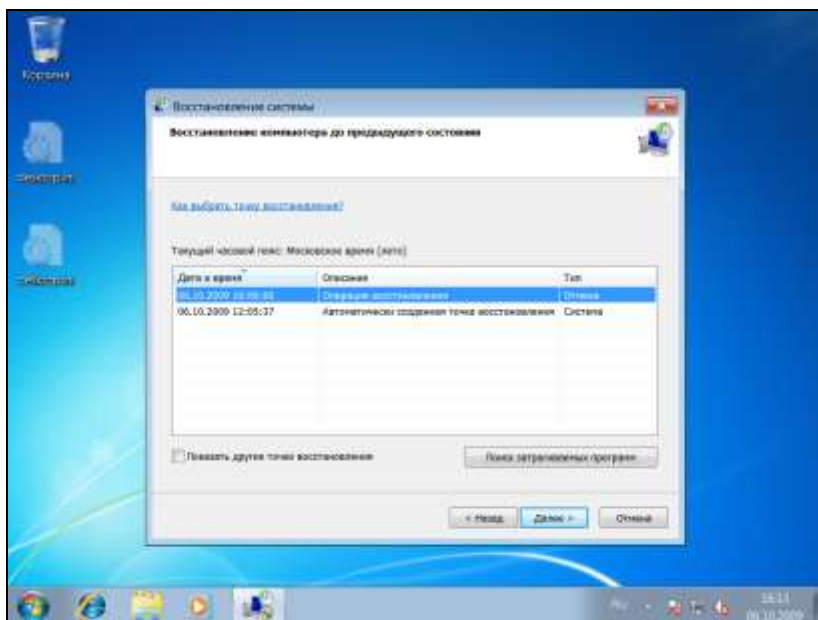


Рис. 2.14. Выбор точки восстановления для отмены только что выполненного отката

СОВЕТ

Не выполняйте восстановление параллельно с инсталляцией программного обеспечения — при этом могут быть повреждены начальные точки восстановления, созданные средством восстановления системы (System Restore) в момент ее активизации, а также последующие точки восстановления. Обратите внимание, что невозможно визуально определить, повреждена ли начальная точка восстановления.

ПРИМЕЧАНИЕ

Если у вас установлена система с двойной или тройной загрузкой, где кроме Windows Vista/7 установлены более ранние версии Windows — Windows XP или Windows Server 2003, то вы столкнетесь с проблемой несовместимости реализаций функции восстановления системы в Windows XP и Windows Vista/7. Результатом этого является затирание точек восстановления Windows Vista и Windows 7 после того, как вы загрузитесь и поработаете в Windows XP. Суть проблемы заключается в том, что Windows XP автоматически монтирует все диски, какие только сможет обнаружить в системе. В ходе этого процесса драйвер volsnap.sys из состава Windows XP не может распознать точки восстановления, созданные драйвером volsnap.sys более поздних версий — Windows Vista и Windows 7. Windows XP, таким образом, не имея возможности поддерживать целостность области теневого копирования, во избежание порчи нераспознанных точек восстановления их просто удаляет. Простейшим способом избежать этой проблемы является использование утилиты TweakUI (<http://download.microsoft.com>) в Windows XP. С помощью этой утилиты скройте от Windows XP тот раздел, на котором установлена более поздняя версия Windows — Windows Vista или Windows 7. Если Windows XP не сможет "видеть" раздела, то она и не сможет удалять точки восстановления. Кроме того, можно воспользоваться еще одним методом решения этой проблемы — с помощью реестра. Этот метод будет описан в *главе 4*. Наконец, если вы пользуетесь такими редакциями Windows Vista/7, как Professional, Enterprise и Ultimate, той же цели можно добиться и с помощью функции BitLocker Drive Encryption.

Восстановление предыдущих версий файлов

В начале этой главы уже говорилось о том, что, начиная с Windows Vista, средство восстановления системы (System Restore) базируется на теновом копировании томов (Volume Shadow Copy).

ПРИМЕЧАНИЕ

В данном случае под термином "том" мы будем понимать раздел (логический диск) жесткого диска.

Теневые снимки тома представляют собой исходные копии тома, "снятые" на момент выполнения операции создания точки восстановления. И именно на основе теневого копирования томов (оно будет подробно рассмотрено в разд. *Конфигурирование средства восстановления системы из командной строки*)

реализована очень удобная функция восстановления предыдущих версий файлов, появившаяся в Windows Vista и, безусловно, присутствующая в Windows 7. Чтобы воспользоваться этой функцией, достаточно щелкнуть мышью по диску, папке или файлу и из появившегося контекстного меню выбрать опцию **Восстановить прежнюю версию** (Restore previous versions), как показано на рис. 2.15.

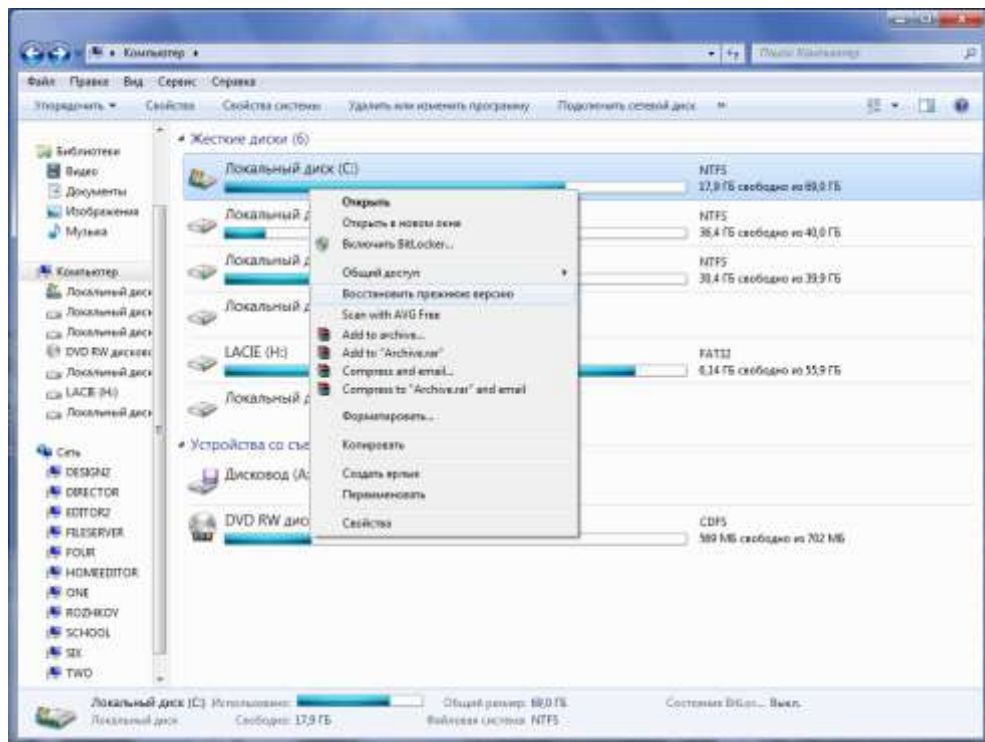


Рис. 2.15. Выбрав из контекстного меню команду **Восстановить прежнюю версию** (Restore previous versions), вы можете восстановить предыдущие версии ваших пользовательских данных

После выбора этой команды на экране откроется окно свойств диска, папки или конкретного файла, раскрытое на вкладке **Предыдущие версии** (Previous versions), как показано на рис. 2.16. В нем вы увидите список резервных копий ваших файлов, причем каждую из этих резервных копий можно в полном объеме восстановить, скопировать или открыть для просмотра. Обратите внимание — открыв одну из предыдущих версий, вы получите возможность их избирательного копирования (рис. 2.17).

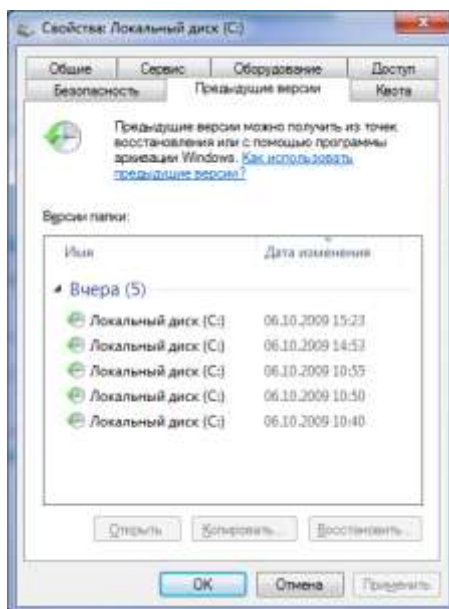


Рис. 2.16. Вкладка **Предыдущие версии** (Previous Versions) окна свойств папки моего пользовательского профиля

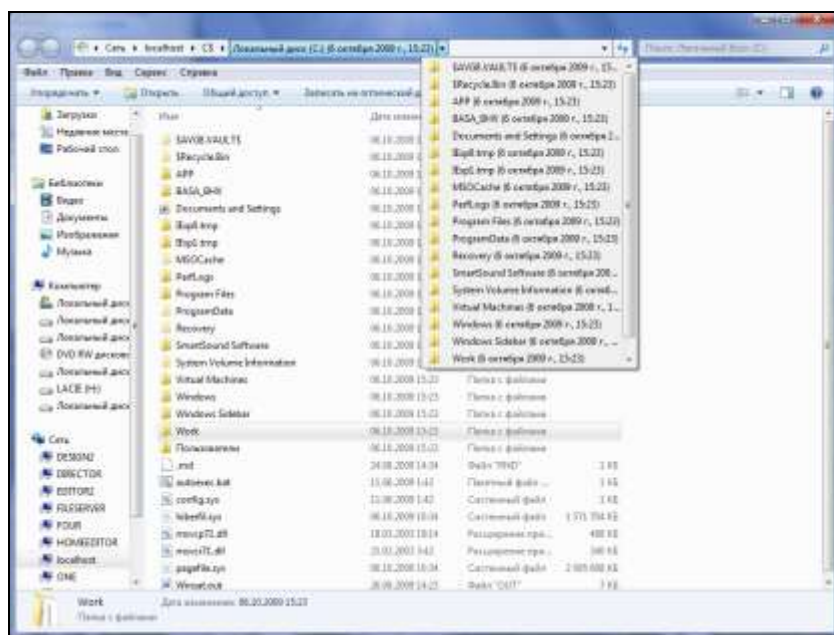


Рис. 2.17. Просмотр и избирательное копирование предыдущих версий ваших файлов

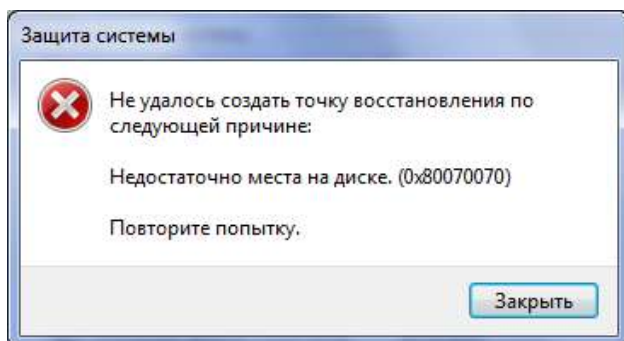


Рис. 2.18. Сообщение об ошибке создания точки восстановления при нехватке дискового пространства на одном из защищаемых томов

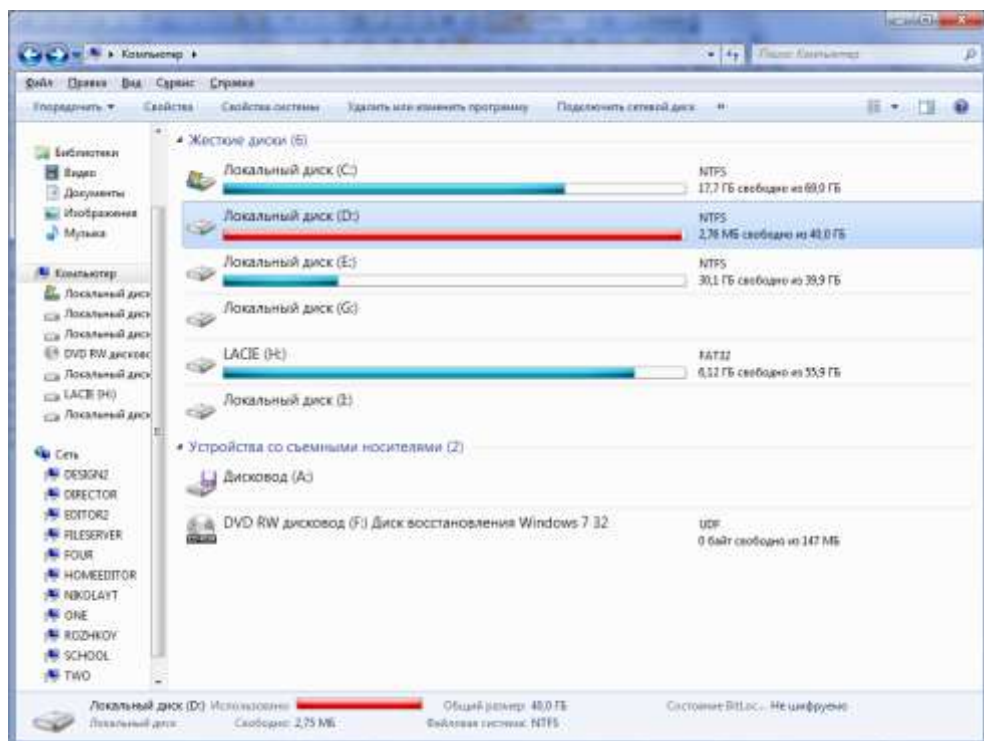


Рис. 2.19. А вот и причина, по которой точка восстановления не была создана — нехватка дискового пространства для сохранения теневой копии на одном из защищаемых дисков

Итак, как уже говорилось ранее, средство восстановления системы (System Restore) в Windows Vista и Windows 7 генерирует точку восстановления и наряду с этим сохраняет так называемую *теньевую копию* каждого из разделов (томов), для которых она активизирована.

ВНИМАНИЕ!

Если на одном из защищаемых томов объем свободного дискового пространства падает ниже 100 Мбайт, то точки восстановления не создаются (рис. 2.18). Обратите внимание — в данном случае причиной отказа в создании точки восстановления послужила нехватка дискового пространства на одном из защищаемых дисков (рис. 2.19). На диске **D:** доступно всего 93,6 Мбайт, и этого не хватает для создания теневой копии тома.

ПРИМЕЧАНИЕ

Чтобы все-таки создать точку восстановления, попробуйте вручную отключить функцию защиты системы (System Protection) для этого диска, и вы убедитесь, что после этого точка восстановления будет успешно создана. Теперь создайте резервную копию данных с диска, на котором не хватает доступного свободного пространства, затем освободите необходимый объем пространства и вновь активизируйте для него защиту. О том, как это делается, будет рассказано в разд. *Ручное конфигурирование средства восстановления системы*.

Ручное конфигурирование функции защиты системы

Чтобы вручную сконфигурировать средство восстановления системы (System Restore), выполните следующие действия:

1. Запустите утилиту **Система** (System) из Панели управления (Control Panel) и в окне **Свойства системы** (System Properties) выберите опцию **Защита системы** (System Protection). Откроется окно **Свойства системы** (System Properties), раскрытое на вкладке **Защита системы** (System Protection) (рис. 2.20).
2. В группе опций **Параметры защиты** (Protection Settings) выделите диск, для которого вы желаете сконфигурировать средство восстановления системы (System Restore).
3. Затем нажмите кнопку **Настроить** (Configure). На экране откроется окно параметров настройки функции защиты системы (System Protection) для выбранного вами диска (рис. 2.21), где и можно осуществить требуемые настройки.

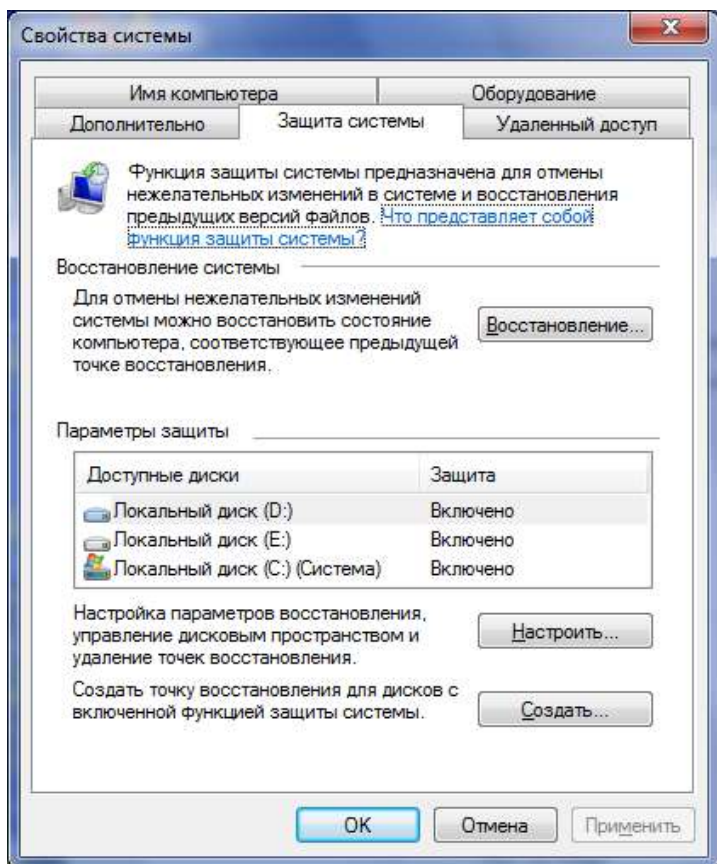


Рис. 2.20. Вкладка **Защита системы** (System Protection) окна **Свойства системы** (System Properties)

Обратите внимание на то, как изменилось это окно в Windows 7, — теперь вы имеете возможность не только активизировать или блокировать средство восстановления системы, но и выбрать режим его работы: можно сохранять и системные настройки, и предыдущие версии файлов или же только предыдущие версии файлов (теньевую копию тома). Выполняется это с помощью переключателей из группы опций **Параметры восстановления** (Restore Settings):

- если установлена опция **Восстановить параметры системы и предыдущие версии файлов** (Restore system settings and previous versions of files), то будут сохранены не только параметры системы, но и теньевая копия тома;

- в случае выбора второй опции — **Восстановить только предыдущие версии файлов** (Only restore previous versions of files), будет сохранена только теньевая копия тома;
- наконец, последняя опция — **Отключить защиту системы** (Turn off system protection) — позволяет отключить защиту системы для данного тома.

Далее, вы имеете возможность указать, какой максимальный объем свободного дискового пространства резервируется для средства восстановления системы. Делается это с помощью ползункового регулятора **Максимальное использование** (Max Usage).

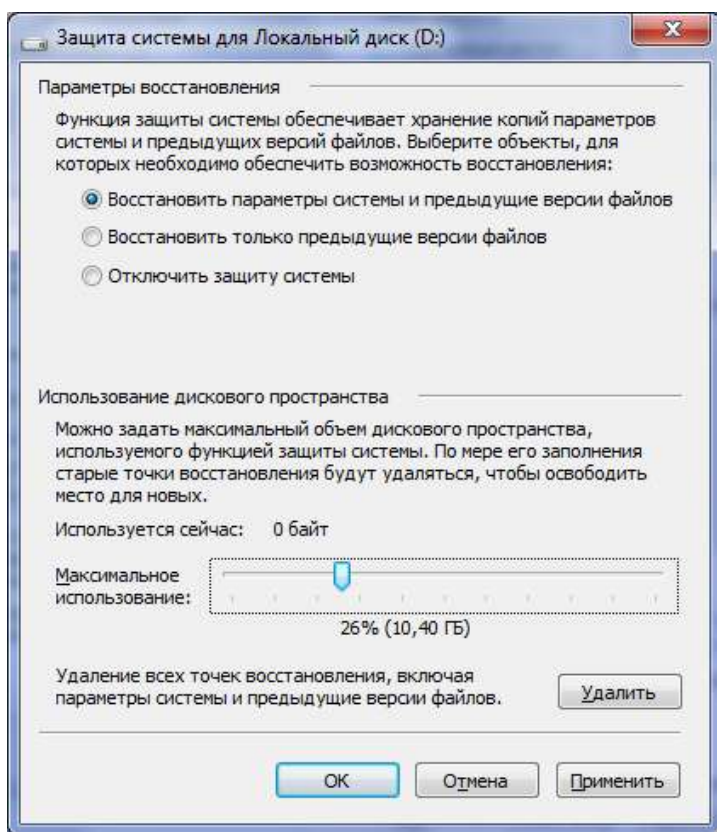


Рис. 2.21. Окно параметров настройки функции защиты системы для выбранного тома

Наконец, в этом окне вы имеете возможность удалить все точки восстановления. Для этого достаточно нажать кнопку **Удалить** (Delete). Система

выведет предупреждение, показанное на рис. 2.22. Если вы твердо уверены в необходимости выполняемого действия, нажмите кнопку **Продолжить** (Continue).

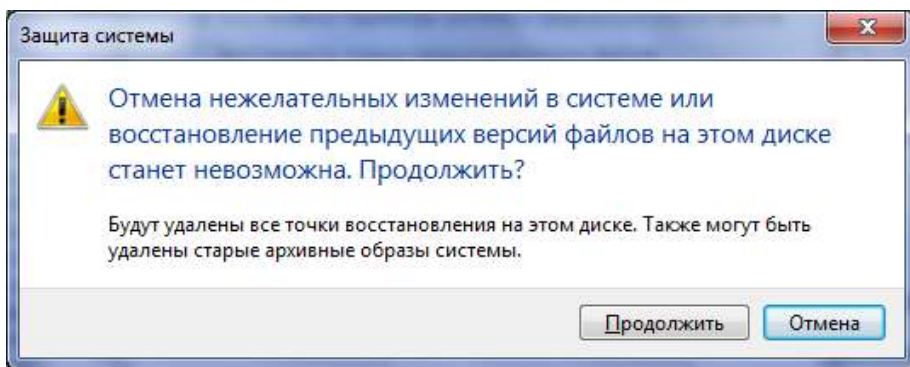


Рис. 2.22. Предупреждающее сообщение, выводимое при удалении точек восстановления

К вопросу об объеме свободного дискового пространства для средства восстановления системы

Обратите внимание, что средство восстановления системы (System Restore) в Windows XP требовало не менее 200 Мбайт свободного дискового пространства на разделе, где установлена операционная система. В Windows Vista и Windows 7 для этой же цели требуется уже не менее 300 Мбайт. Если объем доступного дискового пространства на этом разделе падает ниже критического уровня, то функция восстановления системы автоматически блокируется. Впоследствии, освободив требуемый объем дискового пространства, вы сможете активизировать средство восстановления системы (System Restore), однако все ваши точки восстановления будут потеряны, поскольку утилита не сможет отследить изменения и, следовательно, отменить их. Более того, если на момент инсталляции Windows 7 у вас остается меньше 300 Мбайт свободного дискового пространства на разделе, куда устанавливается операционная система, то после того, как вы освободите необходимое пространство, вам потребуется вручную активизировать средство восстановления системы (System Restore).

Далее напомним, что по умолчанию средство восстановления системы (System Restore) в Windows XP резервирует 12 процентов дискового пространства на жестких дисках объемом более 4 Гбайт или 400 Мбайт — на дисках меньшего объема. В Windows Vista средство восстановления системы по умолчанию

резервирует до 15 процентов от общего объема тома или не более 30 процентов свободного дискового пространства (в зависимости от того, какое из этих значений меньше). Что касается Windows 7, то если она установлена на диске, объем которого превышает 64 Гбайт, то по умолчанию она может резервировать за собой до 5 процентов свободного дискового пространства или не более 10 Гбайт (в зависимости от того, какое значение меньше). На жестких дисках объемом менее 64 Гбайт средство восстановления системы по умолчанию резервирует за собой не более 3 процентов дискового пространства. Эта информация будет вам полезна при ручном конфигурировании объема дискового пространства, отводимого для средства восстановления системы.

Кроме того, отметим, что в Windows Vista вас ожидал неприятный сюрприз — возможность ручного конфигурирования максимального объема дискового пространства, которое может быть использовано средством восстановления системы, отсутствовала. Если в Windows Vista вам требовалось изменить значения, заданные по умолчанию, необходимо было пользоваться утилитой командной строки `vssadmin.exe`, предназначенной для администрирования службы теневого копирования тома (Volume Shadow Copy Administrative Command-Line Tool). Как видите, в Windows 7 возможность конфигурирования через пользовательский интерфейс появилась вновь. Тем не менее, существует возможность конфигурирования службы теневого копирования тома и через командную строку, о чем будет рассказано в следующем разделе этой главы.

Конфигурирование средства восстановления системы из командной строки

В Windows 7 ограничить максимальный объем дискового пространства, которое может быть использовано средством восстановления системы, или изменить значение, заданное по умолчанию, возможно как через пользовательский интерфейс (см. предыдущий разд. *Ручное конфигурирование средства восстановления системы*), так и с помощью утилиты командной строки `vssadmin.exe`, предназначенной для администрирования службы теневого копирования тома (Volume Shadow Copy Administrative Command-Line Tool). Утилита эта называется *Сервис теневого копирования тома* (Volume Shadow Copy Service, VSS), поскольку она управляет не только средством восстановления системы (System Restore), но и дополнительными расширениями (в частности, функцией восстановления предыдущих копий).

Чтобы воспользоваться утилитой `vssadmin.exe`, необходимо запустить сеанс командной строки от имени пользователя с административными правами. О том, как это делается, было рассказано в *главе 1*.

Просмотреть список опций утилиты `vssadmin.exe` можно, выполнив следующую команду:

```
vssadmin /?
```

Чтобы проверить объем минимального пространства, требуемого службе теневого копирования тома, объем дискового пространства, выделенного этой службе, а также объем фактически использованного пространства, выполните следующую команду:

```
vssadmin List ShadowStorage
```

Вывод этой команды будет выглядеть примерно так, как показано на рис. 2.23.

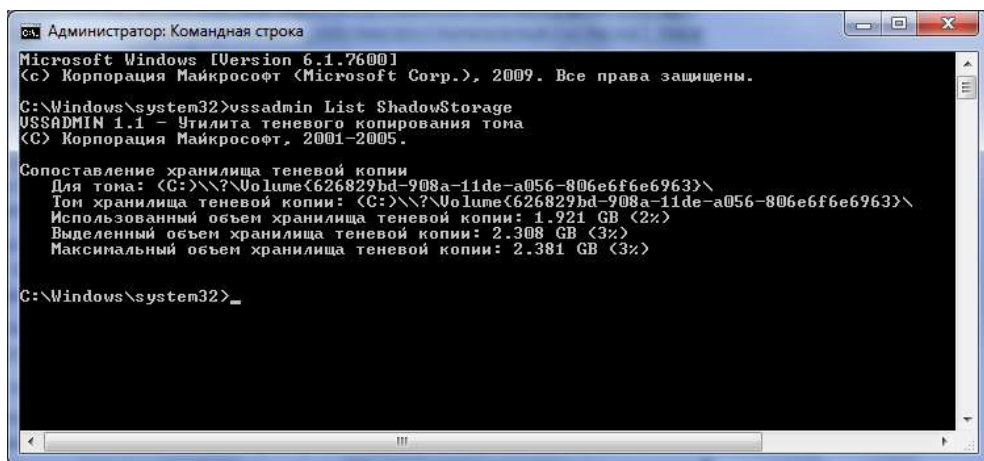


Рис. 2.23. Вывод команды `VSSadmin.exe` при просмотре параметров службы теневого копирования тома

Чтобы изменить объем свободного пространства, выделенного службе теневого копирования, а значит, и средству восстановления системы, использует следующая команда:

```
vssadmin Resize ShadowStorage /On=[drive]: /For=[drive]: /Maxsize=[size]
```

Например, чтобы ограничить объем свободного пространства, используемый службой VSS, на диске **C:** до 5 Гбайт, дайте команду:

```
vssadmin Resize ShadowStorage /On=C: /For=C: /MaxSize=5GB
```

Значение параметра `MaxSize` должно быть не менее 300 Мбайт, причем для его указания допускается использовать следующие суффиксы: **кБ** (Кбайт), **МБ** (Мбайт), **ГБ** (Гбайт) и т. д. (разумеется, при использовании этих суффиксов следует учитывать реальный объем свободного пространства, доступного на ваших жестких дисках). Если суффикс не указан, то система будет считать,

что значение `MaxSize` указано в байтах. Если вы не намереваетесь ограничивать объем свободного пространства, отведенный для использования службой теневого копирования (VSS) и средством восстановления системы (System Restore), просто опустите параметр `MaxSize`.

СОВЕТ

Прежде чем отключать средство восстановления системы (System Restore) или устанавливать ограничения на объем свободного пространства, которое позволено использовать службе теневого копирования VSS и средству восстановления системы, серьезно задумайтесь! Что для вас важнее: возможность быстрого восстановления системы или выигрыш по свободному дисковому пространству?

Центр архивации и восстановления

Официальным методом резервного копирования реестра Windows 7 является использование утилиты резервного копирования, встроенной в состав операционной системы. Средства архивации данных в Windows 7 обеспечивают поддержку различных видов носителей резервной копии, что позволяет выполнять резервное копирование на любое устройство хранения информации, поддерживаемое операционной системой. К числу таких устройств относятся любые гибкие или жесткие диски, магнитооптические накопители, CD/DVD и другие устройства.

ПРИМЕЧАНИЕ

Начиная с Microsoft Windows XP, операционные системы из семейства Windows NT начали использовать так называемые *моментальные снимки тома* (volume snapshots) — технологию, которая предоставляет исходную копию тома по состоянию на момент создания снимка. Снимок тома создается на момент инициации резервной копии. Затем данные резервируются, но не с исходного тома, а с его снимка. По мере работы содержимое исходного тома изменяется, а снимок тома остается постоянным. Это удобно, если пользователям нужен доступ к файлам во время процесса резервного копирования, поскольку существенно снижается время, затрачиваемое на резервирование. К тому же, программа резервного копирования может осуществлять резервирование тех файлов, которые остаются открытыми. В предыдущих версиях утилиты архивации данных (Backup), в том числе и в Windows 2000, те файлы, которые на момент резервного копирования были открыты, пропускаются.

Для запуска архивации файлов в Windows 7 в окне **Панель управления** (Control Panel) выберите опции **Система и безопасность** (System and Security) | **Архивация и восстановление** (Backup and Restore), и на экране откроется окно, показанное на рис. 2.24.

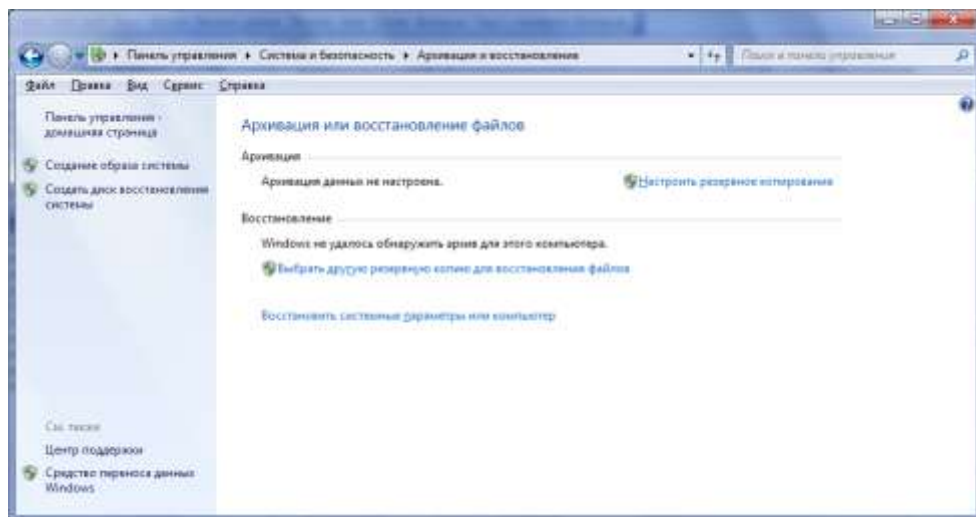


Рис. 2.24. Встроенная утилита для резервного копирования и восстановления данных в Windows 7

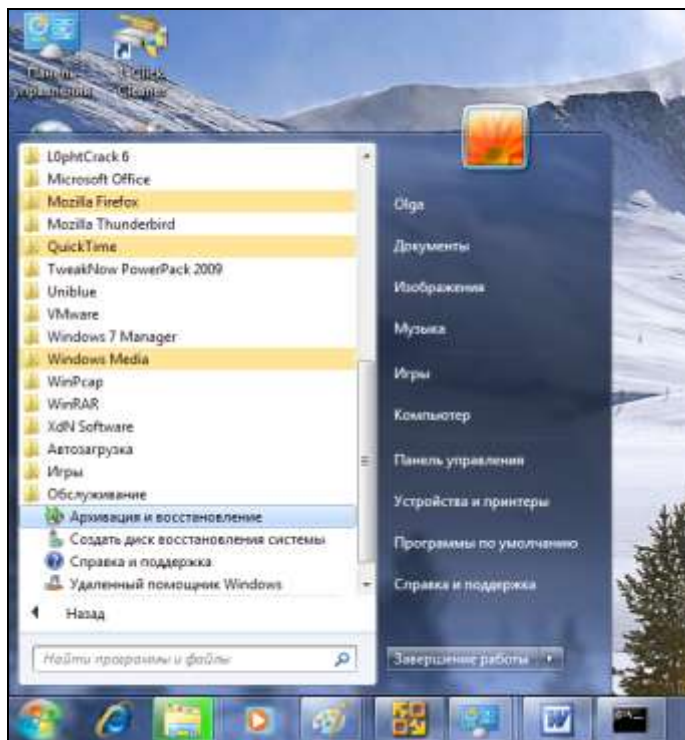


Рис. 2.25. Вызов встроенной программы резервного копирования через меню Пуск

Запустить утилиту **Архивация и восстановление** (Backup and Restore) можно и через меню **Пуск** (Start), выбрав из него команды **Все программы** (All programs) | **Обслуживание** (Maintenance) | **Архивация и восстановление** (Backup and Restore) (рис. 2.25). Впрочем, зачем без конца дергать мышью, выбирая все эти команды? Вместо этого вы можете просто ввести в поле **Найти программы и файлы** (Search programs and files), расположенное в нижней части меню (см. рис. 2.25), команду `sdclt.exe`, и добиться точно такого же результата. Как вариант, можно запустить сеанс работы с командной строкой и дать оттуда следующую команду:

```
%systemroot%\system32\control.exe /name Microsoft.BackupAndRestoreCenter
```

Наконец, выполнить ту же задачу можно и еще одним способом, универсальным для Windows XP/Vista/7. Для этого откройте окно Проводника (Explorer) или **Компьютер** (Computer), щелкните правой кнопкой мыши на диске, резервную копию которого необходимо создать, и в контекстном меню выберите команду **Свойства** (Properties) — откроется окно, снабженное вкладками. Перейдите на вкладку **Сервис** (Tools) (рис. 2.26).

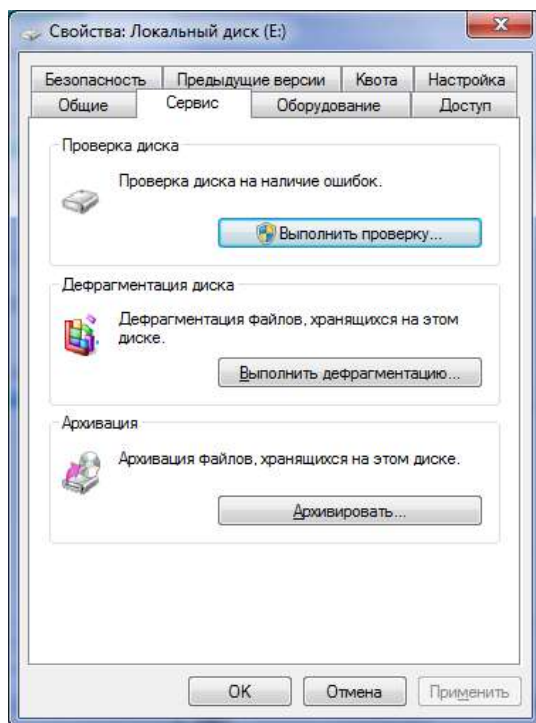


Рис. 2.26. Вкладка **Сервис** (Tools) в окне свойств диска — нажатие кнопки **Архивировать** (Back up now) представляет собой универсальный метод запуска программы архивации для Windows XP/Vista/7

Нажмите кнопку **Архивировать** (Back up now), расположенную в группе **Архивация** (Backup), и на экране откроется окно мастера резервного копирования, показанное на рис. 2.24.

О новых возможностях резервного копирования в Windows 7

Обратите внимание на новые возможности, появившиеся в Windows 7 и выгодно отличающие новое средство резервного копирования от имевшегося в Windows Vista. По отзывам многих авторитетных пользователей, Центр архивации и восстановления (Backup and Restore Center) в Windows Vista был сделан настолько неконфигурируемым и неуклюжим, что многие из них либо искали программное обеспечение от сторонних поставщиков, либо шли на ухищрения, пытаясь установить в ней средство резервного копирования из состава Windows XP. Подумать только!

Впрочем, в Windows 7 все изменилось в лучшую сторону. Давайте изучим эти новые возможности чуть подробнее.

В первую очередь, ваше внимание должны привлечь опции, расположенные в левой части окна средства **Архивация и восстановление** (Backup and Restore): это опции **Создание образа системы** (Create a system image) и **Создать диск восстановления системы** (Create a system repair disc) — см. рис. 2.24.

Для начала давайте создадим диск восстановления системы — в сущности, это одна из первоочередных задач, которые необходимо выполнить сразу же после установки Windows 7 (или сразу же после того, как вы начали работать на компьютере с предустановленной версией этой операционной системы).

Создание диска аварийного восстановления системы

Сначала зададимся вопросом: что же представляет собой диск аварийного восстановления системы? Как логично будет предположить, этот диск должен применяться в том случае, когда система Windows 7 по той или иной причине отказывается загружаться (причиной может быть и повреждение системного реестра). С помощью такого диска вы сможете загрузить компьютер и получить доступ к набору диагностических и восстановительных утилит среды восстановления Windows 7 (WinRE, Windows Recovery Environment): **Восстановление запуска** (Startup Repair), **Восстановление системы** (System Restore), средствам восстановления системы из архива и прочим, о чем будет подробно рассказано в разд. *Выполнение аварийного восстановления системы*. Процедура эта очень проста, и занимает совсем непродолжи-

тельное время — так, у меня в только что установленной системе Windows 7 Ultimate на создание диска аварийного восстановления потребовалось менее 5 минут.

ВНИМАНИЕ!

Для создания диска аварийного восстановления ваша система должна быть оснащена пишущим приводом CD или DVD. Устройства USB для использования с этой опцией, к сожалению, не годятся. Кроме того, вам потребуется "болванка" компакт-диска достаточной емкости (впрочем, у меня в абсолютно новой, только что установленной системе объем файлов, записанных на этот диск, оказался равным примерно 142 Мбайт). Разумеется, если у вас под рукой не окажется "болванки" CD, то подойдет и DVD.

Итак, чтобы создать диск аварийного восстановления Windows 7, проделайте следующие шаги:

1. В окне **Архивация или восстановление файлов** (Backup and Restore your files) щелкните по ссылке **Создать диск восстановления системы** (Create a system repair disc). В раскрывшемся окне **Создать диск восстановления системы** (Create a system repair disc), показанном на рис. 2.27, из раскрывающегося списка **Диск:** (Drive:) выберите подходящий пишущий привод CD или DVD (если их у вас несколько). Имейте в виду — диск в приводе должен быть пустым. Если диск CD или DVD у вас перезаписываемый, и на нем уже содержится некая информация, то перед тем, как начинать процедуру, этот диск необходимо очистить. Для этого вставьте диск в привод, щелкните по нему правой кнопкой мыши и из контекстного меню выберите команду **Затереть** (Erase).
2. Выбрав привод и вставив в него диск, щелкните мышью по кнопке **Создать диск** (Create disc). Появится индикатор процесса (progress bar), отображающий степень завершенности процесса создания диска аварийного восстановления (рис. 2.28).

ПРИМЕЧАНИЕ

Обратите внимание, что для осуществления этой процедуры вам не требуется иметь в системе никакого специализированного стороннего программного обеспечения для прожига CD и DVD.

3. Когда процедура завершится, на экране откроется окно, показанное на рис. 2.29.
4. Нажмите кнопку **ОК** в окне, отображенном после завершения создания диска аварийного восстановления (см. рис. 2.29). Затем пометьте этот диск как диск аварийного восстановления Windows 7 и положите его в надежное место — теперь, в случае возникновения неполадок с загруз-

кой операционной системы Windows 7, вы сможете загрузить компьютер с этого диска и выполнить работы по восстановлению поврежденной системы.

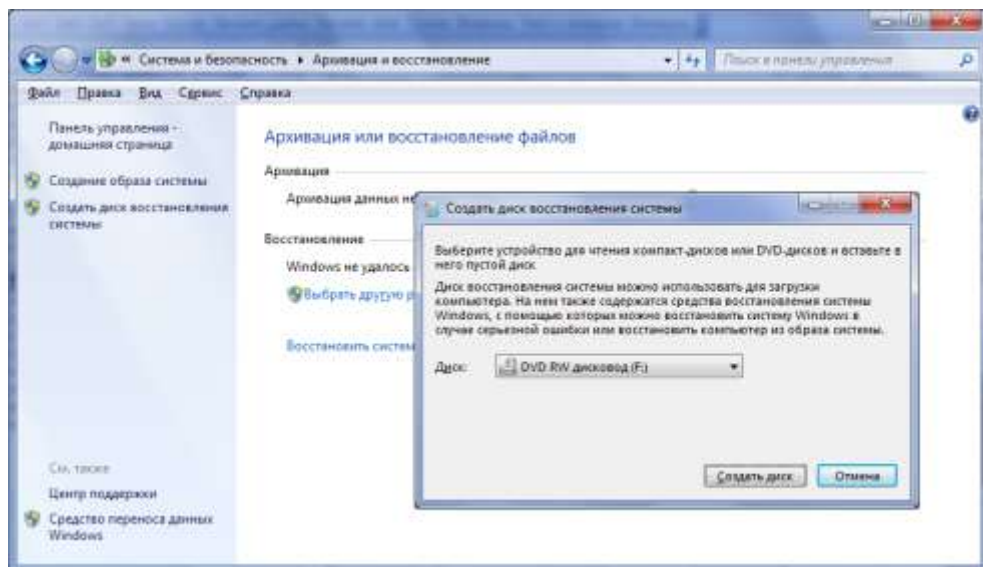


Рис. 2.27. Первый шаг процедуры создания диска аварийного восстановления Windows 7 — выбор пишущего привода CD или DVD

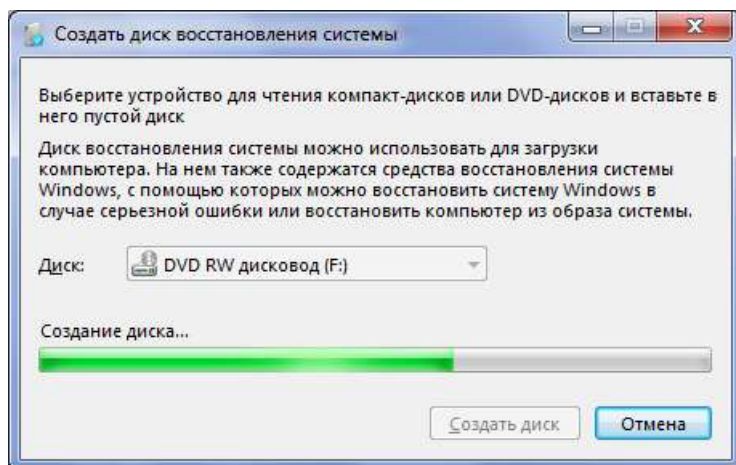


Рис. 2.28. Процедура создания диска восстановления системы началась

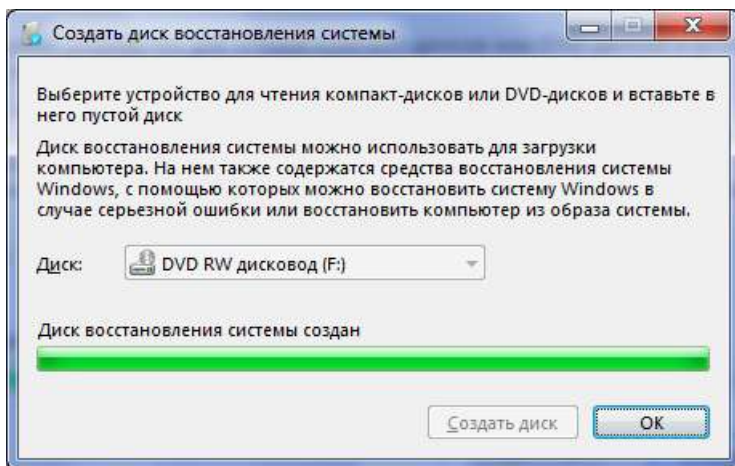


Рис. 2.29. Процесс создания диска аварийного восстановления Windows 7 успешно завершен

Создание образа системы

Windows 7 предоставляет опцию создания образа системы (system image), с помощью которой вы можете создать "моментальный снимок" вашего раздела, на который установлена сама Windows 7 и все программы и файлы, присутствующие на нем.

ПРИМЕЧАНИЕ

Эта функциональная возможность аналогична предоставляемой утилитами резервного копирования от сторонних разработчиков (например, Acronis True Image), предназначенными для выполнения резервного копирования содержимого вашего компьютера с целью последующего восстановления в случае катастрофических сбоев. Преимущество данного встроенного средства состоит в том, что оно дает возможность обойтись без полной переустановки Windows 7, если система окажется незагружаемой, и никакие из средств восстановления не помогут исправить проблему.

Чтобы создать образ системы, действуйте следующим образом:

1. В окне **Архивация или восстановление файлов** (Backup and Restore your files) щелкните мышью по ссылке **Создание образа системы** (Create a system image). На экране появится окно, показанное на рис. 2.30, в котором система предложит вам выбрать местоположение для создаваемого образа.

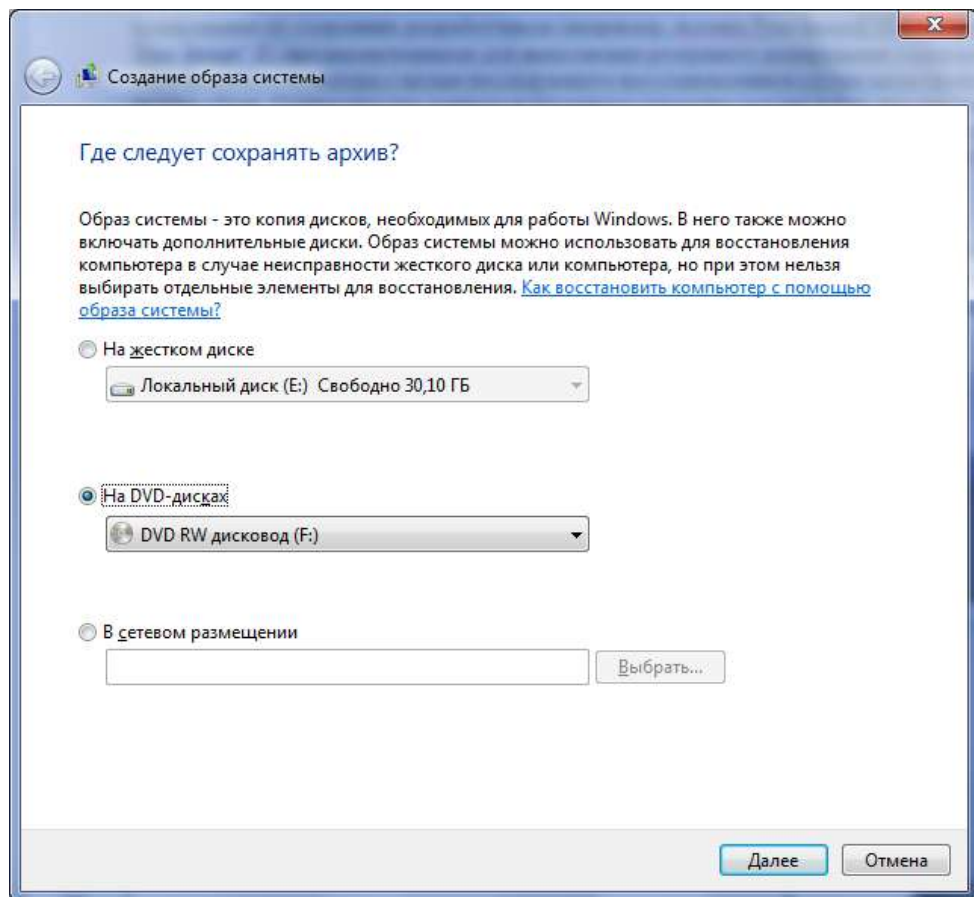


Рис. 2.30. Выбор местоположения для создаваемого образа

Для сохранения образа вам будут доступны следующие три опции:

- на другом разделе жесткого диска (On a hard disk) — лучше всего выбрать для этой цели другой жесткий диск, поскольку в случае аварийного отказа жесткого диска вы можете потерять и резервную копию;
 - на нескольких носителях DVD (On one or more DVDs) — количество носителей DVD (носители CD для этой цели не подходят вследствие недостаточной емкости), которое может вам потребоваться, зависит от размера раздела, который вы собираетесь резервировать;
 - на одном из сетевых дисков (On a network location).
2. Кроме основного раздела Windows 7, вы можете включить в создаваемый образ и другие разделы на жестких дисках вашей системы. Выберите

нужные тома и нажмите кнопку **Архивировать** (Start backup). Начнется подготовка процесса резервного копирования, а после этого, если вы выбрали носители DVD, система предложит вам вставить в привод пустой носитель, объем которого превышает 1 Гбайт (рис. 2.31).

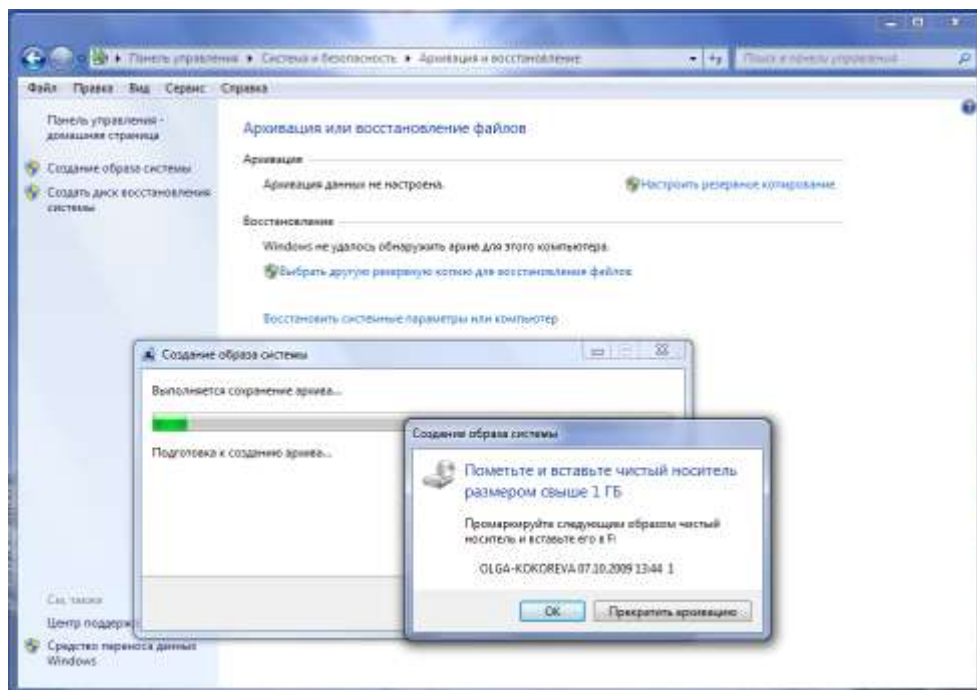


Рис. 2.31. Вставьте носитель, емкость которого превышает 1 Гбайт, и нажмите кнопку **ОК**, чтобы начать процесс копирования

3. Теперь вам останется только дождаться конца процедуры резервного копирования (он будет зависеть от объема копируемой информации). В случае, если вы выберете создание образа на носителях DVD, система несколько раз предложит вам вставить в привод следующий пустой носитель (см. рис. 2.31).

После завершения процесса копирования вам будет предложено создать диск восстановления системы, если вы не сделали этого ранее (см. разд. *Создание диска аварийного восстановления*).

4. Теперь вам останется только пометить все созданные диски и вместе с диском аварийного восстановления положить их на хранение в надежное место (например, в сейф).

Ограничения процедуры создания образа системы

Если описанная в предыдущем разделе процедура завершилась успехом, можете считать, что вы "натянули страховочную сетку" и готовы встретить неприятности во всеоружии.

Тем не менее, стоит отметить, что и в этом случае не все и не всегда пройдет гладко. Процедура создания образа системы имеет свои ограничения, о которых следует упомянуть хотя бы вкратце:

- ❑ первое, и главное — к сожалению, возможность создания образа системы включена только в Windows 7 Professional, Windows 7 Ultimate и Windows 7 Enterprise, а пользователям других вариантов поставки Windows 7, если они желают обладать такими же возможностями, придется присмотреться к утилитам сторонних разработчиков (например, к уже упоминавшемуся ранее в этой главе продукту Acronis True Image);
- ❑ неприятная неожиданность ожидает и любителей мультизагрузочных систем. Дело в том, что средство создания образа системы не поддерживает файловую систему FAT. А теперь представьте себе такую ситуацию, когда кроме систем из семейства Windows вы хотите установить на своем компьютере, например, Linux. В целях совместимости вы создаете на жестком диске первый раздел небольшого размера, помечаете его как активный и форматируете его для использования файловой системы FAT32. Затем вы производите установку операционных систем, например, в следующем порядке: Windows XP, Windows Vista, Windows 7, Linux¹. Установка Windows Vista и Windows 7 проходит нормально, но при этом файлы, необходимые для загрузки системы²: загрузочный менеджер (Bootmgr) и база данных BCD, представляющая собой улей реестра, попадут на раздел C:, отформатированный для использования файловой системы FAT32. Ваша мультизагрузочная конфигурация окажется вполне рабочей, и все операционные системы будут загружаться нормально. Но вот в процессе работы с Windows 7 вы наткнетесь на обещанную ранее неприятную неожиданность, а именно — вам не удастся создать архивный образ системы (рис. 2.32). Почему это происходит? А дело в том, что программа создания образа системы работает только с томами NTFS! Так что если вы желаете иметь возможность полной архивации всех своих данных и не хотите отказываться от мультизагрузочной конфигурации, то и в этом случае вам придется искать стороннюю утилиту резервного копирования, предлагающую аналогичные возможности.

¹ При этом для загрузки всех ОС Windows будет использоваться загрузчик Linux GRUB.

² Процесс нормальной загрузки Windows 7 будет подробно рассматриваться в главе 7.

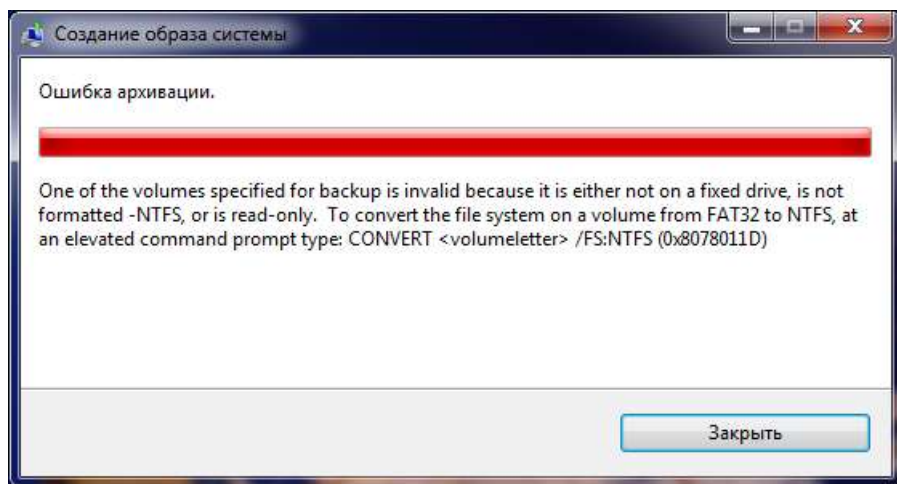


Рис. 2.32. Ошибка создания образа системы из-за того, что один из дисков отформатирован под FAT32

Настройка и выполнение резервного копирования

Наконец, в Windows 7 существует и возможность настроить и регулярно выполнять резервное копирование вашей пользовательской информации. Обратите внимание, что при первом запуске средства архивации файлов вам предлагается выполнить настройку автоматической архивации файлов. В целом, этот процесс очень хорошо описан в справочной системе Windows 7, поэтому останавливаться на нем во всех подробностях мы не будем.

Выполнение аварийного восстановления системы

Как уже говорилось, Windows 7 реализует улучшенную среду восстановления Windows (Windows Recovery Environment, WinRE) — набор средств, позволяющих ускорить и упростить диагностику системы и ее восстановление после серьезных сбоев, в том числе мешающих успешной загрузке (рис. 2.33).

Как уже говорилось в *главе 1*, WinRE позволяет восстановить, в том числе, и поврежденный реестр. WinRE замещает собой консоль восстановления (Recovery Console), имевшуюся в Windows 2000/XP. В Windows 7 ее можно запустить с установочного дистрибутивного DVD-диска, с диска аварийного восстановления системы, а можно и установить на локальном жестком диске. В случае установки на жестком диске, доступ к WinRE можно получить по нажатию клавиши <F8> в процессе загрузки системы.

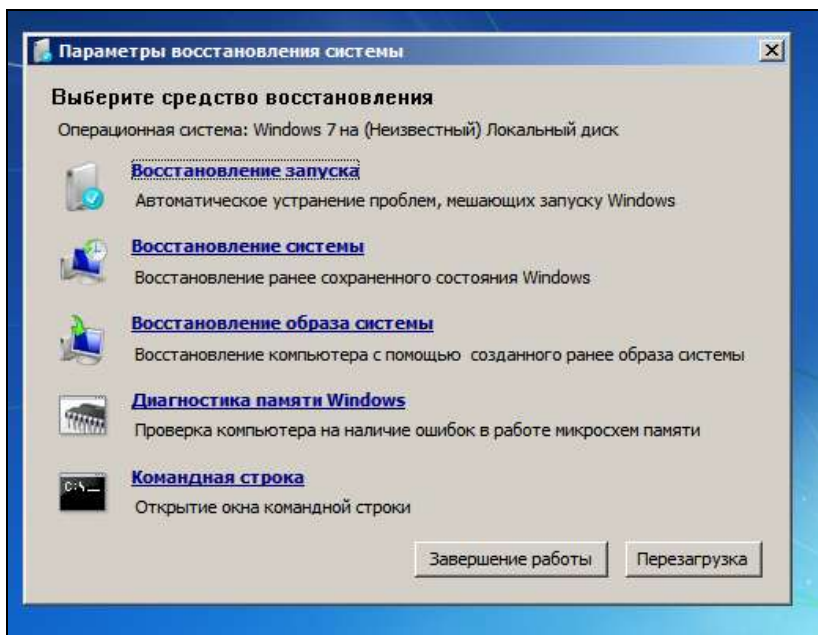


Рис. 2.33. Улучшенная среда восстановления Windows 7 — WinRE

Среда восстановления Windows предоставляет следующие опции:

- ❑ **Восстановление запуска** (Startup Repair) — автоматический поиск и исправление ошибок в загрузочной конфигурации Windows 7, включая поврежденную базу данных BCD. Более подробно об этом будет рассказано в *главе 11*;
- ❑ **Восстановление системы** (System Restore) — эта опция позволяет воспользоваться сервисом теневого копирования тома, чтобы вернуть систему в состояние, в котором она работала стабильно, используя одну из точек восстановления;
- ❑ **Восстановление образа системы** (System Image Recovery) — данная опция позволяет выполнить полное восстановление системы на основе ранее созданного образа (к сожалению, данная опция доступна только в Windows 7 Professional, Enterprise и Ultimate);
- ❑ **Средство диагностики памяти Windows** (Windows Memory Diagnostic Tool) — анализ памяти Windows на предмет выявления аппаратных неполадок;
- ❑ **Командная строка** (Command Prompt) — предоставляет интерфейс командной строки, такой же, как и существовавший в консоли восстановления (Recovery Console) в Windows XP, но с меньшим количеством ограничений.

Ручное резервное копирование и восстановление реестра Windows 7

Как уже говорилось в *главе 1*, большинство файлов ульев реестра Windows 7 хранится в каталоге %SystemRoot%\System32\Config. Чтобы выполнить ручное резервное копирование реестра Windows 7, все содержимое этого каталога, вместе со всеми вложенными папками, копируется на другое устройство (например, перезаписываемый компакт-диск или портативный жесткий диск).

Процедура восстановления реестра в случае применения этого метода резервного копирования требует загрузки компьютера под управлением другой операционной системы. После загрузки компьютера файлы резервной копии следует скопировать обратно в папку %SystemRoot%\System32\Config.

Экспорт и импорт файлов реестра

Редактор реестра (Regedit.exe), который более подробно будет рассматриваться в *главе 3*, позволяет экспортировать весь реестр целиком или отдельные его ключи. Экспорт может производиться на любое устройство, имеющееся в локальной системе.

СОВЕТ

Экспорт файлов реестра очень удобно выполнять в каталог, созданный специально для этой цели. Он может располагаться на сетевом диске и иметь индивидуальные подкаталоги, назначенные каждому из пользователей для экспорта файлов реестра. Если этот каталог включить в список каталогов, подлежащих регулярному резервному копированию, то и вы, и все ваши пользователи получите дополнительные гарантии надежности.

Чтобы выполнить экспорт реестра, сделайте следующее:

1. Вызовите Редактор реестра Regedit.exe и выделите значок **Компьютер** (Computer) — для экспорта всего реестра целиком — или конкретный ключ, который требуется экспортировать.
2. Выберите команду **Экспорт** (Export Registry File) в меню **Файл** (File).
3. В открывшемся диалоговом окне **Экспорт файла реестра** (Export Registry File) (рис. 2.34) выберите папку для экспорта и укажите имя файла, в который будет экспортирован реестр или его часть.

Экспортированный файл реестра представляет собой обычный текст в формате ASCII, который можно читать и редактировать при помощи любого текстового редактора.

Экспорт всего реестра или отдельных его ключей является простейшим способом резервного копирования перед выполнением каких бы то ни было операций, способных внести изменения в содержимое реестра. Чтобы аннулировать некорректные изменения, внесенные в реестр, импортируйте в его состав предварительно экспортированный файл.

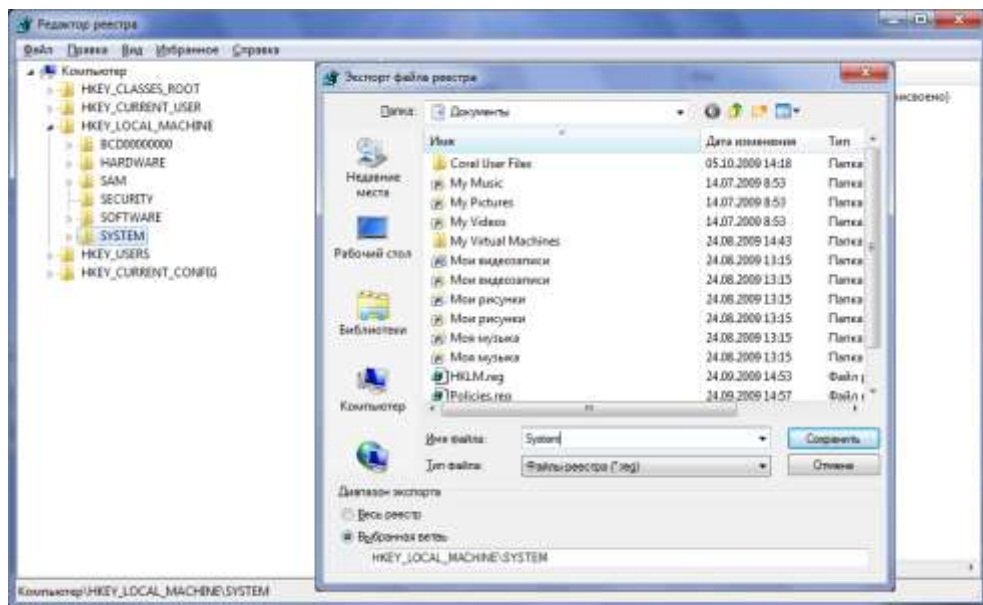


Рис. 2.34. Диалоговое окно **Экспорт файла реестра**.

Процесс экспорта очень похож на обычный процесс сохранения файла

Чтобы восстановить ключи реестра с помощью Редактора реестра (Regedit.exe), выберите в меню **Файл** (File) команду **Импорт** (Import Registry File). В диалоговом окне **Импорт файла реестра** (Import Registry File) (рис. 2.35) следует указать файл, который требуется импортировать.

СОВЕТ

Когда вы хорошо ознакомитесь с реестром, то сможете экспериментировать со своей системой или решать некоторые проблемы путем редактирования экспортированного файла реестра перед его импортом в систему. Однако до того как вносить такие изменения, рекомендуется предварительно сделать резервную копию этого файла, чтобы подстраховаться на случай ошибок.

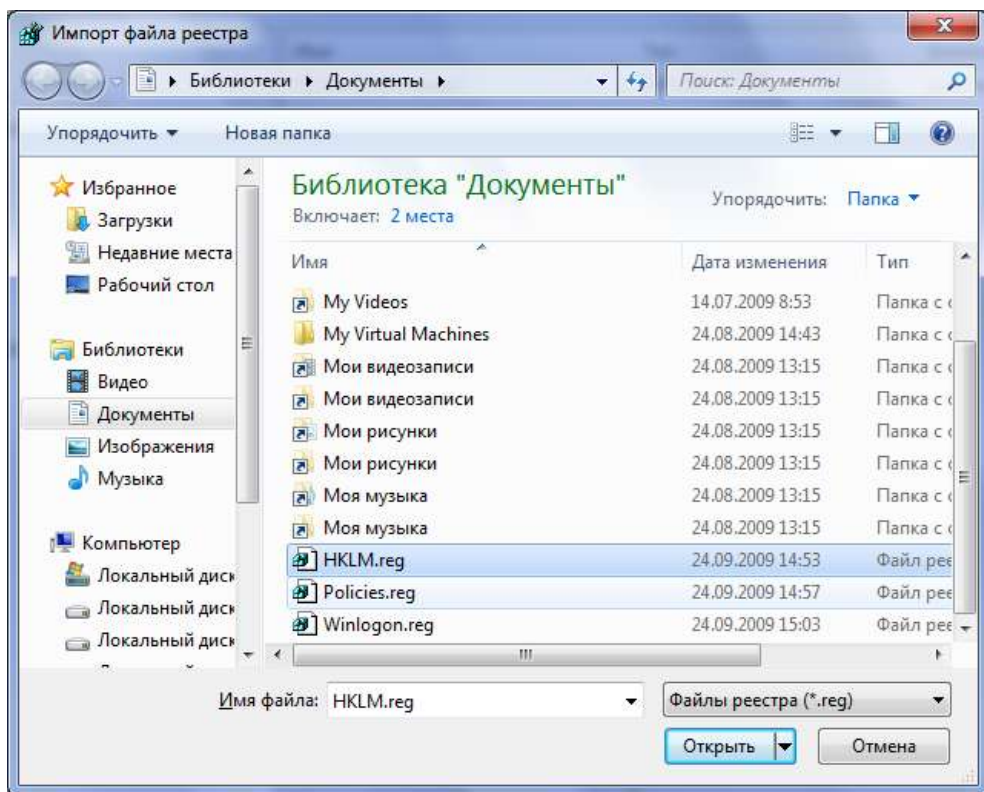


Рис. 2.35. Импорт файла реестра

Приведем ряд рекомендаций по работе с функциями импорта и экспорта реестра.

- ❑ Если функции импорта и экспорта используются для резервного копирования реестра, то простого импорта реестра в файл на локальном жестком диске недостаточно для полной уверенности в том, что в случае неполадок поврежденный реестр будет восстановлен. Скопируйте экспортированные файлы реестра на съемный носитель или сетевой диск.
- ❑ Перед тем как завершить операцию экспорта, убедитесь в том, что вы экспортируете нужный диапазон ключей. Если установлен переключатель **Весь реестр** (All), то будет экспортирован весь реестр. При установленном переключателе **Выбранная ветвь** (Selected branch) будет экспортирован ключ, имя которого указано в расположенном ниже переключателя поле.
- ❑ Соблюдайте осторожность, работая с экспортированными файлами реестра. Не пытайтесь импортировать несовместимые файлы реестра (например,

не следует импортировать в реестр Windows 7 файлы реестра, экспортированные из Windows 2000/XP/Vista, и обратно). Скорее всего, в процессе импорта произойдет ошибка, и если процедура импорта до появления ошибки успеет записать в реестр некорректные параметры (а это произойдет в большинстве случаев), то нормально работать после этого вы сможете только до первой перезагрузки.

- ❑ Избегайте выполнять двойной щелчок мышью, указывая при этом на экспортированный файл реестра, о происхождении которого нельзя сказать ничего определенного. По умолчанию файлы реестра при экспорте получают расширение `reg`, которое ассоциировано с Редактором реестра (`Regedit.exe`). Если такие действия проделать по отношению к несовместимому файлу реестра, экспортированному из другой операционной системы, то его импорт начнется быстрее, чем вы успеете осознать свою ошибку, и результат будет плачевным.

ВНИМАНИЕ!

Будьте осторожны с REG-файлами! Дистрибутивы некоторых приложений включают такие файлы и используют их при инсталляции для установки необходимых параметров реестра. Не пренебрегайте мерами предосторожности! Если вы выполните двойной щелчок мышью, указав на файл с расширением `reg`, программа `Regedit.exe` прочтет этот файл и вставит его содержимое в реестр. Если в реестре уже существовали такие же ключи, как в REG-файле, то они будут замещены новыми ключами из этого файла. Прежде чем переносить содержимое REG-файла в реестр, просмотрите его, например, с помощью Блокнота (`Notepad`). В этом случае вы хотя бы будете знать, что добавили в свой реестр.

Резервное копирование реестра с помощью утилит командной строки

Утилита `Reg.exe`, которая ранее поставлялась в составе программного продукта `Resource Kit`, начиная с Windows XP входит в комплект поставки операционной системы. Она позволяет добавлять, редактировать, удалять и искать ключи и значимые элементы реестра, производить их резервное копирование и восстановление, а также выполнять над ними другие операции. Утилита `Reg.exe` может использоваться из командной строки или применяться в командном файле. Она позволяет выполнять операции над реестрами как локального, так и удаленных компьютеров. Одним из ее применений является резервное копированию ключей и ульев реестра. Однако

этот материал для данной главы несколько сложноват, и поэтому мы отложим его рассмотрение до следующей главы, где эта тема будет описана подробно и всесторонне.

Заключение

Открывая реестр для внесения модификаций, следует иметь в виду возможность наступления такой ситуации, когда вы не сможете нормально загрузить операционную систему из-за ошибки в реестре. Для таких случаев нужно постоянно иметь в запасе свежую резервную копию реестра, в надежности и работоспособности которой вы уверены. Рассмотренные в этой главе вопросы должны показать, как следует выполнять резервное копирование реестра. Помимо этого, приведены необходимые инструкции на случай возникновения критических ситуаций.

Глава 3



Методы редактирования реестра Windows 7

Если вам все равно, где вы находитесь, значит, вы не заблудились.

Правило Руна

Предупреждения о том, что неумелое редактирование реестра может привести к необходимости переустановки операционной системы, встречаются в официальной документации Microsoft постоянно. Вероятно, разработчики являются большими поклонниками законов Мэрфи и прекрасно знают, что даже если ваше объяснение настолько ясно, что исключает всякое ложное толкование, все равно найдется человек, который поймет вас неправильно. Тем не менее, утилиты, предназначенные для редактирования реестра, имеются. Более того, они даже устанавливаются по умолчанию во всех операционных системах из семейства Windows. Не является исключением из этого правила и Windows 7, в комплект поставки которой входят целых три встроенных утилиты для работы с реестром:

- ❑ традиционный Редактор реестра (Registry Editor) с графическим пользовательским интерфейсом (Regedit.exe);
- ❑ утилита командной строки Reg.exe, поддерживающая большинство возможностей программы Regedit.exe, но, наряду с этим, предоставляющая ряд возможностей, которые в утилите Regedit.exe отсутствуют;

ПРИМЕЧАНИЕ

До выпуска Windows XP эта утилита поставлялась в комплекте программных продуктов Resource Kit, но, начиная с Windows XP, входит в состав самой операционной системы.

- ❑ утилита командной строки Regini.exe, позволяющая редактировать права доступа пользователей к отдельным ключам реестра.

Использование Редактора реестра *Regedit.exe*

В составе ранних версий операционных систем из семейства Windows NT (вплоть до Windows 2000) фактически имелось два редактора реестра. Традиционная программа редактирования реестра Windows NT носила название Regedt32.exe. Более новая программа, Regedit.exe, была первоначально написана для Windows 95. Она обладает многими из возможностей Regedt32.exe и снабжена интерфейсом Проводника (Explorer). Версия Regedit.exe, которая имеется в составе Windows Vista/7, очень похожа на аналогичные приложения из Windows NT/2000/XP.

ПРИМЕЧАНИЕ

Начиная с Windows XP, все задачи, относящиеся к администрированию и редактированию реестра, решаются с помощью одной утилиты — Regedit.exe, которая соединила свои самые сильные свойства с теми функциональными возможностями, которыми раньше обладала лишь программа Regedt32.exe. Как и в Windows XP/Vista, в Windows 7 в каталоге %SystemRoot%\System32 присутствует небольшая (размером около 9 Кбайт) программа Regedt32.exe. Но, если пользователь дает из командной строки команду regedt32, эта программа не делает ничего, а лишь вызывает редактор реестра Regedit.exe. Кроме того, начиная с Windows XP, в каждой из следующих версий Regedit.exe добавляются некоторые новые возможности — например, по импорту и экспорту, по редактированию данных различных типов и т. д. Однако в программе Regedit.exe отсутствует одна из наиболее полезных возможностей, имевшихся в программе Regedt32.exe, — режим доступа *только для чтения* (read-only).

Все версии программ редактирования реестра устанавливаются автоматически в процессе установки операционной системы. Однако ни один из редакторов реестра не попадает в меню **Пуск** (Start), и ни для одного из них не создается ярлык на рабочем столе. Впрочем, это и понятно. Редактор реестра не является "услужливой программой, делающей дополнительные шаги, чтобы облегчить жизнь пользователя"¹ (несмотря на то, что в Windows 7 некоторые шаги в этом направлении все же были предприняты). Справедливо как раз обратное — с помощью редакторов реестра пользователь (особенно новичок) может здорово осложнить свою жизнь и собственными руками создать себе множество проблем. Впрочем, эта книга предназначена для опытных пользователей, желающих самостоятельно устранять возникающие проблемы. Именно поэтому овладение приемами работы с реестром для вас — жизненная необходимость.

¹ "Услужливые программы делают дополнительные шаги для того, чтобы облегчить жизнь пользователям (особенно новичкам)" — цитата из книги Лу Гринзоу "Философия программирования для Windows 95/NT".

По умолчанию утилита Regedit.exe в процессе установки операционных систем копируется в каталог %SystemRoot% (например, C:\WINDOWS). Найдите этот файл и запустите его двойным щелчком мыши. Еще один, простейший вариант запуска редактора реестра — с помощью меню **Пуск** (Start). Для этого просто введите строку `regedit` в поле поиска, и вы немедленно увидите Редактор реестра в списке программ (рис. 3.1). При этом обратите внимание на возможность запуска редактора реестра с административными полномочиями. Для этого достаточно щелкнуть по ярлыку правой кнопкой мыши и выбрать из контекстного меню команду **Запуск от имени администратора** (Run as administrator).

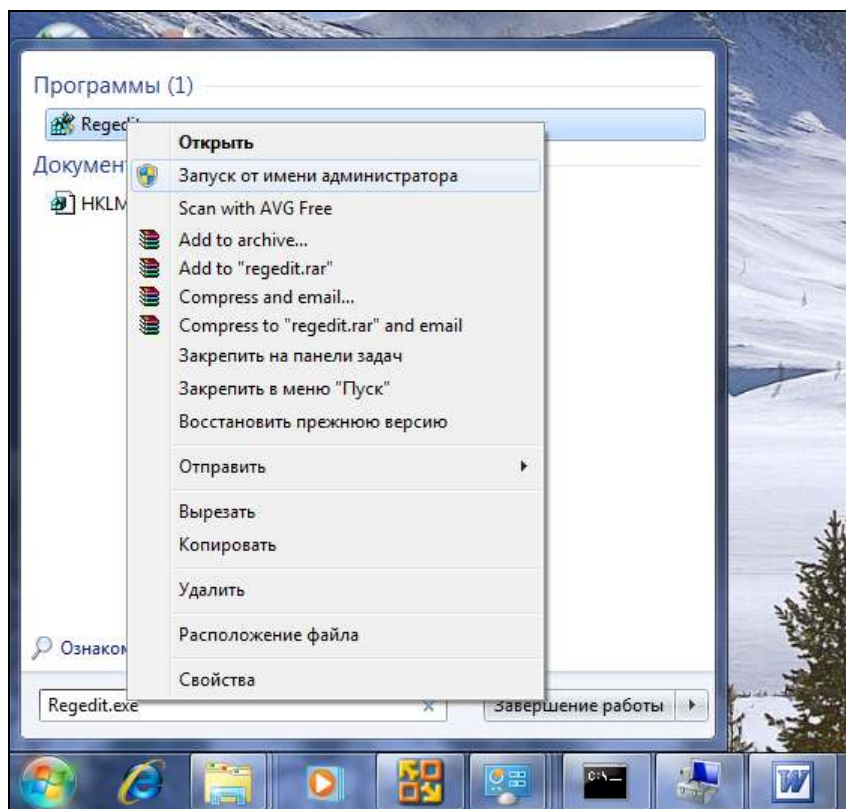


Рис. 3.1. Простейший способ запуска Редактора реестра

Не упустите также из виду новые приятные особенности пользовательского интерфейса Windows 7 — возможность быстро поместить ярлык, ссылающийся на часто используемую вами программу (это не обязательно должен быть

Редактор реестра, так можно поступить с любой программой, которую вы часто вызываете), в меню **Пуск** и на Панель задач (Taskbar). Делается это командами **Закрепить в меню "Пуск"** (Pin to Start Menu) и **Закрепить на панели задач** (Pin to Taskbar), соответственно (см. рис. 3.1). Разумеется, в случае, если впоследствии вы захотите убрать ярлык программы как из меню **Пуск** (Start), так и с Панели задач (Taskbar), то соответствующие опции в любой момент можно выбрать из контекстного меню, выводимого по нажатию правой кнопки мыши (рис. 3.2).

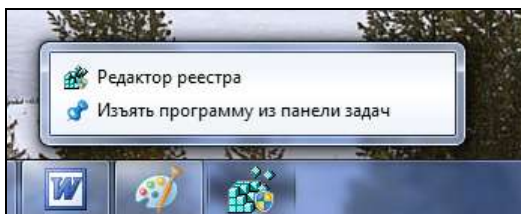


Рис. 3.2. При желании ярлык программы, закрепленный на Панели задач, всегда можно убрать

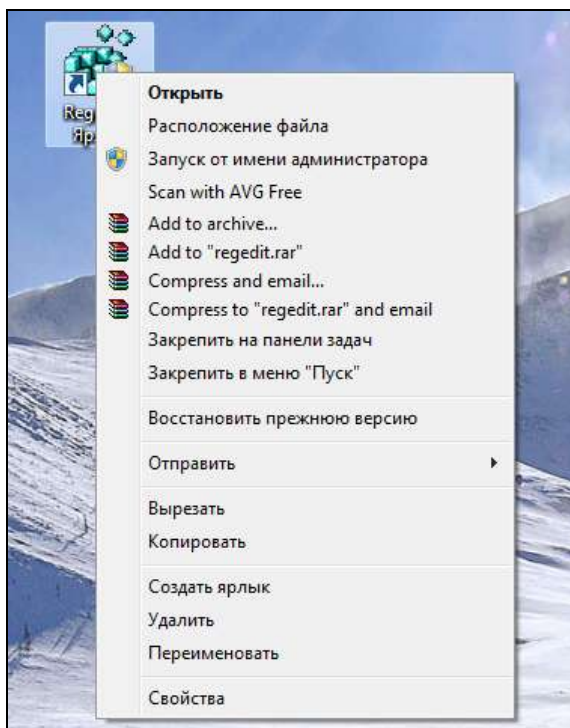


Рис. 3.3. Как и в предшествующих версиях Windows, в Windows 7 для Редактора реестра можно создать ярлык на рабочем столе

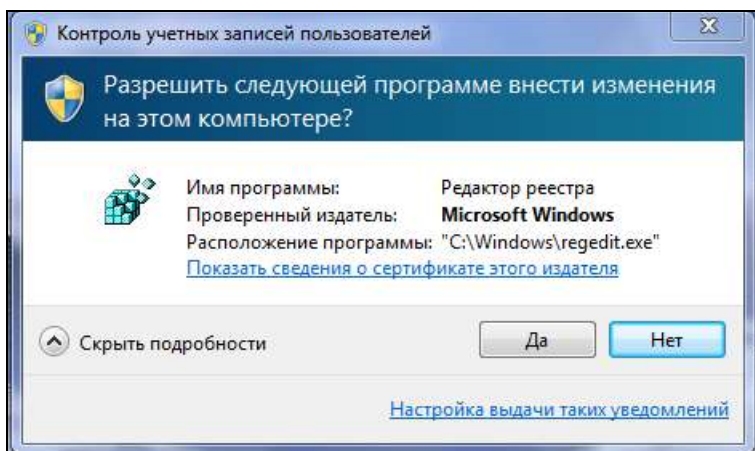


Рис. 3.4. Редактор реестра защищен функцией контроля учетных записей пользователей (UAC)

Наконец, как и в более ранних версиях Windows, вы можете создать для этой программы ярлык на рабочем столе (рис. 3.3). Как и в Windows Vista, в Windows 7 Редактор реестра защищен функцией контроля учетных записей пользователей (UAC), и поэтому при его запуске с помощью команды **Выполнить** (Run) из меню **Пуск** (Start) вам потребуется подтвердить это действие нажатием кнопки **Продолжить** (Continue) в открывшемся окне (рис. 3.4).

Исследование интерфейса Редактора реестра

Этот раздел построен таким образом, чтобы служить кратким справочником по работе с Редактором реестра. Здесь показаны и описаны все его возможности. Последующие разделы содержат инструкции по использованию этих возможностей, а также указания по внесению модификаций в реестр.

Окно Редактора реестра, вызываемого по команде Regedit.exe, состоит из четырех основных областей (рис. 3.5):

- ❑ строка меню — в этой строке содержатся основные пункты меню: **Файл** (File), **Правка** (Edit), **Вид** (View), **Избранное** (Favorites) и **Справка** (Help);
- ❑ левая панель — отображает иерархию реестра, организованную в виде ключей (в литературе они часто обозначаются термином "разделы") и вложенных ключей (другие часто встречающиеся термины — "подключи" или "подразделы");

- ❑ правая панель — показывает текущие параметры выбранного ключа реестра, известные также как *значимые элементы* (value entires). Каждый параметр реестра характеризуется именем, отображаемым в столбце **Имя** (Name) правой панели, типом данных, отображаемым в столбце **Тип** (Type) и значком чуть левее имени, и значением, отображаемым в столбце **Значение** (Data);
- ❑ строка состояния — указывает путь к выбранному элементу реестра. Она нужна, чтобы отображать полный путь к ключу реестра, в составе которого содержится выделенный параметр.

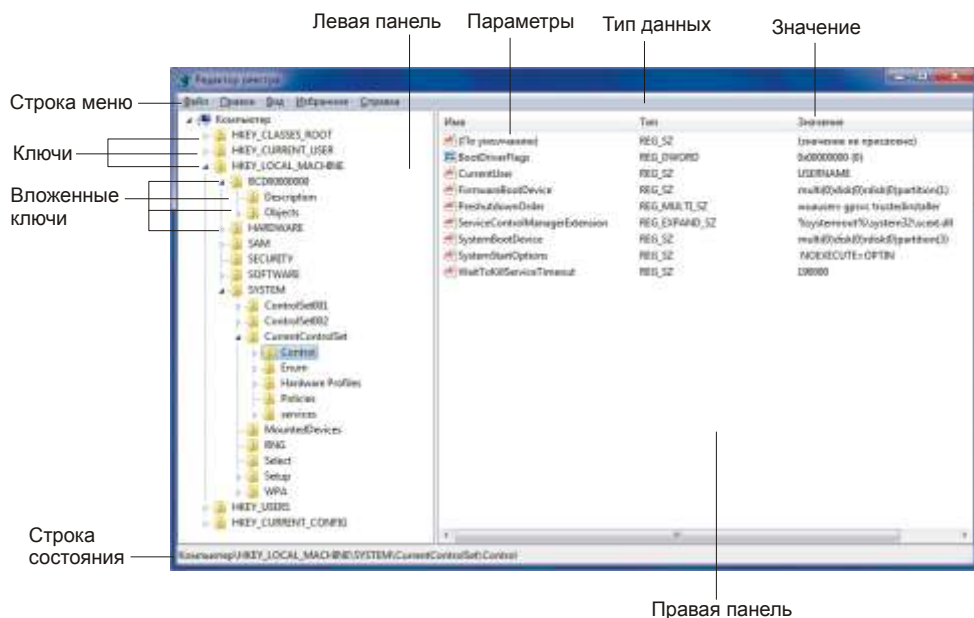


Рис. 3.5. Окно Редактор реестра

Итак, при вызове Regedit раскрывается окно **Редактор реестра** (Registry Editor), в котором отображаются ключи только верхнего уровня иерархии реестра, отвечающие от значка **Компьютер** (Computer). Это имена корневых ключей, базовая информация о которых была приведена в *главе 1*.

Если выполнить щелчок мышью, указав курсором на значок ▾, расположенный левее значка любой из папок, то развернется соответствующий ключ, в котором отобразится иерархия содержащихся в его составе вложенных

ключей. Эта операция разворачивает дерево ключа реестра до следующего уровня вложенности и во многом напоминает аналогичную операцию раскрытия папок и вложенных папок в Проводнике (Explorer).

Если в составе вложенных ключей имеются другие вложенные ключи, то слева от них тоже будут находиться значки ▸, которые можно, в свою очередь, развернуть для просмотра следующего уровня иерархии. Этот послыйный метод организации реестра известен под названием *вложения* (nesting) и допускает множество уровней. Такая иерархическая организация представляет собой основное отличие реестра от файлов инициализации (INI-файлов).

По достижении самого нижнего уровня вложенности слева от вложенного ключа появится значок ▴, который указывает, что дальнейшее раскрытие невозможно. После этого перемещаться по иерархическому дереву удастся только в одном направлении — вверх.

Если рядом с ключом нет ни значка ▸, ни значка ▴, этот ключ не содержит вложенных ключей.

В табл. 3.1 приведен список клавиатурных комбинаций, используемых для просмотра реестра и ориентации в нем с помощью Редактора реестра (Registry Editor).

Таблица 3.1. Клавиатурные комбинации, используемые в Regedit.exe

Клавиша	Действие
<↑>	Перемещает вверх к предыдущему ключу
<↓>	Перемещает вниз к следующему ключу
<→> или <+>	Разворачивает выделенный ключ на один уровень, показывая его подключи; если подключ уже развернут, то перемещает вниз к следующему ключу
<←> или <->	Сворачивает выделенный ключ, если он был развернут; в противном случае перемещает вверх к предыдущему ключу
<Tab>	Перемещает в другое подокно окна Редактора реестра (Registry Editor)
<Home>	Позволяет вернуться к началу иерархии (значку Компьютер)
<End>	Позволяет перейти к последнему видимому разделу
<Page Up>/ <Page Down>	Выполняет переход вверх/вниз на одну страницу в панели разделов

Таблица 3.1 (окончание)

Клавиша	Действие
<Ctrl>+<F>	Открывает окно поиска: команды меню Правка Найти (Edit Find)
<F3>	Выполняет поиск с указанными ранее параметрами: команды меню Правка Найти далее (Edit Find Next)
<Delete>	Удаляет выбранный параметр или выбранную ветвь
<F2>	Используется для переименования выбранного параметра или раздела
<F10>	Осуществляет быстрый доступ к меню
<Shift>+<F10>	Открывает контекстное меню для раздела или параметра. Комбинация клавиш очень удобна для пользователей, имеющих старые клавиатуры без клавиши вызова контекстного меню
<F5>	Обновляет данные на экране (другие программы могли изменить реестр, пока вы его просматривали). Соответствует командам меню Правка Обновить (Edit Refresh)

В правой панели окна **Редактор реестра** (Registry Editor) располагаются параметры реестра, каждый из которых характеризуется именем, типом данных и собственно данными:

- ❑ многие параметры, предоставляемые Microsoft, используют *имя* (По умолчанию) (Default) — вы убедитесь в этом, когда начнете интенсивно работать с Редактором реестра (Regedit). Имена параметров располагаются в столбце **Имя** (Name) правой панели окна **Редактор реестра** (Registry Editor). Эти имена присваиваются значимым элементам разработчиками приложений и физических устройств;
- ❑ *типы данных*, характеризующие параметры реестра, отображаются в столбце **Тип** (Type). Утилита Regedit.exe для удобства отображает также специальные значки, возникающие чуть левее имен параметров и позволяющие быстро отличить двоичные данные от текстовых. Краткое описание значков, отображаемых в окне Редактора реестра, приведено в табл. 3.2;

Таблица 3.2. Значки, соответствующие типам данных в Regedit.exe

Тип данных	Описание
	Означает, что данные имеют двоичный формат (типы данных REG_BINARY и REG_DWORD)
	Означает текст и символы, которые вы можете прочесть, например, "Сеть" (строковые типы данных: REG_EXPAND_SZ, REG_MULTI_SZ и REG_SZ)

- в столбце **Значение** (Data) располагаются собственно *данные* (текстовые или двоичные), соответствующие значению выбранного параметра. Эти данные можно редактировать, модифицировать или создавать в целях оптимизации той или иной функции.

Далее приведено краткое описание команд меню Редактора реестра (Registry Editor).

Команды меню **Файл**

Меню **Файл** (File) содержит следующие команды:

- **Импорт** (Import);
- **Экспорт** (Export);
- **Загрузить куст** (Load Hive);
- **Выгрузить куст** (Unload Hive);
- **Подключить сетевой реестр** (Connect Network Registry);
- **Отключить сетевой реестр** (Disconnect Network Registry);
- **Печать** (Print);
- **Выход** (Exit).

Рассмотрим их поподробнее.

Команда **Импорт** (Import)

Команда позволяет импортировать в реестр предварительно экспортированные файлы ульев и ключей реестра.

Мелкие, но приятные усовершенствования встречаются в Windows 7 буквально на каждом шагу. Вот, например, сравните окно импорта файла реестра в Windows Vista (рис. 3.6) и в Windows 7 (рис. 3.7). Вы сразу же заметите, что в Windows Vista в панели предварительного просмотра (даже если она активизирована), никакой информации о файлах, которые вы собираетесь импортировать, не отображается. Зато в Windows 7 вы сразу же можете посмотреть, что именно собираетесь импортировать в реестр.

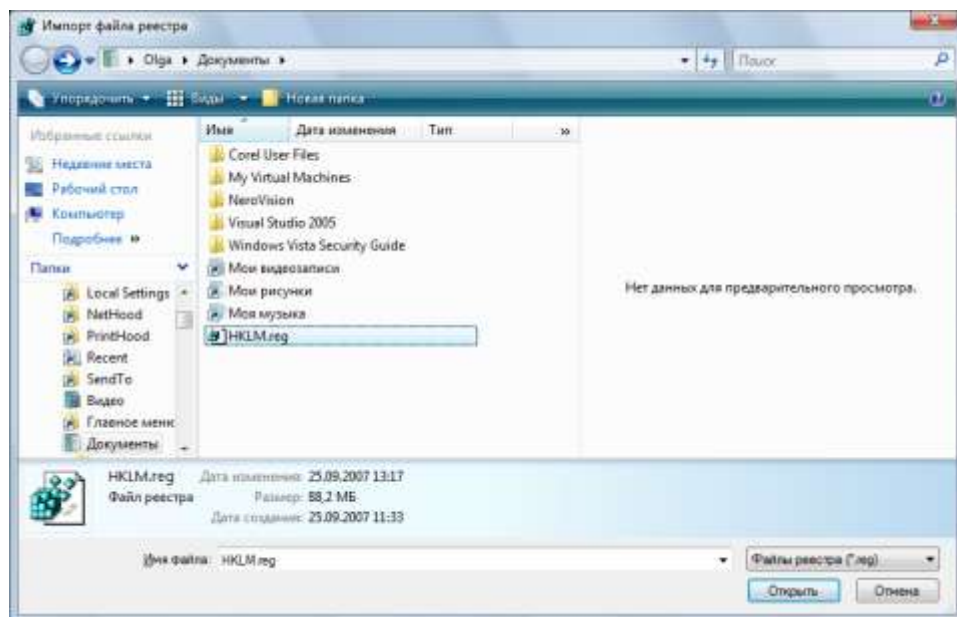


Рис. 3.6. Окно импорта REG-файла в Windows Vista, обратите внимание на правую панель окна — данных для предварительного просмотра нет

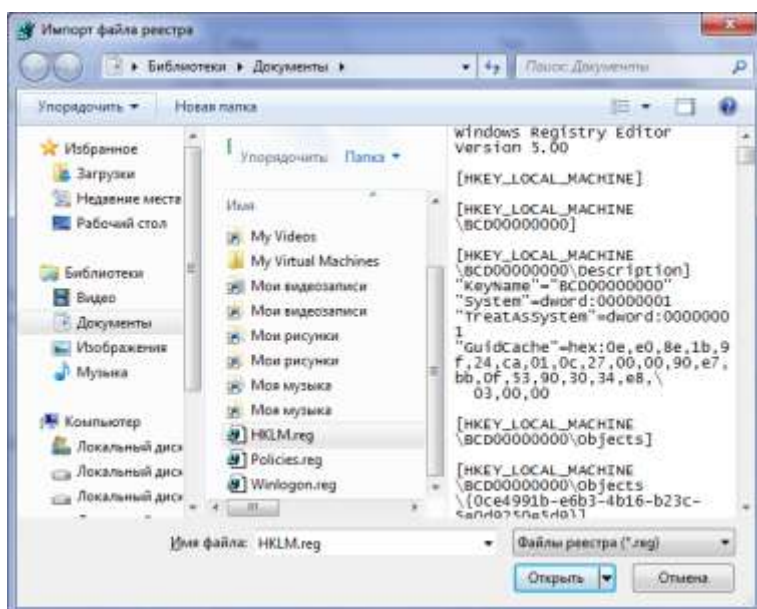


Рис. 3.7. Точно такое же окно импорта в реестр, но в Windows 7 — как говорится, почувствуйте разницу!

Команда Экспорт (Export)

Команда дает возможность сохранить весь реестр или его часть в виде REG-файла или файла другого типа, например, в текстовом файле формата ASCII.

Чтобы экспортировать ветвь реестра, выполните следующие действия:

1. Выделите ветвь реестра, затем выберите команду **Экспорт** (Export) в меню **Файл** (File).
2. В поле **Имя файла** (File name) открывшегося диалогового окна **Экспорт файла реестра** (Export Registry File) (рис. 3.8) введите имя файла.

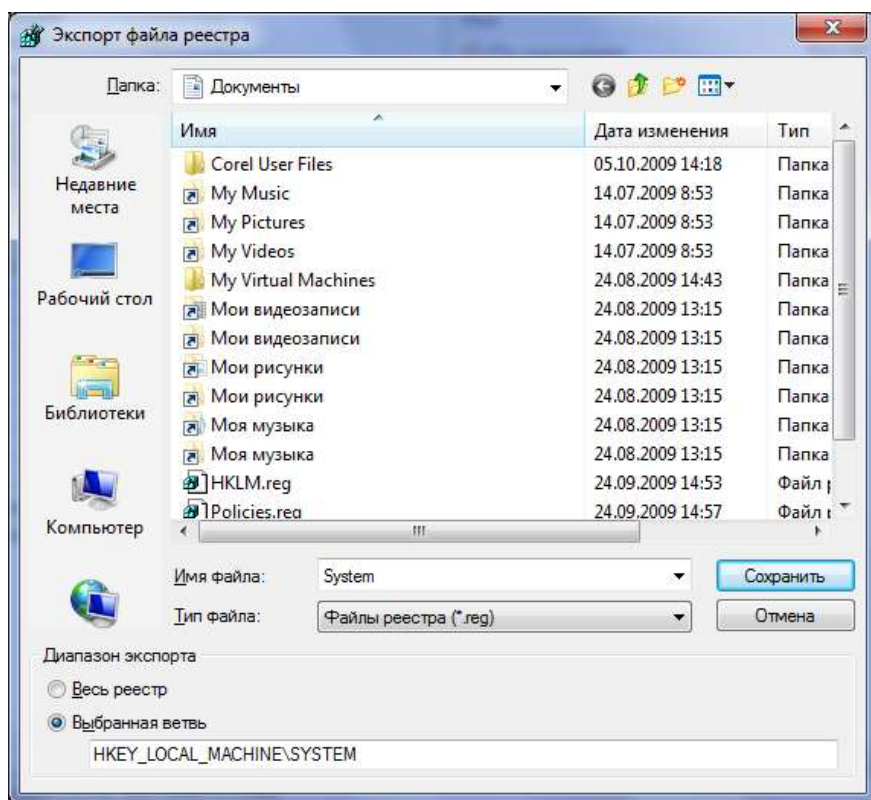


Рис. 3.8. Диалоговое окно **Экспорт файла реестра**

По умолчанию файлу будет присвоено расширение reg. Чтобы сохранить экспортируемый файл в другом формате, выберите нужную опцию из списка **Тип файла** (Save as type), расположенного непосредственно под

полем **Имя файла** (File name). Версия Regedit.exe из Windows 7 позволяет сохранять экспортированные файлы реестра в различных форматах, в том числе:

- в формате Windows 2000/XP/Vista/7 — для этой цели служит опция **Файлы реестра (*.reg)** (Registration Files (*.reg));
- в формате файлов реестра Windows 9x/NT 4 — для этой цели служит опция **Файлы реестра Win9x/NT 4 (*.reg)** (Win9x/NT 4 Registration Files (*.reg));
- начиная с Windows XP, вы можете сохранять файлы экспортированного реестра как ульи, выбрав опцию **Файлы кустов реестра (*.*)** (Registry Hive Files (*.*)
- в текстовом формате — используя опцию **Текстовые файлы (*.txt)** (Text Files (*.txt)).

ВНИМАНИЕ!

Между операцией импорта REG-файла (это файл текстового формата) и операцией импорта файла, сохраненного в формате улья реестра (ульи реестра представляют собой файлы двоичного формата) существует одно не слишком заметное на первый взгляд, но очень важное отличие. После импорта в реестр REG-файла все параметры реестра, указанные в импортируемом файле, будут соответствующим образом изменены. При этом все новые ключи и параметры, созданные в реестре уже после создания REG-файла, останутся в неприкосновенности. Если же вы импортируете обратно в реестр файл, сохраненный в формате улья, то все содержимое конкретной ветви реестра будет замещено содержимым импортируемого файла. Таким образом, все новые подключи и параметры, созданные в составе этой ветви реестра уже после ее экспорта в формате улья, будут удалены.

3. Если требуется сохранить часть реестра, выбирайте опцию сохранения только выделенной ветви реестра. Для этого установите переключатель **Выбранная ветвь** (Selected branch) в группе **Диапазон экспорта** (Export range). Однако если вы часто модифицируете реестр, то экспорт всего реестра целиком — неплохая идея. Это даст вам дополнительные гарантии восстановления в случае ошибки.

4. Нажмите кнопку **Сохранить** (Save).

Сохраненный файл можно просмотреть в текстовом редакторе, чтобы убедиться в правильности сохранения. Экспортированные файлы реестра содержат текст ASCII без каких-либо символов форматирования.

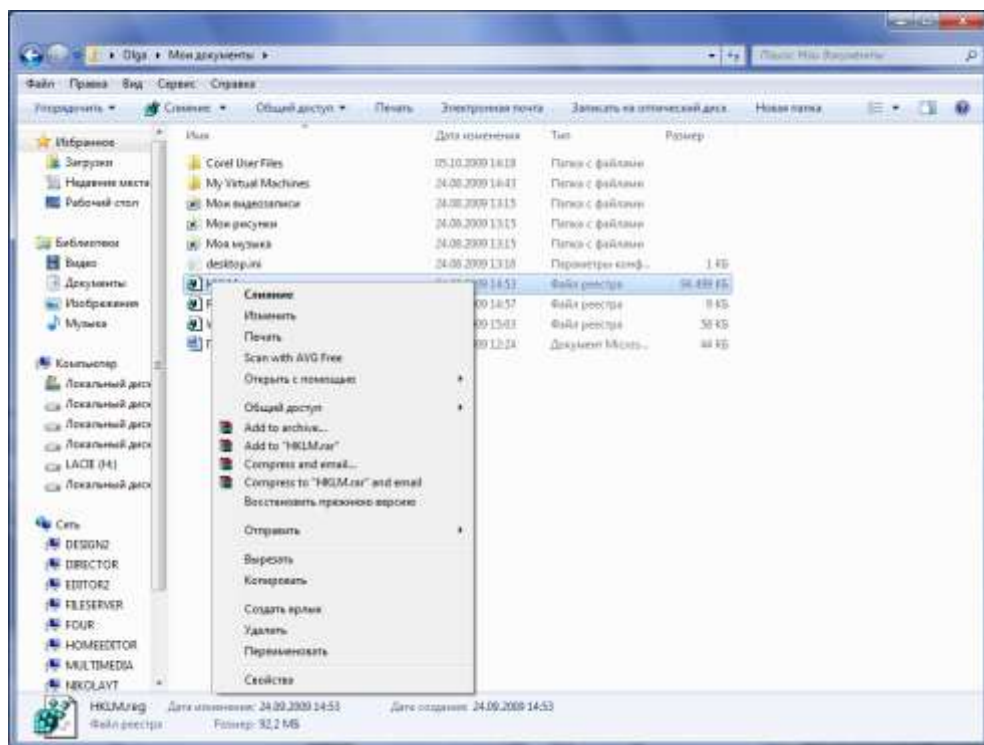


Рис. 3.9. По умолчанию файлы с расширением reg ассоциируются с приложением **Редактор реестра**, и (также по умолчанию) над такими файлами выполняется операция **Слияние** (Merge), импортирующая содержимое файла в реестр

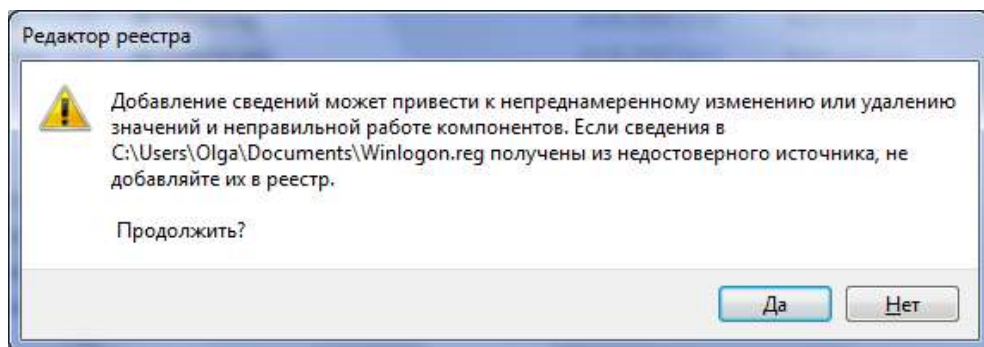


Рис. 3.10. Редактор реестра предлагает подтвердить, действительно ли вы хотите добавить содержимое экспортированного REG-файла в реестр

Обращаясь с экспортированными файлами реестра, следует соблюдать осторожность, особенно в том случае, если экспорт производится в экспериментальных целях. Не секрет, что опытные администраторы, хорошо знакомые с реестром, экспериментируют над своей системой или решают некоторые проблемы путем редактирования экспортированного файла реестра с последующим импортированием его обратно в систему. Однако, перед тем как вносить такие изменения, рекомендуется принять следующие меры предосторожности:

- ❑ предварительно создайте резервную копию экспортированного файла, который требуется редактировать. Если при редактировании будет допущена ошибка, которая приведет к возникновению проблем, можно будет импортировать в реестр резервную копию этого REG-файла;
- ❑ если вы часто экспериментируете с реестрами различных операционных систем (Windows 9x, Windows NT/2000/XP и Windows Vista/7), то экспортированные файлы реестров каждой из этих операционных систем рекомендуется держать отдельно друг от друга и в различных каталогах, специально выделенных для такой цели. Это поможет избежать случайного импорта в систему несовместимого файла реестра;
- ❑ файлы с расширением reg по умолчанию ассоциированы с приложением **Редактор реестра** (Registry Editor). И по умолчанию над такими файлами выполняется операция **Слияние** (Merge), которая импортирует содержимое данного файла в реестр (рис. 3.9). В Windows Vista/7, когда вы двойным щелчком щелкаете мышью по такому файлу, сначала появляется до боли знакомое окно **Контроль учетных записей пользователей** (User Account Control), предлагающее подтвердить запуск Редактора реестра, а затем запускается программа Regedit.exe и тоже предлагает подтвердить намерение добавить содержимое экспортированного файла в реестр (рис. 3.10). Будьте предельно внимательны на этом этапе, чтобы избежать случайного импорта в реестр несовместимых или ошибочных данных.

Команды *Загрузить куст* (Load Hive) и *Выгрузить куст* (Unload Hive)

Эти команды появились в Редакторе реестра, начиная с Windows XP. Они предоставляют те же функциональные возможности, которые обеспечивались аналогичными командами старого приложения Regedt32.exe. Команды **Загрузить куст** (Load Hive) и **Выгрузить куст** (Unload Hive) позволяют загружать предварительно экспортированные и сохраненные в формате ульев файлы реестра или, соответственно, выгружать ульи реестра. Обратите внимание, что эти команды применимы лишь к ключам, которые соответствуют ульям реестра, — в остальных случаях эти опции меню недоступны. Экспор-

тированный файл улья, загруженный в реестр, становится одним из вложенных ключей под корневыми ключами `HKEY_LOCAL_MACHINE` или `HKEY_USERS`. Процесс загрузки улья реестра показан на рис. 3.11.

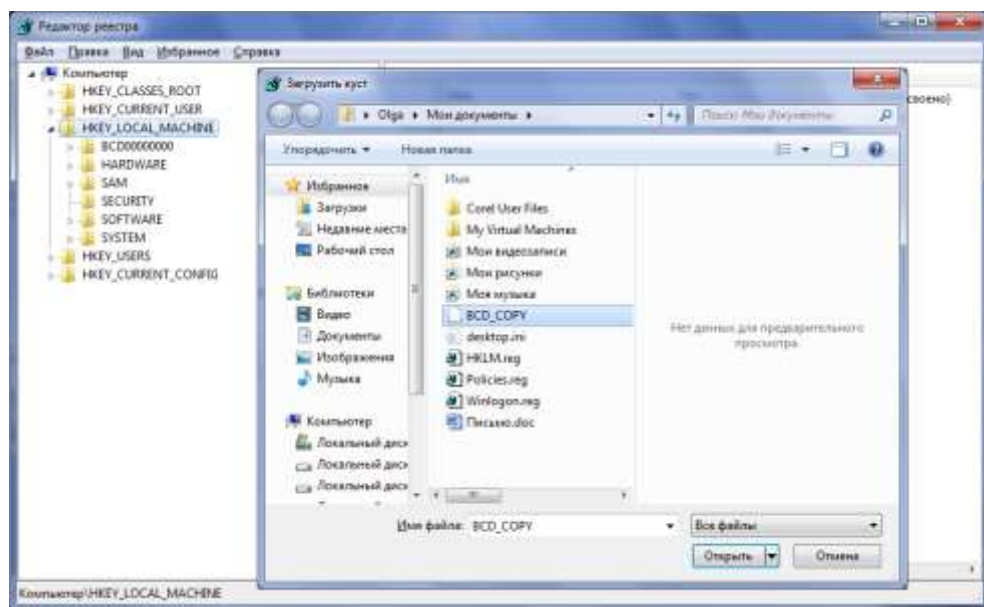


Рис. 3.11. Загружаем улей реестра

Чтобы загрузить в реестр файл, предварительно экспортированный в формате улья, необходимо выполнить следующие действия:

1. Выберите ключ реестра `HKEY_USERS` или `HKEY_LOCAL_MACHINE` для активизации соответствующей команды меню.
2. Выберите команду **Загрузить куст** из меню **Файл**. Откроется окно **Загрузить куст** (Load Hive), в котором следует выбрать ранее экспортированный улей реестра. Укажите требуемый файл улья и нажмите кнопку **Открыть** (Open).
3. В появившемся окне **Загрузка куста реестра** (Load Registry Hive) введите имя, которое будет использоваться для вновь загруженного улья (рис. 3.12). Это имя необходимо для нового вложенного ключа, который появится в реестре после того, как вы загрузите улей. Теперь вы сможете редактировать загруженный улей реестра (а выполнив необходимые операции, вновь экспортировать его для сохранения изменений) и выгрузить улей (рис. 3.13).

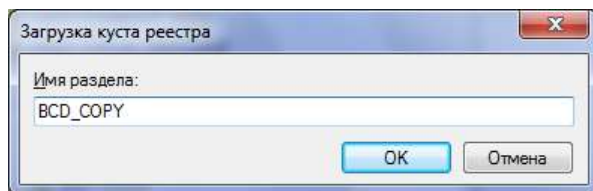


Рис. 3.12. Ввод имени для нового вложенного ключа, который появится в реестре после загрузки улья

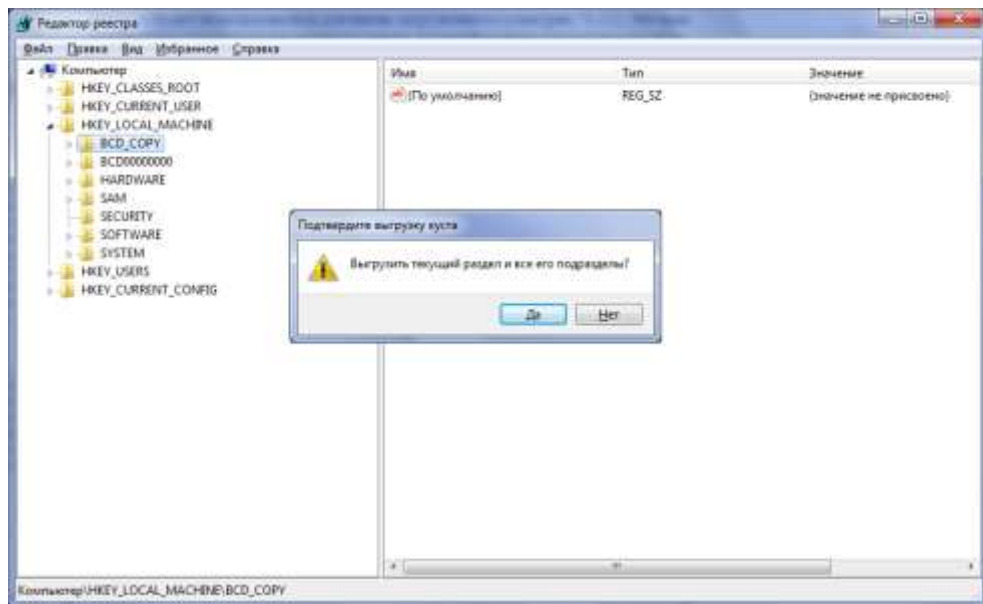


Рис. 3.13. Вновь загруженная копия улья BCD00000000 теперь отображается как вложенный ключ BCD_COPY под корневым ключом HKEY_LOCAL_MACHINE, и ее можно отредактировать, а затем, после внесения необходимых изменений, выгрузить

4. Выполнив редактирование загруженного улья реестра, вы можете выгрузить его. Для этого его следует выделить, а затем выполнить команду **Выгрузить куст** (Unload Hive) из меню **Файл** (File). Обратите внимание — при выгрузке улья все изменения, внесенные в него, сохраняются автоматически.

ПРИМЕЧАНИЕ

Для выполнения этой процедуры вам необходимо зарегистрироваться в локальной системе в качестве администратора или же пользователя, принадлежащего группе **Администраторы** (Administrators). Если компьютер подключен к сети, то возможность выполнения данных действий будет зависеть также от политики безопасности, установленной администратором этой сети.

Команда Подключить сетевой реестр (Connect Network Registry)

Эта команда доступна лишь в том случае, если компьютер, на котором работает программа **Редактор реестра** (Registry Editor), подключен к сети, и позволяет выполнить редактирование реестра на другом компьютере, работающем в составе сети. Для подсоединения к удаленному реестру, требуется указать имя компьютера, на котором находится копия сетевого реестра, — так называемая *удаленная копия* (рис. 3.14). Начиная с Windows XP, набор опций по просмотру и поиску в сети по сравнению с функциональными возможностями Редактора реестра в Windows NT/2000, в котором имелаась лишь команда **Обзор** (Browse), существенно расширен. В Windows Vista и Windows 7 этот набор опций не изменился.

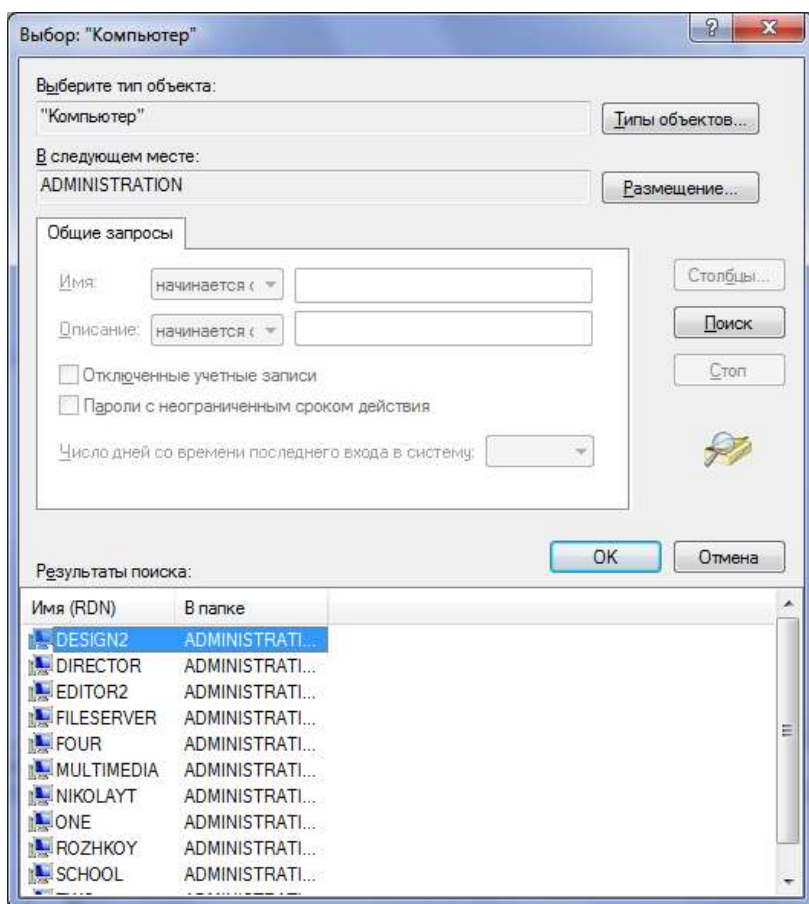


Рис. 3.14. Окно **Выбор: "Компьютер"** обеспечивает расширенные возможности просмотра и поиска

ПРИМЕЧАНИЕ

Для выполнения этой процедуры вам необходимо иметь соответствующие административные права в сети, к которой подключен компьютер.

Команда Отключить сетевой реестр (Disconnect Network Registry)

Чтобы отключиться от реестра, расположенного на удаленном компьютере, используется команда **Отключить сетевой реестр** (Disconnect Network Registry). Если вы на текущий момент не подключены к сетевому реестру, эта опция будет недоступна.

Команда Печать (Print)

Для того чтобы распечатать весь реестр или же его ветвь, что весьма удобно, используется команда **Печать** (Print) из меню **Файл**.

Команда Выход (Exit)

Для закрытия окна программы **Редактор реестра** (Registry Editor) и завершения редактирования реестра необходимо использовать команду **Выход** (Exit).

Команды меню Правка

Меню **Правка** (Edit) содержит команды, которые позволяют находить и модифицировать нужные элементы реестра:

- **Изменить** (Modify) — команда используется для изменения данных, содержащихся в составе параметров реестра. Эта опция будет доступна только в том случае, если выбрать один из параметров, перечисленных в правой панели окна **Редактор реестра** (Registry Editor);
- **Изменить двоичные данные** (Modify Binary Data) — команда позволяет редактировать любые данные (включая другие типы данных) в двоичном редакторе. Так же, как и предыдущая, данная команда станет доступной лишь после того, как вы выберете один из параметров реестра, указанных в правой панели окна;
- **Создать** (New) — команда позволяет добавлять в реестр новые ключи и параметры. Обратите внимание, что по сравнению с версией утилиты Regedt32.exe из состава Windows NT/2000, в которой позволялось добавлять лишь параметры строковых типов, двоичные параметры и параметры типа `DWORD`, версия Редактора реестра в Windows XP обеспечивает расширенный набор опций, в том числе позволяет также добавлять многострочные значения (тип данных `REG_MULTI_SZ`) и расширяемые строковые данные (`REG_EXPAND_SZ`). В Windows Vista этот набор был дополнительно расширен и позволил добавлять в состав реестра 64-разрядные параметры

типа `REG_QWORD` (рис. 3.15). В Windows 7 набор команд, доступных в данном меню, не изменился. Соответствующие команды становятся доступными после выбора команды **Создать** (New). Те же самые опции будут доступны и в контекстном меню, раскрывающемся по щелчку правой кнопки мыши;

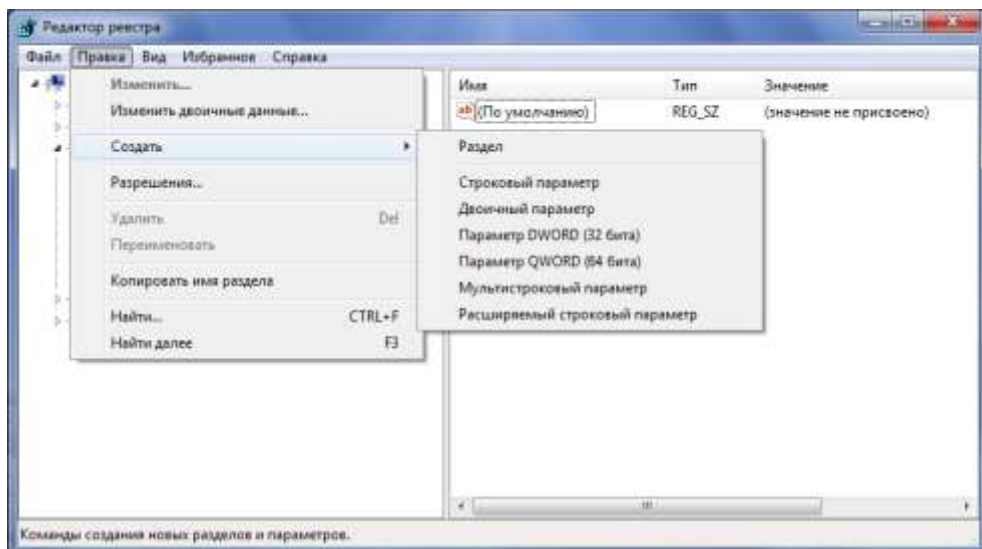


Рис. 3.15. Команда **Создать** позволяет добавлять новые ключи, строковые, двоичные параметры, 32-разрядные параметры типа `REG_DWORD`, 64-разрядные параметры типа `REG_QWORD`, а также многостроковые и расширяемые строковые параметры

❑ **Переименовать** (Rename) и **Удалить** (Delete) — эти команды меню **Правка** (Edit) позволяют соответственно переименовать или удалить значимый элемент реестра. Удалить значимый элемент можно и другим способом — выделите нужный элемент, выполнив на нем щелчок мышью, а затем нажмите клавишу `<Del>`. Аналогичным образом, для быстрого переименования значимого элемента можно указать на него курсором, выполнить щелчок правой кнопкой мыши, выбрать из контекстного меню команду **Переименовать** (Rename) и ввести новое имя;

ВНИМАНИЕ!

Удаление параметров и ключей реестра с помощью утилиты **Редактор реестра** (Registry Editor) — это необратимая операция. Редактор реестра не имеет команды **Отменить** (Undo), поэтому при удалении параметров и ключей следует соблюдать осторожность. Windows отобразит диалоговое окно, в котором вам

будет предложено подтвердить свое намерение удалить элемент реестра, но после того как на запрос будет дан утвердительный ответ, отменить эту операцию уже нельзя.

- ❑ **Копировать имя раздела** (Copy Key Name) — команда дает возможность скопировать в буфер обмена имя ключа, выделенного в текущий момент. Впоследствии скопированное имя можно вставить в произвольный текст с помощью команды **Вставить** (Paste), имеющейся в любом текстовом редакторе. Поскольку реестр представляет собой сложную иерархическую базу данных, пути к нужному элементу могут оказаться очень длинными и сложными для запоминания. Поэтому многие по достоинству оценили удобство этой функции. Команду **Копировать имя раздела** (Copy Key Name) очень удобно использовать в сочетании с командами **Найти** (Find) и **Найти далее** (Find Next), а применения ее могут быть самыми разнообразными — от редактирования реестра до вставки имен ключей в тексты писем, отчетов, книг и т. п.;
- ❑ **Разрешения** (Permissions) — команда, которая позволяет управлять правами доступа к ключам реестра и осуществлять аудит действий, производимых над ними, заслуживает особого внимания. Вновь необходимо отметить тот факт, что в Windows NT/2000 это функциональное свойство имелось лишь в программе Regedt32.exe, где была предусмотрена команда меню **Безопасность** (Security). Начиная с Windows XP, эта функциональная возможность была интегрирована в единую версию редактора реестра — утилиту Regedit.exe. В Windows XP права доступа к ключу реестра могут быть назначены независимо от типа файловой системы в системном разделе. Что касается операционных систем Windows Vista и Windows 7, то, как известно, они могут быть установлены только на раздел, отформатированный для использования NTFS.

Более подробно команда **Разрешения** (Permissions) рассмотрена в этой главе далее, в разд. *Управление безопасностью реестра*.

Команды **Найти** и **Найти далее**

На командах **Найти** (Find) и **Найти далее** (Find Next) хочется остановиться особо. Эти команды используются для поиска конкретных элементов или данных (включая строки и слова) в реестре. Выбор команды **Найти** в меню **Правка** открывает диалоговое окно **Поиск** (Find), в котором можно описать искомые ключ, параметр или его данные (рис. 3.16). Можно выполнять поиск ключей, параметров, данных или любой их комбинации. Искомые значения могут быть как текстовыми, так и числовыми.

Для поиска нужного элемента реестра введите искомое значение в поле **Найти** (Find what). Существует возможность сузить диапазон поиска, отме-

тив один из флажков, имеющихся в группе **Просматривать при поиске** (Look at):

- ☐ **имена разделов** (Keys) — поиск производится только по ключам реестра. Операция находит как корневые ключи, так и вложенные;
- ☐ **имена параметров** (Values) — отыскиваются только имена параметров. Как вы уже знаете, параметры отображаются в правой панели окна **Редактор реестра** в столбце **Имя**;
- ☐ **значения параметров** (Data) — диапазон поиска сужается, ограничиваясь только данными.

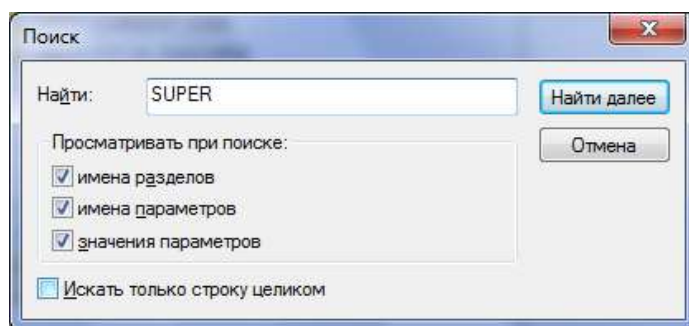


Рис. 3.16. Диалоговое окно Поиск

Диалоговое окно **Поиск** (Find) имеет флажок **Искать только строку целиком** (Match whole string only). При его использовании редактор реестра будет находить только целые слова, исключая из результатов поиска частичные совпадения. Примером может послужить случай поиска слова SUPER. Представьте себе, что вы установили в своей системе такую программу и хотите найти в реестре все элементы, добавленные этой программой.

ПРИМЕЧАНИЕ

SUPER — это программа-конвертатор, позволяющая выполнять преобразование видео и музыкальных файлов практически во все известные форматы. Надо отметить, что название программы — это не безосновательное бахвальство ее разработчиков. Во-первых, оно представляет собой аббревиатуру от Simplified Universal Player Encoder and Renderer (упрощенный универсальный кодировщик и визуализатор для проигрывателей). Во-вторых, программа действительно суперская, и к тому же еще и бесплатная. Скачайте ее с сайта производителя: <http://www.erightssoft.com/SUPER.html#Dnload>.

Если в системе установлены и другие приложения, в состав названия которых входит слово SUPER (например, игра Super Mario), то при снятом флаж-

ке **Искать только строку целиком** (Match whole string only) Редактор реестра найдет их все, что не всегда удобно — мало ли в системе компонентов, в состав которых входит данное слово? Вот, например, функция SuperFetch, о которой будет рассказано в последующих главах этой книги. Так что если вы хотите найти только строку SUPER, то следует установить флажок **Искать только строку целиком** (Match whole string only). Если же вам требуется найти все вхождения, то сбросьте этот флажок. Такая возможность ценна в том случае, когда вы не помните конкретного написания строки и хотите видеть все вариации. Если это не вызывает у вас возражений, то все в порядке.

ПРИМЕЧАНИЕ

Использование опции **Искать только строку целиком** (Match whole string only) увеличивает время поиска, что может быть существенно для больших реестров.

Заполнив все нужные поля в диалоговом окне **Поиск** (Find), нажмите кнопку **Найти далее** (Find Next), и процедура поиска начнется.

Найдя совпадение, Редактор реестра выделит совпадающий элемент подсветкой, помогая определить, в каком ключе (или вложенном ключе) совпадение найдено. Если найдены данные или имена значимых элементов, то в левой панели для просмотра откроются ассоциированные с ними ключи или подключи, а имя элемента выделится подсветкой. Однако, несмотря на эти визуальные подсказки, определить путь к найденному элементу в ряде случаев все равно бывает сложно. Именно поэтому рекомендуется постоянно держать отображаемой строку состояния, где всегда выводится полный путь к выделенному элементу реестра — все ключи, подключи и даже имя компьютера (не во всех случаях это будет локальный компьютер).

Итак, искомый элемент найден. Является ли он именно тем, что вы искали? На этот вопрос вам придется ответить самостоятельно. По результатам поиска можно модифицировать найденный элемент, завершить поиск или игнорировать результат и продолжить поиск. Чтобы найти следующее вхождение совпадающего элемента, нажмите клавишу <F3> или выберите команду **Найти далее** (Find Next) в меню **Правка** (Edit).

ПРИМЕЧАНИЕ

Во время поиска следует иметь в виду, что имена ключей и параметров не являются уникальными. Реестр может (и, чаще всего, это именно так) содержать несколько вхождений одного и того же имени ключа или параметра. По этой причине следует предоставлять как можно больше уточняющей информации.

Модификация ключей и значимых элементов с помощью команд меню *Правка*

Теперь, когда мы в общих чертах рассмотрели команды меню **Правка** (Edit), продолжим более подробное обсуждение их использования для добавления, модификации или удаления ключей и параметров реестра, а также для установки прав доступа к ключам реестра.

Добавление новых ключей

Для добавления нового ключа в любой улей реестра следует в меню **Правка** выбрать команду **Создать | Раздел** (New | Key). Эта процедура является очень простой и напоминает создание новых папок в Проводнике (Explorer). При создании нового ключа пользователю не будет предлагаться ввести для него имя, однако вы можете переименовать новый ключ после того, как он будет создан.

ПРИМЕЧАНИЕ

Обратите внимание лишь на одно существенное ограничение, а именно — вы не можете создавать новых ключей на верхнем уровне иерархии. Как было показано ранее в этой главе, реестр Windows Vista/7, как и реестр Windows 2000/XP, содержит 5 корневых ключей: `HKEY_CLASSES_ROOT`, `HKEY_CURRENT_USER`, `HKEY_LOCAL_MACHINE`, `HKEY_USERS` и `HKEY_CURRENT_CONFIG`, и новые корневые ключи к нему добавляться не могут.

Добавление новых значимых элементов

Для того чтобы добавить новые значимые элементы в реестр, выберите в меню **Правка** команду **Создать** (New), а затем соответствующую команду — в зависимости от типа данных создаваемого элемента. Используя версию программы `Regedit.exe`, входящую в состав Windows 7, можно создавать строковые значения (`REG_SZ`, `REG_MULTI_SZ` и `REG_EXPAND_SZ`), а также двоичные значения (`REG_BINARY`, `REG_DWORD` и `REG_QWORD`). При создании нового элемента пользователю не будет предложено снабдить его именем, однако вы сможете переименовать и отредактировать значение, после того как оно будет создано.

Редактор двоичных значений

Когда вы выбираете двоичное значение (тип данных — `REG_BINARY`), а затем выполняете в меню **Правка** команду **Изменить** (Modify), Редактор реестра открывает окно **Изменение двоичного параметра** (Edit Binary Value) (рис. 3.17). Обратите внимание, что вы можете использовать двоичный редактор для ре-

дактирования значения любого типа, выбирая команду **Изменить двоичные данные** (Modify Binary Data). Введите данные в поле **Значение** (Value data) окна **Изменение двоичного параметра** (Edit Binary Value).

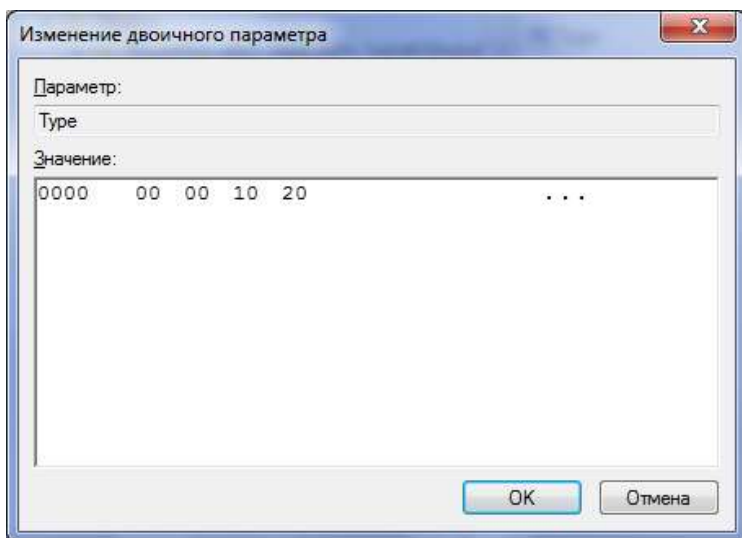


Рис. 3.17. Окно **Изменение двоичного параметра**

Редактирование строковых значений

Выделите значение `REG_SZ` в правой панели окна Редактора реестра, затем выберите в меню **Правка** команду **Изменить** для запуска редактора строковых значений. Окно **Изменение строкового параметра** (Edit String) (рис. 3.18) позволяет редактировать строковые значения.

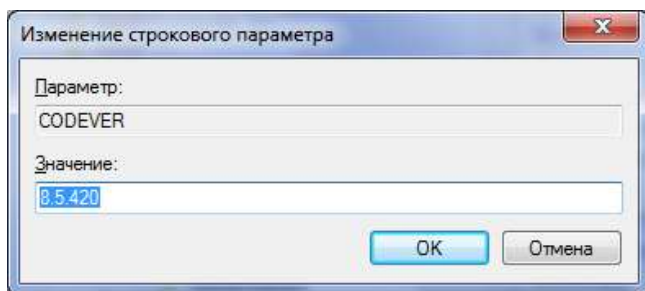


Рис. 3.18. Окно **Изменение строкового параметра**

Редактирование значений типа DWORD и QWORD

Редактор значений типа `DWORD` запускается по двойному щелчку мыши на значимом элементе реестра `REG_DWORD` или при выделении элемента данного типа с последующим выбором команды **Изменить** меню **Правка** (рис. 3.19). По умолчанию, все данные типа `REG_DWORD` отображаются в шестнадцатеричном формате. Однако вы можете также отображать данные в десятичном формате, выбрав соответствующий переключатель **Система исчисления** (Base) в нижней части окна. Редактор значений типа `QWORD` очень похож на редактор значений типа `REG_DWORD` и предоставляет аналогичные возможности (рис. 3.20).

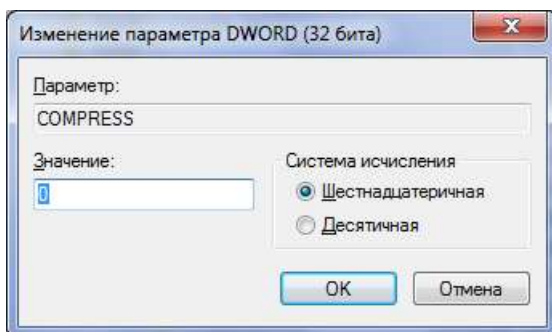


Рис. 3.19. Окно **Изменение параметра DWORD (32 бита)**

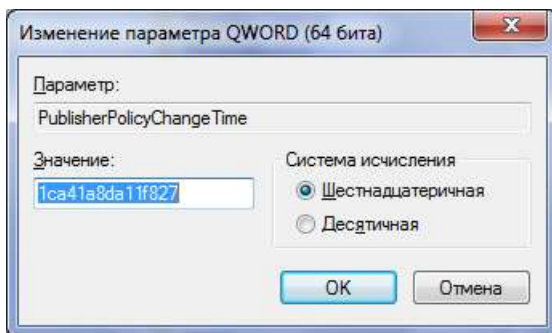


Рис. 3.20. Окно **Изменение параметра QWORD (64 бита)**

Редактирование многострочных значений

Если двойным щелчком щелкнуть мышью по многострочному значению или же выбрать многострочное значение, а затем выполнить команду **Изменить** меню

Правка, то откроется окно **Редактирование мультистроки** (Edit Multi-String) (рис. 3.21), предназначенное для редактирования многострочных значений.

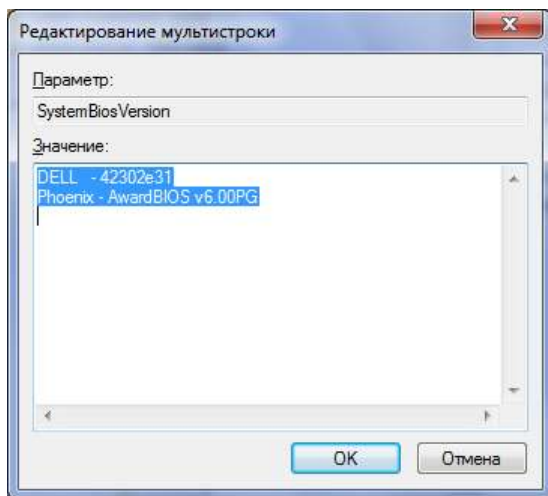


Рис. 3.21. Окно **Редактирование мультистроки**

Просмотр списков ресурсов

Как уже упоминалось в *главе 1*, системный реестр хранит всю информацию об аппаратных средствах компьютера. Для этого в реестре даже предусмотрены специальные типы данных: `REG_RESOURCE_LIST`, `REG_FULL_RESOURCE_DESCRIPTOR` и `REG_RESOURCE_REQUIREMENTS_LIST`. Они используются только в ключе реестра `HKEY_LOCAL_MACHINE\HARDWARE`. Параметры этих типов можно просмотреть в окнах **Списки ресурсов** (Resource Lists) (рис. 3.22) и **Ресурсы** (Resources) (рис. 3.23).

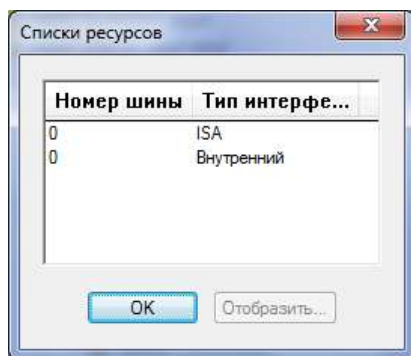


Рис. 3.22. Окно **Списки ресурсов**

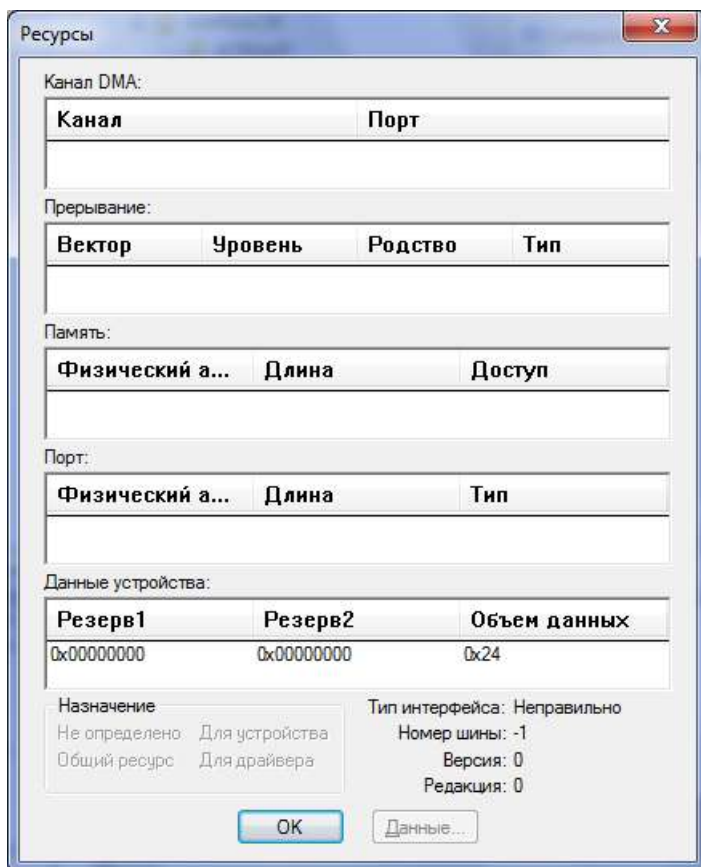


Рис. 3.23. Окно Ресурсы

Удаление ключей и параметров

Чтобы удалить из реестра ключ или параметр, выделите объект, предполагаемый для удаления, и выберите в меню **Правка** (Edit) команду **Удалить** (Delete). Вам будет предложено подтвердить свое намерение удалить выбранный ключ или параметр (рис. 3.24).

ПРИМЕЧАНИЕ

Перед выполнением операции удаления ключа или параметра реестра рекомендуется выполнить резервное копирование ульев реестра, из которых осуществляется удаление. Редакторы реестра не имеют команды отмены **Отменить** (Undo), поэтому после подтверждения операции удаления в вашем распоряжении не будет никакого другого способа восстановить удаленную информацию, кроме ее восстановления по предварительно созданной резервной

копии. Как видно из рис. 3.24, при удалении ключа выводимое на экран сообщение не содержит имени удаляемого ключа. Поэтому, прежде чем продолжать выполнение операции, тщательно проверьте имя выбранного ключа и убедитесь, что это именно тот ключ, который требуется удалить. Если вы случайно удалите что-либо из состава ключа реестра `HKEY_LOCAL_MACHINE\System\CurrentControlSet`, помните о возможности восстановления содержимого этого ключа с помощью последней успешно загруженной конфигурации (см. главу 7).

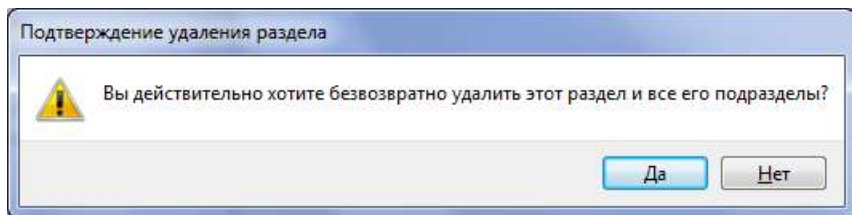


Рис. 3.24. Перед удалением ключа или параметра система предлагает подтвердить операцию

Команды меню *Вид*

Меню **Вид** (View) управляет способом отображения реестра и содержит следующие команды:

- ❑ **Строка состояния** (Status Bar) — команда позволяет при желании отключить строку состояния. Поскольку строка состояния помогает быстрее ориентироваться в реестре, отображая путь к текущему ключу, ее рекомендуется постоянно держать на виду;
- ❑ **Разделить** (Split) — команда перемещает курсор мыши на разделитель левой и правой частей окна **Редактор реестра** (Registry Editor), после чего остается только переместить мышь влево или вправо, чтобы найти удобную позицию для разделителя, и выполнить щелчок левой кнопкой мыши;

ПРИМЕЧАНИЕ

Аналогично способу перемасштабирования подокон в Проводнике (Explorer) или в окне **Компьютер** (Computer), вы можете перемасштабировать подокна Редактора реестра с помощью одной только мыши. Для этого необходимо переместить курсор мыши к разделителю так, чтобы курсор принял форму двусторонней стрелки, нажать левую кнопку мыши и, удерживая ее в этом положении, переместить разделитель в нужное положение, после чего отпустить кнопку мыши.

- ❑ **Вывод двоичных данных** (Display Binary Data) — команда, впервые появившаяся в Windows XP, становится доступной лишь после того, как вы

выберете один из параметров, перечисленных в правой панели окна **Редактор реестра**. В Windows XP она позволяла просмотреть выбранные элементы данных в трех форматах: **1 байт** (Byte), **2 байта** (Word) или **4 байта** (Dword). В Windows Vista и Windows 7 доступен и четвертый формат — **8 байт** (Qword) (рис. 3.25);

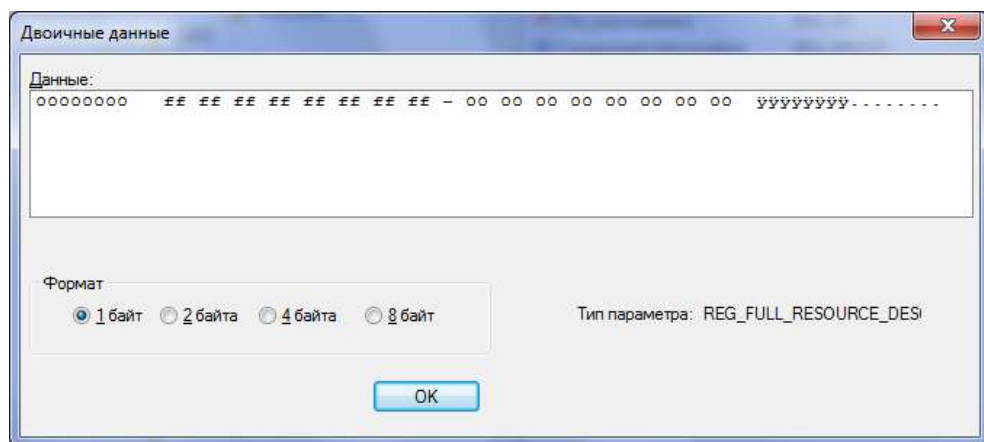


Рис. 3.25. Окно **Двоичные данные**

ПРИМЕЧАНИЕ

Обратите внимание, что с помощью команды **Вывод двоичных данных** (Display Binary Data) нельзя редактировать данные. Если же вам это необходимо, выберите соответствующий параметр, а затем выполните команду **Изменить двоичные данные** (Modify Binary Data) в меню **Правка** (Edit).

- ❑ в меню **Вид** (View) имеется еще одна команда — **Обновить** (Refresh). При внесении изменений в реестр не все они могут отображаться немедленно после внесения модификации. Обновить окно **Редактор реестра** (Registry Editor) можно с помощью команды **Обновить** или нажатием клавиши <F5>.

ПРИМЕЧАНИЕ

Как правило, в Windows NT 4.0 многие изменения (в том числе и внесенные путем редактирования реестра) входят в силу только после перезагрузки системы. В Windows 2000/XP впервые была введена полноценная поддержка Plug and Play, поэтому перезагрузок требовалось меньше. В Windows Vista поддержка Plug and Play расширена и усовершенствована, а в Windows 7 эта технология получила дальнейшее развитие (см. главу 5).

Меню *Избранное*

Одним из полезных новшеств, введенных в Windows 2000/XP, и, разумеется, сохранившимся в Windows Vista/7, является то, что пункт меню **Избранное** (Favorites) присутствует теперь повсюду, и Редактор реестра Regedit.exe — не исключение.

Все, кто часто выполняет поиск ключей и параметров в реестре, а также интенсивно занимается его редактированием, по достоинству оценили эту удобную функциональную возможность. С помощью меню **Избранное** (Favorites) можно создать список наиболее часто редактируемых ключей реестра, чтобы затем не повторять громоздкую процедуру поиска (рис. 3.26).

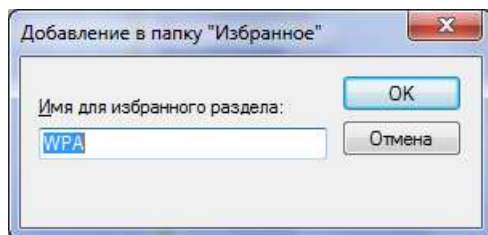


Рис. 3.26. Диалоговое окно **Добавление в папку "Избранное"**

Чтобы добавить ключ реестра в список **Избранное**, проделайте следующее:

1. Выделите ключ реестра, который требуется добавить в список **Избранное**.
2. В меню **Избранное** выберите команду **Добавить в избранное** (Add to Favorites).
3. В раскрывшемся диалоговом окне **Добавление в папку "Избранное"** (Add to Favorites) (см. рис. 3.26) согласитесь с именем ключа, предложенным по умолчанию, или введите новое имя в поле **Имя для избранного раздела** (Favorite name). Нажмите кнопку **ОК**, и ключ появится в списке **Избранное**.

Теперь вы в любой момент сможете быстро перейти к нужному ключу, выбрав его имя из списка **Избранное**. Удалить ключ реестра из списка **Избранное** очень просто — для этого достаточно выбрать в меню **Избранное** команду **Удалить из избранного** (Remove Favorite), а затем в открывшемся диалоговом окне выделить ключ, который требуется удалить, и нажать кнопку **ОК**.

Управление безопасностью реестра

Для управления безопасностью в редакторе реестра Windows XP/Vista/7 предусмотрена команда **Разрешения** (Permissions) из меню **Правка** (Edit), которая используется для редактирования прав доступа к ключам реестра и установки правил аудита на доступ к ним.

ПРИМЕЧАНИЕ

Как уже отмечалось ранее, в Windows NT/2000 этими возможностями обладала только утилита Regedt32.exe, в которой есть специальное меню **Безопасность** (Security), позволяющее задавать права доступа и устанавливать правила аудита (auditing rules). Начиная с Windows XP, эти функциональные возможности были перенесены в программу Regedit.exe.

ПРИМЕЧАНИЕ

В этой главе приводится лишь обзор функций управления безопасностью, а также общие инструкции о выполнении операций, необходимых для защиты реестра. Более подробная информация по этим вопросам содержится в *главе 9*.

Как и предыдущие версии Windows NT/2000/XP/Vista, Windows 7 обладает следующими возможностями по обеспечению защиты системы:

- ☐ доступ к ресурсам системы может жестко контролироваться;
- ☐ все операции по доступу к системным объектам могут регистрироваться в журнале безопасности;
- ☐ для доступа к системе требуется пароль, и операции доступа регистрируются в журнале безопасности.

Установка прав доступа к ключам реестра

Команда **Разрешения** (Permissions) открывает окно **Разрешения для <Имя_ключа>** (Permissions for the <Keyname>), предназначенное для просмотра и установки прав доступа к ключам реестра.

ВНИМАНИЕ!

Изменение прав доступа к ключу реестра может иметь серьезные последствия. Например, если вы установите права доступа типа `No access` на ключ, необходимый для конфигурирования сети с помощью утилиты **Центр управления сетями и общим доступом** (Network Control Center) из Панели управления (Control Panel), то это приложение работать не будет. Права полного доступа (full access) к ключам реестра должны иметь, как минимум, члены группы **Администраторы** (Administrators) и сама операционная система (Operating System). Такая установка прав доступа гарантирует возможность восстановления ключа реестра администратором.

Поскольку установка ограничений на права доступа к ключам реестра может иметь серьезные последствия, зарезервируйте эту меру для ключей, добавляемых с целью настройки отдельных индивидуально разработанных приложений или иных видов индивидуальной настройки.

СОВЕТ

Изменяя права доступа к ключу реестра, установите на этот ключ аудит, чтобы отслеживать, как минимум, неудачные попытки доступа. Минимально необходимая для этой цели информация по аудиту действий в отношении реестра будет приведена далее в этой главе (см. разд. *Аудит действий в отношении реестра*).

Команда **Разрешения** работает по такому же принципу, как и аналогичные команды Проводника по установке прав доступа к файлам и каталогам на разделах NTFS. Чтобы установить права доступа к конкретному ключу реестра, проделайте следующее:

1. Перед внесением изменений выполните резервное копирование тех ключей реестра, на которые будут устанавливаться права доступа.
2. Выделите ключ, на который собираетесь установить права доступа. После этого выберите из меню **Правка** команду **Разрешения**.
3. Откроется окно **Разрешения для <Имя_ключа>** (Permissions for <Keyname>), позволяющее указать права доступа к реестру (рис. 3.27).

ПРИМЕЧАНИЕ

В Windows 7 имеется большое количество усовершенствований, в том числе и по обеспечению безопасности. Тем не менее, основные типы прав доступа и принципы их установки схожи с теми, которые применялись в предыдущих версиях Windows NT/2000/XP/Vista.

Выберите имя пользователя или группы из списка в верхней части этого окна, а затем установите для него необходимый уровень доступа, отметив требуемое значение. Общее описание типов доступа (**Чтение** (Read), **Полный доступ** (Full Control) и **Особые разрешения** (Special Permissions)) приведено в табл. 3.3. Назначение прав доступа к выбранному ключу реестра выполняется следующим образом:

- в списке пользователей и групп, расположенном в верхней части этого окна, выделите имя пользователя или группы, для которых требуется установить права доступа к ключу реестра. Если этот пользователь или группа должны иметь возможность чтения содержимого ключа, но не должны иметь права сохранения внесенных изменений, установите флажок **Разрешить** (Allow) для варианта **Чтение** (Read);

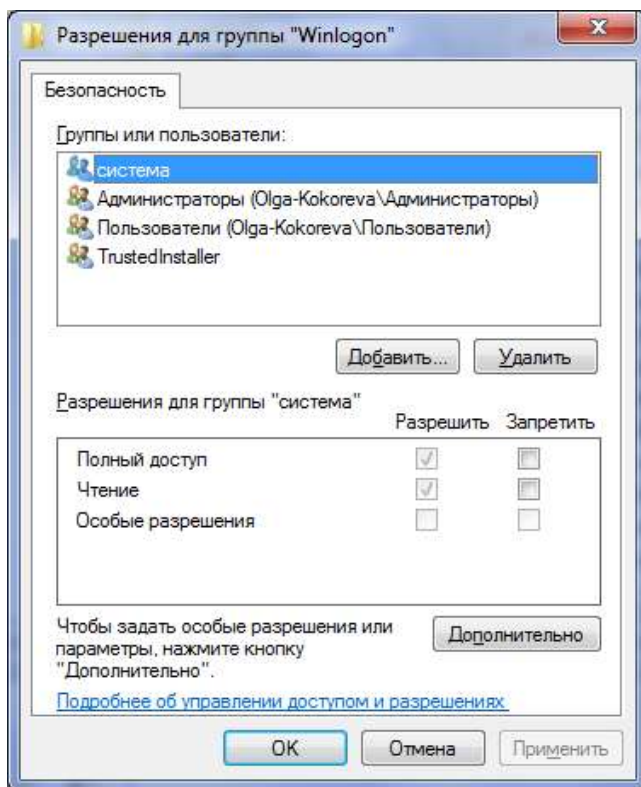


Рис. 3.27. Окно **Разрешения для <Имя_ключа>** позволяет указывать права доступа к ключу реестра

Таблица 3.3. Типы прав доступа к ключам реестра

Тип доступа	Описание
Чтение (Read)	Пользователи, внесенные в список имеющих права доступа к этому ключу, могут просматривать его содержимое, но не сохранять изменения
Полный доступ (Full Control)	Пользователи, внесенные в список имеющих права доступа к этому ключу, могут получать к нему доступ, редактировать его содержимое и изменять уровень прав доступа к нему
Специальные разрешения (Special Permissions)	Предоставляет пользователям, внесенным в список имеющих права доступа к этому ключу, индивидуально назначаемые комбинации прав доступа к избранному ключу и редактирования их. Подробное описание типов и комбинаций особых разрешений можно найти далее в этой главе

- если пользователь или группа должны иметь возможность открывать и редактировать выбранный ключ, а также присваивать права владельца этого ключа, установите флажок **Разрешить** (Enable) для варианта **Полный доступ** (Full access);
 - чтобы предоставить пользователю специальный тип доступа к ключу реестра, нажмите кнопку **Дополнительно** (Advanced).
4. Установите проверку на доступ к реестру (более подробная информация об установке аудита будет приведена далее в этой главе — см. разд. *Аудит действий в отношении реестра*). В течение некоторого времени тщательно наблюдайте за системой и убедитесь, что новые правила контроля доступа не оказывают отрицательного влияния на работу приложений.

Установка специальных комбинаций прав доступа

Для установки специальных типов доступа к ключам реестра Windows Vista и Windows 7 нажмите кнопку **Дополнительно** (Advanced) в диалоговом окне прав доступа к ключам реестра (см. рис. 3.27). При этом откроется окно **Дополнительные параметры безопасности для <Имя_ключа>** (Advanced Security Settings for <Keyname>), как на рис. 3.28.

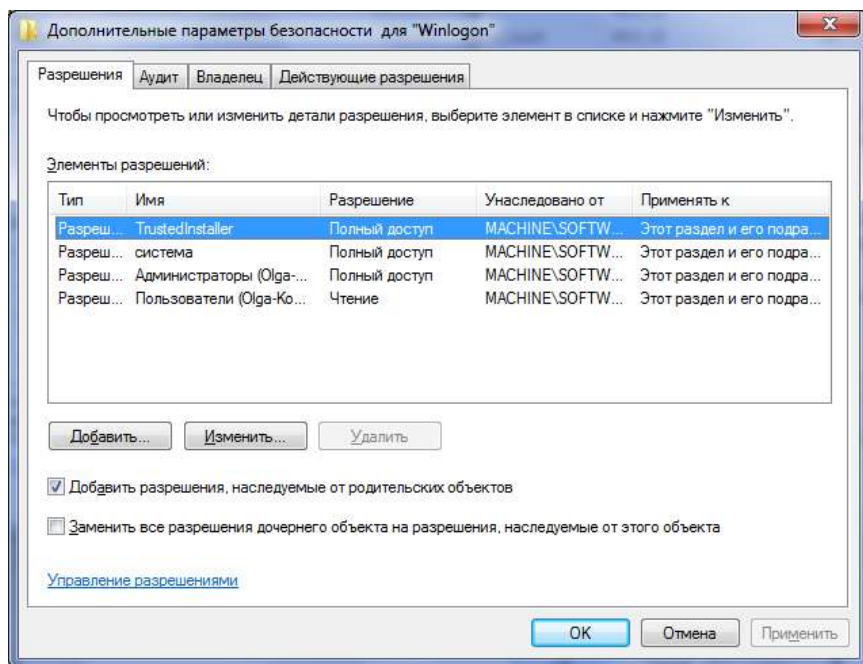


Рис. 3.28. Вкладка **Разрешения** окна **Дополнительные параметры безопасности для <Имя_ключа>**

В этом окне:

- ☐ если вы задаете права доступа для подключа реестра и хотите, чтобы он унаследовал права доступа, заданные для родительского ключа, установите флажок **Добавить разрешения, наследуемые от родительских объектов** (Include inheritable permissions for this object's parent);
- ☐ если вы устанавливаете права доступа к дочерним объектам и хотите, чтобы все они унаследовали права доступа, заданные для данного подключа, отметьте флажок **Заменить все наследуемые разрешения для всех потомков на новые наследуемые разрешения от этого объекта** (Replace all child object permission with inheritable permissions from this object).

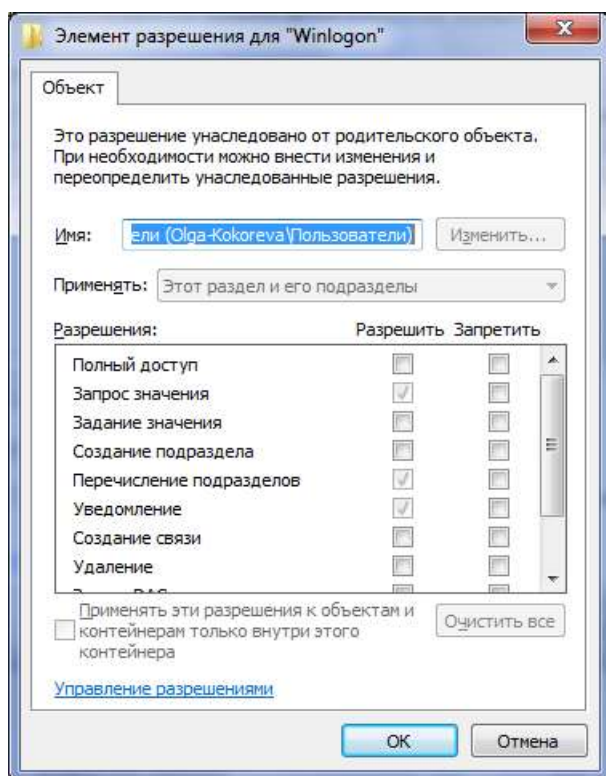


Рис. 3.29. Окно Элемент разрешения для <Имя ключа>

Двойным щелчком щелкните мышью на имени пользователя или группы, для которой вам необходимо установить специальный доступ (или же выберите имя), а затем нажмите кнопку **Изменить** (Edit). При этом откроется окно, представленное на рис. 3.29. В списке **Разрешения** (Permissions) выбо-

рите флажок **Разрешить** (Allow) или **Запретить** (Deny) в соответствии с типом доступа, который необходимо назначить или же отменить для указанного пользователя или группы. Перечень специальных опций доступа представлен в табл. 3.4. Обратите внимание, что этот список не отличается от аналогичного в Windows NT/2000/XP/Vista.

Таблица 3.4. Опции особых разрешений

Флажок	Описание
Запрос значения (Query Value)	Дает право чтения значимых элементов из ключа реестра
Задание значения (Set Value)	Дает право установить значимый элемент в ключе реестра
Создание подраздела (Create Subkey)	Дает право создавать подключи в выбранном ключе реестра
Перечисление подразделов (Enumerate Subkeys)	Дает право идентифицировать подключи выбранного ключа реестра
Уведомление (Notify)	Дает право установить аудит на ключи реестра
Создание связи (Create Link)	Дает право создавать символические ссылки в конкретном подключе реестра
Удаление (Delete)	Дает право удаления выделенного ключа
Запись DAC (Write DAC)	Дает право получать доступ к ключу и создавать/модифицировать для него список контроля доступа ACL (Access Control List)
Смена владельца (Write Owner)	Дает право присвоения прав владельца данного ключа
Чтение разрешений (Read Control)	Дает право просматривать параметры безопасности, установленные для данного ключа

Присвоение прав владельца ключа реестра

Как системный администратор, вы можете присвоить себе права владельца на ключ реестра и ограничить доступ к этому ключу. Пользователь, зарегистрировавшийся на компьютере с использованием учетной записи, принадлежащей к группе **Администраторы** (Administrators), может присвоить себе

права владельца на любой ключ реестра. Однако если вы имеете права владельца без прав доступа типа **Полный доступ** (Full Control), то вы не сможете вернуть ключ первоначальному владельцу, а в журнале безопасности появится соответствующая запись.

Чтобы присвоить права владельца на ключ реестра в Windows Vista/7:

1. Выделите ключ реестра, которому требуется присвоить права владельца.
2. Выберите в меню **Правка** (Edit) команду **Разрешения** (Permissions).
3. Нажмите кнопку **Дополнительно** (Advanced) и в открывшемся диалоговом окне (рис. 3.30) **Дополнительные параметры безопасности для <Имя_ключа>** (Advanced Security Settings for <Keyname>) перейдите на вкладку **Владелец** (Owner).
4. В списке **Изменить владельца на** (Change owner to) выберите нового владельца и нажмите кнопку **ОК**.

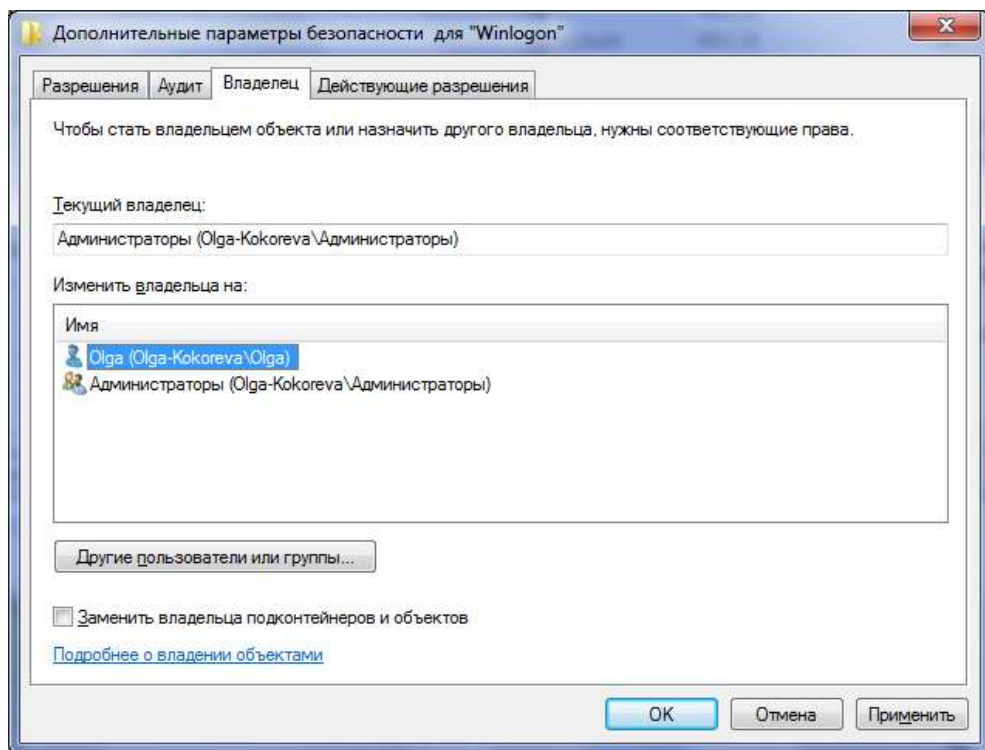


Рис. 3.30. Вкладка **Владелец**
окна **Дополнительные параметры безопасности для <Имя_ключа>**

Обратите внимание, что в Windows Vista/7 в этой области появилось дополнительное усовершенствование по сравнению с Windows XP, а именно — кнопка **Другие пользователи или группы** (Other users or groups). Нажатие на эту кнопку открывает окно **Выбор: "Пользователь" или "Группа"** (Select User or Group), предоставляющее существенно более широкие, чем в Windows XP, возможности поиска пользователей и групп и задания для них полномочий доступа и прав владельца (рис. 3.31).

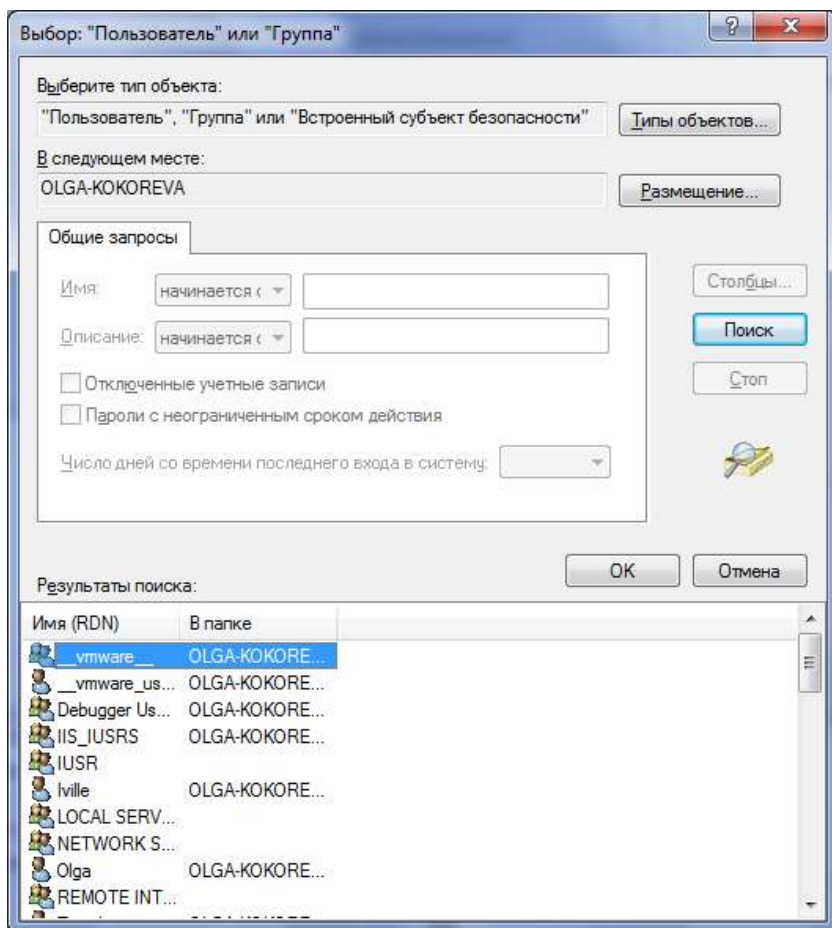


Рис. 3.31. Окно **Выбор: "Пользователь" или "Группа"** (Select User or Group)

ПРИМЕЧАНИЯ

Установите на вкладке **Владелец** в окне **Дополнительные параметры безопасности для <Имя_ключа>** (см. рис. 3.30) флажок **Заменить владельца суб-**

контейнеров и объектов (Replace owner on subcontainers and objects), если требуется также заменить владельца для всех вложенных объектов выбранного ключа. Замену владельца ключа реестра можно выполнить, только зарегистрировавшись в системе от имени администратора, или если прежний владелец явным образом предоставил вам права владельца на доступ к этому ключу.

Аудит действий в отношении реестра

Аудит представляет собой процесс, который операционные системы Windows NT/2000/XP и Windows Vista/7 используют для обнаружения и регистрации событий, связанных с системой безопасности. К таким событиям относятся, например, попытки создания или удаления системных объектов, а также попытки получения доступа к таким объектам. Обратите внимание, что в объектно-ориентированных системах в качестве объекта может рассматриваться все, что угодно — файлы, папки, ключи реестра и т. д. Все эти и другие подобные им события регистрируются в файле, известном под названием *журнала безопасности* (security log). Более подробно мониторинг системных событий будет рассматриваться в *главе 9*. Здесь же отметим, что в системах, более ранних, нежели Windows Vista, аудит в системе по умолчанию не активизировался, поэтому прежде, чем приступить к установке аудита на ключи реестра, требовалось предварительно активизировать аудит системных событий.

Начиная с Windows Vista эта ситуация поменялась — аудит по умолчанию уже активизирован, и отслеживание событий ведется, в чем несложно убедиться, просмотрев журнал безопасности. Чтобы сделать это, раскройте окно Панели управления и выберите опции **Система и безопасность** (System and Security), **Система** (System), **Администрирование** (Administrative Tools). Затем выберите опцию **Просмотр событий** (Event Viewer)² и раскройте журнал **Безопасность** (Security), как показано на рис. 3.32. Как видите, регистрация системных событий, связанных с работой подсистемы безопасности, активизирована по умолчанию.

Поэтому, когда вы впервые откроете окно редактора локальной политики безопасности (рис. 3.33)³, пусть вас не вводит в заблуждение установка значения **Нет аудита** (No auditing) на политики **Аудит событий входа в систему** (Audit account logon events) и **Аудит входа в систему** (Audit logon events).

² Наиболее эффективный и быстрый способ — раскройте меню **Пуск** (Start) и введите команду `eventvwr.msc` в поле поиска, расположенное в нижней части меню.

³ Чтобы открыть окно локальной политики безопасности (Local Security Policy), действуйте точно так же, как делали бы это в Windows Vista. Откройте окно **Панель управления** (Control Panel), затем выберите опции **Система и безопасность** (System and Security) | **Администрирование** (Administrative Tools) | **Локальная политика безопасности** (Local Security Policy). Но наиболее эффективный и быстрый способ — раскройте меню **Пуск** (Start) и введите команду `secpol.msc` в поле поиска, расположенное в нижней части меню.

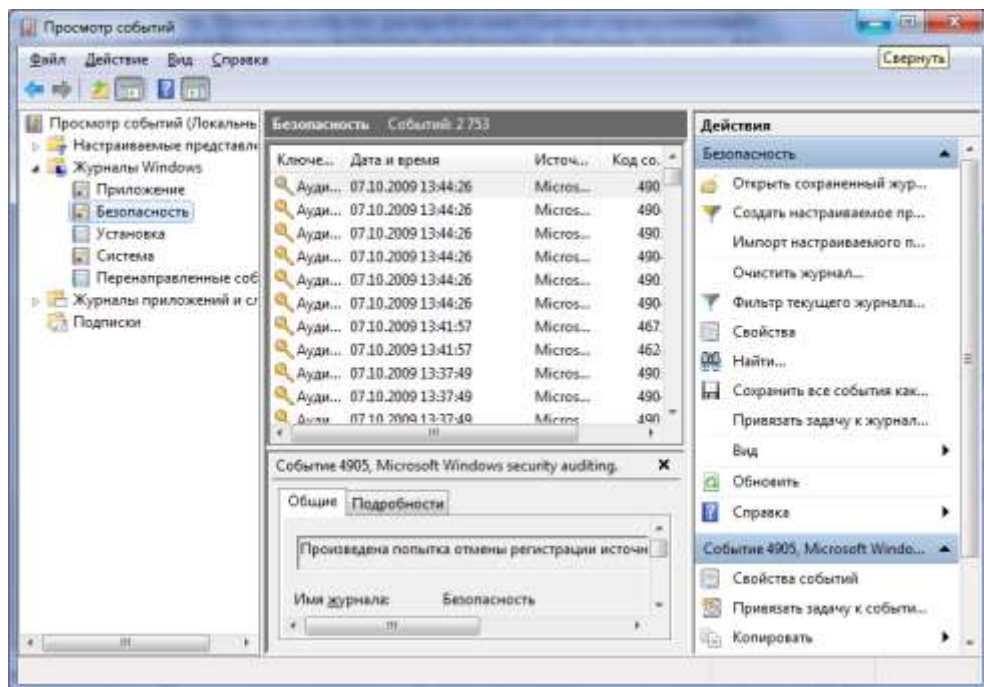


Рис. 3.32. В Windows Vista и Windows 7 аудит системных событий активизируется по умолчанию

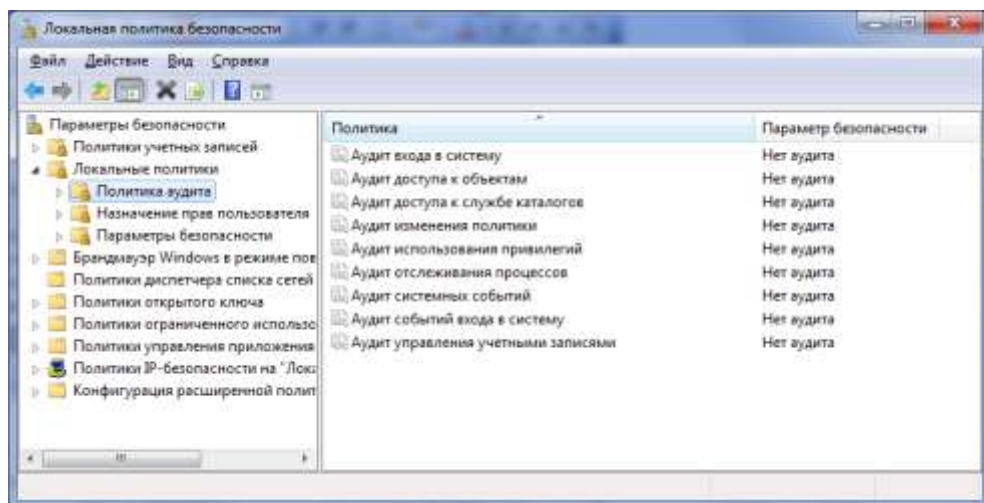


Рис. 3.33. Редактирование политики аудита

Рассмотрим, каким образом можно установить проверку действий в отношении ключей реестра. В частности, в литературе можно встретить рекомендации по установке аудита на следующие ключи:

- ☐ ключи, о которых известно, что пользователи и приложения получают к ним доступ и вносят изменения;
- ☐ созданные вами индивидуальные ключи реестра, которые вы, как разработчик, хотите протестировать.

Чтобы установить аудит на ключи реестра Windows 2000/XP/Vista/7:

1. Выделите ключ, на который требуется установить аудит.
2. Выберите в меню **Правка (Edit)** команду **Разрешения (Permissions)**, нажмите кнопку **Дополнительно (Advanced)** и в открывшемся диалоговом окне **Дополнительные параметры безопасности для <Имя_ключа>** (Advanced Security Settings for <Keyname>) перейдите на вкладку **Аудит (Auditing)** (рис. 3.34).

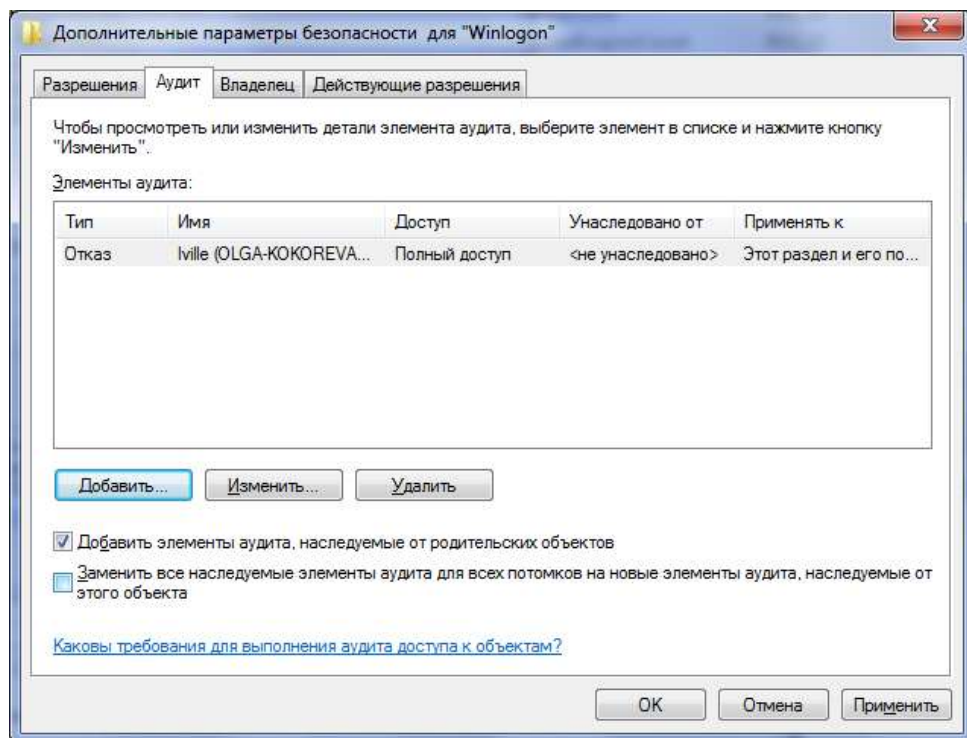


Рис. 3.34. Вкладка **Аудит** окна **Дополнительные параметры безопасности для <Имя_ключа>**

3. Если аудит на выбранный ключ устанавливается впервые, то список **Элементы аудита** (Auditing Entries) будет пуст. Нажмите кнопку **Добавить** (Add), расположенную непосредственно под этим списком, выберите из предложенного списка пользователей и группы, на действия которых требуется установить аудит, и добавьте их в список.
4. Для установки аудита на действия конкретного пользователя или группы выделите его имя в списке **Элементы аудита** (Auditing Entries), нажмите кнопку **Изменить** (Edit) и в раскрывшемся диалоговом окне (рис. 3.35) в списке **Доступ** (Access) установите флажки **Успех** (Successful) и/или **Отказ** (Failed) для вариантов доступа, на которые требуется установить аудит.
5. Допустимые опции аудита представлены в табл. 3.5.

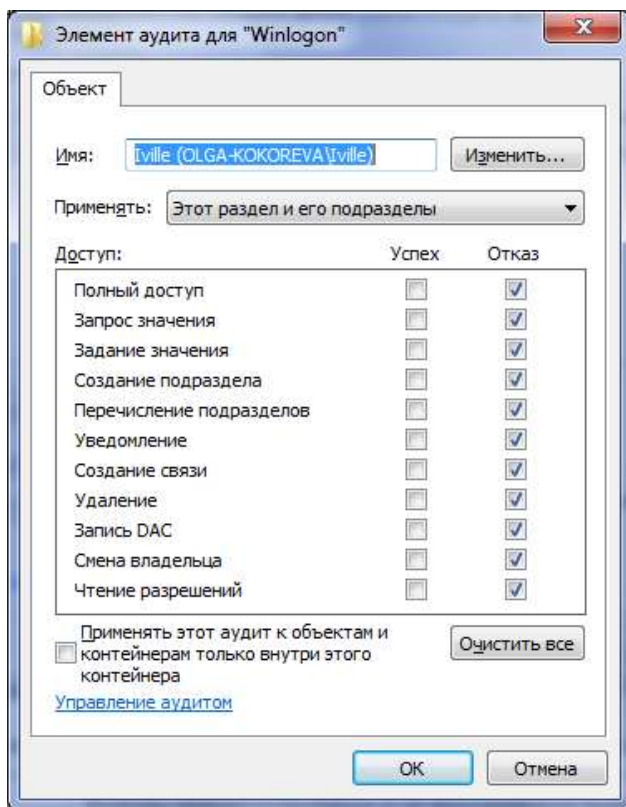


Рис. 3.35. Окно **Элемент аудита для <Имя_ключа>** (Auditing Entry for <Keyname>)

Таблица 3.5. Типы опций аудита на действия в отношении ключей реестра

Опция аудита	Контролирует успешные или неуспешные попытки
Запрос значения (Query Value)	Открытие ключа с правом запроса значения (Query Value)
Задание значения (Set Value)	Открытие ключа с правом установки значения (Set Value)
Создание подраздела (Create Subkey)	Открытие ключа с правом создания подключей (Create Subkeys)
Перечисление подразделов (Enumerate Subkeys)	Открытие ключа с правом перечисления подключей (Enumerate Subkeys). Эта опция устанавливает контроль за событиями, которые открывают ключи и пытаются получить список подключей, содержащихся в открытом ключе
Уведомление (Notify)	Открытие ключа с правом уведомления (Notify)
Создание связи (Create Link)	Открытие ключа с правом создания ссылок (Create Link)
Удаление (Delete)	Удаление ключа
Запись DAC (Write DAC)	Попытка определения пользователей, имеющих доступ к ключу
Чтение разрешений (Read Control)	Поиск владельца ключа

ПРИМЕЧАНИЕ

Для установки аудита на ключи реестра необходимо зарегистрироваться в системе от имени администратора или члена группы **Администраторы** (Administrators). Если компьютер участвует в работе сети, то параметры политики безопасности, установленные для сети, также могут не позволить вам выполнить установку аудита на ключи реестра.

Для просмотра результатов аудита выполните команду **Все программы | Администрирование | Управление компьютером** (All Programs | Administrative Tools | Computer Management) меню **Пуск**. Разверните расположенное в левой панели окна MMC дерево консоли, выбрав опции **Служебные программы | Просмотр событий | Безопасность** (System Tools | Event Viewer | Security Log). В правой панели появится список событий системы безопасности.

Команды, содержащиеся в меню **Окно** (Window) и **Справка** (Help), являются стандартными для большинства приложений Windows.

Работа с реестром с помощью утилит командной строки

Как уже говорилось ранее в этой главе, кроме Редактора реестра Regedit.exe, имеющего графический пользовательский интерфейс, в комплект поставки Windows Vista и Windows 7 входят еще две утилиты командной строки, которые также предназначены для работы с реестром: Reg.exe и Regini.exe. Эти утилиты менее известны, нежели традиционный редактор реестра, но они чрезвычайно полезны для системных администраторов, поскольку могут использоваться в командных сценариях при управлении большим количеством компьютеров.

Утилита Reg.exe

Утилита Reg.exe, которая ранее поставлялась в составе программного продукта Resource Kit, начиная с Windows XP входит в комплект поставки операционной системы. Она позволяет добавлять, редактировать, удалять и искать ключи и значимые элементы реестра, производить их резервное копирование и восстановление, а также выполнять над ними другие операции. Утилита Reg.exe может использоваться из командной строки или применяться в командном файле. Она позволяет выполнять операции над реестрами как локального, так и удаленных компьютеров. Одним из ее применений является резервное копированию ключей и ульев реестра.

Утилита Reg.exe поддерживает следующий общий синтаксис командной строки:

```
reg <command> <RegistryPath> <parameters>
```

Здесь:

- ❑ *<command>* — одна из поддерживаемых команд, список которых приведен в табл. 3.6;
- ❑ *<RegistryPath>* — путь к элементу или ключу реестра в формате [ROOTKEY\]Key. При этом параметр ROOTKEY указывает корневой ключ реестра, который содержит ключ, подлежащий сохранению (по умолчанию этот параметр получает значение HKEY_LOCAL_MACHINE). Корневой ключ реестра может указываться в сокращенном формате, с использованием одной из приведенных аббревиатур:
 - HKEY_LOCAL_MACHINE — HKLM;
 - HKEY_CURRENT_USER — HKCU;
 - HKEY_CLASSES_ROOT — HKCR;
 - HKEY_CURRENT_CONFIGURATION — HKCC;
- ❑ *<parameters>* — список необязательных параметров, зависящих от конкретной команды.

Таблица 3.6. Команды утилиты reg.exe

Команда	Описание
add	Добавляет в состав реестра новый подключ или параметр. Действует по аналогии с командой Создать (Add) из меню Правка (Edit) программы Regedit.exe
delete	Удаляет из реестра подклкюхи или параметры. Действует по аналогии с командой Удалить (Delete) из меню Правка программы Regedit.exe
query	Отображает данные в составе подклкюха или значимого параметра
compare	Выполняет сравнение подклкючей и параметров реестра. Аналогичной возможности в программе Regedit.exe нет
copy	Копирует подклкюх в состав другого подклкюха. Аналогичной возможности в программе Regedit.exe нет
save	Сохраняет копию содержимого указанных подклкючей и параметров в формате улья реестра (т. е. в двоичном формате). Действует аналогично команде Экспорт (Export) из меню Файл (File) программы Regedit.exe, причем экспортируемая часть реестра сохраняется в формате улья
restore	Выполняет запись подклкючей, сохраненных в формате улья (двоичном формате) обратно в реестр. Действует аналогично команде Импорт (Import) из меню Файл программы Regedit.exe, причем в реестр импортируется файл, сохраненный в формате улья
load	Записывает подклкюхи и параметры, сохраненные в двоичном формате, в состав другого подклкюха реестра. Действует аналогично команде Загрузить куст (Load Hive) из меню Файл (File) программы Regedit.exe
unload	Удаляет раздел реестра, созданный командой <code>reg load</code> . Действует аналогично команде Выгрузить куст (Unload Hive) из меню Файл программы Regedit.exe
export	Создает копию указанных подклкючей, параметров и их значений в формате REG-файла (текстовом формате). Действует аналогично команде Экспорт (Export) из меню Файл программы Regedit.exe
import	Импортирует в реестр содержимое предварительно сохраненного REG-файла. Действует аналогично команде Импорт (Import) из меню Файл (File) программы Regedit.exe
flags	Новая команда, появившаяся в Windows Vista в связи с введением функции виртуализации реестра. Эта команда устанавливает или сбрасывает флаги виртуализации для указанного подклкюха. В программе Regedit.exe аналогичная возможность отсутствует

Команда *reg add*

Эта команда используется для добавления в реестр новых ключей и параметров. Она поддерживает следующий синтаксис командной строки:

```
reg add KeyName [/v ValueName | /ve] [/t Type] [/s Separator] [/d Data] [/f]
```

Значения параметров описаны в табл. 3.7.

Таблица 3.7. Опции командной строки команды REG ADD

Параметр	Описание
<i>KeyName</i>	Полный путь к ключу реестра. Для корневых ключей используются сокращения HKCR, HKCU, HKLM и HKU. Чтобы указать реестр удаленного компьютера, параметр <i>KeyName</i> следует указывать в формате <code>\\<ComputerName>\[ROOTKEY\] Key</code> , где <code>\\<ComputerName></code> — имя или IP-адрес удаленного компьютера. Если параметр <code>\\ComputerName\</code> пропущен, то по умолчанию операция будет произведена над локальным реестром. Следует иметь в виду, что на удаленных компьютерах доступны только ключи HKLM и HKU
<i>/v ValueName</i>	Добавляет новый параметр реестра или модифицирует значение уже существующего параметра
<i>/ve</i>	Используется при необходимости выполнения операции над параметром По умолчанию (Default) в составе указанного ключа реестра
<i>/t Type</i>	Задаёт тип данных для нового параметра реестра. Допускается использование типов данных REG_BINARY, REG_DWORD, REG_SZ, REG_MULTI_SZ и т. д. По умолчанию используется тип REG_SZ
<i>/s Separator</i>	Указывает символ-разделитель, использующийся для разделения строк в параметрах типа REG_MULTI_SZ. По умолчанию используется символ /0
<i>/d Data</i>	Значение, присваиваемое параметру
<i>/f</i>	Задаёт принудительную перезапись существующих значений (без вывода запроса на подтверждение)

Команда `reg add` предоставляет быстрый и удобный метод для добавления в реестр новых ключей или модификации уже существующих ключей. Например, чтобы добавить в состав ключа `HKLM\Software\` новый ключ `HackerApp`, дадим следующую команду:

```
reg add HKLM\Software\HackerApp
```

Теперь, чтобы добавить в состав этого ключа параметр `Hacked` и присвоить ему двоичное значение `0001`, дадим следующую команду:

```
reg add HKLM\Software\HackerApp /v Hacked /t REG_BINARY /d 0001
```


Команда *reg delete*

Команда `reg delete` используется для удаления из состава реестра ключей и параметров. Она использует следующий синтаксис командной строки:

```
reg delete KeyName [/v ValueName | /ve | /va] [/f]
```

Опции командной строки *KeyName*, */v ValueName*, */ve* и */f* имеют точно такой же смысл, как аналогичные опции команды `reg add`. При использовании опции */va* будут удалены все параметры, содержащиеся в составе указанного ключа реестра.

Команды утилиты *reg.exe* для резервного копирования и восстановления реестра из командной строки

Как уже говорилось ранее в этой главе, Редактор реестра (приложение *Regedit.exe*) предоставляет возможности резервного копирования и восстановления реестра с помощью команд **Экспорт** (Export) и **Импорт** (Import) из меню **Файл** (File). При этом подчеркивалась разница между импортом/экспортом файлов текстового формата (REG-файлов) и файлов двоичного формата (формат улья реестра). Напомним, что после импорта в реестр REG-файла все параметры реестра, указанные в импортируемом файле, будут соответствующим образом изменены. При этом все новые ключи и параметры, созданные в реестре уже после создания REG-файла, останутся в неприкосновенности. Если же вы импортируете обратно в реестр файл, сохраненный в формате улья, то все содержимое конкретной ветви реестра будет замещено содержимым импортируемого файла. Таким образом, все новые подключи и параметры, созданные в составе этой ветви реестра уже после ее экспорта в формате улья, будут удалены.

Аналогичные возможности предоставляет и утилита *Reg.exe*:

- ❑ для экспорта ветви реестра в формате файла улья используется командная строка следующего вида:

```
reg save <KeyName> <FileName> [/y]
```

Если используется опция */y*, то существующий файл с именем *FileName* будет перезаписан без вывода запроса на подтверждение;

- ❑ для импорта в реестр файла, экспортированного в формате улья, используется следующая команда:

```
reg restore <KeyName>
```

ПРИМЕЧАНИЕ

Формат улья является предпочтительным, если ваша цель — именно создание резервной копии, поскольку при восстановлении вы действительно восстановите работоспособную копию реестра и, таким образом, сможете решить возникшую проблему.

Для экспорта и импорта ветвей реестра в формате REG-файлов используются командные строки следующего вида:

- ❑ `reg export <KeyName> <FileName>` — для экспорта;
- ❑ `reg import <FileName>` — для импорта.

ПРИМЕЧАНИЕ

REG-файлы тоже могут использоваться для резервного копирования, но, как уже упоминалось, в этом случае следует иметь в виду, что ключи и параметры, не указанные в REG-файле, при последующем импорте останутся в неприкосновенности. Поэтому если причиной неполадок являются именно такие ключи и значения, то проблему вы этим не решите. Использование REG-файлов рекомендуется для распространения небольших модификаций реестра.

Команды `reg load` и `reg unload` абсолютно аналогичны командам **Загрузить куст** (Load Hive) и **Выгрузить куст** (Unload Hive) из меню **Файл** программы Regedit.exe, а синтаксис командной строки абсолютно аналогичен используемому командами `reg export` и `reg import`.

Команда `reg query`

Команда `reg query` выводит список подключей реестра, вложенных в указанный ключ на следующем уровне иерархии реестра. Она использует следующий синтаксис командной строки:

```
reg query <KeyName> [{/v <ValueName> | /ve}] [/s] [/se <Separator>] [/f <Data>]
[/{k | /d}] [/c] [/e] [/t <Type>] [/z]
```

Опции командной строки для этой команды кратко описаны в табл. 3.8.

Таблица 3.8. Опции командной строки команды RegQuery

Параметр	Описание
<KeyName>	Этот параметр используется всеми командами одинаково. Подробное описание см. в табл. 3.7
/v <ValueName>	Указывает имя параметра реестра, содержимое которого требуется просмотреть. Если этот параметр пропущен, то будут возвращены имена всех параметров реестра, содержащихся в составе ключа <KeyName>. Если используется опция /f, то параметр <ValueName> будет не обязательным
/ve	Выполняет запрос на вывод имен параметров, которые являются пустыми
/s	Выполняет рекурсивный запрос по всем подключам и параметрам указанной ветви реестра

Таблица 3.8 (окончание)

Параметр	Описание
/se <Separator>	Указывает символ-разделитель, использующийся для разделения строк в параметрах типа REG_MULTI_SZ. По умолчанию используется символ /0
/f <Data>	Задаёт данные или шаблон для поиска. Если строка-шаблон содержит пробелы, она должна быть заключена в кавычки. Если параметр пропущен, то в качестве шаблона для поиска используется символ (*)
/k	Дает указание выполнять поиск только по именам ключей
/d	Дает указание выполнять поиск только по данным
/c	Дает указание выполнять поиск с учетом регистра символов. По умолчанию поиск к регистру символов нечувствителен
/e	Дает указание возвращать лишь точные совпадения. По умолчанию будут возвращены все вхождения
/t <Type>	Указывает типы данных, по которым должен выполняться поиск. Допустимыми являются значения REG_SZ, REG_MULTI_SZ, REG_EXPAND_SZ, REG_DWORD, REG_BINARY, REG_NONE. Если тип данных не указан, будет выполняться поиск по данным всех типов
/z	Дает указание включать в результаты поиска числовой эквивалент типа данных реестра

Команда reg compare

Команда reg compare выполняет сравнение указанных ключей или параметров реестра. Как уже говорилось, в приложении Regedit.exe эквивалента для этой команды не существует. Команда использует следующий синтаксис командной строки:

reg compare <KeyName1> <KeyName2> [{/v ValueName | /ve}] [{/oa | /od | /os | on}] [/s]
Опции командной строки для этой команды вкратце перечислены в табл. 3.9.

Таблица 3.9. Опции командной строки команды Reg compare

Параметр	Описание
<KeyName1>	Указывает полный путь к первому подключу, участвующему в операции сравнения. Для корневых ключей используются сокращения HKCR, HKCU, HKLM и HKU. Чтобы указать реестр удаленного компьютера, параметр KeyName следует указывать в формате \\<ComputerName>\[ROOTKEY\] Key, где \\<ComputerName> — имя или IP-адрес удаленного компьютера. Если параметр \\<ComputerName>\ пропущен, то по умолчанию операция будет произведена над локальным реестром. Следует иметь в виду, что на удаленных компьютерах доступны только ключи HKLM и HKU

Таблица 3.9 (окончание)

Параметр	Описание
<KeyName2>	Указывает путь ко второму подключу, участвующему в операции сравнения. Для корневых ключей используются сокращения HKCR, HKCU, HKLM и HKU. Чтобы указать реестр удаленного компьютера, параметр <i>KeyName</i> следует указывать в формате \\<ComputerName>\[ROOTKEY\]Key, где \\<ComputerName> — имя или IP-адрес удаленного компьютера. Если параметр \\<ComputerName>\ пропущен, то по умолчанию операция будет произведена над локальным реестром. Следует иметь в виду, что на удаленных компьютерах доступны только ключи HKLM и HKU
/v <ValueName>	Указывает имя сравниваемого параметра в составе подключа
/ve	Указывает, что сравнению подлежат только значимые элементы с именем null
[{/oa /od /os on}]	Указывает, как следует отображать результаты сравнения. Использоваться может только одна из этих опций. По умолчанию применяется опция /od
/oa	Указывает все отличия и все совпадения. По умолчанию отображаются только отличия
/od	Указывает только отличия. Эта опция используется по умолчанию
/os	Указывает только совпадения. По умолчанию отображаются только отличия
/on	Не указывает ни совпадений, ни отличий. По умолчанию отображаются только отличия
/s	Задаёт рекурсивное сравнение всех подключей и параметров

Команда reg flags

Как уже говорилось ранее в этой главе, команда *flags* — новая команда, которая впервые появилась в Windows Vista в связи с введением функции UAC и виртуализации реестра. Разумеется, присутствует она и в Windows 7. Команда *reg flags* устанавливает или сбрасывает флаги виртуализации для указанного подключа (в программе Regedit.exe аналогичная возможность отсутствует). Чтобы понять смысл этой команды, необходимо вернуться к более подробному рассмотрению виртуализации реестра.

Несколько слов о виртуализации реестра

Как говорилось уже неоднократно, функция UAC (User Account Control, контроль учетных записей пользователей) была введена с тем, чтобы сделать

работу с правами обычного пользователя общепринятой практикой. Дело в том, что при работе от имени учетной записи обычного пользователя (а не администратора) снижается риск случайного или преднамеренного внесения нежелательных изменений в настройку системы. Даже если на компьютер проникает вредоносная программа, изменение параметров системной безопасности или отключения антивирусного ПО окажется затруднено, и в любом случае ущерб от работы вредоносной программы будет смягчен.

До появления Windows Vista многие приложения разрабатывались таким образом, чтобы получать доступ и изменять любой файл, параметр реестра или настройку операционной системы. С появлением Windows Vista ситуация изменилась, и теперь Microsoft рекомендует, чтобы приложения, которые действительно должны работать с административными правами, пользовались защищенными областями файловой системы и реестра. Так, для хранения исполняемых файлов и вспомогательных данных приложений, исполняющихся с административными правами, должны создаваться подкаталоги в каталоге `%ProgramFiles%`, а для хранения параметров таких приложений должен использоваться ключ реестра `HKEY_LOCAL_MACHINE\Software`.

Чтобы обеспечить возможность работы старых приложений, необоснованно стремящихся получить доступ к этим областям при работе от имени учетной записи обычного пользователя, Windows Vista и Windows 7 реализуют т. н. *виртуализацию* файловой системы и пространства имен реестра. Суть ее заключается в том, что в ситуациях, когда приложение изменяет данные в частях файловой системы или реестра, общих для всей системы, и эта операция проходит неудачно из-за отказа в доступе, Windows перенаправляет операцию в область соответствующего пользователя. Когда приложение считывает данные из системно-глобального размещения, Windows сначала проверяет данные в области пользователя и, если их там не находит, разрешает чтение из глобального размещения.

Чтобы Windows трактовала приложение, как наследуемое, оно должно подпадать под следующее определение:

процесс этого приложения 32-разрядный (а не 64-разрядный), выполняется не с административными правами и не имеет файла манифеста, указывающего, что он написан для Windows Vista/7.

Если приложение подпадает под это определение, то для него осуществляется виртуализация, причем делается это прозрачно для пользователя. Если же приложение действительно должно выполнять запись именно в защищенные области файловой системы и реестра, то UAC потребует ввода пароля администратора.

Чтобы просмотреть статус виртуализации процессов, запустите Диспетчер задач Windows (Windows Task Manager)⁴, перейдите на вкладку **Процессы** (Processes) и из меню **Вид** (View) выберите команду **Выбрать столбцы** (Select columns). Добавьте к отображаемым столбцам столбец **Виртуализация контроля учетных записей** (User Account Control (UAC) Virtualization), как показано на рис. 3.36.

Как видите, для большинства компонентов Windows Vista/7, включая Диспетчер окон рабочего стола (Dwm.exe), подсистему клиент-серверной среды выполнения (Csrss.exe) и Проводник, виртуализация отключена, поскольку они либо обладают манифестом Windows Vista/7, либо выполняются с административными правами и, следовательно, не допускают виртуализацию (рис. 3.37).

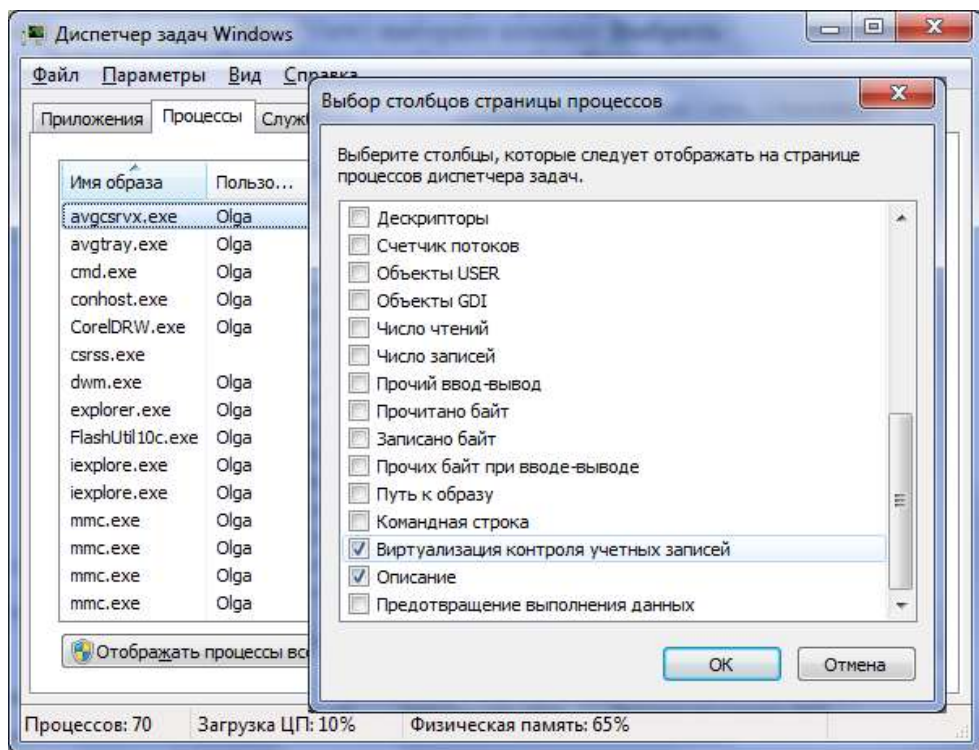


Рис. 3.36. Выбор столбца **Виртуализация контроля учетных записей** (User Account Control (UAC) Virtualization) для просмотра статуса виртуализации процессов через Диспетчер задач Windows

⁴ Самый быстрый и удобный способ запуска Диспетчера задач в Windows 7 — нажатие клавиатурной комбинации <Ctrl>+<Shift>+<Esc>.

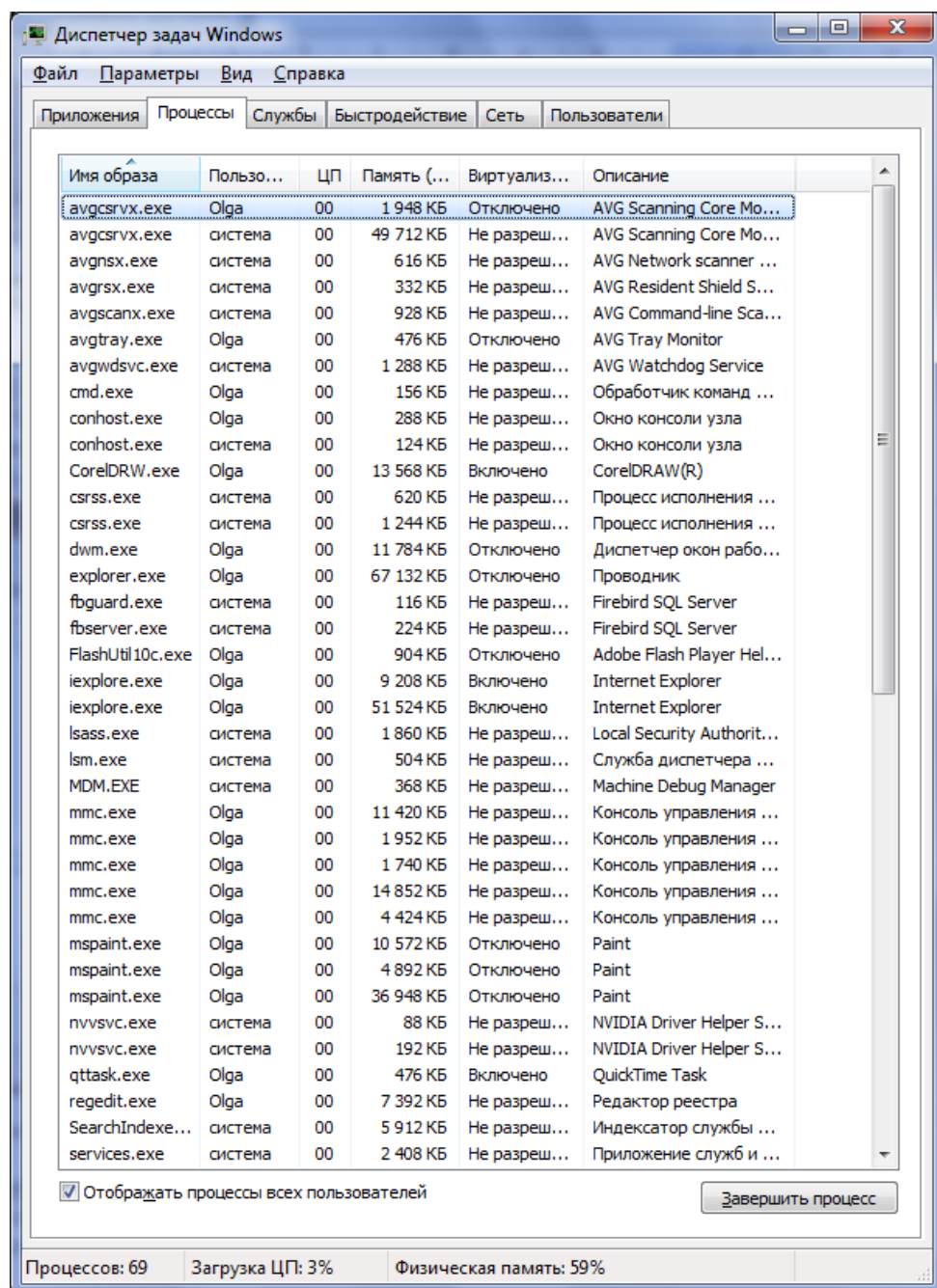


Рис. 3.37. Просмотр статуса виртуализации процессов через Диспетчер задач Windows (Windows Task Manager)

Если говорить о реестре, то в нем виртуализована большая часть ключа `HKEY_LOCAL_MACHINE\Software`, хотя есть и исключения, к числу которых относятся разделы `HKLM\Software\Microsoft\Windows`, `HKLM\Software\Microsoft\Windows NT` и `HKLM\Software\Classes`.

Виртуализуются только ключи, которые часто изменяются устаревшими приложениями, но не вызывают проблем совместимости или взаимодействия. Windows перенаправляет операции изменения виртуализуемых разделов устаревшим приложением в виртуальный корневой раздел реестра пользователя в разделе `HKEY_CURRENT_USER\Software\Classes\VirtualStore`. Этот раздел расположен в файле `%LocalAppData%\Microsoft\Windows\UsrClass.dat` в улье `Classes` пользователя, который, как и все прочие данные виртуализованных файлов, с перемещаемым профилем пользователя не перемещается.

Статус виртуализации раздела хранится в виде флага `REG_KEY_DONT_VIRTUALIZE` в самом разделе. С помощью служебной программы `Reg.exe` можно просмотреть этот флаг, а также два других флага, связанные с виртуализацией, — `REG_KEY_DONT_SILENT_FAIL` и `REG_KEY_RECURSE_FLAG`. Если флаг `REG_KEY_DONT_SILENT_FAIL` установлен и раздел не виртуализован (установлен флаг `REG_KEY_DONT_VIRTUALIZE`), устаревшему приложению, которому иначе было бы запрещено выполнять операции с разделом, предоставляется любой уровень доступа к разделу, который имеет пользователь, вместо доступа, затребованного приложением. Флаг `REG_KEY_RECURSE_FLAG` указывает, наследуют ли новые разделы флаги виртуализации родительского раздела, а не только флаги, применяемые по умолчанию.

Синтаксис команды `reg flags`

Итак, для просмотра флагов виртуализации и управления ими и предназначена команда `reg flags`. Она использует следующий синтаксис командной строки:

```
reg flags <KeyName> [QUERY | SET [DONT_VIRTUALIZE] [DONT_SILENT_FAIL] [RECURSE_FLAG]]
```

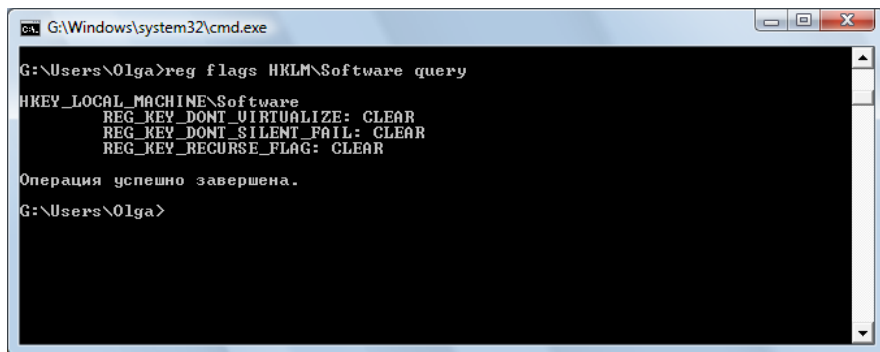


Рис. 3.38. Просмотр флагов виртуализации с помощью команды `reg flags`

Здесь `KeyName` — имя ключа реестра в формате `HKLM\Software"[\subkey]` (ограничивается только ключом `HKLM\Software` на локальном компьютере). Для просмотра флагов виртуализации служит опция `QUERY`, а для установки — опция `SET`. Имена флагов используются с параметром `SET`, причем указанные флаги будут установлены, а пропущенные — удалены. Пример вывода программы `reg flags` показан на рис. 3.38.

Утилита *Regini.exe*

Программа `Regini.exe` представляет собой утилиту командной строки, которая ранее, как и утилита `Reg.exe`, поставлялась как часть программного продукта `Resource Kit` для соответствующих версий операционных систем `Windows NT`. Однако, начиная с `Windows Vista`, эта программа теперь тоже входит в стандартный комплект поставки операционной системы. `Regini.exe` позволяет изменять права доступа пользователей к определенным ветвям реестра. Она особенно удобна для системных администраторов, которые хотят автоматизировать свою работу путем написания командных сценариев.

Синтаксис утилиты *Regini.exe*

Принцип работы программы основан на сценарии, который определяет ветви реестра, права для которых должны быть изменены. Команда использует следующий синтаксис командной строки:

```
regini.exe [-m \\<machinename> | -h <hivefile> <hiveroot>]
           [-i n] [-o OutputWidth]
           [-b] TextFile(s)
```

Здесь:

- ❑ `\\<machinename>` — имя компьютера в формате `UNC` (`Universal Naming Convention`). Разумеется, если вам необходимо изменить права доступа к ветвям реестра локального компьютера, использование опции `-m \\<machinename>` не обязательно;
- ❑ опция `-i n` задает интервалы табуляции экранного вывода, а опция `-o OutputWidth` — ширину экранного вывода (по умолчанию — соответствует ширине окна командной строки);
- ❑ опция `-b TextFile(s)` задает один или несколько командных скриптовых файлов, в которых каждая строка имеет формат `Registry\hive\<остальная часть ветви реестра> [права доступа]`.

Немного о типах прав доступа

Рассмотрим поподробнее опцию: `-h <hivefile> <hiveroot>` — имя улья или корневого ключа, права доступа к которым требуется изменить. При этом вместо указания корневого раздела ветви реестра, необходимо указывать следующие обозначения (при помощи данной программы можно обращаться только к соответствующим корневым разделам реестра):

- ❑ `HKEY_LOCAL_MACHINE` — если ветвь начинается с данного корневого раздела, его нужно заменить строкой `\Registry\Machine`;
- ❑ `HKEY_USERS` — если ветвь начинается с данного корневого раздела, его нужно заменить строкой `\Registry\Users`;
- ❑ `HKEY_CURRENT_USER` — если ветвь начинается с данного корневого раздела, его нужно заменить строкой `\Registry\User\"User_SID"`.

Это означает, что каждая строка в сценарии должна соответствовать следующему формату:

`\Registry\hive\<остальная часть ветви реестра>[права доступа]`

Параметры `[права доступа]` представляют собой числа, которые одновременно определяют группу пользователей и права доступа, которые ей предоставляются. Типы прав доступа представляются следующими числами:

- ❑ 1 — Administrators: Full Control;
- ❑ 2 — Administrators: Read Access;
- ❑ 3 — Administrators: Read and Write Access;
- ❑ 4 — Administrators: Read, Write and Delete Access;
- ❑ 5 — Creator: Full Control;
- ❑ 6 — Creator: Read and Write Access;
- ❑ 7 — World: Full Control;
- ❑ 8 — World: Read Access;
- ❑ 9 — World: Read and Write Access;
- ❑ 10 — World: Read, Write and Delete Access;
- ❑ 11 — Power Users: Full Control;
- ❑ 12 — Power Users: Read and Write Access;
- ❑ 13 — Power Users: Read, Write and Delete Access;
- ❑ 14 — System Operators: Full Access;
- ❑ 15 — System Operators Read and Write Access;
- ❑ 16 — System Operators: Read, Write and Delete Access;

- ☐ 17 — System: Full Control;
- ☐ 18 — System: Read and Write Access;
- ☐ 19 — System: Read Access;
- ☐ 20 — Administrators: Read, Write and Execute Access;
- ☐ 21 — Interactive User: Full Control;
- ☐ 22 — Interactive User: Read and Write Access;
- ☐ 23 — Interactive User: Read, Write and Delete Access.

Например, команда:

```
Regini -h \Registry\machine\software\mycompany\myprogram [1 5 7 17]
```

даст следующие права доступа к ключу HKLM\SOFTWARE\Mycomany\Myprogram:

- ☐ Administrators: Full Control;
- ☐ Creator/Owner: Full Control;
- ☐ World (Everyone): Full Control;
- ☐ System: Full Control.

Более подробно мы рассмотрим консольные утилиты для работы с реестром, а также приведем практические примеры их использования в командных сценариях в последующих главах этой книги.

Заключение

В этой главе внимание было сконцентрировано на Редакторе реестра Regedit.exe и его использовании для внесения модификаций в базу данных реестра, ее просмотра, импорта, экспорта и распечатки. Знание операций, которые можно выполнять при помощи редакторов реестра, позволит существенно упростить устранение неполадок, и поэтому они по праву относятся к наиболее полезным средствам из арсенала каждого системного и сетевого администратора.

Редакторы реестра предоставляют очень простой способ управления реестром, но, наряду с этим, при их использовании возникает множество ситуаций, в которых можно внести ошибку непосредственно в реестр. Открывая любой из редакторов реестра, соблюдайте осторожность и старайтесь не допускать случайных изменений и удалений. Если вы собираетесь внести изменение, запомните исходное значение. Это сэкономит ваше время, если понадобится восстанавливать это значение.

Глава 4



Приступаем к редактированию реестра

Даже маленькая практика стоит большой теории.

Закон Букера

Пришла нужда постучать по дереву — обнаруживаешь, что мир состоит из алюминия и пластика.

Закон Флагга

Как и в Windows NT/2000/XP/Vista, в Windows 7 большинство конфигурационных изменений можно внести в систему при помощи средств Панели управления (Control Panel) и административных утилит, но некоторые изменения удастся осуществить только путем непосредственного редактирования реестра.

Предполагается, что к данному моменту даже те, кто впервые сталкивается с реестром, уже получили необходимый минимум информации о нем и подготовились к его редактированию. И все же, будем считать эту главу "разминочной", потому что ее цель — помочь читателю, овладевшему необходимыми начальными знаниями о реестре, овладеть и практическими навыками. Для этого здесь будут продемонстрированы практические приемы работы с реестром и различные методы его редактирования. Применяя их, можно выполнить индивидуальную настройку системы и оптимизировать ее работу. Многие вопросы, которых мы лишь коснемся в этой главе, в дальнейших главах будут рассмотрены более подробно и углубленно.

Однако перед тем как приступить непосредственно к работе, следует дать несколько важных рекомендаций.

- ❑ Регулярно выполняйте резервное копирование реестра. Частота резервного копирования должна зависеть от частоты модификации параметров

реестра, а также от средства, с помощью которого производятся эти изменения. В качестве общей рекомендации можно посоветовать выполнять резервное копирование не реже одного раза в неделю. Если вы редактируете реестр ежедневно, рекомендуется выполнять резервное копирование в конце каждого рабочего дня. Подробную информацию о резервном копировании и восстановлении реестра можно найти в *главе 2*. Даже если вы — опытный пользователь, стремящийся сразу же узнать, "а что же нового появилось в реестре Windows 7" и как ее поскорее "потвикать" и понастраивать (а потому первые главы сочли скучными и просмотрели их бегом), я настоятельно рекомендую вам вернуться к *главе 2* и прочесть ее внимательно. Во-первых, в Windows 7 в процессы резервного копирования и восстановления были введены важные новшества, которые я постаралась подробно отразить и с которыми следует ознакомиться каждому. Во-вторых, там даны очень важные предостережения о ряде малоизвестных особенностей. Эти знания позволят вам защититься от ложного чувства безопасности и избежать неприятных неожиданностей.

ЛЮБИТЕЛИ "ТРЮКОВ", ВНИМАНИЕ!

Имейте в виду, что даже профессиональный трюкач не будет выполнять свои "смертельные номера", не позаботившись о надлежащей страховке. Так натяните "страховочную сетку" и только тогда приступайте. Я вас предупредила, и потом не жалуйтесь, что, следуя моим советам, вы "все порушили и сломали". Помните, что если вы и ошибетесь, то данные в *главе 2* советы даже в наихудшем случае позволят вам выйти из ситуации с наименьшими потерями.

- ❑ Выполняйте модификацию только в тех случаях, когда вы наверняка знаете правильные значения ключей, параметров, а также ограничения для конкретных устройств и приложений.
- ❑ Приступайте к редактированию реестра только в тех случаях, когда все попытки установить или модифицировать конкретную функциональную возможность с помощью опций Панели управления (Control Panel) и административных утилит не удалось. При модификации параметров аппаратных устройств наилучшим способом внесения изменений является использование Диспетчера устройств (Device Manager), поскольку при этом вы застрахованы от таких ошибок, как случайное удаление нужного ключа реестра. Применение редактора реестра всегда сохраняет вероятность такой ошибки.
- ❑ Запуская Редактор реестра, помните, что в нем не существует средств отмены внесенных изменений или повторного выполнения операции. Реестр сохраняет внесенные изменения автоматически (и очень быстро). Единственным средством исправления допущенной ошибки является импорт

предварительно сохраненного файла реестра перед перезагрузкой компьютера.

- ❑ Никогда не вносите много изменений за один раз. Наилучшим методом представляется внесение изменений по одному за сеанс редактирования с последующим выходом из системы или ее перезагрузкой и, наконец, с дальнейшим тестированием внесенной модификации. Убедившись в работоспособности реестра после внесенного изменения, можете осуществлять следующее. Если вы за один раз внесете несколько изменений, и реестр после этого окажется неработоспособным, то впоследствии будет довольно сложно выяснить, какое конкретно изменение вызвало проблему.
- ❑ Прежде чем вносить в реестр то или иное изменение, задумайтесь, а нужно ли это вам (или пользователю, чей компьютер вы конфигурируете), и если да — то насколько. Описываемые в этой главе методы индивидуальной настройки Windows 7 изменяют стандартные параметры, назначаемые по умолчанию, а стандартные значения подходят для большинства пользователей.
- ❑ Наконец, перед тем как вносить изменения, экспортируйте ключи реестра, которые будут модифицированы. Это позволит вам быстро восстановить их исходное состояние, если при редактировании вы допустите ошибку или если эффект от внесенного изменения вам не понравится.

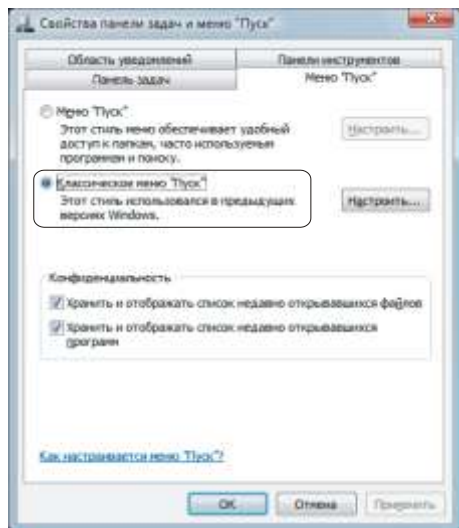
Популярные постинсталляционные настройки

Итак, вы запустили Windows 7 и ознакомились с ее нововведениями. Если только вы не занимались бета-тестированием этой ОС, начиная с ранних версий и заканчивая сборками Release Candidate (кандидат на выпуск) и RTM (Release to Manufacturing), то вы наверняка испытаете своеобразный "культурный шок", особенно — если в свое время полностью проигнорировали Windows Vista. Ничего удивительного — не только у вас возникает множество вопросов о том, куда же девались привычные настройки, как теперь выполнять ту или иную привычную операцию и т. п. Именно поэтому многие опытные пользователи испытывают просто непреодолимое желание настроить поведение Windows 7 на свой вкус, а не так, как считает нужным Microsoft. В данном разделе собран ряд полезных настроек, которые помогут вам добиться этой цели. И начнем мы с самых простых, элементарных вещей, постепенно продвигаясь от простого — к более сложному.

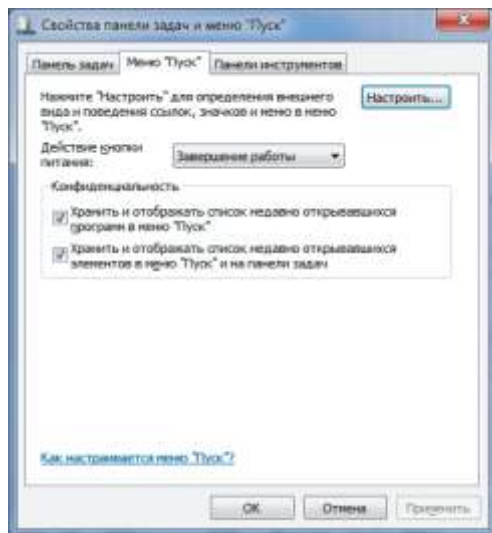
Настройки пользовательского интерфейса

В отличие от Windows Vista, своей непосредственной предшественницы, Windows 7 представляет собой не такой гигантский "рывок вперед", а скорее, концентрируется на исправлении всех недочетов, за которые пользователи критиковали Vista, зачастую вполне справедливо. В общем, мне уже часто доводилось слышать, что Windows 7 — это и есть Vista, но только лишенная всех недостатков. И это действительно так — поэтому, в отличие от Windows Vista, Windows 7 имеет все шансы на успех у пользователей. Так что прежде, чем приступать к перенастройке пользовательского интерфейса Windows 7, для начала просто попробуйте с ним поработать — и вы ее полюбите!

Хотя... Находятся и критики. Вот, например, многие пользователи, установив Windows 7, сразу же пытаются создать себе привычную рабочую среду. При этом те из них, кто привык к классическому меню **Пуск** (Start), первым делом стремятся настроить именно его — точно так же они поступали в Windows XP, так же делали и в Vista (в обеих этих операционных системах такая возможность была). Каково же бывает их удивление и возмущение, когда они обнаруживают, что в Windows 7 эта возможность пропала (рис. 4.1).



а) Windows Vista



б) Windows 7

Рис. 4.1. В Windows 7 пропала возможность быстрого возврата к классическому меню **Пуск** (Start)

Что делают эти пользователи? Правильно — бомбардируют интернет-форумы вопросами о том, нет ли какого-нибудь "хака" реестра, который бы

дал им возможность вернуть старую любимую возможность. Впрочем, понять-то их можно — классическое меню **Пуск** (Start) хорошо уже хотя бы своей простотой и незатейливостью, да и, наконец, люди к нему просто привыкли. Вот они и возмущаются. А когда им объясняют, что "хака" реестра для решения этой проблемы нет, и сколько ни добавляй в реестр ключи и параметры по образу и подобию имевшихся в Windows XP/Vista, эффекта не будет никакого, их возмущение и раздражение только растет.

Я на это отвечаю так. Во-первых, не стоит по одной только такой вот мелочи сразу же охаивать новую (и очень хорошую!) систему. Во-вторых, попробуйте привыкнуть к новому — поверьте, вы получаете действительно удобный пользовательский интерфейс, и не надо пытаться опираться на старые привычки, как на костыли. И, наконец, в-третьих — ну, если нельзя, но очень хочется, то можно! И даже не просто, а очень просто, причем для этого вам даже не потребуется редактировать реестр. Итак, выполним первое, феноменально простое упражнение, и создадим в Windows 7 "модель", имитирующую классическое меню **Пуск** (Start).

Имитируем классическое меню **Пуск**

Во-первых, для начала я объясню, почему "хака реестра" для решения этой проблемы действительно не существует. Дело в том, что изменения внесены в сам код операционной системы. Поэтому просто так добавить в реестр те ключи и параметры реестра, которые имелись, например, в Windows Vista, и надеяться на успех — дело безнадежное. Другой путь — добавление в состав операционной системы каких-либо фрагментов кода от ее предшественниц — дело слишком сложное и трудоемкое¹. И потом, для этого нужны настоящие хакерские навыки, а ими, скажем прямо, обладают немногие.

Есть гораздо более простой путь! Именно по нему мы и пойдем.

1. Создадим новую инструментальную панель — для этого щелкните правой кнопкой мыши по Панели задач (Taskbar) и из раскрывшегося контекстного меню выберите команды **Панели** (Toolbars) | **Создать панель инструментов...** (New toolbar...), как показано на рис. 4.2.
2. Откроется окно Проводника (Windows Explorer), показанное на рис. 4.3. В этом окне раскройте папку C:\ProgramData\Microsoft\Windows\Главное меню\Программы (C:\ProgramData\Microsoft\Windows\Start Menu\Programs). Обратите внимание, что эта папка будет видима только в том случае, если вы предварительно сделали видимыми скрытые файлы и папки — о том, как это делается, было рассказано в *главе 1*.

¹ См., например, дискуссию на эту тему вот здесь: <http://www.windows7taskforce.com/view/1198>.

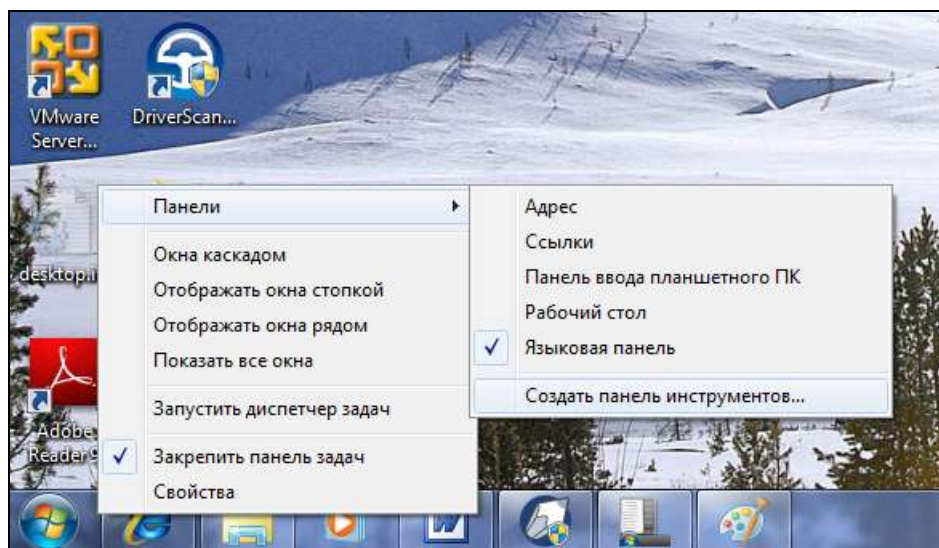


Рис. 4.2. Создадим новую инструментальную панель

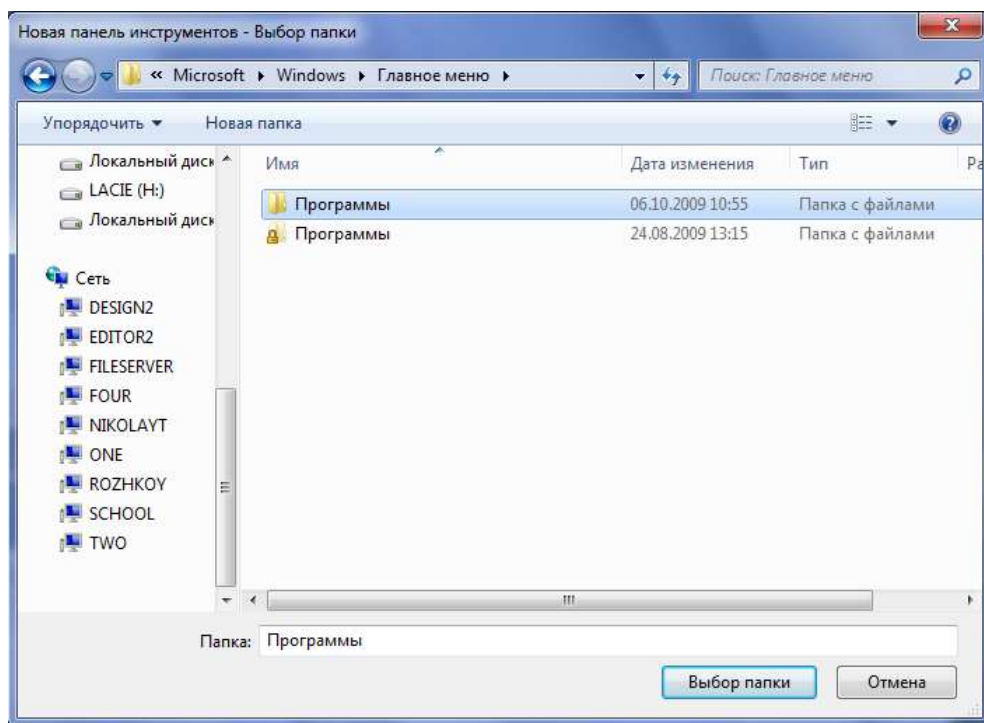


Рис. 4.3. Выбор папки C:\ProgramData\Microsoft\Windows\Start Menu\Programs

НАПОМИНАНИЕ

Чтобы сделать видимыми скрытые файлы и папки, необходимо в окне Проводника выбрать опции **Упорядочить** (Organize) | **Параметры папок и поиска** (Folder and Search Options), в раскрывшемся диалоговом окне перейти на вкладку **Вид** (View) и выбрать опцию **Показывать скрытые файлы, папки и диски** (Show hidden files, folders and drives), а также сбросить флажок **Скрывать защищенные системные файлы (рекомендуется)** (Hide protected operating system files (Recommended)) в списке **Дополнительные параметры** (Advanced settings) — см. рис. 1.15.

ПРИМЕЧАНИЕ

Обратите внимание и на то, что названия некоторых папок отображаются в локализованных версиях в локализованном виде только через графический интерфейс Проводника. Если же вы будете просматривать эти каталоги в режиме командной строки (командой `dir /a`, как показано на рис. 4.4, то вы увидите, что на самом деле названия папок НЕ ЛОКАЛИЗОВАНЫ (скорее всего — во избежание проблем с совместимостью различных локализованных версий).

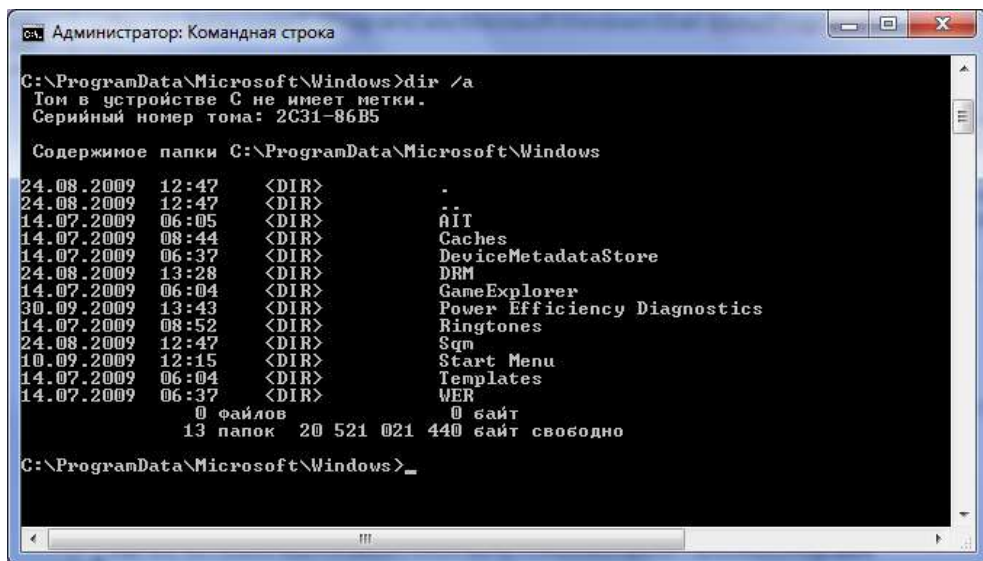


Рис. 4.4. Названия упоминавшихся чуть ранее папок при просмотре в режиме командной строки НЕ ЛОКАЛИЗОВАНЫ

3. Нажмите кнопку **Выбор папки** (Select Folder), и на Панели задач сразу же появится новая инструментальная панель с названием **Программы** (Programs) (рис. 4.5).



Рис. 4.5. На Панели задач появилась новая инструментальная панель с названием **Программы** (Programs)

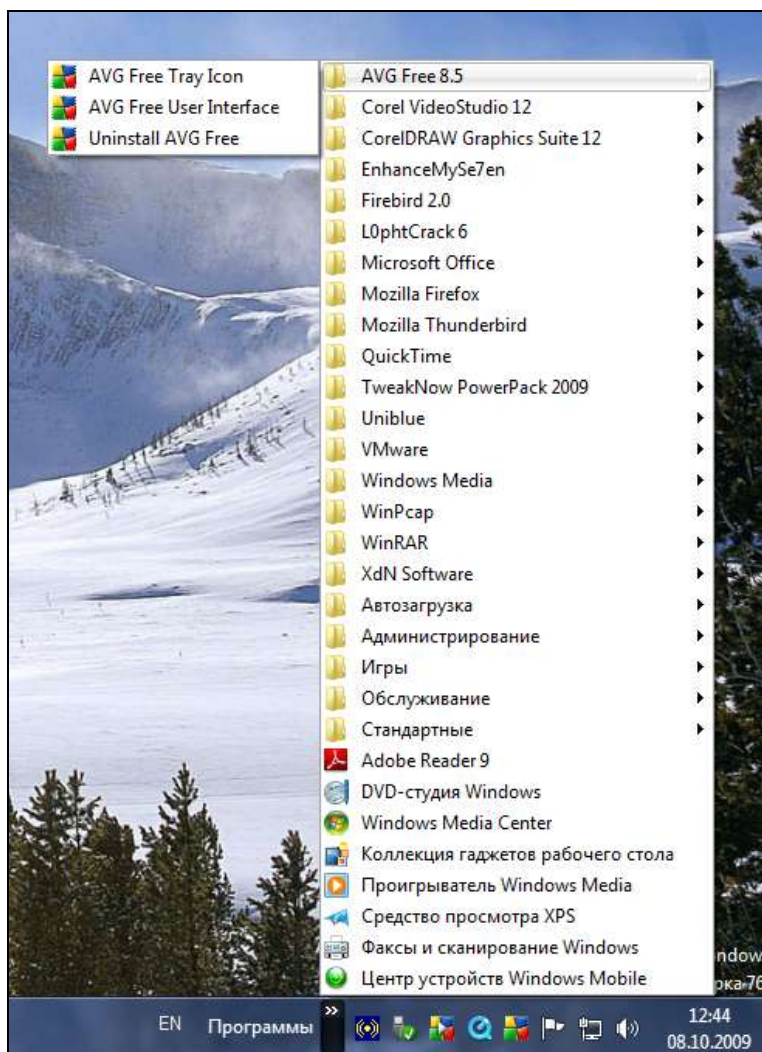


Рис. 4.6. Новая инструментальная панель **Программы** (Programs) — да это же наше привычное классическое меню **Пуск**!

4. Щелкните мышью по значку "шеврона" на правой границе этой инструментальной панели. Посмотрите (рис. 4.6), это вам ничего не напоминает?
5. Итак, мы добились появления чего-то, более или менее похожего на классическое меню **Пуск** (Start). Но мы не будем на этом останавливаться, а пойдем еще дальше и сделаем так, чтобы как можно больше приблизить эту панель к привычному меню, которого многим (мне — в том числе) так не хватает. Для этого щелкните по инструментальной панели правой кнопкой мыши. Раскроется контекстное меню, показанное на рис. 4.7. Чтобы модифицировать нашу новую инструментальную панель, сбросьте флажок **Закрепить панель задач** (Lock the taskbar).

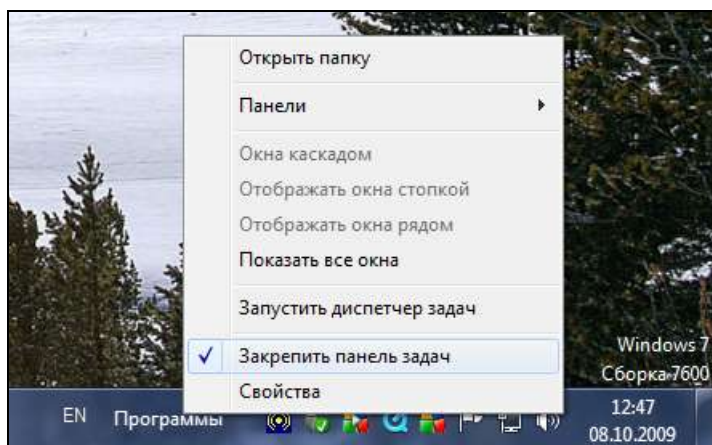


Рис. 4.7. Контекстное меню инструментальной панели **Программы** (Programs)

6. На левой границе нашей инструментальной панели в Панели задач появится разделитель в виде трех вертикальных столбцов из точек (на рис. 4.8 на него указывает белая стрелка). Щелкните по этому разделителю правой кнопкой мыши — появится контекстное меню, показанное на рис. 4.9.

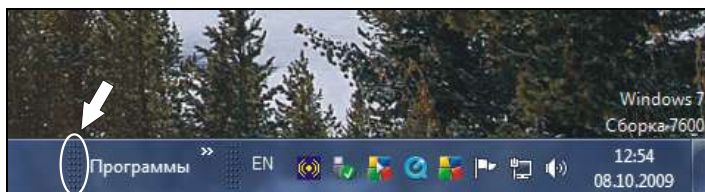


Рис. 4.8. На левой границе новой инструментальной панели появился разделитель

7. Сбросьте флажки **Показывать подписи** (Show text) и **Показывать заголовок** (Show title), а флажок **Крупные значки** (Large Icons), наоборот, установите.
8. Инструментальная панель "сожмется" и будет выглядеть примерно так, как показано на рис. 4.10.

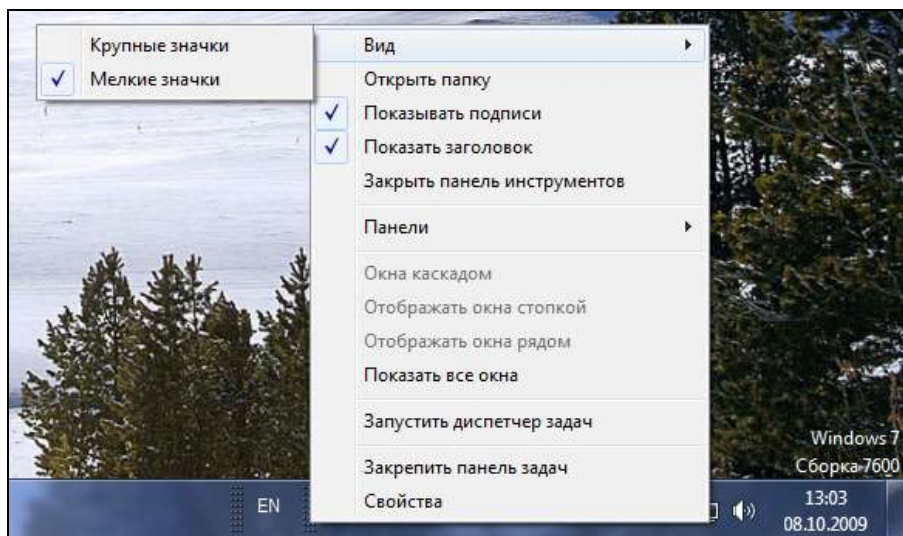


Рис. 4.9. Контекстное меню, появляющееся при щелчке правой кнопкой мыши по разделителю



Рис. 4.10. Вот так теперь выглядит новая инструментальная панель

9. Давайте теперь выберем для нее другой значок — поприятнее, чем типовая "раскрытая папка". Перетяните мышью левый ограничитель новой инструментальной панели как можно ближе к кнопке **Пуск** (Start), щелкните по значку "шеврона" на правой границе, выберите какой-нибудь ярлык (я выбрала Windows Media Center) и мышью перетащите его в крайнюю левую позицию нашей новой инструментальной панели. У вас должно получиться что-то похожее на то, что вышло у меня (рис. 4.11).



Рис. 4.11. Вот что должно у вас получиться

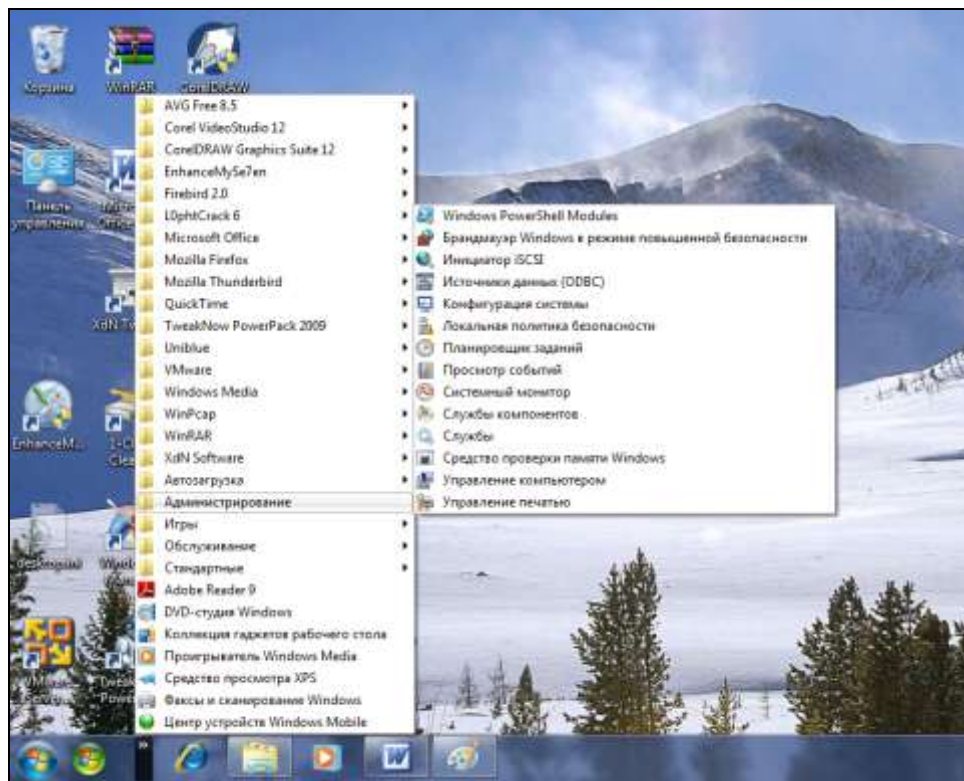


Рис. 4.12. Реконструированное классическое меню **Пуск** (Start) в Windows 7 — вот оно, счастье-то!

10. Теперь "сожмите" инструментальную панель, потянув влево ее ограничитель, так, чтобы на ней остался только один значок. После этого снова заблокируйте Панель задач — для этого щелкните правой кнопкой мыши по инструментальной панели и вновь взведите флажок **Закрепить панель задач** (Lock the taskbar). Получиться должно примерно так, как показано на рис. 4.12.

Только имейте в виду — чтобы воспользоваться нашим "классическим меню **Пуск**", щелкать мышью нужно по значку "шеврона", а не по краси-

вому значку-кнопке, похожему на значок кнопки **Пуск** (и расположившемся справа от кнопки **Пуск** натуральной), потому что в этом случае вы запустите приложение Windows Media Center. Но, я думаю, вы очень быстро к этому привыкнете. Во всяком случае, вот оно — так необходимое вам меню, наслаждайтесь!

СОВЕТ

Вы думаете, это все? Нет, не совсем. То, что вы получили, это еще не полное классическое стартовое меню. Дело в том, что в задействованной нами папке `C:\ProgramData\Microsoft\Windows\Главное меню\Программы` (`C:\ProgramData\Microsoft\Windows\Start Menu\Programs`)² содержатся только те пункты меню, которые доступны всем пользователям. Желательно дополнить это меню, чтобы в нем отображались все программы, с которыми вы работаете. Для этого раскройте папку `C:\Users\<user name>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs` (здесь *user name* — это ваше пользовательское входное имя). В ней содержатся программы, доступные только вам. Скопируйте содержимое этой папки в папку `C:\ProgramData\Microsoft\Windows\Start Menu\Programs`. Вот теперь действительно все!

Активизируем и блокируем панель быстрого запуска в Windows 7

Наверняка вы уже заметили, что в Windows 7 отсутствует и панель быстрого запуска (Quick Launch), имевшаяся в предшествующих версиях. Вообще-то в ней более нет необходимости, потому что приложения, которые вы часто используете, можно закрепить прямо на панели задач (Taskbar). Тем не менее, если вам не хватает панели быстрого запуска, то вернуть ее можно точно таким же способом, каким было сконструировано классическое меню **Пуск** (Start) в предыдущем разделе.

Папка, которую при этом надо выбрать при создании новой панели инструментов, располагается по следующему адресу: `%userprofile%\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch`. Все остальные операции по ее настройке выполняются точно так же, как и при воссоздании классического меню **Пуск** (Start). Более подробные иллюстрированные пошаговые инструкции можно найти здесь: <http://www.sevenforums.com/tutorials/888-quick-launch-enable-disable.html>.

² Не забываем о том, что локализованными названия папок выглядят только при просмотре через графический интерфейс Проводника, а в действительности, при просмотре в режиме командной строки, они НЕ ЛОКАЛИЗОВАНЫ и выглядят в точности так, как и в англоязычной версии.

Настройка Панели задач — с помощью реестра и без него

Как вы наверняка уже заметили, в Windows 7 имеется новая, полностью переработанная Панель задач. На этот счет существует множество самых разных мнений — одни разражаются восторженными охами и ахами, называя ее "суперпанелью" (Superbar), а другие пренебрежительно говорят — "бантики для блондинок". Я на это замечу, что, во-первых, натуральная блондинка, а не пергидрольная — это очень красиво (вот бы мне такой цвет волос), а Панель задач в Windows 7 — это очень удобно. Главное, что сразу же бросается в глаза — так это то, что она больше не загромождена. Кнопки группируются, и эту возможность можно настраивать по желанию, а часто используемые приложения можно закрепить на Панели задач (Pin to Taskbar) или открепить от нее (как это делается, уже было показано в *главе 3* на примере Редактора реестра). Экземпляры активных приложений разворачиваются над Панелью задач маленькими окошками ("миниатюрами", Thumbnail Preview), как только на соответствующем значке остановится указатель мыши (рис. 4.13). Окошки эти "живые", изображение в них, если надо, движется (например, при воспроизведении видео). При этом, что удобно, все необходимые настройки можно выполнить через пользовательский интерфейс.



Рис. 4.13. Новая Панель задач в Windows 7

Я откровенно не понимаю, почему это может кому-то не нравится, но вот вам совет, как заблокировать эти окошки, если они вас так раздражают.

Для начала я дам два гарантированно полезных совета, которые действительно работают в Windows 7, а потом наглядно продемонстрирую, что среди множества советов и "твиков", которые можно найти на просторах Интернета, часто можно встретить и неработающие.

Два рабочих совета по блокировке "миниатюр"

Эта книга писалась по материалам бета-версий и Windows 7 RC (Release Candidate). Но оба совета были протестированы мною и в Windows 7 RTM (Release To Manufacturing), так что можно гарантировать, что они будут работать и в окончательной версии Windows 7. Вот они:

- ❑ во-первых, вы можете заблокировать интерфейс Windows Aero — для этого достаточно выбрать какую-нибудь классическую тему оформления рабочего стола через Панель управления (Control Panel) или в окне **Персонализация** (Personalization), открыть которое можно, щелкнув правой кнопкой мыши в любой незанятой точке Рабочего стола (Desktop) и выбрав из контекстного меню команду **Персонализация** (Personalization). Тогда Панель задач (Taskbar) будет выглядеть так, как показано на рис. 4.14;
- ❑ во-вторых, можно открыть редактор реестра, найти в нем ключ `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced` и создать в нем параметр `ExtendedUIHoverTime` (DWORD). Присвойте этому параметру достаточно высокое значение — например 20000 (dec). Этот прием не блокирует всплывающие "миниатюры" как таковые, но они будут появляться с существенным запаздыванием, только если вы задержите курсор над кнопкой панели задач очень надолго.

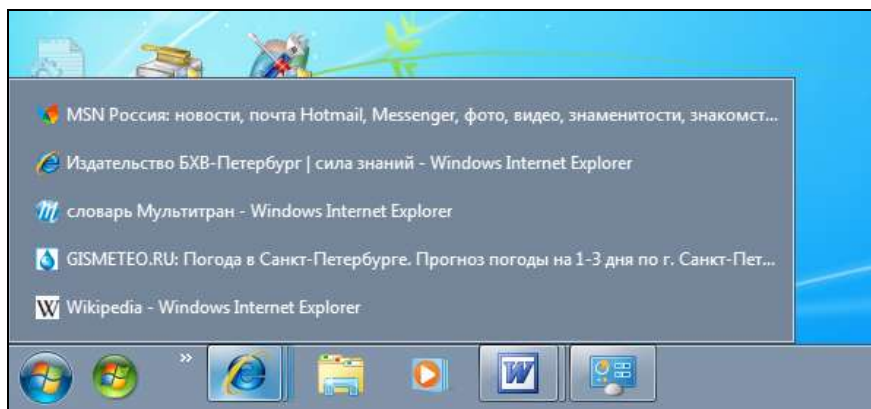


Рис. 4.14. Выбор классической темы оформления рабочего стола блокирует и "миниатюры"

Пример совета, который не работает

На многих Интернет-форумах можно встретить рекомендацию по блокировке "миниатюр" в Windows 7 с помощью редактирования системных политик, и обходным — путем непосредственного редактирования реестра.

ПРИМЕЧАНИЕ

Вообще-то, полноценными "хаками" настройки, которые можно задать с помощью системных политик, считать не следует. Я лично не считаю полноценными "хаками реестра" все те настройки, которые можно отрегулировать, не залезая в реестр непосредственно. Но все же такие советы могут быть полезны тем, в чьих версиях Windows 7 отсутствует возможность редактирования групповых политик (например, Home Edition). Вот им придется выполнять эту работу через реестр.

Рассмотрим эти советы и разберемся, почему они не работают.

Блокировка "миниатюр" в панели задач Windows 7 путем прямого редактирования реестра

Совет по блокировке "миниатюр" в панели задач путем непосредственного редактирования реестра сводится к следующему:

1. Запустите редактор реестра любым из способов, описанных в *главе 3* (наверняка вы уже заметили, что практически любая задача в Windows 7 может быть выполнена множеством различных способов, и выбор любого из них — это вопрос личных предпочтений).
2. В открывшемся окне редактора реестра разверните следующий ключ:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
```

ПРИМЕЧАНИЕ

Здесь и далее по всему тексту книги предполагается, что если указанный ключ или параметр реестра не существует, то его следует создать. И еще — практически все параметры, которые находятся в составе ключа `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies`, можно изменить с помощью оснастки MMC **GPEdit.msc**.

3. Создайте в составе этого ключа параметр типа `DWORD`, дайте ему имя `TaskbarNoThumbnail` и присвойте ему значение 1.
4. Чтобы внесенные изменения вошли в силу, выйдите из системы, а затем снова зарегистрируйтесь.

Если впоследствии вы захотите отменить внесенное изменение, запустите редактор реестра, найдите ключ `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer` и удалите параметр `TaskbarNoThumbnail` или присвойте ему значение 0.

Попробуйте выполнить этот совет и убедитесь в том, что в Windows 7 он не работает. Во всяком случае, у меня (Windows 7 RTM, Сборка 7600) он не сработал.

Блокировка "миниатюр" в Windows 7 с помощью редактирования системных политик

А теперь рассмотрим еще один вариант — блокировку "миниатюр" с помощью редактирования системных политик:

1. Щелкните мышью по кнопке **Пуск** (Start), введите в поле поиска строку `GPedit.msc`, а затем нажмите клавишу `<Enter>`.
2. Разверните окно консоли в левой панели окна **Редактор локальной групповой политики** (Local Group Policy Editor), как показано на рис. 4.15. Для этого выберите в дереве консоли следующие узлы: **Конфигурация пользователя** (User Configuration) | **Административные шаблоны** (Administrative Templates) | **Меню "Пуск" и панель задач** (Start Menu and Taskbar).

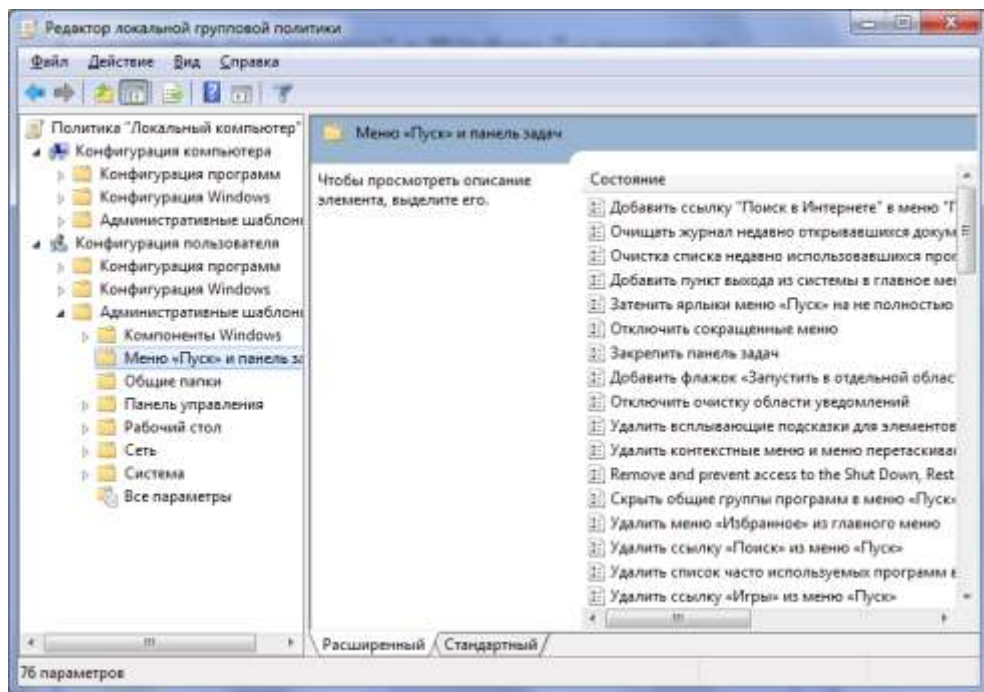


Рис. 4.15. Редактирование системных политик

3. Посмотрите, какое огромное количество локальных политик! Найдите в этом списке политику **Отключить эскизы в Панели задач** (Turn off taskbar thumbnails).

ПРИМЕЧАНИЕ

Имейте в виду, что если вы — счастливый обладатель полноценной версии Windows 7 (Professional, Ultimate или Enterprise), то большинство настроек пользовательского интерфейса лучше всего выполнять именно отсюда — это и проще, и безопаснее, чем прямое редактирование реестра.

4. Выполните по этой политике двойной щелчок мышью. Раскроется окно, показанное на рис. 4.16. Советы, опубликованные на форумах, рекомендуют выбрать опцию **Отключить** (Disabled), а затем нажать кнопки **Применить** (Apply) и **ОК**. Далее рекомендуется протестировать внесенные изменения, для чего следует сначала выйти из системы, а затем — зарегистрироваться повторно. Последуйте этим рекомендациям и убедитесь, что совет НЕ РАБОТАЕТ.

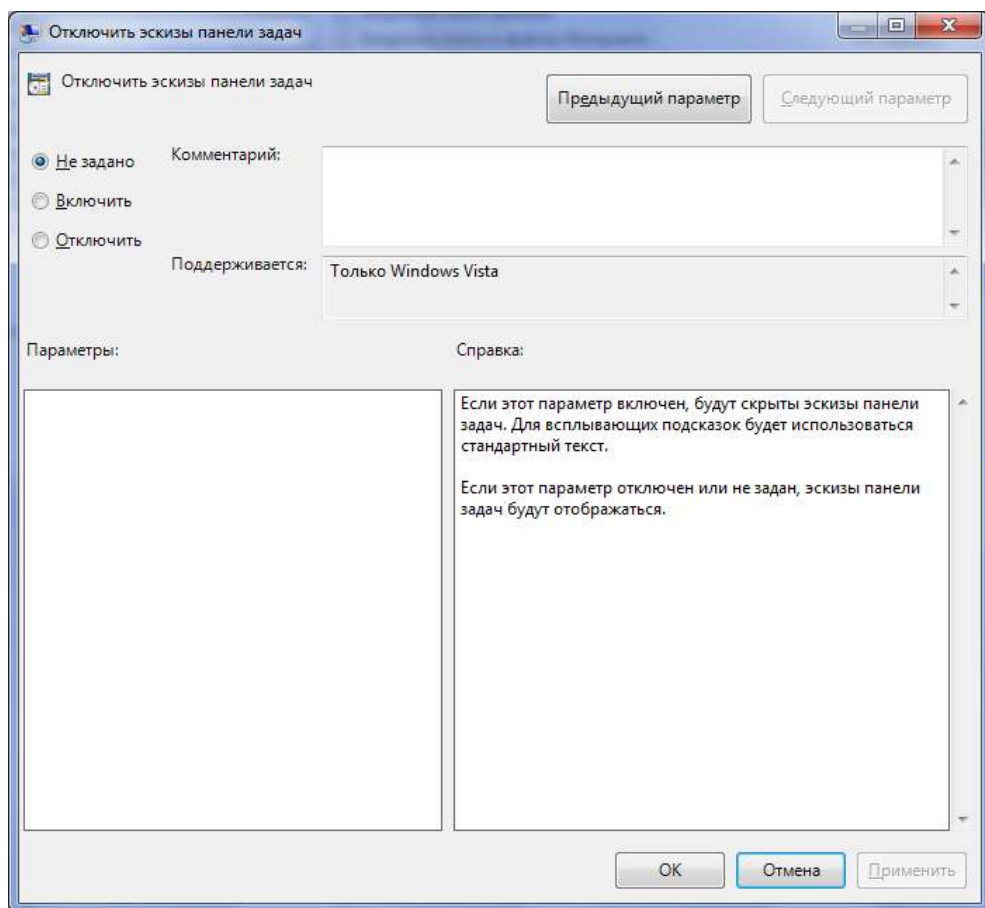


Рис. 4.16. Блокировка "миниатюр" в Панели задач — пример неработающего совета

5. А теперь давайте разберемся — почему он не работает. Посмотрите внимательно на окно, показанное на рис. 4.15. Посмотрите — в этом окне явно указывается, какие операционные системы поддерживают ту или иную политику. В данном случае политика **Отключить эскизы в Панели задач** (Turn off taskbar thumbnails) зарезервирована исключительно для Windows Vista, а это значит, что даже если она и работала в ранних бета-версиях, она совершенно не обязана работать ни в последующих версиях, ни, тем более, в окончательной. Кстати, этот пример очень показателен, поэтому я умышленно не выкинула его из окончательной версии книги. Он демонстрирует два факта:

- все настройки, которые можно выполнять через административные утилиты, лучше всего выполнять именно так;
- не все "твики" реестра одинаково работоспособны, не все из них полезны, а некоторые даже вредны. Так, например, конкретно вот этот совет не только не позволяет добиться поставленной задачи, но и имеет неприятный побочный эффект, а именно уничтожает все ваши заботливо созданные инструментальные панели (например, имитацию "классического меню Пуск", создание которой было описано в разд. *Имитируем классическое меню Пуск*).

Активизация Windows Aero

Одни пользователи любят блокировать "бантики", а другие, наоборот, ими восхищаются и очень хотят их иметь. При этом большая часть, если не все эти возможности, зависят не от чего-нибудь, а от функций Windows Aero.

В большинстве случаев, если видеоадаптер удовлетворяет минимальным требованиям, необходимым для работы Windows Aero, то Windows Aero будет активизирован автоматически. В Windows 7 минимальные аппаратные требования, необходимые для Windows Aero, не слишком сильно отличаются от аналогичных требований, имевшихся в Windows Vista. Напомним их вкратце: процессор с тактовой частотой 1 ГГц (x86 или x64), 1 Гбайт RAM, видеоадаптер с поддержкой DirectX 9, имеющий не менее 128 Мбайт видеопамяти, драйвер, удовлетворяющий модели Windows Display Driver Model (WDDM).

Однако в некоторых случаях интерфейс Windows Aero может оказаться заблокированным. Обычно это происходит из-за того, что при установке не было обнаружено подходящего видеодрайвера, после неудачной установки драйвера видеоадаптера, или же если компьютер не удовлетворяет минимальным требованиям, необходимым для Windows 7 Aero.

Какова бы ни была причина, прежде всего, попробуйте решить проблему стандартным методом, и только затем попробуйте рецепт по редактированию реестра, который будет предложен далее.

Через пользовательский интерфейс

Идя по стандартному пути, выполните следующие шаги:

1. Запустите Панель управления (Control Panel) и выберите опции **Система и безопасность** (System and Security) | **Система (System)**. Убедитесь в том, что индекс производительности Windows (**Rating**) имеет значение не менее 3 (рис. 4.17).
2. Откройте окно **Панель управления** (Control Panel) и выберите опцию **Поиск и устранение проблем** (Find and Fix Problems) в группе опций **Система и безопасность** (System and Security). Раскроется окно, показанное на рис. 4.18.

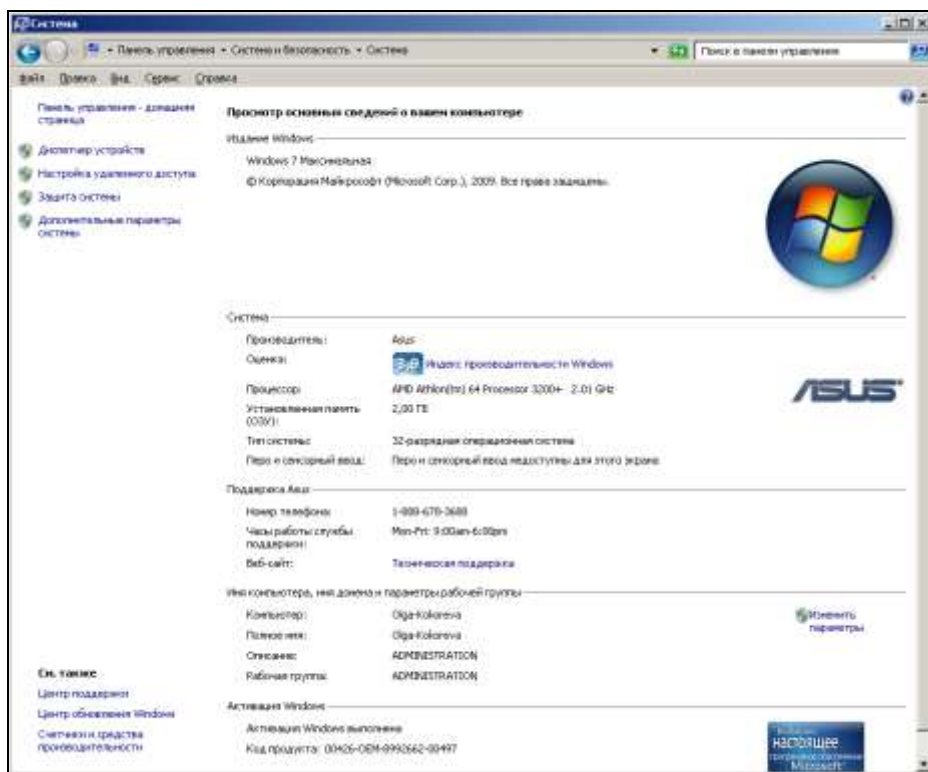


Рис. 4.17. Индекс производительности Windows превышает значение 3, но интерфейс Аего почему-то не активизирован

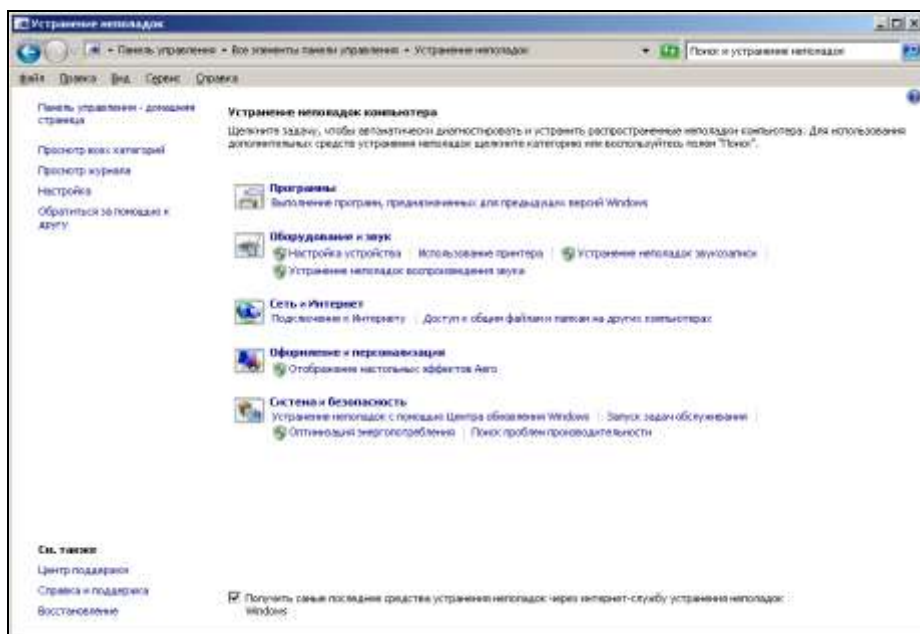


Рис. 4.18. Запуск мастера по устранению неполадок, препятствующих работе Windows Aero

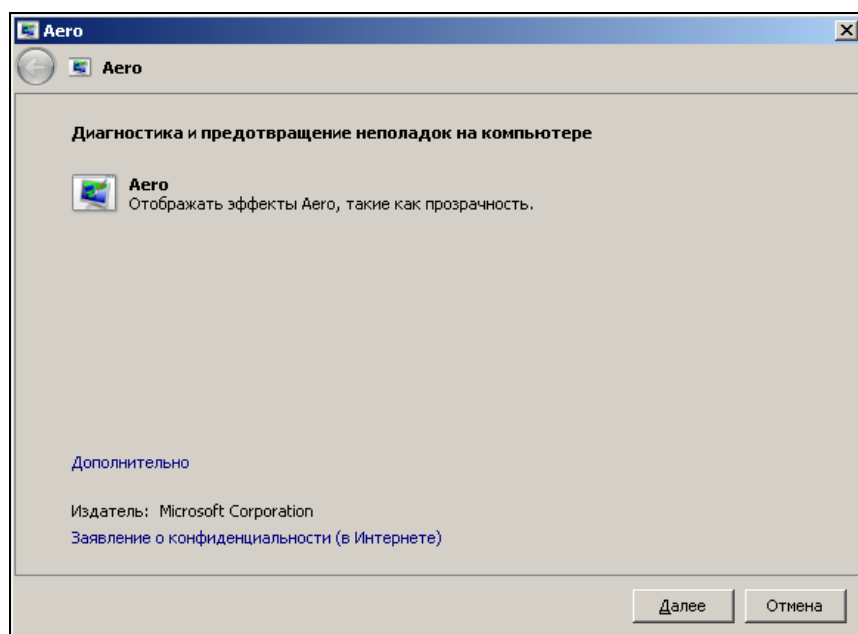


Рис. 4.19. Первое окно мастера по устранению неполадок Aero

3. В этом окне щелкните по ссылке **Отображение настольных эффектов Aero** (Find and fix problems with transparency and other visual effects). На экране откроется окно, показанное на рис. 4.19. Нажмите в этом окне кнопку **Далее** (Next) и следуйте выводимым на экран инструкциям.
4. Мастер по устранению неполадок попытается выполнить серию проверок различных компонентов вашей системы — видеопамять, сервис оконного менеджера Desktop Windows Manager (DWM) — и выполнит анализ причин, препятствующих работе Aero. Как правило, проверка оказывается успешной, и причина будет найдена (рис. 4.20).

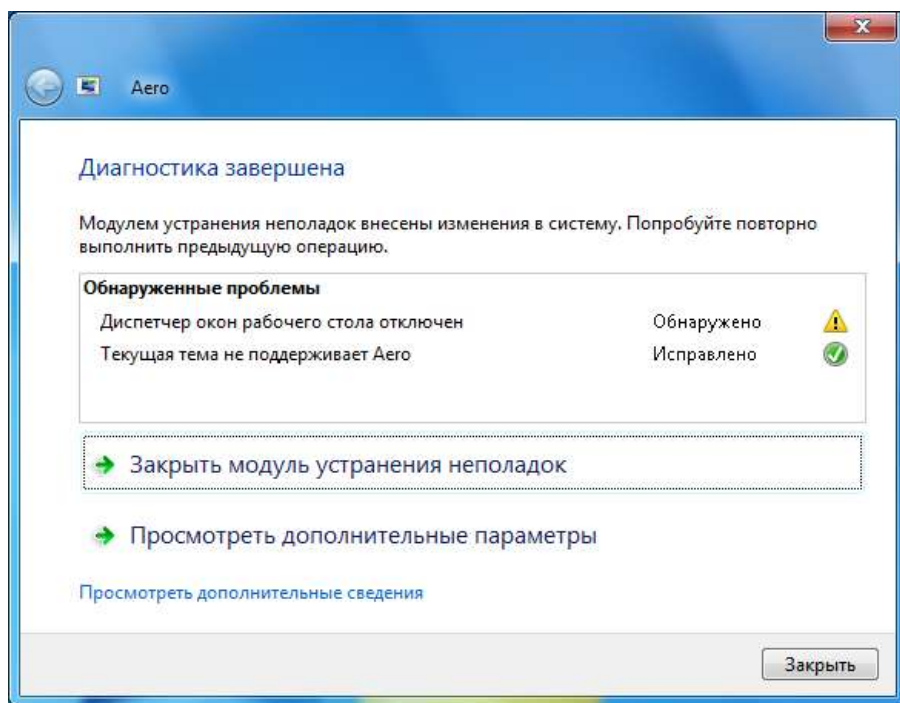


Рис. 4.20. Причина, по которой не работает Aero, найдена

Через реестр

Если же все ваши усилия оказались тщетными, то попробуйте следующий метод принудительной активизации Aero через реестр. Для этого проделайте следующее:

1. Запустите редактор реестра и перейдите в раздел `HKCU\Software\Microsoft\Windows\DWM`.

2. Создайте в нем следующие три параметра с типом данных `DWORD`:

```
UseMachineCheck;  
Blur;  
Animations
```

и установите для всех параметров значение 0.

3. Запустите сеанс командной строки с правами администратора (о том, как это делается, уже было рассказано в *главе 1*). Дайте следующие две команды:

```
net stop uxsms  
net start uxsms
```

Эти команды остановят и перезапустят Менеджер рабочего стола (Desktop Window Manager Session Manager).

4. После этого щелкните правой кнопкой мыши на рабочем столе, выберите команду изменения свойств рабочего стола и активируйте тему Windows Aero.

Открытие "суперсекретной" администраторской учетной записи

Так, побаловались, и хватит. Перейдем к более серьезным и не столь уж очевидным вещам. Как вы, вероятно, помните, в Windows NT/2000/XP существовала учетная запись **Администратор** (Administrator), она не была скрытой, и многие использовали ее в качестве основной или даже чуть ли не единственной. Эта учетная запись давала полные права по управлению компьютером. Начиная с Windows Vista, ситуация кардинально поменялась — учетная запись Администратора по умолчанию заблокирована и сделана скрытой. Естественно, та же самая ситуация имеет место и в Windows 7. Поэтому первое, что мы сделаем, — разблокируем эту учетную запись. Итак, запустим командную строку с правами администратора (о том, как это сделать, было рассказано в *главе 1*) и дадим следующую команду (рис. 4.21):

```
net user Administrator /active:yes
```

ПРИМЕЧАНИЕ

В русских версиях Windows Vista и Windows 7 эта учетная запись называется **Администратор**, и именно так, на кириллице, ее и следует вводить в составе данной команды.

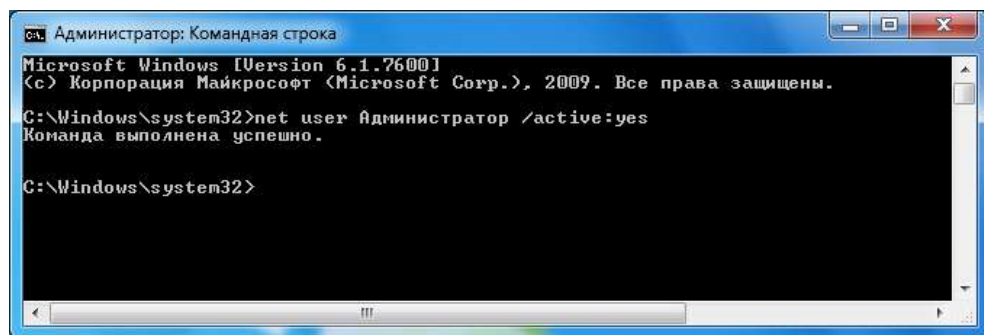


Рис. 4.21. Разблокирование скрытой учетной записи **Администратор**

С этого момента учетная запись **Администратор** (Administrator) будет доступна для выбора на экране приветствия наряду с другими учетными записями, созданными в системе. Используйте ее так же, как и любую другую учетную запись (рис. 4.22).



Рис. 4.22. После разблокирования скрытая учетная запись **Администратор** (Administrator) стала доступной для выбора

ВНИМАНИЕ!

Здесь нелишним будет напомнить о необходимости соблюдать меры безопасности. Только что разблокированная суперсекретная учетная запись администратора не имеет пароля (странно, что задать административный пароль при установке ни Windows Vista, ни Windows 7 не предлагают, а ведь так делается во всех порядочных версиях Linux и во всех предшествующих версиях систем из семейства Windows NT). Поэтому, сразу же после разблокирования учетной записи **Администратор**, немедленно создайте для нее пароль, соответствующий всем традиционным требованиям к "сильным" паролям (не менее 8 символов — цифр и букв, желательно в разных регистрах клавиатуры).

Если впоследствии вы захотите отключить эту учетную запись и сделать ее скрытой, запустите сеанс командной строки с повышенными привилегиями и введите следующую команду:

```
net user Администратор /active:no
```

Настройка контроля учетных записей пользователей

Одно из самых раздражающих нововведений, которые появились в Windows Vista — это контроль учетных записей пользователей (User Account Control, UAC). Как уже говорилось в *главе 1*, цель этой функции состоит в реализации одного из фундаментальных принципов безопасности — принципа минимальных достаточных полномочий (Least-Privileged User Account, LUA). При активизированной функции UAC с повышенным уровнем привилегий запускаются лишь приложения, которым пользователь доверяет (рис. 4.23).

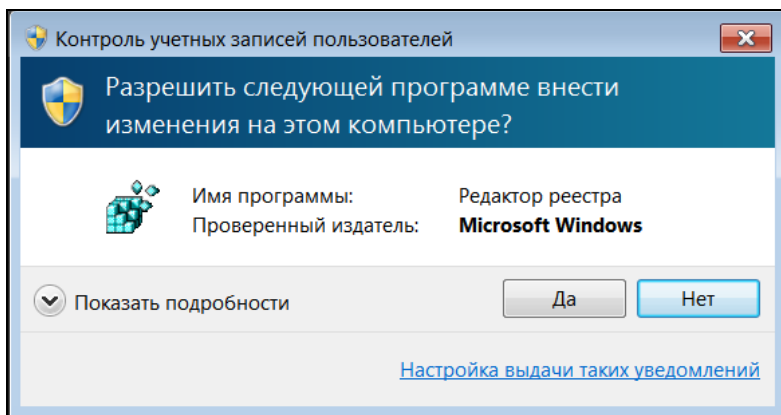


Рис. 4.23. Функция контроля учетных записей пользователей позволяет запускать с повышенным уровнем привилегий лишь приложения, которым пользователь доверяет

Контроль учетных записей предоставляет дополнительную защиту и администраторам за счет реализации режима административного подтверждения (Administrator Approval Mode). При работе в этом режиме Windows Vista выполняет большинство задач со стандартными полномочиями даже в тех случаях, когда пользователь зарегистрировался в системе от имени учетной записи с административными правами. Если пользователь желает запустить программу или выполнить операцию, требующую административных полномочий, система выводит диалоговое окно, в котором предлагает подтвердить согласие на выполнение операции с административными правами.

Хотя эта мера действительно помогает снизить риск несанкционированной модификации системы случайно запущенными вредоносными программами, именно UAC вызывает у пользователей наибольшее раздражение. UAC является причиной и еще одной "надоедливости" Windows Vista, а именно — необходимости запускать команды из командной строки, введенной с правами администратора, о чем уже говорилось в *главе 1*.

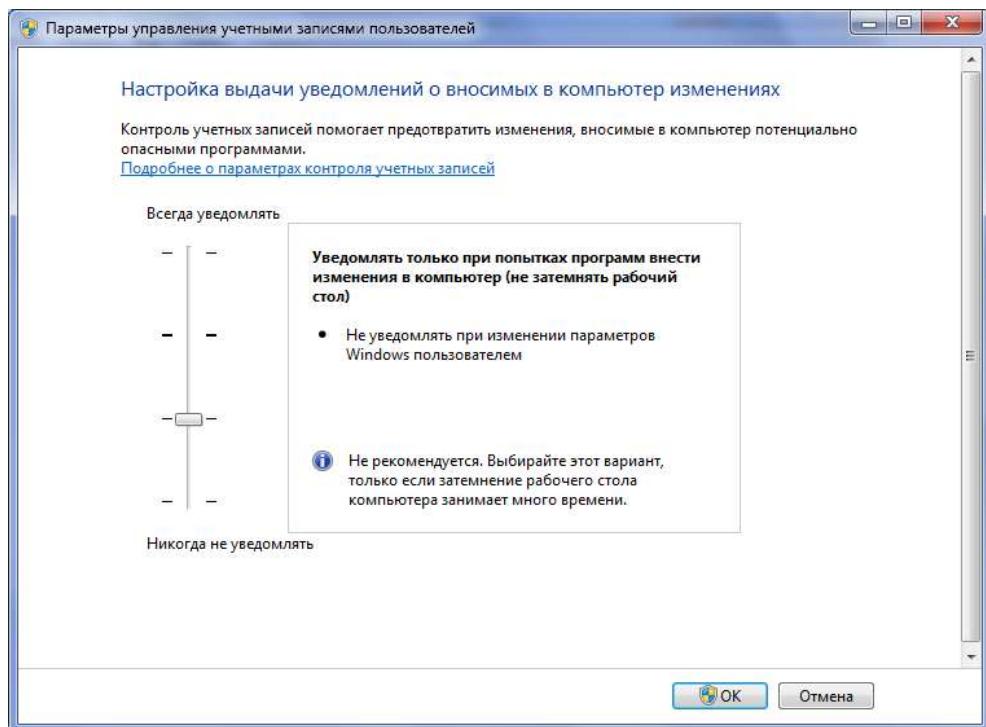


Рис. 4.24. Изменение параметров UAC в Windows 7

В Windows 7 ситуация слегка поменялась в лучшую сторону — теперь вам предоставляется несколько большее количество возможностей по контролю над UAC— посмотрите на рис. 4.24. В отличие от Windows Vista, где имелось только две возможности (включение и выключение UAC), в Windows 7 появились две промежуточные градации уровня UAC. Когда срабатывает UAC, весь рабочий стол затемняется и блокируется, так что вы не можете больше обратиться ни к одной программе, пока не разрешите или не запретите выполнение программы, в результате которой появился запрос UAC. Теперь эту функцию можно отменить.

Через пользовательский интерфейс

Как всегда, добраться до нужных настроек Windows 7 можно несколькими способами. Первый из них — открыть Панель управления (Control Panel), выбрать опцию **Учетные записи пользователей и семейная безопасность** (User Accounts and Family Safety), затем — опцию **Учетные записи пользователей** (User Accounts). Раскроется окно, показанное на рис. 4.25. Чтобы настроить поведение UAC, щелкните в этом окне по ссылке **Изменение параметров контроля учетных записей** (Change User Account Control (UAC) Parameters), и на экране появится окно, позволяющее выполнить настройку UAC (см. рис. 4.24).

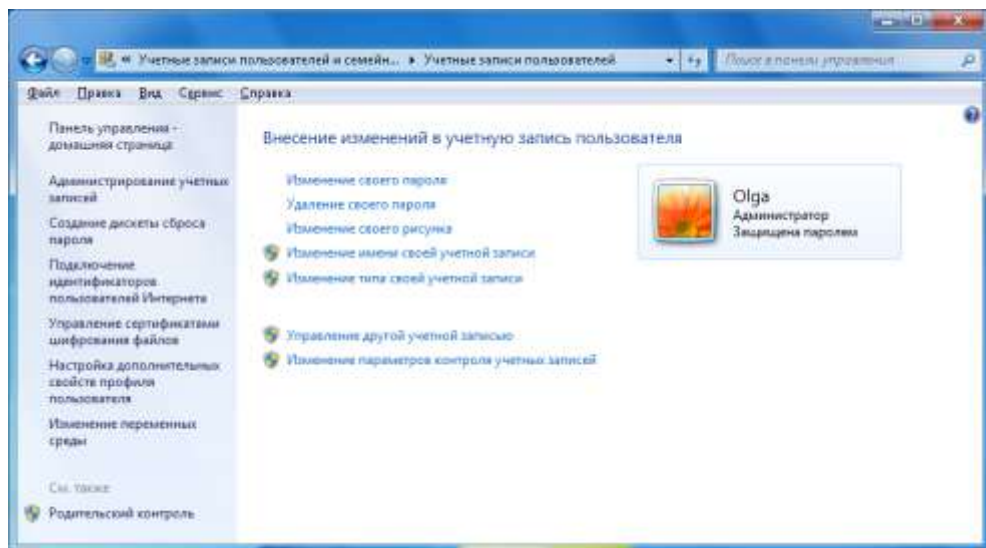


Рис. 4.25. Окно **Внесение изменений в учетную запись пользователя** (Change User Account Control settings)

Этого же результата можно добиться и через **Центр поддержки** (Action center) — там такая опция тоже присутствует. **Центр поддержки** (Action Center) — это еще одно нововведение Windows 7, пришедшее на смену **Центру обеспечения безопасности** (Windows Security Center), появившемуся в Windows Vista и вызвавшему огромное количество нареканий со стороны пользователей. Это и неудивительно — данный компонент выводил огромное количество назойливых сообщений (вот из-за чего многие говорили о "параноидальной" системе безопасности Windows Vista), причем работать с ним было довольно затруднительно для рядовых пользователей. Разработчики Microsoft пошли пользователям навстречу и создали гораздо менее навязчивый и гораздо более удобный и информативный **Центр поддержки** (Action Center), который предоставляет пользователям единую, централизованную отправную точку по решению всех проблем — как связанных с обслуживанием компьютера и устранением неполадок в его работе, так и с обеспечением безопасности. По умолчанию, значок Центра поддержки (Action Center) ненавязчиво присутствует в области уведомлений на панели задач (рис. 4.26), и, щелкнув по нему левой кнопкой мыши, вы увидите небольшое всплывающее окно, позволяющее прочитать сообщения от Центра поддержки или открыть окно Центра поддержки (рис. 4.27). В левой части этого окна присутствует ссылка **Изменение параметров контроля учетных записей** (Change User Account Control (UAC) Parameters). Щелчок мышью по этой ссылке откроет уже знакомое окно, позволяющее выполнить настройку UAC (см. рис. 4.24).

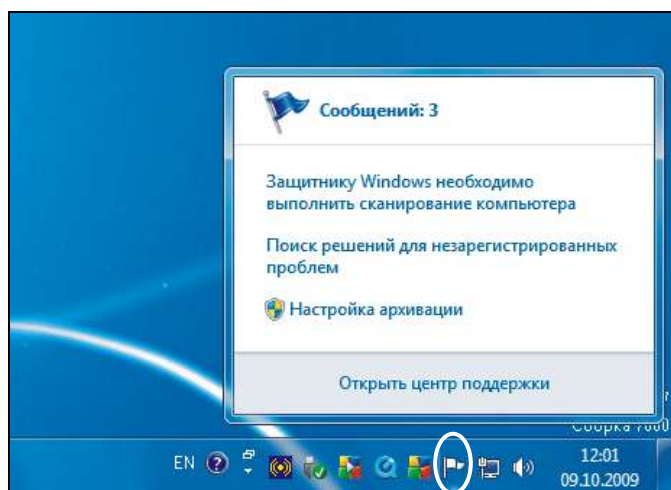


Рис. 4.26. По умолчанию значок Центра поддержки ненавязчиво присутствует в области уведомлений

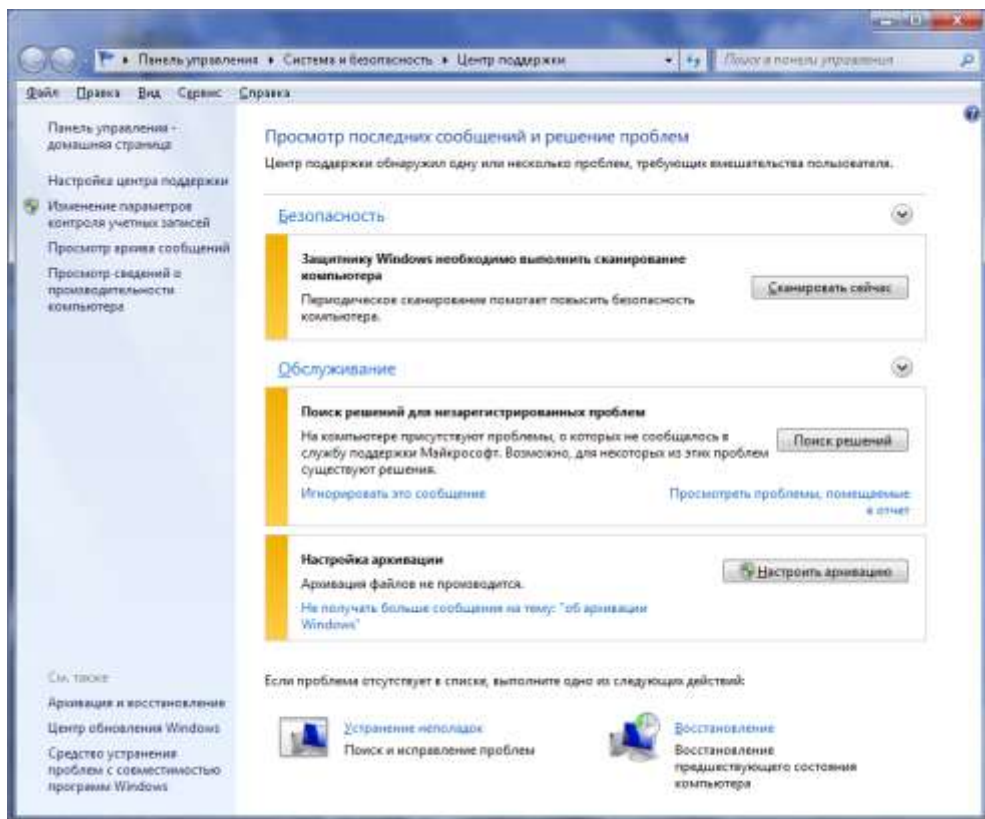


Рис. 4.27. Окно Центра поддержки (Action Center)

Еще один вариант — запустить утилиту `msconfig.exe` — **Конфигурация системы** (System Configuration Utility). Для этого введите команду `msconfig` в командной строке или в поле поиска, а после ее запуска в открывшемся окне перейдите на вкладку **Сервис** (Tools), как показано на рис. 4.28. прокрутите список до пункта **Change User Account Control settings** и нажмите кнопку **Запуск** (Launch). На экране появится все то же знакомое нам окно (см. рис. 4.23). Внесите необходимые изменения, затем перезагрузитесь, и модификации вступят в силу.

ПРИМЕЧАНИЕ

Посмотрите внимательно на окно, показанное на рис. 4.28 — там отображается команда, которая должна быть запущена. Вот вам и самый простой способ — ввести в поле поиска меню **Пуск** (Start) или из командной строки указанную команду — `UserAccountControlSettings`. Тогда апплет, позволяющий выполнить настройку УАС, запустится сразу же, минуя все промежуточные шаги.

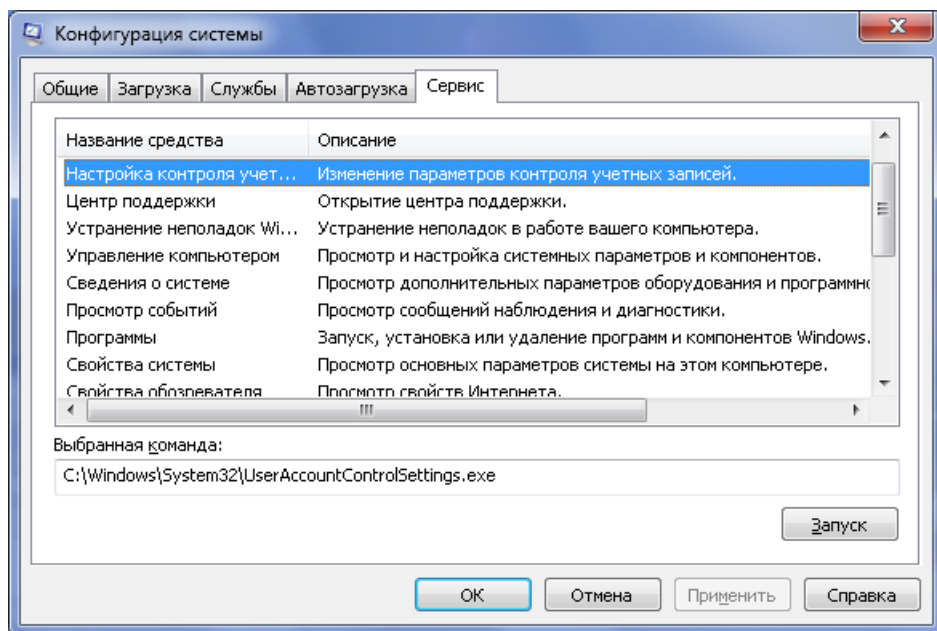


Рис. 4.28. Запуск апплета, управляющего поведением UAC, через утилиту msconfig.exe

Через групповые политики

Теперь попробуем выполнить настройку UAC через групповые политики. Для этого:

1. Щелкните мышью по кнопке **Пуск** (Start), введите в поле поиска строку `GPedit.msc`, а затем нажмите клавишу `<Enter>`.
2. Разверните окно консоли в левой панели окна **Редактор локальной групповой политики** (Local Group Policy Editor), как показано на рис. 4.29. Для этого выберите в дереве консоли следующие узлы: **Конфигурация компьютера** (Computer Configuration) | **Конфигурация Windows** (Windows Settings) | **Параметры безопасности** (Security Settings) | **Локальные политики** (Local Policies) | **Параметры безопасности** (Security Options).
3. Посмотрите, какое тут огромное количество локальных политик безопасности! Намного больше, чем в стандартных утилитах, которые мы рассмотрели только что. Это уже что-то, и оно гораздо интереснее, чем менять цвета кнопочек и рамок (хотя — как на чей вкус). Вот мне более интересно разобраться с UAC.

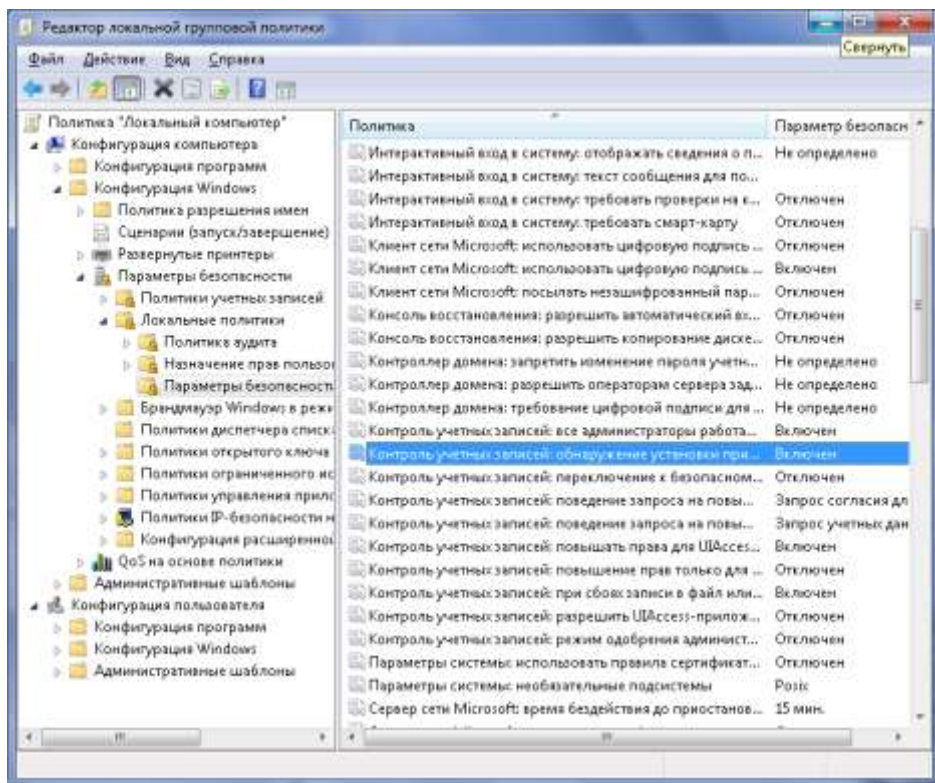


Рис. 4.29. Настройка параметров UAC через групповые политики

Чтобы блокировать работу UAC через групповые политики, настройте эти политики следующим образом:

- ❑ политика **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) — выберите значение **Повышение без запроса** (Elevate without prompt), как показано на рис. 4.30;
- ❑ политика **Контроль учетных записей: обнаружение установки приложений и запрос на повышение прав** (User Account Control: Detect application installations and prompt for elevation) — выберите значение **Отключен** (Disabled), как показано на рис. 4.31;
- ❑ политика **Контроль учетных записей: все администраторы работают в режиме одобрения администратором** (User Account Control: Run all administrators in Admin Approval Mode) — выберите значение **Отключен** (Disabled), как показано на рис. 4.32;

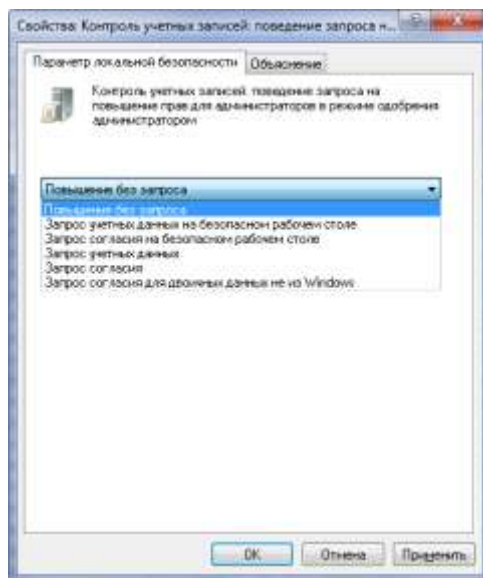


Рис. 4.30. Настройка политики **Контроль учетных записей: поведение запроса на повышение прав для администраторов в режиме одобрения администратором** (User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode)

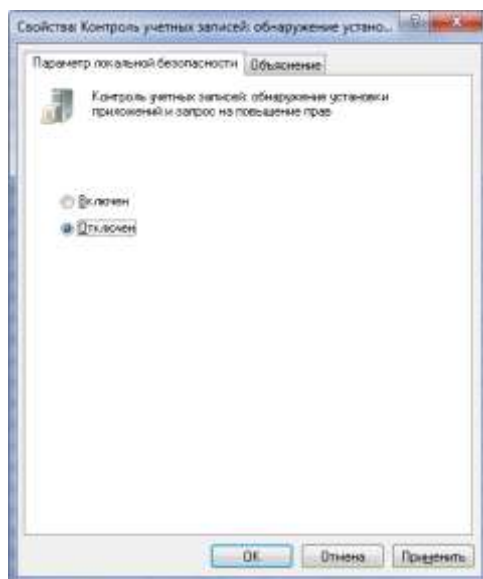


Рис. 4.31. Настройка политики **Контроль учетных записей: обнаружение установки приложений и запрос на повышение прав** (User Account Control: Detect application installations and prompt for elevation)

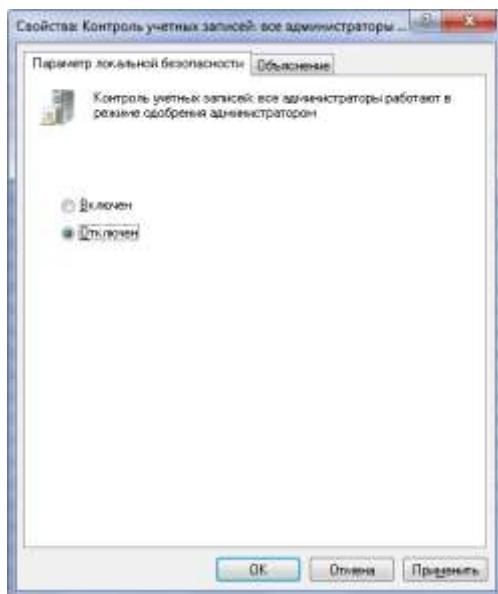


Рис. 4.32. Настройка политики **Контроль учетных записей: все администраторы работают в режиме одобрения администратором**
(User Account Control: Run all administrators in Admin Approval Mode)

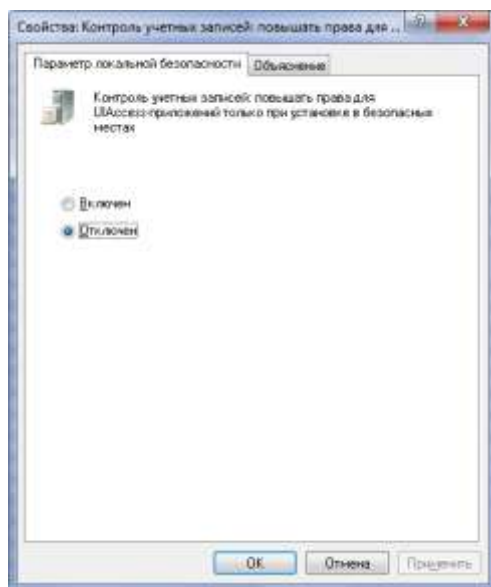


Рис. 4.33. Настройка политики **Контроль учетных записей: повышать права для UIAccess-приложений только при установке в безопасных местах**
(User Account Control: Only elevate UIAccess applications that are installed in secure locations)

- ❑ политика **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) — установите значение **Отключен** (Disabled), как показано на рис. 4.33.

Перезагрузите компьютер. Все, никакого UAC! Но тогда вы спросите — а почему тогда не пользоваться стандартными программами? Мой ответ будет таким: взгляните, ведь уровень избирательности тут намного выше, и вы можете выбирать различные комбинации различных политик. То есть настройка UAC окажется еще намного более точной и тонкой. Так, в приведенном примере UAC отключен только для пользователей с административными правами, а в отношении обычных пользователей UAC все равно продолжит действовать.

Через реестр

Давайте разберемся со всеми этими вопросами на примере настройки UAC через реестр. Для этого сделайте следующее:

1. Запустите Редактор реестра Regedit.exe любым из способов, описанных в главе 3.
2. Перейдите к ключу HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System (рис. 4.34).

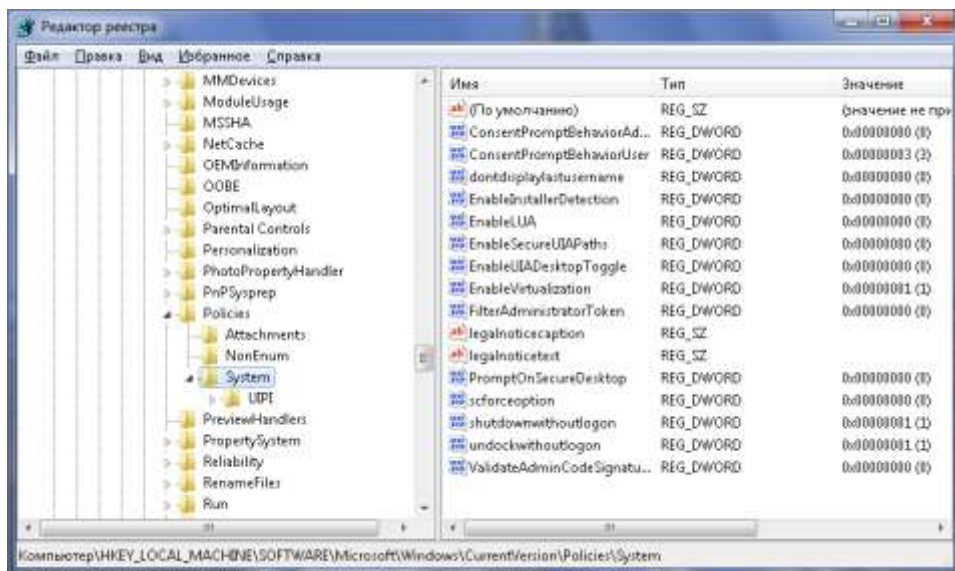


Рис. 4.34. Содержимое ключа реестра

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

ПРИМЕЧАНИЕ

Кстати, вы, наверное, уже обратили внимание, что все параметры, которые находятся в составе ключей с именем `Policies`, могут быть установлены и с помощью групповых политик, что и является более правильным и безопасным подходом, чем редактирование реестра. Напрямую редактировать реестр следует только тем, у кого нет возможности пользоваться групповыми политиками — например, пользователям Windows Vista/7 Home Edition. Ну, и, как вариант — если вы "воюете" с администратором, который вам что-то запретил.

3. Найдите параметр `EnableLUA` (тип данных `REG_DWORD`) и измените его значение на 0. Параноидальная система безопасности Windows Vista немедленно сигнализировала вам об этом, как об ошибке (рис. 4.35). Windows 7 относится к этому гораздо спокойнее и просто рекомендует выполнить перезагрузку (рис. 4.36). Чтобы внесенные изменения вошли в силу, сделайте именно то, о чем вас просят.

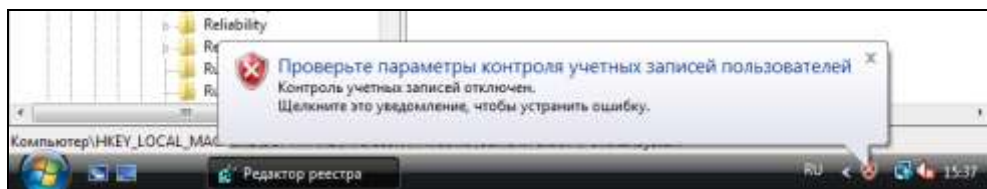


Рис. 4.35. Реакция Windows Vista на отключение UAC через реестр

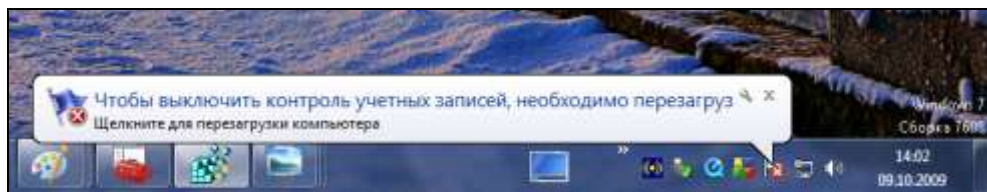


Рис. 4.36. Windows 7 реагирует на отключение UAC гораздо спокойнее

4. После перезагрузки попробуем запустить тот же редактор реестра, чтобы убедиться в том, что внесенные изменения вошли в силу. Да, так и есть — надоедливое окно UAC больше не появляется. Зато следует иметь в виду, что программа будет запущена с правами администратора, но ведь это ничуть нам не мешает.

Итак, мы добились своей цели — блокировали UAC и так и этак и, в конце концов — через реестр. Но нужно ли было это делать, если той же самой цели можно было добиться и через пользовательский интерфейс? Чтобы отве-

тить на этот вопрос, давайте исследуем содержимое ключа реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System` более подробно (листинг 4.1). Ведь, кроме параметра `EnableLUA`, там есть еще немало интересного! Чем же управляют эти параметры? А управляют они как раз настройками групповых политик.

В Windows Vista и Windows 7 в вариантах поставки Home и Home Premium, как уже говорилось, возможности управлять настройками групповых политик через пользовательский интерфейс нет, однако, несмотря на это, гибкую настройку можно произвести через реестр. Вот классический пример того, когда редактирование реестра просто необходимо для достижения требуемого результата!

Листинг 4.1. Параметры ключа реестра `[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]`, управляющие настройками UAC

```
"ConsentPromptBehaviorAdmin"=dword:00000000
"ConsentPromptBehaviorUser"=dword:00000001
"EnableInstallerDetection"=dword:00000001
"EnableLUA"=dword:00000001
"EnableSecureUIAPaths"=dword:00000001
"EnableVirtualization"=dword:00000001
"PromptOnSecureDesktop"=dword:00000000
"ValidateAdminCodeSignatures"=dword:00000000
"FilterAdministratorToken"=dword:00000000
```

Давайте поиграем с этими настройками! Вот, например, параметр `ConsentPromptBehaviorAdmin`, который по умолчанию установлен в значение 2. Логично будет предположить, что он управляет настройками UAC для пользователей с административными правами. Проведем простой эксперимент: вместо 2 установим для него значение 3, перезагрузимся и посмотрим, как изменилось поведение UAC (рис. 4.37).

Да, изменение действительно произошло! Если при заданном значении 2 в окне UAC для продолжения требовалось лишь нажать кнопку **Продолжить** (Continue), то теперь требуется ввести пароль, собственный или Администратора (надеюсь, вы не забыли его установить). Не знаю, как кому, а мне такое поведение нравится существенно больше, чем заданное по умолчанию.

В табл. 4.1 приведены установленные экспериментальным путем данные соответствия параметров ключа реестра `[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]` политикам безопасности, регулирующим настройки UAC.

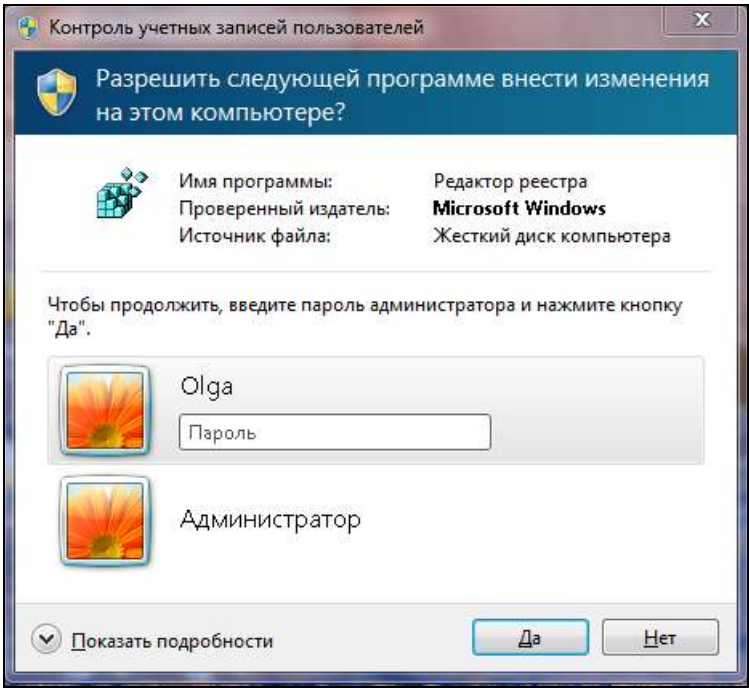


Рис. 4.37. Обратите внимание, как изменение параметра реестра ConsentPromptBehaviorAdmin изменило поведение UAC

Таблица 4.1. Параметры ключа реестра, отвечающие за настройку поведения UAC и их соответствие политикам безопасности

Параметр	Политика
ConsentPromptBehaviorAdmin	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)
ConsentPromptBehaviorUser	Контроль учетных записей: поведение запроса на повышение прав для обычных пользователей (User Account Control: Behavior of the Elevation Prompt For Standard Users)
EnableInstallerDetection	Контроль учетных записей: обнаружение установки приложений и запрос на повышение прав (User Account Control: Detect Application Installations and Prompt For Elevation)

Таблица 4.1 (окончание)

Параметр	Политика
EnableLUA	Контроль учетных записей: все администраторы работают в режиме одобрения администратором (User Account Control: Run All Administrators in Admin Approval Mode)
EnableSecureUIAPaths	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)
EnableVirtualization	Контроль учетных записей: при сбоях записи в файл или реестр виртуализация в место размещения пользователя (User Account Control: Virtualizes file and registry write failures to per-user locations)
FilterAdministratorToken	Контроль учетных записей: режим одобрения администратором для встроенной учетной записи администратора (User Account Control: Admin Approval Mode for the Built-in Administrator Account)
PromptOnSecureDesktop	Контроль учетных записей: переключение к безопасному рабочему столу при выполнении запроса на повышение прав (User Account Control: Switch to the secure desktop when prompting for elevation)
ValidateAdminCodeSignatures	Контроль учетных записей: повышение прав только для подписанных и проверенных исполняемых файлов (User Account Control: Only elevate executables that are signed and validated)

Настройка активации Windows

Как известно, в целях борьбы с пиратством Microsoft, начиная с выпуска Windows XP (а произошло это еще в 2001 году), требует т. н. *активации* продукта. В ранних выпусках Windows Vista существовала лазейка, позволяющая отложить процедуру активации на срок до 120 дней. Причем эта процедура была проста (выполнить ее мог даже новичок), не нарушала лицензионного соглашения и даже документирована³. Аналогичная лазейка есть и в Windows 7.

³ Более подробную информацию можно найти здесь: <http://technet2.microsoft.com/WindowsVista/en/library/aefc41f4-a3ec-4f98-a1dc-88a0d045172b1033.mspx?mfr=true>.

ПРИМЕЧАНИЕ

В этой главе процедура настройки активации Windows 7 рассматривается лишь на уровне инструкций. Вполне возможно также, что к тому моменту, когда эта книга окажется опубликованной, данная лазейка будет уже закрыта (скорее всего, именно так и будет). Тем не менее, на момент написания этой книги она действовала, причем отмечалось, что эта процедура абсолютно законна. А раз так, то почему бы не попробовать воспользоваться ею? В любом случае, даже если она и не сработает, вреда это не принесет и послужит хорошим упражнением на редактирование реестра.

Итак, чтобы отложить активацию, вам необходимо проделать следующее:

1. Установите копию Windows 7 и поработайте в ней в течение срока, не превышающего льготный период (30 дней). Просмотреть статус активации проще всего через Панель управления (Control Panel) — выполните двойной щелчок мышью на опции **Система** (System), и статус активации отобразится в нижней части окна (рис. 4.38). Еще один вариант просмотра срока истечения льготного периода заключается в том, чтобы запустить командную строку с правами администратора и дать команду `slmgr -xpr` (рис. 4.39).

ПРИМЕЧАНИЕ

Как известно, после истечения льготного периода Windows Vista позволяла пользователю зарегистрироваться в системе лишь для того, чтобы открыть Internet Explorer и активировать продукт через Интернет или приобрести новую лицензию, не позволяя выполнять никаких других действий. Впрочем, начиная с Windows Vista Service Pack 1, Microsoft от этой политики отошла, и даже при наличии проблем с активацией пользователи все же смогут получать к системе полный доступ. Правда, не спешите радоваться — проблемы у вас все равно возникнут. Во-первых, Windows (и Vista, и Windows 7) периодически будет назойливо напоминать о том, что данная копия должна быть активирована. Кроме того, каждый час экранные обои будут сбрасываться, изменяясь на пустой черный экран. Наконец, вы будете иметь ограниченный доступ к обновлениям и ограниченные возможности загрузки программ с сайта Microsoft. Дело в том, что Microsoft предоставляет доступ к этим возможностям только тем пользователям, которые прошли процедуру проверки с помощью программы проверки подлинности Windows (Windows Genuine Advantage), о чем будет рассказано далее в одной из последующих глав этой книги.

Так что, до истечения льготного периода лучше не доводить. Но и выполнять процедуру откладывания активации при таком статусе активации, как показано на рис. 4.40, тоже не рекомендуется, поскольку процедура отодвигает срок активации продукта ровно на 30 суток, считая с момента ее выполнения.

2. Запустите Редактор реестра и раскройте следующий ключ: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform` (рис. 4.41). Обратите внимание, что в Windows Vista этот ключ назывался `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SL`.

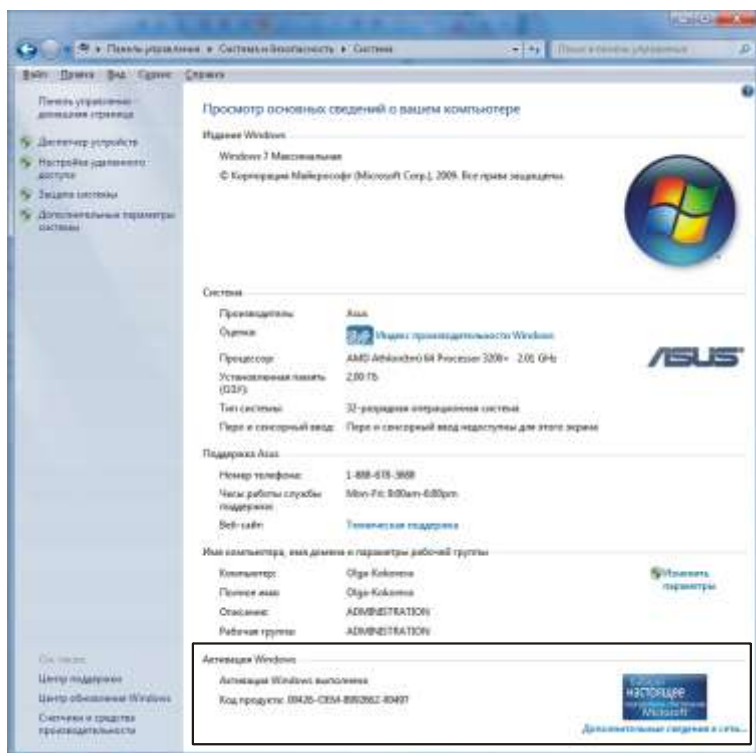


Рис. 4.38. Просмотр статуса активации через Панель управления

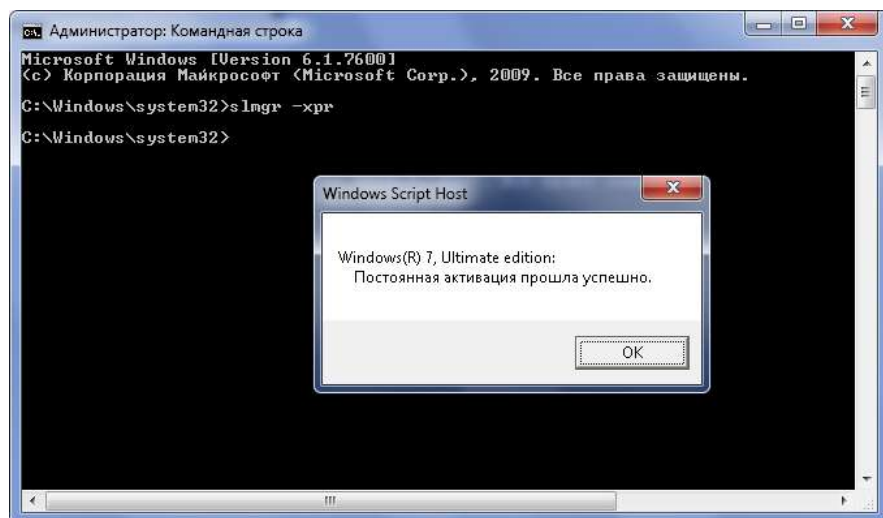


Рис. 4.39. Просмотр срока окончания льготного периода при помощи командной строки

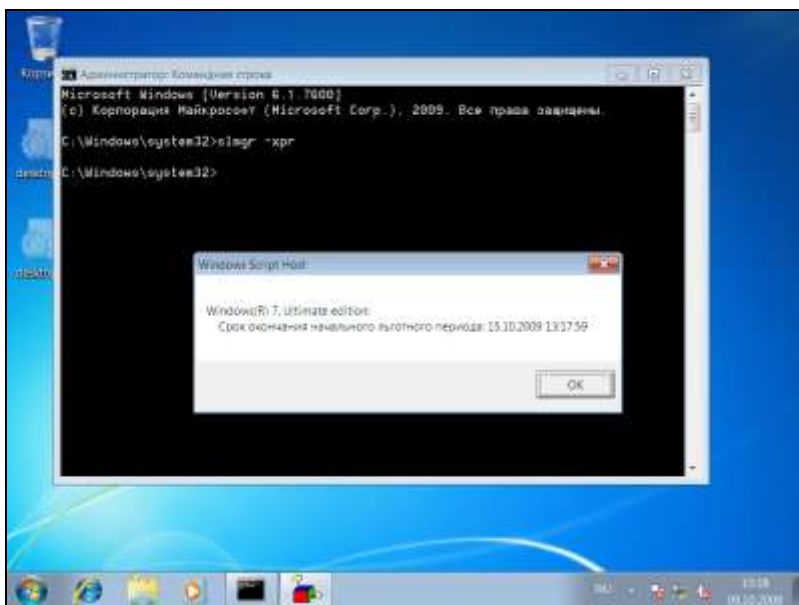


Рис. 4.40. Снимок был сделан 9 октября — у нас есть еще целых 5 дней...

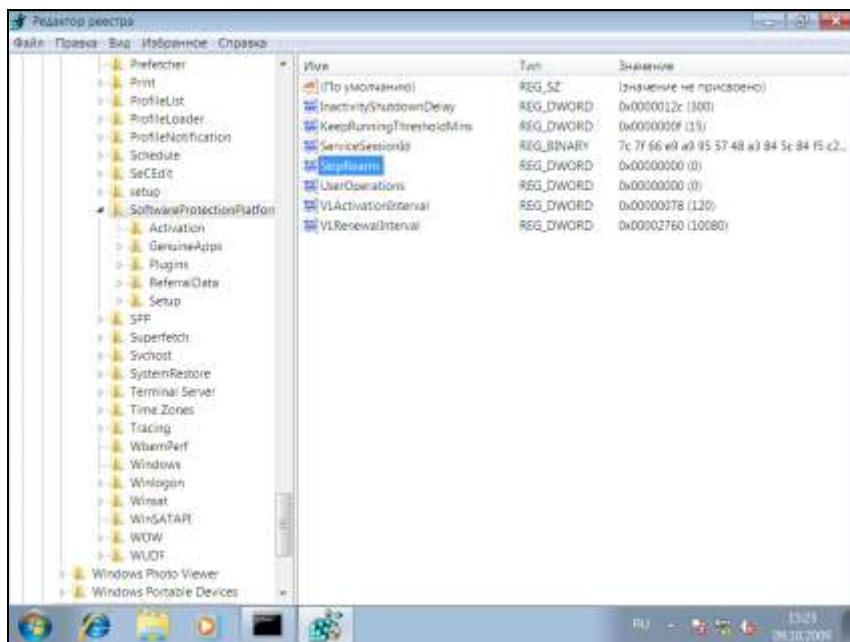


Рис. 4.41. Содержимое ключа реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform

3. Найдите в составе этого ключа параметр `SkipRearm`. По умолчанию этот параметр имеет тип данных `REG_DWORD` и значение `00000000h`. Установите для него значение `00000001h` и закройте редактор реестра.
4. Запустите командную строку с административными правами и дайте команду `slmgr -rearm`. Встроенный модуль Software Licensing Manager (SLMGR) передвинет срок активации на 30 суток с момента выполнения команды, причем ранее упомянутый параметр реестра `SkipRearm` при этом вновь будет переустановлен в 0. Внесенное изменение войдет в силу после перезагрузки.

ПРИМЕЧАНИЕ

Единственное, чего вам следует опасаться — так это того, что компьютер с предустановленной Windows 7 может оказаться настроенным таким образом, что описанная здесь процедура будет выполняться автоматически неопределенное количество раз, и вам как бы вовсе не придется заботиться об активации. Тем не менее, модуль SLMGR поддерживает счетчик количества запусков команды `slmgr -rearm`, так что в один далеко не прекрасный для вас день ваш компьютер все-таки потребует активации. Добросовестные поставщики компьютеров с предустановленными версиями — хоть Windows Vista, хоть Windows 7 — так не делают: обманывать клиента им просто невыгодно. Но вот если вы покупаете компьютер у малоизвестной фирмы или с рук, а цена кажется вам ну очень выгодной, — вот тут стоит задуматься.

Рассмотрим вкратце другие опции командной строки `slmgr`:

- ☐ `slmgr -dli` — отображает текущий статус активации и информацию о лицензии;
- ☐ `slmgr -ipk xxxx-xxxx-xxxx-xxxx` — позволяет заменить текущий ключ продукта (product key);
- ☐ `slmgr -xpr` — отображает дату истечения текущей лицензии;
- ☐ `slmgr -upk` — деинсталлирует текущий ключ продукта и переводит систему в состояние льготного периода;
- ☐ `slmgr -ato` — активирует текущую лицензию.

ПРИМЕЧАНИЕ

В целом тема активации Windows настолько сложна, что выходит за рамки данной главы. Она заслуживает более глубокого и серьезного рассмотрения и будет обсуждаться в одной из последующих книг.

Индивидуальная настройка процесса загрузки системы

Все современные операционные системы семейства Windows самостоятельно конфигурируют правильную последовательность загрузки, но огромному большинству пользователей требуется вносить в эту конфигурацию некоторые

изменения. Например, иногда необходимо изменить операционную систему, загружаемую по умолчанию (в системах с двойной загрузкой), увеличить интервал, в течение которого на экране отображается меню загрузки, добавлять индивидуальные файлы логотипа и т. п. В данном разделе рассмотрены основные методы, применяя которые можно выполнить индивидуальную настройку процесса загрузки. Эти необходимо знать каждому системному администратору, специалисту по поддержке и просто опытному пользователю.

ПРИМЕЧАНИЕ

Подробное рассмотрение всех процессов, происходящих при загрузке Windows Vista и Windows 7, а также описание роли реестра во всех этих процессах приведено в *главе 7*.

Простейший способ редактирования процесса загрузки

Простейший способ редактирования процесса загрузки операционной системы Windows 7 заключается в установке параметров ее запуска через утилиту **Система** (System) из Панели управления (Control Panel). С помощью этой утилиты можно задать временной интервал, в течение которого на экране должно отображаться меню загрузки. Если система мультизагрузочная, то пользователь сможет выбрать операционную систему, которая по истечении этого интервала будет загружена по умолчанию, если не выбрана ни одна из опций меню загрузки.

Вызовите утилиту **Система** (System) из Панели управления (Control Panel) и выберите опцию **Дополнительные параметры системы** (Additional system parameters). Перейдите к вкладке **Дополнительно** (Advanced) (рис. 4.42) и нажмите кнопку **Параметры** (Settings) в группе **Загрузка и восстановление** (Startup and Recovery). Откроется окно **Загрузка и восстановление** (Startup and Recovery) (рис. 4.43).

В верхней части этого окна имеется группа опций **Загрузка операционной системы** (System Startup), позволяющая указать операционную систему по умолчанию (в случае, когда на компьютере установлено несколько операционных систем) и задать временной интервал, в течение которого на экране будет отображаться меню загрузки.

Напомним, что в Windows XP в группе опций **Загрузка операционной системы** (System Startup) была предусмотрена возможность ручного редактирования файла Boot.ini. Для того чтобы перейти к этому варианту, достаточно было нажать кнопку **Правка** (Edit). Ни в Windows Vista, ни в Windows 7 вы ничего подобного не обнаружите — возможность редактирования загрузочного меню через пользовательский интерфейс была упразднена (см. рис. 4.43).

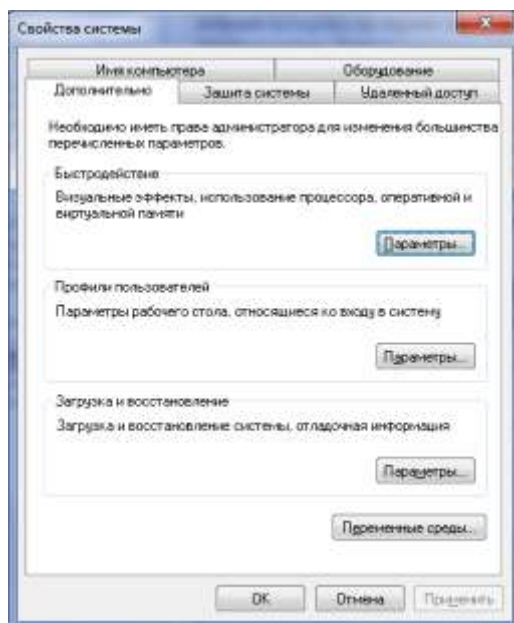


Рис. 4.42. Индивидуальная настройка процесса запуска Windows 7 через Панель управления

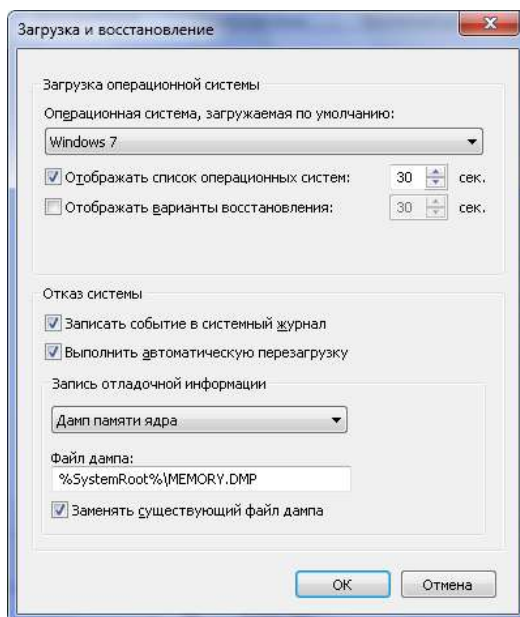


Рис. 4.43. Окно Загрузка и восстановление

С чем это связано? Как уже говорилось, в Windows Vista файл Boot.ini (обычный файл текстового формата, хранящийся в корневом каталоге системного раздела жесткого диска) был заменен базой данных BCD (Boot Configuration Data), которая унифицирует загрузочный механизм Windows Vista/7 таким образом, чтобы сделать его независимым от платформы (PC/AT BIOS или EFI).

ПРИМЕЧАНИЕ

EFI (Extensible Firmware Interface) — интерфейс расширяемого микропрограммного обеспечения. Это модель микропрограммного обеспечения следующего поколения, которая призвана заменить широко распространенные BIOS в течение ближайшего десятилетия. Более подробную информацию по данному вопросу можно найти в следующей книге: Салихан Д. *"BIOS: дизассемблирование, модификация, программирование"*. СПб., БХВ-Петербург, 2007.

База данных BCD хранится в реестре в двоичном виде, и, следовательно, теперь для конфигурирования загрузочного меню и его опций необходимо редактировать реестр. Однако делается это не с помощью редактора реестра, а с помощью специальных средств, к числу которых относятся:

- ❑ утилита **Система** (System) из Панели управления — с помощью этой утилиты (см. рис. 4.43) пользователи могут задать значения для следующих двух глобальных элементов BCD:
 - операционной системы, загружаемой по умолчанию и ее конфигурации;
 - времени ожидания (timeout), в течение которого на экране будет отображаться меню загрузки и список операционных систем;
- ❑ утилита **Конфигурация системы** (MSConfig.exe) — запустить эту утилиту можно в окне Панели управления опцией **Администрирование** (Administrative Tools) | **Конфигурация системы** (System Configuration) либо из командной строки с административными правами командой `Msconfig.exe`. Запустив утилиту, перейдите на вкладку **Загрузка** (Startup) (рис. 4.44). Утилита MSConfig.exe представляет собой основной инструмент редактирования параметров загрузки. Она позволяет устанавливать порядок загрузки операционных систем, а также указывать параметры отладки и загрузки в безопасном режиме (Safe Mode);
- ❑ утилита командной строки `BCDEdit.exe` — разумеется, эта утилита должна запускаться из командной строки с административными правами, причем в данном случае это вполне оправданно, поскольку она имеет множество опций, ее синтаксис не так уж и прост, а при редактировании следует соблюдать осторожность, так как многие опции придется вводить в шестнадцатеричных кодах. Эта утилита предназначена для специалистов из отдела

технической поддержки, а также для разработчиков ПО. Иными словами, по сложности эта операция не сравнима с ручным редактированием файла `Boot.ini`, поэтому в данной главе будет дана лишь вводная информация (более подробно и углубленно база данных BCD, ее формат, а также опции команды `Bcdedit` будут приведены в *главе 7*, посвященной детальному рассмотрению последовательности загрузки Windows Vista и Windows 7, а также в *главе 11*, посвященной вопросам устранения серьезных неполадок).

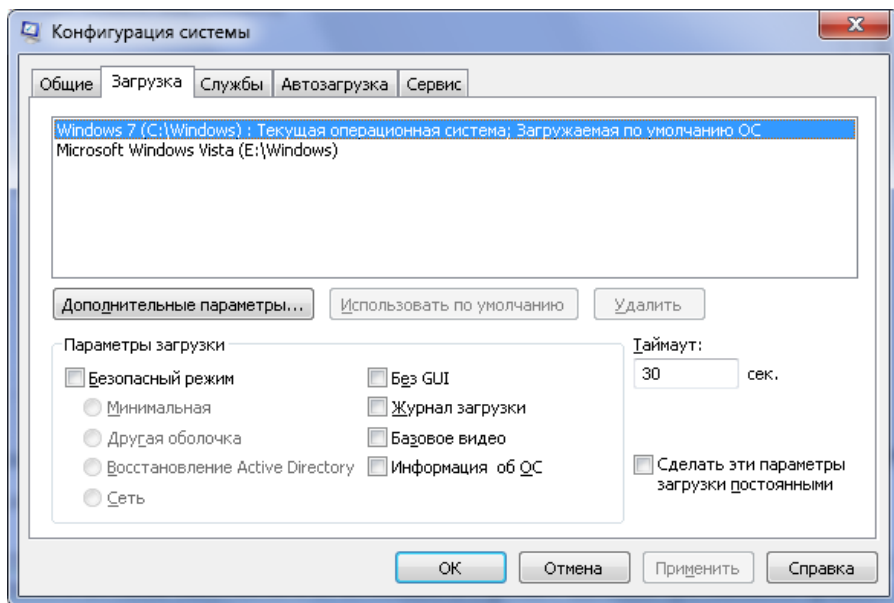


Рис. 4.44. Вкладка Загрузка (Boot) окна Конфигурация системы (System Configuration)

Вводная информация о редактировании базы данных BCD

Итак, начиная с Windows Vista, в системе появился новый компонент — база данных конфигурации загрузки (Boot configuration data, BCD), которая приходит на смену файлу `Boot.ini` и служит той же самой цели. Однако, в отличие от файла `Boot.ini`, BCD представляет собой улей реестра (`HKEY_LOCAL_MACHINE\BCD00000000`) и имеет иерархическую структуру (рис. 4.45), основными компонентами которой являются:

- ❑ *хранилища BCD* (компьютер со сложной загрузочной конфигурацией может иметь несколько хранилищ BCD), находящиеся на верхнем уровне

иерархии — служат контейнерами для объектов и элементов BCD, которые фактически и содержат данные, используемые при загрузке операционной системы. Обратите внимание, что эта структура повторяет иерархическую структуру реестра, который также содержит корневые ключи (root keys), вложенные ключи (keys) и параметры (value entries);

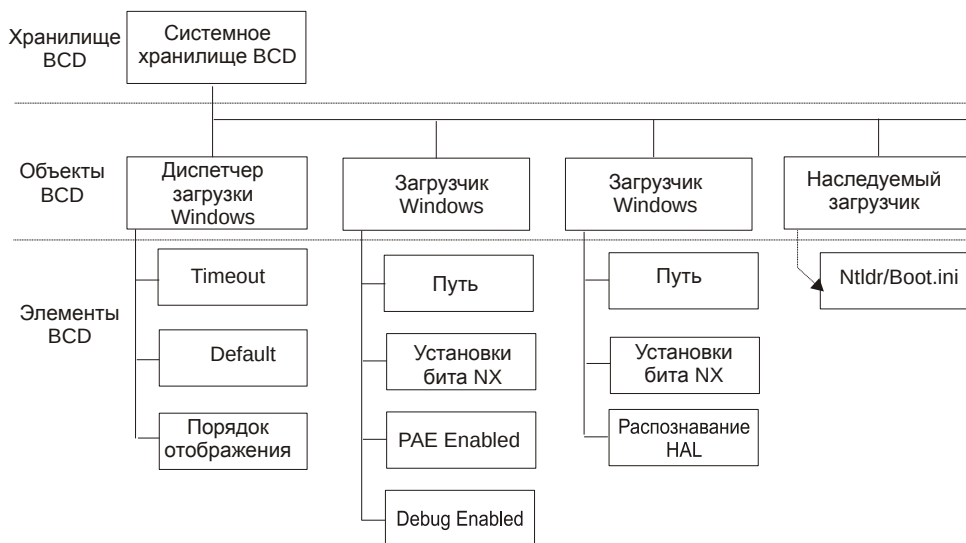


Рис. 4.45. Иерархическая структура BCD

□ *объекты BCD* — являются контейнерами элементов BCD. Наиболее распространенный тип объектов BCD описывает приложения среды загрузки (boot environment applications), например, один или несколько экземпляров загрузчика Windows. Windows Vista/7 включает целый ряд новых загрузочных приложений, в том числе:

- Bootmgr — Диспетчер загрузки, управляющий ходом загрузки системы. В мультизагрузочных системах диспетчер загрузки отображает меню, позволяющее выбрать операционную систему, которая должна быть загружена;
- Winload.exe — Загрузчик операционной системы Windows Vista/7, он создает среду исполнения при загрузке, а также загружает ядро Windows Vista/7, уровень аппаратных абстракций (HAL) и драйверы времени загрузки;
- Winresume.exe — загрузчик возобновления (resume loader). Каждая копия Windows Vista/7 или Windows Server, установленная на компьюте-

ре, имеет собственную копию Winresume.exe, которая восстанавливает систему в ее рабочее состояние после режима "сна" (hibernation);

- ❑ *элементы BCD* — элементы данных, например, имена загрузочных приложений (Bootmgr, Winload, Winresume и т. д.), устройств операционной системы, отладочные параметры.

Как правило, типичное хранилище BCD имеет не менее двух (а в случае мультизагрузочной системы — и большее количество) объектов BCD, в том числе:

- ❑ объект Диспетчера загрузки Windows (Windows boot manager) — в составе этого объекта хранятся элементы, ответственные за вывод меню выбора операционной системы, меню выбора загрузчика, операционной системы, загружаемой по умолчанию (параметр `Default`, см. рис. 4.37), и времени ожидания (Timeout), в течение которого меню загрузки отображается на экране;
- ❑ один или несколько объектов Загрузчика Windows (Windows boot loader), которые хранят конфигурационную информацию Windows Vista/7 или Windows Server для каждой из копий операционной системы, установленной на компьютере. Эти объекты содержат элементы BCD, использующиеся при загрузке и инициализации Windows, например, параметры защиты страниц памяти от исполнения (настройки бита `no-execute`, NX), политики расширения физических адресов (Physical Address Extension, PAE), настройки отладчиков уровня ядра (kernel debugger settings) и т. д. Опытные системные администраторы, имеющие богатый опыт ручного редактирования файла `Boot.ini`, без особого труда найдут аналогии между этими параметрами и соответствующими ключами файла `Boot.ini`;

ПОЯСНЕНИЕ

Расширение физических адресов (Physical Address Extension, PAE) X86 позволяет программному обеспечению с интерфейсом программирования AWE (Address Windowing Extensions) на компьютерах с процессором Intel Pentium Pro или более поздним и с объемом физической памяти свыше 4 Гбайт отобразить в виртуальное адресное пространство приложения больший объем физической памяти.

- ❑ если на компьютере присутствует одна из предшествующих версий Windows, например, Windows XP, то в хранилище BCD будет присутствовать и объект `Ntldr`. Назначение этого объекта состоит в указании пути к файлу `Ntldr`, который будет использоваться для загрузки более ранних версий Windows;
- ❑ необязательные приложения времени загрузки, например, Windows Memory Tester — приложение, использующееся для выполнения диагностики памяти.

Как уже говорилось ранее, для выполнения элементарной настройки процесса загрузки системы рекомендуется использовать утилиту **Система** из Панели управления или утилиту MSconfig.exe. Утилиту BCDedit, по крайней мере, на первых порах, следует применять с большой осторожностью. Сейчас мы не будем останавливаться на ней подробно, так как ее неумелое применение практически гарантирует повреждение загрузочной конфигурации вашей системы. Детальное обсуждение утилиты BCDedit мы отложим до *главы 7*. Тем не менее, в качестве простого ознакомительного упражнения запустите командную строку с административными правами и выполните следующую команду:

```
bcdedit /enum all /v
```

Как несложно догадаться, эта команда выведет подробную информацию о загрузочной конфигурации вашей системы. Пример вывода этой команды показан в листинге 4.2 (в вашем случае эта информация будет отличаться).

Листинг 4.2. Пример вывода команды Bcdedit /enum all /v

```
Windows Boot Manager
```

```
-----
```

```
identifier          {9dea862c-5cdd-4e70-accl-f32b344d4795}
device              partition=\Device\HarddiskVolume1
description         Windows Boot Manager
locale              en-US
inherit              {7ea2elac-2e61-4728-aaa3-896d9d0a9f0e}
default              {ef9cdb11-2f8b-11de-a6b2-cd25fb59494a}
resumeobject        {ef9cdb10-2f8b-11de-a6b2-cd25fb59494a}
displayorder         {466f5a88-0af2-4f76-9038-095b170dc21c}
                    {ef9cdb11-2f8b-11de-a6b2-cd25fb59494a}
                    {88ea8542-64ff-11dc-9914-e5e19e823720}
                    {58013c5c-7309-11db-a958-dd89cfabe520}
toolsdisplayorder    {b2721d73-1db4-4c62-bf78-c548a880142d}
timeout              30
```

```
Windows Boot Loader
```

```
-----
```

```
identifier          {58013c5c-7309-11db-a958-dd89cfabe520}
device              unknown
path                \Windows\system32\winload.exe
```

```
description      Microsoft Windows Vista
locale           en-US
inherit          {6efb52bf-1766-41db-a6b3-0ee5eff72bd7}
osdevice         unknown
systemroot       \Windows
resumeobject     {58013c5d-7309-11db-a958-dd89cfabe520}
nx               OptIn
custom:42000002  \system32\winload.exe
custom:45000001  2
custom:47000005  301989892
                  3
```

Windows Boot Loader

```
identifier       {88ea8542-64ff-11dc-9914-e5e19e823720}
device           partition=E:
path             \Windows\system32\winload.exe
description      Microsoft Windows Vista
locale           ru-RU
inherit          {6efb52bf-1766-41db-a6b3-0ee5eff72bd7}
osdevice         partition=E:
systemroot       \Windows
resumeobject     {88ea8543-64ff-11dc-9914-e5e19e823720}
nx               OptOut
custom:42000002  \system32\winload.exe
custom:45000001  2
custom:47000005  301989892
                  3
```

Windows Boot Loader

```
identifier       {ef9cdb0e-2f8b-11de-a6b2-cd25fb59494a}
device           ramdisk=[C:]\Recovery\ef9cdb0e-2f8b-11de-a6b2-
cd25fb59494a\Winre.wim, {ef9cdb0f-2f8b-11de-a6b2-cd25fb59494a}
path             \windows\system32\winload.exe
description      Windows Recovery Environment
inherit          {6efb52bf-1766-41db-a6b3-0ee5eff72bd7}
osdevice         ramdisk=[C:]\Recovery\ef9cdb0e-2f8b-11de-a6b2-
cd25fb59494a\Winre.wim, {ef9cdb0f-2f8b-11de-a6b2-cd25fb59494a}
```

systemroot	\windows
nx	OptIn
detecthal	Yes
winpe	Yes
custom:46000010	Yes

Windows Boot Loader

```
-----
identifier          {ef9cdb11-2f8b-11de-a6b2-cd25fb59494a}
device              partition=C:
path                \Windows\system32\winload.exe
description          Windows 7
locale              en-US
inherit              {6efb52bf-1766-41db-a6b3-0ee5eff72bd7}
recoverysequence     {ef9cdb12-2f8b-11de-a6b2-cd25fb59494a}
recoveryenabled      Yes
osdevice             partition=C:
systemroot           \Windows
resumeobject         {ef9cdb10-2f8b-11de-a6b2-cd25fb59494a}
nx                  OptIn
```

Windows Boot Loader

```
-----
identifier          {ef9cdb12-2f8b-11de-a6b2-cd25fb59494a}
device              ramdisk=[C:]\Recovery\ef9cdb12-2f8b-11de-a6b2-
cd25fb59494a\Winre.wim,{ef9cdb13-2f8b-11de-a6b2-cd25fb59494a}
path                \windows\system32\winload.exe
description          Windows Recovery Environment
inherit              {6efb52bf-1766-41db-a6b3-0ee5eff72bd7}
osdevice             ramdisk=[C:]\Recovery\ef9cdb12-2f8b-11de-a6b2-
cd25fb59494a\Winre.wim,{ef9cdb13-2f8b-11de-a6b2-cd25fb59494a}
systemroot           \windows
nx                  OptIn
winpe                Yes
custom:46000010      Yes
```

Resume from Hibernation

```
-----
identifier          {58013c5d-7309-11db-a958-dd89cfabe520}
```

device	unknown
path	\Windows\system32\winresume.exe
description	Windows Resume Application
locale	en-US
inherit	{1afa9c49-16ab-4a5c-901b-212802da9460}
filepath	\hiberfil.sys
pae	Yes
debugoptionenabled	No
custom:42000002	\system32\winresume.exe
custom:45000001	2
custom:46000004	Yes

Resume from Hibernate

```

-----
identifier      {88ea8543-64ff-11dc-9914-e5e19e823720}
device          partition=E:
path            \Windows\system32\winresume.exe
description     Windows Resume Application
locale          ru-RU
inherit         {1afa9c49-16ab-4a5c-901b-212802da9460}
filedevice      partition=E:
filepath        \hiberfil.sys
pae             Yes
debugoptionenabled No
custom:42000002 \system32\winresume.exe
custom:45000001 2
custom:46000004 Yes

```

Resume from Hibernate

```

-----
identifier      {ef9cdb10-2f8b-11de-a6b2-cd25fb59494a}
device          partition=C:
path            \Windows\system32\winresume.exe
description     Windows Resume Application
locale          en-US
inherit         {1afa9c49-16ab-4a5c-901b-212802da9460}
filedevice      partition=C:
filepath        \hiberfil.sys
pae             Yes

```

debugoptionenabled No

Windows Memory Tester

identifier	{b2721d73-1db4-4c62-bf78-c548a880142d}
device	partition=\Device\HarddiskVolume1
path	\boot\memtest.exe
description	Windows Memory Diagnostic
locale	en-US
inherit	{7ea2e1ac-2e61-4728-aaa3-896d9d0a9f0e}
badmemoryaccess	Yes

Windows Legacy OS Loader

identifier	{466f5a88-0af2-4f76-9038-095b170dc21c}
device	partition=\Device\HarddiskVolume1
path	\ntldr
description	Earlier Version of Windows

EMS Settings

identifier	{0ce4991b-e6b3-4b16-b23c-5e0d9250e5d9}
bootems	Yes

Debugger Settings

identifier	{4636856e-540f-4170-a130-a84776f4c654}
debugtype	Serial
debugport	1
baudrate	115200

RAM Defects

identifier	{5189b25c-5558-4bf2-bca4-289b11bd29e2}

Global Settings

identifier	{7ea2e1ac-2e61-4728-aaa3-896d9d0a9f0e}
inherit	{4636856e-540f-4170-a130-a84776f4c654}

```
{0ce4991b-e6b3-4b16-b23c-5e0d9250e5d9}
{5189b25c-5558-4bf2-bca4-289b11bd29e2}
```

Boot Loader Settings

```
identifier      {6efb52bf-1766-41db-a6b3-0ee5eff72bd7}
inherit         {7ea2e1ac-2e61-4728-aaa3-896d9d0a9f0e}
               {7ff607e0-4395-11db-b0de-0800200c9a66}
```

Hypervisor Settings

```
identifier      {7ff607e0-4395-11db-b0de-0800200c9a66}
hypervisordebugtype  Serial
hypervisordebugport  1
hypervisorbaudrate   115200
```

Resume Loader Settings

```
identifier      {1afa9c49-16ab-4a5c-901b-212802da9460}
inherit         {7ea2e1ac-2e61-4728-aaa3-896d9d0a9f0e}
```

Device options

```
identifier      {ef9cdb0f-2f8b-11de-a6b2-cd25fb59494a}
description     Ramdisk Options
ramdisksddevice partition=C:
ramdisksdipath  \Recovery\ef9cdb0e-2f8b-11de-a6b2-cd25fb59494a\boot.sdi
```

Device options

```
identifier      {ef9cdb13-2f8b-11de-a6b2-cd25fb59494a}
description     Ramdisk Options
ramdisksddevice partition=C:
ramdisksdipath  \Recovery\ef9cdb12-2f8b-11de-a6b2-cd25fb59494a\boot.sdi
```

В качестве полезного упражнения рекомендуется также поменять, например, время ожидания при выводе меню загрузки, дав команду `bcdedit /timeout 60`.

Решение проблемы с несовместимостью точек восстановления в системах с двойной загрузкой Windows XP и Windows Vista/7

Наконец, в заключение этой длинной-предлинной главы, приведем обещанное решение проблемы с исчезновением точек восстановления Windows Vista и Windows 7 в системах, где она сосуществует с Windows XP.

Решение это очень простое — загрузитесь в Windows XP, запустите редактор реестра и найдите ключ `HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices\Offline`. В состав этого ключа добавьте параметр `\DosDevices\D:` с типом данных `REG_DWORD` и установите для него значение 1.

ПРИМЕЧАНИЕ

Эта рекомендация приведена в предположении, что Windows XP установлена на разделе C:, а Windows Vista или Windows 7 — на разделе D:. Кроме того, если подключ `HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices\Offline` не существует, его следует создать вручную.

Заключение

Рекомендации, приведенные в этой "разминочной" главе, отнюдь не охватывают всего спектра настроек Windows 7. Напротив, ее цель — помочь читателю, овладевшему необходимыми начальными знаниями о реестре, овладеть практическими навыками и "обжиться" в системе Windows 7, попутно ознакомившись с некоторыми из наиболее важных ее нововведений.

Глава 5



Реестр и аппаратные средства в Windows 7

Когда дела идут хорошо, что-то должно случиться в самом ближайшем будущем.

Второй закон Чизхолма

Все мы пленники в тюрьме наших устройств... Plug and Pray!

Фольклор

Ограниченная поддержка аппаратных средств и частые перезагрузки были наиболее серьезными недостатками Windows NT. Начиная с Windows 2000/XP, Microsoft начала предпринимать последовательные усилия по их устранению за счет реализации поддержки технологии Plug and Play. Так, в системе Windows Vista поддержка устройств подверглась дальнейшей переработке и оптимизации, причем особого внимания заслуживают следующие нововведения:

- ☐ организовано новое хранилище драйверов;
- ☐ введен новый алгоритм классификации драйверов;
- ☐ появились новые средства управления пакетами драйверов.

В Windows 7 был сделан существенный рывок вперед. В числе нововведений в ней реализованы следующие технологии:

- ☐ новая версия Direct3D — Direct3D 11 — предлагает множество новых возможностей, например, многопоточную визуализацию (rendering);
- ☐ существенно расширена поддержка аудиоустройств Bluetooth;
- ☐ появилась поддержка Wireless USB (WUSB) — нового стандарта, направленного на избавление традиционного интерфейса USB от проводов¹;

¹ Более подробно с этим новым стандартом можно ознакомиться, прочитав следующие источники: http://en.wikipedia.org/wiki/Wireless_USB, <http://www.3dnews.ru/communication/wusb/>, <http://www.usb.org/developers/wusb/>.

- ❑ введена новая технология поддержки защищенного вещания (Protected Broadcast Driver Architecture, PBDA) — за счет этого в состав Windows Media Center была встроена поддержка бесплатных и платных TV-сервисов;
- ❑ появилась поддержка телевидения высокой четкости (HDTV) — так, Windows 7 теперь работает с видеокамерами AVCHD² и Web-камерами нового поколения, которые обеспечивают быстрое сжатие;
- ❑ реализована улучшенная поддержка твердотельных накопителей, и теперь операционная система может их уникальным образом идентифицировать;
- ❑ существенно улучшено управление электропитанием и энергосберегающими режимами, а в модель системных сервисов внесены серьезные изменения, призванные ускорить их запуск и усовершенствовать защиту среды;

² **AVCHD** — (Advanced Video Codec High Definition), продвинутый видеокодек высокого разрешения) — формат записи видео, предусматривающий запись на безленточные носители. Формат AVCHD предназначен для записи видео высокой четкости в режимах 720p и 1080i. Здесь значения 720 и 1080 обозначают разрешение (Definition) — количество строк горизонтальной развертки. В принципе, одно изображение может передаваться как полный кадр (p) или как два последовательных поля (i). Характер изображения и соответствующие процессы будут в этих двух случаях различными:

- суффикс p означает progressive (прогрессивный), поскольку в этом случае строки изображения записываются в порядке своего нормального следования (1, 2, 3, 4, 5, ...). Так как при этом полное изображение (полный кадр) получается за один проход, такой режим очень хорошо совместим с компьютерами, плазменными и жидкокристаллическими (TFT) экранами и проекторами, работающими именно с полными кадрами;
- суффикс i означает interlaced (чересстрочный), т. е. систему развертки на базе двух полей. В видеоформатах поля, или "чересстрочные" изображения, использовались для экономии полосы. Первое и второе поля различаются по времени следования и по содержанию изображения. Первое поле содержит нечетные строки (1, 3, 5, 7, ...), второе — только четные (2, 4, 6, 8, ...).

Запись AVCHD производится на 8-сантиметровые перезаписываемые диски (AVCHD, Blu-ray), жесткие диски и карты памяти SD и Memory Stick Pro (http://en.wikipedia.org/wiki/Memory_Stick_Pro) и позиционируется как альтернатива существующим форматам DV и HDV (<http://en.wikipedia.org/wiki/HDV>) в сфере малобюджетного видеопроизводства. Дополнительную информацию об AVCHD и другие сведения о стандартах HDTV можно найти по следующим адресам:

<http://ru.wikipedia.org/wiki/AVCHD>,

<http://en.wikipedia.org/wiki/AVCHD>,

http://en.wikipedia.org/wiki/High-definition_television,

<http://electronics.howstuffworks.com/hdtv.htm>,

<http://www.gs.ru/info/si/hdtv.html>,

<http://hdtv.sharereactor.ru/hdtv-faq.html>,

<http://www.dnk.ru/articles/article.php?LID=1568&AID=30339>,

<http://www.videoton.ru/Articles/HDTV/1080i.html>,

<http://www.gs.ru/info/si/hdtv.html#STAND>, <http://kunegin.narod.ru/ref1/hdtv1/index.htm>.

□ наконец, Windows 7 позволяет примонтировать виртуальный жесткий диск (virtual hard disk, VHD) как обычный диск, а загрузчик, входящий в состав Windows 7, позволяет осуществлять загрузку операционной системы с такого VHD-диска.

В этой главе мы подробно рассмотрим концепцию Plug and Play (PnP), а в дальнейших главах раскроем и все остальные усовершенствования, достигнутые в Windows 7.

Установка новых устройств в Windows 7

Установка в автоматическом режиме

Что происходит с системой при установке в ней нового устройства? Даже если Windows встречает новое устройство, на текущий момент не занесенное в реестр, и система не знает, как с ним работать, то она, прежде всего, пытается его идентифицировать.

ПРИМЕЧАНИЕ

Если вы планируете приобретать новые устройства для установки на компьютер, работающий под управлением Windows 7, то рекомендуется предварительно проверить наличие выбранного вами устройства в списке совместимого оборудования (Hardware compatibility list, HCL). Информацию о HCL для Windows 7 можно найти здесь: <http://www.hclstore.in/windows7/>. Если ваше устройство присутствует в этом списке, оно гарантированно будет работать под Windows 7.

Реакция Windows 7 на появление в системе нового устройства зависит от метода его подключения. Например, если вы подключаете к работающему компьютеру внешнее устройство через порт USB или IEEE 1394, то Windows 7 обнаружит его немедленно и попытается установить для него драйвер. Если для установки нового устройства вы выключали компьютер, то оно будет обнаружено при следующем его включении, и операционная система точно так же попытается установить для этого устройства подходящий драйвер. В любом случае, если новое устройство было успешно определено и распознано, а подходящий драйвер обнаружен и успешно установлен, то все дальнейшие шаги будут выполнены автоматически. Через несколько секунд вы увидите всплывающее окно, сообщающее о том, что новое устройство готово к использованию. Такой пример был приведен в *главе 1* (см. рис. 1.6–1.8).

Установка "вручную"

А что делать, если устройство, которое вы уже приобрели или планируете приобрести, в этом списке отсутствует? И как быть со старыми устройствами

(legacy devices), официально не поддерживаемыми в этой системе? Значит ли это, что такие устройства установить и сконфигурировать нельзя? Проблема действительно существует, но, вопреки распространенному мнению, она во многих случаях может быть решена, просто при этом задачи установки и конфигурирования нового устройства несколько усложняются.

ПРИМЕЧАНИЕ

Даже если имеющееся у вас устройство и не снабжено логотипом Designed for Windows 7 и не перечислено в списке совместимых аппаратных средств, не спешите опускать руки. В этой главе я постараюсь показать вам, что дела не так плохи, и проблема вполне разрешима. Вспомните, за что многие пользователи ругали Vista, причем вполне справедливо? Да, в том числе — и за сильно усеченную поддержку старых, так называемых *наследуемых* (legacy) устройств. Дело в том, что некоторые поставщики действительно не торопились предлагать драйверы для Vista в период ее бета-тестирования. Но к моменту выхода Vista многие из них уже пересмотрели свою позицию и разработали драйверы для выпускаемых ими устройств. Что же касается Windows 7, то в ней разработчики провели серьезную работу над ошибками, и ситуация изменилась в лучшую сторону.

Давайте посмотрим, как следует решать проблему, если Windows 7 не сможет выполнить установку драйвера в автоматическом режиме (рис. 5.1).

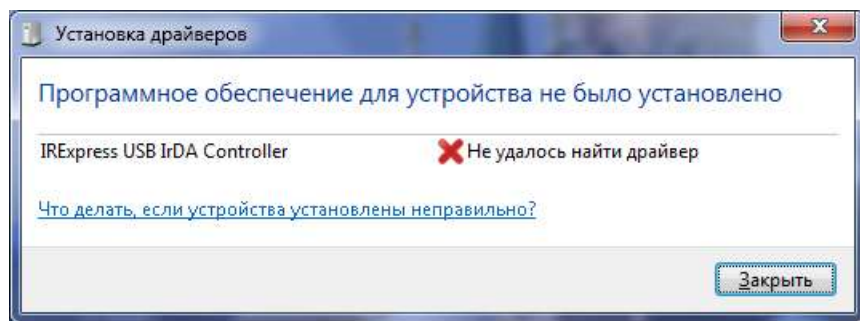


Рис. 5.1. Windows 7 не смогла завершить установку драйвера устройства в автоматическом режиме

В таком случае Microsoft дает несколько рекомендаций, выполнять которые можно в любой последовательности.

Во-первых, можно открыть Панель управления (Control Panel) и проверить, нет ли среди доступных обновлений современной версии драйвера для вашего устройства (рис. 5.2).

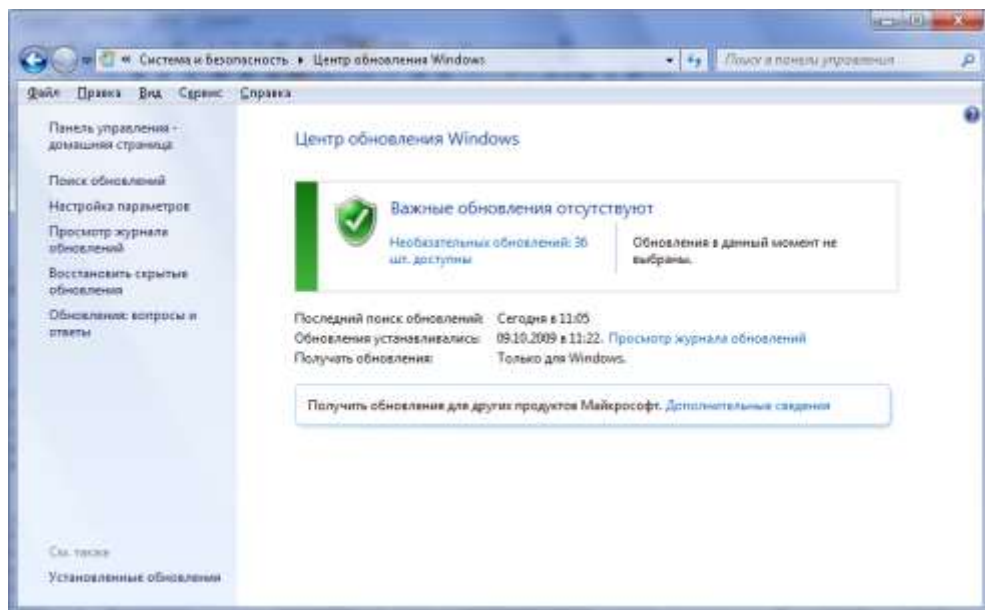


Рис. 5.2. Проверка доступных обновлений

ПРИМЕЧАНИЕ

Чтобы Windows имела возможность устанавливать обновления и в оперативном режиме искать обновления для драйверов устройств, ваш компьютер должен быть подключен к Интернету.

Windows не сможет автоматически искать последние обновления для драйверов, если в системе выключена опция автоматического обновления. Кроме того, вы можете задать опции поведения системы при установке драйверов. Для этого сделайте следующее:

1. Откройте окно Панели управления (Control Panel) и выберите опции **Оборудование и звук** (Hardware and Sound) | **Устройства и принтеры** (Devices and Printers). Щелкните правой кнопкой мыши по значку, соответствующему вашему компьютеру (в приведенном примере это — значок **OLGA-KOKOREVA**) и из раскрывшегося контекстного меню выберите команду **Параметры установки устройств** (Device Installation Settings). Откроется окно, показанное на рис. 5.3.
2. Если вы хотите, чтобы система автоматически загружала драйверы для установленных в вашей системе устройств, выберите из списка опцию **Да, делать это автоматически** (рекомендуется) (Yes, do this automatically (recommended)). С другой стороны, вы можете отказаться от опции авто-

матического режима — выберите для этого опцию **Нет, предоставить возможность выбора** (No, let me choose what to do) и укажите, следует ли всегда устанавливать наиболее подходящие драйверы из Центра обновления Windows (Windows Update Center), устанавливать ли их в том случае, если нужного драйвера нет на вашем компьютере, или же не стоит устанавливать драйверы с сайта Windows Update никогда.

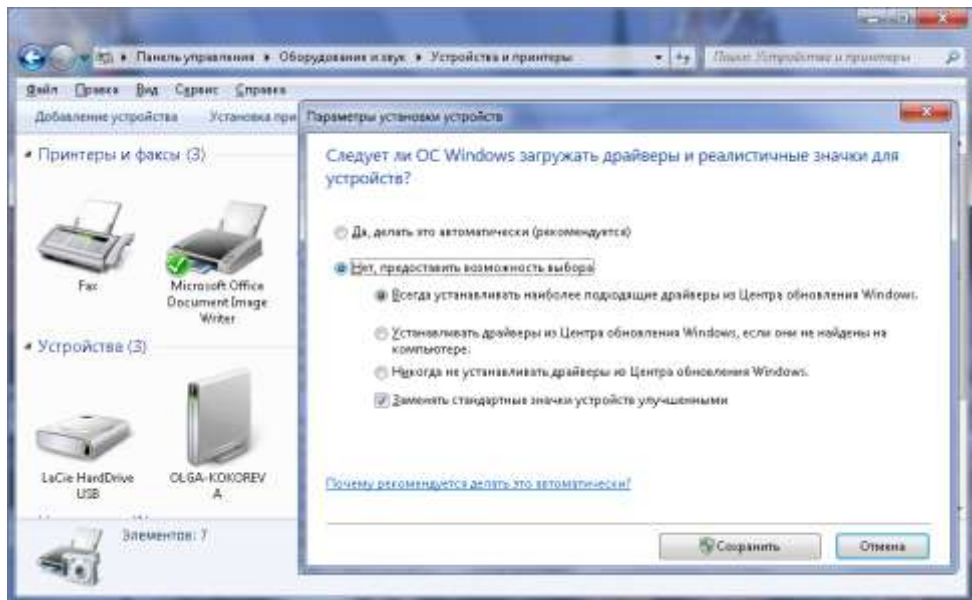


Рис. 5.3. Управление опциями инсталляции драйверов устройств

3. Наконец, вы можете самостоятельно посетить сайт производителя устройства, чтобы скачать драйвер. Во многих (но не во всех) случаях, даже если драйвер для Windows 7 еще не выпущен, можно воспользоваться драйвером для Windows Vista — существует вероятность, что он будет работать вполне удовлетворительно.
4. Скачав драйвер, вы можете действовать "по старинке" — так, как делали это в Windows XP и Windows Vista. Для этого запустите Диспетчер устройств (Device Manager). Самый простой и привычный способ сделать это предоставляется через Панель управления (Control Panel). Когда запустится Диспетчер устройств, выберите из меню **Действие** (Action) команду **Установить старое устройство** (Add legacy hardware), и запустится старый добрый мастер установки аппаратных средств (Add Hardware Wizard), хорошо нам знакомый еще со времен Windows XP (рис. 5.4).

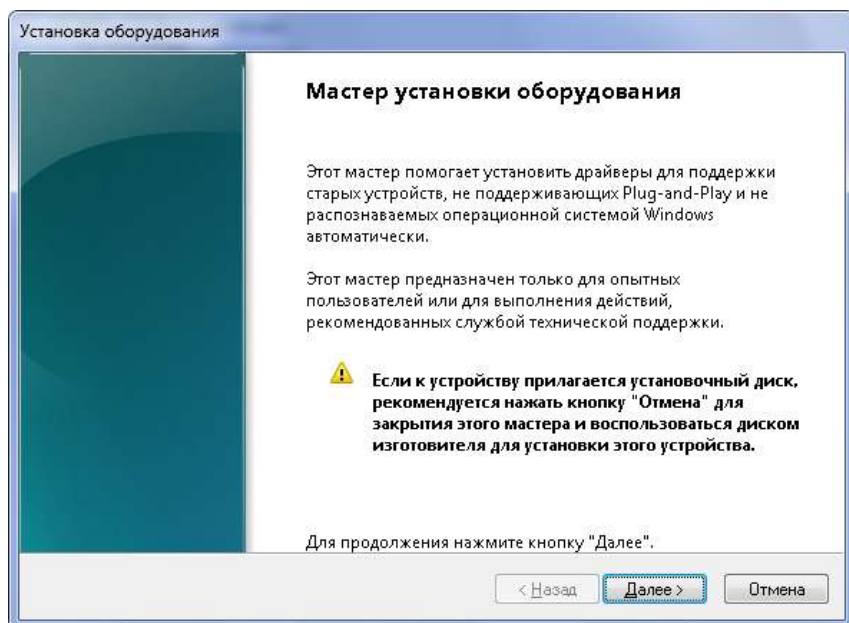


Рис. 5.4. В Windows 7 имеется и старый добрый мастер установки оборудования, так хорошо знакомый всем опытным пользователям Windows XP

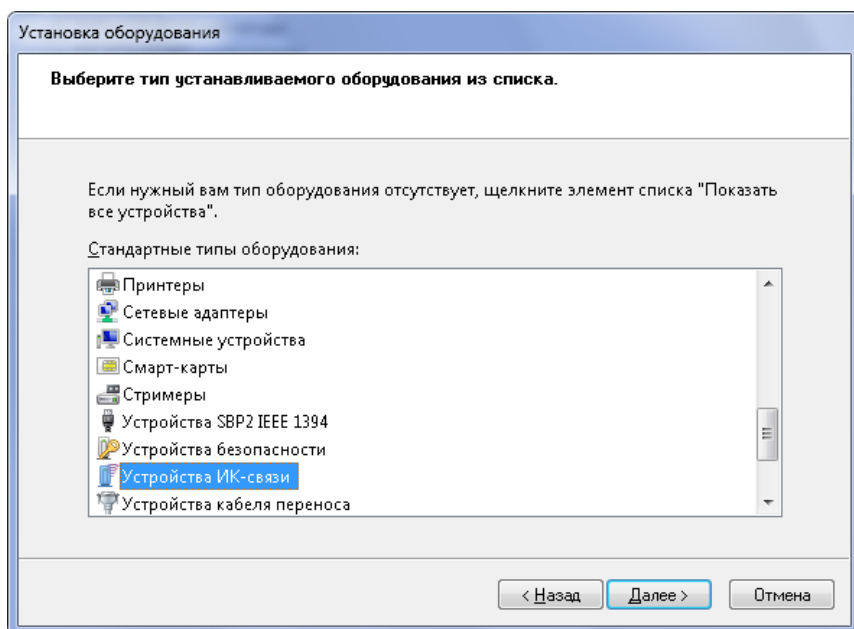


Рис. 5.5. Выбор типа устройства

5. Работа с этим мастером выполняется точно так же, как это делалось в Windows XP, поэтому нет смысла останавливаться на ней слишком подробно. Мастер выводит серию окон с набором подходящих для каждого шага опций и содержит пошаговые инструкции по дальнейшим действиям. На одном из этапов вам будет предложено выбрать тип устройства (рис. 5.5). Тип устройства вы наверняка знаете, поэтому вряд ли затруднитесь сделать этот выбор.
6. Далее вам будет предложено выполнить поиск драйвера на сайте Windows Update или если у вас имеется диск, то нажать кнопку **Установить с диска** (Have disk) и указать путь к установочным файлам (рис. 5.6).

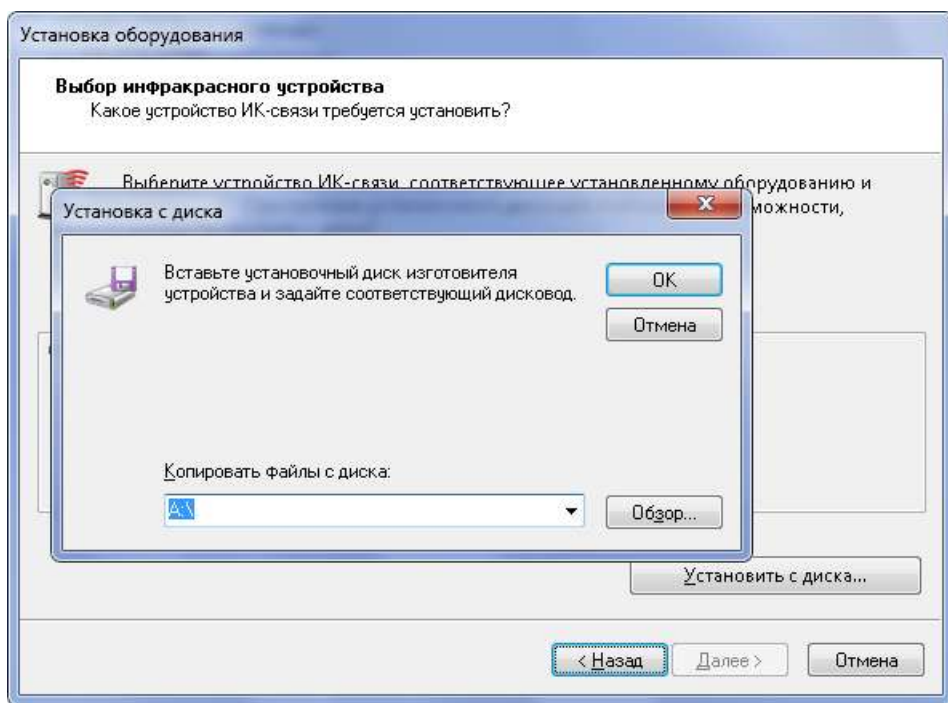


Рис. 5.6. Установка драйвера устройства с указанием пути к файлам драйвера

7. Как показала практика, вставлять диск, поставляемый в комплекте с устройством, следует только в том случае, если он действительно содержит драйверы, совместимые с Windows 7 (или Vista). Внимательно просмотрите сопроводительную документацию, поставляемую в комплекте с устройством, — там должно содержаться упоминание о том, что устройство действительно может работать в среде Windows 7 или что прилагаемые

к нему драйверы совместимы с этой операционной системой. Если диска у вас нет или он заведомо не содержит совместимых драйверов, следует действовать, полностью контролируя процесс установки драйвера, а именно:

- если вы еще не посетили сайт производителя соответствующего оборудования, сделайте это сейчас. Если на сайте производителя имеется обновленный драйвер для вашего устройства, скачайте его. Как правило, драйверы выкладываются в виде упакованных файлов (*.zip, *.rar). Перед тем как переходить к следующему шагу, распакуйте архив. Если обновленного драйвера на сайте производителя нет, попробуйте поискать его в Интернете или задайте соответствующий вопрос на форумах. Вполне возможно, что вам повезет, и кто-то до вас уже решил эту проблему;
- выберите опцию поиска драйвера на своем компьютере и укажите путь к каталогу с распакованными файлами. Если все сделано правильно, и вы действительно скачали совместимый драйвер, то Windows 7 автоматически установит и сконфигурирует устройство.

Метод установки и конфигурирования аппаратных устройств при помощи мастера установки нового оборудования (Add Hardware Wizard) гораздо безопаснее непосредственного редактирования реестра, поскольку исключает риск утраты совместимости или возникновения других проблем. Но время от времени при добавлении новых устройств или изменении параметров, уже установленных, может возникнуть необходимость в непосредственном редактировании реестра. Так, для многих пользователей представляет значительный интерес изменение настройки выделяемых устройству ресурсов. Вы уже знаете, что Диспетчер конфигурации при установке нового устройства и загрузке Windows управляет этими параметрами автоматически. Однако иногда может возникнуть необходимость в ручной настройке указанных параметров. Такая ситуация возможна, например, в случае аппаратного конфликта, который не может быть разрешен Диспетчером конфигурации и реестром. Предположим, к примеру, что конфликтуют настройки IRQ и DMA для двух устройств. В этом случае для редактирования параметров реестра вы также можете использовать Диспетчер устройств (Device Manager).

Теперь мы перейдем к рассмотрению более сложных вопросов и выясним, что же происходит на уровне системы, когда пользователь устанавливает новое устройство. Какие компоненты системы принимают в этом участие, какие процессы происходят?

Подсистема Plug and Play и реестр

Концепция Plug and Play (PnP), призванная упростить установку устройств и управление ими, была впервые введена с появлением Windows 95. Что же представляет собой Plug and Play — стандарт, спецификацию или концепцию? Фактически Plug and Play — это сочетание общей философии разработки и набора спецификаций, описывающих архитектуру аппаратных средств. Строго говоря, поддержка PnP подразумевает комбинацию взаимодействующих между собой системы BIOS, аппаратных устройств, системных ресурсов, драйверов устройств и самой операционной системы.

ПРИМЕЧАНИЕ

В 64-разрядных компьютерах система BIOS известна как Extensible Firmware Interface (EFI).

Все компоненты Plug and Play предназначены для достижения единой цели — обеспечить совместную автоматическую работу компьютера, периферийных устройств и их драйверов, а также операционной системы при минимальном вмешательстве со стороны пользователя. Работая с системой, полностью соответствующей требованиям Plug and Play, пользователи могут не беспокоиться о том, что при установке нового устройства возникнет аппаратный конфликт с другим устройством. Основой, на которой строится такая система конфигурирования, и является реестр Windows.

Ключ реестра `HKEY_LOCAL_MACHINE\HARDWARE` содержит описание аппаратных средств системы и всех соответствий между аппаратными устройствами и их драйверами. Следует сразу же отметить, что этот ключ является *непостоянным* (volatile), и хранящаяся в его составе информация воссоздается при каждом запуске Windows. Ядро операционной системы при запуске³ сохраняет эту информацию в составе ключа `HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION`. По мере запуска драйверов устройств они информируют о себе систему с тем, чтобы она могла ассоциировать устройства с соответствующими им драйверами. Windows помещает эту информацию в состав ключа `HKEY_LOCAL_MACHINE\HARDWARE\DEVICESMAP`. Наконец, информация о ресурсах, необходимых для работы устройств (адреса портов, диапазоны DMA, номера прерываний), сохраняется в составе ключа `HKEY_LOCAL_MACHINE\HARDWARE\RESOURCEMAP`.

Краткая история Plug and Play

Plug and Play представляет собой технологию, которая поддерживает автоматическое конфигурирование ПК и всех установленных на нем устройств.

³ Процесс запуска операционной системы Windows 7 будет подробно рассмотрен в главе 7.

Целью ее разработки являлось обеспечение для пользователя возможности подключить новое устройство (например, звуковой адаптер или факс-модем) и сразу же начать работу без необходимости вручную конфигурировать это устройство. Реализация технологии Plug and Play осуществляется на уровне аппаратных средств, операционной системы, драйверов устройств и BIOS.

Спецификация Plug and Play представляет собой результат работы промышленного комитета, состоящего из фирм-поставщиков, производящих как аппаратные средства, так и программное обеспечение. Комитет был образован в марте 1993 года, и изначально в его состав входили представители фирм Microsoft, Intel и Compaq. К концу 1995 года на рынке аппаратных средств появились сотни устройств, удовлетворяющих этому стандарту и производимых самыми различными фирмами.

Первой операционной системой, обеспечивавшей поддержку Plug and Play, стала Microsoft Windows 95. Однако с момента появления Windows 95 стандарты PnP претерпели существенную эволюцию, которая в основном является результатом инициативы комитета разработчиков OnNow⁴. Промышленная инициатива OnNow пытается определить универсальный подход к управлению операционной системой и конфигурацией устройств. Основным результатом ее деятельности явилась спецификация Advanced Configuration and Power Interface (ACPI) Version 1.0, определившая новый интерфейс системной платы и BIOS. Этот интерфейс расширяет возможности Plug and Play, позволяя операционной системе обеспечить управление питанием, а также открывает другие новые конфигурационные возможности. ACPI представляет собой открытый промышленный стандарт, и в настоящий момент для свободного скачивания доступна новая версия — ACPI 4.0 (<http://www.acpi.info/spec40.htm>).

Технологии Plug and Play определены для устройств IEEE 1394, PCI, PC Card/CardBus, USB, SCSI, ATA, ISA, LPT и COM. Каждое устройство Plug and Play должно обладать следующими возможностями:

- ☐ уникальным образом идентифицироваться;
- ☐ предоставлять список предлагаемых сервисов и необходимых ресурсов;
- ☐ идентифицировать поддерживающий это устройство драйвер;
- ☐ предоставлять программному обеспечению возможности по конфигурированию этого устройства.

Первой операционной системой из семейства Windows NT стала Windows NT 4.0, но поддержка Plug and Play в ней была крайне ограниченной, а ее уровень

⁴ В состав комитета разработчиков OnNow входят следующие компании: Hewlett-Packard, Intel, Microsoft, Phoenix и Toshiba.

был существенно ниже, чем обеспечивавшийся в Windows 9x. За исключением устройств PCI, все параметры настройки аппаратных средств должны были совпадать с установленными в реестре. Если это условие не соблюдалось, то драйвер устройства не загружался и, соответственно, устройство не работало. Все устройства PCI конфигурировались автоматически на этапе запуска системы и после этого, как правило, не менялись (за исключением тех случаев, когда эти параметры не соответствовали количеству или типу устройств на шине PCI). Windows NT 4.0 читала данные BIOS и информацию, полученную от устройств, только один раз — на этапе распознавания аппаратных средств при запуске системы. После запуска все управление устройствами осуществлялось только при помощи драйверов этих устройств и реестра, и обращений к BIOS никогда не происходило. Таким образом, Windows NT 4.0 поддерживала только статические, но не динамические изменения конфигурации и требовала частых перезагрузок.

Начиная с Windows 2000, в составе ОС появились две новые подсистемы модуля Executive — это Диспетчер Plug and Play (Plug and Play Manager) и Диспетчер управления электропитанием (Power Manager). Диспетчер Plug and Play интегрирован с Диспетчером ввода/вывода (I/O Manager) и не принимает участия в инициализации, но инициализация драйверов происходит таким образом, что некоторые устройства распознаются драйверами Plug and Play. В следующей системе из данного семейства, Windows XP, поддержка Plug and Play была дополнительно усилена, усовершенствована и оптимизирована. Общая идея этого проекта заключалась в том, чтобы объединить преимущества двух ветвей семейства Windows: Windows NT/2000 и Windows Millennium Edition (Windows ME). Одним из наиболее значимых преимуществ этих усовершенствований явились повышенная надежность, снижение возможного времени простоя и снижение частоты необходимых перезагрузок. Фактическая поддержка Plug and Play и управления электропитанием во всех версиях Windows, начиная с Windows 2000, обеспечивается интерфейсом ACPI. Чтобы в полном объеме гарантировать функциональные возможности Plug and Play и управления электропитанием, необходимо иметь BIOS, обеспечивающую полную поддержку ACPI (ACPI-совместимую BIOS).

Начиная с Windows Vista, установка и настройка аппаратных устройств и управление их драйверами были существенно изменены, и понимание этих изменений крайне важно для администраторов. В частности, особо пристального внимания заслуживают следующие понятия:

- ❑ новое хранилище драйверов и упаковка драйверов, обеспечивающие их централизованное хранение;
- ❑ процесс промежуточного размещения драйверов (Driver Staging);
- ❑ классификация драйверов.

В последующих разделах данной главы эти концепции будут рассмотрены более подробно.

Поддержка Plug and Play в Windows 7

Основной целью реализации Plug and Play в Windows Vista и Windows 7 является дальнейшее развитие промышленной инициативы, направленной на упрощение работы с персональными компьютерами для конечных пользователей. Кроме того, Plug and Play решает следующие задачи:

- ❑ расширение существующей инфраструктуры ввода/вывода таким образом, чтобы она поддерживала Plug and Play и управление электропитанием при одновременной поддержке промышленных стандартов на аппаратные средства Plug and Play;
- ❑ в новейших версиях Windows — Vista и 7 — реализация Plug and Play направлена на обеспечение поддержки аппаратных средств нового поколения, включая PCI и PCI Express. В отличие от Windows 2000/XP, в Windows Vista/7 поддержка ACPI является обязательной, и Windows Vista/7 обеспечивают полную поддержку ACPI 2.0 и избранные возможности ACPI 3.0;
- ❑ разработка общих интерфейсов драйверов, которые поддерживают Plug and Play и управление питанием для множества классов устройств, и оптимизация поддержки Plug and Play для самых разнотипных компьютеров — портативных, настольных рабочих станций и серверов, имеющих системные платы ACPI.

В дополнение к сказанному, поддержка драйверов устройств Plug and Play для различных классов устройств обеспечивается моделью драйвера Microsoft Win32 (Microsoft Win32 Driver Foundation, WDF⁵), которая, как и более ранние модели, поддерживает управление подачей электропитания и другие новые возможности, которые могут конфигурироваться и управляться операционной системой. Однако, по сравнению с моделью Microsoft Win32 Driver Model (WDM), также поддерживаемой в Windows Vista/7, модель WDF предоставляет ряд преимуществ, а именно:

1. Гибкость и простоту, что позволяет быстро разрабатывать надежные драйверы, поддерживающие Plug and Play, управление электропитанием, синхронизацию, Windows Management Instrumentation (WMI), мно-

⁵ Модель драйвера WDF — это новая модель драйвера, призванная ликвидировать ограничения, присущие более ранним моделям драйверов, например, Windows Driver Model (WDM), и моделям драйверов классов устройств (в том числе драйверов накопителей, сетевых устройств и аудио).

гоуровневые драйверы и асинхронный ввод/вывод. Гибкость новой модели позволяет с легкостью приспосабливаться к будущим инновационным возможностям системы;

2. Новую модель драйверов, изолирующую драйвер от основных компонентов операционной системы, что позволяет разработчикам Microsoft вносить изменения в операционную систему, избегая проблем с несовместимостью драйверов;
 3. Совместимость на уровне двоичного кода в различных версиях операционной системы, что упрощает тестирование и снижает требования к установке;
 4. Расширяемость, позволяющую реализовать функции, необходимые одному или нескольким, но не всем классам устройств. За счет стандартизации функциональных возможностей, общих для каждого класса, разработчики могут сконцентрироваться на реализации уникальных возможностей конкретного устройства;
 5. Возможность написания драйверов режима пользователя. В настоящий момент многие устройства (например, USB) требуют реализации закрытых (proprietary) протоколов и поддержки сторонних разработчиков;
 6. Возможность написания драйверов на языках высокого уровня с поддержкой объектно-ориентированного программирования (ООП);
 7. Изоляцию драйверов, что позволит запускать их в защищенной среде и обеспечит восстановление системы после сбоя в работе драйверов;
- автоматическое и динамическое распознавание установленных аппаратных средств — в число обеспечиваемых функций входят начальная установка системы, распознавание аппаратных изменений Plug and Play между перезагрузками системы и реакция на аппаратные события времени исполнения, в том числе установку и удаление устройств, а также отключение/подключение док-станций.

Например, часто устройства Plug and Play могут быть установлены или отключены во время работы Windows и система распознает и корректно обрабатывает эту ситуацию. К таким устройствам можно отнести, например, все USB-устройства, некоторые устройства IEEE 1394 и т. п. Снижение частоты необходимых перезагрузок является одним из наиболее значимых преимуществ, поскольку упрощает как установку операционной системы, так и процедуры установки нового оборудования.

Удаление устройства из компьютера без предварительного уведомления об этом операционной системы называют *внезапным удалением* (surprise

removal). Как правило, Windows корректно справляется с этой ситуацией, поскольку драйверы устройств, разработанные в соответствии со спецификацией Windows Logo Requirements, должны уведомлять операционную систему об удалении устройства. Тем не менее, для ряда устройств — таких как некоторые запоминающие устройства, модемы и сетевые адаптеры — производить внезапное удаление не рекомендуется. При внезапном удалении таких устройств операционная система отображает экран с сообщением о некорректном отключении устройства (Unsafe Removal of Device) и рекомендует пользователю в следующий раз при отключении устройства использовать безопасное отключение (Safe Removal). Пользователь может блокировать генерацию этого сообщения для тех устройств, для которых внезапное отключение неприемлемо. Безопасное отключение (Safe Removal) предназначено для уведомления операционной системы о том, что устройство будет отключено, и его можно найти в зоне уведомления, если такое устройство установлено в системе.

Однако некоторые устройства необходимо устанавливать или удалять лишь при выключенной системе. Это относится к тем устройствам, для установки которых требуется вскрывать системный блок. К тому же, если при удалении устройства выполняется передача данных, или же операционная система пытается обратиться к некоторым типам устройств, которые отсоединены, то может произойти потеря данных, их разрушение или даже сбой системы. Например, внезапное отсоединение устройств PC Card, CardBus, устройств параллельного или COM-порта в то время когда драйвер устройства выполняет попытки записи по соответствующим портам, может привести к зависанию системы или к ошибке типа **STOP**, что потребует произвести перезагрузку системы.

С учетом сказанного, в Windows Vista и Windows 7 были внесены следующие усовершенствования:

1. Возможность выполнения запуска устройств и выполнения других операций PnP в асинхронном режиме, что позволяет ускорить запуск операционной системы. В более ранних версиях Windows все эти операции выполнялись последовательно;
2. Улучшенные возможности по управлению динамическим отключением и подключением устройств, включая добавление памяти без перезапуска компьютера;
3. Улучшенная управляемость и диагностические возможности. Например, Windows Vista/7 регистрируют в системном журнале такие события, как неудачные попытки запуска устройств (Code 10 — Device failed to start) и неудачные попытки динамического отключения устройств,

ошибки, связанные с работой жесткого диска (рис. 5.7). Собранные в журнале данные могут использоваться для идентификации проблемных устройств и выявление тенденций, ведущих к сбоям;

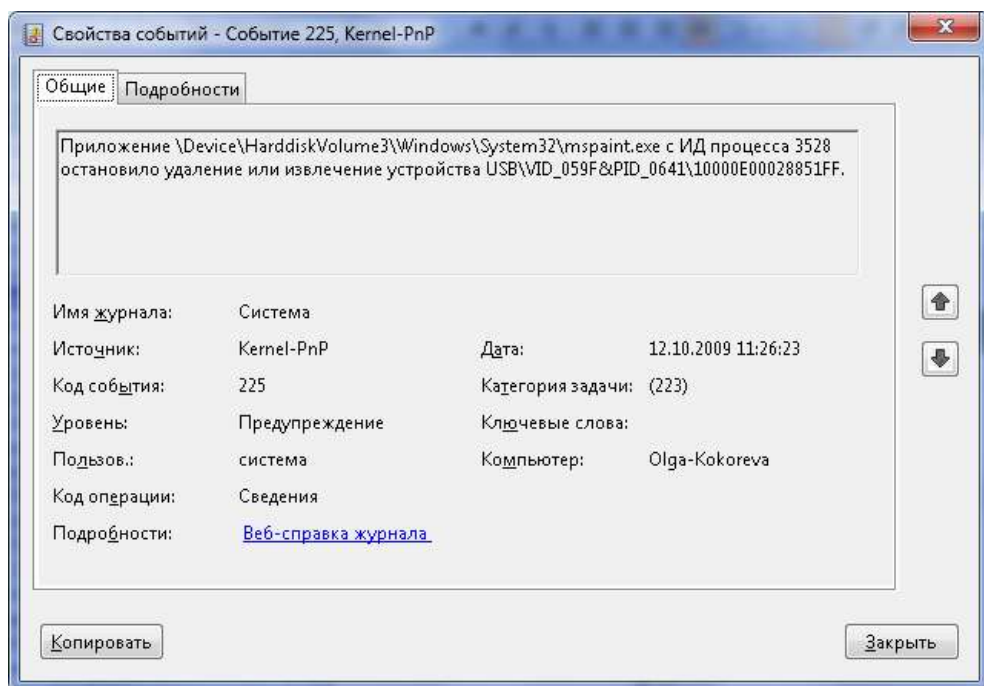


Рис. 5.7. Неудачные попытки динамического отключения устройств отражаются в системном журнале

- назначение и переназначение аппаратных ресурсов — драйверы устройств Plug and Play не назначают собственных ресурсов. Вместо этого необходимые для устройства ресурсы идентифицируются операционной системой при эnumерации устройства. Диспетчер Plug and Play (Plug and Play Manager) запрашивает эти требования при выделении ресурсов каждому устройству. На основании запросов диспетчер Plug and Play назначает устройствам соответствующие ресурсы, включая порты ввода/вывода, прерывания (IRQ), каналы DMA и адреса памяти. При необходимости Диспетчер Plug and Play переконфигурирует назначение ресурсов. Такая необходимость возникает, например, при добавлении в систему нового устройства, которое запрашивает ресурсы, уже назначенные другому устройству;

- ❑ загрузка соответствующих драйверов — Диспетчер Plug and Play определяет, какие драйверы необходимы для поддержки конкретного устройства, и выполняет загрузку этих драйверов;
- ❑ интерфейс для взаимодействия драйверов с системой Plug and Play — состоит в основном из процедур ввода/вывода, пакетов запроса ввода/вывода для системы Plug and Play (I/O Request Packets, IRP), а также содержит необходимые точки входа драйверов и информацию реестра;
- ❑ взаимодействие с системой управления электропитанием — ключевой особенностью системы Plug and Play является динамическая обработка событий. Добавление или удаление устройства служит примером такого динамического события. Еще один пример — это способность динамического перевода устройства в режим энергосбережения и обратно. Plug and Play и система управления электропитанием используют функции WDM и применяют схожие методы реагирования на динамические события. Начиная с Windows Vista, обеспечивается улучшенная поддержка режимов сна (sleep) и гибернации (hibernation). За счет этого ликвидированы ошибки в управлении электропитанием в драйверах и приложениях, присущие предшествующим версиям Windows. В частности, эти ошибки создавали серьезные проблемы мобильным пользователям, которые часто ожидали, что при закрытии крышки ноутбука система перейдет в ждущий режим или в режим гибернации, хотя в действительности этого не происходило. В результате пользователи теряли данные. Ситуация эта возникала потому, что Windows 2000/XP запрашивает согласия приложений и драйверов устройств на переход в другой режим энергопотребления. Если хотя бы один драйвер не отвечал на эти запросы, то смены режима не происходило. В Windows Vista и Windows 7 Диспетчер управления электропитанием уведомляет драйверы и приложения о смене режима энергопотребления, чтобы они могли подготовиться к переходу в другой режим, но не спрашивает у них разрешения. Сокращено и время ожидания ответа, в результате чего пользователи действительно могут быть уверены в том, что система перейдет в нужный режим;
- ❑ регистрация событий уведомления устройств — Plug and Play предоставляет возможность коду режима пользователя регистрировать и получать уведомления об определенных событиях Plug and Play. Процедура `RegisterDeviceNotification` позволяет осуществляющему вызов коду фильтровать класс или устройство, от которого требуется получать уведомления. Фильтр может быть специфическим, например, как дескриптор файловой системы, или общим, например, как класс устройств. Методы уведомлений, наследуемые от предыдущих версий Windows, также продолжают поддерживаться и работают, как прежде.

Уровни поддержки устройств и драйверов

Уровень поддержки Plug and Play, обеспечиваемый устройством, зависит как от аппаратной поддержки Plug and Play, так и от поддержки, обеспечиваемой драйвером этого устройства. На схематическом уровне эта концепция иллюстрируется табл. 5.1.

Таблица 5.1. Уровни поддержки Plug and Play для устройств и драйверов

Тип устройства	Драйвер Plug and Play	Драйвер без поддержки Plug and Play
Устройство Plug and Play	Полная поддержка Plug and Play	Поддержка Plug and Play отсутствует
Устройство без поддержки Plug and Play	Возможна частичная поддержка Plug and Play	Поддержка Plug and Play отсутствует

Как показывают данные таблицы, для обеспечения полной поддержки устройством технологии PnP необходим соответствующий драйвер. Рассмотрим все возможные конфигурации и дадим их краткое описание:

- ❑ *полная поддержка* — и устройство, и драйвер поддерживают Plug and Play. Чтобы обеспечить оптимальную поддержку Plug and Play, аппаратная реализация должна соответствовать спецификации ACPI;
- ❑ *устройство Plug and Play, драйвер без поддержки Plug and Play* — поддержка Plug and Play отсутствует. Если драйвер не поддерживает Plug and Play, то устройство, аппаратно поддерживающее спецификацию PnP, будет вести себя как обычное устройство. Обратите особое внимание, что это может ограничить функциональные возможности Plug and Play для всей системы;
- ❑ *устройство без поддержки Plug and Play, драйвер Plug and Play* — эта комбинация может обеспечить частичную поддержку Plug and Play. Устройство, не поддерживающее Plug and Play на аппаратном уровне, может обеспечивать ее частичную поддержку при условии загрузки соответствующего драйвера Plug and Play. Хотя такая система не сможет автоматически и динамически распознавать аппаратные средства и загружать соответствующие драйверы, она обеспечит возможность управления выделением ресурсов Plug and Play, а также предоставит интерфейс для взаимодействия драйвера с системой Plug and Play и позволит взаимодействовать с системой управления электропитанием и регистрировать события, связанные с уведомлением устройств. Если такое устройство имеет драйвер

Plug and Play, то оно будет отображаться Диспетчером устройств (Device Manager), и для него будут доступны страницы конфигурирования свойств;

- *ни устройство, ни драйвер не поддерживают Plug and Play* — в этом случае поддержка Plug and Play отсутствует. Драйверы, разработанные до включения поддержки Plug and Play в операционную систему, будут функционировать точно так же, как раньше (без функций Plug and Play). Все новые драйверы должны поддерживать PnP.

Как видите, поддержка Plug and Play зависит как от устройства, так и от его драйвера. Например, если вы вручную установили устройство, которое не поддерживает Plug and Play, то, тем не менее, можно расширить его функциональные возможности и обеспечить частичную поддержку Plug and Play, установив соответствующий драйвер Plug and Play.

Архитектура Plug and Play

Ядро Windows 7 обеспечивает поддержку Plug and Play в процессе загрузки и предоставляет интерфейсы для взаимодействия с такими компонентами операционной системы, как уровень аппаратных абстракций (HAL)⁶, исполняющая подсистема (модуль Executive) и драйверы устройств.

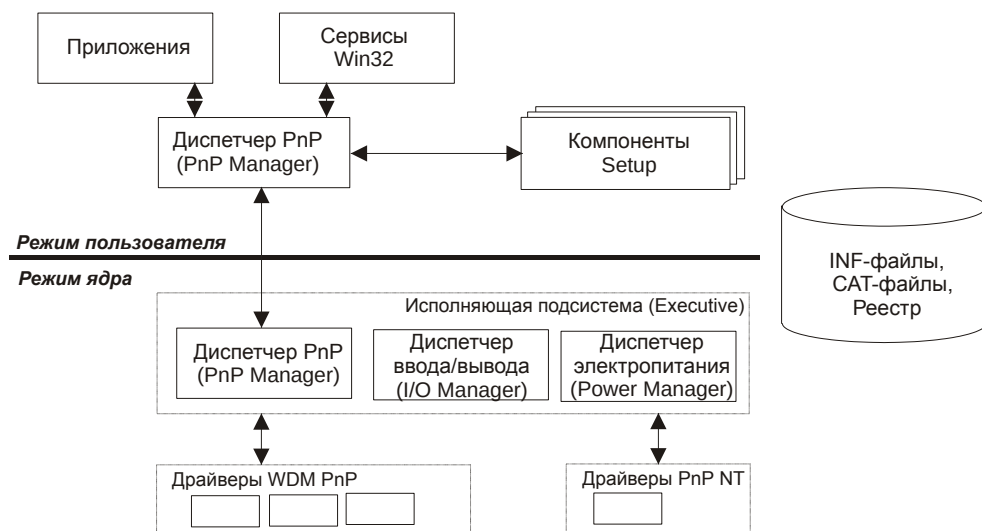


Рис. 5.8. Архитектура Plug and Play

⁶ В отличие от предшествующих версий, Windows Vista и Windows 7 больше не поддерживают стандартные (не ACPI) уровни HAL. На практике это означает, что все системное программное обеспечение должно быть совместимо с ACPI.

Функции режима пользователя взаимодействуют с функциями режима ядра, обеспечивая возможности динамической конфигурации и интерфейса с остальными компонентами, которые должны поддерживать Plug and Play, например, с программой Setup и приложениями Панели управления (Control Panel). На рис. 5.8 представлена схема архитектуры PnP. Следующие разделы содержат подробное описание модулей Plug and Play.

Диспетчер Plug and Play в режиме ядра

Диспетчер Plug and Play (Plug and Play Manager), работающий в режиме ядра, поддерживает функции центрального управления, управляет шинными драйверами при выполнении эnumерации и драйверами устройств при добавлении устройства, его запуске и т. д.

Так, Диспетчер Plug and Play направляет запросы, чтобы определить, может ли устройство быть удалено, и дать драйверу устройства возможность синхронизировать незавершенные запросы ввода/вывода с поступающим запросом. Диспетчер Plug and Play режима ядра взаимодействует с диспетчером Plug and Play режима пользователя при определении устройств, доступных для выполнения таких операций.

Диспетчер электропитания и Диспетчер политики

Диспетчер электропитания (Power Manager) — это компонент режима ядра, который работает совместно с Диспетчером политики (Policy Manager) и обрабатывает вызовы интерфейса прикладного программирования (API) управления электропитанием, координирует события и генерирует запросы на прерывания, связанные с управлением электропитанием (IRP). Например, если различные устройства отправляют запросы на отключение, Диспетчер электропитания собирает эти запросы, определяет, какие запросы должны быть сериализованы, и генерирует соответствующие IRP.

Диспетчер политики (Policy Manager) наблюдает за активностью системы и собирает интегрированную информацию о статусе пользователей, приложений и драйверов устройств. При определенных обстоятельствах или по запросу Диспетчер политики генерирует IRP для изменения статуса драйверов устройств.

Диспетчер ввода/вывода

Диспетчер ввода/вывода (I/O Manager) представляет собой компонент режима ядра, который выполняет трансляцию команд чтения и записи режима пользователя в соответствующие IRP. Таким образом он обеспечивает базовые сервисы для драйверов устройств. Помимо этого, Диспетчер ввода/вывода управляет всеми остальными основными IRP операционной системы.

В Windows Vista и Windows 7 Диспетчер ввода/вывода поддерживает асинхронный ввод/вывод. В дополнение к этому, модель ввода/вывода обладает следующими отличительными чертами:

- ❑ Диспетчер ввода/вывода предоставляет последовательный и непротиворечивый интерфейс для всех драйверов уровня ядра (в том числе для самых низкоуровневых, промежуточных) и драйверов файловой системы. Все запросы к драйверам на ввод и вывод отправляются в виде пакетов запроса на ввод/вывод (I/O request packets, IRPs);
- ❑ операции ввода/вывода являются многоуровневыми — Диспетчер ввода/вывода экспортирует системные сервисы, которые защищенные подсистемы режима пользователя вызывают от имени приложений или пользователей. Диспетчер ввода/вывода перехватывает эти вызовы, устанавливает один или несколько пакетов IRP и перенаправляет их физическим устройствам через многоуровневые драйверы;
- ❑ Диспетчер ввода/вывода определяет набор стандартных процедур, часть которых является обязательной, а часть — опционной;
- ❑ как и сама операционная система, драйверы базируются на объектах. Драйверы, соответствующие им устройства, а также все аппаратные устройства, представлены в виде объектов. Диспетчер ввода/вывода и другие системные компоненты экспортируют процедуры, которые драйверы могут использовать для манипулирования соответствующими объектами.

В дополнение к IRP, Диспетчер ввода/вывода работает с Диспетчером PnP и Диспетчером электропитания, отправляя пакеты IRP, содержащие запросы к подсистемам PnP и управления электропитанием. Наконец, Диспетчер ввода/вывода предоставляет уровневую структуру драйверов, а также интерфейсы для драйверов WDM и WDF⁷.

Кроме того, в состав Windows Vista и Windows 7 входит компонент PnP-X — расширение PnP. Этот компонент интегрирует устройства, подключенные к сети, в состав подсистемы PnP Windows, что позволяет устройствам, подключенным к сети, выглядеть как устройства, подключенные к локальному компьютеру, и предоставляет интерфейс, аналогичный интерфейсу, используемому для конфигурирования устройств, физически подключенных к компьютеру.

Дерево устройств Plug and Play

Диспетчер Plug and Play (Plug and Play Manager) поддерживает дерево устройств, которое может просматриваться из Диспетчера устройств (Device Manager) (рис. 5.9).

⁷ Более подробную информацию о WDF можно найти здесь:

<http://www.microsoft.com/whdc/driver/wdf/default.mspx>.

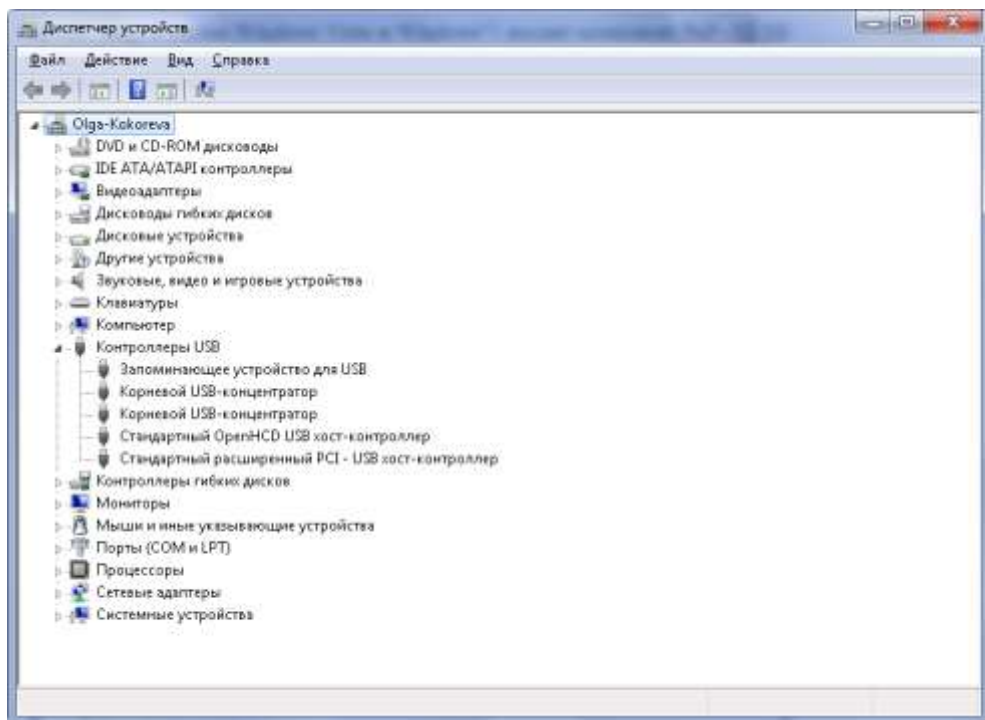


Рис. 5.9. Дерево устройств, отображаемых Диспетчером устройств

Диспетчер Plug and Play обновляет дерево устройств при добавлении или удалении устройств или по мере переназначения ресурсов. Дерево устройств является иерархическим, при этом каждое устройство на шине представляется как дочернее устройство шинного адаптера или контроллера. Вся статическая информация об аппаратных средствах хранится в реестре, а компоненты системы Plug and Play и драйверы осуществляют, поддерживают и получают доступ к новым и существующим поддеревьям реестра.

В процессе энумерации данные для каждого устройства сохраняются в реестре под ключом `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum`. Система Plug and Play принимает решения о том, какие драйверы устройств должны загружаться, на базе информации, полученной в результате процесса энумерации. Таким образом, между деревом Enum и списком сервисов, расположенным под ключом `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services`, существует исключительно важная связь.

Следует отметить, что Диспетчер устройств позволяет просматривать устройства как по типу, так и по подключению. Для просмотра устройств

по подключению необходимо в меню **Вид (View)** выбрать команду **Устройства по подключению (Devices by connection)**. Дерево устройств, в котором отображены устройства, сгруппированные по их подключению, представлено на рис. 5.10. В этом представлении Диспетчер устройств отображает ресурсы компьютера в соответствии с тем, как они подключены.

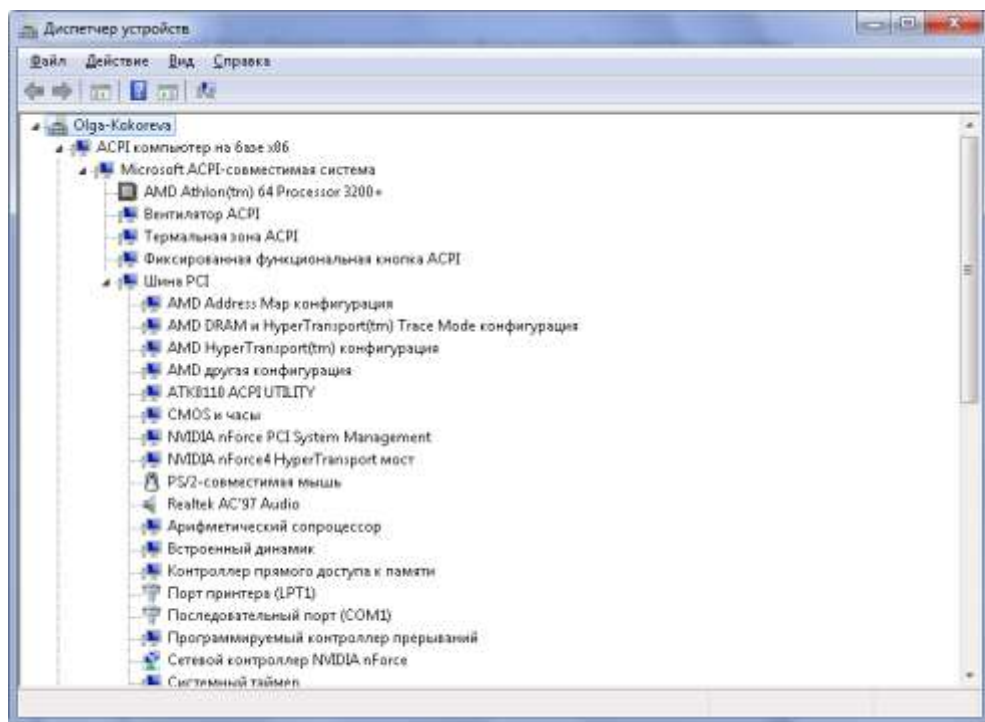


Рис. 5.10. Просмотр устройств, упорядоченных по подключению

Каждая ветвь в дереве определяет узел устройства со следующими требованиями для конфигурации системы:

- ☐ уникальный идентификатор устройства (Device ID, DID), обычно представляющий имя устройства;
- ☐ ресурсы, например IRQ и DMA, включая тип ресурса;
- ☐ выделенные (allocated) ресурсы;
- ☐ уточнение, является ли узел устройства шиной, если это применимо (каждое устройство шины имеет дополнительные узлы устройств, расположенные под ним в дереве).

Специальные значки служат для указания типа устройства, а также для обозначения возможных конфликтов. В случае наличия проблем также отображаются их кодовые номера и значки, инициирующие их решение.

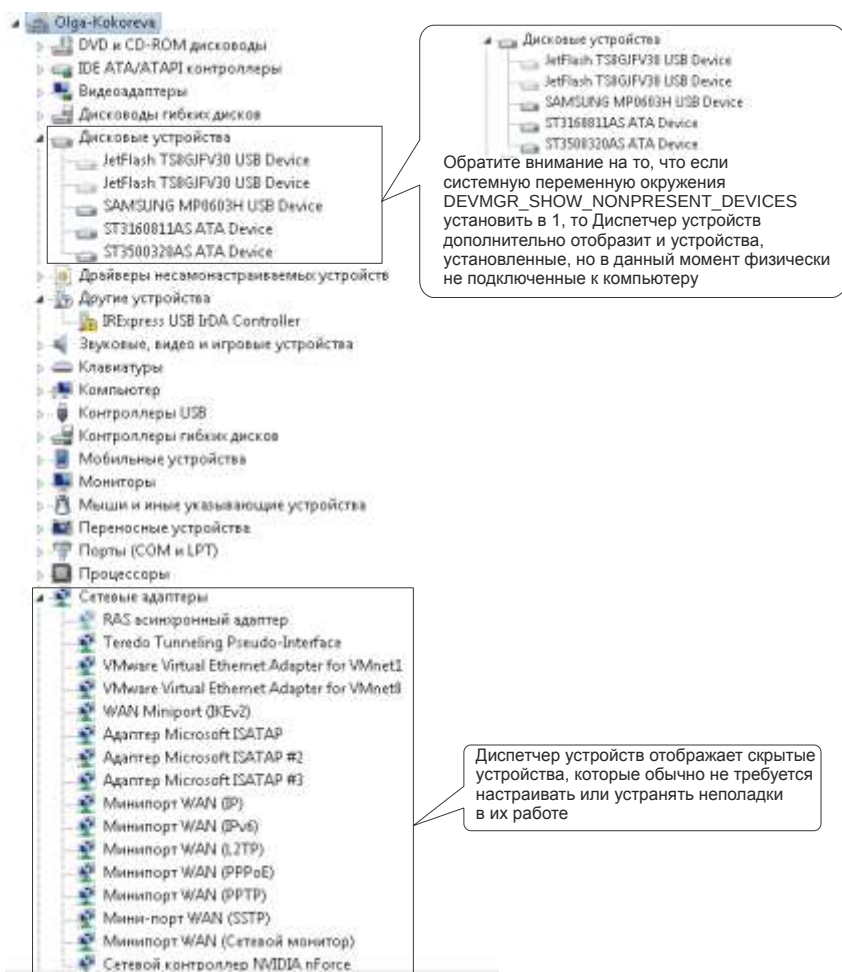


Рис. 5.11. Отображение скрытых устройств в режиме **Show hidden devices**

Диспетчер устройств по умолчанию показывает не все устройства. Некоторые устройства являются *скрытыми* (hidden devices). В частности, к ним относятся так называемые *унаследованные* устройства (legacy devices). Наследуемые устройства не поддерживают технологию Plug and Play, и обычно вам не приходится их настраивать или устранять неполадки в их работе.

Кроме того, при просмотре списка устройств по их подключению Диспетчер устройств в Windows Vista/7 может отображать и *отсутствующие* (nonpresent) устройства — те, которые были установлены в вашей системе, но в данный момент больше не подключены к компьютеру. Чтобы увидеть скрытые устройства (рис. 5.11), выберите в меню **Вид** (View) команду **Показать скрытые устройства** (Show hidden devices). Обратите внимание на то, что физически не подключенные устройства отображаются затененными (grayed).

ПРИМЕЧАНИЕ

Диспетчер устройств не всегда показывает список устройств, установленных, но в данный момент не подключенных к системе. Обратите внимание, что если вы просто выберете команду **Показать скрытые устройства** (Show hidden devices), то Диспетчер устройств отобразит только скрытые устройства, не нуждающиеся в конфигурировании. Чтобы отобразить установленные, но физически не присутствующие в системе устройства, необходимо создать переменную среды `DEVMGR_SHOW_NONPRESENT_DEVICES` и присвоить ей значение 1. Для этого запустите сеанс командной строки с административными правами и дайте следующую команду: `set devmgr_show_nonpresent_devices=1`, нажмите клавишу <Enter> и запустите Диспетчер устройств командой `devmgmt.msc`.

Можно также запустить утилиту Панели управления (Control Panel) **Система** (System), выбрать опцию **Свойства системы** (System Properties), перейти на вкладку **Дополнительно** (Advanced), а затем в диалоговом окне **Переменные среды** (Environment Variables) (рис. 5.12) создать системную переменную окружения `DEVMGR_SHOW_NONPRESENT_DEVICES` и присвоить ей значение 1.

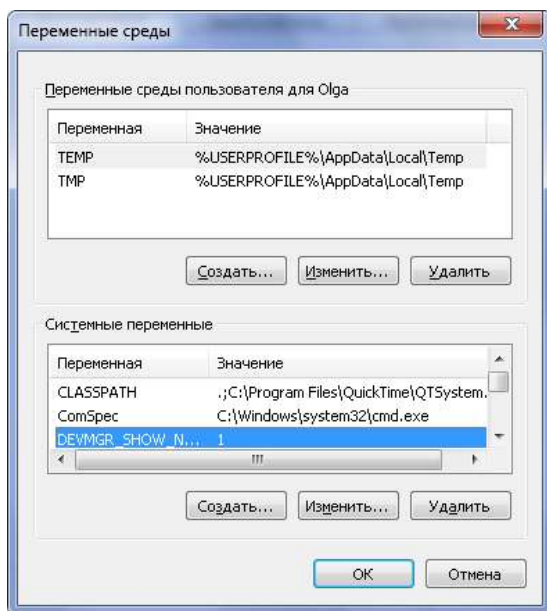


Рис. 5.12. Окно Переменные среды

Диспетчер устройств может использоваться для активизации и отключения устройств, устранения неполадок, обновления драйверов, выполнения *откатов драйвера* (driver rollback) и изменения ресурсов, назначенных устройствам. Для того чтобы проверить изменения в аппаратной конфигурации, обновить драйвер устройства, отключить или деинсталлировать устройство, выявить неполадки в нем или просмотреть его свойства, необходимо щелкнуть правой кнопкой мыши по соответствующему узлу устройства в дереве устройств, а затем выбрать нужную команду в контекстном меню.

Распознавание устройств Plug and Play

Реализация Plug and Play обеспечивает следующие преимущества:

- осуществляется распознавание и эnumерация (enumeration, "перечисление") устройств;
- распределяются ресурсы в ходе распознавания устройства;
- динамически загружаются, инициализируются и выгружаются драйверы;
- уведомляются другие драйверы и приложения о подключении нового устройства;
- осуществляется взаимодействие с системой управления питанием при подключении и отключении устройств;
- поддерживается широкий спектр типов устройств.

После того как Windows распознает устройство Plug and Play, его драйвер может быть динамически сконфигурирован и загружен. При этом от пользователя потребуется ввести минимум данных или же вовсе ничего не потребуется. Некоторые шины, например, PCI и USB, позволяют полностью использовать возможности Plug and Play и определяются автоматически. После распознавания устройства диспетчер Plug and Play и драйвер шины осуществляют эnumерацию устройства, загрузят необходимый драйвер (или несколько драйверов). При подключении нового устройства (о котором нет информации в реестре) Windows выполнит инсталляцию и запуск драйверов для данного устройства.

Как уже отмечалось, программа Setup проверяет конфигурацию аппаратных средств компьютера и записывает в реестр информацию об определенном устройстве. Программа Setup получает информацию о конфигурации устройств системы из соответствующих этим устройствам INF-файлов, а о тех устройствах, которые поддерживают Plug and Play, — непосредственно от самих устройств. В Windows Vista/7 синтаксис INF-файлов был изменен по сравнению с INF-файлами, применявшимися в Windows XP. Это было сделано с тем, чтобы обеспечить проверку совместимости с Windows Vista/7.

В системе PnP устройство переходит через различные состояния PnP: конфигурируется, запускается, возможно, останавливается для балансировки ресурса и может быть удалено. Переходы между различными состояниями PnP-устройства показаны на рис. 5.13.

Когда устанавливается новое устройство, Windows использует уникальный идентификатор устройства для поиска INF-файлов, соответствующих этому устройству. На основании полученной информации создается элемент для данного устройства в ветви `HKEY_LOCAL_MACHINE` реестра и копируются необходимые драйверы. Затем в соответствии с командами INF-файла создаются остальные ключи и параметры реестра, необходимые драйверу.

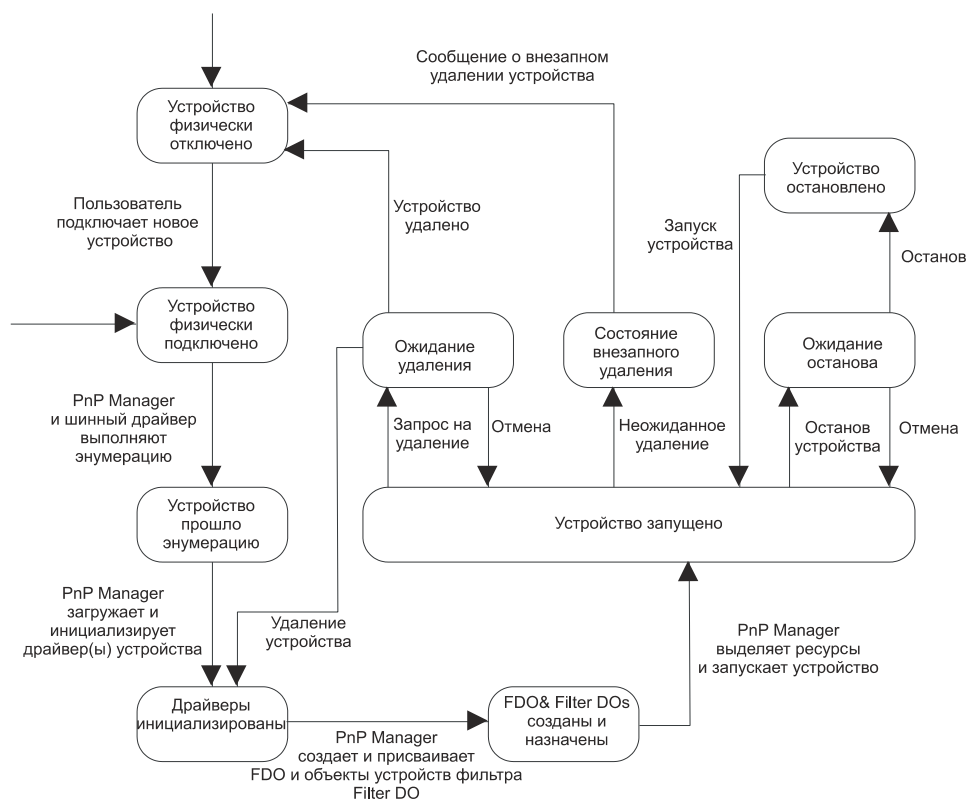


Рис. 5.13. Состояния устройства PnP

Отличия установки устройств в Windows Vista/7 от Windows XP

Начиная с Windows Vista в централизованное хранилище драйверов и архитектуру пакетов драйверов были внесены изменения. Так, в Windows XP для

2. Диспетчер Plug and Play (PnP Manager) и драйвер шины осуществляют эnumерацию. Сначала драйвер шины посредством самой шины принимает уведомление о новом устройстве, а затем уведомляет Диспетчер Plug and Play, работающий в режиме ядра, об изменении в аппаратной конфигурации (в нашем случае было добавлено новое устройство). Затем Диспетчер Plug and Play, работающий в режиме ядра, запрашивает у драйвера шины список устройств, физически к ней подключенных, и сравнивает новый список с предыдущей копией — так диспетчер Plug and Play определяет, какое устройство было добавлено, и запрашивает у драйвера шины информацию о новом устройстве (идентификатор устройства, идентификатор поставщика, идентификаторы совместимости и характеристики устройства).
3. Диспетчер Plug and Play, работающий в режиме ядра, уведомляет Диспетчер Plug and Play, работающий в режиме пользователя, о наличии устройства, которое необходимо установить.
4. PnP Manager, работающий в режиме пользователя, создает новый процесс с помощью утилиты rundll32.exe и запускает динамическую библиотеку нового устройства (New Device DLL, newdev.dll) для инсталляции устройства.
5. Динамическая библиотека нового устройства (New Device DLL) вызывает функции инсталляции устройства Setup API, а также функции Диспетчера конфигурации — PnP Configuration Manager (CfgMgr API) — для выполнения задач инсталляции. Одновременно динамически загружаемая библиотека нового устройства создает список драйверов, которые подходят для данного устройства, и при необходимости запускает мастер обнаружения новых устройств (Found New Device wizard). Выбор драйверов обсуждался ранее в этой главе.
6. В инсталляции устройства могут использоваться *инсталлятор класса* (class installer) и *дополнительные инсталляторы* (при необходимости).
7. Программа Setup передает управление *режиму ядра* (Kernel Mode) для загрузки драйверов и запуска устройства. Когда будет выбран наиболее подходящий драйвер для устройства, программа Setup копирует соответствующие файлы драйвера, регистрирует дополнительный инсталлятор, предназначенный исключительно для данного устройства, и т. д. Затем управление передается режиму ядра для загрузки драйверов и запускается устройство. Соответствующая функция Диспетчера конфигурации (CfgMgr) отправляет запрос Диспетчеру Plug and Play (PnP Manager), работающему в режиме ядра.
8. Диспетчер Plug and Play загружает соответствующий драйвер функции, а также необязательный драйвер фильтра для устройства.

9. Инсталляторы могут поддерживать страницы программы-мастера, служащие для установок устройства.

В Windows Vista и Windows 7 процесс установки новых устройств в целом протекает похожим образом, но с рядом различий, которые будут описаны в следующих нескольких подразделах.

Централизованное хранилище драйверов Windows Vista/7

В новейших версиях Windows драйверы хранятся централизованно. Хранилище файлов расположено в папке %SystemRoot%\System32\DriverStore. В этой папке содержится вложенная папка с именем FileRepository, и файлы драйверов хранятся в папках, вложенных в эту папку и названных по именам соответствующих драйверов. В составе каждой папки драйвера есть файлы собственно драйверов (SYS-файлы), файлы установки драйверов (INF-файлы), так называемые *прекомпилированные INF-файлы* (precompiled inf-files, PNF-файлы) и файл, содержащий манифест всех файлов в данном пакете драйвера (MAN-файл)⁸.

ПРИМЕЧАНИЕ

Прекомпилированные INF-файлы автоматически создаются Windows Vista/7 для каждого INF-файла в процессе установки драйвера с тем, чтобы обеспечить более быструю и эффективную обработку данных в процессе установки. PNF-файлы содержат информацию об оригинальном содержимом соответствующих INF-файлов, а также их имена и прочие атрибуты. Процедура установки использует PNF-файлы вместо исходных INF-файлов. Если PNF-файл отсутствует, то процедура установки автоматически создаст новый на основе имеющегося INF-файла. Для INF-файлов сторонних поставщиков в PNF-файлы включается информация об оригинальном местоположении исходного INF-файла. PNF-файлы используются Windows и некоторыми приложениями, и не должны открываться вручную.

Благодаря централизации хранения драйверов новейшие версии Windows получают следующие возможности:

- ❑ ускорение процесса установки драйвера и обеспечение более надежного отката драйверов. Для ускорения процесса установки используются индексные файлы, что позволяет быстро найти нужный драйвер устройства среди всех доступных (а их количество обычно исчисляется тысячами);
- ❑ защита драйверов с помощью механизма защиты ресурсов Windows (Windows Resource Protection, WRP), пришедшего на смену механизму защиты файлов (Windows File Protection, WFP) из предшествующих версий Windows.

⁸ Файлы манифестов (MAN-файлы) — это файлы формата XML, которые Windows Vista/7 использует для запуска приложений с повышенным уровнем привилегий в соответствии с UAC.

Промежуточное размещение драйверов (Driver Staging)

Процесс Driver Staging обеспечивает проверку драйверов, чтобы при установке некорректно написанного драйвера не происходило сбоев в процессе обнаружения устройств Plug and Play. Процесс Driver Staging является одним из принципиальных нововведений, впервые появившихся в Windows Vista и, безусловно, присутствующих в Windows 7. Суть его заключается в том, что в отличие от Windows XP, в новейших версиях Windows установка драйверов производится в два этапа:

1. Подсистема PnP осуществляет поиск драйвера и помещает его *в промежуточную область хранения* (Staging). Администратор может добавлять драйверы устройств в хранилище с тем, чтобы впоследствии, при подключении соответствующего устройства, установка драйвера произошла в автоматическом режиме. С целью уменьшения риска внесения в систему вредоносного ПО, обычным пользователям такой возможности не предоставляется, за исключением случаев, когда администратор явным образом предоставит им такое право. Драйверы могут добавляться в хранилище в автономном режиме (offline) путем добавления их к установочному образу Windows на этапе развертывания. Кроме того, драйверы могут помещаться в хранилище и в оперативном режиме, при работающей операционной системе. Перед тем как поместить драйвер в хранилище, Windows проверяет его целостность. При этом для того, чтобы драйвер мог быть помещен в хранилище, проверяется его соответствие следующим критериям:

- пакет драйвера должен содержать все файлы, необходимые для установки устройства (см. предыдущий раздел);
- устанавливаемый драйвер не должен присутствовать в списке драйверов, известных как проблемные драйверы⁹;
- все его компоненты, работающие в режиме ядра, могут быть установлены в неинтерактивном защищенном контексте **LocalSystem**.

2. На втором этапе производится установка драйвера из хранилища.

Установка драйвера устройства происходит следующим образом:

- Windows обнаруживает, что к компьютеру подключено новое устройство.
- Сервис Plug and Play запрашивает идентификатор обнаруженного устройства.

⁹ Подробнее об этом рассказано в статье "Improvements in Device Driver Management in Windows Vista" (http://download.microsoft.com/download/7/6/7/767548f8-d54b-4b87-963a-9506d993830f/Vista_Devices.doc).

- Windows проверяет три индексных файла в централизованном хранилище драйверов (Driver Store): `infpub.dat`, `infstore.dat` и `drvindex.dat`, расположенные в папке `%SystemRoot%\inf`. Это делается с тем, чтобы определить, доступен ли для устройства встроенный (inbox) драйвер или драйвер, временно помещенный в хранилище. В этом случае Windows может установить драйвер, не требуя от пользователя административных полномочий и в полностью автоматическом режиме. Иными словами, установку драйвера сможет произвести обычный пользователь, и произойдет это так, как в примере из главы 1 (см. рис. 5.6–5.8).
3. Если Windows не сможет обнаружить пакет драйвера в хранилище (Driver Store), то процесс установки пойдет так, как было описано в начале данной главы — Windows произведет рекурсивный поиск по всем областям, которые могут содержать драйверы. Если подходящий драйвер будет найден, то Windows запросит подтверждения наличия у пользователя прав на установку устройств и выполнит проверку цифровой подписи драйвера. Если пакет драйвера удовлетворяет всем предъявляемым требованиям, то он будет скопирован в хранилище (staged). Если драйвер не найден, то поиск подходящего драйвера будет выполнен в Windows Update. Если же подходящего драйвера не найдется и там, то пользователю потребуется или вставить диск, содержащий драйвер, или вручную указать путь к нужному каталогу, в который скопирован драйвер, скачанный из Интернета. Затем сервис Plug and Play обнаружит файлы драйвера, помещенные в хранилище, и разместит их в системных папках.
 4. После копирования драйверов сервис Plug and Play внесет необходимые изменения в реестр, чтобы операционная система могла использовать новый драйвер.
 5. Сервис Plug and Play запустит драйвер, после чего устройство будет готово к работе.

Схема ранжирования драйверов

Windows 2000/XP использовали схему ранжирования драйверов (driver ranking scheme) для того, чтобы определить, какой драйвер необходимо загрузить, если устройству соответствует множество драйверов. Драйверы ранжируются на основе сведений о том, снабжены ли они цифровой подписью (digital signature), и степени соответствия так называемому *аппаратному идентификатору устройства*. Если для какого-либо устройства имеется несколько драйверов, то для инсталляции будет выбран драйвер с наивысшим

рангом. Далее представлен список схем ранжирования Windows XP (от высшего к низшему рангу):

- ☐ драйвер с цифровой подписью, четыре части `HW ID` соответствуют драйверу;
- ☐ драйвер с цифровой подписью, две части `HW ID` соответствуют драйверу;
- ☐ драйвер без цифровой подписи, четыре части `HW ID` соответствуют драйверу;
- ☐ драйвер без цифровой подписи, две части `HW ID` соответствуют драйверу.

Когда вам необходимо установить новое устройство, следует сначала предоставить операционной системе автоматически распознать и сконфигурировать его. В зависимости от конкретного устройства, нужно сделать следующее:

- ☐ если устройство поддерживает Plug and Play, его следует просто подключить;
- ☐ перед установкой карт PCI и ISA, поддерживающих Plug and Play, сначала необходимо выключить компьютер. При перезагрузке Windows распознает установленное в компьютер устройство и автоматически запускает инсталляционную процедуру Plug and Play;
- ☐ если устройство не поддерживает Plug and Play, запустите программу установки оборудования (Add Hardware) и предоставьте распознавание устройства системе. Для этого потребуются права администратора.

Устройства будут установлены после того, как пользователь зарегистрируется на компьютере.

СОВЕТ

Для того чтобы использовать функциональные возможности технологии Plug and Play, выбирайте новые устройства, которые ее поддерживают, даже если на компьютере нет ACPI BIOS.

В отличие от Windows XP, Windows Vista и Windows 7 используют не четыре, а восемь уровней цифровой подписи. Перечислим эти схемы ранжирования (от высшего к низшему рангу):

- ☐ драйверы, снабженные цифровой подписью Microsoft и сертифицированные WHQL¹⁰;

¹⁰ WHQL (Windows Hardware Quality Labs) — подразделение Microsoft, выполняющее тестирование и сертификацию аппаратных устройств и драйверов сторонних производителей на соответствие требованиям совместимости с операционными системами Windows. Продукты, прошедшие сертификацию, снабжаются логотипом Windows, что свидетельствует о том, что они полностью соответствуют всем требованиям Microsoft и предназначены для работы с операционными системами Windows (в данном случае — Windows Vista/7).

- ☐ встроенные драйверы с цифровой подписью Microsoft (NT Build Lab);
- ☐ драйверы с цифровой подписью Microsoft и сертификацией WinSE;
- ☐ драйверы с цифровой подписью Authenticode (Enterprise CA);
- ☐ драйверы с цифровой подписью Authenticode (Class 3 CA);
- ☐ драйверы с цифровой подписью Authenticode (Macecert.exe);
- ☐ драйверы с цифровой подписью WHQL от Microsoft для низкоуровневой операционной системы;
- ☐ драйверы без цифровой подписи.

Откат драйвера

Это новое свойство, впервые представленное в Windows XP, обеспечивает усовершенствование, направленное на повышение надежности. Такие проблемы, как аппаратные конфликты, повторяющиеся ошибки **STOP** или же проявления нестабильности возникают после установки несовместимого драйвера. Очевидно, что в подобной ситуации крайне необходимо иметь возможность замены драйвера, вызывающего проблемы, без повторной установки операционной системы.

Комплекс опций отката драйвера (Driver Rollback) является ценным средством устранения неполадок, когда необходимо восстановить поврежденную систему, а также может использоваться при отладке бета-версий драйверов. Например, если после обновления версии драйвера ваша система выводит сообщение **STOP**, следует попытаться загрузить систему в безопасном режиме и заменить неподходящий драйвер.

Для использования отката драйвера выполните следующее:

1. В окне Панели управления (Control Panel) запустите утилиту **Система** (System) и пройдите по ссылке **Диспетчер устройств** (Device Manager).
2. Укажите правой кнопкой мыши устройство, обновленный драйвер которого вызвал проблему, и в контекстном меню выберите команду **Свойства** (Properties).
3. В открывшемся диалоговом окне перейдите на вкладку **Драйвер** (Driver) (рис. 5.15). Нажмите кнопку **Откатить** (Roll Back Driver).
4. Диспетчер устройств (Device Manager) предложит подтвердить откат драйвера. Нажмите кнопку **Да** (Yes). Если предыдущей версии драйвера нет, то программа отката Driver Rollback отобразит сообщение об ошибке и затем предложит воспользоваться другими средствами для устранения неполадки.

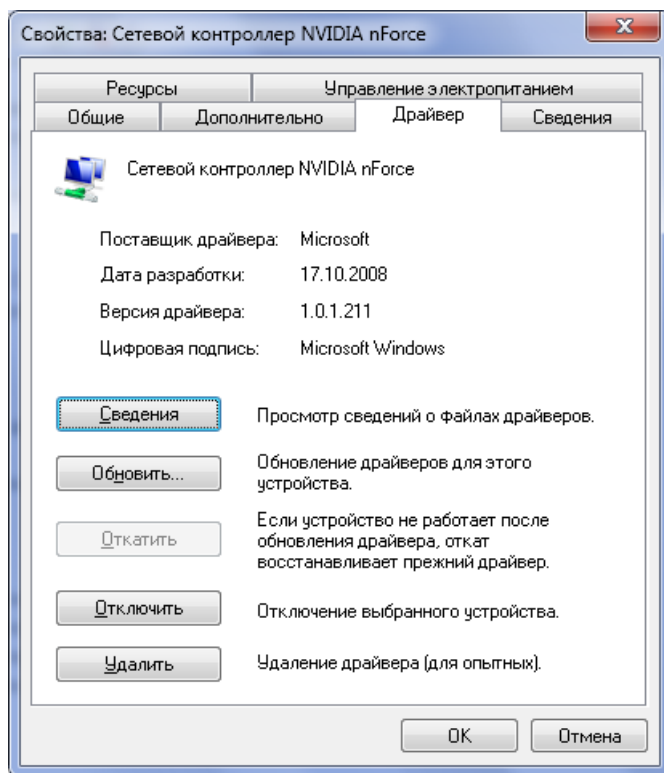


Рис. 5.15. На вкладке **Драйвер** свойств устройства предусмотрена возможность выполнения отката драйвера (замены текущего драйвера на предыдущий)

Аппаратные профили

В Windows 2000/XP обеспечивалась возможность создания множества аппаратных конфигураций, хранящихся в реестре. Начав работать в Windows Vista, многие пользователи удивлялись, почему эта опция стала недоступна. Недоступной она осталась и в Windows 7. Зачастую можно даже встретить утверждение, что новейшие версии Windows больше не поддерживают аппаратных профилей. Так ли это? Так, но не совсем. На самом деле проблема заключается в том, что Windows Vista и Windows 7 автоматически создают аппаратные профили в зависимости от типа используемого компьютера и больше не предоставляют пользователям возможности их ручного конфигурирования. Отсутствует и опция выбора аппаратного профиля во время загрузки системы. Тем не менее, аппаратные профили по-прежнему присутствуют в системном реестре в составе ключа `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles` (рис. 5.16).

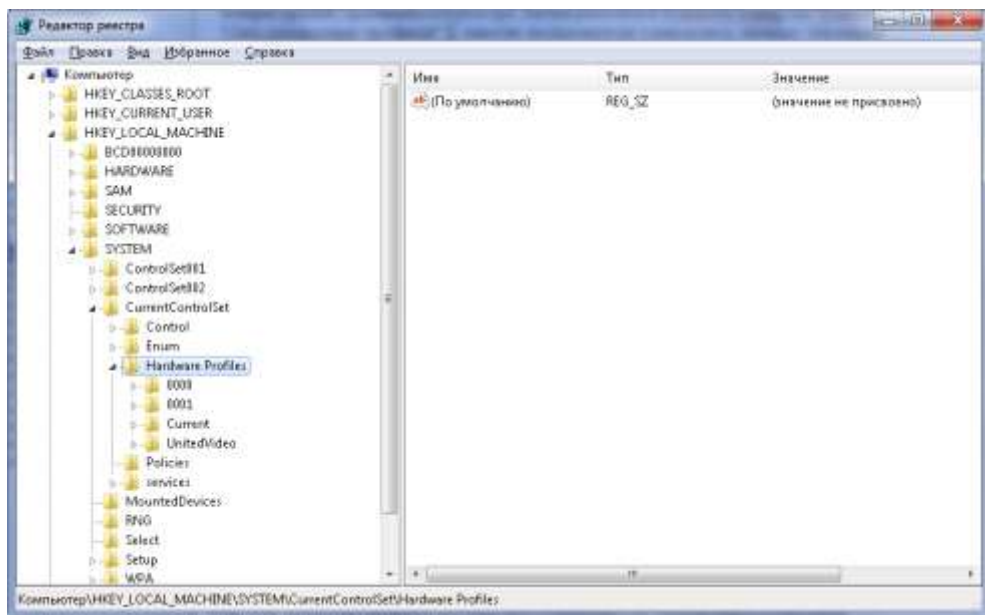


Рис. 5.16. Аппаратные профили по-прежнему присутствуют в реестре Windows Vista и Windows 7 в составе ключа `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles`

Кроме того, с аппаратными профилями в Windows Vista все еще можно было работать, блокируя сервисы и драйверы для конкретного аппаратного профиля. Это делается так:

1. Нажмите кнопку **Пуск** (Start), затем выберите опции **Все программы** (All Programs), **Служебные** (Accessories) и, наконец, **Администрирование** (Administrative Tools).
2. Выберите опцию **Службы** (Services), затем выберите сервис, подлежащий блокированию, щелкните правой кнопкой мыши и выберите из контекстного меню опцию **Свойства** (Properties).
3. Перейдите на вкладку **Вход в систему** (Log On), и в нижней части окна вы увидите список имеющихся аппаратных профилей (рис. 5.17).
4. Выберите из списка нужный профиль и нажмите кнопку **Запретить** (Disable).
5. Нажмите кнопку **ОК**.
6. Теперь, когда Windows Vista запустится с использованием выбранного аппаратного профиля, конфигурированный сервис будет блокирован.

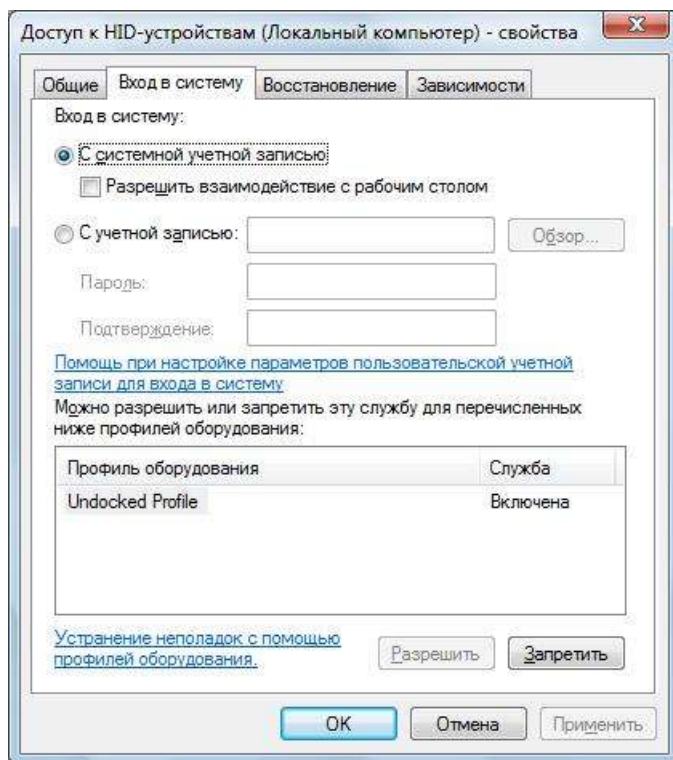


Рис. 5.17. Устранение неполадок в работе сервисов с помощью аппаратных профилей

ПРИМЕЧАНИЕ

В Windows 7 и эта возможность работы с аппаратными профилями через пользовательский интерфейс была ликвидирована. Впрочем, вот для таких случаев и предназначен редактор реестра. В последующих главах этой книги будет приведен пример, иллюстрирующий эту возможность.

Ключи реестра, используемые драйверами устройств

Операционная система, драйверы, а также компоненты, принимающие участие в установке устройств, хранят необходимую им информацию о драйверах и устройствах в реестре. В общем случае, драйверы и компоненты инсталляторов устройств должны использовать реестр для хранения данных, которые должны сохраняться неизменными в течение интервала времени между перезагрузками системы. Таким образом, система использует реестр

для хранения информации о драйверах и устройствах, а драйверы устройств могут хранить в реестре информацию, предназначенную исключительно для их собственных нужд.

Исполняющая подсистема Windows (модуль Executive) предоставляет следующие наборы процедур для манипулирования реестром¹¹:

- ❑ процедуры для манипулирования объектами "ключ реестра" (Registry Key Object Routines);
- ❑ процедуры для манипулирования библиотекой времени исполнения (Registry Run-Time Library Routines);
- ❑ процедуры Plug and Play для манипулирования реестром (Plug and Play Registry Routines).

ПРИМЕЧАНИЕ

Компоненты реестра должны трактоваться как модифицируемая информация. Если один из компонентов драйвера пишет информацию в реестр, а другой компонент впоследствии читает эту информацию, не следует полагаться на то, что информация за это время не изменилась. Поэтому, считав информацию из реестра, компоненты драйвера всегда должны произвести проверку информации перед ее использованием.

Перечислим основные ключи реестра, используемые драйверами устройств:

- ❑ HKLM\SYSTEM\CurrentControlSet\Services;
- ❑ HKLM\SYSTEM\CurrentControlSet\Control;
- ❑ HKLM\SYSTEM\CurrentControlSet\Enum;
- ❑ HKLM\SYSTEM\CurrentControlSet\Hardware Profiles.

Обратите внимание, что драйверы не получают к этим ключам непосредственного доступа. Компоненты инсталлятора драйвера режима пользователя и сами драйверы используют для этого системные функции, информацию о которых можно найти в сопроводительной документации к WDK. Кроме того, доступ к реестру может осуществляться с помощью директив файлов INF.

Ключ HKLM\SYSTEM\CurrentControlSet представляет собой самое надежное хранилище данных драйверов, так как эти данные хранятся в улье SYSTEM, и операционная система предпринимает дополнительные меры для защиты системных ульев.

¹¹ Более подробную информацию об этих процедурах следует искать в сопроводительной документации к программному продукту Windows Driver Kit (WDK), который можно загрузить со следующего адреса: <http://www.microsoft.com/whdc/DevTools/WDK/WDKpkg.mspk>.

Ключ **HKLM\SYSTEM\CurrentControlSet\Services**

Ключ реестра **HKLM\SYSTEM\CurrentControlSet\Services** хранит информацию обо всех сервисах, установленных в системе. Для каждого из установленных в системе драйверов в составе этого ключа создается подключ вида **HKLM\SYSTEM\CurrentControlSet\Services\DriverName**, где *DriverName* — имя конкретного драйвера. Диспетчер Plug and Play передает этот путь к драйверу через параметр *RegistryPath* при вызове процедуры *DriverEntry*. В составе этого ключа драйвер хранит определенную для него глобальную информацию, и эта информация доступна драйверу при его инициализации во время загрузки системы.

Особый интерес представляют следующие вложенные ключи и значимые элементы этого ключа:

- ❑ **ImagePath** — параметр, указывающий полный путь к файлу драйвера. Типичное значение этого параметра выглядит следующим образом: `%windir%\system32\Drivers\DriverName.sys`, где *DriverName* — имя вложенного ключа драйвера в составе ключа **HKLM\SYSTEM\CurrentControlSet\Services**, а `%windir%` — имя папки, в которой установлена операционная система Windows Vista/7. Программа установки создает это значение, руководствуясь значением, задаваемым параметром *ServiceBinary* в разделе *service-install-section* INF-файла соответствующего драйвера;
- ❑ **Parameters** — ключ, используемый для хранения индивидуальной информации драйвера. Параметры в состав этого ключа добавляются с помощью директивы *AddReg* в INF-файле соответствующего драйвера;
- ❑ **Performance** — ключ, задающий необязательную информацию для мониторинга производительности устройства. Параметры в составе этого ключа указывают имя DLL мониторинга производительности, специфичной для этого драйвера, а также имена функций, экспортируемых этой DLL. Как и в случае ключа **Parameters**, значимые элементы в состав этого ключа добавляются с помощью утилиты *AddReg* в INF-файле соответствующего драйвера.

ПРИМЕЧАНИЕ

Более подробно ключ **HKLM\SYSTEM\CurrentControlSet\Services** будет обсуждаться в *главе 8*, в разделе, посвященном инициализации сервисов и драйверов в процессе загрузки Windows Vista/7.

Ключ **HKLM\SYSTEM\CurrentControlSet\Control**

Ключ **HKLM\SYSTEM\CurrentControlSet\Control** содержит информацию, управляющую конфигурированием устройств в процессе загрузки системы. Более подробно он будет рассматриваться в *главе 7*, здесь же отметим лишь

ряд вложенных ключей, представляющих особый интерес для разработчиков драйверов:

- ❑ **Class** — содержит информацию о классах инсталляции устройств (Device Setup Classes), имеющихся в системе. Классы инсталляции устройств используются для группировки устройств, устанавливаемых и конфигурируемых аналогичным образом. Для каждого класса инсталляции в составе ключа `HKLM\SYSTEM\CurrentControlSet\Control\Class` имеется вложенный ключ, имя которого совпадает с номером GUID¹² соответствующего класса инсталляции (рис. 5.18). В составе каждого из ключей `HKLM\SYSTEM\CurrentControlSet\Control\Class\Class_GUID` содержится информация о классе инсталляции, в том числе: сведения об инсталляторе класса (class installer), если он имеется, и о зарегистрированных драйверах фильтра;

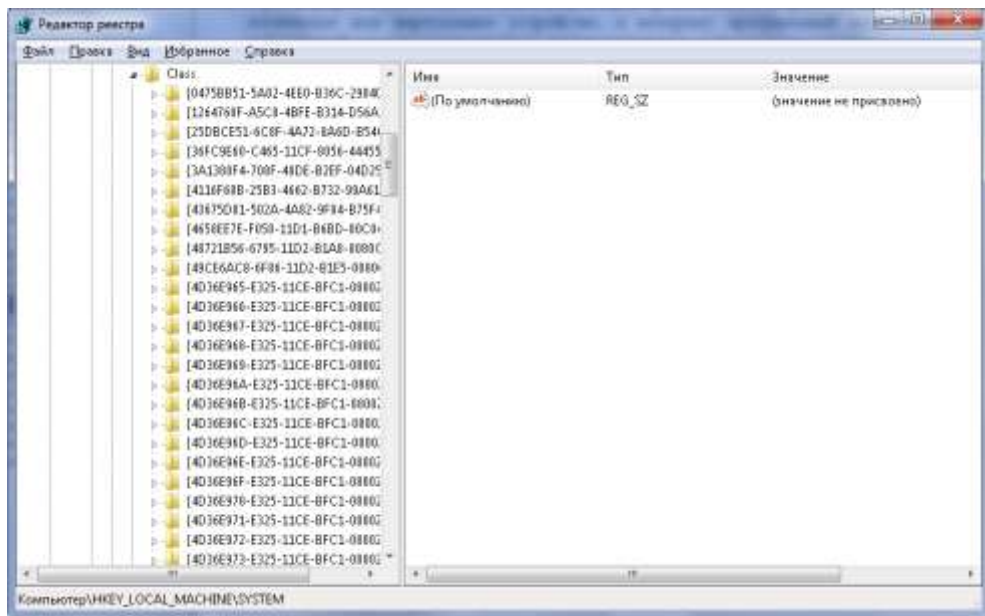


Рис. 5.18. Информация о классах инсталляции устройств в составе ключа `HKLM\SYSTEM\CurrentControlSet\Control\Class`

¹² GUID (Globally Unique Identifier) — статистически уникальный 128-битный идентификатор, позволяющий создавать расширяемые сервисы и приложения без опасения конфликтов, вызванных совпадением идентификаторов. Хотя уникальность каждого отдельного GUID не гарантируется, общее количество уникальных ключей настолько велико (2^{128} или $3,4028 \times 10^{38}$), что вероятность того, что в мире будут независимы сгенерированы два совпадающих ключа, достаточно мала. Значения GUID можно получить с помощью утилиты `Uuidgen.exe` (более подробную информацию о ней можно найти в документации Windows Platform SDK).

- ❑ `CoDeviceInstallers` — содержит информацию о ко-инсталляторах класса (class-specific co-installers), зарегистрированных в системе;
- ❑ `DeviceClasses` — содержит информацию об интерфейсах устройств, зарегистрированных в системе. Любой драйвер устройства, будь то физическое, логическое или виртуальное устройство, к которому программный код, работающий в режиме пользователя, может отправлять запросы на ввод/вывод, должен предоставлять интерфейс клиентам режима пользователя. Класс интерфейса устройства предоставляет функциональные возможности устройства и его драйвера другим системным компонентам и приложениям режима пользователя. Для каждого класса интерфейса в составе этого ключа имеется вложенный ключ, ассоциированный с соответствующим GUID.

Ключ `HKLM\SYSTEM\CurrentControlSet\Enum`

Ключ `HKLM\SYSTEM\CurrentControlSet\Enum` содержит информацию об устройствах, имеющихся в системе. Диспетчер Plug and Play создает в составе этого ключа вложенный ключ для каждого устройства. Эти вложенные ключи имеют вид `HKLM\SYSTEM\CurrentControlSet\Enum\enumerator\deviceID`. В составе каждого из этих ключей есть вложенный ключ для каждого экземпляра устройства, присутствующего в системе. Этот вложенный ключ, известный как *аппаратный ключ устройства* (hardware key или device key), содержит следующую информацию: описание устройства, его аппаратный идентификатор (hardware ID), идентификаторы совместимых устройств (compatible IDs) и требования к ресурсам.

Ключ `HKLM\SYSTEM\CurrentControlSet\Enum` зарезервирован для внутреннего использования компонентами операционной системы, и его внутренняя структура может изменяться. Драйверы и компоненты инсталлятора, работающие в пользовательском режиме, должны получать доступ к этому ключу, используя документированные функции операционной системы. Ни драйверы, ни программы-инсталляторы не должны получать прямого доступа к этому ключу.

Ключ `HKLM\SYSTEM\CurrentControlSet\Hardware Profiles`

Ключ `HKLM\SYSTEM\CurrentControlSet\Hardware Profiles` содержит информацию об аппаратных профилях, имеющихся в системе.

Встроенные средства Windows 7 по управлению надежностью

Целью обсуждаемых в данном разделе мероприятий является обеспечение надежности работы системы Windows Vista/7 для обеспечения возможности ее запуска при любых обстоятельствах. Процедура нормальной загрузки Windows 7 будет рассмотрена в *главе 7*, а диагностика проблем с загрузкой и примеры восстановления системы после сбоев — в *главах 11* и *12*. Однако само собой разумеется, что мероприятия по обеспечению защиты данных и меры по предотвращению сбоев должны быть спланированы заранее.

Регулярное выполнение плановых профилактических процедур позволит предотвратить возможные проблемы или свести к минимуму их последствия. Наиболее общие рекомендации сводятся к следующему:

- ❑ довольно часто причиной некорректной работы системы или даже проблем с ее загрузкой может быть перезапись системного файла или же установка несовместимого драйвера. Обычно это происходит во время инсталляции дополнительного программного обеспечения, не совместимого с операционной системой. Эта проблема существовала во всех предыдущих версиях Windows NT. Начиная с Windows 2000/XP, были введены дополнительные средства защиты системных файлов и драйверов с помощью цифровой подписи, которая гарантирует их совместимость и корректную работу. В новейших версиях Windows эти защитные средства получили дальнейшее развитие;
- ❑ выполнение резервного копирования системных файлов конфигурации, в том числе и реестра, а также выполнение процесса полного резервного копирования системы. Не забывайте выполнять эти операции прежде, чем вносить какие-либо существенные изменения в конфигурацию системы (к этому также относится установка новых устройств и программного обеспечения). Эти меры были рассмотрены в *главе 2*;
- ❑ не отключайте функцию восстановления системы (System Restore). Некоторые пользователи полагают, будто это инструментальное средство занимает слишком много пространства на жестком диске, однако оно окажется необходимым в случае восстановления поврежденной системы. Подробные инструкции по выполнению восстановления системы приведены в *главе 2*;
- ❑ рекомендуется ежедневно просматривать журналы системных событий (как минимум, журналы **System** и **Application**). В особенности обращайте внимание на ошибки, генерируемые драйверами жестких дисков, т. к. они

могут указывать на возможные повреждения файловой системы. Если эта рекомендация не выполняется, то ошибки файловой системы могут оставаться незамеченными до тех пор, пока программа Chkdsk не укажет на их существование. Стоит отметить, что при этом поврежденные данные могут попасть и на резервную копию, поскольку программы резервного копирования не распознают ошибки и повреждения в пользовательских данных;

- регулярно выполняйте проверку дисков для своевременного обнаружения ошибок файловой системы. Кроме того, рекомендуется регулярно проводить и дефрагментацию дисков, что позволит избежать проблем с низкой производительностью. Имейте в виду, что для дефрагментации следует применять только встроенные средства Windows или утилиты сторонних производителей, имеющие статус Designed for Windows 7. Информацию о программном обеспечении, тестировавшемся на совместимость с Windows 7, в том числе и об утилитах дефрагментации дисков, можно найти по адресу **<https://connect.microsoft.com/site/sitehome.aspx?SiteID=831>**;
- если есть возможность, установите избыточную копию операционной системы, чтобы сделать систему более надежной.

В составе Windows 7 имеется целый набор средств, позволяющих предотвратить повреждение системы и выполнить ее восстановление, если система все же получила повреждения. К их числу относятся:

- *защита ресурсов Windows* (Windows Resource Protection, WRP) — во всех ранних версиях операционных систем из семейства Windows NT вплоть до Windows NT 4.0 системные файлы, в т. ч. библиотеки динамической компоновки (DLL) и исполняемые файлы (EXE) не имели защиты от модификации или умышленного повреждения. При их замене некорректно работающей или несовместимой версией оказывались возможными самые разнообразные последствия — от снижения общей производительности системы до ее катастрофического сбоя. Начиная с Windows 2000/XP, Microsoft начала предоставлять набор средств, позволяющих гарантировать защиту системных файлов и драйверов устройств от их случайной замены при установке дополнительного программного обеспечения. Набор средств защиты файлов цифровой подписью, появившийся в Windows XP, включил в свой состав такие средства, как защита системных файлов (System File Protection, SFP), проверка системных файлов (System File Checker, SFC) и верификация цифровой подписи файлов (File Signature Verification, FSV). Начиная с Windows Vista, эти средства получили дальнейшее развитие и в новейших версиях Windows известны под собирательным названием Windows Resource Protection (WRP);

- ❑ *откат драйвера (Driver Rollback)* — пожалуй, одно из самых полезных средств восстановления. Если вы установили и обновили версию драйвера после инсталляции Windows и подозреваете, что сделанное вами обновление драйвера дестабилизирует работу системы или же вызовет проблемы с загрузкой, вы можете вместо новой версии драйвера восстановить прежнюю версию. Замена драйвера представляет собой самый простой способ восстановления системы, разумеется, в том случае, если именно новый драйвер является причиной возникновения проблемы. Кнопка **Откатить (Roll Back Driver)** в окне **Диспетчер устройств (Device Manager)** позволяет вернуться к использованию предыдущего драйвера, пока вы будете исследовать вопрос о новом драйвере. Процедура отката драйверов (Driver Rollback) описана чуть ранее. Обратите внимание, что если вы обновили несколько драйверов в течение одного сеанса, то удобнее будет воспользоваться опцией запуска — **Загрузка последней удачной конфигурации (Last Known Good Configuration)** или же средством восстановления системы (System Restore), а не возвращаться к использованию прежних драйверов по отдельности;
- ❑ *автоматическое обновление (Automatic Updates)* — автоматизирует процесс загрузки обновлений с сайта Windows Update. Хотя в Windows 7, как и в Windows Vista, установка многих обновлений по-прежнему требует перезагрузки, сам процесс установки обновлений стал гораздо менее назойливым, чем это было в Vista, и более удобным. Так, например, само диалоговое окно теперь позволяет пользователю отложить перезагрузку и указать более продолжительный временной период (до четырех часов), по истечении которого окно, предлагающее перезагрузить компьютер, появится вновь (рис. 5.19). Обновление происходит в фоновом режиме, причем сервис Windows Update (wuauserv) использует преимущества NTFS на базе транзакций (Transactional NTFS), что позволяет Windows выполнить откат незавершившихся транзакций в случае неожиданного сбоя в процессе внесения изменений в систему в ходе автоматической установки обновлений;
- ❑ *безопасный режим загрузки (Safe Mode)* — предоставляет средства быстрого восстановления системы после сбоев, вызванных некорректной установкой нового программного обеспечения или драйверов устройств. Безопасный режим загрузки будет рассмотрен в главе 7, а также в главах 11 и 12. Здесь же следует отметить, что применение безопасного режима загрузки помогает не во всех случаях. Так, этот режим не поможет, если повреждены системные файлы, а также при повреждениях жесткого диска;
- ❑ *составление отчета об ошибках (Error Reporting)* — отслеживаются проблемы в системе, влияющие на компоненты Windows 7 и работающие

в ней приложения. При возникновении проблемы вы можете отослать отчет о ней в Microsoft и получить ответ;

□ *среда восстановления Windows* (Windows Recovery Environment, WinRE) — содержит новый набор функций восстановления поврежденной системы:

- восстановление запуска (Startup Repair);
- восстановление системы (System Restore);
- восстановление образа системы;
- средство диагностики памяти Windows (Windows Memory Diagnostics Tool);
- командная строка (Command Prompt).

Более подробно эти функции будут рассмотрены в *главах 7, 11 и 12*.

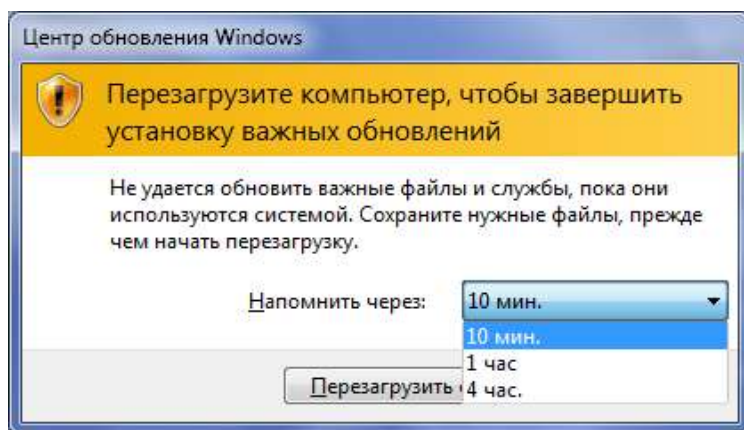


Рис. 5.19. Пользовательский интерфейс автоматических обновлений Windows стал более удобным и гибким, позволяя отложить перезагрузку системы, требуемую при установке некоторых обновлений

Защита системных файлов Windows

Все системные файлы и драйверы в Windows Vista и Windows 7 защищены с помощью цифровой подписи, гарантирующей их совместимость с операционной системой. Цифровая подпись Microsoft удостоверяет, что файл, снабженный ею, тестировался на совместимость с соответствующей версией Windows и не был модифицирован или переписан во время установки дополнительного программного обеспечения.

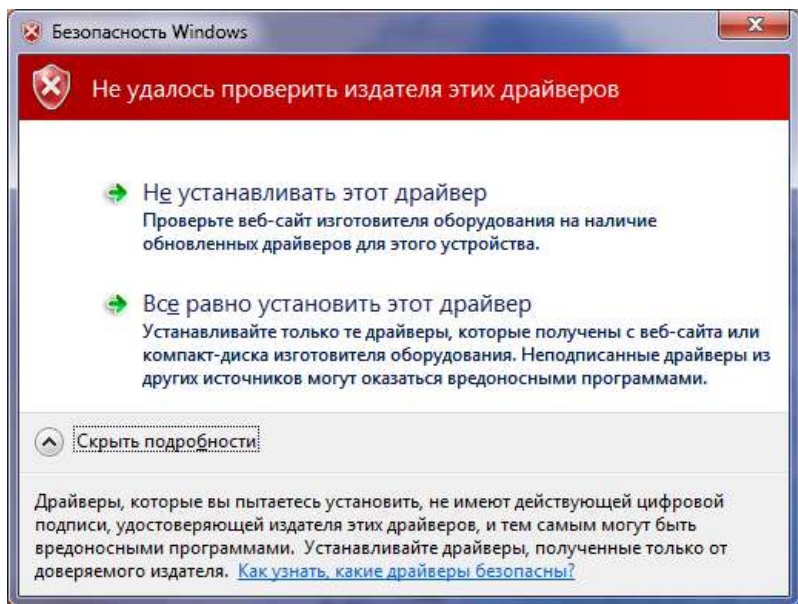


Рис. 5.20. Диалоговое окно, отображаемое Windows 7, когда при установке драйвера выясняется, что он не имеет цифровой подписи

В зависимости от опций настройки Windows 7 может либо игнорировать драйверы, не имеющие цифровой подписи, либо выводить предупреждение при обнаружении таких драйверов (рис. 5.20) или же просто не допускать их установки. По умолчанию Windows 7 выводит предупреждение, позволяющее пользователю самостоятельно решить, следует ли отменять установку драйвера.

Чтобы установить опции защиты драйверов цифровой подписью в Windows 7 через пользовательский интерфейс, следует воспользоваться Редактором групповой политики. Для этого сделайте следующее:

1. Запустите сеанс командной строки с административными полномочиями и введите команду `gpedit.msc`.
2. Разверните ветвь **Конфигурация пользователя** (User Configuration) | **Административные шаблоны** (Administrative Templates) | **Система** (System) | **Установка драйвера** (Driver Installation). Установите для параметра **Цифровая подпись драйвера** (Driver Digital Signature) опцию **Включен** (Enabled), после чего вы сможете выбрать нужную опцию из списка, расположенного в нижней части окна (рис. 5.21):
 - если установлена опция **Пропустить** (Ignore), то система даст возможность устанавливать любые драйверы, игнорируя наличие или отсутст-

вие цифровой подписи (именно так ведет себя Windows NT 4.0). Как уже упоминалось, отсутствие у драйвера или системного файла цифровой подписи указывает, что его совместимость с Windows 7 официально не подтверждена, и он может стать источником неприятностей;

- если установлена опция **Предупредить** (Warn), то система будет выводить предупреждающие сообщения при попытке установить драйвер, не имеющий цифровой подписи. Обратите внимание, что несмотря на вывод предупреждения, драйвер, тем не менее, будет установлен;
- если установлена опция **Блокировка** (Block), то драйверы, не имеющие цифровой подписи, устанавливаться не будут.

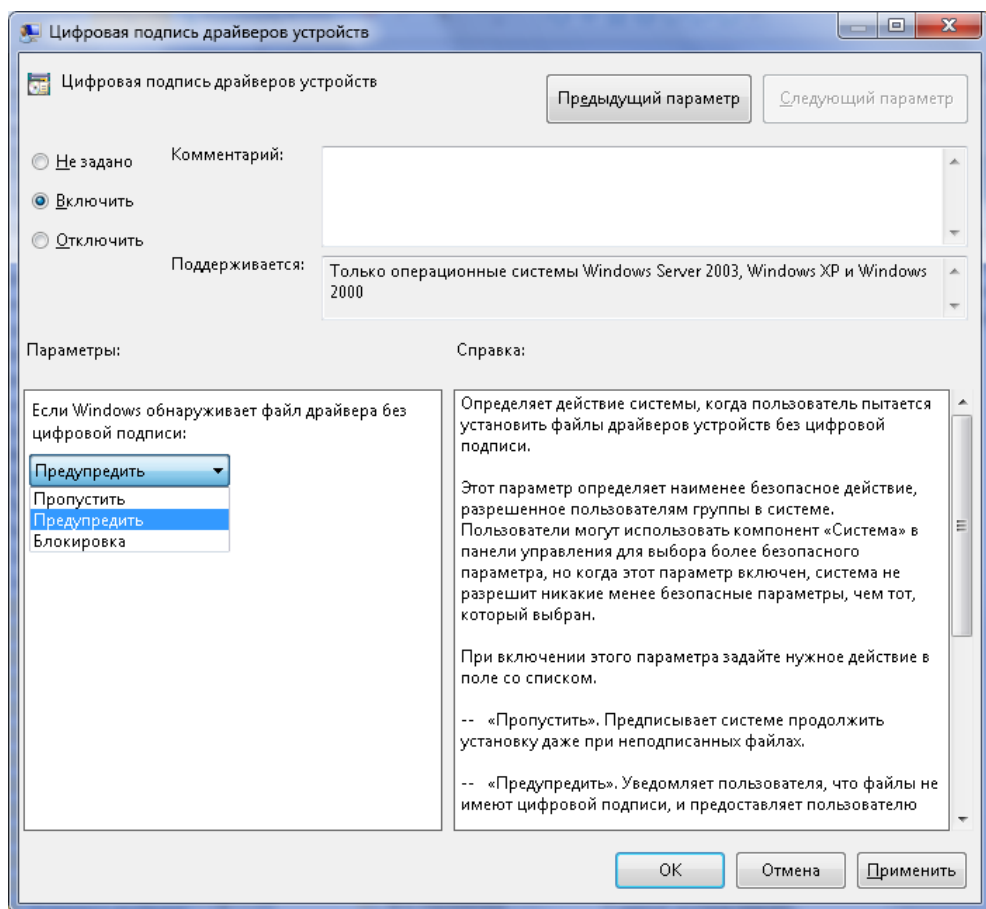


Рис. 5.21. Выбор опций поведения системы в отношении драйверов, не имеющих цифровой подписи

Механизм защиты драйверов цифровой подписью

Каким образом обычно происходит установка драйверов в новейших версиях Windows? Есть два способа:

- ❑ автоматическая установка драйвера подсистемой PnP. Этот метод впервые появился в Windows 2000, был "подхвачен" в Windows XP и в Windows Vista/7 является рекомендуемым. Более подробная информация по данному вопросу была приведена ранее в этой главе. Здесь лишь следует напомнить, что Windows пытается установить драйвер, после того как подсистема Plug and Play (PnP subsystem) обнаружит новое устройство. Диспетчер Plug and Play, предназначенный для работы в пользовательском режиме (UMPNPMGR, системная динамически загружаемая библиотека %SystemRoot%\System32\Umpnpgm.dll) ожидает, когда подсистема PnP режима ядра уведомит ее об обнаружении нового устройства. Получив такое уведомление, UMPNPMGR ищет информационный файл драйвера устройства (файл с расширением inf), в котором содержится информация, необходимая для установки драйвера. Все файлы INF для драйверов, имеющих в составе дистрибутива Windows, располагаются в каталоге %SystemRoot%\INF. Если вы устанавливаете драйвер OEM, то его INF-файл должен находиться на дистрибутивном носителе, полученном от поставщика устройства (как правило, это либо трехдюймовая дискета, либо компакт-диск);
- ❑ использование мастера установки аппаратных средств (Hardware Installation Wizard, %SystemRoot%\System32\Newdev.dll). Мастер установки аппаратных средств выполняет аналогичные шаги и тоже ищет файл INF устанавливаемого драйвера.

Как UMPNPMGR, так и мастер установки аппаратных средств, используют интерфейс прикладного программирования установки (SETUPAPI — %SystemRoot%\System32\Setupapi.dll) для чтения информации, содержащейся в файле с расширением inf. Помимо обработки инструкций по установке драйвера, Windows в обязательном порядке проводит проверку значения параметра реестра Policy, расположенного под ключом HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Driver Signing (рис. 5.22).

Если параметр Policy имеет значение 0, это соответствует опции установки драйверов, не имеющих цифровой подписи. Если для этого параметра установлено значение 1, то такие драйверы будут устанавливаться с выводом предупреждающего сообщения, а если установлено значение 2, все драйверы, не имеющие цифровой подписи, станут игнорироваться.

Начиная с Windows Vista, технологии защиты драйверов цифровой подписью были усовершенствованы. Для установки неподписанных компонентов

режима ядра теперь в обязательном порядке требуются административные привилегии. К числу таких компонентов относятся драйверы устройств, драйверы фильтра, сервисы и т. п.

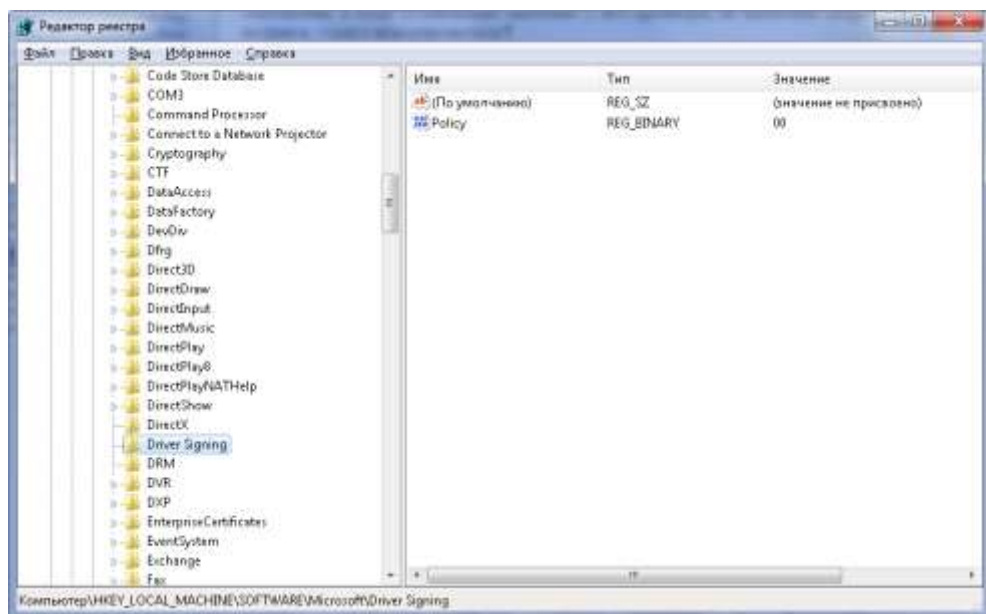


Рис. 5.22. Ключ реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Driver Signing

ПРИМЕЧАНИЕ

В 64-разрядных версиях Windows для загрузки ПО, работающего на уровне ядра, цифровая подпись необходима. Тем не менее, исследователи обнаружили методы обхода этого ограничения. Более подробную информацию на эту тему можно найти на сайте <http://www.invisiblethings.org>.

Драйверы и сервисы, загрузка которых осуществляется загрузчиком операционной системы перед инициализацией ядра, должны иметь цифровую подпись.

Если политика, действующая в отношении установки драйверов, не имеющих цифровой подписи, диктует необходимость проверки цифровой подписи, то библиотека Setupapi.dll обращается к криптографическим сервисам CryptoAPI для расшифровки цифровой подписи с использованием открытого ключа VeriSign.

Где же хранятся цифровые подписи, защищающие драйверы и системные файлы Windows? Microsoft хранит цифровые подписи драйверов, входящих

в состав дистрибутива, в *файлах каталога* (catalog files) в папке %SystemRoot%\System32\Catroot. Драйверы устройств OEM должны поставляться вместе с их собственными файлами каталога, которые Microsoft предоставит фирме-разработчику после успешного тестирования устройства и включения его в список совместимых аппаратных средств (Hardware Compatibility List, HCL). В каталоге \Catroot содержится мастер-индекс файлов каталога драйверов (sysmast.cbd и sysmast.cbk) и вложенная папка, имя которой представляет собой длинную комбинацию букв и цифр. Раскрыв эту папку, вы обнаружите файлы каталога для всех встроенных компонентов.

Если результат расшифровки цифровой подписи драйвера или системного файла не совпадет с цифровой подписью, найденной в файле каталога драйверов, или если драйвер не имеет файла каталога, то, в зависимости от установленных опций, или пользователь получит предупреждающее сообщение, или же установка драйвера завершится неудачей.

Другие средства защиты системных файлов Windows

Кроме указанных, в состав Windows Vista и Windows 7 входят следующие функциональные возможности по защите драйверов и системных файлов, гарантирующие их неизмененное состояние:

- ☐ защита ресурсов Windows (Windows Resource Protection);
- ☐ проверка системных файлов (System File Checker);
- ☐ верификация цифровой подписи (File Signature Verification).

Защита ресурсов Windows

Все ранние версии Windows имели один общий недостаток — при установке дополнительного программного обеспечения практически любые совместно используемые системные файлы, в том числе DLL и EXE, могли быть изменены. Последствия замены этих файлов некорректными или несовместимыми версиями могли быть непредсказуемыми — от снижения производительности операционной системы до некорректного поведения остальных приложений, периодического появления ошибок **STOP** и даже проблем с загрузкой.

В Windows 2000 впервые за всю историю Windows была сделана попытка исправления этой ситуации. Разумеется, эта функциональная возможность существовала и в Windows XP. Наконец, в Windows Vista и Windows 7 функция Windows File Protection (WFP) была заменена механизмом Windows Resource Protection (WRP). В отличие от функции WFP в предшествующих

версиях, механизм WRP в Windows Vista/7 защищает не только файлы и папки, но и ключи реестра. В число ресурсов, защищаемых WRP, входят:

- ☐ все файлы, установленные Windows Vista/7 и имеющие расширения `dll`, `exe`, `ocx` и `sys`;
- ☐ критические файлы, установленные Windows Vista/7 и имеющие расширения `acm`, `ade`, `adp`, `app`, `asa`, `asp`, `aspx`, `ax`, `bas`, `bat`, `bin`, `cer`, `chm`, `clb`, `cmd`, `cnt`, `cnv`, `com`, `cpl`, `cpx`, `crt`, `csch`, `dll`, `drv`, `dtd`, `exe`, `fxp`, `grp`, `h1s`, `hlp`, `hta`, `ime`, `inf`, `ins`, `isp`, `its`, `js`, `jse`, `ksh`, `lnk`, `mad`, `maf`, `mag`, `mam`, `man`, `maq`, `mar`, `mas`, `mat`, `mau`, `mav`, `maw`, `mda`, `mdb`, `mde`, `mdt`, `mdw`, `mdz`, `msc`, `msi`, `msp`, `mst`, `mui`, `nls`, `ocx`, `ops`, `pal`, `pcd`, `pif`, `prf`, `prg`, `pst`, `reg`, `scf`, `scr`, `sct`, `shb`, `shs`, `sys`, `tlb`, `tsp`, `url`, `vb`, `vbe`, `vbs`, `vs macros`, `vss`, `vst`, `vs w`, `ws`, `wsc`, `wsf`, `wsh`, `xsd` и `xsl`;
- ☐ критические папки, содержащие только файлы, защищенные механизмом WRP, могут быть заблокированы таким образом, что лишь сервис **TrustedInstaller** (установщик модулей Windows) сможет создавать в них файлы и вложенные папки. Кроме того, папка может быть заблокирована частично, и в этом случае создавать в ней файлы и вложенные папки смогут только администраторы;
- ☐ критически важные ключи реестра — если ключ реестра защищен WRP, то могут быть защищены и все его вложенные параметры и подключи.

Файлы, защищенные WRP и необходимые для перезагрузки Windows, копируются в папку `%Windir%\winsxs\Backup`. Размер этой папки и список файлов, копируемых в кэш, не подлежат изменению.

Проверка системных файлов

В состав Windows Vista и Windows 7 включено средство проверки системных файлов (System File Checker, `sfc.exe`), которое представляет собой утилиту командной строки. Эта утилита сканирует все установленные системные файлы и выполняет проверку их версий при перезагрузке компьютера. Если данная утилита обнаружит, что один из защищаемых системных файлов был замещен, она найдет корректную версию этого файла и запишет ее поверх измененного файла. Аналогичная утилита имела еще в Windows XP. Отличие между версиями `sfc.exe`, включенными в состав Windows XP и Windows Vista/7, состоит в наборе поддерживаемых опций.

Утилита командной строки имеет следующий синтаксис:

```
sfc [/option 1] [/option 2] ... [option n] [=full file path]
```

К числу опций команды `sfc` относятся:

- ☐ `/scannow` — параметр, при использовании которого выполняется немедленное сканирование всех защищаемых системных файлов. Поддерживается в Windows XP, Windows Vista и Windows 7;

- ❑ `/scanonce` — в Windows XP/2000 и Windows Server 2003 этот параметр указывает на необходимость однократного сканирования всех защищаемых системных файлов. Начиная с Windows Vista, параметр не поддерживается;
- ❑ `/scanboot` — в Windows XP/2000 и Windows Server 2003 этот параметр задает опцию сканирования всех защищаемых системных файлов при каждой перезагрузке. Начиная с Windows Vista, параметр не поддерживается;
- ❑ `/cancel` — в Windows 2000 этот параметр отменяет все отложенные запросы на сканирование защищаемых системных файлов. Начиная с Windows XP, параметр не поддерживается;
- ❑ `/quiet` — в Windows 2000 при установке этого параметра замена всех некорректных версий защищаемых файлов будет происходить без вывода предупреждения для пользователя. Начиная с Windows XP, параметр не поддерживается;
- ❑ `/enable` — в Windows 2000 этот параметр устанавливает стандартный режим работы средства System File Checker. Начиная с Windows XP, параметр не поддерживается;
- ❑ `/purgecache` — в Windows Server 2003 и Windows XP/2000 этот параметр очищает файловый кэш System File Protection и выполняет немедленное сканирование системных файлов. Начиная с Windows Vista, параметр не поддерживается;
- ❑ `/cachesize=x` — в Windows XP/2000 и Windows Server 2003 этот параметр устанавливает размер файлового кэша System File Protection (в мегабайтах). Значение по умолчанию составляет 0x32 (50 Мбайт). Начиная с Windows Vista, параметр не поддерживается;
- ❑ `/FILESONLY` — верифицирует и заменяет только файлы, но не ключи реестра. Поддерживается только в Windows Vista и Windows 7, но не в Windows 2000/XP;
- ❑ `/OFFBOOTDIR` — применяется для верификации и замены файлов в автономном режиме (offline repairs). При его использовании необходимо также указать путь к каталогу автономной загрузки (offline boot directory). Поддерживается только в Windows Vista и Windows 7, но не в Windows 2000/XP;
- ❑ `/OFFWINDIR` — для верификации и замены в автономном режиме. При его использовании необходимо указать путь к автономному каталогу Windows (offline Windows directory). Поддерживается только в Windows Vista и Windows 7, но не в Windows 2000/XP;

- ❑ /REVERT — устанавливает настройки по умолчанию. Поддерживается только в Windows XP;
- ❑ /SCANFILE — сканирует и замещает указанный файл (при использовании этого параметра необходимо указать полный путь к файлу). В Windows 2000/XP параметр не поддерживается;
- ❑ /VERIFYFILE — верифицирует указанный файл (но не выполняет замены). При использовании этого параметра необходимо указать полный путь к нужному файлу. Поддерживается только в Windows Vista и Windows 7, но не в Windows 2000/XP;
- ❑ /VERIFYONLY — сканирует все защищенные системные файлы, но не выполняет замены. Поддерживается только в Windows Vista и Windows 7, но не в Windows 2000/XP.

Верификация цифровой подписи файлов

В некоторых случаях установка нового программного обеспечения приводит к замещению системных файлов некорректными или несовместимыми версиями (которые, естественно, не имеют цифровой подписи). Такая замена, как уже неоднократно упоминалось, как раз и может послужить источником нестабильности системы (в том числе ошибок типа "синий экран" и проблем с загрузкой системы).

Во избежание такого рода проблем все системные файлы, устанавливаемые в процессе инсталляции Windows, снабжены цифровой подписью Microsoft, гарантирующей его совместимость с соответствующей версией Windows и указывающей, что данный файл либо представляет собой оригинальную версию, разработанную Microsoft, либо прошел тестирование и признан пригодным для использования с Windows 7. Верификация цифровой подписи файлов позволяет идентифицировать все установленные на проверяемом компьютере файлы, не имеющие цифровой подписи, и получить об этих файлах следующую информацию:

- ❑ имя файла и точный путь к нему;
- ❑ дату модификации файла;
- ❑ тип файла и точный номер его версии.

Чтобы запустить средство верификации цифровых подписей файлов, нажмите кнопку **Пуск** (Start), выберите команду **Выполнить** (Run) и введите команду `sigverif`.

Максимальную практическую пользу при устранении проблем, связанных с заменой системных файлов некорректными версиями, можно получить,

регистрируя информацию, собранную программой `sigverif`, в файле журнала. Для этой цели сделайте следующее:

1. Запустите программу `sigverif`, и в открывшемся окне **Проверка подписи файла** (File Signature Verification) нажмите кнопку **Дополнительно** (Advanced) (рис. 5.23).
2. В окне **Дополнительные параметры проверки подписи файла** (Advanced File Signature Verification Settings) перейдите на вкладку **Ведение журнала** (Logging) и установите флажок **Сохранять результаты проверки подписи в журнале** (Save the file signature verification results to a log file) (рис. 5.24).

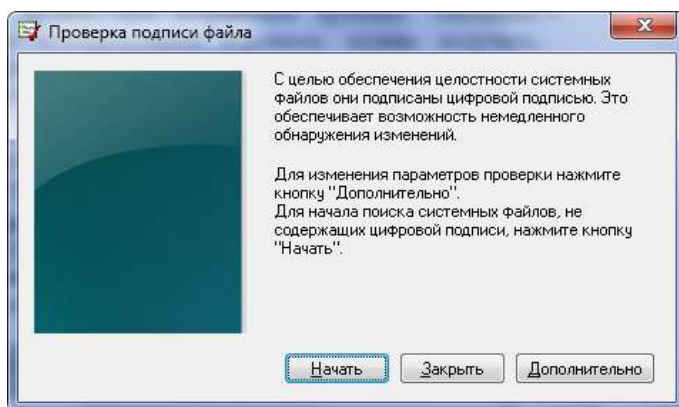


Рис. 5.23. Начальное окно программы **Проверка подписи файла** (File Signature Verification)

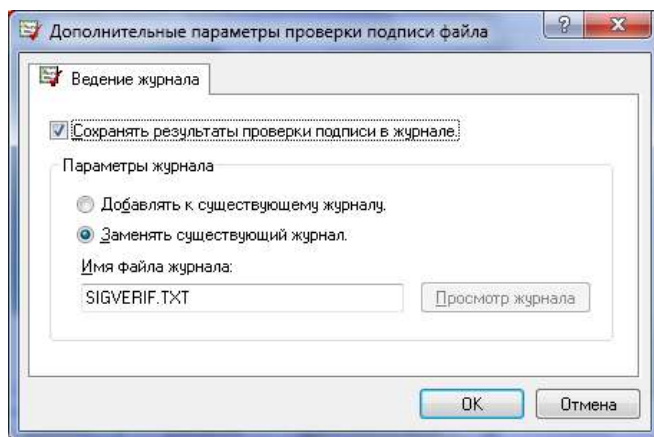


Рис. 5.24. Вкладка **Ведение журнала** окна **Дополнительные параметры проверки подписи файла**

3. Перейдите в группу **Параметры журнала** (Logging options), где имеется возможность установить по выбору следующие опции ведения файла журнала:
 - **Добавлять к существующему журналу** (Append to existing log file) — результаты новой операции поиска будут добавлены в конец существующего файла журнала;
 - **Заменять существующий журнал** (Overwrite existing log file) — результаты новой операции сканирования запишутся поверх существующего файла журнала;
 - **Имя файла журнала** (Log file name) — можно вручную ввести имя файла журнала.
4. Нажмите кнопку **ОК**. Вы вернетесь в окно **Проверка подписи файла** (File Signature Verification). Чтобы начать операцию сканирования, нажмите в этом окне кнопку **Начать** (Start). Степень завершенности процесса сканирования будет отражаться индикатором **Просмотр файлов...** (Scanning files...) (рис. 5.25). Для отмены сканирования нажмите кнопку **Остановить** (Stop). По окончании сканирования, если будут обнаружены файлы, не имеющие цифровой подписи, на экране появится окно, отображающее полный список таких файлов.

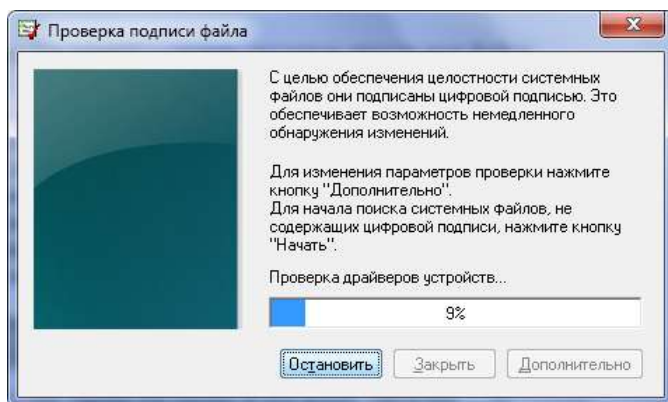


Рис. 5.25. Идет процесс сканирования системных файлов на наличие цифровой подписи

Заключение

В данной главе были рассмотрены системные сервисы и драйверы Windows 7, их роль и место в системе, включая взаимодействие с реестром, а также модернизированные средства повышения надежности и защиты системы. Вся эта информация необходима для правильного понимания процесса загрузки Windows Vista, который будет рассматриваться в *главе 7*.

Глава 6



Диагностика и устранение неполадок в работе с аппаратными средствами

Машина должна работать, человек — думать.

Принцип IBM

Проблемы, вызванные неполадками оборудования, подпадают под одну из следующих категорий:

- ❑ проблемы, препятствующие загрузке Windows. Эти проблемы будут рассматриваться в *главах 7, 11 и 12*, поэтому здесь мы не будем останавливаться на них подробно. Отметим только, что они могут быть как чисто аппаратными (устройство физически неисправно), так и вызываться некорректными или несовместимыми драйверами;
- ❑ проблемы, возникающие при установке нового оборудования. При этом новые устройства могут либо не обнаруживаться, либо работать не так, как ожидалось, либо даже вызывать системные сбои;
- ❑ непредсказуемые проблемы, когда аппаратные компоненты вызывают сбои приложений и сервисов, зависания, ошибки **STOP** и т. п.;
- ❑ проблемы, вызванные перегревом устройств, медленным выходом из спящих режимов, медленной работой устройств, от которых мы вправе ожидать более высокой производительности.

В этой главе мы рассмотрим большинство перечисленных проблем и дадим рекомендации по их устранению.

Проблемы, связанные с установкой нового оборудования

Проблемы с установкой нового оборудования могут возникать в любой ОС, и Windows 7 — не исключение из этого правила. Если вновь установленное устройство не обнаруживается или ведет себя не так, как ожидалось, в первую очередь проверьте его состояние с помощью средства **Диспетчер устройств** (Device Manager), общие принципы работы с которым были описаны в *главе 5*. Диспетчер устройств в Windows 7 является основным средством, позволяющим решить проблемы неполадок оборудования и ассоциированных с ним драйверов.

Чтобы выполнить диагностику аппаратных устройств, запустите Диспетчер устройств, действуя по инструкциям, приведенным в *главе 5*. Диспетчер устройств отобразит дерево аппаратных средств (рис. 6.1).

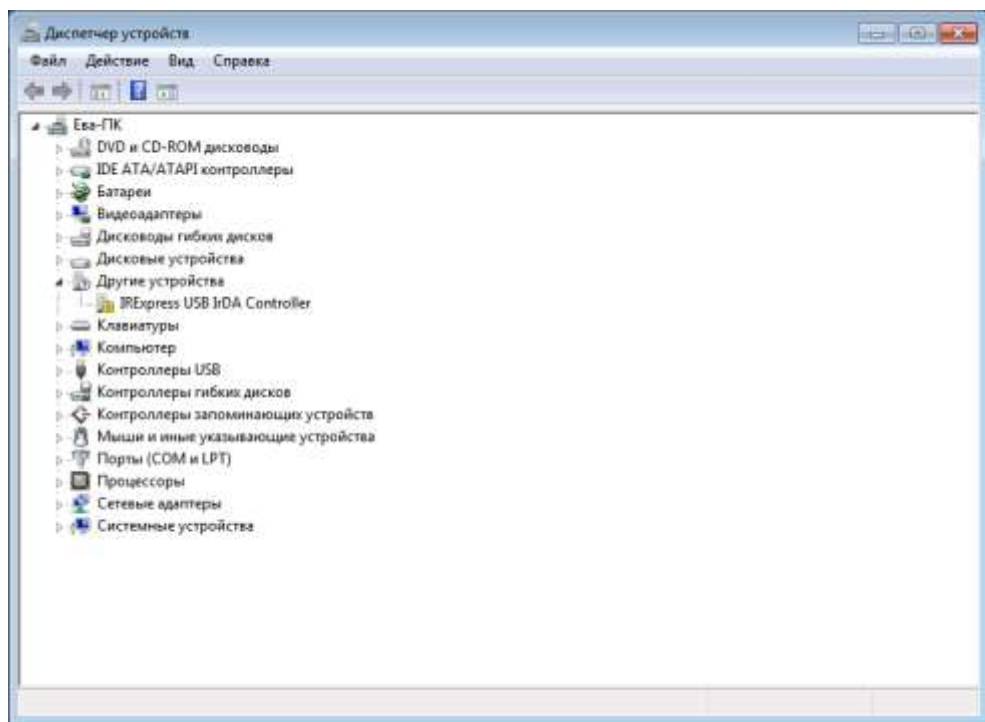


Рис. 6.1. Дерево аппаратных средств, отображаемое Диспетчером устройств (Device Manager)

В главе 5 уже говорилось, что Диспетчер устройств может отображать устройства как по типу, так и по подключению. Используя команду **Вид** (View) в главном меню, выберите наиболее удобный для вас режим отображения и найдите в списке устройство, которое работает некорректно. Это не трудно, поскольку устройства, вызывающие проблему, будут помечены предупреждающими значками. На данном этапе вы можете столкнуться со следующими тремя проблемами:

□ *аппаратное устройство, вызывающее проблему, не присутствует в списке* — если проблемное устройство не показано, это означает, что Windows 7 не может определить проблемы с устройством. Вполне возможно, устройство либо неисправно, либо неправильно подключено. Чтобы попытаться решить эту проблему, выключите компьютер и проверьте, правильно ли подключено проблемное устройство. Исправьте проблему с физической конфигурацией и перезагрузите компьютер. Если устройство исправно и корректно подключено, то после перезагрузки Windows сделает попытку автоматически распознать его и установить для него драйверы. Процесс установки новых устройств был подробно рассмотрен в главе 5;

□ *проблемное устройство помечено треугольным значком с восклицательным знаком в центре:*  — наличие такого значка означает, что Windows сумела распознать устройство, но работает оно некорректно. Чаще всего эта проблема бывает вызвана отсутствием драйверов, некорректно установленным или несовместимым драйвером (рис. 6.2);

чтобы решить эту проблему, выполните щелчок правой кнопкой мыши, наведя курсор на проблемное устройство, из контекстного меню выберите команду **Обновить драйверы** (Update driver) и далее действуйте в соответствии с инструкциями, выводимыми на экран. Если драйвер в системе установлен, но работает некорректно, то, в случае, если проблема была вызвана установкой одного из обновлений, вы сможете выполнить откат этого драйвера. Такой пример будет приведен далее в этой главе;

□ *проблемное устройство помечено значком с изображением направленной вниз стрелки:*  — это означает, что устройство присутствует в системе, но его работа заблокирована (рис. 6.3). Чтобы решить эту проблему, либо нажмите в окне свойств устройства кнопку **Включить** (Enable), либо наведите курсор на проблемное устройство, щелкните правой кнопкой мыши и из контекстного меню выберите команду **Задействовать** (Enable).

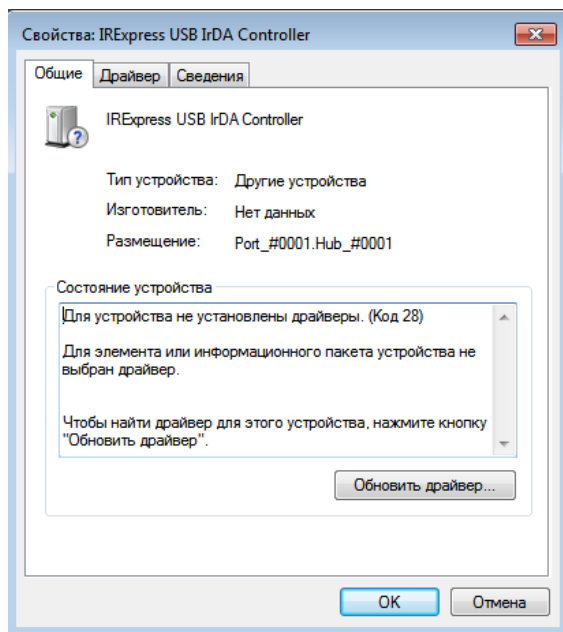


Рис. 6.2. Проблема, вызванная отсутствием драйверов устройства

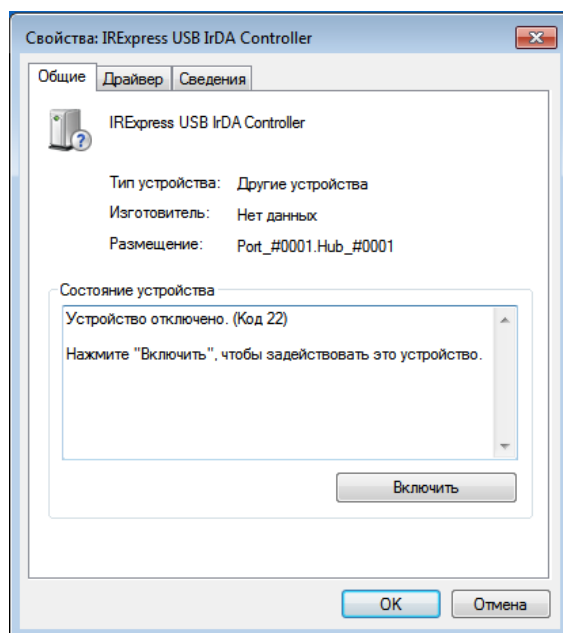


Рис. 6.3. Устройство блокировано

Диагностика проблем с аппаратными средствами с помощью встроенных средств мониторинга

Кроме Диспетчера устройств, в систему встроено множество средств мониторинга, которые могут и должны активно применяться для диагностики проблем с оборудованием. В первую очередь это средство **Отчеты о проблемах и их решениях** (Problem Reports and Solutions), которое, помимо всего прочего, решает и проблемы с установкой драйверов. Чтобы воспользоваться этим средством, раскройте окно Панели управления, и в группе опций **Система и безопасность** (System and Security) выберите ссылку **Поиск и исправление проблем** (Problem reports and solutions). На экране откроется окно, показанное на рис. 6.4.

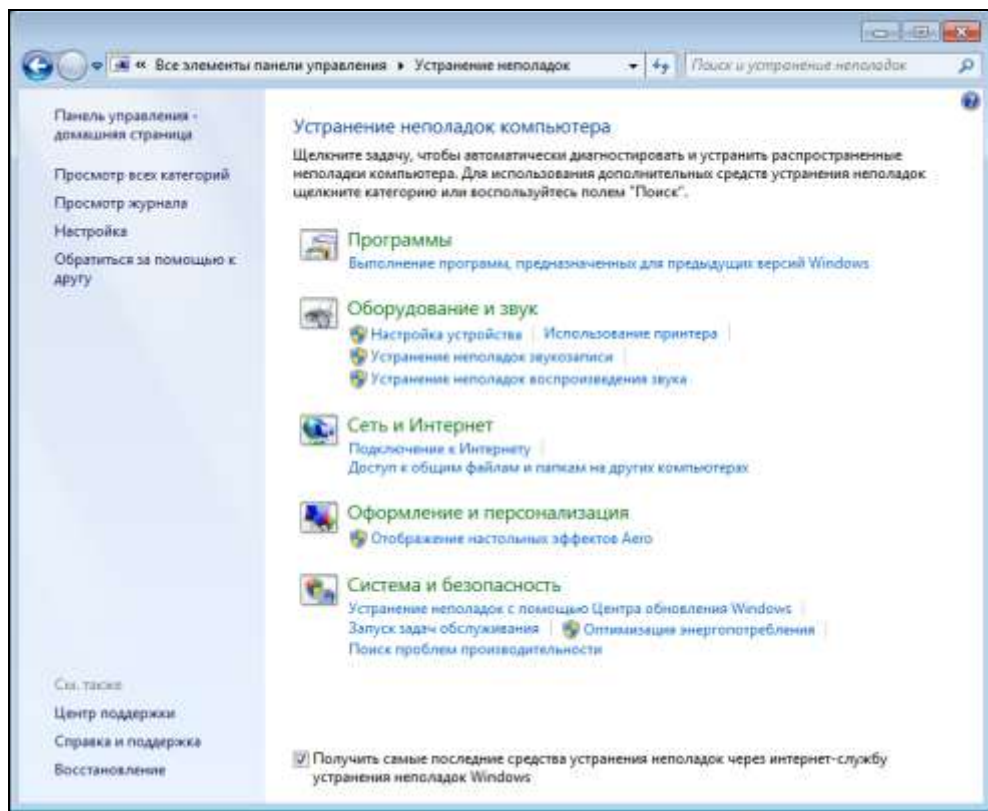


Рис. 6.4. Окно Устранение неполадок компьютера (Troubleshooting computer problems)

В большинстве случаев, если проблема тривиальна, то решение находится почти всегда (рис. 6.5). В данном случае вновь подключенный сетевой адаптер просто еще не настроен. К сожалению, средство **Отчеты о проблемах и их решениях** (Problems Reports and Solutions) предоставляет готовое решение по устранению аппаратных неполадок не всегда. Тем не менее, даже если доступных решений еще нет, отправка отчета о возникшей проблеме повышает шансы на ее исправление в будущем.

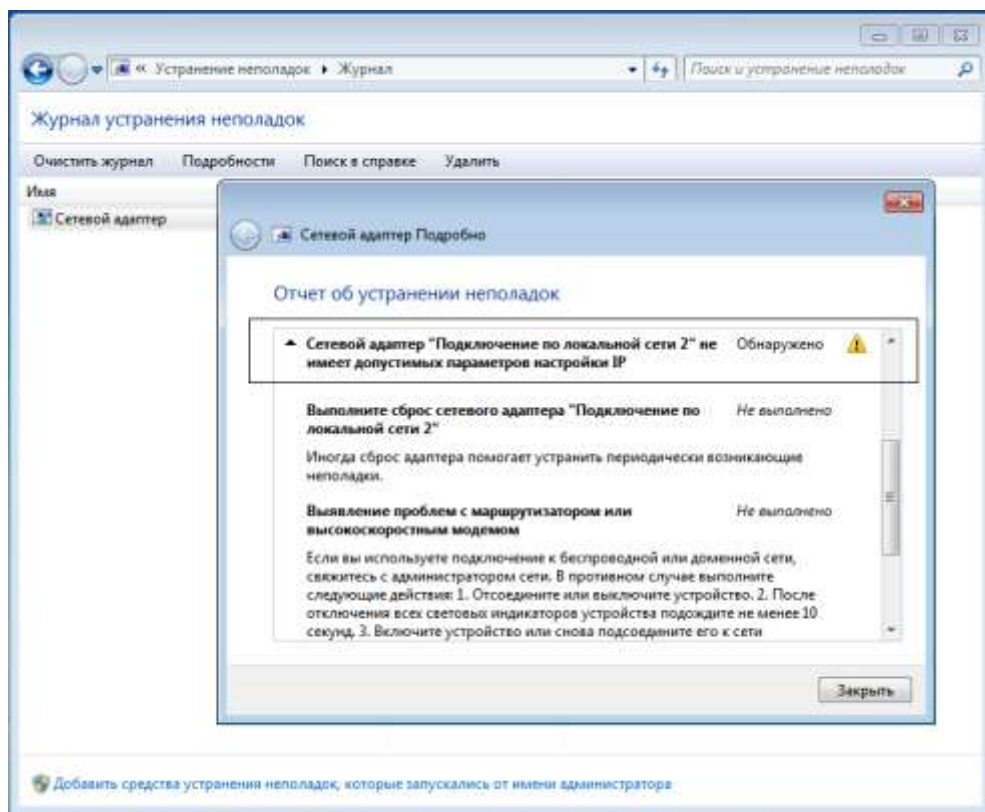


Рис. 6.5. Отчет об устранении неполадок — обратите внимание, что по тривиальным проблемам обычно всегда предлагается решение

Помимо средства **Отчеты о проблемах и их решениях** (Problem Reports and Solutions) серьезную помощь в диагностике аппаратных проблем может оказать и просмотр системного журнала событий, поскольку внесенные в Windows 7 усовершенствования системного мониторинга предоставляют весьма удобные возможности по отслеживанию проблем, вызванных неполадками

аппаратуры. Чтобы воспользоваться этими возможностями, действуйте следующим образом:

1. Запустите оснастку MMC **Просмотр событий** (Event Viewer). Сделать это можно через Панель управления (Control Panel). Для этого откройте окно Панели управления, выберите опцию **Система и безопасность** (System and Security), а затем щелкните по ссылке **Просмотр журналов событий** (View Event Logs) из группы **Администрирование** (Administrative Tools). Как вариант, можно ввести из командной строки команду `eventvwr.msc`. Когда на экране появится окно консоли, откройте папку **Журналы Windows** (Windows Logs).
2. На панели **Действия** (Actions) щелкните мышью по значку **Фильтр текущего журнала** (Filter Current Log) и в раскрывшемся окне **Фильтровать текущий журнал** (Filter Current Log) установите флажки **Критическое** (Critical), **Предупреждение** (Warning) и **Ошибка** (Error). Затем нажмите кнопку **ОК**.
3. Просмотрите информацию обо всех событиях из приведенного списка. Особое внимание обращайте на события, для которых в столбце **Источник** (Source) указан источник, так или иначе связанный с оборудованием. Например, это может быть подсистема ACPI, или Plug and Play Manager, или, например, события от дисковой подсистемы (рис. 6.6).

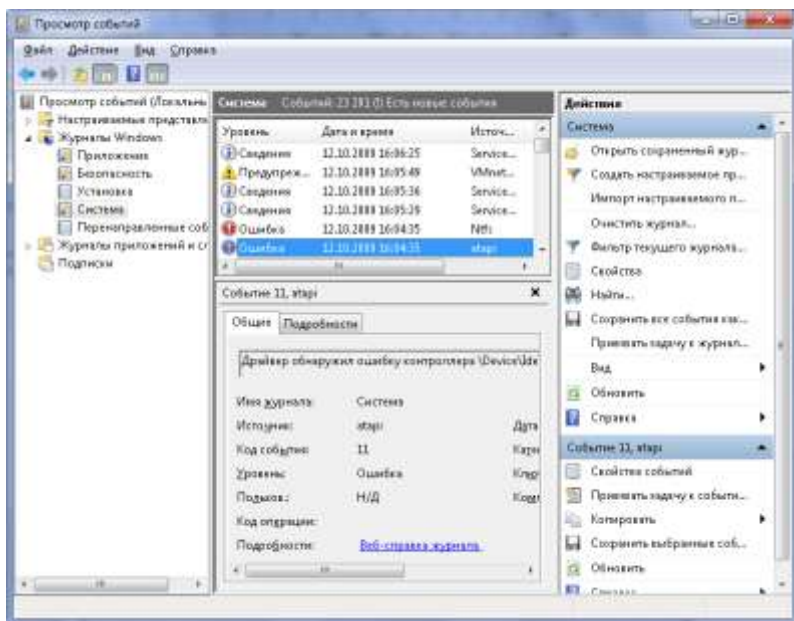


Рис. 6.6. Отслеживание событий, вызванных неполадками с аппаратурой, с помощью системного журнала событий

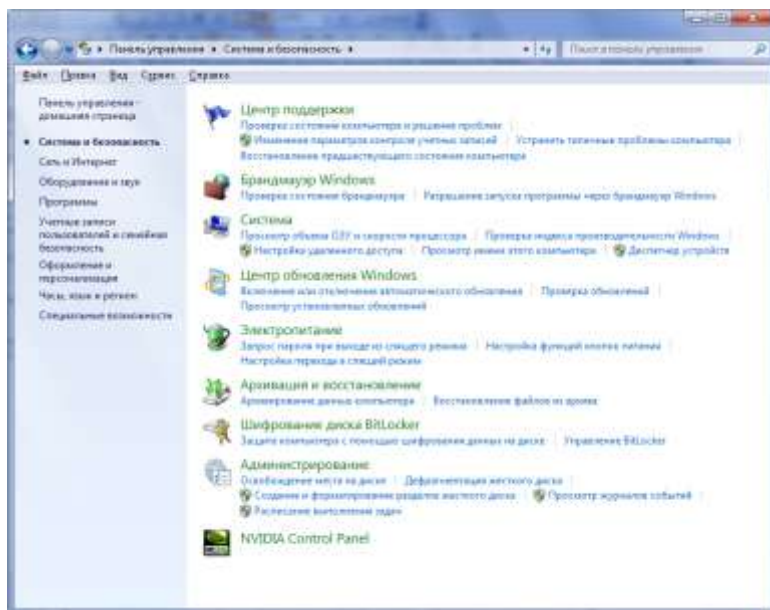


Рис. 6.7. Опции из группы **Система и безопасность** (System and Security) — нас в данном случае интересует группа опций **Центр поддержки** (Action Center)

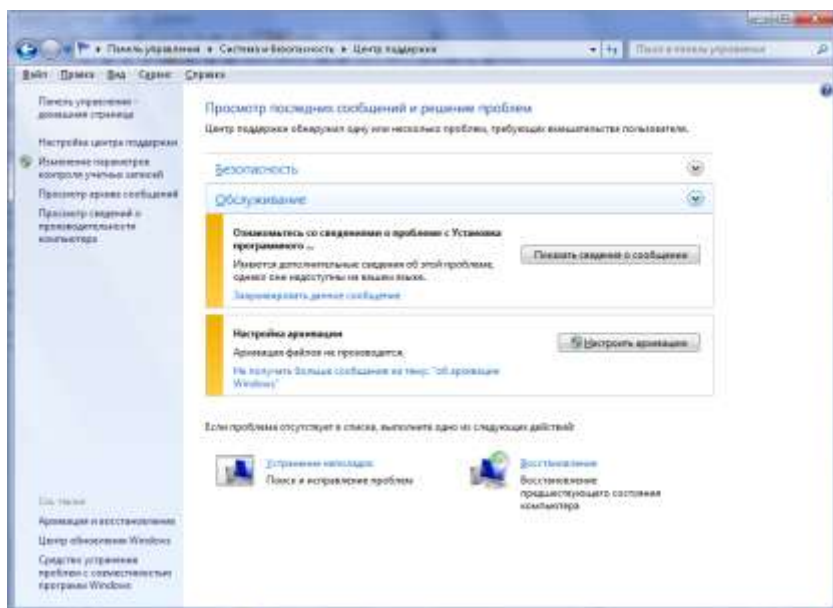


Рис. 6.8. Окно **Центр поддержки** (Action Center) позволяет просмотреть наиболее важные системные сообщения и решить имеющиеся проблемы

Наконец, для диагностики проблем можно использовать и оснастку **Монитор стабильности системы** (Reliability Monitor). По сравнению с Windows Vista, где этот компонент был составной частью оснастки Монитор производительности (Performance Monitor), в Windows 7 процедура запуска этой оснастки изменилась. Действуя через пользовательский интерфейс, запустить ее в Windows 7 можно следующим образом:

1. Раскройте окно **Панель управления** (Control Panel) и щелкните по значку **Система и безопасность** (System and Security). В раскрывшемся окне щелкните по значку **Центр поддержки** (Action Center) (рис. 6.7). Раскроется окно **Просмотр последних сообщений и решение проблем** (Review recent messages and resolve problems), показанное на рис. 6.8.

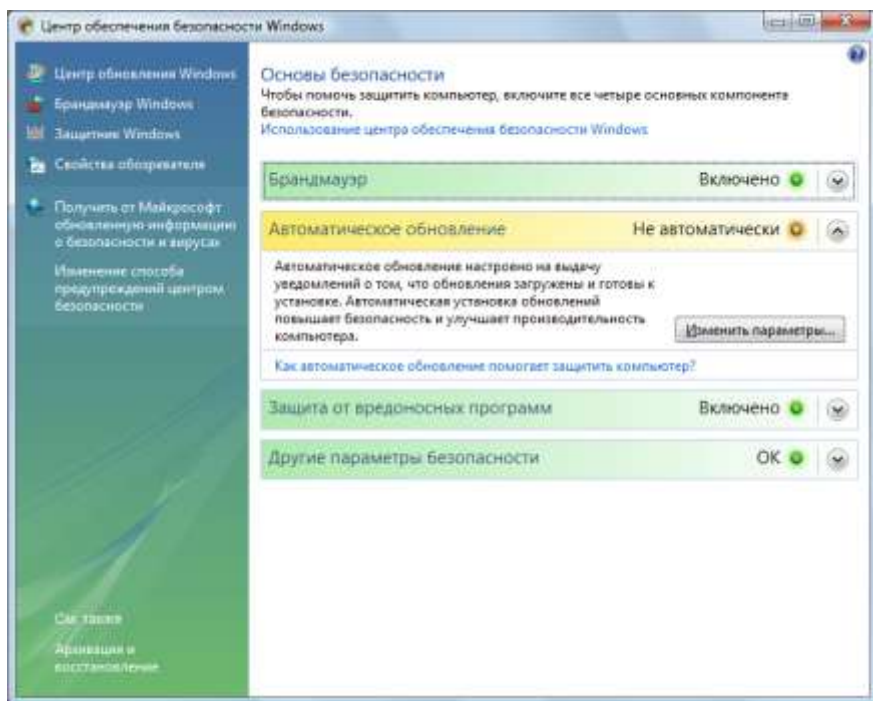


Рис. 6.9. Окно **Центр обеспечения безопасности Windows** в Windows Vista

ПРИМЕЧАНИЕ

Те из вас, кто работал с Windows Vista, наверняка помнят, что там впервые появился так называемый Центр обеспечения безопасности (Windows Security Center), который представлял собой своего рода "центральный пульт управления" всеми вопросами, имеющими отношение к безопасности и решению связанных с ней проблем (рис. 6.9). Так что вы наверняка заметили сходство между

Центром обеспечения безопасности Windows Vista и Центром поддержки (Action Center) в Windows 7. В этом нет ничего удивительного, поскольку Центр обеспечения безопасности Windows, в сущности, и есть непосредственный предшественник Action Center в Windows 7. Связано это с тем, что ряд вопросов Центр обеспечения безопасности не решал, устранение проблем с его помощью представляло собой работу "не для среднестатистического пользователя", и, кроме того, для решения некоторых проблем пользователям приходилось пользоваться другими инструментами Панели управления (Control Panel). Центр поддержки (Action Center) в Windows 7 как раз и призван устранить все перечисленные недостатки. Он является центральной отправной точкой, откуда удобно начинать любые операции по управлению системой, поддержанию ее в работоспособном состоянии и решению возникающих проблем — в том числе и связанных с безопасностью.

2. В раскрывшемся окне **Центр поддержки** (Action Center) (см. рис. 6.8) щелкните мышью по ссылке **Обслуживание** (Maintenance), чтобы развернуть список доступных опций по поддержанию системы в рабочем состоянии и устранению проблем в ее работе (в том числе — и аппаратных). Окно примет такой вид, как показано на рис. 6.10.
3. В раскрывшемся списке выберите опцию **Показать журнал стабильности работы** (View reliability history), как показано на рис. 6.10. Откроется окно диаграммы стабильности системы, показанное на рис. 6.11.

ПРИМЕЧАНИЕ

Если вам показалось, что весь этот алгоритм действий слишком длинен и даже усложнился по сравнению с Windows Vista, не горячитесь. Есть и гораздо более простые методы открыть окно Монитора стабильности системы:

- первый простой метод заключается в том, чтобы нажать кнопку **Пуск** (Start) и начать вводить в поле поиска строку *Reliability* (в английской версии) или **Монитор** (кириллицей в русской версии). Обратите внимание, как быстро начнут появляться результаты поиска! Теперь вам будет достаточно только щелкнуть мышью по опции **Просмотр журнала надежности системы** (View reliability history), как показано на рис. 6.12;
- еще один способ строгого открытия окна Монитора стабильности — через сеанс командной строки. Откройте сеанс командной строки и дайте следующую команду:

```
perfmon /rel
```

Метод запуска Монитора стабильности системы (Reliability Monitor) через командную строку универсален и работает как в Windows Vista, так и в Windows 7.

В диаграмме стабильности системы вы найдете ежедневные отчеты обо всех ошибках, проблемах и важных изменениях в системе. Чтобы выбрать отчет за конкретный день, щелкните соответствующую дату на временной шкале. Монитор стабильности позволяет собрать детальную информацию обо всех событиях, имевших место в системе, в том числе — и вызванные неполадками в работе оборудования.

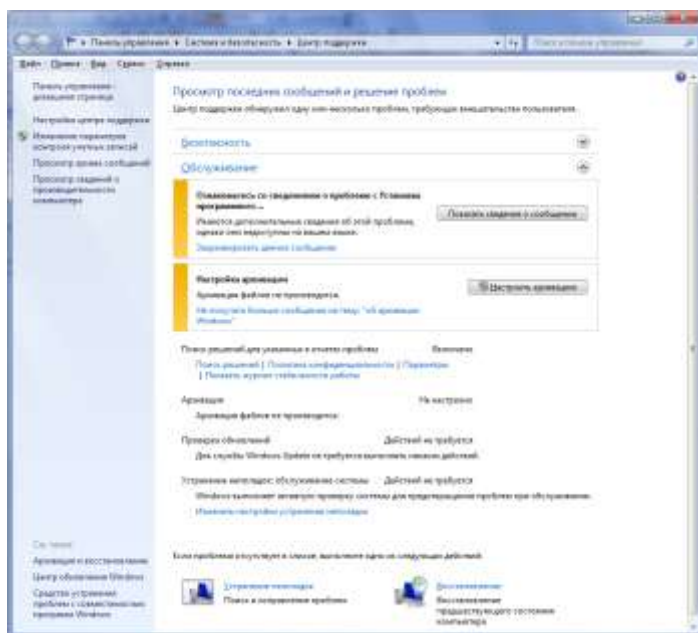


Рис. 6.10. Развернутый список опций по мониторингу и поддержке системы

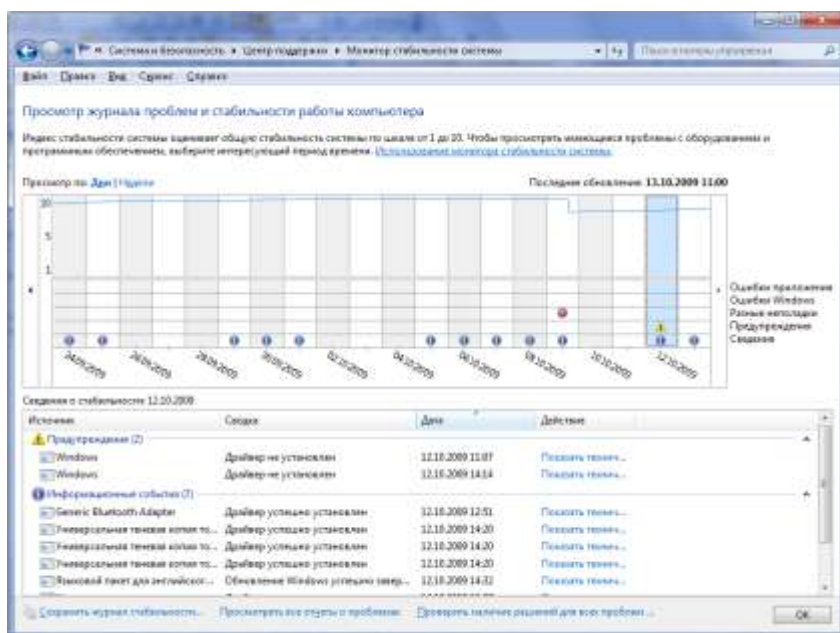


Рис. 6.11. Диаграмма стабильности системы

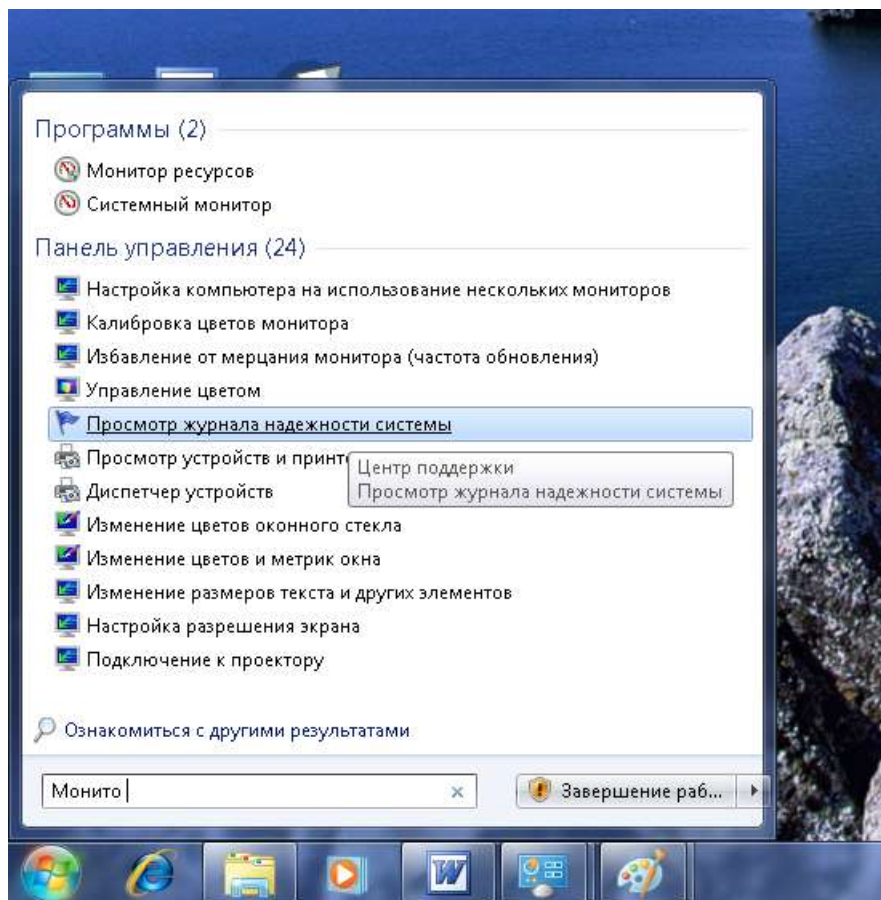


Рис. 6.12. Запуск Монитора стабильности системы (Reliability Monitor) через меню **Пуск** (Start)

С помощью Монитора стабильности вы можете выполнять следующие действия (рис. 6.13):

- ❑ в группе опций **Просмотр по:** (View by) — выбрать режим просмотра диаграммы по дням или по неделям и просмотреть, как с течением времени изменялся индекс стабильности Windows (Windows reliability index);
- ❑ в верхней панели — щелкнув мышью по любому из событий, отображенных на графике, просмотреть в нижней панели детальную информацию о надежности;
- ❑ в нижней панели, **Сведения о стабильности:** (Reliability details), — щелкнув мышью по любой из ссылок в столбце **Действие** (Actions).

Например, щелкнув по ссылке **Показать технические подробности** (View technical details), вы сможете найти более подробную информацию о зарегистрированной проблеме, а щелчок мышью по ссылке **Поиск решения** (Check for a solution) даст возможность проверить, не найдено ли уже готового решения для возникшей критической проблемы;

- в самой нижней части окна имеются три ссылки: **Сохранить журнал стабильности** (Save reliability history), **Просмотреть все отчеты о проблемах** (View all problem reports) и **Проверить наличие решений для всех проблем** (Check for solutions to all problems). С их помощью можно сохранить отчет об ошибках в формате XML для дальнейшего изучения проблемы, просмотреть полный отчет обо всех ошибках и, наконец, выполнить поиск новых решений для возникших проблем.

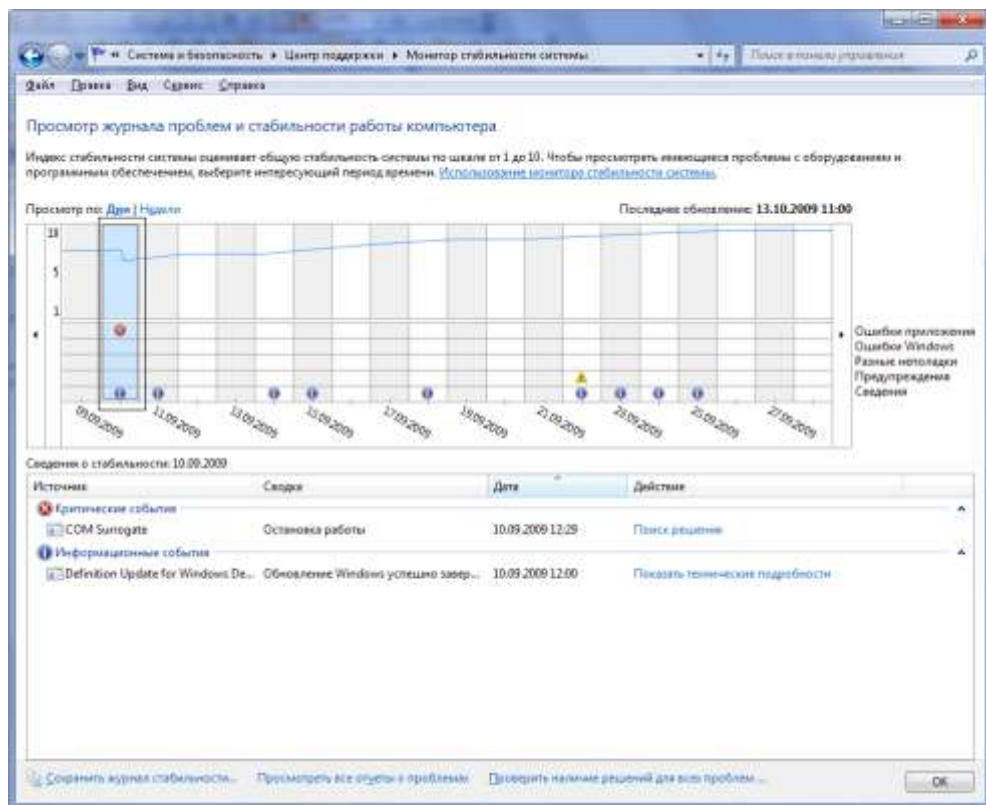


Рис. 6.13. Пример использования Монитора стабильности системы (Reliability Monitor)

Устранение проблем с использованием энергосберегающих режимов

Об энергетических кризисах, экологических проблемах, глобальном потеплении и прочих неприятных явлениях сегодня не слышал только ленивый. Энергосберегающие режимы вводятся и пропагандируются повсеместно — и на уровне всевозможных международных организаций, и в масштабах государств и крупных предприятий, и, конечно, в быту. Не обошла эта не только модная, но и действительно актуальная тема и компьютерную индустрию. Сбережение энергии не только позволяет экономить на оплате счетов, но и реально продлевает срок службы вашего компьютера. Итак, поговорим об энергосберегающих режимах.

Энергосберегающие режимы — о чем речь?

Управление электропитанием (power management) представляет собой интегрированный подход к энергосбережению в масштабах всей системы, т. е. на уровне аппаратных средств и программного обеспечения. Это означает, что компьютерная система, в полном объеме поддерживающая функции управления питанием и энергосбережения, должна включать как аппаратную, так и программную поддержку для следующих функций:

- обеспечения минимальных временных затрат на запуск и останов компьютера — достигается это возможностью перевода системы в "спящий" режим с минимальным потреблением энергии. Из "спящего" режима она может быстро возобновить работу (без необходимости полной перезагрузки);
- обеспечения эффективного и экономного энергопотребления, увеличения срока службы аппаратных устройств — устройства при этом потребляют электроэнергию только в том случае, когда выполняют полезную работу (запросы системы или пользователя). Устройства, которые в течение заданного временного интервала не используются, отключаются, и впоследствии включаются по требованию;
- обеспечения бесшумной работы.

Требования к аппаратным средствам и программному обеспечению по управлению электропитанием и энергосбережению определены спецификацией ACPI. Начиная с Windows Vista, такая поддержка обеспечивается, и как компьютер в целом, так и каждое отдельное его устройство, потребляют только минимально необходимые уровни электроэнергии. Разумеется, это справедливо лишь при условии, что аппаратные средства удовлетворяют требованиям спецификации ACPI. Здесь следует отметить, что управление электропитанием и PnP тесно связаны между собой и взаимозависимы.

В Windows 7 энергосберегающие технологии получили дальнейшее развитие и теперь обеспечивают эффективную работу как процессора, так и остальных компонентов системы. Это позволяет не только снизить энергозатраты, но и продлить "жизнь" компьютеров. Так, например, Windows 7 включает эффективные технологии, способные при определенных обстоятельствах продлить срок службы батареи ноутбуков и нетбуков. Наконец, в ее состав входят новые диагностические средства, которые позволяют производителям (OEM), независимым поставщикам аппаратных средств и программного обеспечения, а также опытным специалистам лучше управлять энергопотреблением компьютеров и устранять неполадки с работой энергосберегающих режимов.

Такой подход к управлению электропитанием и энергосбережению обеспечивает следующие преимущества:

- ☐ интеллектуальное поведение системы в отношении энергосбережения;
- ☐ повышенную надежность и снижение риска потери данных (как вследствие увеличения срока службы аппаратных средств, так и вследствие снижения количества перезагрузок);
- ☐ более высокий уровень взаимодействия устройств.

При помощи утилиты **Электропитание** (Power Options) из Панели управления (Control Panel) можно снизить потребление энергии любым количеством устройств компьютера. Однако надо понимать — чтобы использовать эти функции, необходимо иметь компьютер, удовлетворяющий спецификации ACPI. ACPI представляет собой открытый промышленный стандарт (для свободного скачивания доступен на <http://www.acpi.info/spec.htm>).

Основные сведения о спецификации ACPI

В наследуемых аппаратных устройствах и операционных системах управление конфигурацией устройств и их энергопотреблением осуществлялось через BIOS. Однако с течением времени политики управления энергопотреблением существенно усложнились, а код вырос в объеме настолько, что его реализация в ROM BIOS стала проблематичной. По этой причине и возникла необходимость передать эти функции операционной системе. Одна из основных целей разработки спецификации ACPI как раз и состояла в выработке стандартных интерфейсов, позволяющих операционной системе выполнять эти функции как для отдельных устройств, так и в масштабах всей системы. ACPI представляет собой ключевой элемент стандарта управления энергопотреблением под руководством операционной системы (Operating System-directed configuration and Power Management, OSPM). ACPI обеспечивает воз-

возможность удобного перехода от существующего (наследуемого) оборудования к оборудованию, полностью поддерживающему стандарт ACPI, а также позволяет механизмам ACPI и наследуемым механизмам управления энергопотреблением сосуществовать в пределах одной компьютерной системы. Уровни поддержки ACPI различными типами устройств в различных операционных системах иллюстрируются данными табл. 6.1.

Таблица 6.1. Поддержка различных типов оборудования в зависимости от типа операционной системы

Аппаратные средства	Операционная система	
	Наследуемая (Legacy) ОС	ACPI ОС с поддержкой OSPM
Наследуемые аппаратные средства	Наследуемые ОС на наследуемой аппаратной платформе ведут себя как обычно	Если ACPI ОС не поддерживает наследуемое оборудование, то вся поддержка таких устройств осуществляется на аппаратном уровне
Комбинация наследуемого оборудования и устройств с поддержкой ACPI	ОС ведет себя аналогично наследуемой ОС на наследуемом оборудовании	В процессе загрузки ОС переключает оборудование из наследуемого режима в режим OSPM/ACPI, и с этого момента система обеспечивает поддержку OSPM/ACPI
Только оборудование ACPI	Наследуемая ОС не обеспечивает функций по управлению энергопотреблением	Все функции по управлению энергопотреблением осуществляются операционной системой (полная поддержка OSPM/ACPI)

ПРИМЕЧАНИЕ

Модель управления энергопотреблением под руководством операционной системы (OSPM) предоставляет потребителям новые возможности. В частности, некоторые новые компьютеры оснащены так называемой кнопкой **Sleep**, нажатие на которую позволяет перевести компьютер в спящий режим без его физического отключения. Спецификация ACPI допускает два метода реализации этой возможности: первый — для перевода компьютера в спящий режим, и второй — для его программного отключения (OFF). Производители аппаратных средств могут реализовать эту возможность двумя путями, известными как *однокнопочная* и *двухкнопочная* модели. При использовании *однокнопочной* модели традиционная кнопка **Power** в зависимости от заданных пользователем параметров политики поведения кнопок может использоваться как для выключения компьютера, так и для его перевода в спящий режим. При использовании *двухкнопочной* модели на компьютере имеется отдельная кнопка **Sleep** для его перевода в спящий режим и отдельная кнопка **Power** для его отключения. Более подробно об этом будет рассказано далее в этой главе.

Спецификация ACPI определяет аппаратные интерфейсы ACPI, программные интерфейсы ACPI и структуры данных ACPI. Система ACPI как таковая состоит из следующих компонентов:

- таблицы описания системы ACPI — описывают интерфейсы с аппаратными средствами. Большинство этих описаний дает производителям возможность выбора путей реализации аппаратных средств и задания последовательности операций, которые необходимо выполнить для обеспечения работоспособности устройства.

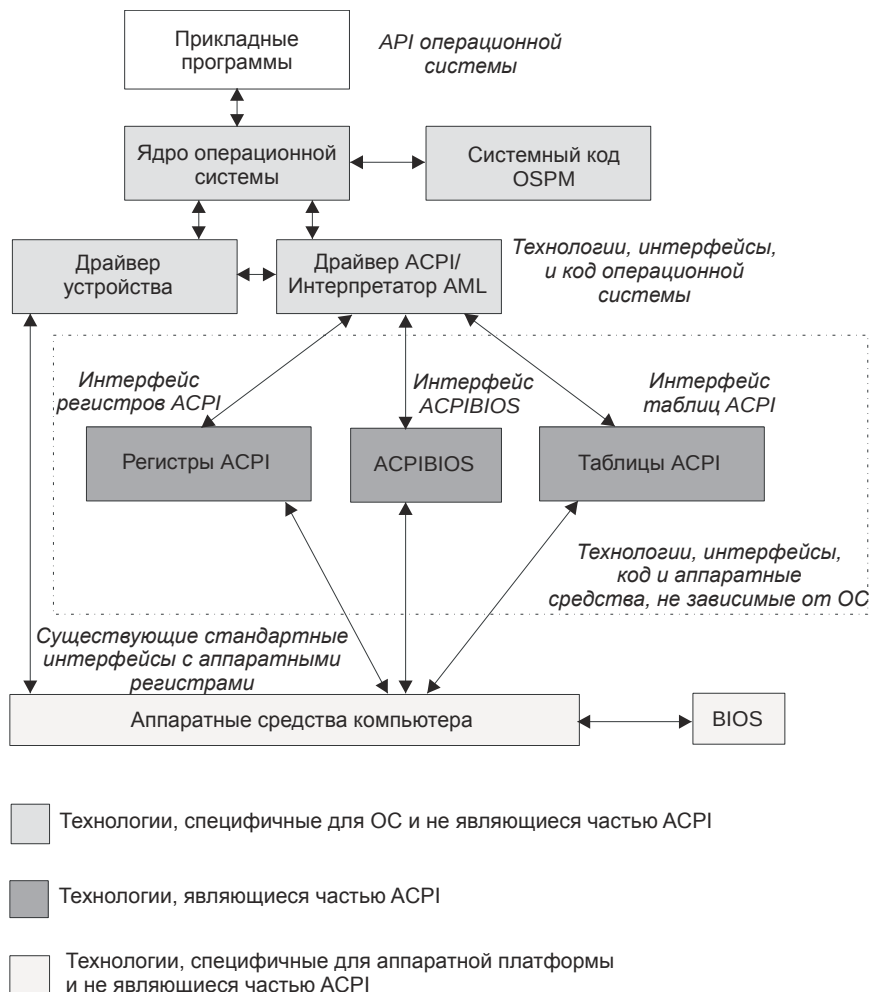


Рис. 6.14. Глобальная структура системы OSPM/ACPI

Таблицы ACPI содержат так называемые *блоки определений* (Definition Blocks), использующие собственный язык ACPI Machine Language (AML), интерпретация которого осуществляется операционной системой. Таким образом, ACPI ОС с поддержкой OSPM содержит встроенный интерпретатор, выполняющий процедуры, закодированные на языке AML в блоках определений таблиц ACPI;

- ❑ регистры ACPI — элементы управления, встроенные в фиксированные блоки регистров. Таблицы ACPI указывают адреса этих блоков;
- ❑ системное микропрограммное обеспечение ACPI — часть микропрограммного обеспечения (firmware), совместимая со спецификацией ACPI. Как правило, этот код загружает компьютер (в точности так, как это осуществляли наследуемые BIOS) и реализует интерфейсы для перевода компьютера из одного режима энергопотребления в другой (операции sleep, wake, restart и т. д.).

Глобальная структура системы OSPM/ACPI со всеми программными и аппаратными компонентами и интерфейсами и их взаимоотношениями показана на рис. 6.14. Как можно видеть, ACPI не является ни чисто программной, ни чисто аппаратной спецификацией. Она описывает как программные, так и аппаратные компоненты.

Настройка планов энергопотребления системы

По сравнению с Windows XP, в Windows Vista механизм управления электропитанием и энергосберегающими режимами был существенно доработан и улучшен, а в Windows 7 появились и дополнительные усовершенствования. Перечислим наиболее важные из них:

- ❑ более удобный пользовательский интерфейс, по умолчанию предоставляющий три плана управления энергосберегающими режимами¹. Пользовательский интерфейс теперь включает удобные возможности управления приложениями, блокирующими останов системы (shutdown), — это характерно и для Windows Vista, и для Windows 7;
- ❑ ограничения возможности приложений влиять на переход в энергосберегающие режимы. Как уже упоминалось ранее в этой главе, улучшенная

¹ В более ранних версиях Windows планы управления энергосберегающими режимами (power plans) назывались схемами управления питанием (power schemes). Фактически, эти термины означают одно и то же понятие, поэтому здесь и далее будем употреблять более привычный термин "схема".

поддержка режимов *сна* (sleep) и *гибернации* (hybernation) актуальна для мобильных пользователей;

- ❑ в Windows 7 появилась новая функция — так называемое *слияние таймеров* (Timer Coalescing). Эта функция позволяет Windows 7 объединять различные задачи, работающие в фоновом режиме, и выполнять их одновременно, чтобы меньше загружать процессор и дать ему возможность работать в холостом режиме в течение более длительных периодов времени. Кроме того, Windows 7 может отложить выполнение некритичных фоновых задач, если ноутбук питается не от сети, а от батареи, что может серьезно продлить срок службы батареи;
- ❑ системные службы часто стартуют автоматически, работают в фоновом режиме и ожидают, когда произойдет то или иное системное событие. Как правило, такие события происходят нечасто. Поэтому в Windows 7 появилось такое нововведение, как *триггерный запуск сервисов* (trigger-starting system services). Суть этого нововведения заключается в том, что подобные сервисы не стартуют при запуске системы, а запускаются тогда и только тогда, когда происходит конкретное событие. Имеется в виду, что только подключение устройства или, скажем, смена IP-адреса могут послужить причиной запуска сервисов, призванных обслуживать такие события. Например, в Windows 7 сервис Windows Bluetooth стартует только тогда, когда к компьютеру подключается устройство Bluetooth;
- ❑ внесены улучшения в управление энергопотреблением различных устройств — в том числе, реализованы такие функции, как адаптивное управление яркостью дисплея (Adaptive Display Brightness), интеллектуальное управление энергопотреблением сетевых устройств (Smart Network Power);
- ❑ организовано управление параметрами электропитания через групповые политики. Windows 7 обеспечивает возможности более тонкой настройки энергопотребления, чем любая из ее предшественниц. Все нововведения, включая адаптивное управление яркостью дисплея (Adaptive Display Brightness), управление уровнем сигнала для перехода в режим резервной батареи (Reserve Battery Notification Level) и разрешение автоматического перехода в спящий режим с открытыми сетевыми файлами (Allowing Automatic Sleep with Open Network Files), нашли свое отражение в системных политиках (которые, как мы уже хорошо знаем, модифицируют системный реестр).

Управление параметрами энергопотребления в Windows 7, как и в Windows Vista, основано на планах электропитания (power plans). План электропитания представляет собой наборы параметров аппаратных средств и системных настроек, используемых для управления режимами энергопотребления ком-

пьютера. Как уже говорилось, в Windows Vista и Windows 7 по умолчанию предоставляются три стандартных плана (рис. 6.15):

- ❑ **Сбалансированный (Balanced)** — при использовании этого плана компьютер работает с максимально возможной производительностью (и соответственно с максимально высоким энергопотреблением) в течение периодов, когда это необходимо пользователю. В то же время компьютер переходит в энергосберегающие режимы по истечении периодов отсутствия пользовательской активности;
- ❑ **Экономия энергии (Power saver)** — при использовании этого плана компьютер работает в энергосберегающем режиме за счет снижения общей производительности системы. Данный режим актуален для пользователей мобильных компьютеров, работающих от аккумулятора;
- ❑ **Высокая производительность (High performance)** — при использовании этого плана производительность и энергопотребление компьютера максимальны. Не рекомендуется пользователям мобильных компьютеров.

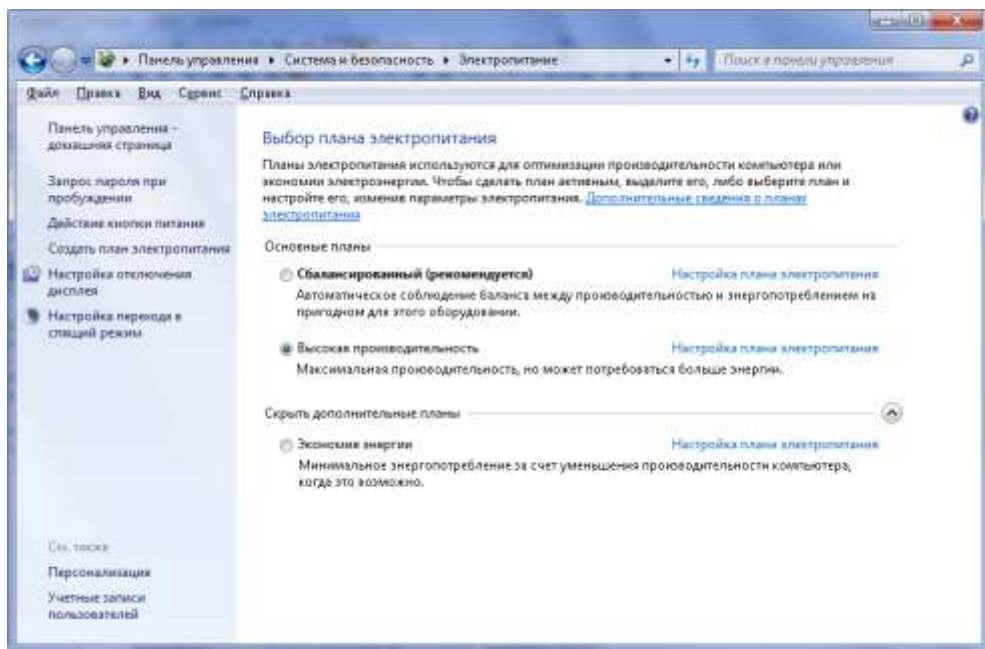


Рис. 6.15. Выбор плана электропитания

Вы можете изменить настройки для каждого из этих планов или создать собственные планы. Откровенно говоря, именно это и рекомендуется сделать,

поскольку ни один из планов, предлагаемых по умолчанию, не является универсальным и подходящим для любой системы.

Чтобы настроить параметры энергосбережения в соответствии с индивидуальными потребностями, сделайте следующее:

1. Откройте окно **Панель управления (Control Panel)** и запустите утилиту **Электропитание (Power Options)**. Щелкните ссылку **Создать план электропитания (Create a power plan)**. В следующем окне (рис. 6.16) вы сможете присвоить новому плану имя или оставить без изменения имя, предложенное по умолчанию. Для перехода к следующему окну нажмите кнопку **Далее (Next)**.

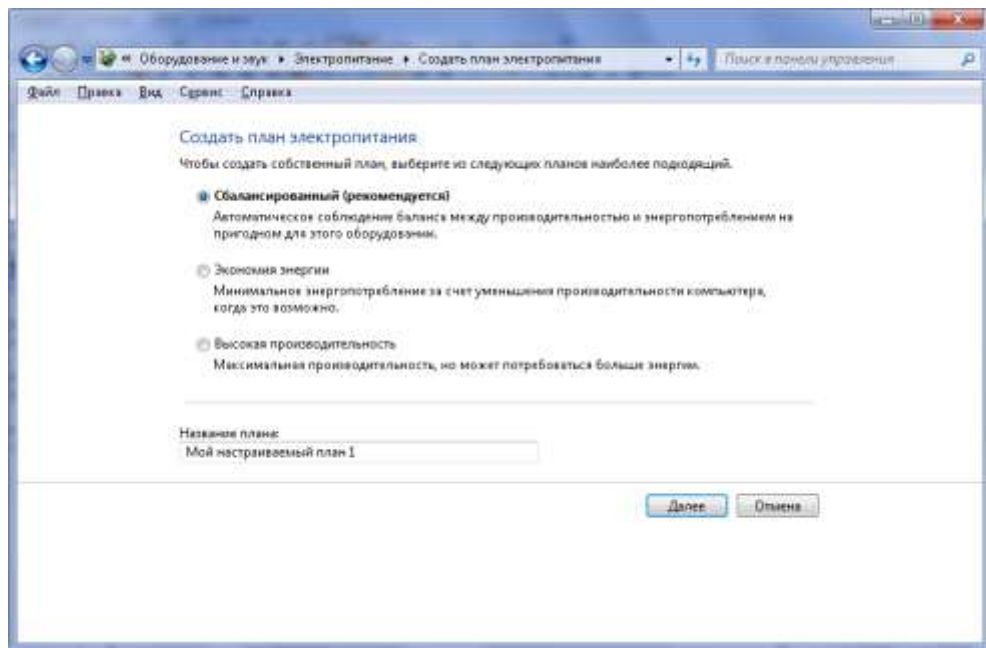


Рис. 6.16. В этом окне вы можете создать новый план электропитания на основе одного из существующих и присвоить ему имя

2. В следующем окне (рис. 6.17) вам будет предложено выбрать параметры спящего режима (sleep mode) и параметры отключения дисплея. Здесь следует заметить, что для большинства настольных компьютеров обычно рекомендуется отключать дисплей примерно через 15–20 минут отсутствия пользовательской активности.

СОВЕТ

Опция **Переводить компьютер в спящий режим** (Put the computer to sleep) предназначена, в основном, для ноутбуков. Для настольных компьютеров лично я рекомендую установить для этой опции существенно более длительный интервал, чем значение 30 минут, предложенное по умолчанию. По личным впечатлениям — при "пробуждении" (выходе из спящего режима) компьютер ведет себя точно так же, как невыспавшийся человек, которого зачем-то будят и заставляют работать. К тому же, все изменения, сделанные в открытых файлах, перед переходом в спящий режим хранятся в памяти, но не записываются на диск. Поэтому, если за время "сна" произойдет сбой питания, все несохраненные данные будут потеряны. С другой стороны, если ваш компьютер почти никогда не выключается, то не рекомендуется устанавливать и значение **Никогда** (Never) — если вы ушли и оставили компьютер включенным, то не слишком благоразумно отказываться от энергосбережения. Исключение составляют только те случаи, когда вы занимаетесь, например, захватом и оцифровкой видео с последующим прожигом DVD. Здесь следует иметь в виду, что все эти процессы происходят в режиме реального времени, а значит — сопряжены с существенными временными затратами. Чтобы все процессы завершились без ошибок, спящий режим желательно отключить.

Установив нужные опции, нажмите кнопку **Создать** (Create).

- Ваш индивидуальный план появится в списке (рис. 6.18). Для дальнейшей настройки параметров щелкните ссылку **Настройка плана электропитания** (Change plan settings). В следующем окне щелкните ссылку **Изменить дополнительные параметры питания** (Change advanced power settings), и на экране появится окно **Электропитание** (Power Options), открытое на вкладке **Дополнительные параметры** (Advanced Settings), в котором и производятся основные манипуляции по настройке параметров электропитания (рис. 6.19).

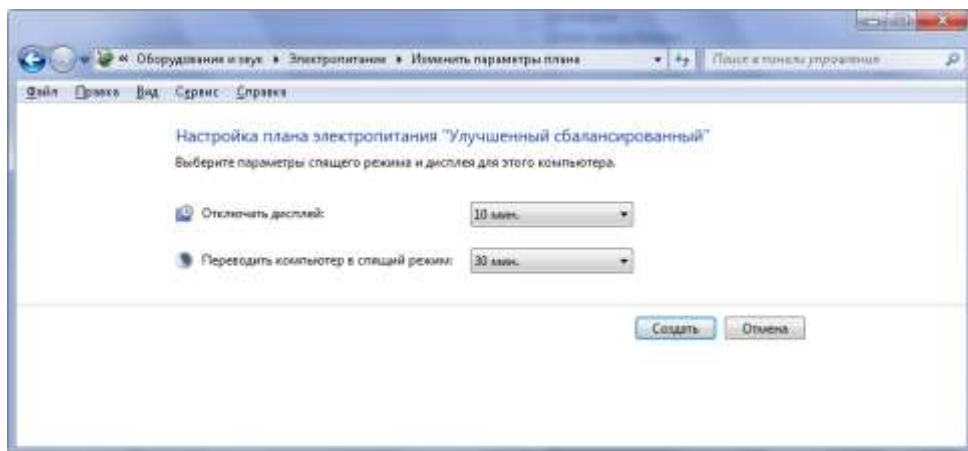


Рис. 6.17. Изменение параметров индивидуального плана электропитания

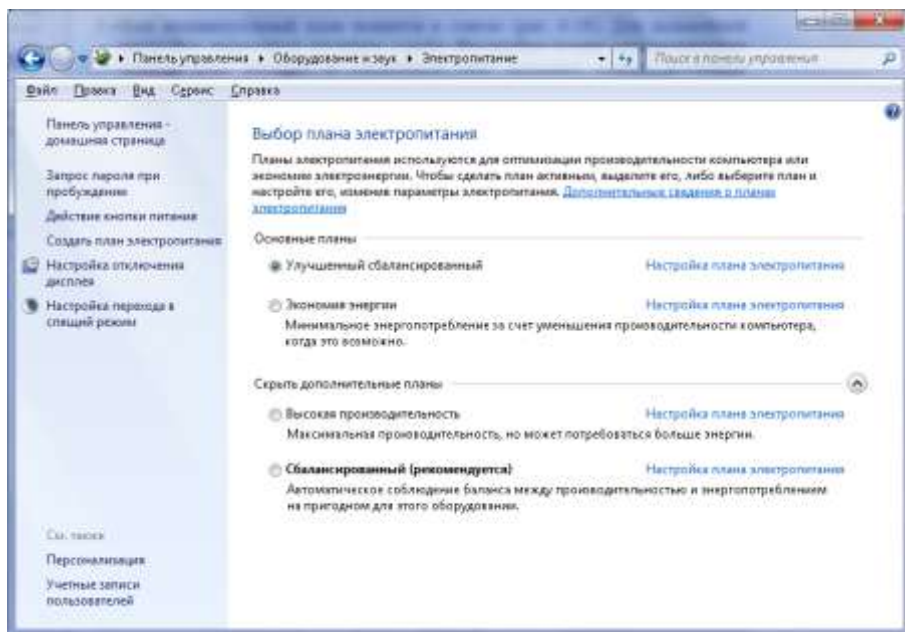


Рис. 6.18. Новый настраиваемый план электропитания появился в списке

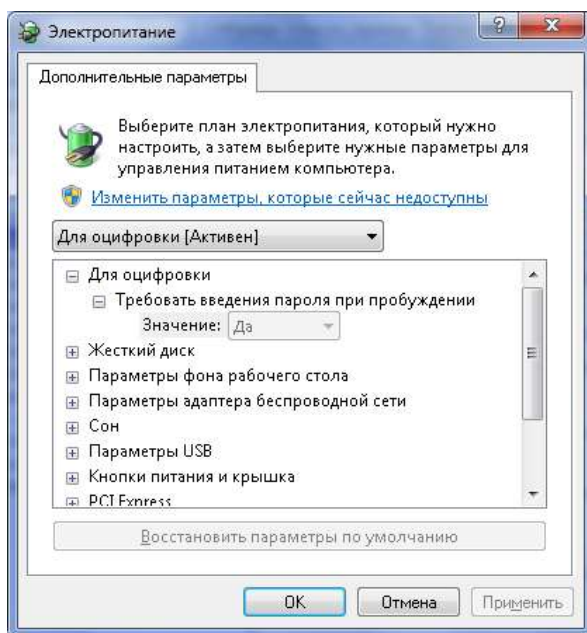


Рис. 6.19. Вкладка Дополнительные параметры окна Электропитание

4. Чтобы раскрыть список возможных опций для каждого из перечисленных в окне параметров, щелкните мышью на значке плюса слева от названия параметра. Обратите внимание, что если вы обнаруживаете параметр, который не поддается изменению, следует щелкнуть ссылку **Изменить параметры, которые сейчас недоступны** (Change settings that are currently unavailable) и повторить попытку.
5. Настройте параметры энергопотребления в соответствии с вашими потребностями. Рассмотрим наиболее актуальные параметры настройки типичного настольного компьютера (для ноутбуков вполне подойдет стандартный план **Экономия энергии**):
 - **Дополнительные параметры** (Additional settings) | **Требовать введения пароля при пробуждении** (Require a password on wakeup) — если этот параметр установлен, то для выхода из спящего режима потребуются ввести пароль той пользовательской учетной записи, от имени которой вы были зарегистрированы в системе перед переходом в спящий режим (рис. 6.20);

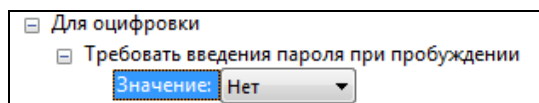


Рис. 6.20. Опции группы **Дополнительные параметры**

- **Жесткий диск** (Hard Disk) | **Отключать жесткий диск через** (Turn off hard disk after) — задайте временной интервал (в минутах), после которого ваш жесткий диск будет отключаться при отсутствии пользовательской активности (рис. 6.21). Рекомендуется установить довольно большое значение, а не 20 минут, потому что частые включения и отключения влияют на диск отрицательно;

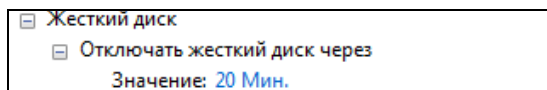


Рис. 6.21. Опции группы **Жесткий диск**

- **Параметры фона рабочего стола** (Desktop background parameters) — укажите, хотите ли вы, чтобы во время вашего отсутствия рабочий стол работал в режиме слайд-шоу (новая возможность Windows 7, при кото-

рой фон рабочего стола меняется через заданный временной интервал). На ваше усмотрение, но я бы отключила (рис. 6.22);

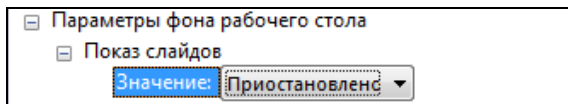


Рис. 6.22. Опции группы Параметры фона рабочего стола

- **Параметры адаптера беспроводной связи (Wireless Adapter Settings) | Режим энергосбережения (Power Saving Mode)** — если в вашей системе имеются адаптеры беспроводной связи, выберите для них один из желаемых режимов (рис. 6.23);

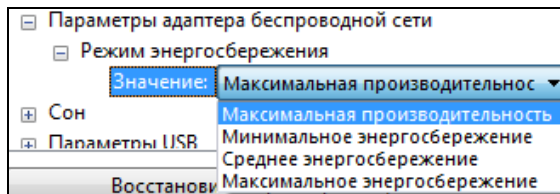
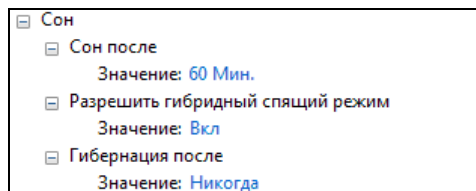
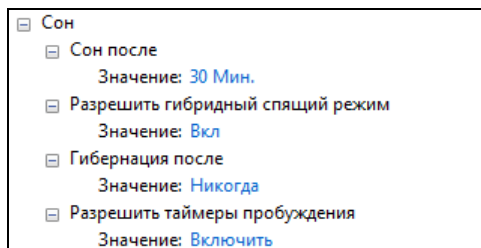


Рис. 6.23. Опции группы Параметры адаптера беспроводной связи

- **Сон (Sleep) | Переход в спящий режим через (Sleep After)** — задайте временной интервал (в минутах), по истечении которого компьютер должен переходить в спящий режим при отсутствии пользовательской активности (рис. 6.24);



а



б

Рис. 6.24. Опции группы Сон: а — Windows Vista; б — Windows 7.
Обратите внимание на новую опцию **Разрешить таймеры пробуждения** (Allow wake-up timers), появившуюся в Windows 7

ПРИМЕЧАНИЕ

Как уже отмечалось, спящий режим хорош только для ноутбуков. Если вы используете этот режим, для подстраховки не забывайте сохранять все несохраненные данные перед тем, как отлучиться с рабочего места. Обратите внимание на новую опцию, впервые появившуюся в Windows Vista — гибридный спящий режим. Предшествующие версии Windows имели энергосберегающую опцию **Ждущий режим** (standby). Однако как переход в это состояние, так и выход из него были медленными и не слишком надежными. Режим сна в Windows Vista решает данную проблему, но делает это исключительно за счет сериализации текущего состояния компьютера в памяти и остановки всех устройств, кроме RAM. Да, переход в спящий режим и выход из него ускорились. Но отрицательной стороной спящего режима остается его ненадежность: если произойдет сбой в подаче электропитания, пока компьютер находится в спящем режиме, то все данные будут потеряны. Эта проблема решается за счет введения так называемого *гибридного спящего режима* (hybrid sleep mode). В гибридном спящем режиме состояние системы сохраняется в памяти, и наряду с этим записывается на диск (примерно так же, как и в случае режима гибернации). Это позволяет избежать потери данных в случае сбоя подачи питания. На первый взгляд, идея кажется хорошей, но на практике переход в гибридный спящий режим оказывается ничуть не быстрее, чем переход в ждущий режим в предшествующих версиях Windows. С учетом того, что большинство современных ноутбуков конфигурируется для перехода в режим гибернации при падении уровня заряда батареи ниже определенного уровня (а это означает, что сбой подачи питания произойдет лишь при физическом удалении батареи), гибридный спящий режим не слишком полезен даже для мобильных пользователей. Что касается настольных систем, то для них рекомендуется блокировать все три опции этой группы.

Наконец, в Windows 7 появилась и еще одна опция конфигурирования спящего режима — **Разрешить таймеры пробуждения** (Allow wake-up timers). Если эта опция установлена, то компьютер будет в ваше отсутствие принудительно выводиться из спящего режима при необходимости выполнения одной из запланированных операций (например, таких, как регулярная проверка обновлений Windows или антивирусных баз, запланированных на определенное время).

- **Параметры USB (USB) | Параметр временного отключения USB-порта** (USB selective suspend), временное отключение порта USB — на настольных компьютерах этот параметр однозначно следует блокировать (рис. 6.25);

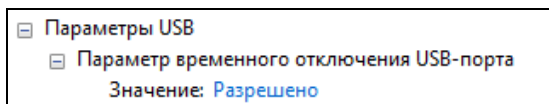


Рис. 6.25. Опции группы Параметры USB

- **Кнопки питания и крышка** (Power buttons and lid) — опции этой группы задают действие, по умолчанию выполняемое при нажатии

кнопки питания **Power** на корпусе компьютера (рис. 6.26). Настоятельно рекомендуется не менять значение по умолчанию (**Завершение работы**). Как уже говорилось, на некоторых компьютерах, соответствующих спецификации ACPI 3.0, есть не только кнопка питания, но и кнопка сна (**Sleep**). В этом случае в данной группе опций будет аналогичная опция, задающая действие этой кнопки — для нее рекомендуется задать значение **Действие не требуется** (Do nothing). Наконец, в этой группе есть и опция **Кнопка питания меню Пуск** (Start menu power button). Это действительно удобная новая опция, для которой рекомендуется задать значение **Завершение работы** (Shut Down);

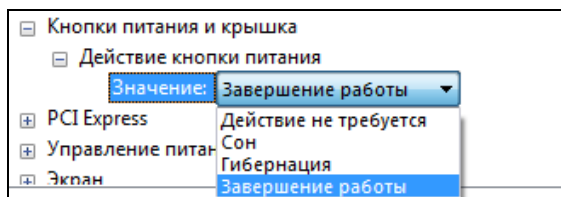


Рис. 6.26. Опции группы **Кнопки питания и крышка**

- **Экран (Display) | Отключать экран через** (Turn off display after) — задайте опцию отключения экрана по истечении интервала времени, в течение которого не будет никакой пользовательской активности. Вполне разумно задать значение примерно 20 минут. Обратите внимание на новую опцию **Адаптивное отключение экрана** (Adaptive display) — эта удобная опция позволяет системе отслеживать интервалы времени, по истечении которых вы вновь активизируете дисплей после его перевода в отключенное состояние. Если система обнаружит, что это происходит вскоре после отключения, то интервал, заданный опцией **Отключать экран через**, будет автоматически увеличен. Очень удобно, поэтому данную опцию рекомендуется активизировать (рис. 6.27).

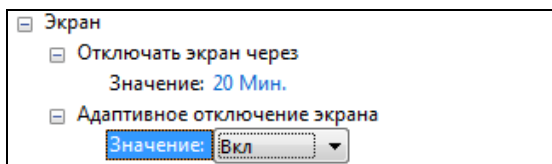


Рис. 6.27. Опции группы **Экран**

На вкладке **Дополнительные параметры** (Advanced Settings) окна **Электропитание** (Power Options) вы найдете и другие опции, помимо перечисленных. Для этих опций можно оставить значения по умолчанию.

Редактирование планов электропитания с помощью групповых политик

Начиная с Windows Vista появилась столь долго ожидаемая крупными корпоративными заказчиками возможность управления параметрами энергосберегающих режимов через групповую политику (Group Policy). Разумеется, существуют и продукты сторонних разработчиков, позволяющие принудительно устанавливать такие настройки, но это сопряжено с дополнительными расходами.

ПРИМЕЧАНИЕ

Групповая политика поддерживалась в Windows XP Professional, но не в Windows XP Home Edition. Аналогичным образом групповая политика поддерживается в Windows Vista Business, Enterprise и Ultimate editions, но не поддерживается в Windows Vista Home Basic и Home Premium. Эта же схема доступности групповой политики сохранилась и в Windows 7.

В Windows 7 количество опций групповой политики увеличилось по сравнению с Windows Vista, а возможности настройки энергосберегающих режимов с их помощью стали более гибкими.

Чтобы принудительно в административном порядке задать параметры управления электропитанием, сделайте следующее:

1. Запустите сеанс командной строки с административными правами и дайте команду `gpedit.msc`.
2. В левой панели найдите узел **Управление электропитанием** (Power Options). Он находится по следующему адресу: **Политика Локальный компьютер | Конфигурация компьютера | Административные шаблоны | Система | Управление электропитанием** (Local computer policy | Computer configuration | System | Power options). Здесь вы увидите несколько вложенных папок, которые позволяют принудительным образом задать политики для всех параметров управления электропитанием (рис. 6.28).
3. Обратите внимание, что параметры управления электропитанием, установленные через групповую политику, имеют приоритет перед параметрами, заданными пользователем через соответствующий апплет Панели управления (рис. 6.29).

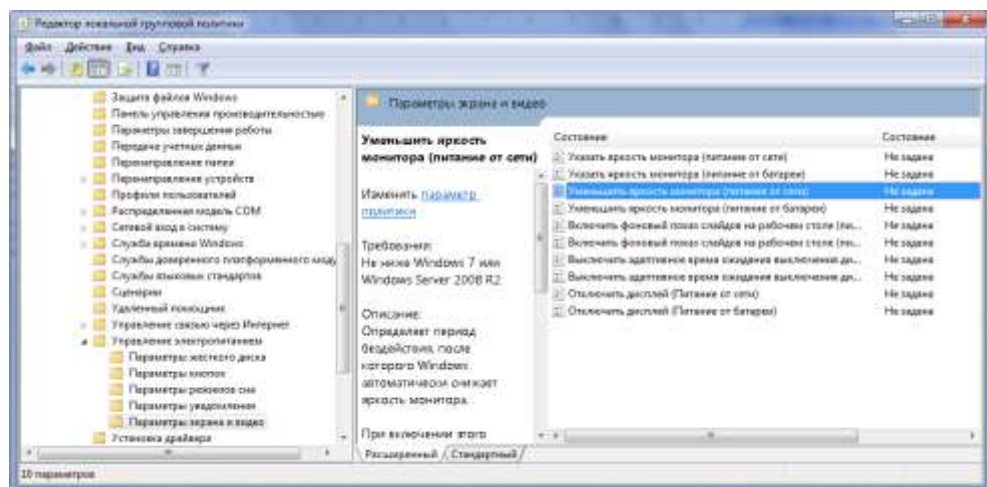


Рис. 6.28. Windows 7 предоставляет администраторам возможности принудительной установки отдельных параметров управления электропитанием

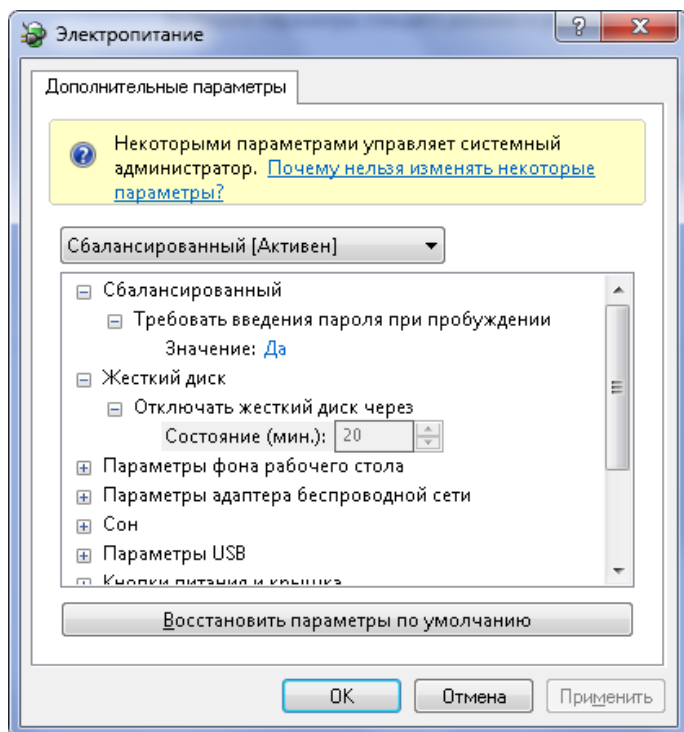


Рис. 6.29. Если параметры управления электропитанием заданы через групповую политику, пользователи лишаются возможности редактировать их через Панель управления

Настройка поведения кнопок

Папка **Параметры кнопок** (Button Settings) содержит следующие опции политики управления их поведением:

- ☐ **Выберите действие кнопки включения питания (питание от сети)** (Select the Power Button action when the computer is plugged in);
- ☐ **Выберите действие кнопки перехода в режим сна (питание от сети)** (Select the Sleep Button action when the computer is plugged in);
- ☐ **Выберите действие кнопки питания в меню "Пуск" (питание от сети)** (Select the Start Menu Power Button action when the computer is plugged in);
- ☐ **Выберите действие при закрытии крышки компьютера (питание от сети)** (Select the Lid Switch action on portables when the computer is plugged in);
- ☐ **Выберите действие кнопки включения питания (питание от батареи)** (Select the Power Button action when the computer is on battery power);
- ☐ **Выберите действие кнопки перехода в режим сна (питание от батареи)** (Select the Sleep Button action when the computer is on battery power);
- ☐ **Выберите действие кнопки питания в меню "Пуск" (питание от батареи)** (Select the Start Menu Power Button action when the computer is on battery power);
- ☐ **Выберите действие при закрытии крышки компьютера (питание от батареи)** (Select the Lid Switch action on portables when the computer is on battery power).

Для каждой из кнопок можно задать следующие варианты действий:

- ☐ **Не предпринимать действий** (Take no action);
- ☐ **Сон** (Sleep);
- ☐ **Гибернация** (Hibernate);
- ☐ **Выключение** (Shut down).

Чтобы задать политику для каждой из опций, выполните на нужной опции двойной щелчок мышью и в раскрывшемся окне установите переключатель **Включен** (Enabled), а затем выберите желаемое действие из списка (рис. 6.30).

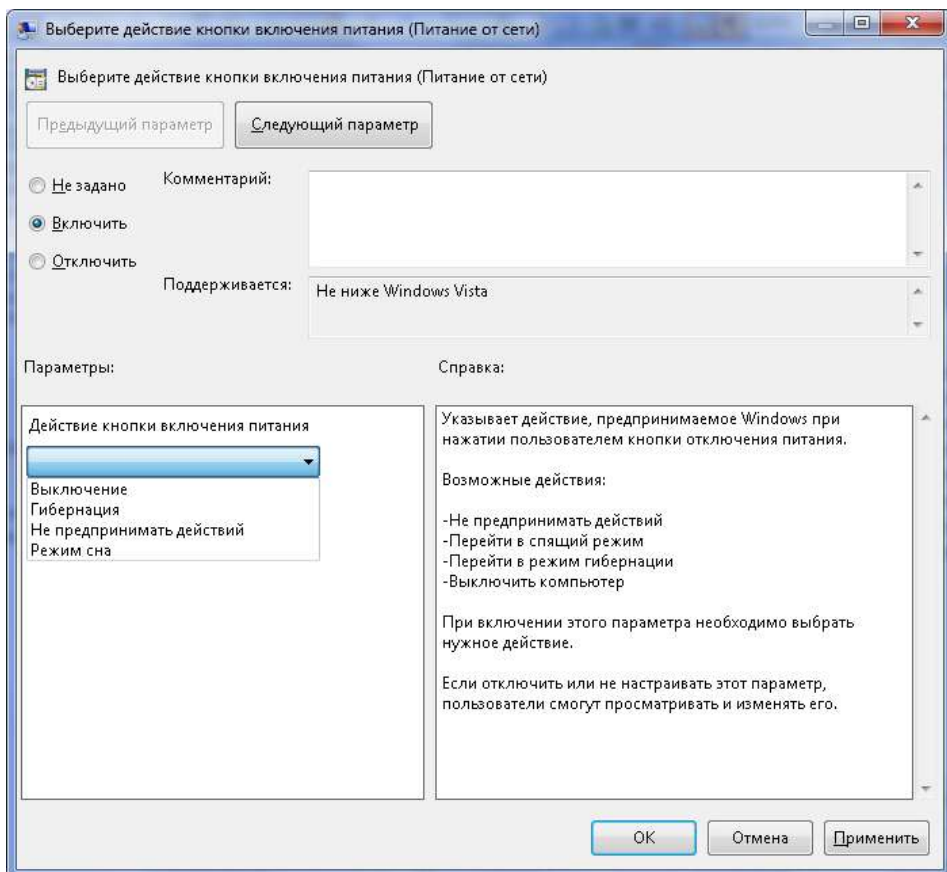


Рис. 6.30. Конфигурирование желаемого эффекта от нажатия на кнопку включения питания на корпусе компьютера

Настройка поведения жесткого диска

Папка **Параметры жесткого диска** (Hard Disk Settings) содержит две политики:

- ☐ **Отключить жесткий диск (питание от сети)** (Turn off the hard disk when the computer is plugged in);
- ☐ **Отключить жесткий диск (питание от батарей)** (Turn off the hard disk when the computer is on battery power).

Эти политики позволяют задать продолжительность периода неактивности компьютера перед отключением жесткого диска. Диапазон возможных значений (в секундах) — от 1 до 999 999.

Настройка параметров уведомления

Для настройки параметров уведомления (Notification Settings) предоставляются следующие возможности:

- ☐ **Действие при почти полной разрядке батареи** (Critical battery notification action);
- ☐ **Действие при низком заряде батареи** (Low battery notification action);
- ☐ **Уровень сигнала при почти полной разрядке батареи** (Critical battery notification level);
- ☐ **Отключить уведомление при низком уровне заряда батареи** (Turn off low battery user notification);
- ☐ **Уровень сигнала низкого заряда батареи** (Low battery notification level);
- ☐ **Уровень сигнала резервной батареи** (Reserve Battery notification level) — новая политика, впервые появившаяся в Windows 7.

Используя эти политики, вы можете задать уровни заряда батареи (низкий или критический), при которых система будет выводить соответствующие уведомления. Когда активизирована политика в отношении уровня заряда батареи, следует указать оставшийся уровень (в процентах от полной мощности). Политики в отношении действия позволяют выбрать, что будет предпринято, если уровень заряда батареи упадет до низкого или критического. Выбрав эти политики, вы сможете задать следующие варианты:

- ☐ **Не предпринимать действий** (Take no action);
- ☐ **Сон** (Sleep);
- ☐ **Гибернация** (Hibernate);
- ☐ **Выключение** (Shut down).

Если будет активизирована политика **Отключить уведомление при низком заряде батареи** (Turn off low battery user notification), то система не будет выводить уведомления при низком уровне заряда батареи.

При включении нового параметра **Уровень сигнала резервной батареи** (Reserve Battery notification level), появившегося в Windows 7, вам потребуется ввести числовое значение (в процентах) уровня заряда батареи, при котором включается сигнал использования резервной батареи. Появление этого сигнала должно предупредить пользователя ноутбука о необходимости подготовиться к принудительному выключению и указывает на необходимость срочного сохранения на диск всех несохраненных документов.

Настройка режима сна

В папке **Параметры режимов сна** (Sleep Settings) содержатся 12 политик. Для каждого из действий имеется по две политики: для случая питания от сети и для случая питания от батареи. Рассмотрим их чуть более подробно:

- ☐ **Разрешить приложениям препятствовать переводу системы в режим сна** (Turn on applications to prevent sleep transition) — если эта политика активизирована, приложения или сервисы смогут предотвращать перевод системы в режимы сна (sleep), гибридного сна (hybrid sleep), ждущие режимы (standby) и режим гибернации (hibernate). В этом случае поведение системы будет аналогично поведению Windows XP;
- ☐ **Укажите время ожидания для перехода в режим гибернации** (Specify the system hibernate timeout) — активизировав эту политику, вы сможете указать интервал неактивности (в секундах), после которого система перейдет в режим гибернации. Диапазон допустимых значений — от 1 до 999 999;
- ☐ **Требовать пароль при выходе из спящего режима** (Require a password when a computer wakes) — если вы активизируете эту политику или она будет оставлена не сконфигурированной, то пользователю будет предложено ввести пароль при выходе системы из спящего режима. Если вы не хотите, чтобы система запрашивала пароль, эту опцию необходимо блокировать;
- ☐ **Укажите время ожидания для перехода в режим сна** (Specify the system sleep timeout) — действует по аналогии с политикой времени ожидания для перехода в режим гибернации;
- ☐ **Отключить гибридный спящий режим** (Turn off hybrid sleep) — если вы активизируете эту политику, то система не будет сохранять текущее состояние в дисковом файле. Фактически она будет вести себя так же, как это делала Windows XP при переходе в ждущий режим (Standby);
- ☐ **Разрешить различные режимы сна (S1–S3) при простое компьютера** (Allow standby states (S1–S3) when sleeping) — если активизировать эту политику, Windows Vista/7 в спящем режиме сможет более гибко использовать различные уровни энергопотребления, определенные спецификацией ACPI. Если эта политика заблокирована, то система сможет переходить только в режим гибернации или гибридного сна. Перечислим уровни энергопотребления системы, определенные в спецификации ACPI:
 - S0 — система находится на максимальном уровне энергопотребления и готова к работе;

- S1 — процессор обесточен, RAM неактивна, но обновляется (refreshed). Система может быть выведена из этого состояния с помощью клавиатуры, мыши и т. д.;
- S2 (обычно не реализуется) — все устройства обесточены, как в следующем режиме (S3), за исключением RAM, которая обновляется с более высокой частотой, чем в режиме S3;
- S3 — все устройства обесточены, включая кулеры и жесткие диски, а все данные текущего состояния сохранены в RAM. События клавиатуры или мыши не обязательно выведут систему из этого состояния (все зависит от аппаратной части) — синоним "ждущего режима" (standby);
- S4 — отключены все устройства, а текущее состояние сохранено в файле на жестком диске (гибернация).

ПРИМЕЧАНИЕ

Более подробную информацию об уровнях энергопотребления можно найти в исходном тексте спецификации ACPI (см. <http://www.acpi.info/>), а упрощенное изложение — по следующему адресу: http://en.wikipedia.org/wiki/Advanced_Configuration_and_Power_Interface.

Настройки видеоподсистемы и дисплея

В папке **Параметры экрана и видеоподсистемы** (Video And Display Settings) в Windows Vista содержались четыре политики. Для каждого из действий имелось по две политики, для случая питания от сети и для случая питания от батареи. С их помощью можно было задать следующие действия:

- ☐ **Выключить адаптивное время ожидания выключения дисплея** (Turn off adaptive display timeout) — если эта политика сконфигурирована, Windows автоматически настраивает интервал ожидания выключения дисплея, основываясь на информации, собранной о действиях пользователя;
- ☐ **Отключить дисплей** (Turn off the display) — если вы активизируете эту политику, вам необходимо будет задать продолжительность интервала неактивности (в секундах), по истечении которого дисплей будет отключен.

Эти политики имеются и в Windows 7, но в дополнение к ним появились еще 6 дополнительных (для каждого из действий, как и в Windows Vista, есть по две политики — для случая питания от сети и для случая питания от батареи). С их помощью можно задать следующие действия:

- ☐ **Указать яркость монитора** (Specify display dim brightness) — если эта политика сконфигурирована, вы сможете указать яркость монитора (в процентах), когда Windows автоматически снижает яркость подсветки по истечении периода неактивности;

- ❑ **Уменьшить яркость монитора** (Reduce display brightness) — если эта политика сконфигурирована, Windows будет автоматически уменьшать яркость монитора после истечения заданного периода неактивности (в секундах);
- ❑ **Включить фоновый показ слайдов на рабочем столе** (Turn on desktop background slideshow) — позволяет активизировать или включить функцию показа слайдов на рабочем столе.

Редактирование с помощью реестра

Как и в Windows 2000/XP, в Windows Vista и Windows 7 средства по управлению подачей электропитания и энергосбережением базируются на концепции схем подачи электропитания, с той лишь разницей, что теперь эти схемы называются планами (power plans). Планы энергопотребления представляют собой группы параметров, управляющих подачей электропитания и энергосбережением, которые передаются модулю **Диспетчер управления питанием** (Power Policy Manager).

Планы энергопотребления

План энергопотребления содержит значения параметров энергопотребления, которые фактически используются в системе. При этом на текущий момент времени активен может быть лишь один из имеющихся планов энергопотребления. Пользователи могут изменять параметры энергопотребления, редактируя имеющиеся планы.

План энергопотребления состоит из следующих компонентов, хранящихся в реестре:

- ❑ **Глобальный уникальный идентификатор плана энергопотребления** (Globally Unique Identifier, GUID)² — GUID плана энергопотребления уникальным образом идентифицирует план энергопотребления, позволяя отличать его от других планов, имеющихся в системе. В Windows Vista и Windows 7 программное обеспечение и конфигурационные утилиты ссылаются на планы энергопотребления по номерам GUID. В предшествующих версиях Windows схемы энергопотребления идентифицировались по целочисленным индексам, отсчитываемым от нуля, или по строкам, со-

² Глобальный уникальный идентификатор (Globally Unique Identifier, GUID) представляет собой специальный тип идентификатора, используемого программным обеспечением и конфигурационными утилитами с тем, чтобы обеспечить ссылочный номер на объект, уникальный в том контексте, в котором он используется. Значения GUID можно получить с помощью утилиты `Uuidgen.exe`, более подробную информацию о которой можно найти в документации Windows Platform SDK. Хотя уникальность каждого вновь создаваемого номера GUID и не гарантируется, их общее количество настолько велико (2^{122} или 5.3×10^{36}), что вероятность повторной генерации один раз сгенерированного номера пренебрежимо мала.

державшим имя соответствующей схемы. GUID плана энергопотребления, активного на данный момент, хранится в реестре в строковом параметре `ActivePowerScheme`, расположенном в составе ключа `HKLM\SYSTEM\CurrentControlSet\Control\Power\User\PowerSchemes` (рис. 6.31).

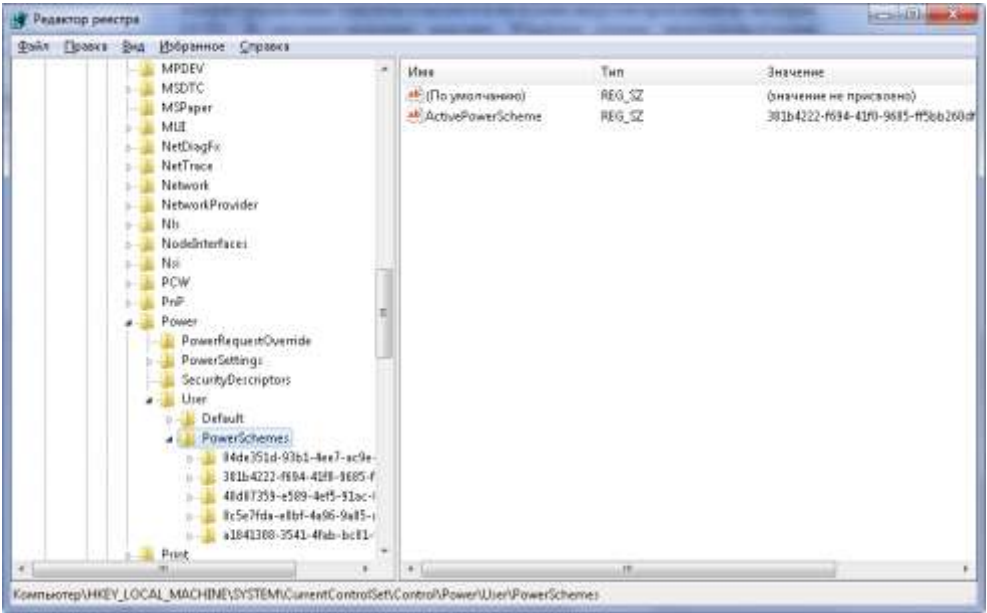


Рис. 6.31. Содержимое ключа реестра

`HKLM\SYSTEM\CurrentControlSet\Control\Power\User\PowerSchemes` — здесь содержится список планов энергопотребления, присутствующих в системе по умолчанию, а также параметр `ActivePowerScheme`, указывающий план, активный на текущий момент

Стандартные планы энергопотребления по умолчанию в Windows Vista и Windows 7, а также их GUID и краткие описания перечислены в табл. 6.2;

Таблица 6.2. Стандартные планы энергопотребления, которые по умолчанию присутствуют в Windows Vista и Windows 7

Название плана	GUID	Краткое описание
Сбалансированный (Balanced)	381b4222-f694-41f0-9685-f55bb260df2e	При использовании этого плана система автоматически балансирует энергопотребление и производительность системы с учетом возможностей имеющихся аппаратных средств

Таблица 6.2 (окончание)

Название плана	GUID	Краткое описание
Высокая производительность (High Performance)	8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c	При использовании этого плана обеспечивается максимальная производительность, но и энергопотребление максимально
Экономия энергии (Power Saver)	a1841308-3541-4fab-bc81-f71556f20b4a	При использовании этого плана предпочтение отдается энергосбережению, а производительность системы снижается до минимума

- ❑ **Строки имени плана энергопотребления (friendly name) и его описания (description string)** — текстовые строки, задающие так называемое "дружественное имя" (friendly name) и краткое описание (description) планов энергопотребления, имеющих на компьютере. Эти строки используются для идентификации планов энергопотребления при конфигурировании опций энергопотребления через Панель управления (Control Panel) или утилиту командной строки `PowerCfg.exe`³. В реестре эти параметры задаются параметрами `FriendlyName` и `Description` в составе `HKLM\SYSTEM\CurrentControlSet\Control\Power\User\PowerSchemes\<Scheme-GUID>`;
- ❑ **Персонализирующий атрибут (Power plan personality attribute)** — персонализирующий атрибут плана энергопотребления задает общее поведение плана в масштабах всей системы. Персонализирующий атрибут задается номером GUID, который должен совпадать с одним из номеров GUID, перечисленных в табл. 6.2. Хотя Windows Vista/7 поддерживает только три персонализирующих атрибута, в системе можно создать более трех планов энергопотребления (но при этом обратите внимание, что вновь создаваемый план энергопотребления может быть создан только на базе одного из трех планов, предоставляемых по умолчанию). Смысл персонализирующего атрибута заключается в упрощении процесса, используемого Windows для информирования приложений об общесистемной политике энергопотребления. Windows просто рассылает этот атрибут всем приложениям и драйверам устройств. Благодаря этому, приложения, вместо того чтобы проверять отдельные параметры управления электропитанием, руководствуются персонализирующим атрибутом при определении своего поведения в отношении энергопотребления и производительности;

³ Конфигурирование опций энергопотребления с помощью утилиты `PowerCfg.exe` будет кратко описано далее в этой главе.

- ❑ **Предпочтительные настройки параметров энергопотребления при работе от сети и от батареи** (AC and DC value preferences for power settings) — для каждого из параметров настройки энергопотребления предоставляются предпочтительные значения для случая работы от сети электропитания (AC) и от батареи (DC). Значения DC используются только в случаях, когда система работает от батареи или подключена к источнику бесперебойного питания (UPS).

Настройки энергопотребления системы

Настройки энергопотребления системы представляют собой базовый компонент политики энергопотребления в Windows. Каждый параметр настройки энергопотребления имеет определение, в которое входит вся информация, необходимая для описания конкретного параметра и его возможных значений. Примерами параметров настройки энергопотребления являются, например, **Отключать экран через** (Display Idle Timeout) и **Действие кнопки питания** (System Power Button action).

Хранилище политик энергопотребления в Windows 7, как и в Windows Vista, содержит отдельные определения параметров энергопотребления для случаев питания от сети (AC) и от батареи (DC). Этот подход позволяет обеспечить расширяемость политик энергопотребления, так как сторонние производители аппаратных средств и приложений могут добавлять в это хранилище новые настройки.

Определение параметра настройки энергопотребления состоит из следующих компонентов:

- ❑ **GUID параметра настройки энергопотребления** — каждый параметр настройки энергопотребления уникальным образом идентифицируется ассоциированным с ним номером GUID, который используется всеми конфигурационными утилитами и функциями API при установке значений этого параметра. Сторонние разработчики аппаратных средств и прикладных программ могут добавлять новые параметры настройки энергопотребления, расширяющие стандартный набор политик энергопотребления в Windows Vista;
- ❑ **"Дружественное имя"** (Friendly name) и **строки описания** (description strings). "Дружественное имя" и строка описания, как и следует из их названий, описывают назначение параметра настройки энергопотребления. Они фигурируют в панели управления и других приложениях GUI в Windows Vista;
- ❑ **Разрешенные значения** (Allowed values) — указывают разрешенные значения, которые может принимать конкретный параметр. Параметры настройки энергопотребления задаются в виде диапазонов значений или

в виде дискретных величин. Например, для них можно задавать диапазоны от 0 до 100 процентов или дискретные значения ON и OFF;

- ❑ **Атрибуты (Attributes)** — каждое определение параметра энергопотребления имеет собственный набор атрибутов. В Windows Vista/7 по умолчанию определен единственный атрибут — `ATTRIB_HIDE`, который указывает, должен ли этот параметр отображаться в расширенных настройках в панели управления (Control Panel);
- ❑ **Дескриптор безопасности (Security descriptor)** — позволяет администраторам ограничивать доступ к параметрам настройки энергопотребления для отдельных пользователей и групп.

Важно понимать, что *определение* (definition) параметра настройки энергопотребления перечисляет возможные значения этого параметра, в то время, как *план энергопотребления* (power plan) указывает фактическое значение этого параметра, которое и будет использоваться.

Модификация предпочтительного плана настройки параметров энергопотребления через реестр

Чтобы модифицировать предпочтительный план настройки энергопотребления через реестр, действуйте следующим образом:

Запустите редактор реестра с административными полномочиями.

1. Найдите и раскройте следующий ключ реестра:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
explorer\ControlPanel\NameSpace\
{025A5937-A6BE-4686-A844-36FE4BEC8B6D}
```

2. Выполните щелчок правой кнопкой мыши по параметру `PreferredPlan`, затем из появившегося контекстного меню выберите команду **Изменить** (Modify).

3. В поле **Значение** (Value) введите один из следующих GUID:

- 381b4222-f694-41f0-9685-ff5bb260df2e — для использования сбалансированного плана (Balanced plan);
- a1841308-3541-4fab-bc81-f71556f20b4a — для использования плана экономии энергии (Power saver plan);
- 8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c — для настройки на максимальную производительность (High performance plan).

Кроме того, вы можете ввести GUID индивидуально настроенного плана энергопотребления, который вы, разумеется, должны предварительно создать.

ПРИМЕЧАНИЕ

Чтобы определить номера GUID для всех существующих планов энергопотребления, введите из командной строки команду `Powercfg /List`.

В Windows 7 уже упомянутая команда `Powercfg` дополнилась новыми опциями. В частности, с ее помощью теперь можно активизировать в системе регистрацию событий, связанных с управлением электропитанием и сервисами, имеющими к этому отношение. В частности, особого упоминания заслуживают две из них:

- команда `powercfg /ENERGY` (она требует административных полномочий) запускает на компьютере трассировку событий и генерирует файл журнала (в формате HTML или XML), который позволит выявить все возможные источники неэффективного энергопотребления и связанных с ним проблем;
- команда `powercfg /REQUESTS` — позволяет определить, какие приложения и процессы мешают автоматическому переходу компьютера в спящий режим.

4. Нажмите кнопку **ОК** и закройте редактор реестра.

Заключение

В данной главе рассмотрены вопросы диагностики и устранения неполадок, связанных с установкой и использованием нового оборудования, использованием встроенных средств мониторинга Windows 7. Во второй части этой главы обсуждалась спецификация ACPI, управление энергосберегающими режимами, а также те ключи реестра, которые отвечают за управление питанием компьютером. Если ваша система соответствует спецификации ACPI, то при добавлении в систему нового устройства вы не должны сталкиваться с задачей обеспечения его сосуществования с устройствами, которые уже установлены в системе.

Глава 7



Процесс нормальной загрузки Windows 7

Сложность увеличивает вероятность поломки; двухмоторный самолет, по сравнению с одномоторным, имеет, по крайней мере, вдвое больше проблем с двигателями.

Правило самолета

Когда бы мы могли начать
С печальной мудрости огарка,
Как помогла бы нам свеча,
Когда она горела ярко.

П. Хэйн, "Грузики"

В отличие от Windows XP, где процесс загрузки системы, несмотря на усовершенствования и нововведения, протекал аналогично процессу загрузки Windows NT/2000, начиная с Windows Vista в последовательность загрузки были внесены существенные изменения, которые с полным правом можно назвать революционными. Что же касается Windows 7, то в ней этот процесс протекает похожим образом, а имеющиеся улучшения и усовершенствования направлены, в основном, на повышение производительности и ускорение загрузки. Для тех пользователей, которые переходят на Windows 7, минуя Windows Vista, понимание этих процессов может представлять сложность, поэтому им рекомендуется прочесть данную главу очень и очень внимательно. Здесь мы подробно и детально рассмотрим процесс нормальной загрузки Windows Vista и Windows 7, а имеющиеся отличия будут подчеркнуты по ходу изложения. Загрузки предшествующих версий Windows¹ мы коснемся лишь вкратце, при рассмотрении мультизагрузочных конфигураций.

¹ На компакт-диске, прилагаемом к этой книге, в каталоге <CD_drive_letter>\Ch08\Supplementary вы найдете отрывок из моей книги по реестру Windows XP, подробно описывающий процесс загрузки Windows NT/2000/XP.

Нововведения в процессе загрузки Windows Vista/7

Как уже неоднократно говорилось ранее в этой книге, по сравнению с Windows XP последовательность загрузки Windows Vista претерпела радикальные изменения. Тем не менее, несмотря на эти модификации, в процессе загрузки все же присутствуют некоторые общие черты, свойственные не только всем операционным системам из семейства Windows NT, но всем операционным системам вообще. Упрощенная схема общего цикла работы системы (от загрузки до завершения работы) показана на рис. 7.1.

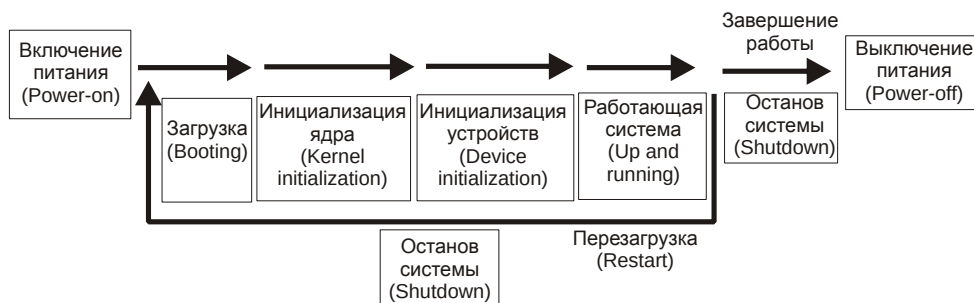


Рис. 7.1. Упрощенная схема рабочего цикла операционной системы от загрузки до перезагрузки или завершения работы

ПРИМЕЧАНИЕ

Схема процесса загрузки, показанная на рис. 7.1, справедлива для каждой операционной системы, и Windows 7 — не исключение из этого правила. Такая последовательность запуска применима к системам, загружаемым или перезагружаемым после нормального завершения работы системы (shutdown). Процедура запуска начнется после того, как пользователь выполнит одно из следующих действий: включит компьютер, который ранее был выключен, или перезагрузит систему, выбрав опцию **Перезагрузка (Restart)**, как показано на рис. 7.2.

Однако при возобновлении работы при выходе из спящих режимов эта последовательность будет иной.

При успешном запуске Windows Vista и Windows 7 процесс загрузки состоит из следующих этапов:

- ❑ самотестирование при включении питания (Power-on self test, POST);
- ❑ процесс начальной загрузки (bootstrap);
- ❑ работа Менеджера загрузки (Boot manager phase);

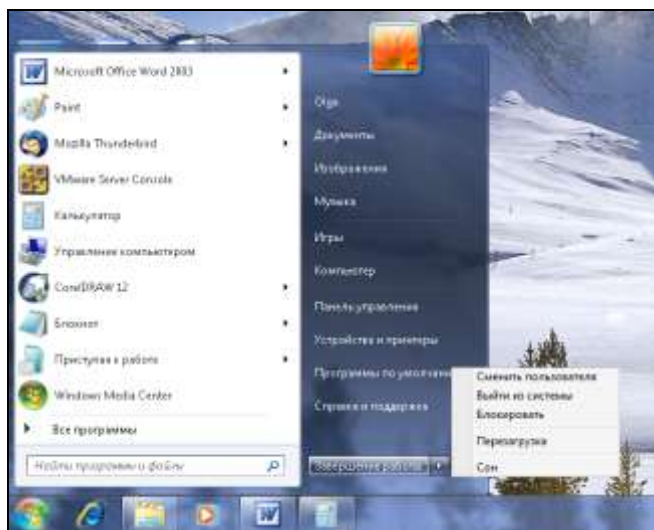


Рис. 7.2. Опции меню Windows 7, позволяющие осуществить завершение работы

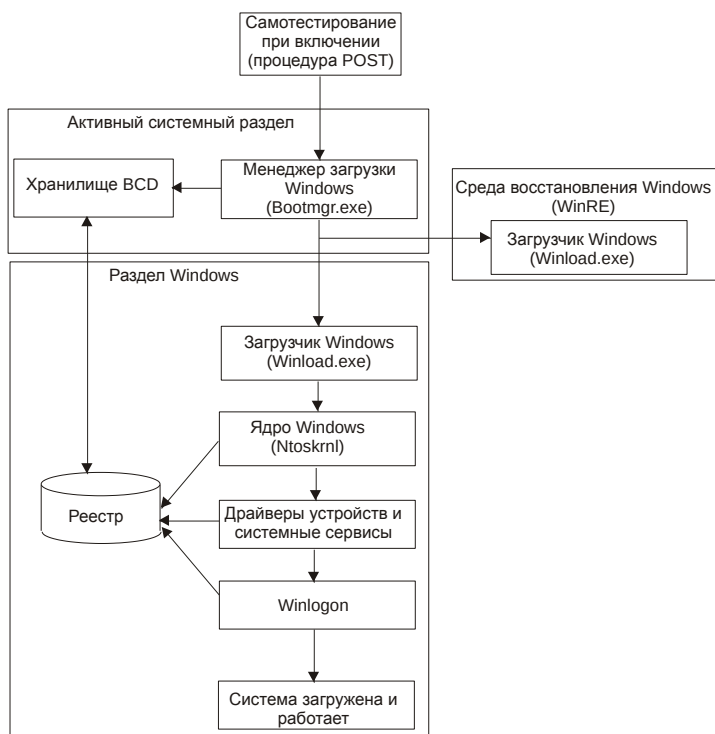


Рис. 7.3. Упрощенная диаграмма процесса загрузки Windows Vista и Windows 7

- загрузка ядра (Kernel loading phase);
- загрузка и инициализация драйверов и сервисов;
- фаза регистрации пользователя в системе Windows Vista (logon phase).

Упрощенная диаграмма процесса загрузки Windows Vista и Windows 7 показана на рис. 7.3.

До выпуска Windows Vista механизм загрузки операционных систем из семейства Windows зависел от аппаратной платформы (x86 или Itanium). Начиная с Windows Vista, этот процесс был унифицирован и, по утверждению разработчиков, больше не зависит от аппаратной платформы.

ПРИМЕЧАНИЕ

В действительности, процессы загрузки Windows Vista и Windows 7 для платформ x86 и Itanium все же имеют незначительные отличия. Это касается только самых ранних стадий загрузки — самотестирования при включении питания и процесса начальной загрузки (bootstrap). Однако, как только управление передается Менеджеру загрузки (файл Bootmgr), дальнейший процесс становится одинаковым для обеих платформ. Более подробная информация по данному вопросу будет приведена далее в этой главе.

За счет чего же была достигнута унификация процесса загрузки? Рассмотрим вкратце нововведения, появившиеся в загрузочной архитектуре операционной системы:

- первое, что немедленно бросается в глаза, — это замена старого загрузчика NTLDR на комбинацию файлов bootmgr (Windows boot manager, Менеджер загрузки), winload.exe (Windows operating system loader, загрузчик Windows) и winresume.exe (Windows resume loader, загрузчик возобновления работы Windows);
- нет больше и хорошо известного пользователям Windows NT/2000/XP файла boot.ini, который был замещен базой данных загрузочной конфигурации (Boot Configuration Database, BCD). К преимуществам, предоставляемым BCD, относятся:
 - возможность абстрагирования от микропрограммного обеспечения, что и позволило унифицировать процесс загрузки Windows для платформ x86 и Itanium;
 - использование строк в формате Unicode, что обеспечивает широкие возможности по интернационализации программного обеспечения;
 - двоичный формат хранения информации в файле BCD. При этом соответствующий улей реестра содержится в каталоге \Boot\BCD на активном системном разделе. В реестре он отображается как ключ HKLM\BCD00000000, для защиты которого предприняты специальные меры безопасности.

Более подробно все перечисленные нововведения будут рассмотрены в последующих разделах данной главы. Перед тем как приступить к их обсуждению, отметим, что, как и в Windows NT/2000/XP, в Windows Vista и Windows 7 к тому моменту, когда производится регистрация пользователя в системе, компьютер уже завершает загрузку Windows и большую часть процесса инициализации. Однако полностью все процессы будут завершены только после успешной регистрации пользователя в системе.

Для начала успешной загрузки Windows Vista и Windows 7 необходимо соблюдение следующих условий:

- ☐ корректная инициализация аппаратных средств компьютера;
- ☐ наличие всех файлов, необходимых для загрузки системы.

Последовательность загрузки Windows Vista и Windows 7

Как уже говорилось, последовательность загрузки Windows Vista и Windows 7 отличается от последовательности загрузки Windows NT/2000/XP. Рассмотрим этот процесс более подробно.

Процесс самотестирования при включении

При включении питания или перезагрузке компьютер проходит стадию *самотестирования при включении* (Power On Self Test, POST), представляющую собой набор тестов, предназначенных для определения правильности функционирования аппаратных средств. В случае возникновения уже на стадии самозагрузки проблем с аппаратными средствами или настройкой компьютера, POST информирует пользователя серией звуковых сигналов. Для их расшифровки следует иметь под рукой сопроводительную документацию, полученную от поставщика в комплекте с компьютером.

Итак, программа POST действует следующим образом:

- ☐ диагностическая подпрограмма, в зависимости от встроенного микропрограммного обеспечения, выполняет некоторые элементарные проверки аппаратных средств, определяет количество доступной памяти, физическое присутствие всех устройств, необходимых для запуска операционной системы (например, жесткого диска), и правильность их инициализации;
- ☐ завершив диагностическую подпрограмму, POST извлекает конфигурационные параметры из CMOS-памяти², размещенной на материнской плате.

² CMOS — Complementary Metal Oxide Semiconductor, комплементарный металлооксидный полупроводник, КМОП.

А после завершения процедуры POST материнской платы каждый дополнительный адаптер со встроенной микросхемой firmware (например, видеоконтроллер или же контроллер жестких дисков) выполняет собственную специализированную подпрограмму POST.

При обнаружении проблем, связанных с аппаратными средствами или установками BIOS, процедура POST, как уже отмечалось ранее, выдает серию звуковых сигналов. Учитывая, что программа POST управляется посредством BIOS компьютера и зависит от конкретного компьютера, документацию на компьютер с расшифровкой этих сигналов рекомендуется всегда иметь под рукой.

ПРИМЕЧАНИЕ

Тема отыскания и устранения неисправностей аппаратных средств компьютера выходит далеко за рамки этой книги. Интересующимся читателям можно рекомендовать замечательную книгу известного хакера Pinckzakko³, а также полезные ресурсы, которые помогут получить представление о кодах ошибок BIOS:

- BIOS Survival Guide — http://burks.bton.ac.uk/burks/pcinfo/hardware/bios_sg/bios_sg.htm;
- "Коды ошибок BIOS и звуковые сигналы" — http://www.4pc.info/hardware/mb/bios_error_sound.php;
- "Звуковые сигналы ошибок BIOS" — <http://tinyurl.com/69hz8l>.

Процессы выполнения POST для систем, функционирующих на основе Itanium, подобны процессам, выполняемым в системах на базе процессоров x86. Расширяемый интерфейс встроенных программных средств (Extensible Firmware Interface, EFI)⁴ так же осуществляет элементарную проверку аппаратного обеспечения, подобную той, которую осуществляет BIOS, и проверяет наличие устройств, необходимых для запуска системы.

Процесс инициализации при запуске

Как уже говорилось ранее, несмотря на унификацию, на ранних стадиях процесс загрузки Windows Vista и Windows 7 для платформ x86 и Itanium все же имеет незначительные отличия. Рассмотрим эти процессы более подробно.

³ Салихан Д. BIOS: дизассемблирование, модификация, программирование: Пер. с англ. — СПб.: БХВ-Петербург, 2007 (<http://www.bhv.ru/books/book.php?id=180728>).

⁴ Спецификация EFI определяет новую модель интерфейса между операционными системами и встроенным программным обеспечением платформы. Более подробную информацию о спецификации EFI можно найти здесь: <http://www.microsoft.com/whdc/system/platform/firmware/efibrief.mspx>.

Процесс начальной загрузки на платформах x86

После успешного завершения процедуры POST начинается процесс инициализации при запуске, в ходе которого BIOS пытается обнаружить загрузочный диск. Порядок поиска загрузочного диска (флоппи-дисководы, жесткие IDE- и SCSI-диски, устройства CD/DVD) задается BIOS, и можно переконфигурировать этот порядок, называемый *последовательностью загрузки* (boot sequence)⁵.

ПРИМЕЧАНИЕ

Практически все современные BIOS предусматривают возможность выбрать загрузочное устройство, нажав и удерживая во время прохождения POST клавишу <Esc> или <F8>.

Если при этом дисковод A: включен в последовательность загрузки первым, и в нем находится дискета, BIOS попытается использовать эту дискету в качестве загрузочной. Если дискеты в дисковом нет, BIOS проверяет первый жесткий диск, который к этому времени уже инициализировался. Для процесса запуска огромное значение играет первый сектор жесткого диска, который содержит *главную загрузочную запись* (Master Boot Record, MBR) и *таблицу разделов* (Partition Table).

BIOS считывает главную загрузочную запись и загружает ее в память, а затем передает ей управление. Код, содержащийся в главной загрузочной записи, сканирует таблицу разделов в поисках системного раздела. Найдя системный раздел, MBR загружает в память его нулевой сектор и исполняет код, содержащийся в этом секторе. Сектор 0 на системном разделе — так называемый *загрузочный сектор раздела* (partition boot sector), содержит загрузочный код операционной системы — загрузочную запись раздела (Partition boot record, PBR). Этот код и осуществляет запуск операционной системы определенным для нее способом.

Если на первом жестком диске нет системного раздела, главная загрузочная запись отобразит одно из следующих сообщений об ошибках:

- ❑ **Invalid partition table** (Неверная таблица разделов);
- ❑ **Error loading operating system** (Ошибка загрузки операционной системы);
- ❑ **Missing operating system** (Отсутствует операционная система).

Для предшествующих версий операционных систем из семейства Windows NT, главная загрузочная запись не зависела от конкретной операци-

⁵ Подробную информацию о редактировании последовательности загрузки можно найти в сопроводительной документации к вашему компьютеру.

онной системы. Например, на компьютерах x86 одна и та же главная загрузочная запись служила для запуска Windows NT/2000/XP, Windows 9x, а также комбинации MS-DOS/Windows 3.1x.

Начиная с Windows Vista эта ситуация поменялась, и, что вполне естественно, она сохранилась и в Windows 7. В процессе загрузки операционные системы Windows Vista и Windows 7 несколько иначе, чем их предшественницы, используют поле сигнатуры диска (drive ID) в главной загрузочной записи жесткого диска. Это поле, расположенное по смещению 0x01B8 от начала сектора, содержит уникальное число, идентифицирующее данный диск для операционной системы. Windows использует эту сигнатуру в качестве индекса для хранения информации о диске в подключе реестра `HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices`. В Windows NT/2000/XP эта сигнатура в MBR в большинстве случаев была не критичной, и загрузчик NTLDR мог инициировать процесс загрузки даже в случае нарушения ее целостности.

В Windows Vista и Windows 7 изменение или затирание этой сигнатуры приведет к остановке процесса загрузки с выдачей следующего сообщения об ошибке: **winload.exe..... is missing or corrupt**. Стоит отметить, что это сообщение является абсолютно неточным и никак не отражает фактической ситуации, потому что файл `winload.exe` как таковой может быть вполне корректным и находиться на своем месте. Действительная причина состоит в том, что если изменить хотя бы один бит в этой сигнатуре, Менеджер загрузки просто не сможет найти файл `winload.exe`, чтобы передать ему управление. Если эту сигнатуру восстановить, то и возможность загрузки Windows будет восстановлена.

Что касается загрузочного сектора раздела, то он зависит как от операционной системы, так и от используемой файловой системы. На компьютерах x86 загрузочный сектор раздела Windows Vista/Windows 7 отвечает за выполнение следующих действий:

- распознавание используемой файловой системы и ее применение для поиска Менеджера загрузки (`bootmgr`) и базы данных конфигурационной информации (BCD) в корневом каталоге системного раздела. На томах FAT структура данных, называемая загрузочным сектором раздела, действительно имеет длину в 1 сектор физической разметки диска. На томах FAT32 эта структура занимает уже 2 сектора физической разметки диска, поскольку загрузочный код имеет длину более 512 байтов. На томах NTFS структура данных, называемая загрузочным сектором раздела, может занимать до 16 секторов, причем дополнительные секторы могут содержать код файловой системы, необходимой для поиска требуемых файлов;
- нахождение Менеджера загрузки (`bootmgr`), его загрузку в память и передачу ему управления.

ПРИМЕЧАНИЕ

В Windows NT/2000/XP и Windows Server 2003 функции Менеджера загрузки и Диспетчера загрузки выполнялись файлами NTLDR, ntldetect.com и boot.ini, причем все три файла должны были находиться в корневом каталоге активного главного раздела первого жесткого диска (раздела System). Начиная с Windows Vista, эти три файла были заменены на bootmgr (Менеджер загрузки), BCD (базу данных конфигурационной информации) и winload.exe (загрузчик операционной системы), но только bootmgr и BCD остались на системном разделе. Файл загрузчика winload.exe переместился в каталог %SystemRoot%\system32 загрузочного раздела (раздел Boot).

В Windows 7 появилось и еще одно очень важное усовершенствование, нацеленное на повышение ее надежности и отказоустойчивости. Если Windows 7 — это единственная операционная система, установленная на компьютере, то при ее установке программа Windows 7 Setup во время разбиения диска на разделы создаст скрытый раздел с именем System Reserved, на который будут записаны все файлы, необходимые для начала процесса загрузки системы: Менеджер загрузки (bootmgr), улей реестра BCD и некоторые другие. Если же Windows 7 устанавливалась в качестве второй или даже третьей операционной системы, то все будет практически так же, как было в Windows Vista.

На компьютерах x86 системный раздел должен находиться на первом физическом жестком диске. Загрузочный раздел (тот, что содержит системные файлы операционной системы) может совпадать с системным разделом, но допустимо также его размещение и в другом разделе того же жесткого диска или даже на другом жестком диске.

Если первый жесткий диск не содержит системного раздела, который должен использоваться для запуска компьютера, необходимо отключить этот диск, чтобы системная BIOS могла получить доступ к нужному жесткому диску, с которого будет запускаться операционная система.

ПРИМЕЧАНИЕ

Отключить, разумеется, логически, то есть назначить в BIOS первым диском именно тот, который и содержит системный раздел.

Загрузочная дискета

Как уже отмечалось ранее, если в дисковом **A:** имеется загрузочная (системная) дискета, BIOS загрузит в память ее первый сектор, представляющий собой *загрузочный сектор раздела* (Partition Boot Sector). Если дискета не является загрузочной, то вы увидите на экране примерно следующие сообщения об ошибках:

- ❑ для дискеты, отформатированной в формате DOS или Windows 9x/ME —
Non-System disk or disk error
Replace and press any key when ready.

- ❑ для дискеты, отформатированной в Windows NT/2000/XP —

Ntldr is missing

Replace and press any key when ready.

- ❑ для дискеты, отформатированной в Windows Vista/7 —

Bootmgr is missing

Replace and press any key when ready.

Для успешной загрузки операционных систем из семейства Windows NT с дискеты требуется, чтобы ее первым сектором был загрузочный сектор раздела. Кроме того, на этой дискете должны присутствовать все файлы, необходимые для начала процесса загрузки. Как и в случае с Windows NT/2000/XP, Windows Vista и Windows 7 тоже могут быть загружены с дискеты. Чтобы изготовить загрузочную дискету Windows Vista или Windows 7, необходимо сделать следующее:

1. Возьмите чистую дискету и отформатируйте ее под управлением соответствующей операционной системы (Windows Vista или Windows 7).
2. Скопируйте на эту дискету файл bootmgr из корневого каталога системного раздела.
3. Создайте на этой дискете папку \Boot и скопируйте в нее улей реестра BCD — это файл ВСД, расположенный в скрытой папке \Boot на первом (активном) разделе первого жесткого диска. Для локализованных версий Windows Vista/Windows 7 в эту папку следует скопировать и папку, содержащую локализованную версию Менеджера загрузки (например, для русской версии это будет папка \Boot\ru-RU).

Загрузочный компакт-диск

Если необходимо загрузить систему с загрузочного компакт-диска (например, для инсталляции Windows с дистрибутивного диска или для восстановления системы), то вам следует установить в BIOS привод компакт-дисков в качестве основного загрузочного устройства — первым пунктом в списке порядка загрузки. При загрузке системы с загрузочного компакт-диска с системой Windows Vista или Windows 7, программа Setup проверяет жесткий диск на наличие установленной копии Windows. Если программа Setup обнаружит, что на диске имеется установленная система, то она предложит опцию обхода запуска с CD/DVD-ROM (для этого достаточно не отреагировать на предложение системы **Press any key to boot from CD-ROM**). Если в течение трех секунд вы не нажмете какую-либо клавишу, то программа Setup выполняться не будет, и компьютер передаст управление от CD/DVD-ROM к жесткому диску.

СОВЕТ

Если вы не хотите запускать программу Setup для инсталляции или же восстановления поврежденной системы, извлеките компакт-диск из дисководы — это позволит минимизировать время, необходимое для запуска Windows.

Процесс начальной загрузки на платформах Itanium

На платформах Itanium этот процесс протекает иначе. После стандартной инициализации микропрограммного обеспечения EFI производится загрузка драйверов и приложений EFI. Код микропрограммного обеспечения EFI должен содержать *собственный менеджер загрузки*, который загрузит первую исполняемую программу EFI (это может быть специализированная утилита или загрузчик операционной системы). Программа Windows Setup добавляет в меню Менеджера загрузки EFI всего одну строку — **Windows Boot Manager**. Эта строка указывает на файл \EFI\Microsoft\Boot\Bootmgfw.efi как на исполняемую программу EFI, которая должна запускаться, когда пользователь выбирает эту опцию из загрузочного меню. Обратите внимание, что таким образом в системах EFI фактически появляется два менеджера загрузки: собственный Менеджер загрузки и Менеджер загрузки Windows Vista или Windows 7. Таким образом, различия в процессе загрузки Windows Vista/Windows 7 на платформах x86 и Itanium наблюдаются только на самых ранних этапах загрузки (рис. 7.4).

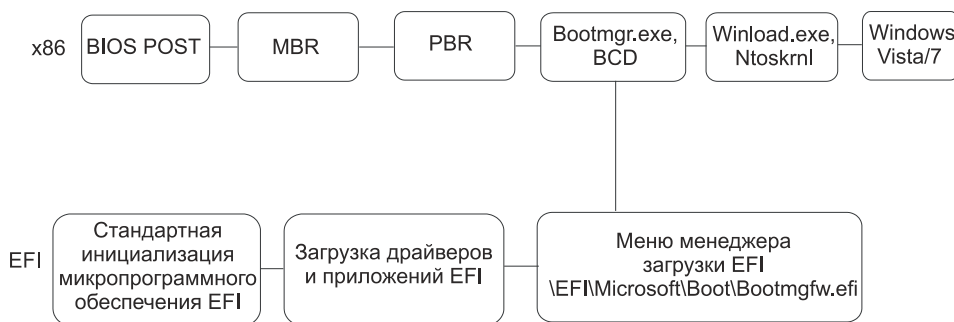


Рис. 7.4. Различия в последовательности загрузки Windows Vista/7 на платформах x86 и EFI

Файлы, необходимые для запуска системы

Успешное завершение процедуры POST свидетельствует о корректной инициализации аппаратных средств компьютера. Теперь необходимо запустить операционную систему, а для этой цели требуется присутствие всех файлов,

необходимых для загрузки. Процедура запуска системы закончится неудачей, если хотя бы один из файлов, необходимых для ее загрузки, не будет найден или окажется поврежденным.

Файлы, необходимые для успешного запуска Windows Vista/Windows 7 на компьютерах x86, перечислены в табл. 7.1.

Таблица 7.1. Файлы, необходимые для запуска Windows Vista/Windows 7

Файлы	Местоположение	Краткое описание
Bootmgr	Корневой каталог системного раздела	Менеджер загрузки Windows, загружаемый и запускаемый на исполнение кодом загрузочного сектора раздела. Менеджер загрузки выполняет следующие задачи: • читает данные BCD, выполняя таким образом первую часть функций NTLDR (чтение файла boot.ini); • запускает остальные предзагрузочные приложения Windows (Windows pre-boot applications)
Улей реестра \BCD	\Boot\BCD	База данных конфигурационной информации загрузки (Boot Configuration Database, BCD). BCD заменяет собой файл boot.ini, который был необходим для загрузки предшествующих версий операционных систем из семейства Windows NT
Memtest.exe	\Boot\Memtest.exe	Встроенная предзагрузочная утилита Windows Vista для диагностики проблем с памятью. Не является абсолютно необходимой для загрузки, но полезна при диагностике и устранении проблем
Winload.exe	%Systemroot%\System32\Winload.exe	Загрузчик операционной системы, выполняющий вторую часть набора функций, ранее выполнявшихся NTLDR, а именно: • загрузку образа ядра ОС; • загрузку драйверов и ульев системного реестра. Каждая из установленных копий Windows Vista имеет собственный загрузчик

Таблица 7.1 (продолжение)

Файлы	Местоположение	Краткое описание
Winresume.exe	%Systemroot%\System32\Winresume.exe	Новый загрузчик возобновления (resume loader), который ускоряет выход системы из состояния сна. До Windows Vista эти функции были реализованы загрузчиком NTLDR. Bootmgr запускает этот файл, если обнаруживает, что компьютер находится в спящем режиме
Ntoskrnl.exe	%SystemRoot%\System32	Ядро (kernel) операционной системы Windows Vista. Программный код операционной системы, являющийся частью ядра, выполняется в специальном привилегированном процессорном режиме, с прямым доступом к системным данным и аппаратным средствам
Hal.dll	%SystemRoot%\System32	Файл динамически загружаемой библиотеки уровня аппаратных абстракций (Hardware Abstraction Layer, HAL). HAL обеспечивает изолирование или абстрагирование операционной системы от низкоуровневой аппаратной ее части и предоставляет общий программный интерфейс для однотипных устройств (например, видеоадаптеров)
Ульи реестра	%SystemRoot%\System32\Config	Ульи реестра
Smss.exe	%SystemRoot%\System32	Файл подсистемы диспетчера сеансов (Session Manager). Процесс Smss.exe создается ядром во время загрузки пользовательского режима. Управляет критически важными задачами запуска — например, он создает файл подкачки и выполняет отложенные операции (удаление или переименование файлов и т. п.)
Crss.exe	%SystemRoot%\System32	Файл подсистемы режима пользователя (Win32). Подсистема Win32 необходима для функционирования операционной системы
Winlogon.exe	%SystemRoot%\System32	Файл процесса регистрации в системе, который запускается диспетчером сеансов. Компонент, необходимый для функционирования операционной системы

Таблица 7.1 (окончание)

Файлы	Местоположение	Краткое описание
Services.exe	%SystemRoot%\System32	Диспетчер управления сервисами Windows (Service Control Manager). Отвечает за запуск и остановку сервисов, необходим для функционирования операционной системы
Lsass.exe	%SystemRoot%\System32	Процесс сервера локальной аутентификации пользователей — необходим для регистрации пользователей в системе
Драйверы устройств	%SystemRoot%\System32\Drivers	Файлы драйверов различных устройств

ПРИМЕЧАНИЕ

В Windows NT/2000/XP/Vista/7 понятия *системный раздел* (system partition) и *загрузочный раздел* (boot partition) различаются. Это очень важно знать:

- в системном разделе находятся файлы, необходимые для запуска Windows NT/2000/XP/Vista/7;
- загрузочный раздел, в котором содержатся каталоги %SystemRoot% и %SystemRoot%\System32, может располагаться на этом же или другом физическом диске. %SystemRoot% является переменной окружения⁶.

Работа Менеджера загрузки Windows Vista и Windows 7

После запуска Менеджера загрузки Windows дальнейший процесс начальной загрузки Windows Vista/Windows 7 на различных платформах (EFI и IBM PC-совместимых) во многом схож.

Менеджер загрузки читает информацию из системного хранилища BCD и использует ее для отображения загрузочного меню. В системах EFI, где существует собственный менеджер загрузки, Менеджер загрузки Windows Vista/7 фигурирует в качестве отдельного пункта меню, отображаемого Менеджером загрузки EFI. Он представляет собой самостоятельное приложение EFI, хранящееся на системном разделе EFI (см. рис. 7.4). Microsoft просто добавляет записи в меню BCD и устанавливает время ожидания (timeout) для

⁶ Переменные окружения Windows Vista и их изменения по сравнению с Windows XP перечислены и обсуждаются в следующей статье:

http://vistaonwindows.com/environment_variables.html.

загрузочного менеджера EFI на 2 с. Таким образом, в системах EFI пользователь фактически видит два меню.

Перед тем как отобразить меню загрузки, Менеджер загрузки проверяет собственную целостность. Затем он выясняет, не находится ли компьютер в режимах сна или гибернации. Если файл `hiberfil.sys` содержит данные спящего режима, то вместо отображения меню менеджер загрузки начинает вывод компьютера из спящего режима, копируя содержимое файла `hiberfil.sys` обратно в оперативную память, а затем перезапуская драйверы, запущенные в системе до перехода в режим сна.

Системное хранилище BCD

Файл BCD, содержащий системное хранилище BCD, имеет формат улья реестра и в зависимости от типа микропрограммного обеспечения (EFI или x86) хранится в различных каталогах. На IBM PC-совместимых компьютерах — это файл `\Boot\BCD` в системном разделе. На компьютерах с микропрограммным обеспечением EFI этот файл находится в каталоге `\EFI\Microsoft\Boot\` системного раздела EFI.

Системное хранилище BCD содержит Windows-эквивалент конфигурационных данных загрузочного менеджера EFI. Типичное системное хранилище BCD, как правило, содержит два или большее количество объектов BCD (в случае сложной загрузочной конфигурации). Существуют три основных типа объектов BCD:

- ❑ *приложения* (application objects) — наиболее распространенный тип объектов BCD, используемый для описания приложений, работающих в процессе загрузки. Примерами являются загрузочный менеджер Windows (Windows boot manager) или загрузчик Windows (Windows boot loader);
- ❑ *наследуемые объекты* (inheritable objects) — своего рода "контейнеры" для элементов BCD, которые могут совместно использоваться многими экземплярами объектов BCD. Этот подход более эффективен, нежели создание отдельного экземпляра такого элемента для каждого объекта BCD. Примерами являются наследуемые объекты, задающие опции отладчика ядра Windows, описывающие соединения через порты COM, USB или 1394;
- ❑ *устройства* (device objects) — большинство устройств (например, разделы на жестком диске) могут быть описаны единственным элементом BCD. Однако более сложные устройства требуют для своего описания нескольких элементов. Примером может служить объект устройства при загрузке с RAM-диска, созданного на основе WIM-файла (Windows Image File). В этом случае объект устройства должен описывать путь к WIM-файлу и (при загрузке через сеть) информацию сетевого порта.

Каждый объект имеет 32-битовое поле описания, содержащее код объекта и данные, специфичные для конкретной категории объектов. С точки зрения работы менеджера загрузки, наибольший интерес представляют объекты типа "приложение".

Объекты BCD типа "приложение" обладают двумя ключевыми характеристиками: *тип образа* (image type) и *тип приложения* (application type):

- тип образа задается числовым кодом и указывает метод загрузки соответствующего приложения. Например, исполняемый файл может загружаться через микропрограммное обеспечение или менеджером загрузки Windows. Типы образа, характеризующие объекты BCD типа "приложение" и соответствующие им числовые коды, перечислены в табл. 7.2;

Таблица 7.2. Типы образов объектов приложений BCD

Тип образа (метод загрузки приложения)	Описание	Код
Микропрограммное приложение (Firmware application)	Приложение загружается микропрограммным кодом	0x1
Загрузочное приложение (Boot application)	Менеджер загрузки Windows и загружаемые им приложения	0x2
Объект на основе NTLDR (Ntldr-based loader object)	Загрузчик Windows NT/2000/XP и загружаемые им приложения	0x3
Приложение реального режима (Real-mode application)	Приложения, работающие в реальном режиме	0x4

- тип приложения (application type) указывает задачи, выполняемые приложением. Каждый из типов приложения также ассоциируется с соответствующим ему числовым кодом. Стандартные типы приложений и соответствующие им числовые коды перечислены в табл. 7.3.

Таблица 7.3. Типы стандартных приложений BCD

Приложение BCD	Код	Описание
Менеджер загрузки EFI (Firmware boot manager)	0x1	Менеджер загрузки, используемый в системах EFI
Менеджер загрузки Windows Vista (Windows boot manager)	0x2	Управляет ходом загрузки. В мультизагрузочных системах отображает загрузочное меню, позволяющее пользователю выбрать операционную систему

Таблица 7.3 (окончание)

Приложение BCD	Код	Описание
Загрузчик Windows Vista (Windows boot loader)	0x3	Загружает выбранную версию или конфигурацию Windows
Загрузчик возобновления (Windows resume application)	0x4	Выводит Windows из состояния сна
Приложение Memtest.exe (Windows memory tester)	0x5	Приложение для тестирования RAM
Ntldr	0x6	Используется только в системах x86 (PC/AT BIOS). Загружает операционные системы семейства Windows NT, более ранние, чем Windows Vista
Загрузочный сектор (Boot sector)	0x8	16-разрядное приложение реального режима, используется только в системах x86 (PC/AT BIOS). Может применяться для перезапуска процесса загрузки и загрузки операционных систем, отличных от Windows

Номера GUID стандартных приложений BCD, а также их псевдонимы, используемые при конфигурировании BCD с помощью утилиты командной строки BCDEdit, вводная информация о которой была приведена в главе 4, перечислены в табл. 7.4.

Таблица 7.4. Номера GUID и псевдонимы стандартных приложений BCD

Приложение	Псевдоним	GUID
Менеджер загрузки Windows (Windows Boot Manager)	{bootmgr}	9dea862c-5cdd-4e70-acc1-f32b344d4795
Менеджер загрузки EFI (Firmware Boot Manager)	{fwbootmgr}	a5a30fa2-3d06-4e9f-b5f4-a01df9d1fcba
Приложение memtest.exe	{memdiag}	b2721d73-1db4-4c62-bf78-c548a880142d
Приложение Winresume.exe (Windows Resume Application)	Нет псевдонима	147aa509-0358-4473-b83b-d950dda00615
Наследуемый загрузчик Windows (Legacy Windows Loader)	{ntldr}	466f5a88-0af2-4f76-9038-095b170dc21c

Таблица 7.4 (окончание)

Приложение	Псевдоним	GUID
Объект, описывающий копию Windows, загруженную на текущий момент (Current boot entry)	{current}	fa926493-6f1c-4193-a414-58f0b2456d1e
Копия Windows, загружаемая по умолчанию (Default boot entry)	{default}	Равен GUID той копии Windows Vista или Windows 7, которая назначена для загрузки по умолчанию

Рассмотрим приложения BCD чуть подробнее:

- менеджер загрузки Windows — состоит из элементов BCD, управляющих поведением менеджера загрузки Windows, в число которых входят:
 - пункты меню, позволяющего выбрать операционную систему для загрузки;
 - пункты меню, позволяющего запустить предзагрузочное приложение (например, memtest.exe);
 - время ожидания, в течение которого меню отображается на экране.

Объект "Менеджер загрузки Windows" и его элементы служат той же цели, что и раздел [boot loader] файла boot.ini, использовавшегося в более ранних версиях операционных систем из семейства Windows NT. Хранилище BCD может содержать более одного объекта "Менеджер загрузки", но только один из них может быть представлен стандартным GUID. Для манипулирования хранилищем BCD с помощью утилиты BCDEdit может использоваться псевдоним {bootmgr};

- хранилище BCD содержит, как минимум, один объект "Загрузчик Windows" (если на компьютере установлено несколько копий Windows Vista или Windows 7, таких объектов будет больше — по одному на каждую установленную копию). Эти объекты хранят элементы BCD, используемые в процессе загрузки и инициализации ядра. Каждый объект и его ассоциированные элементы служат той же цели, что и строки раздела [operating systems] файла boot.ini. Объект "загрузчик Windows", ассоциированный с загруженной на текущий момент копией Windows, представлен псевдонимом {current}. Загрузчик, ассоциированный с копией Windows, загружаемой по умолчанию, имеет псевдоним {default};
- необязательный объект Windows Ntldr — описывает расположение файла Ntldr, использовавшегося для загрузки Windows NT/2000/XP. Он нужен

только в том случае, если на компьютере установлены более ранние версии операционных систем из семейства Windows NT. В хранилище BCD может существовать несколько экземпляров объекта Ntldr. Как и в случае с объектом Winload.exe, только один из этих объектов может быть представлен стандартным GUID (см. табл. 7.4). При манипулировании хранилищем при помощи утилиты командной строки BCDEdit используется псевдоним {ntldr};

- необязательные предзагрузочные приложения — выполняют разнообразные операции, относящиеся к диагностике и устранению неполадок (например, приложение memtest.exe, выполняющее тестирование RAM).

Редактирование BCD с помощью утилиты *BCDEdit*

Утилита командной строки BCDEdit (см. главу 4), служит той же цели, что и аналогичная утилита Bootcfg.exe, использовавшаяся в предшествующих версиях операционных систем из семейства Windows NT для редактирования файла boot.ini. Однако по сравнению с Bootcfg.exe, эта утилита предоставляет существенно более широкий набор опций, а также обеспечивает улучшенную поддержку скриптов. Разумеется, как и большинство остальных конфигурационных утилит командной строки Windows Vista/7, BCDEdit требует административных привилегий.

ПРИМЕЧАНИЕ

Утилита BCDEdit может использоваться и в предшествующих версиях операционных систем из семейства Windows NT. Кроме того, в состав дистрибутива Windows Vista/Windows 7 входит и утилита Bootcfg.exe. Однако, применяться она может только для редактирования загрузочной конфигурации систем, более ранних, чем Windows Vista.

Для манипулирования информацией BCD используется следующий синтаксис командной строки:

```
bcdedit /команда [аргумент 1] [аргумент 2] ...
```

Перечислим наиболее широкоупотребительные опции утилиты BCDEdit:

- `/?` — вывод справочной информации об опциях командной строки. Чтобы получить более подробную информацию о конкретной опции, дайте следующую команду: `bcdedit /? command`, где *command* — имя конкретной команды, например: `bcdedit /? export`;
- `/createstore` — создает новое пустое хранилище BCD;
- `/export` — экспортирует в файл содержимое системного хранилища. Применима только к системному хранилищу. Команда представляет собой удобный способ резервного копирования загрузочной конфигурации;

- ❑ `/import` — импортирует информацию загрузочной конфигурации из файла, предварительно созданного командой `/export`. При этом вся информация, хранящаяся в системном BCD, будет затерта. Как и в предыдущем случае, эта команда применима только к системному хранилищу;
- ❑ `/store` — эта опция применяется для указания хранилища BCD, отличного от системного. Может использоваться с большинством команд. Если опция пропущена, то по умолчанию будет использовано системное хранилище. Команда `bcdedit /store` эквивалентна команде `bcdedit /enum ACTIVE`;
- ❑ `/copy` — создает в системном хранилище еще одну копию указанного элемента загрузочного меню;
- ❑ `/create` — создает новый элемент загрузочного меню;
- ❑ `/delete` — удаляет элемент из загрузочного меню;
- ❑ `/deletevalue` — удаляет указанный параметр из элемента загрузочного меню;
- ❑ `/set` — устанавливает значение параметра для элемента загрузочного меню;
- ❑ `/enum` — выводит список всех элементов загрузочного меню. Если команда `bcdedit` дана без параметров, она эквивалентна команде `bcdedit /enum ACTIVE`;
- ❑ `/v` — режим подробного вывода (Verbose mode). Как правило, все номера GUID замещаются их псевдонимами. Если команда дана с ключом `/v`, то утилита BCDEdit выведет и все номера GUID;
- ❑ `/bootsequence` — задает порядок отображения элементов загрузочного меню, который будет использован только при следующей загрузке. После этого система вернется к исходному порядку отображения;
- ❑ `/default` — указывает элемент загрузочного меню, выбираемый по умолчанию по истечении периода тайм-аута;
- ❑ `/displayorder` — команда аналогична `/bootsequence`, но порядок отображения элементов меню загрузки изменяется перманентно;
- ❑ `/timeout` — задает интервал времени (в секундах), в течение которого менеджер загрузки ожидает, когда пользователь выберет один из элементов меню. По истечении этого интервала, если пользователь так и не сделал выбора, будет загружен элемент меню, выбираемый по умолчанию.

Другие опции командной строки BCDEdit, а также практические примеры, иллюстрирующие работу с этой утилитой, будут приведены в *главе 11*.

Загрузочное меню Windows 7

Загрузочное меню Windows 7 очень похоже на меню, отображаемое Менеджером загрузки Windows Vista, и оба этих меню в чем-то подобны загрузочному меню, которое выводил загрузчик Ntldr в Windows 2000/XP. Впрочем, конечно, загрузочное меню Windows 7 изменилось и стало более удобным и функциональным (рис. 7.5).

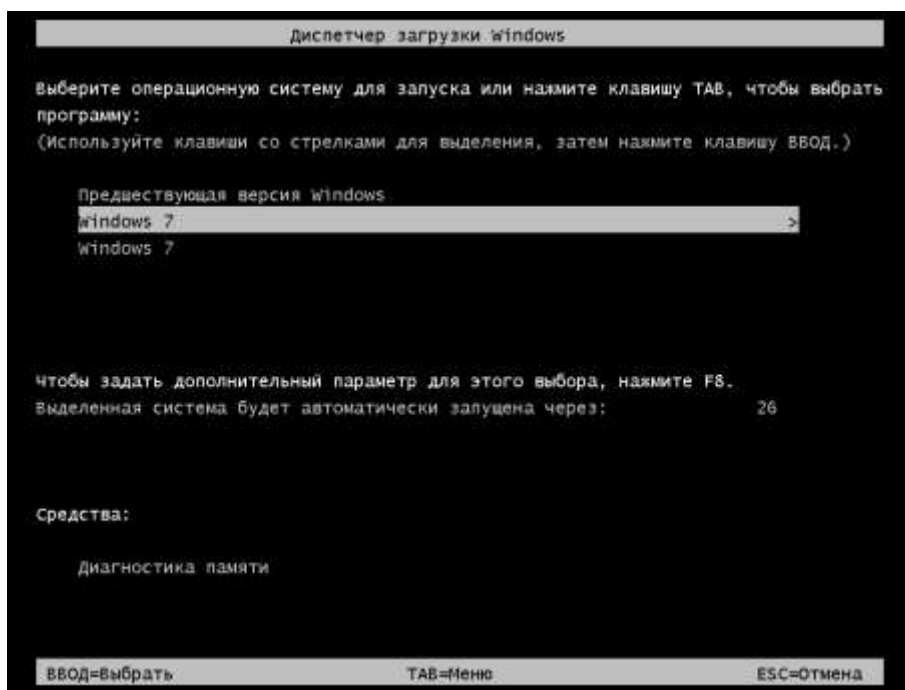


Рис. 7.5. Загрузочное меню Windows 7

Обратите внимание, что, начиная с Windows Vista, загрузочное меню содержит новый пункт — **Средства** (Tools). В стандартной конфигурации в составе этого пункта есть лишь один подпункт **Диагностика памяти** (Windows Memory Diagnostic), выбрав который можно запустить встроенную предзагрузочную программу Windows Vista/7 для тестирования оперативной памяти компьютера (Memtest.exe). Следует отметить, что OEM-производители могут добавлять в состав предзагрузочной среды Windows (Windows Vista/7 Pre-boot eXecution Environment) дополнительные приложения.

В верхней части загрузочного меню традиционно содержится список операционных систем, которые может запустить Менеджер загрузки. Если на ком-

пьютере присутствует не только Windows 7, но и Windows Vista, то в меню будет присутствовать пункт **Microsoft Windows Vista**. Если в дополнение к этому установлена и еще какая-нибудь версия Windows, более ранняя, чем Vista, то в меню будет присутствовать и пункт **Предшествующая версия Windows** (Earlier version of Windows). При выборе этого пункта меню управление будет передано загрузчику Ntldr, который прочтет файл boot.ini, после чего процесс загрузки пойдет образом, обычным для более ранних версий Windows. В примере, показанном на рис. 7.5, на компьютере установлена Windows XP и две различных копии Windows 7.

Выбор операционной системы, которую требуется запустить, ничем не отличается от аналогичного процесса при работе с Windows Vista и еще более ранними версиями Windows. Операционная система, указанная в базе данных загрузочной конфигурации как система, загружаемая по умолчанию, изначально подсвечивается курсором. Чтобы выбрать для запуска другую операционную систему, воспользуйтесь клавишами перемещения курсора (<↑> и <↓>), выберите нужную операционную систему и нажмите клавишу <Enter>.

Если вы не выберете ни один из пунктов меню к тому моменту, когда счетчик, указанный в строке:

Выделенная система будет автоматически запущена через: 22

(Seconds until highlighted choice will be started automatically: 22)

достигнет нуля, то менеджер загрузки начнет запуск операционной системы по умолчанию.

Все элементы загрузочного меню, включая операционные системы, которые можно загрузить, и дополнительные программы, которые можно запустить, описываются полями хранилища BCD.

Опции отладочного меню при загрузке Windows 7

В загрузочном меню Windows 7 (см. рис. 7.5), как и в Windows Vista, а также в предшествующих версиях Windows 2000/XP, имеется возможность выбрать дополнительные варианты загрузки, нажав клавишу <F8>. При этом на экране отобразится отладочное меню, показанное на рис. 7.6. Это меню останется на экране до тех пор, пока не будет выбрана одна из опций.

СОВЕТ

Если на компьютере установлена только одна копия системы Windows 7, то, как и в случае с более ранними версиями систем из семейства Windows NT, меню начального запуска отображаться не будет. В этом случае Windows 7 игнорирует значение тайм-аута, указанное в базе данных BCD, и запускается сразу же.

Тем не менее, если вам требуется получить доступ к опциям, предоставляющим дополнительные варианты загрузки, вы и в этом случае можете воспользоваться клавишей <F8>. Единственная проблема здесь заключается в том, что ее нужно успеть нажать в течение первых двух секунд загрузки Windows. Чтобы успеть это сделать (а это нелегко), нажмите клавишу <F8>, когда еще не завершились процедуры самотестирования при включении, и удерживайте ее нажатой до тех пор, пока не появится меню.

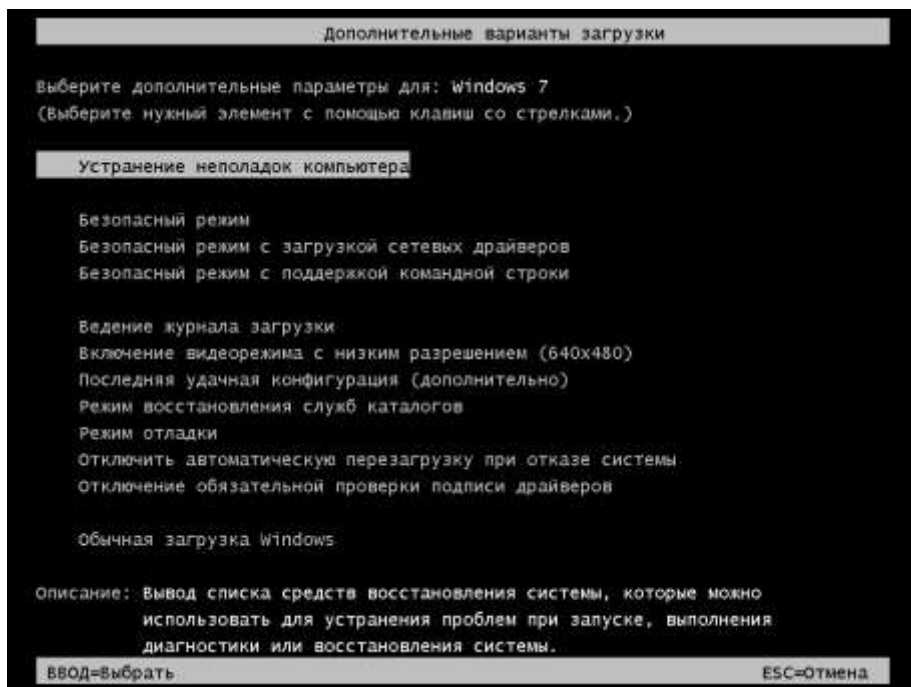


Рис. 7.6. Отладочное меню Windows 7, позволяющее выбрать дополнительные варианты загрузки операционной системы

Если вы хоть немного поработали с Windows Vista, то легко обнаружите, что отладочное меню Windows 7 очень похоже на аналогичное меню Vista, с одним лишь отличием — в нем первым пунктом стоит строка **Устранение неполадок компьютера** (Troubleshoot computer problems), которой в Windows Vista не было. Эта опция меню запускает уже упомянутую ранее среду восстановления Windows (WinRE) — набор инструментов с графическим пользовательским интерфейсом, позволяющих выявить и ликвидировать проблемы, препятствующие загрузке системы. Если вы выберете эту опцию, то сначала на экране откроется окно, предлагающее выбрать метод ввода с клавиатуры (рис. 7.7).

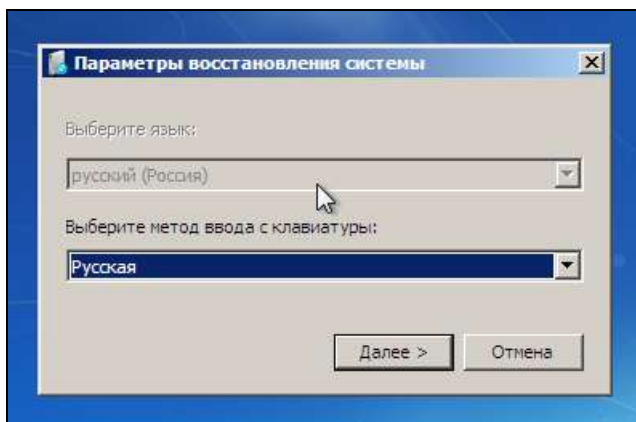


Рис. 7.7. Первое окно, появляющееся при запуске WinRE, предлагает выбрать метод ввода с клавиатуры

После того как вы выберете метод ввода с клавиатуры, вам будет предложено выбрать учетную запись пользователя для регистрации в системе и ввести пароль этого пользователя (рис. 7.8).

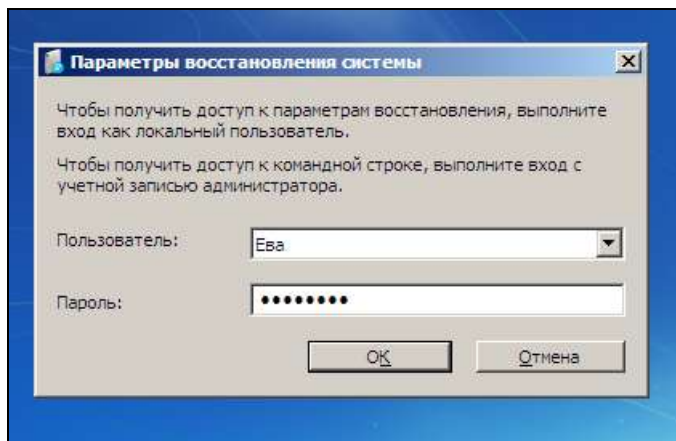


Рис. 7.8. Ввод пароля пользователя для доступа к среде восстановления системы

После того как вы введете правильный пароль, на экране откроется окно WinRE (рис. 7.9), очень похожее на аналогичное окно в Windows Vista. Обратите внимание на то, что это — пусть маленькое, но очень приятное усовершенствование, обеспечивающее более быстрый и удобный доступ к среде восстановления системы, нежели в Windows Vista.

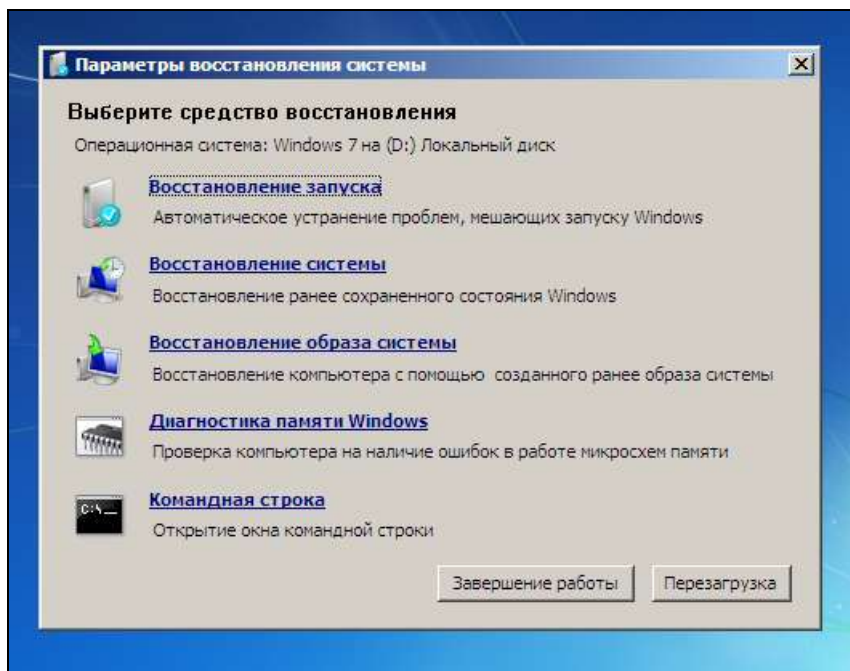


Рис. 7.9. Среда восстановления системы

Остальные опции меню дополнительных вариантов загрузки (см. рис. 7.6) аналогичны существовавшим в Windows Vista. Рассмотрим их чуть более подробно.

При загрузке в безопасном режиме (Safe Mode) Windows использует стандартные параметры настройки (монитор VGA, без сетевых средств, с минимальным количеством драйверов — фактически, запускаются только драйверы, абсолютно необходимые для загрузки Windows). Идея, лежащая в основе безопасного режима загрузки, заключается в том, что одной из наиболее распространенных причин, препятствующих успешной загрузке, является несовместимый с системой или поврежденный сервис/драйвер. Таким образом, безопасный режим повышает вероятность успешной загрузки, поскольку загружается усеченная версия операционной системы с минимальным набором сервисов и драйверов. Например, если после инсталляции нового программного обеспечения операционная система перестала запускаться, то вполне возможно, что попытка загрузки в безопасном режиме завершится удачно. После загрузки вы сможете изменить параметры настройки компьютера, не позволяющие выполнить корректную загрузку ОС, или удалить программное обеспечение, вызвавшее эти проблемы.

Остальные опции дополнительного меню загрузки Windows Vista и Windows 7 с их краткими описаниями перечислены далее:

- ❑ **Безопасный режим (Safe Mode)** — загружаются только базовые файлы и драйверы, абсолютно необходимые для работы Windows (стандартные драйверы мыши и клавиатуры, накопителей, базовый драйвер видеоадаптера VGA и минимальный объем стандартных системных сервисов). Если операционную систему невозможно загрузить даже в этом режиме, то, вероятнее всего, придется прибегнуть к процедуре восстановления поврежденной системы;
- ❑ **Безопасный режим с загрузкой сетевых драйверов (Safe Mode with Networking)** — Windows начнет загружаться в безопасном режиме (почти так же, как и в предыдущем режиме), но в дополнение делается попытка запуска сетевых служб и восстановления сетевых соединений;
- ❑ **Безопасный режим с поддержкой командной строки (Safe Mode with Command Prompt)** — запуск Windows с использованием только базовых файлов и драйверов, и вместо графического интерфейса Windows отображает на экране командную строку;
- ❑ **Ведение журнала загрузки (Enable Boot Logging)** — в процессе запуска Windows в каталоге %Systemroot% будет создан файл ntbtlog.txt с информацией о сервисах и драйверах, которые были запущены успешно, а также о тех, запуск которых завершился неудачей;
- ❑ **Включение видеорежима с низким разрешением (640×480) (Enable low resolution video (640×480))** — позволяет запустить Windows с низким разрешением экрана;

Последняя удачная конфигурация (дополнительно) (Last Known Good Configuration (Advanced)) — Windows запускается с использованием информации реестра, сохраненной после того, как система в последний раз была успешно загружена. Ее рекомендуется использовать только в тех случаях, когда точно известно, что допущена конфигурационная ошибка. Дело тут в том, что перед обновлением текущего набора драйверов Windows создает резервные копии всех установленных драйверов. Кроме восстановления самых последних установок реестра, опция начальной загрузки **Последняя удачная конфигурация (дополнительно)** также восстанавливает самый последний набор драйверов, который использовался после последней успешной регистрации пользователя. Это позволяет избавиться от системных ошибок, вызванных неверно установленными приложениями и драйверами, препятствующими запуску Windows. Однако проблемы, вызванные отсутствием или повреждением системных файлов или драйверов, этим способом не исправить. Кроме того, следует помнить,

что в случае применения данной опции все изменения, внесенные позже последней успешной загрузки Windows, будут потеряны;

ПРИМЕЧАНИЕ

Как уже говорилось, запись последней удачной конфигурации производится немедленно после успешной регистрации пользователя в системе. Поэтому если запуск системы произошел с проблемами (в ходе запуска появлялись сообщения об ошибках), а пользователь после этого зарегистрировался в системе, опция **Последняя удачная конфигурация (дополнительно)** станет неэффективной, поскольку действительно удачная конфигурация будет перезаписана проблематичной.

- ☐ **Режим восстановления служб каталогов (только для контроллеров домена Windows)** (Directory Services Restore Mode) — не следует использовать на рабочих станциях Windows Vista или Windows 7, поскольку она предназначена для контроллеров доменов, функционирующих под управлением операционных систем из линейки серверных платформ. Как следует из названия этой опции, она служит для восстановления служб каталога;
- ☐ **Режим отладки (Debugging Mode)** — запускает Windows в отладочном режиме и активизирует отладчик ядра для передачи отладочной информации на удаленный компьютер;
- ☐ **Отключить автоматическую перезагрузку при отказе системы** (Disable automatic restart on system failure) — эта опция позволяет выполнить стандартный запуск операционной системы, но при возникновении критической ошибки типа **STOP** не перезагружать компьютер автоматически, а отобразить так называемый "синий экран смерти" (Blue Screen of Death, BSOD);
- ☐ **Отключение обязательной проверки подписи драйверов** (Disable Driver Signature Enforcement) — если выбрать этот элемент меню, то будет отключена обязательная проверка цифровой подписи драйверов в процессе загрузки системы. Таким образом, драйвер будет загружен и в том случае, если он содержит неверную цифровую подпись;
- ☐ **Обычная загрузка Windows** (Start Windows Normally) — эта опция впервые появилась в Windows XP и по-прежнему присутствует в Windows Vista и Windows 7. Она позволяет запускать ОС в обычном режиме.

Хранение информации о загрузочном меню в реестре

Где же хранятся настройки загрузочного и отладочного меню Windows Vista и Windows 7? Вероятно, ответ не покажется слишком уж неожиданным — как и все системные параметры, эти настройки находятся в реестре. Ключ

реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot` (рис. 7.10) содержит параметры конфигурации при загрузке в безопасном режиме. В его составе имеются вложенные ключи `Network` и `Minimal`. Как несложно догадаться, ключ `Network` содержит информацию, необходимую для загрузки при выборе опции **Безопасный режим с загрузкой сетевых драйверов** (Safe Mode with Networking), а ключ `Minimal` — ту же самую информацию, за исключением данных о сетевых параметрах. Помимо этого, в составе ключа `SafeBoot` имеется параметр `AlternateShell`, указывающий имя программы, которая используется вместо графической оболочки Windows. Как правило, значение этого параметра устанавливается равным `cmd.exe` (командный процессор Windows), что соответствует опции отладочного меню **Безопасный режим с поддержкой командной строки** (Safe Mode with Command Prompt).

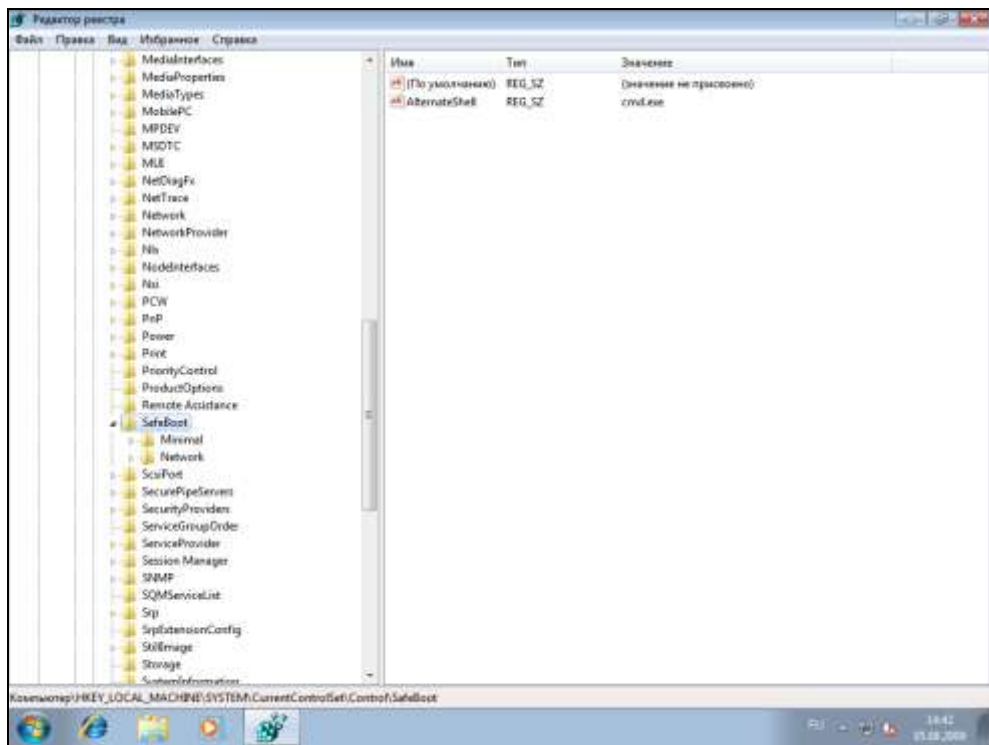


Рис. 7.10. Опции отладочного меню в Windows 7, как и в предшествующих версиях Windows 2000/XP/Vista, заданы ключом реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot`

ПРИМЕЧАНИЕ

Чтобы узнать, с какими опциями загрузочного меню была запущена работающая система, просмотрите, какое значение имеет параметр реестра `SystemStartOptions` под ключом `HKLM\System\CurrentControlSet\Control`. В примере, показанном на рис. 7.11, работающая копия системы Windows 7 была загружена с использованием опции **Ведение журнала загрузки** (Enable Boot Logging).

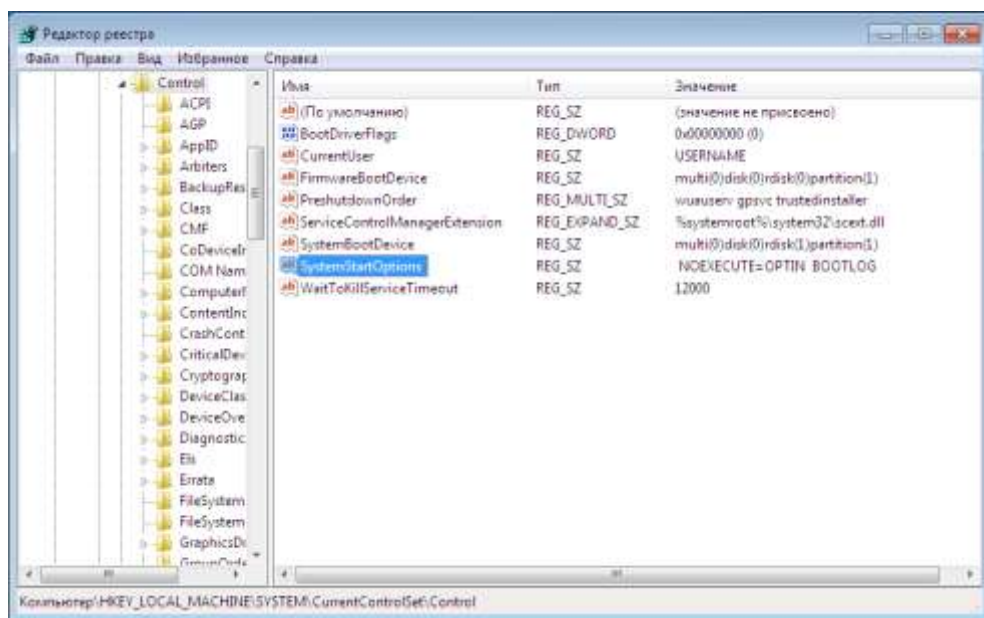


Рис. 7.11. Параметр реестра `SystemStartOptions` под ключом `HKLM\System\CurrentControlSet\Control` показывает, какая из опций меню дополнительных опций загрузки была выбрана в этот раз

Работа загрузчика *Winload.exe*

`Winload`, новый загрузчик ядра, введенный с выпуском Windows Vista, загружает ядро операционной системы (`Ntldr.exe`), необходимые драйверы, которые должны загружаться на ранних стадиях запуска системы, а также утилиты реестра. Таким образом, `Winload.exe` выполняет вторую часть задач, которые в более ранних системах из семейства Windows NT выполнялись загрузчиком `Ntldr`.

ПРИМЕЧАНИЕ

Фактически, файл `Winload.exe` способен загружать и ядра более ранних систем из семейства Windows NT. Так, в ранних бета-версиях Windows Vista (до введения базы данных BCD), по-прежнему использовался файл `boot.ini`, причем он

был разбит на два раздела. В первом разделе перечислялись операционные системы, которые могли загружаться с помощью старого загрузчика Ntldr, а во втором — операционные системы, для которых требовался загрузчик Winload.exe. Бета-тестеры обнаружили, что, например, Windows XP Service Pack 2 и Windows Server 2003 успешно загружались при помощи Winload.exe (разумеется, если в файле boot.ini эти системы указывались как загружаемые с помощью Winload.exe), а сам этот файл был скопирован в каталог %SystemRoot%\System32 в соответствующем разделе.

По своей структуре загрузчик Winload.exe существенно проще, чем Ntldr. В число задач, выполняемых Ntldr, входят разбор файла boot.ini, выбор загружаемой операционной системы (в мультизагрузочных системах), выход из режима гибернации, а также отображение загрузочного меню и, наконец, осуществление загрузки выбранной операционной системы. Загрузчик Winload.exe от этих задач освобожден, и они переданы другим компонентам — Менеджеру загрузки (Bootmgr) и приложению Winresume.exe, выводящему систему из спящего режима. Winload.exe выполняет лишь последнюю из задач Ntldr — фактическую загрузку операционной системы.

Winload.exe даже не должен выполнять переключение в защищенный режим. Как вы помните, в 32-разрядных системах x86, загрузчик Ntldr инициировался кодом загрузочного сектора и начинал работу в 16-разрядном реальном режиме. Поэтому он состоял из добавленной в начало загрузчика "заглушки" реального режима (real-mode stub executable), которая переключала процессор в защищенный режим и устанавливала 32-разрядную плоскую модель памяти, и только затем запускала собственно загрузчик, который и выполнял остальные задачи. С вводом Winload.exe необходимость в этом отпала. Теперь переключение в защищенный режим выполняется или микропрограммным обеспечением EFI (на платформах Itanium), или Менеджером загрузки Bootmgr (на платформах x86).

Загрузка ядра

Winload.exe загружает в память ядро операционной системы — файл %SystemRoot%\System32\ntoskrnl.exe, уровень аппаратных абстракций %SystemRoot%\System32\hal.dll, содержимое улья реестра %SystemRoot%\System32\config\system, все драйверы устройств, загружающиеся на ранних стадиях запуска системы, а также все DLL режима ядра, импортируемые любыми из ранее упомянутых компонентов.

Однако в первую очередь загрузчик Winload.exe загружает в память улей реестра SYSTEM. Сразу же после этого он выполняет верификацию собственного образа, загруженного в память. Для этой цели он сверяет свою цифровую подпись с цифровой подписью, хранящейся в файле каталога цифровых

подписей `%SystemRoot%\system32\CatRoot\F750E6C3-38EE-11D1-85E5-00C04FC295EE\nt5.cat`. Если эти подписи не совпадают, процесс загрузки системы останавливается, за исключением случаев, когда активизирован режим отладки на уровне ядра.

После этой проверки `Winload.exe`, как уже было сказано, загружает ядро операционной системы, уровень аппаратных абстракций, а также все импортируемые ими DLL уровня ядра. Если активизирован режим отладки ядра, то `Winload.exe`, в дополнение к перечисленным компонентам, загружает ряд отладочных библиотек: `%SystemRoot%\system32\kdcom.dll`, `%SystemRoot%\system32\kd1394.dll` и `%SystemRoot%\system32\kdbus.dll`, которые активизируют отладку ядра с коммуникациями через последовательные порты RS232, IEEE 1394 и USB, соответственно.

В ходе загрузки компонентов `Winload.exe` проверяет соответствие образов всех файлов цифровым подписям, содержащимся в уже упомянутом каталоге цифровых подписей `%SystemRoot%\system32\CatRoot\F750E6C3-38EE-11D1-85E5-00C04FC295EE\nt5.cat`. Проверка цифровой подписи осуществляется кодом, который загружает файлы в память. Если проверка оказывается неудачной, `Winload.exe` останавливает процесс загрузки, за исключением случаев, когда активизирован режим отладки на уровне ядра. При этом даже если режим отладки активизирован, `Winload.exe` все равно остановит работу, если проверка окажется неудачной хотя бы для одного из следующих файлов: `winload.exe`, `ntoskrnl.exe`, `hal.dll`, `bootvid.dll`, `tpm.sys`, `ksecdd.sys`, `clfs.sys`, `ci.dll`, `kdcom.dll`, `kdbus.dll`, `kd1394.dll` и `spldr.sys`.

О начале фазы загрузки ядра сигнализирует появление на экране загрузочной анимации — в Windows Vista это был анимированный индикатор степени завершенности загрузки ядра и уровня аппаратных абстракций (рис. 7.12).

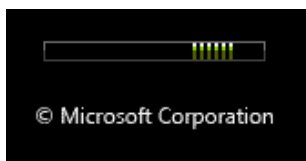


Рис. 7.12. Начало фазы загрузки ядра — загрузочная анимация Windows Vista

В Windows 7 загрузочная анимация существенно "похорошела" (рис. 7.13). Наверняка вы заметили, что сначала на экране появляются 4 разноцветных движущихся точки, которые меняют свою форму и размер и, наконец, формируют светящийся логотип Windows. Помимо новой анимации, на этой фазе между загрузочными экранами Windows 7 и Windows Vista имеются и неко-

торые "физические" отличия (какими бы несущественными они вам ни показались, они потребовали переработки кода). Так, разрешение картинки в Windows 7 теперь составляет 1024×768 (в Windows Vista разрешение составляло 640×480), а звук, воспроизводимый при запуске, теперь синхронизирован с анимацией (в Windows Vista воспроизведение было асинхронным). Глубина цветности в Windows Vista составляла 16 bpp (bits per pixel), а в Windows 7 она была увеличена до 32 bpp.

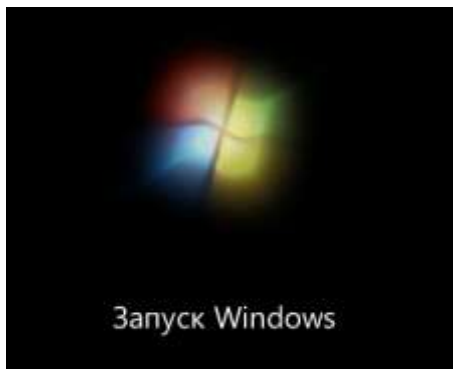


Рис. 7.13. Начало загрузки ядра — загрузочная анимация Windows 7

ПРИМЕЧАНИЕ

Если вы считаете, что эти изменения носят лишь косметический характер, то вы заблуждаетесь. Разработчики Windows 7 очень серьезно поработали над оптимизацией процесса загрузки и существенно ускорили его. В действительности, совершенствование этой загрузочной анимации фактически стало возможным лишь благодаря проделанной работе — если бы не эти принципиально новые подходы, то анимационная заставка осталась бы точно такой же аскетичной, какой она и была в Windows Vista. Фактически, в Windows 7 загрузчик использует принципиально иной метод для показа загрузочной анимации — и это делается еще до того, как в память будет загружен и инициализирован "родной" драйвер видеокарты. Эта работа выполняется процессором параллельно загрузке и инициализации драйверов, что свидетельствует о том, что разработчики Windows 7 проделали очень большую работу по оптимизации кода загрузчика и его взаимодействию с процессором. Более подробно об этом можно прочесть в блоге разработчиков Windows 7 по адресу <http://blogs.msdn.com/e7/archive/2009/02/18/engineering-the-windows-7-boot-animation.aspx>.

На этапе загрузки ядра и уровня аппаратных абстракций они еще не инициализированы. Далее загрузчик просматривает реестр, извлекает информацию о заданных по умолчанию или определенных пользователем размерах *резидентного пула памяти* (nonpaged pool) и загружает улей реестра `HKEY_LOCAL_MACHINE\SYSTEM` из каталога `%SystemRoot%\System32\Config`.

Затем загрузчик активизирует API для работы с реестром и создает *набор опций управления* (control set), который будет использоваться для инициализации компьютера. Эти задачи являются подготовительными для загрузки драйверов. Значение, заданное в ключе реестра `HKEY_LOCAL_MACHINE\SYSTEM\Select` (рис. 7.14), определяет, какой набор опций управления из перечисленных в ключе `HKEY_LOCAL_MACHINE\SYSTEM` должен быть задействован при загрузке. По умолчанию загрузчик выбирает набор опций управления, определяемый значением `Default`. Если пользователь выбрал опцию **Последняя удачная конфигурация (дополнительно)** (Last Known Good Configuration (Advanced)), то загрузчик использует набор опций управления, определяемых значением `LastKnownGood`. На основании сделанного пользователем выбора и значений подключа `Select` загрузчик определяет, какой из наборов опций управления (`ControlSet00x`) будет активизирован. После этого загрузчик устанавливает значение `Current` подключа реестра `Select` на номер набора управляющих опций, который он будет использовать.

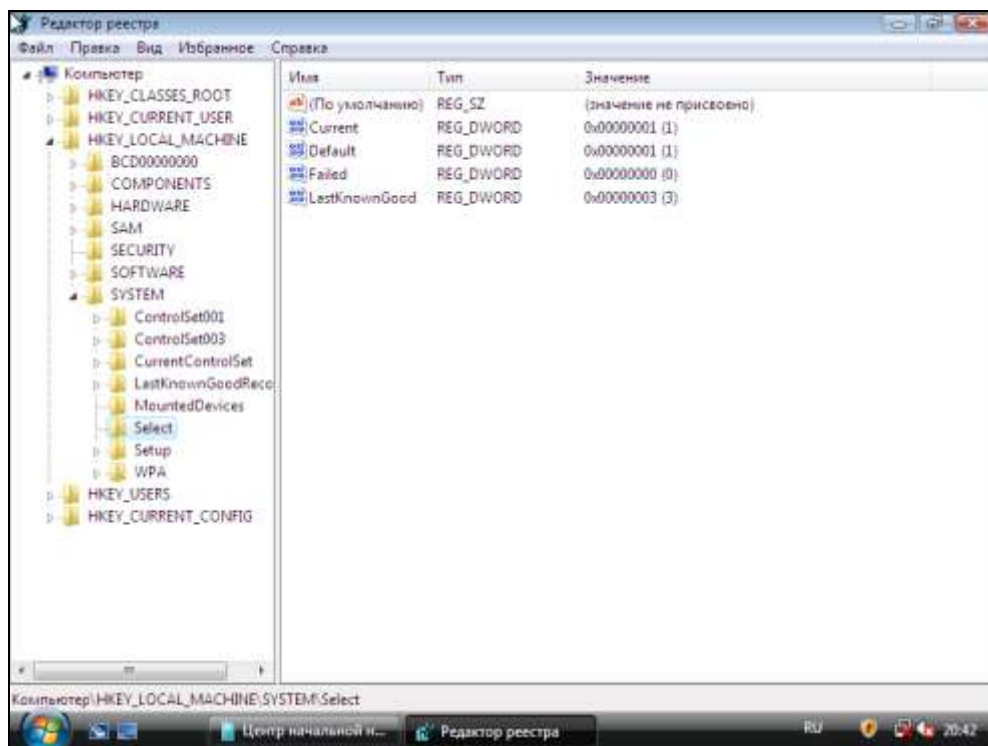


Рис. 7.14. Ключ реестра `HKEY_LOCAL_MACHINE\SYSTEM\Select`

Далее загрузчик сканирует все сервисы (службы), определенные ключом реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services`, и ищет драйверы устройств, для которых значение параметра `Start` равно `0x0`. Этот параметр располагается под следующим ключом реестра:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ServiceName`

Здесь *ServiceName* представляет собой имя сервиса, например:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\atapi`

Как правило, драйверы с такими значениями представляют собой низкоуровневые драйверы устройств, например, драйверы дисков. Значение параметра `Group` для каждого драйвера устройства определяет порядок, в котором загрузчик должен его загружать. Ключ реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ServiceGroupOrder` определяет порядок загрузки.

К моменту завершения этой фазы все базовые драйверы загружены и активны, за исключением случаев, когда один из критически важных драйверов не инициализировался, вследствие чего началась перезагрузка системы.

Наконец, `Winload.exe` активизирует *подкачку* (paging) и передает управление ядру операционной системы.

Инициализация ядра

В общих чертах процессы, происходящие при инициализации ядра Windows 7, во многом аналогичны процессам, которые имели место при инициализации ядра Windows Vista, да и ядер более ранних версий операционных систем из семейства Windows NT. Впрочем, отличия действительно имеются, и они будут подчеркнуты далее по ходу изложения.

Ядро создает ключ `HKEY_LOCAL_MACHINE\HARDWARE` на основании информации, полученной от загрузчика. Ключ `HKEY_LOCAL_MACHINE\HARDWARE` содержит данные об аппаратных средствах, распознавание которых осуществляется каждый раз при запуске системы. В состав этих данных входит информация об аппаратных компонентах на системной плате и о прерываниях, используемых конкретными аппаратными устройствами.

Ядро создает также набор опций управления `Clone`, копируя в него опции управления из набора `CurrentControlSet`. Набор опций управления `Clone` никогда не модифицируется, т. к. он должен представлять собой полностью идентичную копию данных, которые использовались для конфигурирования компьютера.

ПРИМЕЧАНИЕ

В Windows NT 4.0 набор опций управления `Clone` был виден в составе реестра, но после успешной загрузки он становился недоступным, и при попытке его

открытия выводилось сообщение о невозможности это сделать. Начиная с Windows 2000/XP, набор опций управления Clone просто не отображается редакторами реестра.

Операции, осуществляемые на стадии инициализации ядра

На стадии инициализации ядро выполняет следующие операции:

- ☐ запрос к уровню аппаратных абстракций (HAL) на инициализацию контроллера прерываний;
- ☐ инициализация Диспетчера памяти (Memory Manager), Диспетчера объектов (Object Manager), Монитора подсистемы безопасности (Security Reference Monitor), а также Диспетчера процессов (Process Manager);
- ☐ запрос к HAL на активизацию прерываний;
- ☐ переинициализация Диспетчера объектов (Object Manager);
- ☐ инициализация исполняющей подсистемы (модуля Executive);
- ☐ инициализация микроядра (Microkernel);
- ☐ переинициализация Монитора подсистемы безопасности (Security Reference Monitor);
- ☐ переинициализация Диспетчера памяти (Memory Manager);
- ☐ инициализация Диспетчера кэша (Cache Manager);
- ☐ инициализация системы локальных вызовов процедур (Local Procedure Call, LPC);
- ☐ инициализация Диспетчера ввода/вывода (I/O Manager). При этом Диспетчер ввода/вывода, в свою очередь, инициализирует все предварительно загруженные драйверы устройств;
- ☐ инициализация Диспетчера процессов (Process Manager).

Затем ядро операционной системы сканирует копию реестра, загруженную в память Winload.exe, и загружает все драйверы устройств, принадлежащие к классу `system`.

Ядро проверяет цифровые подписи всех файлов, из которых производится загрузка драйверов устройств. Для этой цели используются процедуры, экспортированные из `ci.dll`, — DLL режима ядра, которая предоставляет библиотечные функции для проверки целостности кода.

Наконец, ядро инициирует первый пользовательский процесс, так называемую *подсистему диспетчера сеансов* (Session Manager Subsystem, SMSS).

Загрузка и инициализация драйверов устройств

Ядро (Ntoskrnl.exe) инициализирует низкоуровневые драйверы устройств, которые были загружены на стадии загрузки ядра. В случае ошибки при инициализации одного из драйверов система предпринимает корректирующее действие, основываясь на данных, определенных параметром реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DriverName\ErrorControl`.

Далее Ntoskrnl.exe сканирует реестр, на этот раз — в поисках драйверов устройств, для которых значение ключа реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DriverName\Start` установлено как `0x01`. Значение `Group` для каждого драйвера устройства определяет порядок, в котором производится их загрузка. Ключ реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ServiceGroupOrder` определяет порядок загрузки.

В отличие от фазы загрузки ядра, драйверы устройств, для которых параметр `Start` имеет значение `0x01`, загружаются не за счет вызовов BIOS, а с помощью драйверов устройств, загруженных на стадии загрузки ядра и только что инициализированных на этой стадии. Обработка ошибок в процессе инициализации этой группы драйверов устройств также основана на значении элемента `ErrorControl` для соответствующих драйверов устройств.

ПРИМЕЧАНИЕ

Windows осуществляет одновременную инициализацию драйверов, что сокращает время загрузки. Системе не нужно ожидать окончания инициализации каждого устройства, т. к. многие устройства позволяют проводить параллельную инициализацию. При этом на время загрузки определяющее влияние оказывает "самое медленное" устройство.

Инициализация пользовательского режима

При инициализации пользовательского режима параллельно и согласованно выполняется целый ряд процессов. Как уже говорилось, первый из этих процессов — подсистема Диспетчера сеансов (SMSS). Она запускает остальные процессы, которые, в свою очередь, запускают другие процессы. Все эти процессы запускаются и работают от имени учетной записи `LocalSystem`. Если запуск одного из исполняемых процессов от имени этой учетной записи завершается неудачей, то завершится неудачей и весь процесс инициализации системы.

Процесс SMSS использует API ядра (native kernel API) для запуска высокоуровневых подсистем — в том числе: Win32, 16-разрядной подсистемы OS/2 и подсистемы POSIX, а также сервисов (служб) операционной системы.

В первую очередь SMSS монтирует файлы ульев реестра. Когда SMSS монтирует улей `SYSTEM`, ядро комбинирует его с копией этого улья, загруженной

в память загрузчиком Winload.exe. Таким образом, все дополнения и изменения (но не удаленные подключи и параметры), внесенные в эту часть реестра на предшествующих этапах загрузки, вносятся в системный реестр. Информация, предназначенная для Диспетчера сеансов, находится под ключом реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager`.

Диспетчер сеансов исполняет инструкции, которые содержатся в следующих элементах реестра:

- ☐ параметр `BootExecute`;
- ☐ ключ `Memory Management`;
- ☐ ключ `DOS Devices`;
- ☐ ключ `SubSystems`.

Параметр реестра *BootExecute*

Параметр реестра `BootExecute`, расположенный в составе ключа `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager`, указывает одну или несколько программ, которые Диспетчер сеансов (`Smss.exe`) должен запустить во время загрузки (*boot-time programs*). Значением по умолчанию для этого элемента является `Autochk.exe` — вариант утилиты `Chkdsk.exe` для операционных систем из семейства Windows NT. Следующий пример показывает установку этого значения, задаваемую по умолчанию:

```
BootExecute: REG_MULTI_SZ: autocheck autochk*
```

Диспетчер сеансов может запустить несколько программ. Следующий пример показывает запуск утилиты `Convert`, которая при следующем запуске системы преобразует том `x` из формата FAT в формат NTFS:

```
BootExecute: REG_MULTI_SZ: autochk autochk* autoconv \DosDevices\х:  
/FS:ntfs
```

SMSS запускает эти программы синхронно и прежде, чем продолжить выполнение остальных задач, ожидает их завершения.

Ключ *Memory Management*

Далее Диспетчер сеансов иницирует информацию о файле подкачки, необходимую Диспетчеру виртуальной памяти. Конфигурационная информация располагается в следующих значимых элементах:

- ☐ `PagedPoolSize: REG_DWORD 0`;
- ☐ `NonPagedPoosSize: REG_DWORD 0`;
- ☐ `PagingFiles: REG_MULTI_SZ: c:\pagefile.sys 32`.

Повышение производительности процесса загрузки в Windows Vista и Windows 7

Начиная с Windows XP, Microsoft ввела возможность так называемой *быстрой загрузки* (Fast Boot), которая была реализована путем увеличения производительности загрузчика. В Windows XP версия загрузчика Ntldr была оптимизирована для выполнения быстрого считывания диска. При первой загрузке системы вся информация о конфигурации диска, включая системные метаданные, помещается в кэш. Программа упреждающей выборки — Logical Prefetcher, появившаяся в Windows XP, записывает большую часть этих данных в системный кэш, обладающий возможностью выполнения эффективных дисковых операций ввода/вывода в асинхронном режиме, что существенно снижает время поиска. Во время начальной загрузки программа предварительной выборки завершает большинство операций ввода/вывода, необходимых для запуска системы, параллельно с инициализацией устройства, обеспечивая ускоренную начальную загрузку и регистрацию пользователя. Более того, каждый системный файл во время начальной загрузки считывается только один раз — за одну операцию. В результате, загрузчик Windows XP стал работать примерно в 4–5 раз быстрее загрузчика Windows 2000.

В ОС Windows Vista впервые были представлены четыре новые технологии увеличения производительности: SuperFetch, ReadyBoost, ReadyBoot и ReadyDrive. С точки зрения повышения производительности процесса загрузки особый интерес представляют технологии SuperFetch, ReadyBoost и ReadyBoot. Разумеется, все эти технологии реализованы и в Windows 7. Рассмотрим их чуть подробнее.

- ❑ Функция SuperFetch основывается на технологии упреждающей выборки (Prefetch), впервые появившейся в Windows XP. Однако ее преимущество перед технологией упреждающей выборки Windows XP состоит в том, что, кроме статистики недавнего доступа, она учитывает и историю обращений к памяти за длительный период времени.
- ❑ Функция ReadyBoost, впервые добавленная в Windows Vista, дает возможность воспользоваться преимуществами запоминающих устройств на основе флэш-памяти, чтобы создать на них промежуточный кэш, логически расположенный между оперативной памятью и жестким диском. Дело в том, что хотя RAM и идеально подходит для кэширования дисковых данных, ее стоимость выше, чем стоимость флэш-памяти. При этом время произвольного доступа у флэш-памяти примерно на порядок меньше, чем у жесткого диска. К числу поддерживаемых устройств относятся устройства USB Flash, флэш-карты Secure Digital, Compact Flash, а также внутренние карты PCI Express.

- ❑ Функция ReadyBoot, впервые введенная в Windows Vista, как и следует из ее названия, предназначена для ускорения процесса загрузки. Если в системе установлено менее 512 Мбайт оперативной памяти, то механизм упреждающего чтения при загрузке Windows Vista ничем не отличается от механизма, использовавшегося при загрузке ОС Windows XP. Однако если размер оперативной памяти превышает 700 Мбайт, то процесс загрузки оптимизируется за счет создания кэша в RAM. Размер этого кэша зависит от общего объема доступной памяти — он достаточно велик, чтобы обеспечить эффективное кэширование, но оставляет при этом достаточно свободной памяти для нормального выполнения процедуры загрузки системы. Как правило, использование функции ReadyBoot обеспечивает повышение производительности загрузки на 20% по сравнению с Windows XP.
- ❑ Функция ReadyDrive, также впервые появившаяся в Windows Vista, предназначена для поддержки возможностей новых, так называемых *гибридных* жестких дисков (дисков H-HDD). Гибридный жесткий диск представляет собой жесткий диск со встроенной энергонезависимой флэш-памятью, известной также под названием NVRAM (рис. 7.15). Как правило, гибридные жесткие диски содержат от 50 Мбайт до 512 Мбайт кэш-памяти, но ОС Windows Vista поддерживает кэши размером до 2 Тбайт. Кэш активен, даже когда диск остановлен, и система может использовать флэш-память для кэширования записи на диск — это позволяет не раскручивать диск, если компьютер питается от аккумулятора. Кэш диска может использоваться для хранения данных SuperFetch, что ускоряет загрузку приложений. При остановке системы этот кэш служит местом хранения данных загрузки, что позволяет ускорить последующий запуск системы. Наконец, при переходе в спящий режим, в кэше может храниться часть данных гибернации, что позволяет ускорить выход из спящего режима.

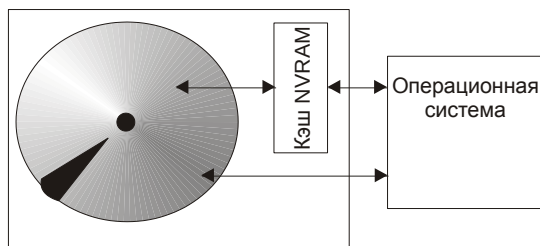


Рис. 7.15. Гибридный жесткий диск со встроенной энергонезависимой флэш-памятью

Функция SuperFetch

Как несложно предположить, параметры всех функций увеличения производительности также хранятся в реестре. В частности, параметры функции SuperFetch находятся в реестре (рис. 7.16) под следующим ключом:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
\Session Manager\Memory Management\PrefetchParameters
```

Нас интересуют, прежде всего, параметры `EnablePrefetcher` и `EnableSuperfetch` (оба параметра имеют тип данных `REG_DWORD`). Параметр `EnablePrefetcher` управляет опциями упреждающей выборки в стиле Windows XP, а параметр `EnableSuperfetch` — параметрами функции SuperFetch в Windows Vista и Windows 7. Оба параметра могут иметь следующие значения:

- ❑ `0x00000001` — активизирована соответствующая функция (предварительная выборка в стиле Windows XP или функция SuperFetch в стиле Windows Vista/7) при запуске приложения;
- ❑ `0x00000002` — активизирована соответствующая функция (предварительная выборка в стиле Windows XP или функция SuperFetch в стиле Windows Vista/7) при выполнении загрузки.

Если активизированы обе опции, то соответствующий параметр примет значение `0x00000003`. Данные установки вступают в силу немедленно. Обратите внимание, что на серверных системах по умолчанию установлена лишь опция предварительной выборки при начальной загрузке.

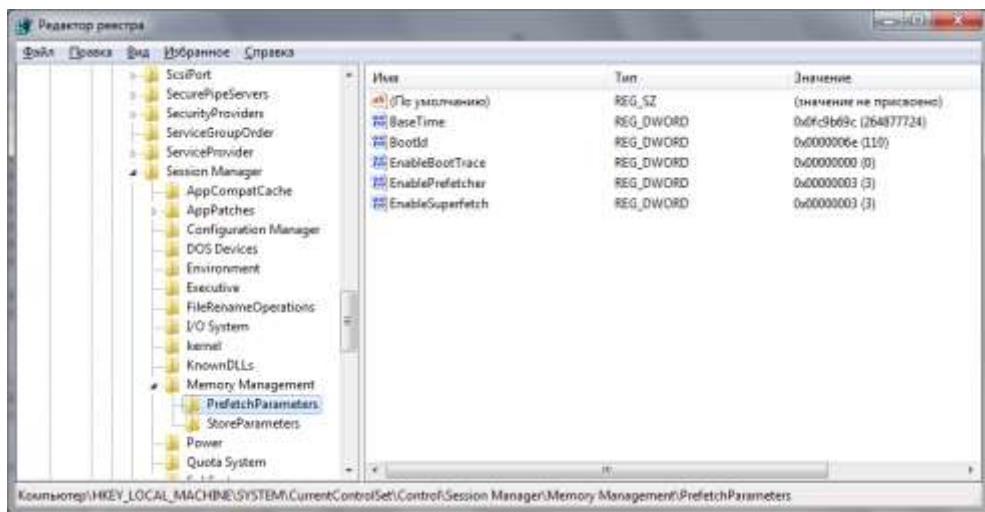


Рис. 7.16. Установки упреждающего чтения (Prefetching) в реестре Windows 7

Функция SuperFetch реализована в библиотеке %SystemRoot%\System32\Sysmain.dll. Выполняется она в качестве сервиса Windows внутри процесса Service Host (%SystemRoot%\System32\Svchost.exe). Сервис SuperFetch существенно расширяет отслеживание страниц памяти, учитывая страницы, которые были ранее загружены в память, но впоследствии освобождены диспетчером памяти для других данных и кода. Эта информация хранится в папке %SystemRoot%\Prefetch в виде файлов сценариев с расширением db вместе со стандартными файлами упреждающего чтения, используемыми для оптимизации запуска приложений. Располагая подробной информацией об использовании памяти, служба SuperFetch может осуществлять предварительную загрузку данных и кода при освобождении физической памяти.

Функция ReadyBoost

Функция ReadyBoost, основное назначение которой состоит в оптимизации работы с внешними устройствами памяти, определяет производительность запоминающего устройства на основе флэш-памяти и записывает результат в ключ реестра HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Emdmgmt (рис. 7.17). Состоит эта функция из сервиса Emdmgmt, реализованного в файле %SystemRoot%\System32\Emdmgmt.dll и выполняющегося в процессе Service Host, и драйвера фильтра томов %SystemRoot%\System32\Drivers\Ecache.sys (Windows Vista) или драйвера %SystemRoot%\System32\Drivers\Rdyboost.sys (Windows 7).

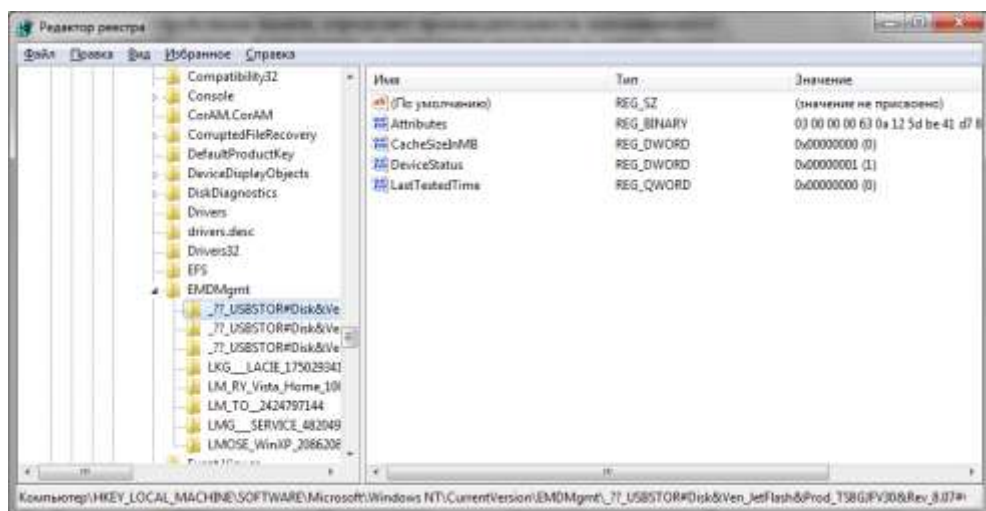


Рис. 7.17. Результаты тестирования производительности устройств на основе флэш-памяти в системном реестре

ПРИМЕЧАНИЕ

В процессе разработки функция ReadyBoost, предназначенная для оптимизации работы с внешними устройствами памяти, так и называлась — External Memory Device (EMD). Отсюда и название соответствующего сервиса — Endmgmt.

Функция ReadyBoot

Функция ReadyBoot, как и следует из ее названия, предназначена для ускорения процесса загрузки Windows Vista/7. После каждой загрузки системы служба ReadyBoost (та же самая служба, которая реализует и функцию ReadyBoost) планирует кэширование для следующей загрузки системы. Планирование это производится в моменты простоя процессора. Служба анализирует информацию об обращениях к файлам за пять предыдущих загрузок и определяет, к каким файлам производились обращения и где эти файлы расположены на диске. Обработанная информация об обращениях сохраняется в папке %SystemRoot%\Prefetch\ReadyBoot в виде файлов с расширением fx, а план кэширования сохраняется в разделе реестра HKLM\System\CurrentControlSet\Services\Ecache\Parameters (Windows Vista) или HKLM\System\CurrentControlSet\Services\Rdyboost\Parameters (Windows 7) в виде значений типа REG_BINARY с именами, соответствующими именам внутренних дисков.

Кэширование реализуется с помощью того же драйвера, что и в функции ReadyBoost (драйвер Ecache.sys — для Windows Vista или драйвер Rdyboost.sys — для Windows 7), но управление заполнением кэша во время загрузки осуществляется службой ReadyBoost. Служба ReadyBoost удаляет кэш через 90 секунд после начала загрузки или в случае, если требуется дополнительная оперативная память.

Ключ DOS Devices

Продолжим рассмотрение инструкций, исполняемых Диспетчером сеансов в процессе инициализации пользовательского режима в Windows Vista/7.

Итак, Диспетчер сеансов создает символические ссылки. Эти ссылки направляют определенные классы команд на конкретные компоненты файловой системы. Конфигурационная информация для обнаруженных устройств DOS содержится в следующих значимых элементах реестра:

- ☐ PRN: REG_SZ:\DosDevices\LPT1;
- ☐ AUX: REG_SZ:\DosDevices\COM1;
- ☐ NUL: REG_SZ:\Device\Null;
- ☐ UNC: REG_SZ:\Device\Mup;
- ☐ PIPE:\REG_SZ:\Device\NamedPipe;
- ☐ MAILSLLOT:\REG_SZ:\Device\MailSlot.

Ключ *SubSystems*

Затем SMSS запрашивает у ядра запуск драйвера устройства, указанного параметром реестра `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Subsystem\KMode`. По умолчанию этот параметр имеет значение `SystemRoot\system32\win32k.sys` — данный драйвер реализует Win32 API режима ядра, т. е. инициализирует графическую подсистему Win32, переключающую дисплей из текстового режима в графический.

После этого SMSS выполняет следующие задачи по инициализации системы:

- ❑ выполняет незавершенные операции по переименованию или удалению файлов и каталогов. Эти операции перечислены в реестре под ключом `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\PendingFileRenameOperations`;
- ❑ осуществляет предварительную загрузку DLL, перечисленных под ключом реестра `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\KnownDLLs`. Эти DLL должны всегда быть открыты, чтобы ускорить загрузку остальных процессов;

ПРИМЕЧАНИЕ

Так как предварительная загрузка DLL осуществляется процессом, работающим от имени учетной записи `LocalSystem` и с привилегиями `Trusted Computer Base`, необходимо следить за элементами списка известных DLL в составе ключа реестра `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\KnownDLLs`.

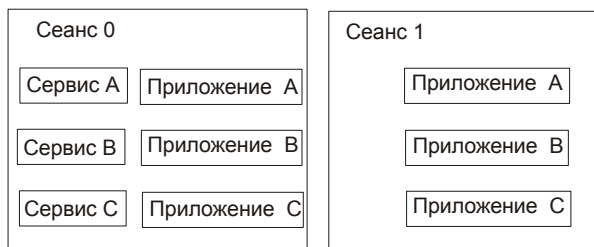
- ❑ читает из реестра содержимое начальной среды процессов и инициализирует на его основании рабочую среду;
- ❑ инициализирует дополнительные файлы подкачки.

Поскольку архитектура подсистем базируется на сообщениях, необходимо запустить подсистему Windows (Win32), которая управляет всем вводом/выводом и доступом к видеодисплею. Процесс этой подсистемы носит имя CSRSS (Client-Server Runtime SubSystem).

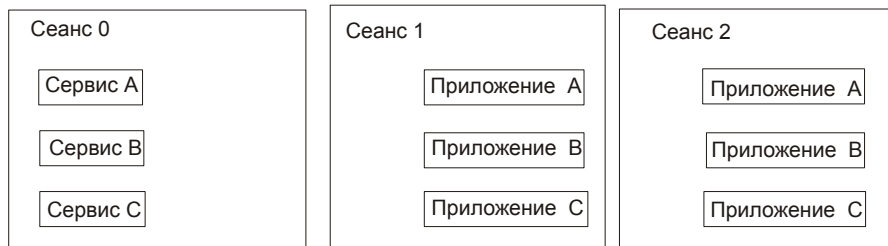
ПРИМЕЧАНИЕ

В предшествующих версиях операционных систем из семейства Windows NT Диспетчер сеансов создавал процессы интерактивного входа в систему (Winlogon) и процесс CSRSS (Client-Server Runtime SubSystem) для каждого сеанса (рис. 7.18, а). Создание сеансов происходило последовательно. Затем процесс Winlogon (`%SystemRoot%\System32\Winlogon.exe`) запускал службу подсистемы локального администратора безопасности (Lsass.exe) и Диспетчер управления службами (Services.exe). При этом пользователь, вошедший в консоль, использовал сеанс 0, в котором работают и системные процессы. Это создавало потенциальную угрозу для безопасности, поскольку некорректно написанный

сервис, работающий в сеансе 0 и отображающий интерактивное окно, мог позволить вредоносным программам атаковать окно такой службы, получая административные привилегии. В Windows Vista и Windows 7 этот недостаток был исправлен за счет реструктурирования и переработки ряда системных процессов. Системные процессы в этих ОС теперь изолированы в сеансе 0 (рис. 7.18, б).



а) Сеансы в Windows NT/2000/XP — пользователь, вошедший в консоль, использовал нулевой сеанс, в котором работают и системные процессы



б) Изоляция сеанса 0 в Windows Vista и Windows 7 — пользователь, вошедший в консоль, использует сеанс 1 и не может подключиться к сеансу 0, который зарезервирован за системными процессами

Рис. 7.18. Изоляция сеанса 0 в Windows Vista/7

Как была достигнута изоляция сеанса 0? На предпоследнем шаге процесс SMSS запускает процессы подсистем для сеансов 0 и 1. При этом он запускает еще одну свою копию для настройки сеанса 0, который выделен исключительно для системных процессов.

ПРИМЕЧАНИЕ

На рабочей станции Windows Vista/7 запуск Диспетчером сеансов собственных копий для инициализации каждого нового сеанса не дает существенных преимуществ. Это нововведение, в основном, ориентировано на компьютеры Windows Server 2008 в роли терминального сервера. В этом случае множественные копии Диспетчера сеансов позволяют ускорить одновременную регистрацию в системе нескольких пользователей, получающих к системе удаленный доступ.

Процесс Диспетчера сеансов для сеанса 0 запускает приложение инициализации Windows (Wininit.exe), процесс подсистемы Windows (Csrss.exe) для сеанса 0, а затем завершает свою работу. Далее приложение инициализации Windows запускает Диспетчер управления службами, подсистему локального администратора безопасности и новый процесс — Диспетчер локальных сеансов (Lsm.exe), который управляет сеансами терминального сервера на этом компьютере. Обратите внимание — процесс Wininit является новым процессом, впервые появившимся в Windows Vista. Запуск множества процессов SMSS (по одному на каждый сеанс) позволяет запускать сеансы параллельно, а не последовательно, как это было в Windows NT/2000/XP.

ПРИМЕЧАНИЕ

Wininit, новый процесс, появившийся, начиная с Windows Vista, выполняет большую часть задач, которые в предыдущих версиях выполнялись процессом Winlogon. По умолчанию SMSS запускает его в только сеансе 0. В остальных сеансах необходимости в этом процессе нет. Процесс Wininit, в свою очередь, запускает процесс локального распорядителя безопасности (Local Security Authority SubSystem), используя файл `%SystemRoot%\system32\lsass.exe`, процесс контроллера сервисов (Service Controller, `%SystemRoot%\system32\services.exe`) и локальный процесс Диспетчера сеансов (Local Session Manager, `%SystemRoot%\system32\lsm.exe`). В Windows NT/2000/XP двумя последними процессами управлял процесс Winlogon. В случае завершения одного из них процесс Winlogon инициировал завершение работы системы и перезагрузку. В Windows Vista запуском и работой этих процессов управляет процесс Wininit, никак не связанный ни с регистрацией пользователя в системе, ни с завершением работы ОС (shutdown).

Чтобы запустить подсистемы для сеансов 0 и 1, SMSS читает параметры реестра в `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SessionManager\SubSystems`. По умолчанию, параметр `Windows` указывает на процесс `%SystemRoot%\system32\csrss.exe`, серверный процесс, который реализует Win32 API режима пользователя. Как только этот процесс стартует, в данном сеансе можно запускать программы Win32.

SMSS запускает в сеансе 0 процесс Wininit (файл `%SystemRoot%\system32\wininit.exe`), а в сеансе 1 — процесс Winlogon (файл `%SystemRoot%\system32\winlogon.exe`). Таким образом, процесс регистрации в системе Winlogon запускается только в сеансе 1.

Наконец, на последнем шаге SMSS входит в цикл и начинает ожидать запросов LPC или завершения процессов Wininit, Winlogon или CSRSS (процесс CSRSS никогда не завершается и имеет флаг "критического процесса"). Остальные процессы могут поддерживать коммуникации с SMSS с целью запуска в сеансе дополнительных подсистем (например, POSIX — `%SystemRoot%\system32\psxss.exe`), сеансов (каждый из которых будет иметь

собственные процессы подсистем и регистрации) или же с целью завершения работы ОС. В случае завершения работы процессов Wininit, Winlogon или CSRSS, SMSS выдает ошибку **STOP**, что приводит к появлению "синего экрана смерти" (Blue Screen of Death, BSOD).

Регистрация в системе

По завершении инициализации ядра необходимо произвести регистрацию пользователя в системе. Процедура регистрации может быть произведена автоматически на основании информации, хранящейся в реестре, или вручную. Если в системе имеется множество учетных записей пользователей или единственная учетная запись защищена паролем, Windows отображает экран приветствия с предложением выбрать пользователя или ввести пароль (рис. 7.19).



Рис. 7.19. Окно регистрации в системе Windows 7

В Windows Vista и Windows 7 пользовательский интерфейс для входа в систему (logon) и выхода из нее (logoff), блокировки и разблокирования сеансов,

а также обработка запросов на завершение работы системы (shutdown) обеспечиваются процессом Winlogon. Этот же процесс управляет запуском пользовательских процессов (userinit.exe) при регистрации пользователя в системе, а также остановкой пользовательских процессов при выходе пользователя из системы. По умолчанию SMSS запускает процесс Winlogon в сеансе 1. Если компьютер работает под управлением Windows Server 2008 в роли терминального сервера, то SMSS обрабатывает запросы на запуск процесса Winlogon в остальных сеансах.

Запустившись, процесс Winlogon создает так называемую *оконную станцию* (window station), которая задает свойства одной или нескольких клавиатур, дисплеев, а также ряд глобальных свойств Win32, и служит основой для интерактивного взаимодействия с отдельным пользователем. Затем процесс Winlogon в масштабах этой "оконной станции" создает три рабочих стола (desktops): рабочий стол Winlogon, рабочий стол пользователя, а также рабочий стол хранителя экрана. При этом процесс Winlogon создает для своего рабочего стола список контроля доступа (Access Control List, ACL) (см. главу 3).

В Windows XP процесс Winlogon загружал компонент Graphical Identification and Authentication (GINA), задачи которого заключались в том, чтобы принять пользовательское регистрационное имя и пароль, а затем безопасным образом передать эту информацию локальному распорядителю безопасности (Local Security Authority, LSA) для аутентификации. Компонент GINA был реализован в виде динамической библиотеки, имя и путь к которой указывались в реестре. Именно эта библиотека и отображала пользовательский интерфейс для входа в систему. Если введенная пользователем учетная информация являлась действительной, то пользователю предоставлялся доступ к компьютеру либо с помощью аутентификации Kerberos V5 (для сети), либо NTLM (локальный компьютер).

Начиная с Windows Vista, архитектура входа в систему, как и весь процесс загрузки, также претерпела существенные изменения. Дело в том, что модель GINA обладала рядом ограничений и недостатков, главными из которых являлись:

- ❑ возможность использования только одной библиотеки GINA;
- ❑ сложность разработки.

Поэтому в Windows Vista на смену модели GINA пришла система поставщиков учетных данных (Credential Providers), применяющаяся и в Windows 7. В этой системе часть функций GINA была передана самому процессу Winlogon (в частности, запуск пользовательских процессов). В динамических библиотеках теперь сосредоточены только такие функции, как получение учетной информации пользователя через пользовательский интерфейс и вы-

полнение аутентификации через процесс локального распорядителя безопасности (Local Security Authority SubSystem, LSASS).

ПРИМЕЧАНИЕ

Процесс LSASS создает порт LPC, а затем входит в цикл обработки запросов к подсистеме безопасности — в том числе, запросов на проверку учетной информации пользователя, поступающих от процессов Winlogon, сетевых сервисов, требующих аутентификации пользователя, а также от пользовательских приложений, нуждающихся в аутентификации.

Теперь процесс Winlogon запускает отдельный процесс — сервер пользовательского интерфейса входа в систему (Logonui.exe). Этот процесс и выполняет загрузку поставщиков учетных данных, читая необходимую информацию из ключа реестра HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers. В отличие от Windows XP, где могла использоваться только одна библиотека GINA, в Windows Vista и Windows 7 процесс Logonui.exe может работать с несколькими поставщиками учетных данных одновременно. Информация о поставщиках учетных данных хранится в реестре под ключом HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers (рис. 7.20).

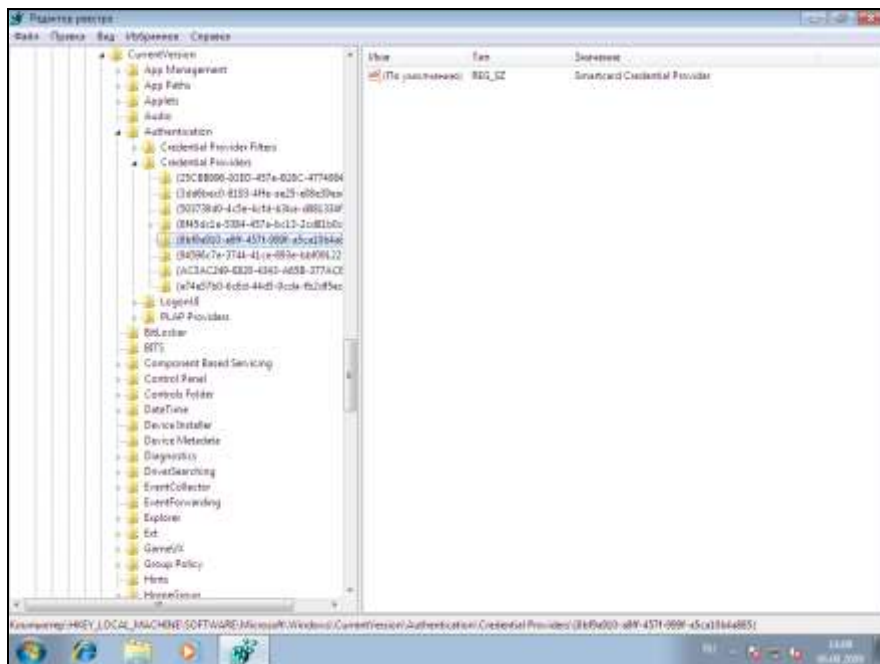


Рис. 7.20. Информация о поставщиках учетных данных в реестре Windows 7

Сторонние разработчики могут добавлять собственные DLL поставщиков учетных данных.

На этапе регистрации пользователя в системе Диспетчер управления сервисами (Service Controller) выполняет загрузку автоматически стартующих сервисов, для которых значение параметра `Start` в ключе реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DriverName` установлено в `0x2`. На этом этапе сервисы загружаются с учетом установленных для них зависимостей, поскольку их загрузка осуществляется параллельно. Зависимости описываются значимыми элементами `DependOnGroup` и `DependOnService` под ключом реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DriverName`. После загрузки этих сервисов и драйверов устройств процесс `Services.exe` входит в цикл обработки запросов и начинает ожидать поступления запросов на запуск и остановку сервисов.

ПРИМЕЧАНИЕ

Загрузка Windows Vista и Windows 7, как и в случае с Windows NT/2000/XP, не считается успешной до тех пор, пока в системе не регистрируется пользователь. После этого набор управляющих опций `Clone` копируется в элемент `LastKnownGood`.

Сервисы, перечисленные в следующих ключах реестра, запускаются и выполняются асинхронно при отображении пользовательского интерфейса для интерактивного входа в систему:

`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce`
`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices`

Процесс определения устройств `Plug and Play` также производится асинхронно с процессом регистрации и зависит от встроенного программного обеспечения системы (firmware), аппаратных средств, драйверов устройств и возможностей операционной системы по определению и эnumерации новых устройств. Когда эти компоненты соответствующим образом скоординированы, механизм `Plug and Play` позволяет определять устройства, производить распределение системных ресурсов, установку драйверов и устройств с минимальным участием пользователя. Подробная информация о процессе определения устройств `Plug and Play` была приведена в *главе 5*.

После регистрации пользователя происходят следующие события:

- ☐ обновляются управляющие наборы (control sets are updated) — управляющий набор, указанный в элементе `LastKnownGood`, обновляется за счет содержимого элемента `Clone`. Здесь `Clone` — копия элемента `CurrentControlSet`, создаваемая каждый раз при запуске компьютера;
- ☐ вступают в силу установки параметров групповой политики;

- ❑ выполняются программы из группы **Автозагрузка** (Startup) — Windows запускает сценарии регистрации, программы, которые должны стартовать при запуске системы, а также сервисы, которые указаны в реестре и в следующих каталогах:
 - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce;
 - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run;
 - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run;
 - HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run;
 - %Systemdrive%\Documents and Settings\All Users\Start Menu\Programs \Startup (Windows XP) или %Systemdrive%\Users\All Users\Start Menu\Programs\Startup (Windows Vista/7);
 - %Systemdrive%\Documents and Settings%\username%\Start Menu\Programs\Startup (Windows XP) или %Systemdrive%\Users\Username\Start Menu\Programs\Startup (Windows Vista/7).

ПРИМЕЧАНИЕ

Как видите, Диспетчер управления сервисами во время входа пользователя в систему запускает множество сервисов и драйверов. Из-за этого пользователю приходится в течение некоторого времени ожидать завершения настройки рабочего стола, и только после этого он может начать нормальную работу. Чтобы преодолеть этот недостаток, начиная с Windows Vista был введен новый тип запуска служб — *отложенный автоматический запуск*. Диспетчер управления сервисами запускает сервисы, настроенные на отложенный автоматический запуск, только после завершения запуска всех сервисов, настроенных на автоматический запуск.

Загрузка остальных сервисов и драйверов

Как уже говорилось, к моменту регистрации пользователя в системе все еще может продолжаться загрузка и инициализация некоторых сервисов и драйверов. Последующие несколько разделов данной главы более подробно описывают следующие важные вопросы:

- ❑ наборы управляющих опций в реестре, которые содержат системную конфигурационную информацию, используемую в процессе загрузки. Хорошее понимание этого материала необходимо для грамотного использования конфигурации LastKnownGood;
- ❑ порядок запуска сервисов и драйверов, задаваемый через реестр (в частности, значимые элементы Start и Error Control, первый из которых задает порядок запуска сервиса или драйвера, а второй — стандартное поведение системы в случае невозможности его запуска или корректной инициализации).

Наборы управляющих параметров в реестре

Набор управляющих параметров (Control Set) содержит системную конфигурационную информацию, включая сведения о загружаемых драйверах устройств и запускаемых сервисах. Наборы управляющих опций хранятся в реестре в виде вложенных подключей ключа `HKEY_LOCAL_MACHINE\SYSTEM`. В системе может существовать несколько наборов управляющих опций, количество которых зависит от того, насколько часто выполняется модификация настройки системы или как часто в ней возникают проблемы. Типичная установленная копия Windows NT/2000/XP/Vista/7 содержит следующие наборы управляющих опций:

- ☐ Clone;
- ☐ ControlSet001;
- ☐ ControlSet002;
- ☐ ControlSet003;
- ☐ CurrentControlSet.

Подключ `CurrentControlSet` представляет собой указатель на один из подключей `ControlSet00x`. Управляющий набор `Clone` — это точная копия (клон) набора управляющих опций, использованного для запуска и инициализации компьютера (`Default` или `LastKnownGood`), и создается процессом инициализации ядра при каждом запуске компьютера. После того как в системе успешно регистрируется хотя бы один пользователь, управляющий набор `Clone` станет недоступным.

Для понимания методов и целей применения этих наборов управляющих опций необходимо ознакомиться с ключом реестра `HKEY_LOCAL_MACHINE\SYSTEM\Select`, который содержит следующие значимые элементы:

- ☐ Current;
- ☐ Default;
- ☐ Failed;
- ☐ LastKnownGood.

Каждый из этих параметров хранит данные типа `REG_DWORD`, которые относятся к конкретному управляющему набору. Например, если значение `Current` установлено равным `0x1`, то параметр `CurrentControlSet` указывает на `ControlSet001`. Аналогично, если параметр `LastKnownGood` установлен равным `0x2`, то он указывает на управляющий набор `ControlSet002`. Значение `Default` обычно совпадает со значением `Current`. Параметр `Failed`

ссылается на набор управляющих опций, на который указывал параметр `Default` в тот момент, когда пользователь последний раз выполнял загрузку компьютера с использованием набора `LastKnownGood`.

Ранее в данной главе в разделе, посвященном выбору конфигурации, была описана инициализация системы с помощью конфигураций по умолчанию (`Default`) и последней удачно загруженной (`LastKnownGood`). При выборе конфигурации `Default` ядро использует значение (`Default`) для определения набора опций управления, который должен применяться для инициализации компьютера. Конфигурацию `LastKnownGood` ядро пытается использовать только в двух ситуациях:

- ❑ при восстановлении системы после серьезной ошибки загрузки одного из жизненно важных для работы системы драйверов устройств;
- ❑ когда пользователь выбирает конфигурацию **Последняя удачная конфигурация (дополнительно)** (`Last Known Good Configuration (Advanced)`).

Запуск системы с применением управляющего набора `LastKnownGood` предоставляет способ восстановления, если имеют место:

- ❑ проблемы, вызванные драйвером устройства, добавленного в систему после последней успешной загрузки;
- ❑ проблемы с загрузкой системы, вызванные ошибками пользователя при модификации значений реестра.

Набор `LastKnownGood` полезен при устранении конфигурационных ошибок.

ВНИМАНИЕ!

Если вы полагаете, что те изменения, которые вы внесли с момента последней успешной регистрации в системе, вызовут проблемы, не спешите зарегистрироваться вновь. Вместо этого перезагрузите компьютер и в соответствующий момент нажмите клавишу <F8>. В **Меню дополнительных вариантов загрузки Windows** (`Advanced Startup Options`) выберите опцию **Последняя удачная конфигурация (дополнительно)** (`Last Known Good Configuration (Advanced)`). Если при загрузке выбрана указанная опция, то все конфигурационные изменения, внесенные с момента последней загрузки системы, будут потеряны.

Сразу же после того, как пользователь регистрируется в системе, любые изменения, вносимые в конфигурацию системы средствами панели управления (`Control Panel`), отражаются только в наборе `CurrentControlSet`. Поэтому, если по той или иной причине необходимо вносить изменения в управляющий набор, `CurrentControlSet` является единственным набором, который имеет смысл редактировать.

Если вы не уверены, где конкретно в управляющем наборе `CurrentControlSet` находится тот или иной ключ, требующий модификации, воспользуйтесь командой **Найти** (Find) меню **Правка** (Edit) редактора реестра (Registry Editor).

Параметр **Start**

В каждом из ключей, содержащихся под ключом реестра `HKEY_LOCAL_MACHINE\SYSTEM\<control set>\Services\DriverName`, присутствует параметр `Start`, определяющий порядок запуска драйвера или сервиса. Он может иметь значения:

- ❑ `0x0` (Boot, Загрузка) — загрузка драйвера или сервиса осуществляется загрузчиком операционной системы перед инициализацией ядра. В качестве примера драйверов с таким режимом загрузки можно привести драйверы дисков;
- ❑ `0x1` (System, Система) — загрузка осуществляется подсистемой ввода/вывода во время инициализации ядра. В качестве примера драйверов, использующих этот тип значения, можно назвать драйверы мыши;
- ❑ `0x2` (Auto load, Автомат) — загружается диспетчером управления сервисами (Service Control Manager). Таким образом загружаются сервисы, которые должны стартовать автоматически при любых обстоятельствах запуска системы, вне зависимости от типа сервиса. В качестве примера можно привести драйверы устройств, работающих через параллельный порт. Одним из сервисов, использующих это значение, является сервис `Alert`;
- ❑ `0x3` (Load on Demand, Manual, Вручную) — загружается диспетчером управления сервисами (Service Control Manager) только в случае получения явной инструкции на загрузку. Сервисы этого типа доступны всегда, но загружаются, только когда пользователь запускает их (например, используя опцию **Службы** (Services) оснастки **Управление компьютером** (Computer Management));
- ❑ `0x4` (Disabled, Запрет) — не загружается. Windows 2000/XP/Vista/7 устанавливает в этот режим драйверы устройств в случае невозможности их загрузки диспетчером сервисов (например, если не установлены соответствующие аппаратные средства). Единственным исключением являются драйверы файловых систем, которые загружаются, даже если для них установлено данное значение в параметре `Start`;
- ❑ `0x5` (Delayed Start, Отложенный запуск) — новый тип запуска сервисов после загрузки. Применяется для тех сервисов, которые не нужны пользователю немедленно после входа в систему. Такие сервисы будут запускаться чуть позднее, и за счет этого система будет быстрее готова к работе после регистрации пользователя.

Параметр *ErrorControl*

Далее перечислены все возможные значения, которые способен принимать значимый элемент `ErrorControl`, находящийся под ключом реестра `HKEY_LOCAL_MACHINE\SYSTEM\<control set>\Services\DriverName`:

- ❑ `Ignore (0x0)` — если при загрузке или инициализации драйвера устройства происходит ошибка, процедура запуска продолжается без вывода сообщения об ошибке;
- ❑ `Normal (0x1)` — если при загрузке или инициализации драйвера устройства происходит ошибка, процедура запуска продолжается после вывода сообщения об ошибке. Значимые элементы `ErrorControl` для большинства драйверов устройств устанавливаются равными этому значению;
- ❑ `Severe (0x2)` — если ядро обнаруживает ошибку загрузки или инициализации этого драйвера или сервиса, происходит переключение на управляющий набор `LastKnownGood`. После этого процесс запуска стартует с начала. Если набор `LastKnownGood` уже используется, процедура запуска продолжается, а ошибка игнорируется;
- ❑ `Critical (0x3)` — та же процедура, что и при значении `Severe`, кроме ситуаций, когда переключение на набор управляющих опций уже произошло, но ошибка не ликвидирована. Тогда процесс загрузки останавливается и выводится сообщение о сбое.

Параметр *DelayedAutoStart*

Как уже говорилось ранее, начиная с Windows Vista для борьбы с задержкой при настройке рабочего стола сразу же после запуска системы и регистрации в ней пользователя предусмотрена возможность отложенного автоматического запуска сервисов. Этот режим удобен для запуска сервисов, которые не обязательно должны быть активными немедленно после запуска системы. К их числу относятся, например, служба **Windows Media Center** и центр обновления Windows (рис. 7.21). Разумеется, для того, чтобы воспользоваться этой возможностью, необходимо настроить сервис на отложенный автоматический запуск. Несложно догадаться, что такая настройка производится через реестр (рис. 7.22).

Для этого в ключе реестра `HKEY_LOCAL_MACHINE\SYSTEM\<control set>\Services\DriverName`, где `DriverName` — имя соответствующего сервиса или драйвера, предусмотрен параметр `DelayedAutoStart`. Он может иметь следующие значения:

- ❑ `0x00000000` — сервис или драйвер не сконфигурирован для отложенного автоматического запуска;
- ❑ `0x00000001` — сервис или драйвер сконфигурирован для отложенного автоматического запуска.

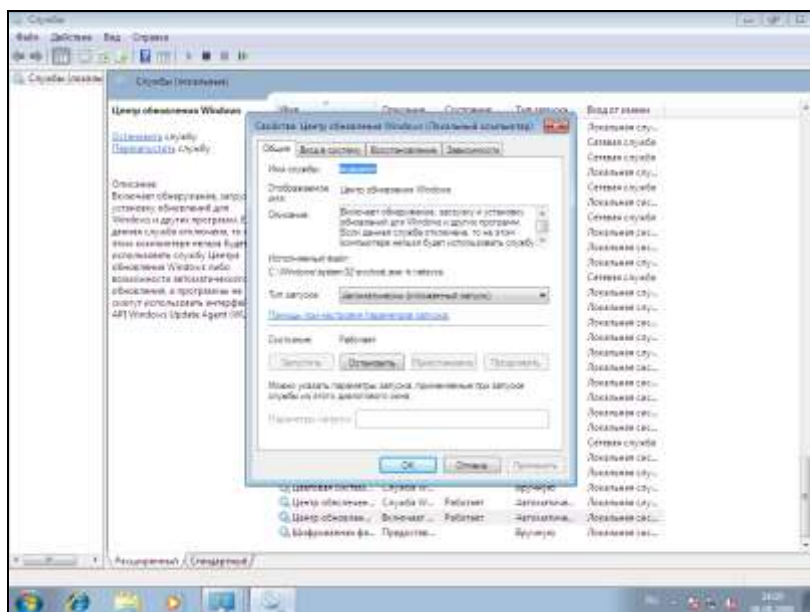


Рис. 7.21. Сервис Центра обновления Windows по умолчанию настроен на отложенный автоматический запуск

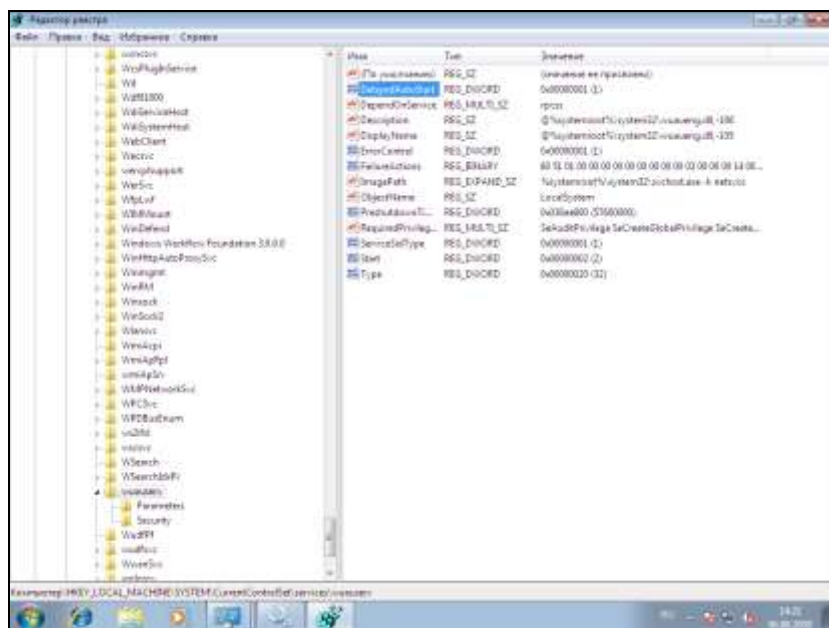


Рис. 7.22. Настройка сервиса на отложенный автоматический запуск через реестр

ПРИМЕЧАНИЕ

Разумеется, этот параметр имеет смысл лишь в комбинации с параметром `Start`, установленным в значение `0x2` (автоматический запуск).

После успешной регистрации пользователя в системе и успешной загрузки всех сервисов и драйверов процесс загрузки Windows Vista/7 считается успешно завершенным.

Обеспечение запуска системы при любых обстоятельствах

Целью обсуждаемых в данном разделе мероприятий является обеспечение загрузки системы при любых обстоятельствах. Само собой разумеется, что мероприятия по обеспечению защиты данных должны быть спланированы заранее.

Регулярное выполнение плановых профилактических процедур позволит предотвратить возможные проблемы или свести к минимуму их последствия. Наиболее общие рекомендации сводятся к следующему:

- ❑ довольно часто причиной некорректной работы системы или даже проблем с ее загрузкой может быть перезапись системного файла или же установка несовместимого драйвера. Обычно это происходит во время инсталляции дополнительного программного обеспечения, не совместимого с операционной системой. Эта проблема существовала во всех предыдущих версиях Windows NT. Начиная с Windows 2000/XP, введены дополнительные средства защиты системных файлов и драйверов с помощью цифровой подписи, которая гарантирует их совместимость и корректную работу. В Windows Vista и Windows 7 эти защитные средства получили дальнейшее развитие. Эти меры (защита драйверов цифровой подписью и защита ресурсов Windows (Windows Resource Protection, WRP) были рассмотрены в *главе 5*;
- ❑ выполнение резервного копирования системных файлов конфигурации, в том числе и реестра, а также выполнение процесса полного резервного копирования системы. Не забывайте выполнять эти операции прежде, чем вносить какие-либо существенные изменения в конфигурацию системы (к этому также относится установка аппаратного и программного обеспечения);
- ❑ не отключайте функцию **Восстановление системы** (System Restore). Несмотря на то, что некоторые пользователи полагают, будто это инструментальное средство занимает слишком много пространства на жестком диске, оно окажется необходимым в случае восстановления поврежденной

системы. Подробные инструкции по выполнению операций резервного копирования и восстановления поврежденной системы приведены в *главе 2*;

- ❑ рекомендуется ежедневно просматривать журналы системных событий (как минимум, журналы System и Application). В особенности обращайте внимание на ошибки, генерируемые драйверами жестких дисков, т. к. они могут указывать на возможные повреждения файловой системы. Если эта рекомендация не выполняется, то ошибки файловой системы могут оставаться незамеченными до тех пор, пока программа Chkdsk не укажет на их существование. Стоит отметить, что при этом поврежденные данные могут попасть и на резервную копию, поскольку программы резервного копирования не распознают ошибки и повреждения в пользовательских данных;
- ❑ регулярно выполняйте проверку дисков для своевременного обнаружения ошибок файловой системы. Кроме того, рекомендуется регулярно проводить и дефрагментацию дисков, что позволит избежать проблем с низкой производительностью. Имейте в виду, что для дефрагментации следует применять только встроенные средства Windows Vista/7 или утилиты сторонних производителей, имеющие статус "Designed for Windows Vista" и "Designed for Windows 7" соответственно. Информацию о программном обеспечении, тестировавшемся на совместимость с Windows Vista и Windows 7, в том числе и об утилитах дефрагментации дисков, можно найти по адресу **<http://support.microsoft.com/kb/933305>**;
- ❑ установите избыточную копию операционной системы, чтобы сделать систему более надежной.

В случае успешного завершения процедуры POST аппаратные средства компьютера инициализируются корректно. Если при этом в процессе загрузки Windows все же происходит сбой, возможно, что проблема с загрузкой возникает по следующим причинам:

- ❑ проблемы с жестким диском, на котором находится системный раздел;
- ❑ повреждение главной загрузочной записи (Master Boot Record, MBR) или загрузочного сектора на системном разделе;
- ❑ отсутствие или повреждение одного из файлов, необходимых для загрузки Windows 7. Список файлов, жизненно важных для загрузки Windows 7, был приведен ранее в этой главе.

Давайте вкратце обсудим средства, которые позволят вам все же загрузить систему в случае возникновения проблем.

- ❑ Безопасный режим загрузки (Safe Mode) — предоставляет средства быстрого восстановления системы после сбоев, вызванных некорректной уста-

новкой нового программного обеспечения или драйверов устройств. Однако применение безопасного режима загрузки помогает не во всех случаях, когда повреждены системные файлы, а также в случаях повреждения жесткого диска;

- ❑ Составление отчета об ошибках (Error Reporting) — отслеживаются проблемы в системе, влияющие на компоненты Windows Vista/7 и работающие в ней приложения. При возникновении проблемы, вы можете отослать отчет о ней в Microsoft и получить ответ;
- ❑ Среда восстановления Windows (Windows Recovery Environment, WinRE) — новый набор функций восстановления поврежденной системы содержит функции:
 - восстановление запуска (Startup Repair);
 - восстановление системы (System Restore);
 - восстановление архива Windows Complete PC;
 - средство диагностики памяти Windows (Windows Memory Diagnostics Tool);
 - командная строка (Command Prompt).

Более подробно эти функции будут рассмотрены в *главе 11*.

Заключение

Итак, в этой главе был рассмотрен процесс нормальной загрузки Windows Vista и Windows 7, их загрузочная архитектура, загрузочное меню и его опции, а также применение этих опций в случае возникновения сбоев в загрузке. Кроме того, были рассмотрены роль и место каждого из системных компонентов в процессе загрузки. Приведенная информация — это тот минимум знаний, которым необходимо обладать для успешного устранения сбоев и неполадок в процессе загрузки. В следующих главах книги будут рассмотрены методы диагностики и устранения проблем с загрузкой, приведены наиболее общие рекомендации по запуску системы с ошибками конфигурации, а также практические примеры устранения таких ошибок.

Глава 8



Параметры настройки сети в реестре

Новые системы создают новые проблемы.

Технологический закон Мэрфи

Когда я думаю о замысле Творца,
Когда меня загадка жизни мучит,
Встают перед глазами два ларца,
И в каждом спрятан от другого ключик.

П. Хэйн,

"Парадокс Жизни. Философский грук"

В отличие от Windows XP, где настройка сети в основном была основана на тех же функциональных возможностях, что и в Windows 2000, Windows Vista представляла собой существенный шаг вперед, как с точки зрения множества новых функциональных возможностей, так и с точки зрения сетевой безопасности. Windows Vista предложила множество существенных нововведений именно в области сетевых технологий, в том числе:

- ☐ новый пользовательский интерфейс;
- ☐ высокопроизводительный самонастраивающийся стек TCP/IP;
- ☐ интегрированную поддержку протоколов IPv4 и IPv6;
- ☐ новые решения в области сетевой безопасности;
- ☐ улучшенные средства сетевой диагностики;
- ☐ набор средств по управлению сетью, включая новые групповые политики для управления качеством обслуживания (Quality of Service), брандмауэром Windows (Windows Firewall), а также настройкой беспроводной сети.

Разработчики Windows 7 сделали еще один шаг в направлении дальнейшего совершенствования поддержки сетевых технологий, в частности:

- ☐ улучшена поддержка беспроводных устройств, в том числе Bluetooth и Wi-Fi;

- обеспечивается встроенная поддержка новой технологии Wireless USB;
- повышена общая производительность работы сети;
- улучшен пользовательский интерфейс, упрощена процедура установки и настройки сети;
- реализованы новые функциональные возможности, которые будут подробно рассмотрены далее в этой главе.

Особенный интерес представляет собой сетевой стек Windows Vista/7 — многие из его компонентов являются абсолютно новыми. Стек TCP/IP полностью переписан и, таким образом, представляет собой полный отход от прежних версий Windows. Новый сетевой стек интегрирует поддержку IPv6 и IPv4, впервые за всю историю Windows обеспечивая поддержку IPv6 в конфигурации по умолчанию. Помимо этого, начиная с Windows Vista, реализована поддержка целого ряда новых протоколов, причем часть из них входит в состав сетевого стека, а часть является новыми компонентами Windows. Каждый новый протокол несет с собой огромный набор сетевых настроек, которые необходимо понять и детально изучить. У администраторов еще недостаточно опыта решения проблем, с которыми они прежде не сталкивались.

Иными словами, проблема рассмотрения параметров настройки сети в Windows 7 широка и неисчерпаема, и рассмотреть абсолютно все новшества в рамках одной главы чисто физически невозможно. Эта тема заслуживает отдельной книги, которую я надеюсь написать в обозримом будущем. Тем не менее, в данной главе сделана попытка рассмотреть наиболее важные из нововведений в сети Windows Vista и Windows 7, а также их взаимосвязь с реестром.

Установка сетевых компонентов с помощью утилит Панели управления

По мере добавления сетевых компонентов и конфигурирования параметров настройки сети, в реестр Windows добавляются новые ключи и параметры. Тем не менее, прежде чем мы раскроем Редактор реестра и углубимся в детали, давайте рассмотрим наиболее простые методы установки сетевых параметров и компонентов.

На первый взгляд, между процедурами настройки и конфигурирования сети в Windows Vista и Windows 7 нет таких радикальных отличий, которые имелись между Windows XP и Windows Vista. Однако это впечатление обманчиво, в чем вы и убедитесь сразу же, как только начнете работать с Windows 7 и возьметесь за настройку сети. Само собой, особенно разительными эти

отличия покажутся тем из вас, кто переходит на использование Windows 7, минуя Vista.

Итак, приступим. Как вы, вероятно, помните, в Windows Vista все управление сетевыми возможностями осуществляется через Центр управления сетями и общим доступом (Network and Sharing Center). Чтобы начать процедуру настройки сети в этой операционной системе, раскройте окно **Панель управления** (Control Panel) и выберите опцию **Сеть и Интернет** (Network and Internet). В раскрывшемся окне (рис. 8.1) выполните щелчок мышью по значку **Центр управления сетями и общим доступом** (Network and Sharing Center), и вы попадете в окно Центра управления сетями и общим доступом, который и является отправной точкой для начала конфигурирования сети.

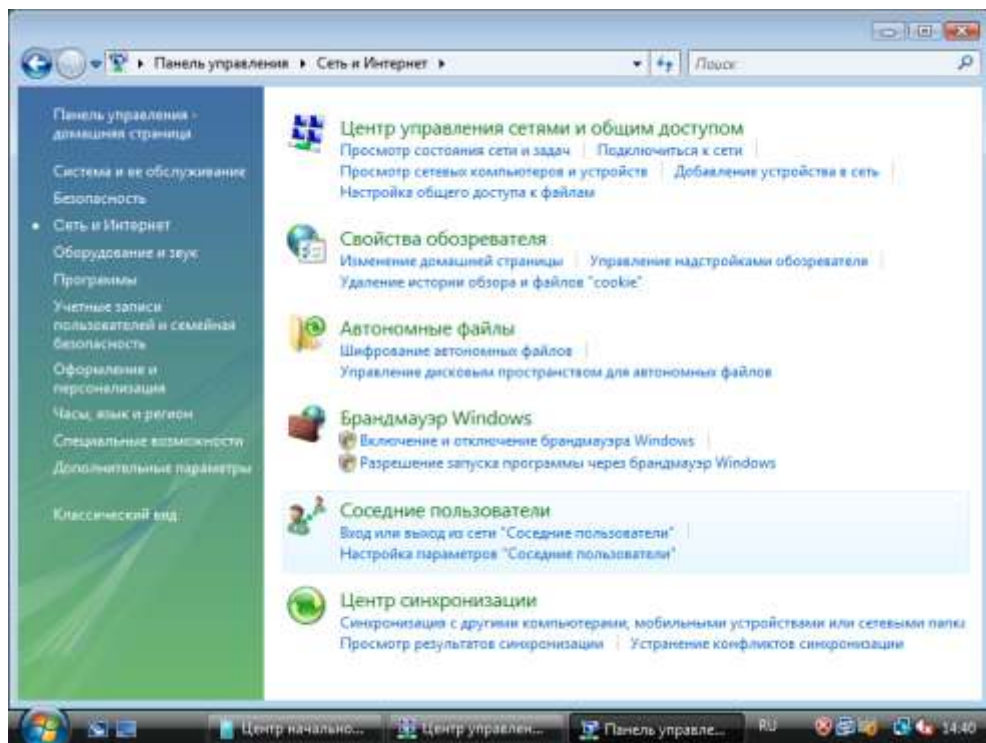


Рис. 8.1. Опции управления сетью и подключением к Интернету в Windows Vista

Как осуществляется эта же процедура в Windows 7? Да точно так же! Раскройте окно Панели управления (Control Panel) и выберите опцию **Сеть и Интернет** (Network and Internet). На первый взгляд, никаких различий

в подходе не наблюдается, но это только на первый взгляд. Посмотрите, как изменилось само окно (рис. 8.2).

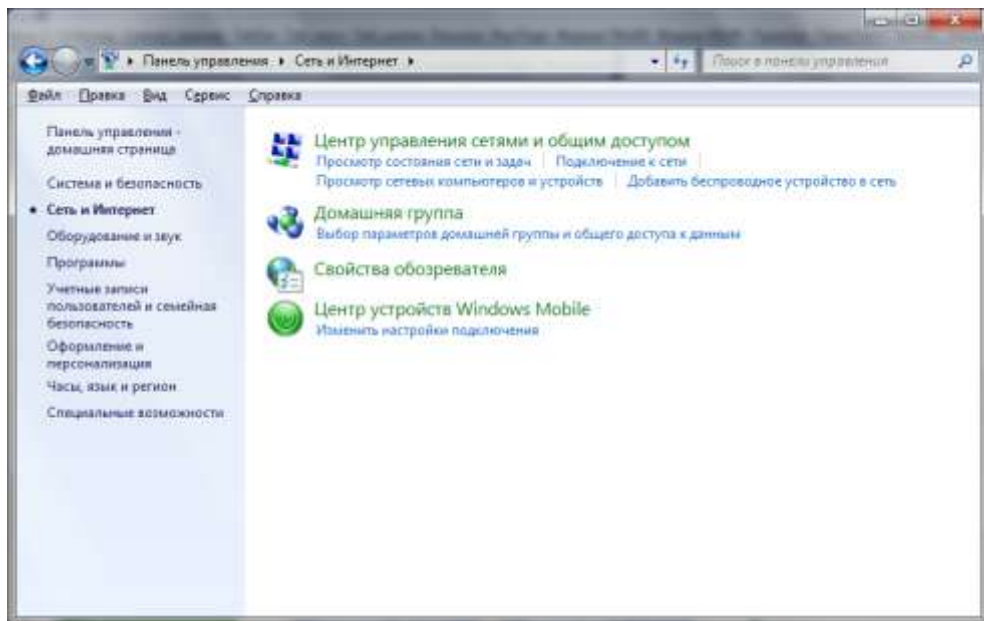


Рис. 8.2. Опции управления сетью и подключением к Интернету в Windows 7

Как видите, новое окно с опциями управления сетью и подключением к Интернету в Windows 7 предлагает некоторые из ранее имевшихся опций и ряд новых. Однако, в целом, оно стало гораздо менее загроможденным, что существенно упрощает процедуру выбора нужной опции. А ведь в Vista новички, увидев такое изобилие опций, просто терялись и не знали, что делать дальше.

ПРИМЕЧАНИЕ

Наверняка те из вас, кто работал с Windows Vista, сразу же обратят внимание на опцию **Домашняя группа** (HomeGroup), появившуюся в Windows 7. Она представляет собой принципиальное нововведение, которое заслуживает отдельного рассмотрения. Но пока мы не будем на него отвлекаться и продолжим конфигурирование сети, а к Домашней группе вернемся чуть позже. Впрочем, название у нее "говорящее", так что о ее предназначении нетрудно и догадаться.

В 99% всех случаев, в Windows 7, как и в Windows Vista, для конфигурирования сети необходимо открыть окно Центра сетей и управления общим доступом. Переход в это окно тоже осуществляется аналогично тому, как это

делалось в Windows Vista. Щелкните мышью по значку **Центр управления сетями и общим доступом**, и оно перед вами откроется (рис. 8.3).

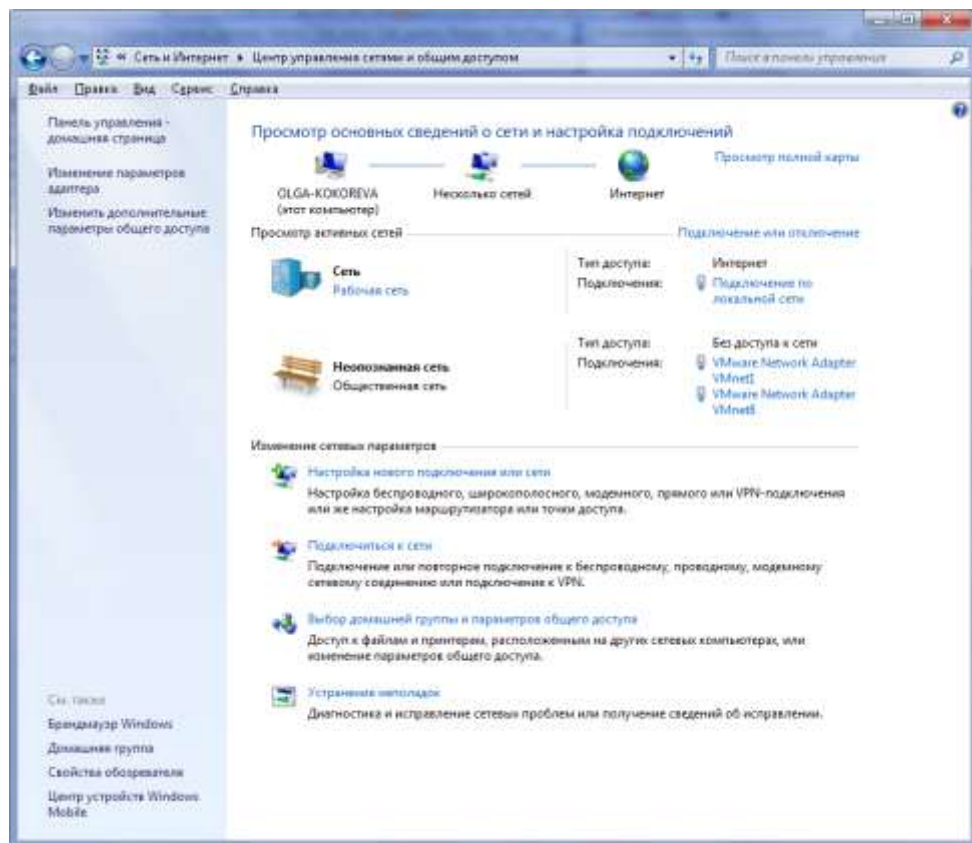


Рис. 8.3. Окно Центра управления сетями и общим доступом в Windows 7

Окно Центра управления сетями и общим доступом визуализирует структуру сети и позволяет вам выполнять такие задачи, как проверка статуса сетевого соединения, выявление и устранение существующих проблем, подключение к Интернету и просмотр карты сети (Network Map). Как и в более ранних версиях Windows, компьютеры Windows Vista и Windows 7 могут иметь несколько сетевых адаптеров. Если один из адаптеров, подключенных к сети, теряет соединение с Интернетом, то в области уведомлений появляется сигнализирующий об этом значок (рис. 8.4). Вы можете щелкнуть по этому значку правой кнопкой мыши, раскрыть Центр управления сетями и общим доступом и выяснить, какое из подключений не работает. Для выяснения причины

возникшей проблемы и поиска путей ее решения следует воспользоваться средством диагностики и восстановления (Network Diagnostics and Troubleshooting). Для этого в окне, показанном на рис. 8.3, достаточно щелкнуть по ссылке **Устранение неполадок** (Troubleshooting), и на экране откроется окно, позволяющее устранить все виды возможных проблем (рис. 8.5).

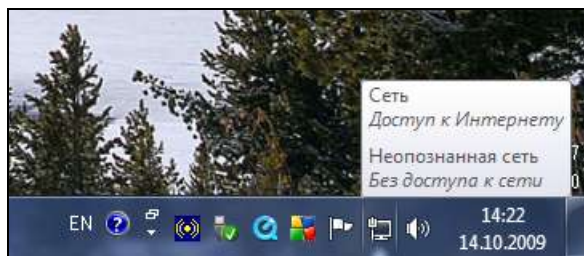


Рис. 8.4. Случай потери соединения с Интернетом

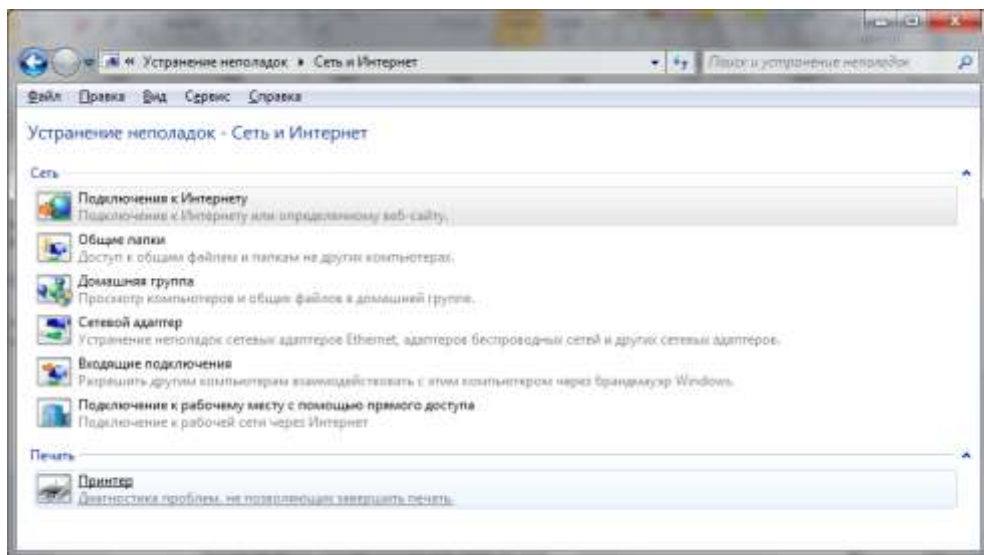


Рис. 8.5. Средства устранения неполадок сети и подключения к Интернету

Windows 7 попытается выявить все возможные виды неполадок, а завершив работу, предложит устранить их, выступив от имени администратора (рис. 8.6).

Завершив работу, модуль устранения неполадок отобразит окно отчета о проблемах и их устранении (рис. 8.7).

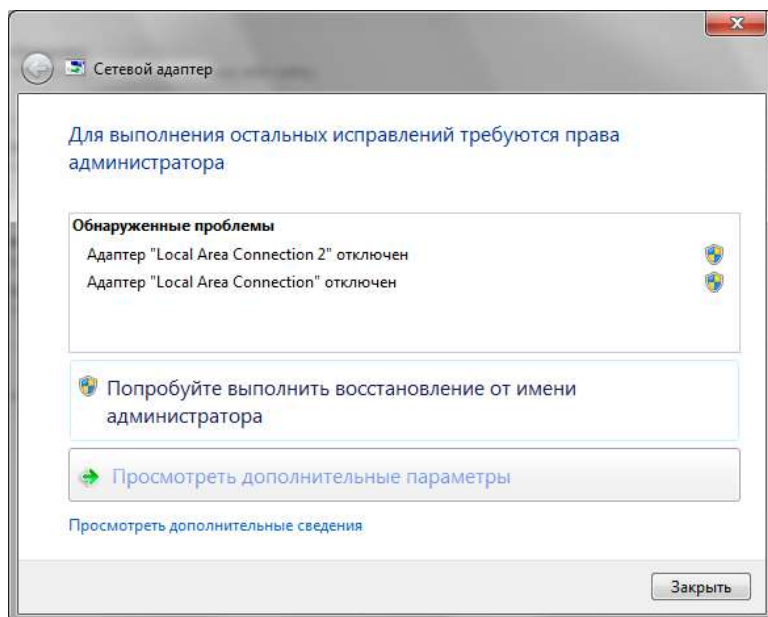


Рис. 8.6. Windows 7 выведет список обнаруженных проблем и предложит устранить их от имени администратора

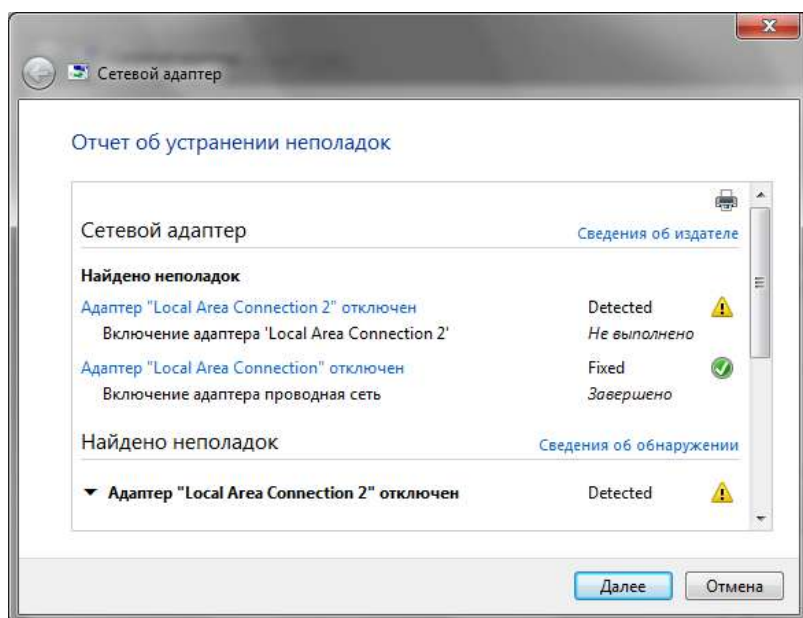


Рис. 8.7. Окно отчета об обнаруженных проблемах и результатах их устранения

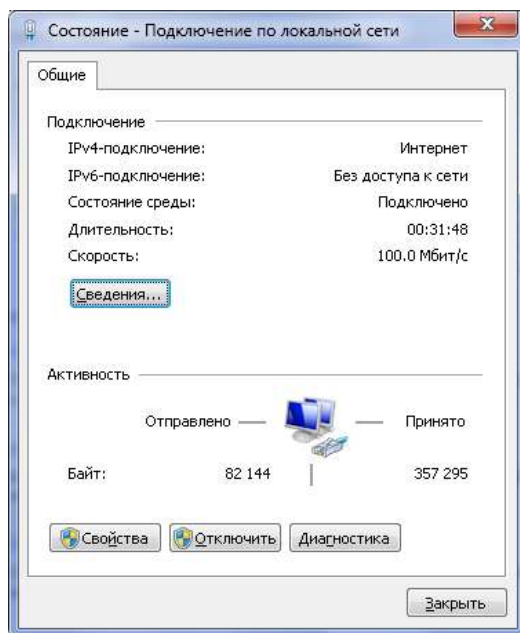


Рис. 8.8. Окно, позволяющее просмотреть статус сетевого подключения

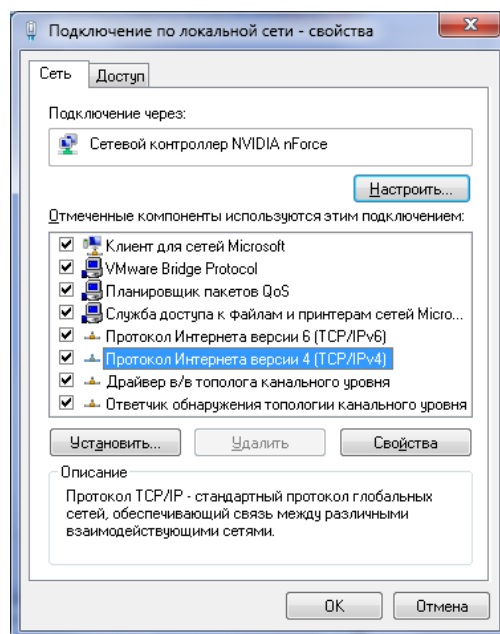


Рис. 8.9. Окно свойств сетевого подключения

ПРИМЕЧАНИЕ

Некоторые из функциональных возможностей Центра управления сетями и общим доступом могут требовать установки совместимого сетевого оборудования и доступа к проводной или беспроводной сети.

Чтобы просмотреть или модифицировать параметры настройки сети, выполните щелчок мышью по ссылке, расположенной справа от названия одной из доступных сетей и указывающей тип подключения в окне Центра управления сетями и общим доступом (см. рис. 8.3). Так, в примере, приведенном на рис. 8.3, щелкните по ссылке **Подключение по локальной сети** (Local Area Connection). В раскрывшемся окне (рис. 8.8) щелкните кнопку **Свойства** (Properties), и на экране откроется окно **Подключение по локальной сети — свойства** (Local Area Connection Properties) (рис. 8.9).

Расположенное в верхней части этого окна поле **Подключение через** (Connect using) указывает сетевой адаптер, используемый для подключения к локальной сети.

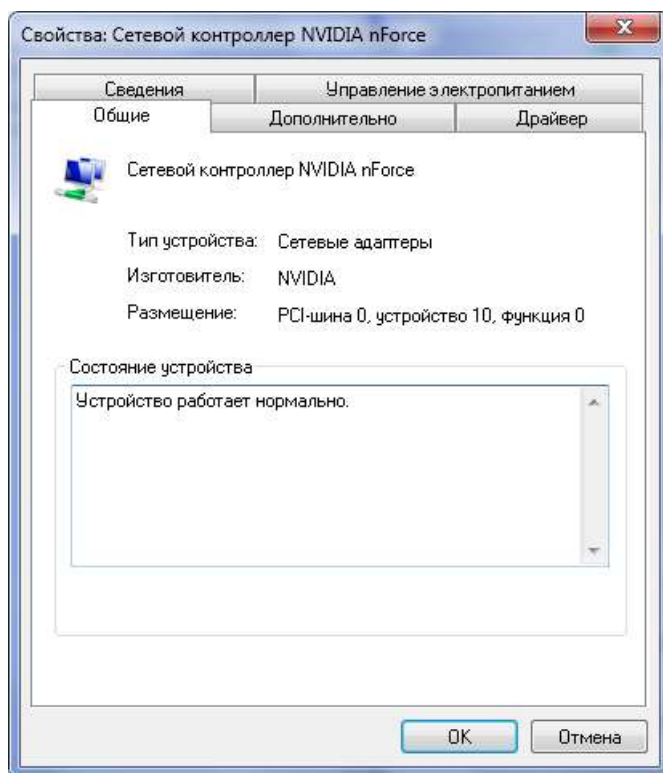


Рис. 8.10. Диалоговое окно свойств установленного сетевого адаптера

Пользователь может конфигурировать сетевые адаптеры, нажав расположенную ниже этого поля кнопку **Настроить** (Configure). Следует отметить, что таким образом можно только настроить уже установленные сетевые адаптеры, а добавление новых сетевых адаптеров следует производить при помощи утилиты **Установка и удаление программ** (Add/Remove Hardware) из Панели управления (Control Panel). Диалоговое окно (рис. 8.10), которое раскрывается при нажатии кнопки **Настроить** (Configure), полностью соответствует окну свойств сетевого адаптера, открываемому при использовании Диспетчера устройств (Device Manager). Это окно позволяет только сконфигурировать свойства сетевого адаптера, для которого уже установлен драйвер.

В списке **Отмеченные компоненты используются этим подключением** (This connection uses the following items) окна свойств соединения (см. рис. 8.9) перечислены сетевые протоколы и сервисы, используемые данным сетевым адаптером, а кнопки **Установить** (Install), **Удалить** (Uninstall) и **Свойства** (Properties) позволяют установить, удалить или сконфигурировать сетевые протоколы и сервисы.

Сетевые параметры в реестре Windows Vista и Windows 7

При установке сетевых компонентов в реестр добавляется соответствующая информация. Для установки сетевых компонентов Windows Vista и Windows 7 требуются:

- ❑ *Инсталлятор класса* (class installer) — динамически загружаемая библиотека (DLL), которая выполняет установку, конфигурирование или удаление из системы устройств определенного класса. Установка сетевых компонентов Windows Vista/7 производится сетевым инсталлятором класса Windows (Windows network class installer) или инсталлятором класса, разработанным поставщиком устройства.

Если стандартный инсталлятор класса не предоставляет всех функциональных возможностей, необходимых для конкретного устройства, поставщик устройства может разработать так называемый *вспомогательный инсталлятор*, который представляет собой динамически загружаемую библиотеку Win32, реализующую функции, недостающие для установки индивидуального устройства.

Существуют следующие классы сетевых компонентов:

- Net — класс, определяющий сетевые адаптеры;

- **NetTrans** — класс, определяющий сетевые протоколы (например, IPv4, IPv6), сетевые клиенты, ориентированные на установление соединения (connection-oriented client);
- **NetClient** — класс, указывающий сетевого клиента (например, Microsoft Client for Networks). Компонент **NetClient** считается сетевым провайдером (network provider) и, если он используется для предоставления сервиса печати через сеть, он также является и провайдером печати (print provider);
- **NetService** — класс, который указывает сетевой сервис (например, файл-сервис или сервис печати).

Сетевой инсталлятор класса определяет класс устанавливаемого сетевого компонента по значению параметра **ClassGuid**. Параметр **ClassGuid** представляет собой *глобальный уникальный идентификатор* (Globally Unique Identifier, GUID) для этого класса. Значения GUID можно получить с помощью утилиты **Uuidgen.exe** (более подробную информацию о ней можно найти в документации Windows Platform SDK).

Классы сетевых компонентов и соответствующие им значения **ClassGuid** перечислены в табл. 8.1.

Таблица 8.1. Классы сетевых компонентов и соответствующие им значения **ClassGuid**

Класс сетевого компонента	Значение ClassGuid
Net	{4D36E972-E325-11CE-BFC1-08002BE10318}
NetTrans	{4D36E973-E325-11CE-BFC1-08002BE10318}
NetClient	{4D36E974-E325-11CE-BFC1-08002BE10318}
NetService	{4D36E975-E325-11CE-BFC1-08002BE10318}

Информация инсталляторов классов хранится в реестре в составе ключа **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class**. Для каждого инсталлятора класса в составе этого ключа имеется вложенный ключ с именем... Нет, не ждите, что это будет имя типа "Net" — это как раз будет значение **ClassGuid** (рис. 8.11), то самое, которое приведено в табл. 8.1 для класса **Net** (сетевые адаптеры);

- **INF-файлы** — содержат сведения, необходимые инсталлятору класса сетевого компонента для установки этого компонента. Подробную информацию о формате INF-файлов можно найти в документации, поставляемой в составе программного продукта Windows Driver Development Kit (DDK);

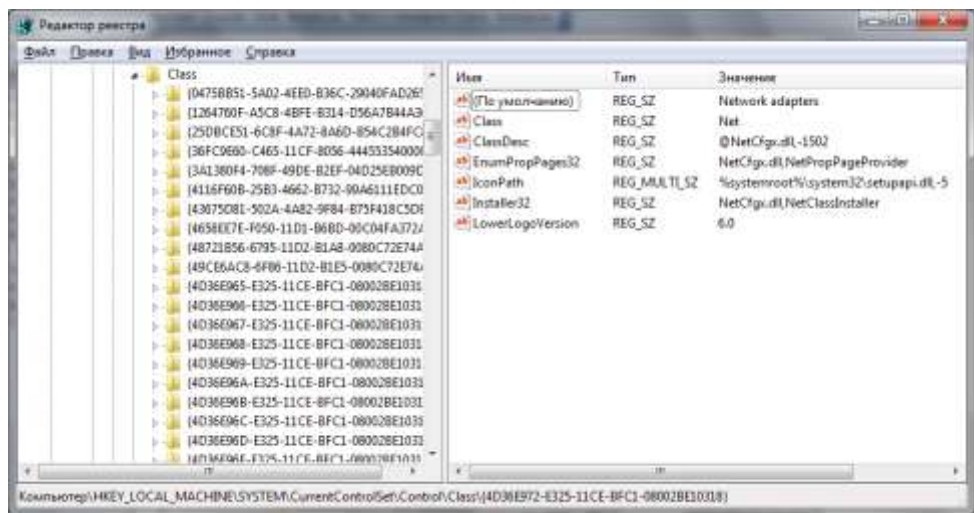


Рис. 8.11. Содержимое ключа реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}` определяет параметры инсталлятора класса сетевых адаптеров

- **уведомляющий объект (notify object)** — компоненты сетевого программного обеспечения, такие как сетевые протоколы, сервисы или сетевые клиенты, могут иметь уведомляющие объекты, которые позволяют отображать пользовательский интерфейс для ручного конфигурирования соответствующих компонентов, предоставляют ручной контроль за процессом привязки (binding) и т. д. Аппаратные компоненты (сетевые адаптеры) тоже способны предоставлять пользовательский интерфейс и программный контроль над привязкой протоколов, но все эти задачи выполняются не уведомляющими объектами, а через INF-файл или вспомогательный инсталлятор. На рис. 8.12 приведена информация об уведомляющем объекте, который выполняет конфигурирование клиента для сетей Microsoft, а на рис. 8.13 — информация об уведомляющем объекте, выполняющем конфигурирование протокола TCP/IP;
- **миграционная DLL и ассоциированные с ней файлы** — если драйвер для сетевого устройства не входит в поставку Windows Vista или Windows 7, поставщик должен предоставлять поддержку обновления версий для программного обеспечения, управляющего работой этого устройства.

В дополнение к перечисленным файлам для установки сетевых компонентов требуется следующее:

- **один или несколько драйверов устройства** — как правило, драйвер состоит из *образа драйвера (driver image)* — файла с расширением SYS и *библиотеки драйвера (DLL)*;

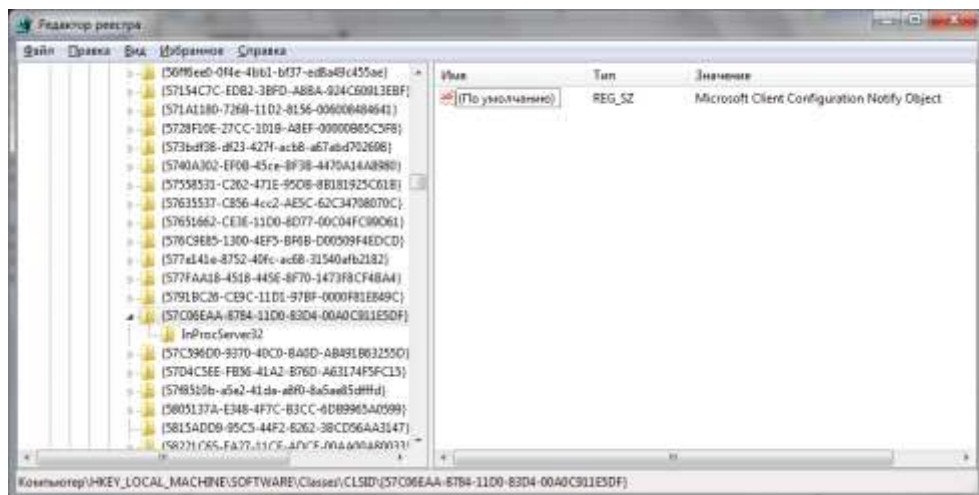


Рис. 8.12. Информация об уведомляющем объекте, конфигурирующем клиента для сетей Microsoft

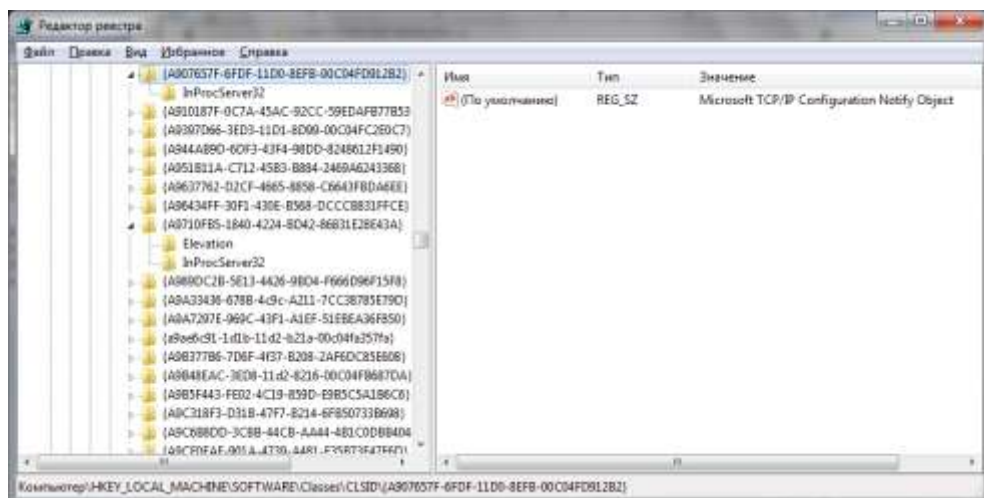


Рис. 8.13. Информация об уведомляющем объекте, конфигурирующем протокол Microsoft TCP/IP

- *необязательный, но весьма желательный файл каталога для драйвера (driver catalog file)* — если поставщик желает, чтобы его устройство было включено в список совместимых аппаратных средств, а драйвер протестирован на совместимость специалистами из Microsoft, то он предоставляет устройство и драйвер на тестирование в *лабораторию тестирования*

качества оборудования для Windows (Windows Hardware Quality Lab, WHQL). Если результаты тестирования были признаны удовлетворительными, то лаборатория WHQL включает устройство в список совместимых аппаратных средств, а для драйвера предоставляет файл каталога (CAT-файл), который содержит цифровую подпись;

- необязательный файл `Txtsetup.oem` — содержит информацию, необходимую программе установки системы для инсталляции драйвера устройства на ранних этапах загрузки системы во время текстовой фазы процесса установки Windows.

Регистрационная информация сетевых адаптеров

В Windows Vista и Windows 7 имеются вложенные ключи регистрации программного обеспечения для всех установленных карт сетевых адаптеров. Эти ключи находятся по адресу `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkCards\Netcard#` (рис. 8.14).

ПРИМЕЧАНИЕ

Обратите внимание, что нумерация начинается с 1, а не с 0.

Помимо этого, в составе ключа `HKEY_LOCAL_MACHINE` имеются еще два вложенных ключа, содержащих информацию о сетевом адаптере:

- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum`, в составе которого системные эnumераторы устройств Plug and Play хранят сведения о конкретных устройствах, например, идентификаторы устройств (device ID), идентификаторы совместимых устройств (если они имеются) и т. д. На рис. 8.15 представлена информация о сетевом адаптере NVIDIA nForce, хранящаяся в составе ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum`;
- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\<ClassGUID>` — в составе этого ключа системные инсталляторы устройств хранят информацию о каждом конкретном классе устройств, инсталляторе класса и вспомогательных инсталляторах (если они имеются). Для каждого установленного драйвера в составе этого ключа есть вложенные ключи типа "0000", "0001", которые содержат информацию о данном драйвере, в том числе строку его описания, путь к INF-файлу, сведения о поставщике драйвера и т. д. На рис. 8.16 представлено содержимое ключа реестра, содержащего информацию о драйвере обсуждаемого сетевого адаптера — NVIDIA nForce.

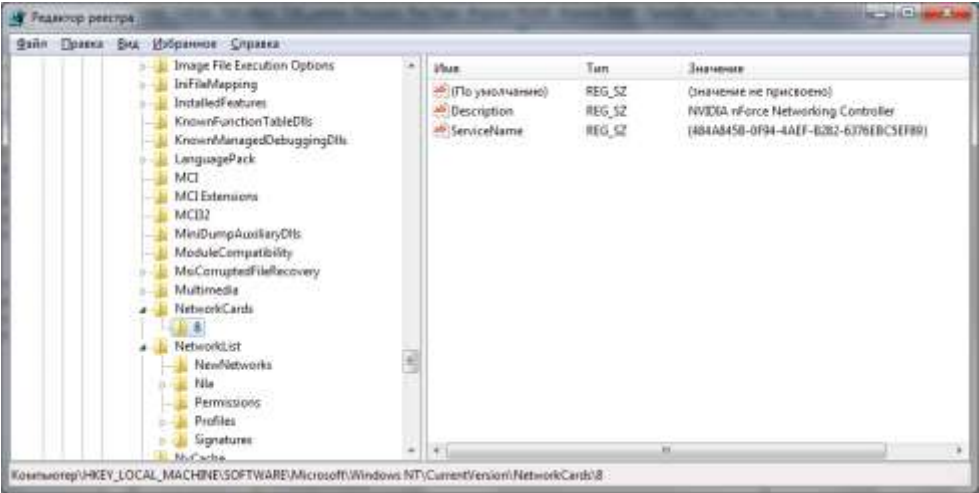


Рис. 8.14. Ключ реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkCards\8 в реестре Windows 7

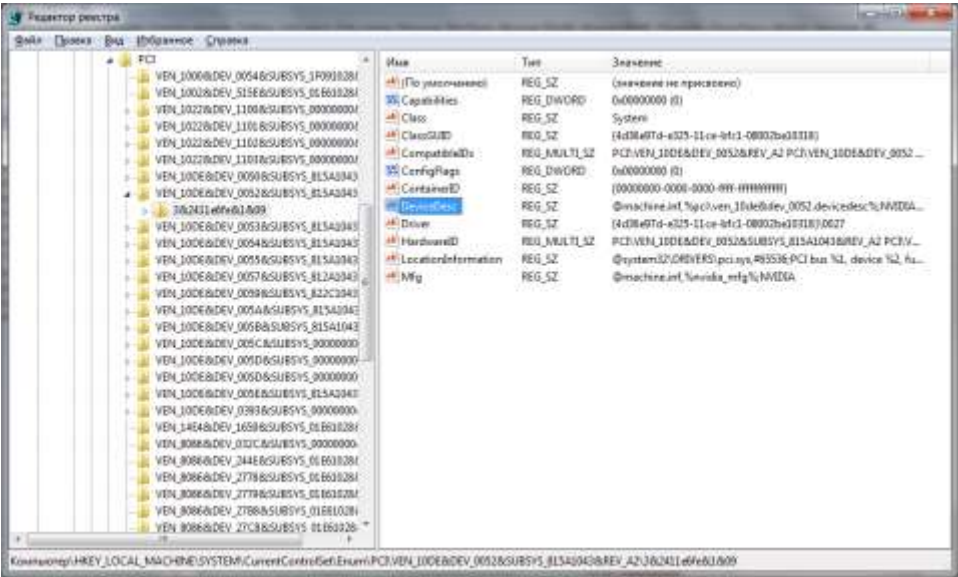


Рис. 8.15. Информация о сетевом адаптере NVIDIA nForce в составе ключа HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum

Кроме того, каждый из ключей драйвера содержит стандартный набор обязательных вложенных ключей: Linkage и Ndi. Типичное содержимое ключа Linkage для драйвера сетевой карты показано на рис. 8.17. Как видно из при-

веденной иллюстрации, стандартными параметрами, содержащимися в составе этого ключа, являются параметр `Export`, значение которого указывает список создаваемых объектов, параметр `RootDevice`, задающий корневое устройство, и параметр `UpperBind`, определяющий привязку протоколов.

Ключ `Ndi` содержит вложенные ключи и параметры, которые зависят от типа установленного сетевого компонента. Если установленный сетевой компонент имеет ассоциированный с ним сервис или драйвер устройства, то в составе ключа `Ndi` обязательно появляется параметр `Service`, который указывает имя соответствующего сервиса или драйвера устройства (рис. 8.18). Если с компонентом ассоциировано несколько сервисов, то в составе ключа `Ndi` должен присутствовать еще один обязательный параметр — `CoServices` с типом данных `REG_MULTI_SZ`, который перечисляет все сервисы, включая основной. Этот параметр обязателен для сетевых компонентов типа `NetTrans` (транспортные протоколы), `NetClient` (сетевые клиенты) и `NetService` (сетевые сервисы). Компоненты типа `Net` (адаптеры) такого параметра не имеют, что и видно из рис. 8.18 (с сетевым адаптером ассоциирован только драйвер `NVENETFD`).

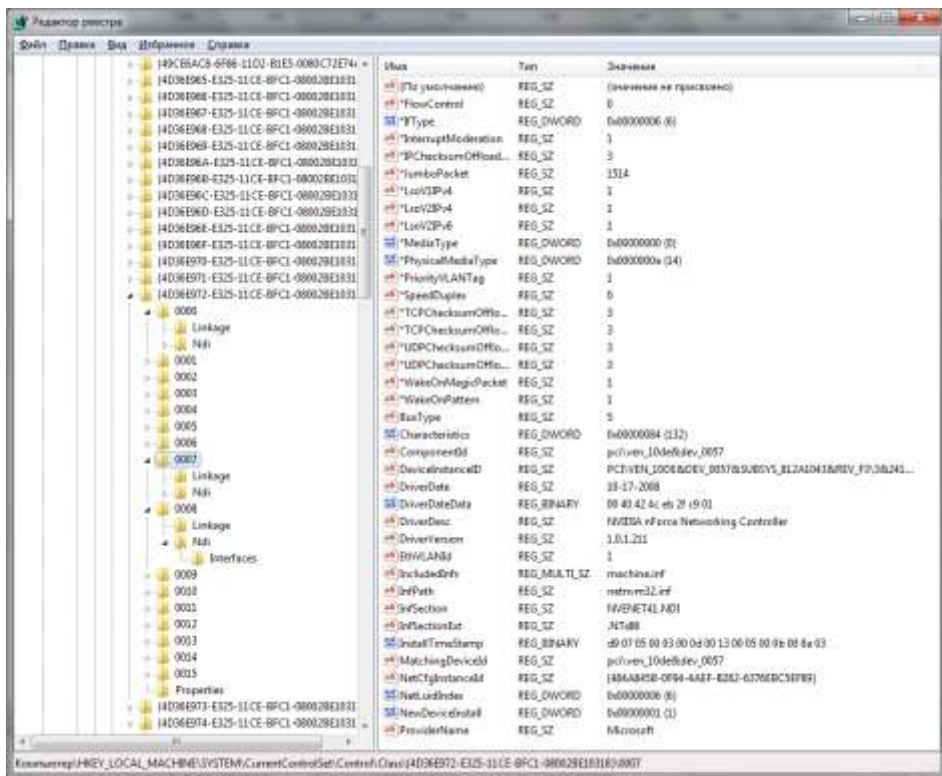


Рис. 8.16. Параметры драйвера сетевого адаптера в реестре

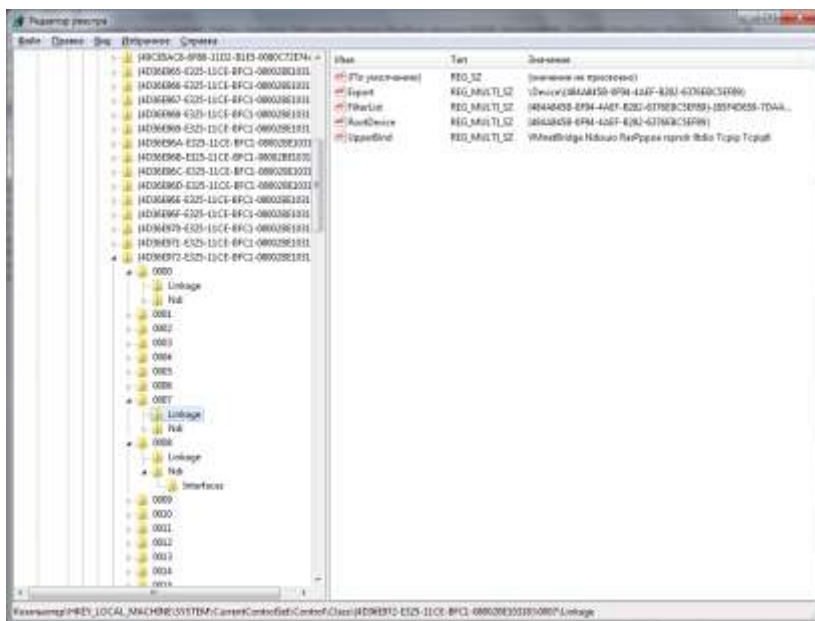


Рис. 8.17. Типичное содержимое ключа Linkage для драйвера карты сетевого адаптера

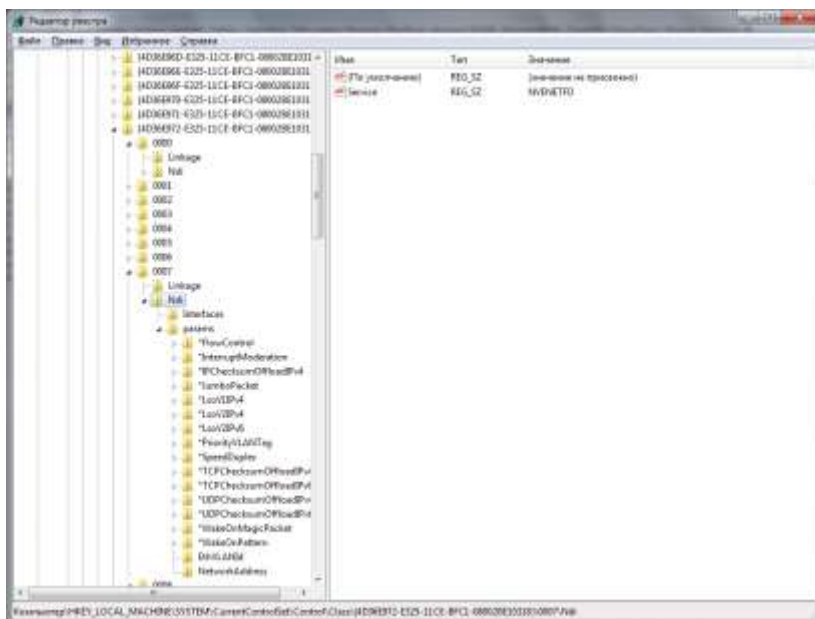


Рис. 8.18. Параметр `.\Ndi\Service` указывает имя ассоциированного с сетевым компонентом драйвера или сервиса

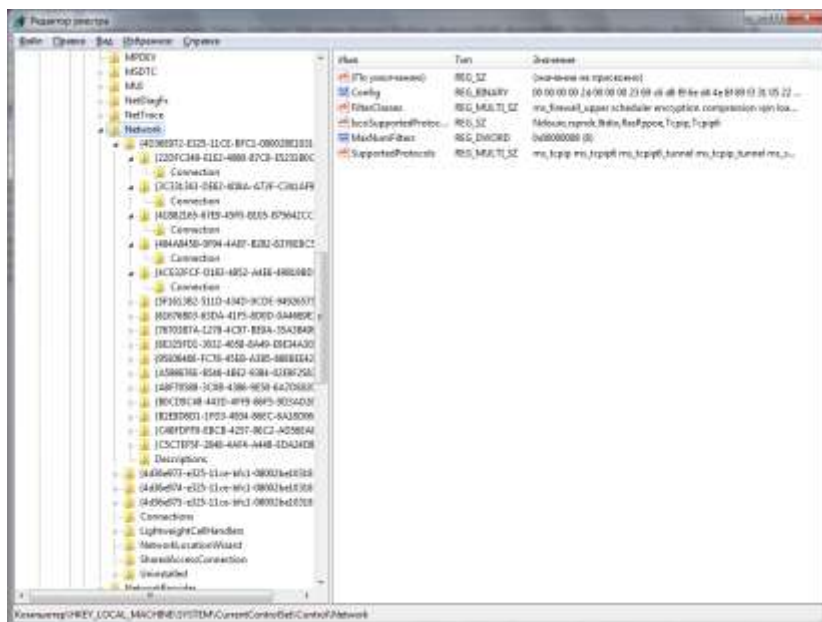


Рис. 8.19. Содержимое ключа реестра
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Network

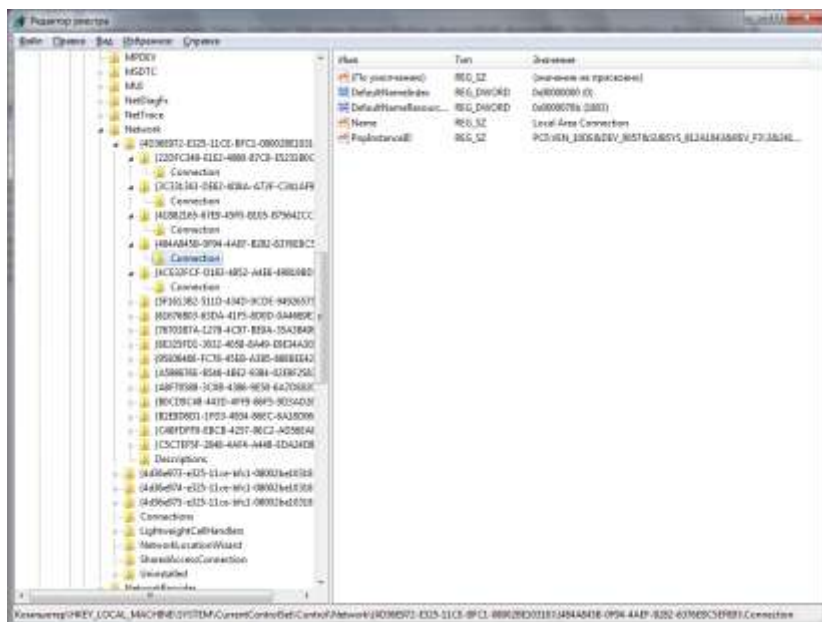


Рис. 8.20. Информация о свойствах соединения с локальной сетью в реестре

Дальнейшая конфигурационная информация о сетевых средствах Windows Vista и Windows 7 находится в составе ключа реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Network`. Обратите внимание на вложенные ключи с именами в виде длинных последовательностей букв и цифр, заключенных в фигурные скобки (рис. 8.19) — те самые значения `ClassGuid`, которые были перечислены в табл. 8.1.

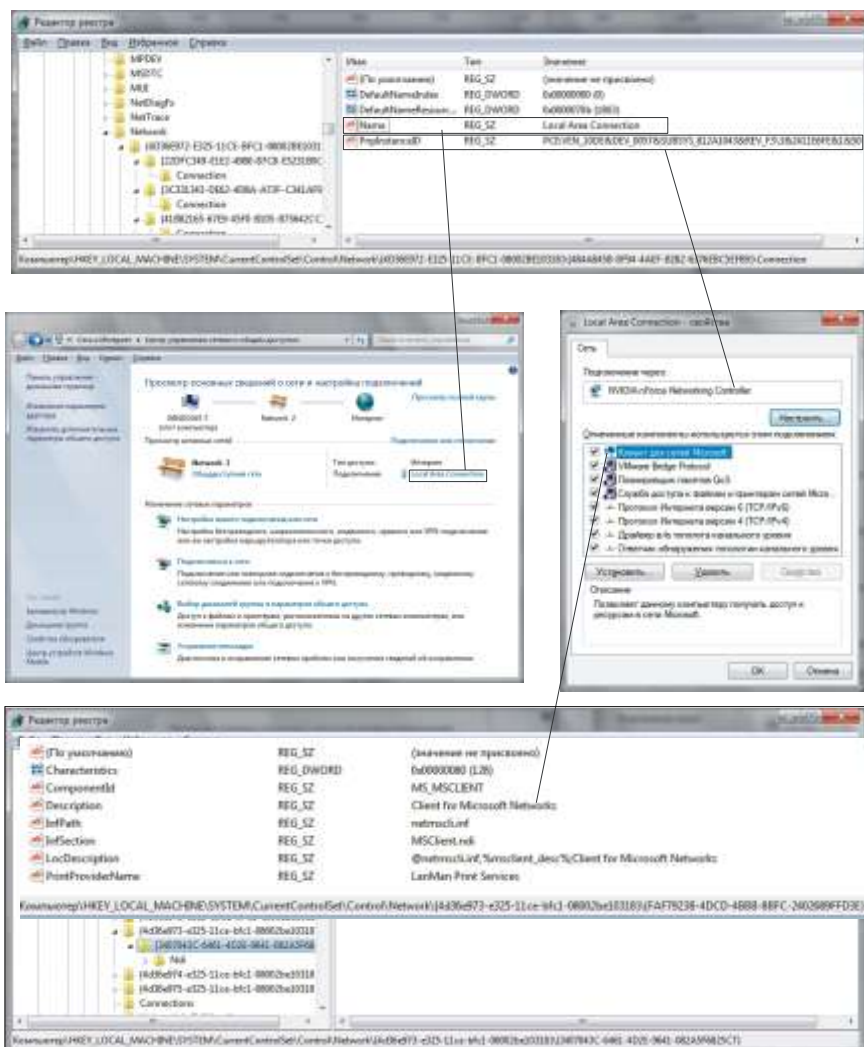


Рис. 8.21. Взаимосвязь информации реестра с параметрами соединения с локальной сетью, устанавливаемыми с помощью Центра управления сетями и общим доступом в Windows 7

Последовательно раскрывая эти ключи и исследуя их содержимое, можно обнаружить всю необходимую информацию о конфигурации сетевых средств. Например, вложенный ключ с именем {4D36E972-E325-11CE-BFC1-08002BE10318} (как вы помните, эта строка обозначает сетевые адаптеры) содержит на нижнем уровне иерархии ключ с именем `Connection` (рис. 8.20). Легко обнаружить, что этот ключ задает свойства соединения с локальной сетью: строковый параметр `Name` задает значение Подключение по локальной сети ("Local Area Connection"), которое вы видите в окне **Сеть и удаленный доступ к сети** (Network and Dial-up Connections), строковый параметр `PnPInstanceID` — это ссылка на ключ с информацией о нашем сетевом адаптере под ключом `Enum`. Информация о сетевых компонентах, используемых этим соединением, например, о клиенте для сетей Microsoft, также содержится в реестре.

Взаимосвязь информации реестра с параметрами соединения с локальной сетью, устанавливаемыми с помощью Центра управления сетями и общим доступом в Windows 7, проиллюстрирована на рис. 8.21.

Регистрационная информация сетевых компонентов

Регистрационная информация сетевых сервисов располагается в составе ключа реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services`. В составе этого ключа реестра, помимо ключей, характеризующих прочие сетевые компоненты, присутствуют и ключи сервисов, ассоциированных с сетевыми адаптерами. Вложенный ключ `nvenetfd`, характеризующий параметры драйвера сетевого адаптера NVIDIA nForce, показан на рис. 8.22.

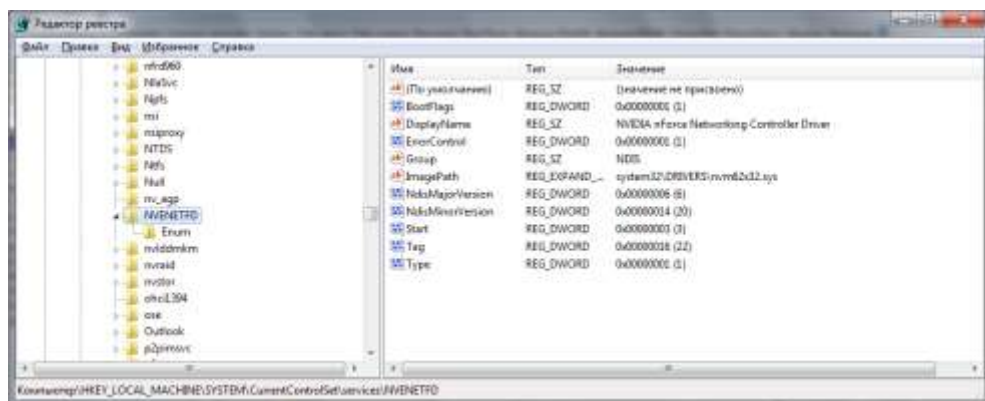


Рис. 8.22. Ключ реестра

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\nvenetfd` содержит конфигурационную информацию драйвера сетевого адаптера NVIDIA nForce

Кроме того, в составе ключа `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services` присутствуют вложенные ключи, характеризующие каждый из установленных сетевых компонентов (рис. 8.23).

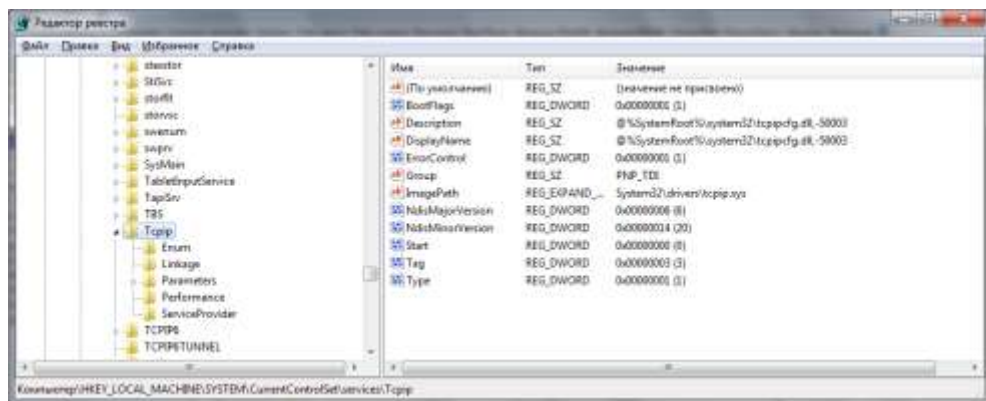


Рис. 8.23. Ключ реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services` содержит вложенные ключи для каждого из установленных сетевых компонентов

Краткий обзор нововведений в сетевых технологиях Windows Vista и Windows 7 и их взаимосвязи с реестром

Разумеется, максимально полное и подробное описание всех сетевых средств Windows Vista/7, а также соответствующих им элементов реестра в рамки одной главы уложить просто невозможно. Тем не менее, в последующих нескольких разделах будет сделана попытка изложить эту информацию хотя бы вкратце. Читателя, решившего исследовать данную тему самостоятельно, ждет на этом пути множество интереснейших находок и открытий.

Карта сети и поддерживающие ее протоколы

Уже начиная с Windows Vista в состав операционной системы было включено множество разнообразных усовершенствований, многие из которых сразу же бросаются в глаза и вызывают оживленную дискуссию среди пользователей. Одним из таких нововведений является Центр управления сетями и общим доступом (Network and Sharing Center) и, в особенности, представляемая им возможность построения миниатюрной карты сети (см. рис. 8.3). Какие же компоненты отвечают за построение карты сети? Внимательные читатели

просто не могли не заметить отличий окна **Подключение по локальной сети — свойства** (Local Area Connection Properties) от аналогичного окна в Windows XP. Взаимосвязь между построением карты сети и новыми компонентами показана на рис. 8.24.

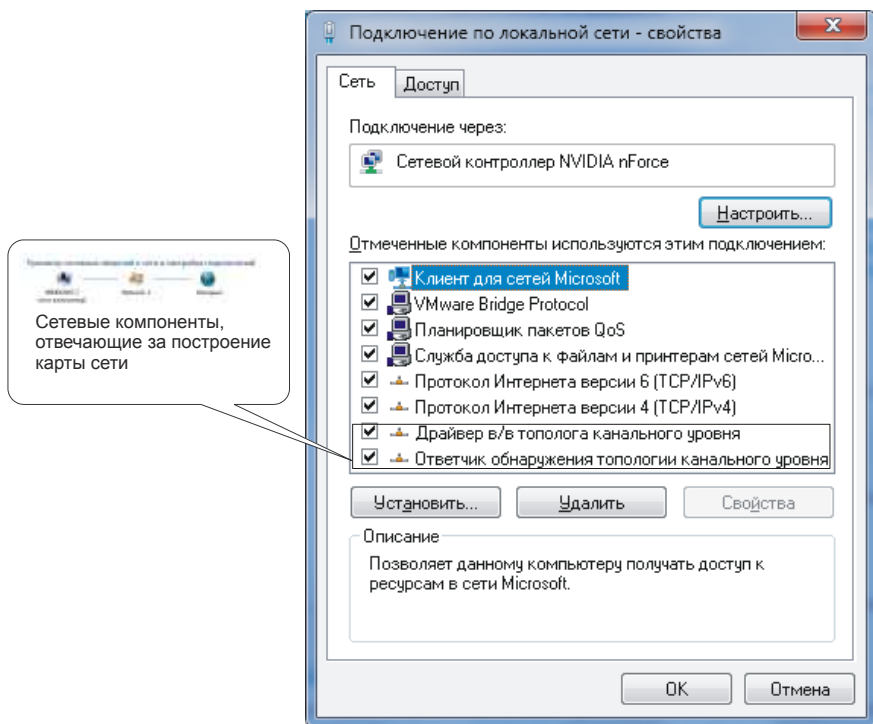


Рис. 8.24. За построение карты сети в Windows Vista и Windows 7 отвечают компоненты, реализующие новый сетевой протокол — Link-Level Topology Discovery (LLTD)

Windows Vista и Windows 7 используют сетевые протоколы канального уровня (Link Layer protocols) для транспортировки пакетов IP и IPv4, распознавания сетевых адресов, выполнения задач автоконфигурации и сбора информации для диагностики сети. Задача же построения карты сети возложена на новый протокол — протокол обнаружения топологии канального уровня (Link Layer Topology Discovery, LLTD). Этот протокол — ключевой компонент новой стратегии Microsoft по выполнению диагностики сети. На практике реализация LLTD в Windows Vista и Windows 7 состоит из двух логических компонентов, которые мы и видим на рис. 8.24:

- ❑ **Драйвер в/в тополога канального уровня** (Link-Layer Topology Discovery Mapper I/O Driver);

- **Ответчик обнаружения топологии канального уровня** (Link Layer Topology Discovery Responder).

ПРИМЕЧАНИЕ

В основе обнаружения топологии канального уровня лежат концепции *тополога* (Mapper) и *ответчика* (Responder). Топологом является хост, иницирующий определение топологии. Именно на нем будет отображаться карта сети. Ответчик представляет собой агента, который должен присутствовать на хостах, опрашиваемых топологом. Тополог может поддерживать коммуникации с одним или несколькими ответчиками одновременно, однако только один тополог может быть активен в сети в текущий момент времени.

Фактическая реализация LLTD в Windows Vista и Windows 7 включает файлы, перечисленные в табл. 8.2.

Таблица 8.2. Компоненты, реализующие протокол LLTD в Windows Vista/7

Файл	Роль
ltdio.sys	Драйвер ввода/вывода уровня ядра, который обрабатывает все запросы на распознавание других хостов сети и определяет ее полосу пропускания. Известен операционной системе как \Device\ltdio
rspndr.sys	Драйвер ввода/вывода уровня ядра, который отвечает за все взаимодействия, направленные на предоставление информации о сетевой топологии. Позволяет сервису тополога (ltdsvc) сделать данный хост видимым в сети
qwavedrv.sys	Драйвер ввода/вывода уровня ядра, связанный с qwave.dll
ltdsvc.dll	Сервис тополога канального уровня (ltdsvc), поддерживающий коммуникации с драйвером ltdio.sys
ltdapi.dll	Применяется пользовательским процессом Explorer для взаимодействия с сервисом ltdsvc
qwave.dll	Компонент, отвечающий за качество сервиса (QoS). Он хранит свои параметры в реестре, что позволяет включать и отключать трассировку
networkmap.dll	Применяется пользовательским процессом Explorer для создания карты сети. Взаимодействует с ltdapi.dll

Сервис тополога канального уровня в реестре носит имя `ltdsvc` (рис. 8.25). Если этот сервис заблокирован, то карта сети не будет функционировать правильно.

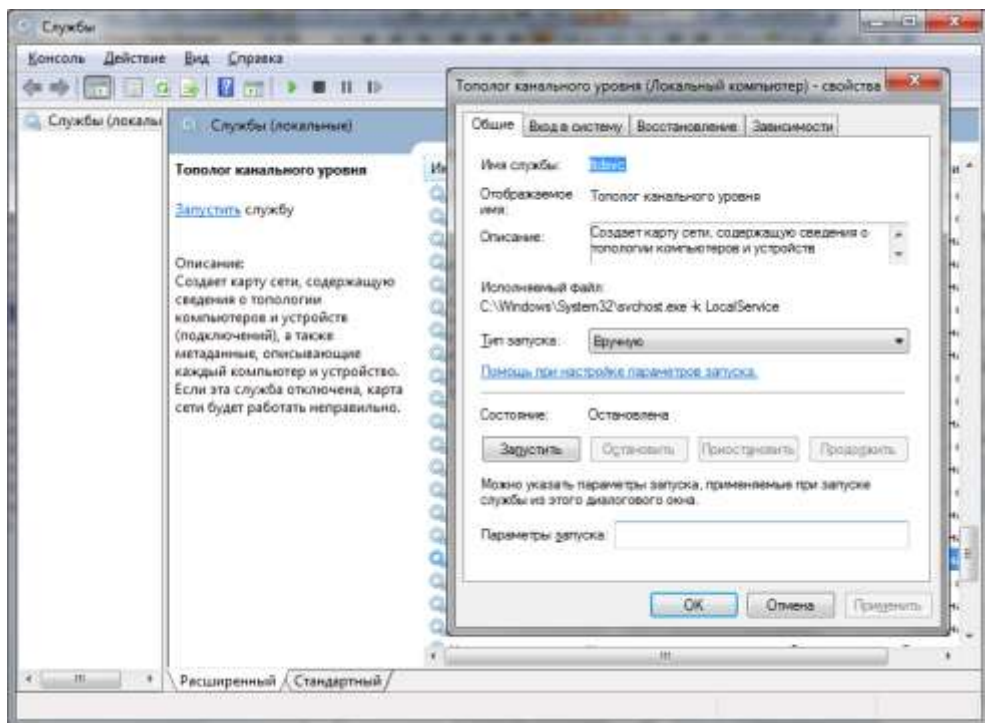


Рис. 8.25. Настройки сервиса тополога канального уровня

Конфигурирование сервиса тополога канального уровня

На компьютерах, подключенных к домену, построение карты сети по умолчанию заблокировано. Если ваш вариант поставки Windows включает групповые политики, то произвести конфигурирование параметров сервиса тополога канального уровня можно через пользовательский интерфейс. Это делается очень просто.

В первую очередь, откройте Редактор групповой политики. Для этой цели запустите сеанс командной строки с административными полномочиями и дайте команду `gpedit.msc`. В левой панели раскрывшегося окна Редактора объектов групповой политики разверните ветвь **Конфигурация компьютера** (Computer Configuration) | **Административные шаблоны** (Administrative Templates) | **Сеть** (Network) | **Обнаружение топологии связи** (Link-Layer Topology Discovery). Окно будет выглядеть примерно так, как показано на рис. 8.26.

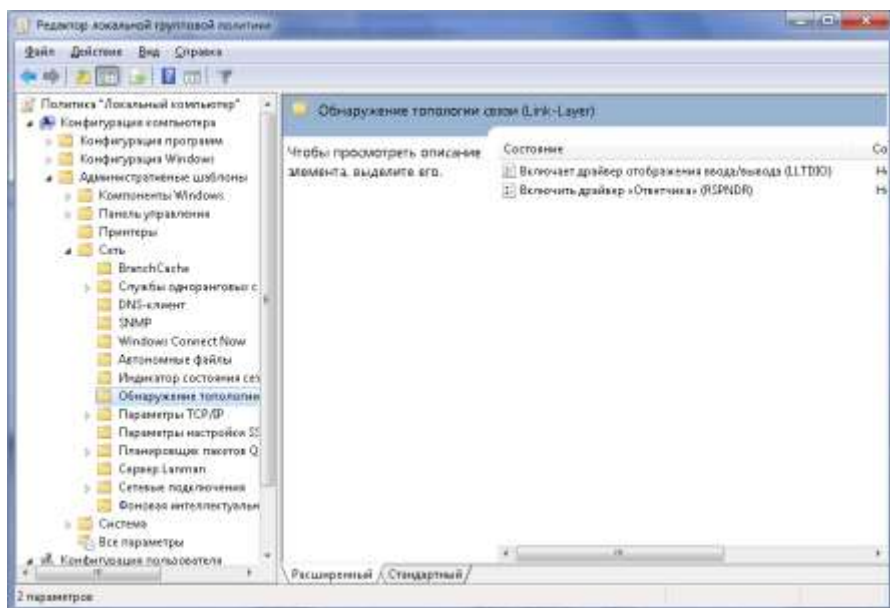


Рис. 8.26. Конфигурирование тополога канального уровня с помощью Редактора объектов групповой политики

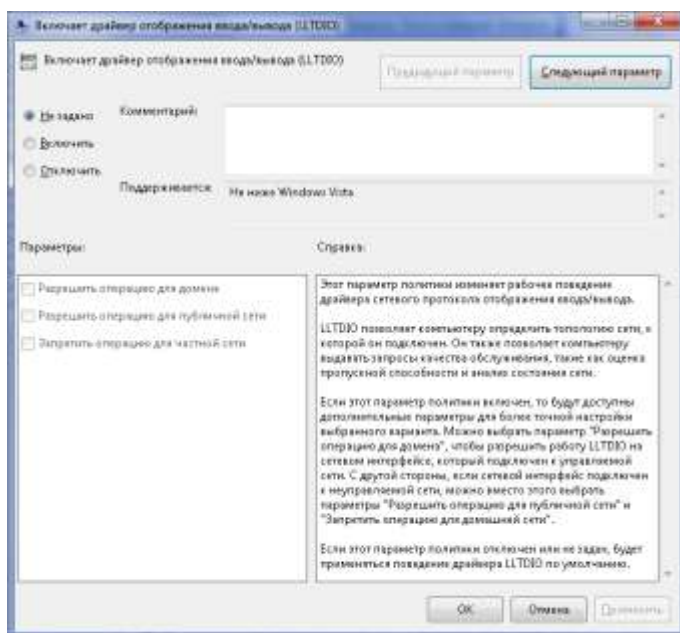


Рис. 8.27. Установка политики для драйвера отображения ввода/вывода (LLTDIO)

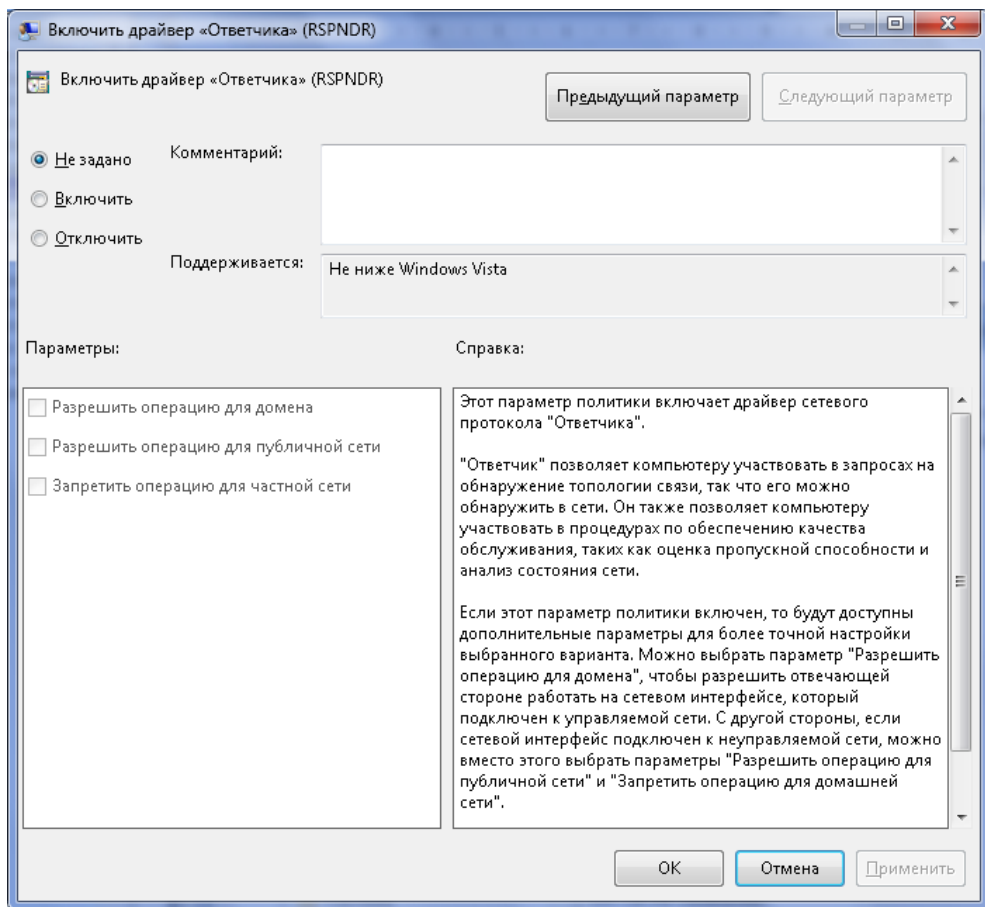


Рис. 8.28. Установка политики для драйвера "Ответчика" (RSPNDR)

В правой панели вы увидите две политики — для драйвера отображения ввода/вывода (LLTDIO) и для драйвера "Ответчика" (RSPNDR). Окна свойств каждой из этих политик показаны на рис. 8.27 и 8.28, соответственно. Чтобы активизировать каждую из политик, установите опцию **Включен** (Enabled), и вы получите возможность разрешить или запретить операцию для домена, публичной или частной сети.

СОВЕТ

Многие пользователи жалуются на то, что текст объяснения, отображаемый в панели **Справка** (Help) окон свойств политик (см. рис. 8.27 и 8.28) кажется им непонятным. Описание параметров реестра, приведенное далее в табл. 8.3, поможет вам лучше понять эти политики.

Настройка параметров групповой политики в отношении LLTD через реестр

Все параметры настройки групповой политики в отношении LLTD хранятся в составе HKLM\SOFTWARE\Policies\Microsoft\Windows\LLTD (рис. 8.29).

ПРИМЕЧАНИЕ

По умолчанию этого ключа в реестре нет, если не заданы соответствующие политики. Поэтому, если у вас имеется возможность редактировать реестр через системные политики, лучше именно так и поступать. Если такой возможности у вас нет, то сам ключ и соответствующие параметры придется создать и установить вручную.

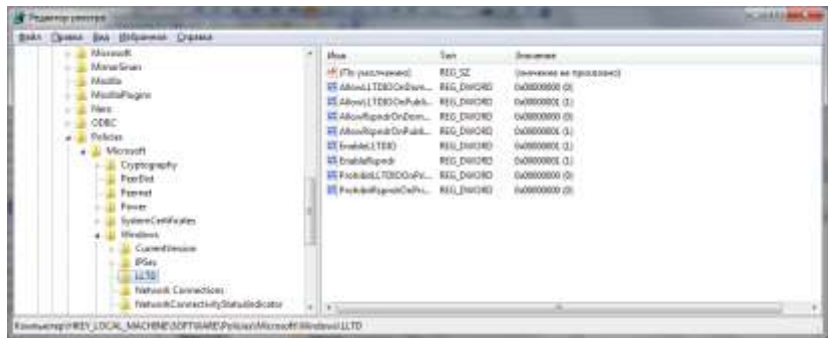


Рис. 8.29. Содержимое ключа реестра
HKLM\SOFTWARE\Policies\Microsoft\Windows\LLTD

Все параметры в составе этого ключа имеют тип данных REG_DWORD и могут принимать значения 1 или 0. Если тот или иной параметр отсутствует, то подразумевается, что он имеет значение по умолчанию. В табл. 8.3 приведены параметры реестра, описывающие настройки групповой политики в отношении LLTD.

Таблица 8.3. Параметры реестра, описывающие настройки групповой политики в отношении LLTD

Параметр	Значение по умолчанию	Описание
AllowLLTDioOnDomain	0	Если этот параметр установлен в 1, работа LLTDIO будет разрешена на сетевом интерфейсе, подключенном к доменной сети, членом которой является данный хост или с которой он может поддерживать коммуникации

Таблица 8.3 (окончание)

Параметр	Значение по умолчанию	Описание
AllowLLTDioOnPublicNet	0	Если этот параметр имеет значение 1, то работа LLTDIO будет разрешена на сетевом интерфейсе, подключенном к публичной сети
ProhibitLLTDioOnPrivateNet	0	Значение 1 запрещает работу LLTDIO на интерфейсах, подключенных к частной сети
EnableLLTDio	1	Значение 0 блокирует работу LLTDIO и отключает возможность построения карты сети
AllowRspndrOnDomain	0	Значение 1 разрешает работу драйвера "Ответчика" (RSPNDR) на сетевом интерфейсе, подключенном к доменной сети
AllowRspndrOnPublicNet	0	Значение 1 разрешает работу драйвера "Ответчика" (RSPNDR) на сетевом интерфейсе, подключенном к публичной сети
ProhibitRspndrOnPrivateNet	0	Значение 1 запрещает работу драйвера "Ответчика" (RSPNDR) на интерфейсах, подключенных к частной сети
EnableRspndr	1	Значение 0 блокирует работу драйвера сетевого протокола "Ответчика" (RSPNDR), запрещая тем самым хосту участвовать в запросах определения топологии сети

ПРИМЕЧАНИЕ

Внесенные изменения должны войти в силу немедленно. Однако в ряде случаев результат этих изменений замечен не сразу. Если вам хочется ускорить этот процесс, запустите сеанс командной строки с административными полномочиями и воспользуйтесь командой `sc` (предназначенной для отображения и конфигурирования сервисов) для останова и запуска сервисов. Для этой цели требуется дать такую последовательность команд:

```
sc stop lltdsvc
sc stop lltdio
sc stop rspndr
sc start rspndr
sc start lltdio
sc start lltdsvc
```

Взаимодействие Windows 7 с компьютерами, работающими под управлением Windows XP

Изначально компонент "Ответчика" (RSPNDR) для операционных систем Windows XP предусмотрен не был. В результате этого компьютеры, работающие под управлением Windows XP, не были видны на карте сети, создаваемой Windows Vista или Windows 7, поскольку они должны поддерживать протокол обнаружения, который может отвечать на запросы сопоставления системой Windows Vista/7. Для устранения этой проблемы на Windows XP следует установить обновление, описанное в статье из Microsoft Knowledge Base номер 922120 (<http://support.microsoft.com/kb/922120>).

Интеграция IPv4 и IPv6 в единый стек

Серьезным достижением Microsoft в области развития сетевых технологий стала интеграция протоколов IPv4 и IPv6 в единый стек (до этого они были реализованы как отдельные компоненты). Основное преимущество этого подхода состоит в том, что конечный пользователь получает готовый IPv6 без всякой головной боли и установки дополнительных пакетов. Вследствие катастрофической нехватки IP-адресов переход на IPv6 неизбежен, но затрудняется необходимостью смены сетевого оборудования и, соответственно, обновления серверных и клиентских операционных систем. Большинство провайдеров пока еще не поддерживают IPv6, а в локальных сетях вполне достаточно и IPv4, поэтому IPv6 в этой главе подробно не рассматривается. Заинтересованным читателям настоятельно рекомендуется прочесть учебник по компьютерным сетям, отражающий современный уровень развития сетевых технологий¹.

В этом разделе будут рассмотрены последствия интеграции IPv4 и IPv6 в единый стек, а именно — введение, начиная с Windows Vista, туннельных протоколов, в частности, Teredo².

Microsoft реализует Teredo в Windows Vista и Windows 7 с тем, чтобы обеспечить промежуточное решение для клиентов, в сетях которых отсутствует глобальная поддержка адресов IPv6. Фактически, протокол Teredo доступен и для более ранних версий Windows: XP SP1 (с дополнительным пакетом Advanced Networking Pack for Windows XP), XP SP2,

¹ См., например, N. Olifer, V. Olifer, "Computer Networks: Principles, Technologies and Protocols for Network Design", Wiley, 2006. Я рекомендую именно английский перевод, потому что он представляет собой существенно улучшенную, доработанную и дополненную версию исходного (русскоязычного) учебника.

² Простое описание Teredo дано на <http://www.microsoft.com/technet/network/ipv6/teredo.mspx>, а подробное — в RFC 4380 по адресу <http://www.rfc-editor.org/rfc/rfc4380.txt>.

а также Windows Server 2003 с SP1 и SP2. Тем не менее, только начиная с Windows Vista, протокол Teredo входит в состав операционной системы и активизирован по умолчанию.

Необходимость в Teredo возникла из-за ограничения, связанного с сетевыми трансляторами адресов (Network Address Translation, NAT) для IPv4 (IPv4 NAT devices), которые широко распространены. Дело в том, что такие устройства не поддерживают прямой передачи пакетов IPv6 или трафика "IPv6 поверх IPv4" (ISATAP/6to4). Поэтому, чтобы обойти проблему NAT, Teredo создает туннели UDP в обход NAT. Упрощенно говоря, Teredo инкапсулирует (упаковывает) трафик IPv6 в пакеты IPv4, используя для этой цели протокол UDP. Если два узла IPv6 разделены сегментом сети IPv4, то Windows Vista/7 использует Teredo для передачи запроса одному из публичных серверов Teredo, который, в свою очередь, передает его получателю. Таким образом, инфраструктура Teredo состоит из трех типов компонентов: клиентов Teredo, ретрансляторов Teredo и серверов Teredo (рис. 8.30).

Компоненты, реализующие Teredo в Windows Vista и Windows 7, перечислены в табл. 8.4.

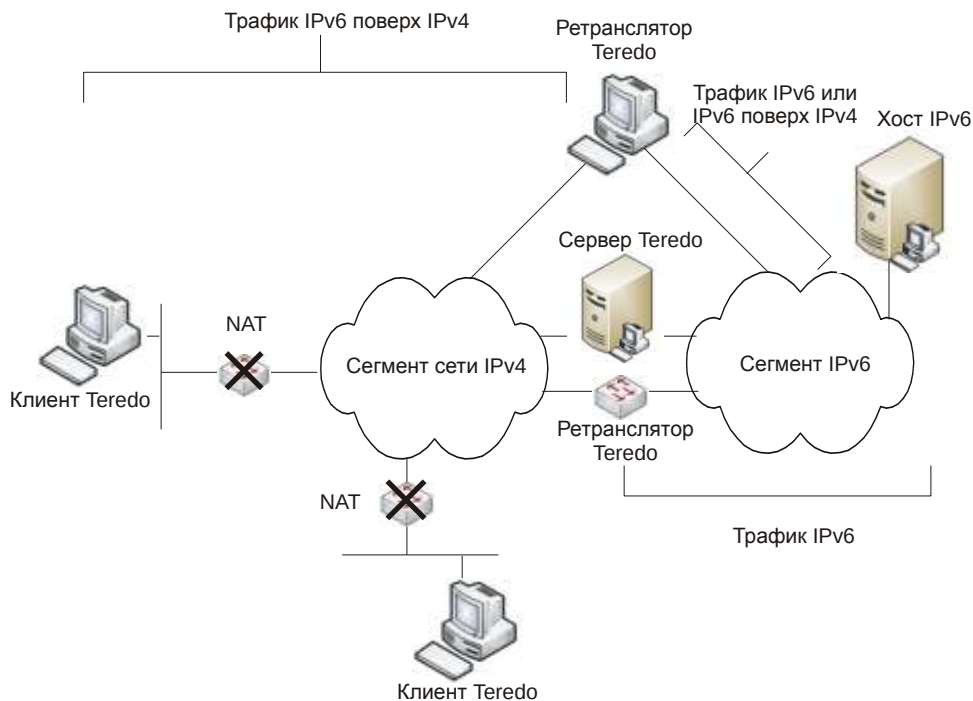


Рис. 8.30. Обход NAT с помощью Teredo

Таблица 8.4. Краткое описание компонентов Teredo в Windows Vista и Windows 7

File	Role
TUNMP.SYS	Драйвер уровня ядра, служащий для создания виртуального сетевого интерфейса, используемого Teredo
TUNNEL.SYS	Драйвер уровня ядра, служащий для создания виртуального сетевого интерфейса, используемого Teredo
IPHLPVC.DLL	Системный сервис (рис. 8.31), запускаемый сервисом SVCHOST и реализующий основной туннелирующий компонент Teredo. Этот сервис отвечает за установку туннеля, его конфигурирование и передачу информации между клиентом Teredo и сервером Teredo

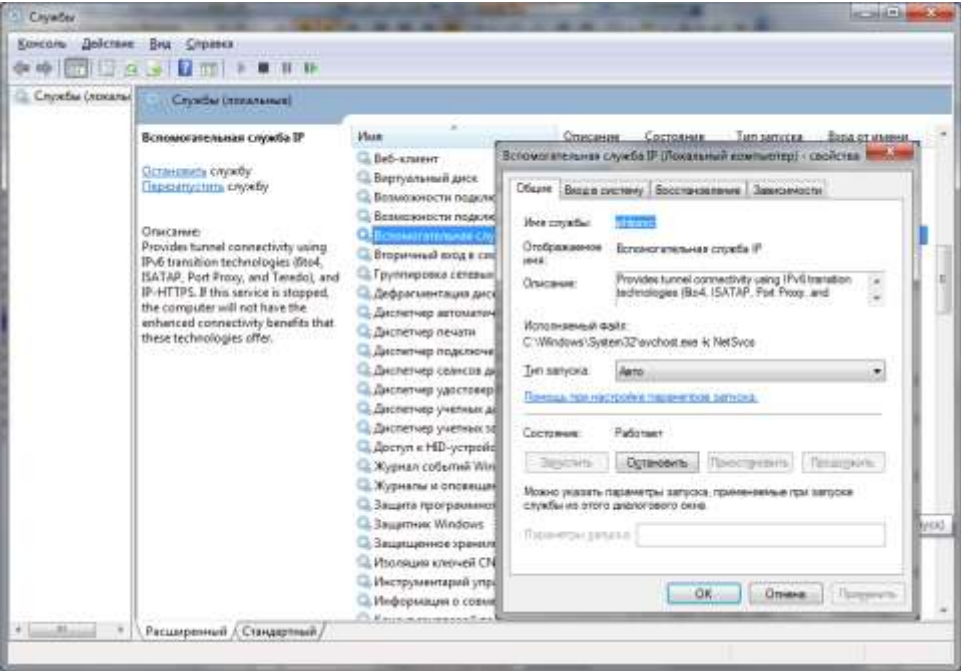


Рис. 8.31. Управление сервисом, реализующим основной туннелирующий компонент Teredo

ПРИМЕЧАНИЕ

В Windows Vista и Windows 7, компонент Teredo **Вспомогательная служба IP** (IP Helper) по умолчанию запускается автоматически, но изначально находится в "дремлющем" (dormant) состоянии. Чтобы этот сервис активизировался, пользователь должен либо установить некое приложение, которому требуется использовать Teredo, либо соответствующим образом сконфигурировать настройки Брандмауэра Windows (Windows Firewall).

Конфигурирование Teredo

Для конфигурирования Teredo в Windows Vista используется команда `netsh.exe`. На рис. 8.32 показан результат работы команды `netsh interface ipv6 show teredo` — на экран выводится информация о текущем состоянии интерфейса Teredo на локальном хосте (в данном случае интерфейс Teredo имел настройки по умолчанию).

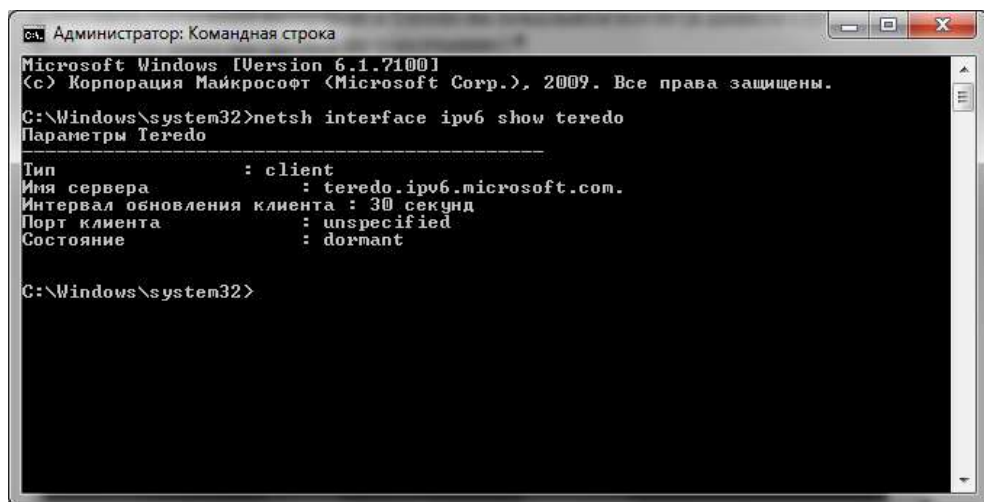


Рис. 8.32. Вывод команды `netsh interface ipv6 show teredo`

ПРИМЕЧАНИЕ

"Неопределенный" (unspecified) порт клиента означает, что сервисом Teredo на клиентском компьютере выбирается анонимный (эфемерный) порт. Обратите внимание, что для серверного порта настроек нет, так как предполагается, что для этой цели всегда используется порт UDP 3544.

Блокировка Teredo

Как уже говорилось, Teredo использует протокол UDP, слабости и недостатки которого хорошо известны. С безопасностью самого Teredo также существуют определенные проблемы³. Поэтому некоторые администраторы могут захотеть блокировать этот интерфейс, если он не нужен. Teredo в Microsoft Windows Vista/7 можно блокировать следующими способами:

- ❑ остановить сервис IPHLPV6 (см. рис. 8.31);

³ См. http://www.symantec.com/avcenter/reference/Teredo_Security.pdf.

- ☐ произвести "отвязку" (unbinding) протокола IPv6 от сетевого интерфейса;
- ☐ сконфигурировать параметры стека IPv6.

Предпочтительный метод блокировки Teredo в Windows Vista и Windows 7 — последний из перечисленных вариантов, а именно: конфигурирование параметров стека IPv6. Параметры стека IPv6 хранятся в реестре под ключом `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\tcpip6\Parameters` (рис. 8.33).

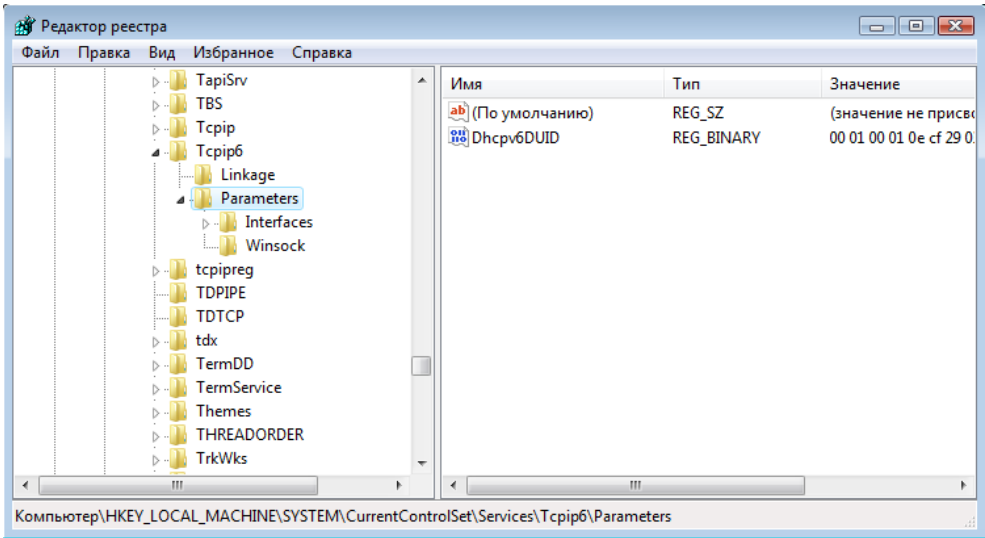


Рис. 8.33. Содержимое ключа реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\tcpip6\Parameters` (настройки по умолчанию)

Для блокировки нужной комбинации туннелирующих протоколов создайте в составе этого ключа параметр `DisabledComponents` (тип данных `REG_DWORD`). Чтобы блокировать все туннелирующие протоколы или некоторую их комбинацию, используйте табл. 8.5.

Таблица 8.5. Значения параметра `DisabledComponents` для блокировки всех туннелирующих протоколов или некоторой их комбинации

Комбинация блокируемых протоколов	Значение параметра <code>DisabledComponents</code>
Все туннелирующие протоколы	0x01
6to4	0x02
ISATAP	0x04

Таблица 8.5 (окончание)

Комбинация блокируемых протоколов	Значение параметра DisabledComponents
Teredo	0x08
Teredo и 6to4	0x0A
Все интерфейсы LAN и PPP	0x10
Все интерфейсы LAN, PPP и туннелирующих протоколов	0x11
IPv4 поверх IPv6	0x20
Блокировать IPv6 поверх всех интерфейсов и IPv4 поверх IPv6	0xFF

Новинка Windows 7 — Домашняя группа

В начале этой главы уже упоминалось сетевое нововведение, появившееся впервые в Windows 7, — а именно *домашняя группа* (home group). Что же она собой представляет?

Домашняя группа (HomeGroup) — это простой и удобный метод объединения компьютеров в вашей домашней сети таким образом, чтобы обеспечить всем пользователям этой сети общий доступ к изображениям, музыкальным файлам, видео, документам и принтерам. Для доступа к домашней группе используется единый общий пароль, благодаря чему подключение упростилось до предела.

Эту новую возможность тяжело переоценить. Если вы работали с более ранними версиями Windows, то наверняка помните, что процесс организации домашней сети был делом, мягко говоря, не слишком простым. Хотя в последующих версиях операционной системы, начиная с Windows XP, в сторону упрощения и совершенствования технологий организации домашних сетей и были выполнены определенные шаги, процесс все равно оставался сложным, причем так было и в Windows Vista. К счастью, в Windows 7 эта проблема наконец-то решена. Домашняя группа — это действительно удобное и удачное решение проблемы.

Итак, что же на самом деле представляет собой HomeGroup в Windows 7? Это — новая реализация мастера организации сети, с помощью которой домашнюю сеть действительно можно создать за три простых шага, которые мы сейчас и рассмотрим.

Если вы устанавливали Windows 7 самостоятельно, а не получили ее в прединсталлированном виде, то наверняка помните, что в процессе установки, на завершающих ее стадиях, вам предлагалось выбрать местоположение

компьютера (фактически — тип сети: домашняя, публичная или сеть предприятия). К домашней группе можно подключить только те компьютеры, для которых выбран тип домашней сети. Впрочем, домашние пользователи, как правило, всегда выбирают именно домашнюю сеть.

Если вы выбрали сеть другого типа, то вы увидите окно, показанное на рис. 8.34.

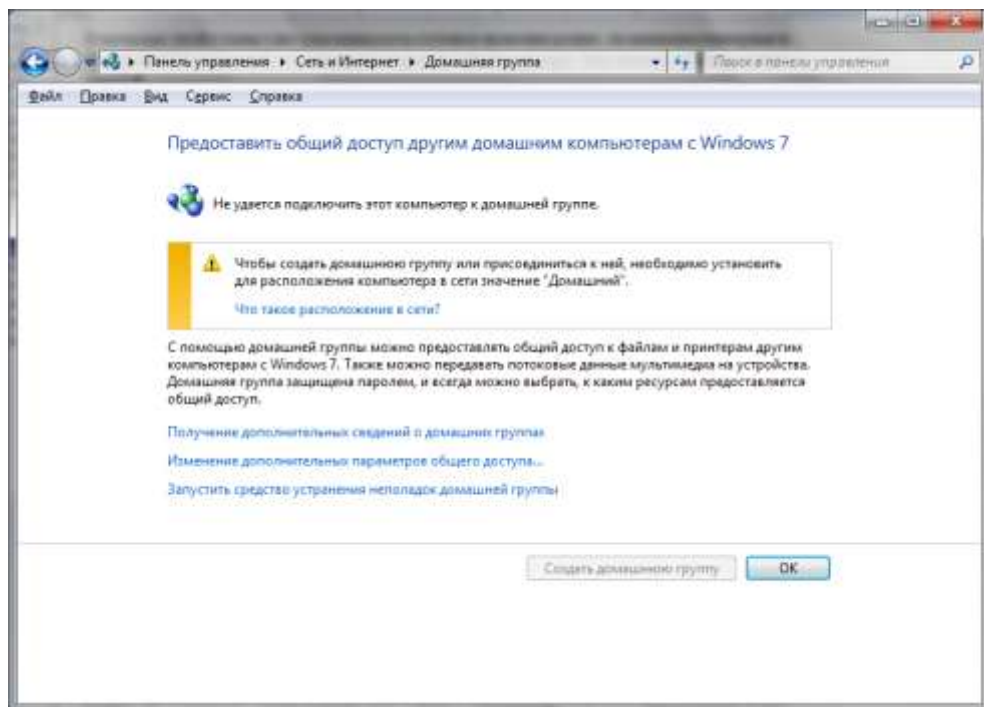


Рис. 8.34. Окно с сообщением о невозможности подключить компьютер к домашней группе

Однако эту сложность легко преодолеть. Все, что потребуется для этого сделать — изменить тип сети (примерно так же, как это делалось в Windows Vista). Однако теперь Windows 7 автоматически модифицирует все настройки таким образом, чтобы обеспечить удобный совместный доступ ко всем ресурсам домашней сети. Вернитесь в окно Центра управления сетями и общим доступом (см. рис. 8.3) и щелкните мышью по ссылке, расположенной под значком, символизирующим тип вашей сети (см. рис. 8.3). На экране откроется окно, предлагающее выбрать расположение для вашей сети (рис. 8.35).

Выберите опцию **Домашняя сеть** (Home), и мастер предложит вам создать домашнюю группу (рис. 8.36).

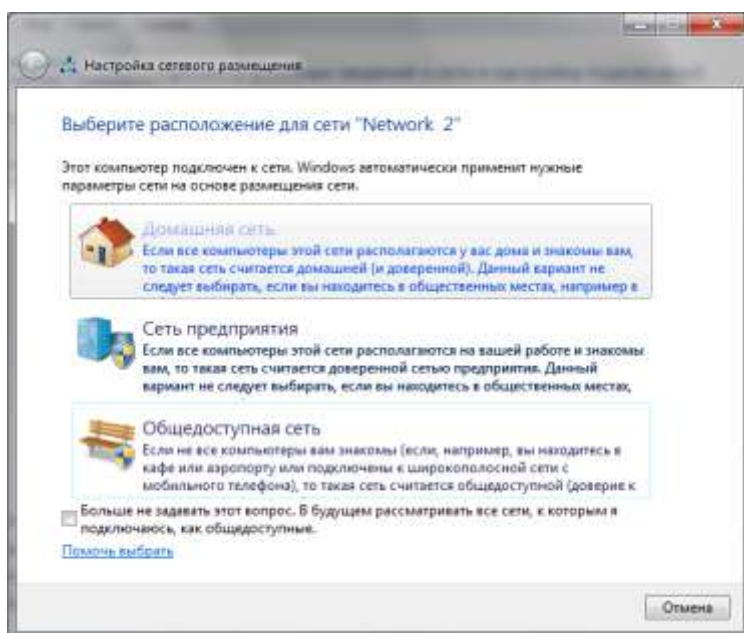


Рис. 8.35. Выбор расположения для вашей сети

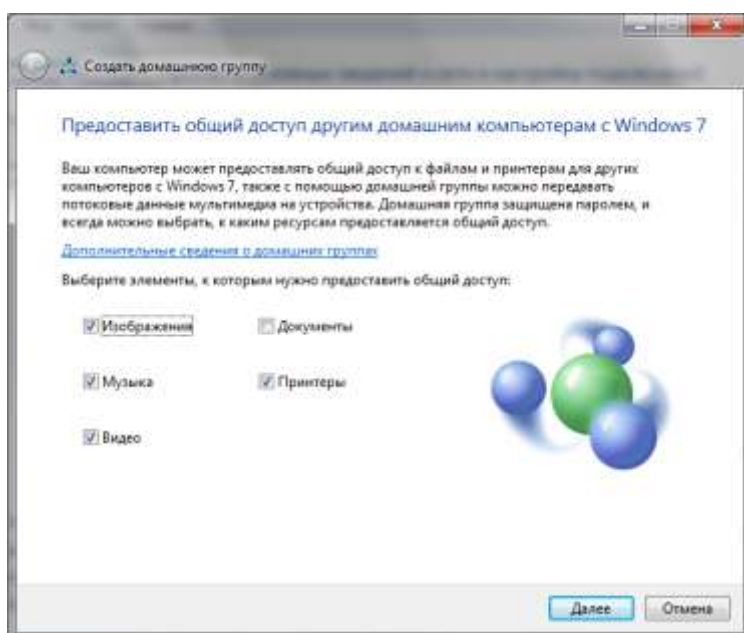


Рис. 8.36. Мастер настройки сети предложит вам создать домашнюю группу

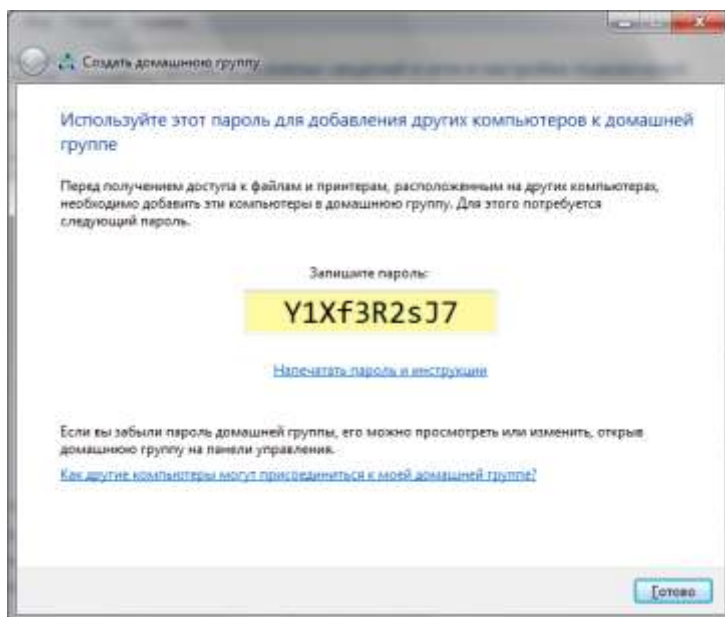


Рис. 8.37. Мастер настройки сети автоматически создает пароль для подключения к домашней группе

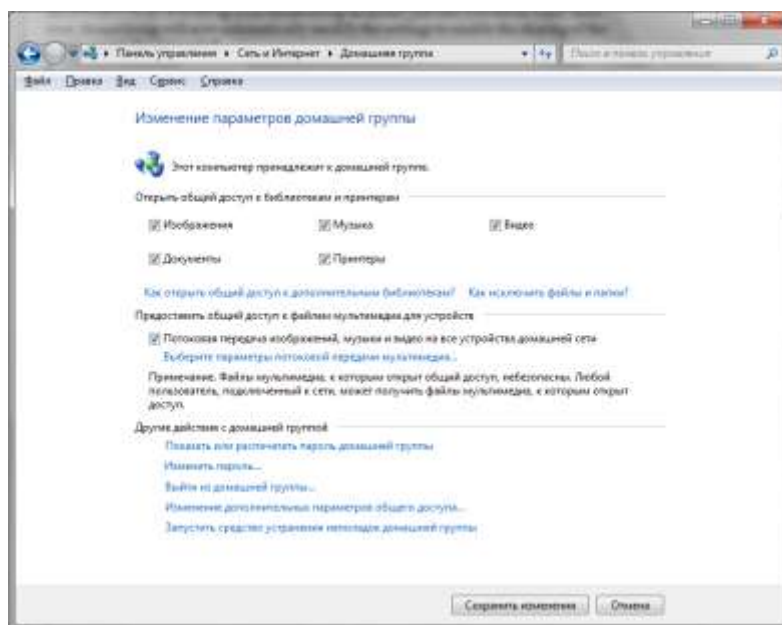


Рис. 8.38. Изменение параметров домашней группы

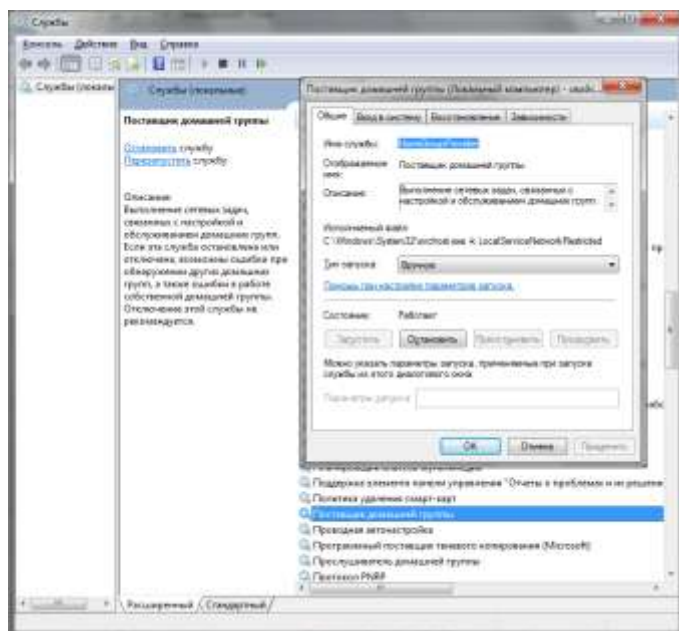


Рис. 8.39. Параметры сервиса Поставщик домашней группы

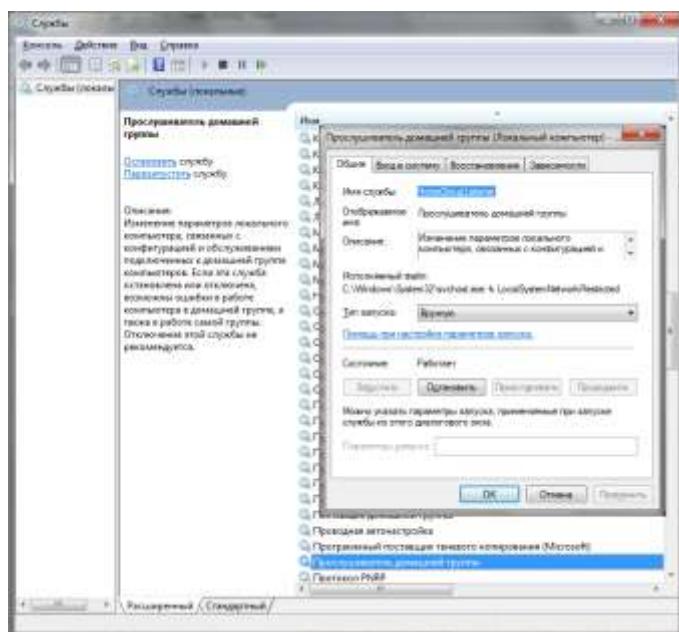


Рис. 8.40. Параметры сервиса Прослушиватель домашней группы

Выберите тип информации, к которой вы хотите предоставить доступ другим компьютерам вашей домашней сети, и нажмите кнопку **Далее** (Next). Мастер настройки сети автоматически сгенерирует для вас достаточно сильный пароль, который вы впоследствии будете использовать для присоединения новых компьютеров к домашней группе (рис. 8.37). Пароль, в соответствии с данными в окне рекомендациями, действительно рекомендуется записать (и, при возможности, распечатать). Впрочем, впоследствии вы всегда сможете его просмотреть и изменить, если в этом возникнет необходимость (рис. 8.38). Нажмите кнопку **Готово** (Finish), и домашняя группа будет создана.

Поддержка функциональных возможностей, предоставляемых домашней группой, осуществляется двумя сервисами: **Поставщик домашней группы** (HomeGroup Provider) и **Прослушиватель домашней группы** (HomeGroup Listener), параметры которых показаны на рис. 8.39 и 8.40, соответственно.

Разумеется, нашли эти сервисы свое отражение и в реестре (рис. 8.41). Их параметры находятся под ключами `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\HomeGroupListener` и `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\HomeGroupProvider`, **соответственно**.

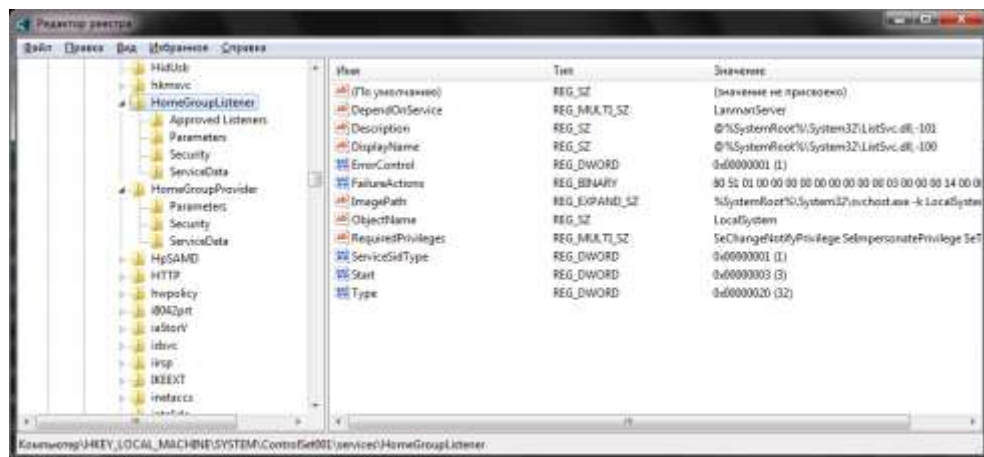


Рис. 8.41. Параметры сервисов, поддерживающих функциональность домашней группы, в реестре Windows 7

Мне уже случалось слышать о том, что HomeGroup — очередная "игрушка", "бантик", "свисток"... Но вот, поверьте, что это не так. Для пользователей домашней сети Домашняя группа — самое то, что надо, особенно в сочетании с такой новой возможностью Windows 7, как **Библиотеки** (Libraries). Встречала я и рекомендации блокировать оба сервиса: и HomeGroup Provider,

и HomeGroup Listener. Замечу здесь, что делать это имеет смысл лишь в тех случаях, когда в вашей сети имеется только один компьютер, работающий под управлением Windows 7 (ваш), а все остальные клиенты сети работают под управлением более ранних версий Windows, а также если вы по каким-либо причинам не хотите пользоваться домашней группой. Тогда — да, блокировка этих сервисов будет представлять собой разумный шаг.

В остальных же случаях это неразумно, поскольку домашняя группа позволяет просто-напросто забыть о множестве проблем с общим доступом к Интернету, общим доступом к файлам и папкам, заданием пользовательских прав и многим-многим другим, которые отравляли жизнь пользователям домашних сетей до последнего времени.

Настройка сетевых средств путем редактирования реестра

В последующих разделах будут описаны некоторые из методов настройки сети путем редактирования реестра, а также возможные методы решения возникающих проблем.

Автоматическое конфигурирование IP-адресов

В Windows 7, как и в Windows 2000/XP/Vista, существует возможность *автоматического конфигурирования IP-адресов* (Automatic Private IP Addressing, APIPA). В чем же заключается эта функциональная возможность и как она работает?

Как известно, при инсталляции Windows стандартный вариант установки сетевых средств включает протокол TCP/IP, причем по умолчанию предполагается, что IP-адрес и маску подсети клиентский компьютер будет получать от сервера DHCP. Многим пользователям известны проблемы, возникающие в случае конфликта IP-адресов или когда сервер DHCP оказывался недоступным. Функция автоконфигурирования IP-адресов позволяет клиентам DHCP автоматически конфигурировать свой IP-адрес и маску подсети в условиях, когда сервер DHCP временно недоступен.

ПРИМЕЧАНИЕ

Функция автоконфигурирования IP-адресов в Windows Vista и Windows 7 имеет небольшое отличие от аналогичной функции в Windows XP. Если при запуске компьютера под управлением Windows XP операционная система не может обнаружить сервер DHCP, она ожидает в течение 3 минут и только затем обращается к APIPA. Windows Vista и Windows 7 в аналогичной ситуации ждут ответа от сервера DHCP только в течение шести секунд и сразу начинают

использовать APIPA. Далее Windows продолжает попытки получить динамический IP-адрес от сервера DHCP.

Для конфигурирования компьютера в качестве клиента DHCP следует установить переключатель **Получить IP-адрес автоматически** (Obtain an IP address automatically) на вкладке **Общие** (General) окна **Свойства: Протокол Интернета версии 4 (TCP/IPv4)** (Internet Protocol (TCP/IPv4) Properties) (рис. 8.42).

ПРИМЕЧАНИЕ

Все клиентские компьютеры Windows 2000/XP/Vista по умолчанию конфигурируются как клиенты DHCP.

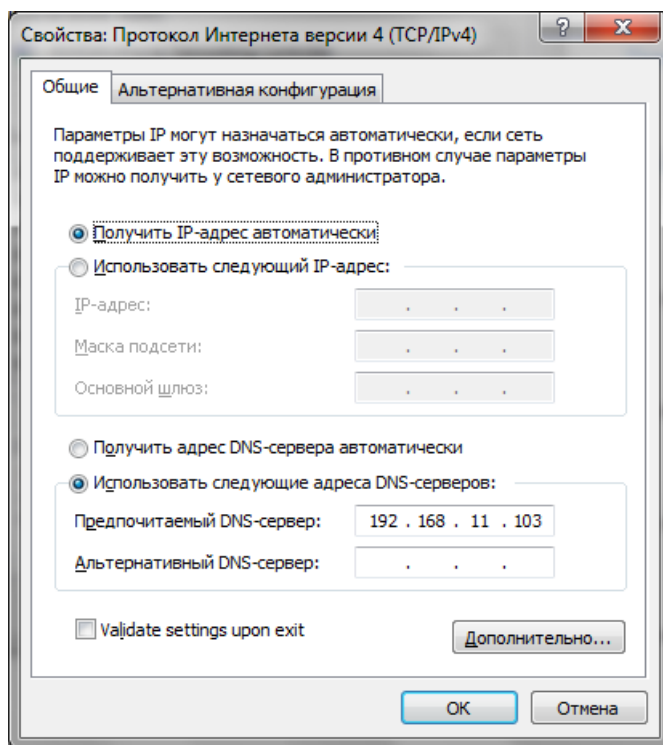


Рис. 8.42. Вкладка **Общие** окна **Свойства: Протокол Интернета версии 4 (TCP/IPv4)**

При загрузке клиент DHCP ищет сервер DHCP, чтобы получить от него конфигурационную информацию TCP/IP (как правило, это IP-адрес, маска подсети и, возможно, некоторые другие опции DHCP). Если клиент не может получить эту информацию от сервера DHCP, он использует APIPA и автома-

тически устанавливает себе IP-адрес из диапазона адресов (от 169.254.0.1 до 169.254.255.254), специально зарезервированных для этой цели и не используемых в Интернете. В качестве маски подсети в этом случае используется стандартная маска подсети класса B: 255.255.0.0. Поскольку в случае самоконфигурирования клиент выбирает IP-адрес случайным образом, в сети могут возникать конфликты IP-адресов, для разрешения которых служит протокол ARP (Address Resolution Protocol). Выбрав произвольный IP-адрес из зарезервированного диапазона, клиент отправляет в сеть пакет ARP, и если на этот пакет не отвечает ни один из остальных компьютеров, он сохраняет этот адрес. Если выбранный IP-адрес уже используется другим компьютером, следует до 10 повторных попыток выбора другого IP-адреса. Клиент использует эту конфигурационную информацию до тех пор, пока сервер DHCP не станет снова доступен. Несложно понять, что функциональная возможность APIPA очень удобна в небольших немаршрутизируемых сетях.

ПРИМЕЧАНИЕ

На рис. 8.42 вы, вероятно, обратите внимание на одно из наиболее полезных свойств, впервые введенных в еще в Windows XP, — так называемую *альтернативную адресацию* (Alternate Addressing), которое по достоинству оценили многие пользователи мобильных компьютеров. Проблема заключается в том, что такие компьютеры часто подключаются к нескольким сетям. При этом в одном случае используется статический IP-адрес, а в другом назначение адреса происходит динамически. Смена подключений каждый раз требует перенастройки установок IP. Начиная с Windows XP, эта проблема успешно решена. Теперь пользователь может сконфигурировать портативный компьютер так, чтобы сначала использовать динамический IP-адрес, а затем — альтернативный IP-адрес, если DHCP-сервер недоступен. Для того чтобы использовать эту функциональную возможность, откройте окно **Свойства: Протокол Интернета версии 4 (TCP/IPv4)** (Internet Protocol (TCP/IPv4) Properties) и выберите переключатель **Получить IP-адрес автоматически** (Obtain an IP address automatically), а затем перейдите на вкладку **Альтернативная конфигурация** (Alternate Configuration) (рис. 8.43) и сконфигурируйте альтернативный IP-адрес. Обратите внимание, что второй адрес может быть как постоянным, так и назначаемым с помощью APIPA.

Если APIPA требуется блокировать, сделайте следующее:

1. Вызовите Редактор реестра и раскройте ключ `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces`.
2. Выделите вложенный ключ адаптера, для которого требуется блокировать APIPA, добавьте в его состав параметр `IPAutoconfigurationEnabled` (тип данных `REG_DWORD`) и установите для этого параметра значение 0 (значение по умолчанию равно 1).

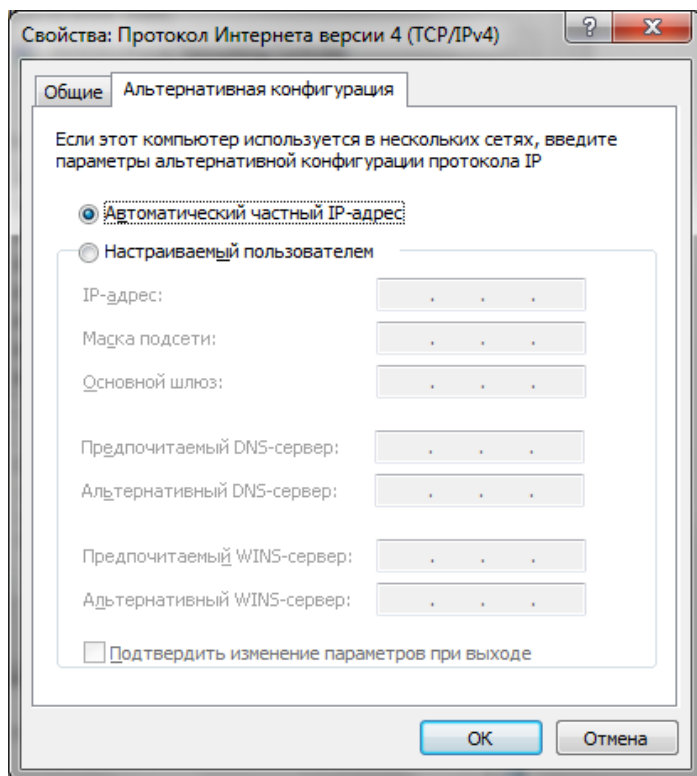


Рис. 8.43. Вкладка **Альтернативная конфигурация** в окне **Свойства: Протокол Интернета версии 4 (TCP/IPv4)**

ПРИМЕЧАНИЕ

Добавлять параметр `IPAutoconfigurationEnabled` следует только в том случае, когда требуется блокировать APIPA. Если на компьютере установлено несколько сетевых адаптеров, и функцию APIPA требуется блокировать для каждого из них, добавьте параметр `IPAutoconfigurationEnabled` в состав ключа `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters` и установите его значение равным 0.

Блокировка динамической регистрации DNS

Компьютеры, работающие под управлением Windows 7, как и компьютеры, работающие под управлением Windows 2000/XP/Vista, пытаются выполнять динамическую регистрацию на серверах DNS, указанных на вкладке **Общие** (General) окна свойств TCP/IP (см. рис. 8.42). Чтобы блокировать эту опцию, нажмите кнопку **Дополнительно** (Advanced), в раскрывшемся диалоговом окне **Дополнительные параметры TCP/IP** (Advanced TCP/IP Settings)

перейдите на вкладку **DNS** (рис. 8.44) и сбросьте флажок **Зарегистрировать адреса этого подключения в DNS** (Register this connection's addresses in DNS).

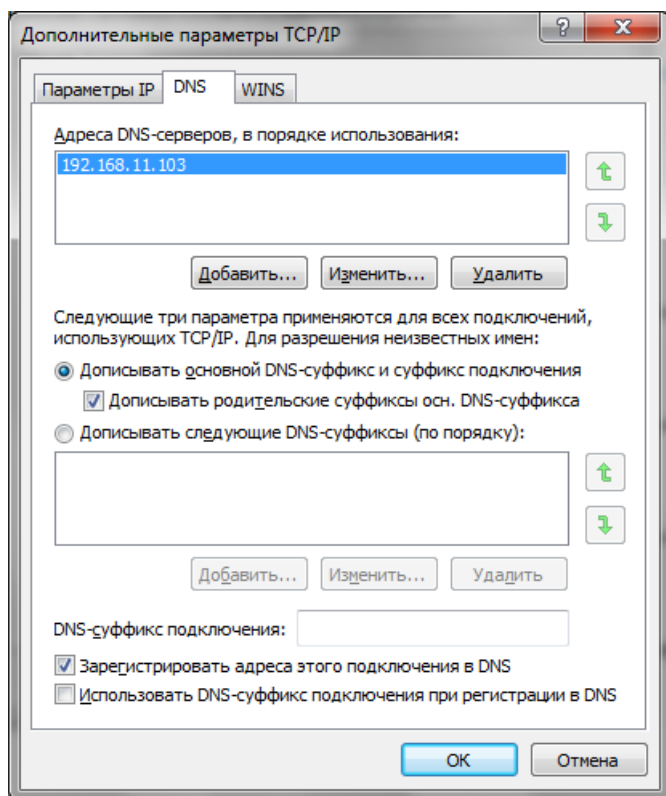


Рис. 8.44. Вкладка **DNS** окна **Дополнительные параметры TCP/IP**

Если вы хотите проделать то же самое путем редактирования реестра, то откройте ключ `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces` и установите значение параметра `DisableDynamicUpdate` (тип данных `REG_DWORD`) равным 1.

Заключение

Итак, в этой главе мы кратко рассмотрели параметры настройки сети в реестре Windows Vista. В следующей главе мы перейдем к важному вопросу защиты реестра Windows Vista (в том числе и от удаленного доступа через сеть).

Глава 9



Защита реестра

Это тайна, страшная тайна! Завещание было запечатано в семи конвертах семью сургучными печатями и скреплено подписями семи тайных советников. Вскрывала и читала завещание принцесса в полном одиночестве. У окон и дверей стояла стража, заткнув уши на всякий случай, хотя принцесса читала завещание про себя. Что сказано в этом таинственном документе, знает только принцесса и весь город.

Е. Шварц, "Тень"

Vista_Error: 01B Illegal error — You are not allowed to get this error¹.

Фольклор

Подсистема безопасности Windows, как и все компоненты операционной системы, тесно взаимосвязана с реестром и реализована через него. При этом реестр, реализуя систему безопасности и взаимодействуя с ней, и сам нуждается в защите.

Наверняка вам не захочется, чтобы выстроенная вами система защиты реестра создавала неудобства легальным пользователям и в то же самое время практически ни от чего не защищала. Стоит сразу же отметить, что обсуждаемые в этой главе меры защиты реестра необходимо знать каждому администратору, всерьез озабоченному проблемой обеспечения безопасности.

Windows NT/2000/XP/Vista, а также Windows 7 — это единственное семейство операционных систем Microsoft, в котором с начального момента разработки

¹ Ошибка Vista: 01B Незаконная ошибка — вам не разрешается получать это сообщение.

было уделено должное внимание требованиям безопасности (класс защищенности C2). Национальное агентство США по безопасности (U. S. National Security Agency, NSA) разработало набор критериев, в соответствии с которыми выполняется оценка защищенности компьютеров и программного обеспечения. Все эти критерии были опубликованы в виде книг, каждая из которых имела обложку определенного цвета, вследствие чего весь набор критериев получил известность под названием "Радужной серии" (Rainbow Series). Критерии TCSEC (Trusted Computer System Evaluation Criteria, TCSEC) — так называемая "Оранжевая книга" (Orange Book) — регламентируют процедуру оценки защищенности информационных систем правительственными организациями. Американский класс защищенности C2 официально считается высшим классом защищенности, сертификацию по которому могут получить потребительские операционные системы общего назначения.

ПРИМЕЧАНИЕ

Уровень защищенности C2 не является наивысшим для всех операционных систем вообще. Для сертификации защищенных операционных систем, применяющихся в военной области, атомной энергетике и других стратегически важных областях, высшим является класс А. Более низкими по отношению к C2 являются только классы C1 (сертификация по которому не проводится) и D (класс, к которому относятся все операционные системы, не попадающие в другие классы). Более подробная информация о существующих классах защищенности есть на <http://www.fas.org/lirp/nsa/rainbow.htm> и <http://www.governmentsecurity.org/articles/RainbowSeriesLibraryTheOneTheOnly.php>, и http://www.windowsecurity.com/whitepapers/rainbow_series/.

Требования к операционной системе, защищенной по классу C2, включают:

- ☐ обязательную идентификацию (identification) и аутентификацию (authentication) всех пользователей операционной системы и предоставление доступа к ресурсам только этим пользователям;
- ☐ разграничительный контроль доступа (discretionary access control, DAC) — предоставление пользователям возможности защиты принадлежащих им данных;
- ☐ системный аудит (system auditing) — способность системы вести подробную проверку всех действий, выполняемых пользователями и самой операционной системой;
- ☐ защиту объектов от повторного использования — способность системы предотвратить доступ пользователя к информации и ресурсам, с которыми до этого работал другой пользователь (например, обеспечение невозможности повторного использования освобожденной памяти или чтения данных из файлов, которые были удалены).

В процесс сертификации операционной системы по уровню защищенности C2 входят:

- исследование исходного кода;
- изучение документации о подробностях реализации, предоставленной разработчиками;
- повторное тестирование с целью устранения всех ошибок, выявленных в ходе оценки.

Что касается Windows 7, то говорить о ее защищенности по классу C2 пока еще очень рано, хотя определенные шаги в этом направлении делаются уже сейчас. Так, в *главе 7*, посвященной процессу загрузки операционной системы, говорилось об усовершенствованиях, которые были внесены в процедуру регистрации в системе (процесс Winlogon), начиная с Windows Vista. Напомним, что использовавшаяся в более ранних версиях Windows инфраструктура GINA (Graphical Identification and Authentication) была заменена моделью поставщиков учетных данных (инфраструктура Credential Provider). В Windows 7 была дополнительно добавлена новая биометрическая инфраструктура Windows (Windows Biometric Framework, WBF), позволяющая пользователям регистрироваться в системе с учетом средств биометрического контроля. На текущий момент WBF поддерживает только устройства, идентифицирующие пользователей по отпечаткам пальцев, но в будущем она вполне может быть расширена.

Разумеется, случаи несанкционированного вмешательства в работу компьютерных сетей — реальность сегодняшней жизни. Примеры, доказывающие распространенность этих явлений, можно в большом количестве найти как на страницах различных изданий, так и в Интернете. Однако гораздо более распространен тот случай, когда вред (причем неумышленный!) наносят пользователи², знающие очень мало, чтобы считаться грамотными, но достаточно, чтобы быть опасными. Практически в каждой организации имеются любознательные, но недостаточно квалифицированные пользователи, которые любят просматривать подряд все исполняемые файлы и пытаются их запускать. Если таким пользователям случайно попадается на глаза Редактор реестра, а меры безопасности не предприняты, то обычно они спохватываются только тогда, когда начинаются проблемы с загрузкой системы.

Простейшие меры ограничения доступа к реестру

Наилучшим вариантом избежать неприятностей, связанных с неквалифицированным вмешательством пользователей в реестр, является установка прав

²User Error: Replace user — Ошибка пользователя: замените пользователя (фольклор).

доступа как к Редактору реестра, так и к файлам ульев реестра в папках пользовательских профилей (о пользовательских профилях речь пойдет в следующей главе).

ПРИМЕЧАНИЕ

Операционные системы Windows NT/2000/XP могли устанавливаться в разделы, отформатированные для использования файловой системы FAT. Довольно часто именно это и делалось (в основном, из-за необходимости обеспечить совместимость с наследуемыми приложениями). В отличие от своих предшественниц, Windows Vista и Windows 7 могут устанавливаться только в разделы, отформатированные под защищенную файловую систему NTFS, поэтому, на первый взгляд, проблемы с правами доступа к ресурсам больше не существует. Однако в ряде случаев пользователи создают мультизагрузочные системы, причем первый раздел жесткого диска по соображениям совместимости с другой операционной системой (в настоящее время чаще всего это бывает Linux) форматируется для использования FAT. При этом ряд файлов, необходимых для загрузки Windows Vista/7, копируется именно в этот раздел и тем самым подвергается риску. В первую очередь, это Менеджер загрузки (bootmgr) и улей реестра BCD (см. главу 7). Поэтому, как бы удобны ни были мультизагрузочные конфигурации, они снижают общий уровень безопасности системы. Если это — ваш случай, предпримите дополнительные меры защиты (как минимум, уделите должное внимание резервному копированию этих файлов).

Дополнительные меры защиты Windows Vista/7

Как уже говорилось, интерфейс Windows 7, как и в случае с ее предшественницами (Windows XP и Vista), максимально ориентирован на начинающих пользователей, которых, может быть, и в самом деле нужно защищать от них же самих. Одной из таких мер являются так называемые *суперскрытые файлы* ("super-hidden" files). В главе 1 говорилось о защищенных файлах операционной системы, которые недоступны для обычного пользователя (и даже не отображаются средствами графического пользовательского интерфейса). Именно подобные файлы иногда называют "суперскрытыми" (super-hidden), хотя, разумеется, такого атрибута у файлов нет. У них просто установлены атрибуты **Скрытый** (Hidden) и **Системный** (System). По умолчанию Проводник (Windows Explorer) их не отображает (рис. 9.1).

В Windows XP администратор вполне мог назначить эти атрибуты Редактору реестра. Таким образом, Редактор реестра оказывался "скрытым" от начинающих пользователей, не умеющих работать с командной строкой (например, команда `dir /a` отображает все файлы, какие бы атрибуты они ни имели).

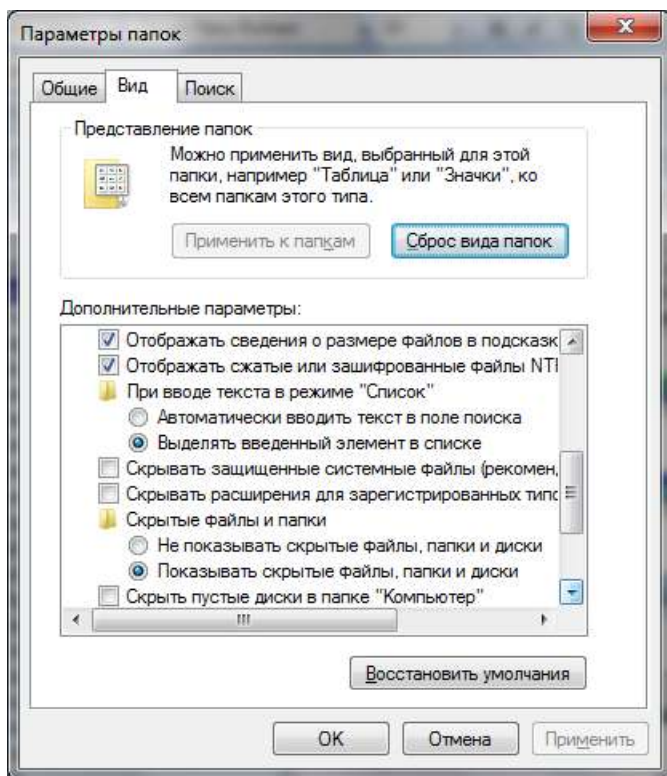


Рис. 9.1. Исходные опции операционной системы, относящиеся к защищенным системным файлам

ПРИМЕЧАНИЕ

Напомним, что делать это следовало не через графический пользовательский интерфейс, а из сеанса командной строки командой примерно следующего вида:

```
Attrib +h +s c:\Windows\regedit.exe
```

Даже в Windows XP такое решение было промежуточным и имело множество недостатков. А вот, начиная с Windows Vista, этот подход стал, во-первых, трудноосуществимым, а во-вторых — совершенно неэффективным:

- ❑ трудноосуществимым — потому, что права доступа к файлу Regedit.exe установлены так, что в доступе на изменение атрибутов будет отказано не только любому пользователю из группы администраторов (рис. 9.2), но даже и пользователю **Администратор** (Administrator), чья учетная запись является скрытой и заблокированной, и на которого не распространяется действие UAC. Справедливости ради надо отметить, что обойти это огра-

ничество можно, забрав себе права владельца. Впрочем, о правах доступа вообще, и о правах доступа к файлу Regedit.exe, в частности, мы поговорим чуть далее в этой главе;

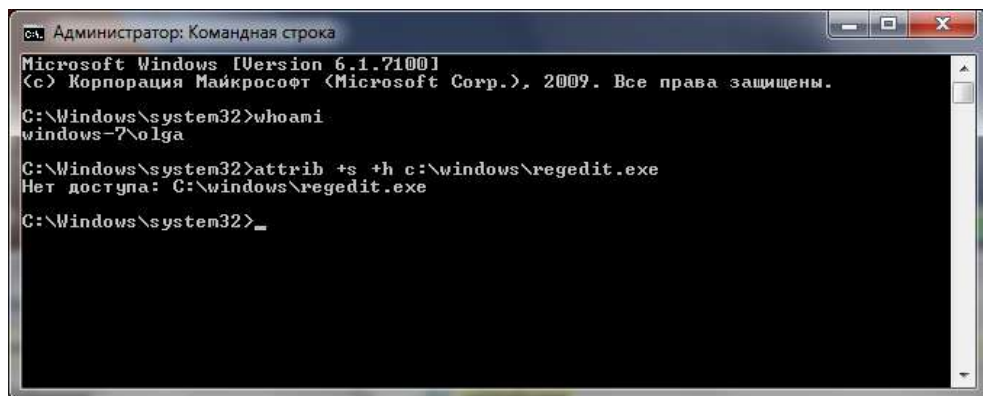


Рис. 9.2. Обратите внимание, что даже пользователю с административными правами отказано в доступе к файлу редактора реестра

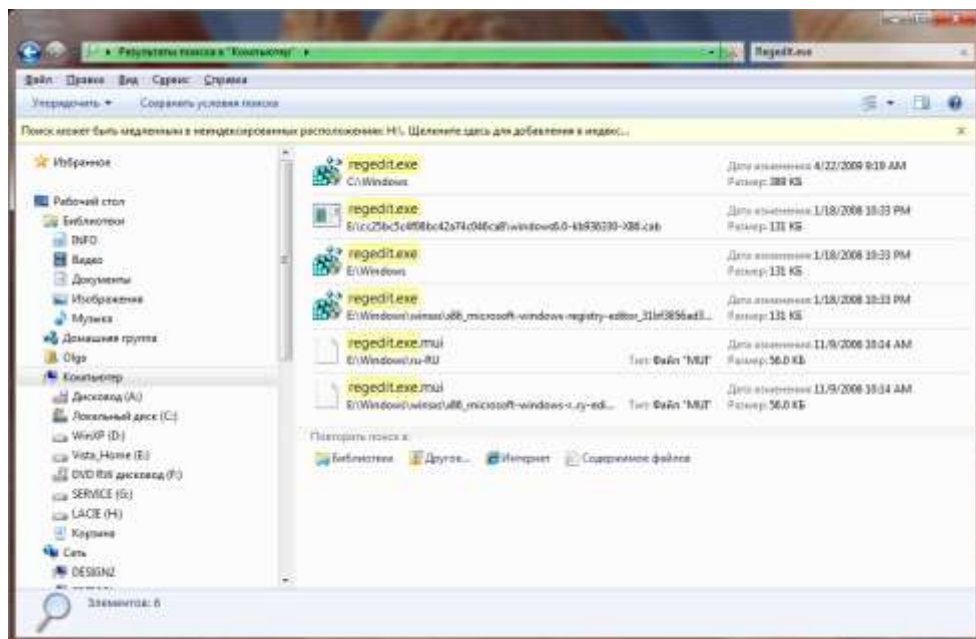


Рис. 9.3. В Windows Vista и Windows 7 функция расширенного поиска позволяет находить все файлы, в том числе — скрытые и системные, и, хотя выводится предупреждение о том, что поиск будет идти медленно, на самом деле не так уж и медленно она их ищет

□ неэффективность же скрытия Редактора реестра проявляется в том, что функция расширенного поиска (Advanced Search), реализованная в Windows Vista и Windows 7, позволяет найти все файлы, в том числе скрытые и системные (рис. 9.3). При этом сделать это может любой пользователь, даже не обладающий административными правами.

Поэтому, если вы желаете полностью перекрыть рядовым пользователям доступ к Редактору реестра, следует искать другое решение. Такие решения есть, и более того, их даже много. Рассмотрим их поочередно.

Запрет доступа к Редактору реестра через групповые политики

Этот способ — самый простой и безопасный, он существовал еще в Windows XP Professional и работает в Windows Vista/7. Но, как уже неоднократно повторялось ранее в этой книге, он недоступен пользователям "домашних" версий Windows Vista и Windows 7.

Чтобы блокировать доступ к редактору реестра через групповые политики, сделайте следующее.

1. В поле поиска, расположенное в нижней части меню **Пуск** (Start), введите команду `GPEdit.msc` и нажмите клавишу <Enter>. Этому же результата можно добиться, дав ту же самую команду из сеанса работы с командной строкой.
2. Разверните дерево консоли, как показано на рис. 9.4 — **Конфигурация пользователя** (User Configuration) | **Административные шаблоны** (Administrative Templates) | **Система** (System). В правой панели выберите политику **Запретить доступ к средствам редактирования реестра** (Prevent access to registry editing tools).
3. Выполните по этому параметру двойной щелчок мышью, и в раскрывшемся окне (рис. 9.5) установите переключатель **Включить** (Enabled). Внимательно прочтите справочную информацию в поле **Справка** (Help) — обратите внимание на то, что если вы хотите надежно перекрыть доступ не только к Regedit.exe, но и к другим средствам редактирования реестра, вам следует воспользоваться параметром **Не запускать указанные приложения Windows** (Do not run specified Windows applications), и вручную создать "черный список" приложений, доступ к которым должен быть перекрыт.
4. Нажмите кнопку **Применить** (Apply), затем — кнопку **ОК**, чтобы сохранить внесенное изменение. После этого попробуйте запустить редактор реестра — вы увидите сообщение, показанное на рис. 9.6.

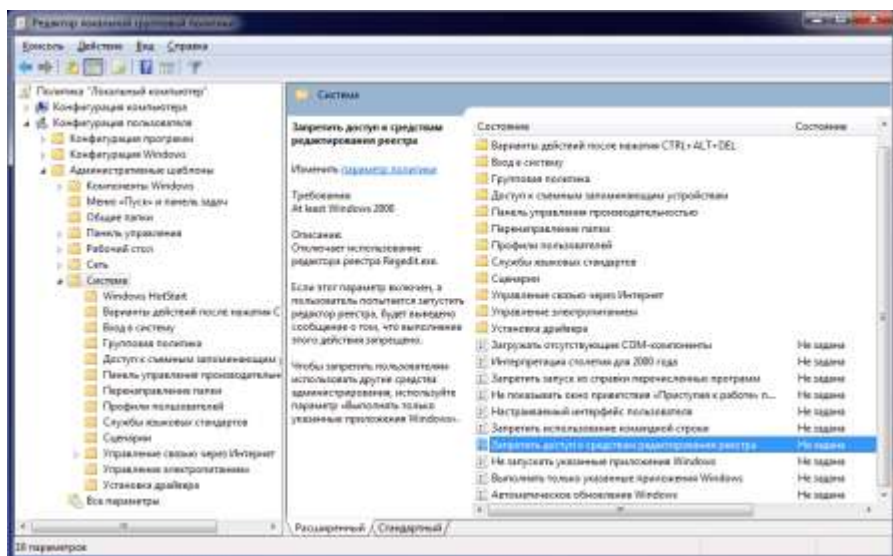


Рис. 9.4. Блокирование доступа к редактору реестра с помощью групповых политик

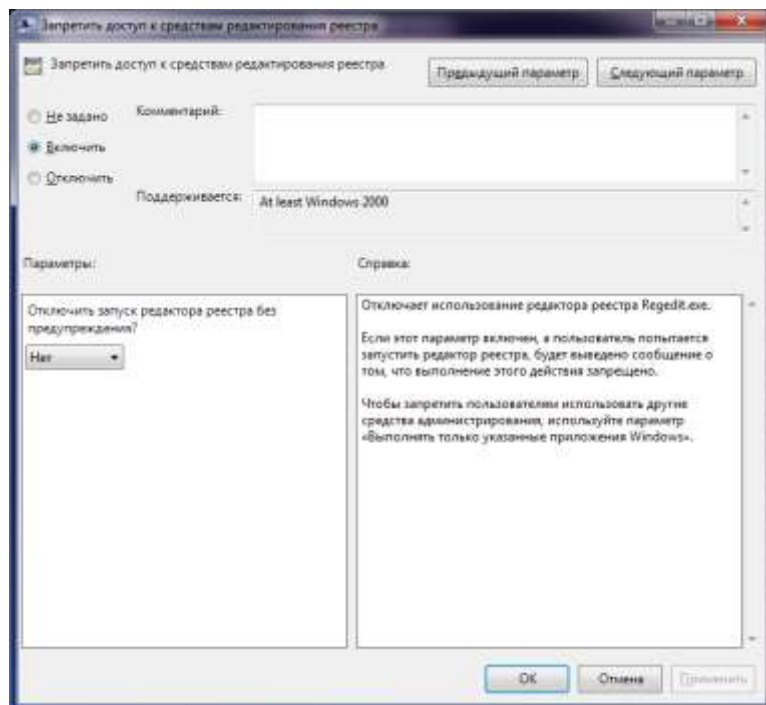


Рис. 9.5. Установка параметров политики доступа к средствам редактирования реестра

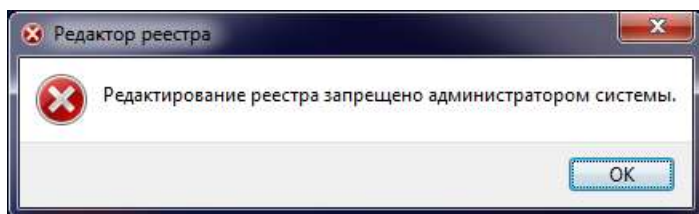


Рис. 9.6. Сообщение о том, что доступ к средствам редактирования реестра запрещен

Запрет доступа к редактору реестра путем редактирования реестра

Фактически, вы уже прекрасно знаете, что, когда вы редактируете системные политики, вы фактически вносите изменения в реестр. В данном случае — вы создаете параметр `DisableRegistryTools` с типом данных `REG_DWORD` и значением 2, расположенный в составе следующего ключа реестра:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\
Policies\System
```

Возможные значения параметра `DisableRegistryTools` и их смысл вкратце описаны в табл. 9.1.

Таблица 9.1. Возможные значения параметра `DisableRegistryTools` и их смысл

Значение	Описание
0	Редактор реестра может быть запущен в любом режиме — как в интерактивном, так и в неинтерактивном
1	Редактор реестра может быть запущен в неинтерактивном режиме (из командной строки командой <code>regedit /s</code>)
2	Редактор реестра вообще не может быть запущен

В целом, это решение не слишком удобно — во-первых, это ограничение не так уж сложно обойти, во-вторых — оно и вам самим создаст определенные неудобства.

Ограничение доступа к редактору реестра путем редактирования прав доступа

Нет ли еще какого-нибудь решения? Оно есть, и состоит именно в изменении прав доступа к файлу нужным образом. Однако и здесь не все так просто,

поэтому рассмотрим эту процедуру чуть более детально. Дело в том, что в Windows Vista/7 на смену механизму Windows File Protection (WFP) пришел механизм Windows Resource Protection (WRP), вкратце рассмотренный в *главе 5*. Редактор реестра Regedit.exe относится к числу файлов, защищаемых этим механизмом, и просто так поменять права доступа к нему, как уже отмечалось, не сможет никто, даже администратор (см. рис. 9.2). Чтобы добиться нужной цели, действуйте следующим образом:

1. Запустите сеанс работы с командной строкой с административными полномочиями и дайте команду `net user Administrator /active:yes`.
2. Войдите в систему от имени учетной записи **Администратор** (Administrator)³.
3. Найдите файл Regedit.exe, щелкните по нему правой кнопкой мыши и из контекстного меню выберите команду **Свойства** (Properties), а затем перейдите на вкладку **Безопасность** (Security). Вы увидите, что ни один пользователь и ни одна группа, даже учетная запись **SYSTEM**, не имеют полного доступа к файлу (рис. 9.7, *а*). Исключение составляет только учетная запись **TrustedInstaller** (рис. 9.7, *б*).

Установленные так права доступа и являются основным признаком того, что файл, папка или ключ реестра защищены механизмом WRP. В Windows Vista и Windows 7 WRP устанавливает права доступа к защищенным ресурсам таким образом, что запись в них может производиться только процессами, имеющими права **TrustedInstaller**. Учетная запись **LocalSystem** и группа **Administrators** имеют к защищенным ресурсам ограниченный доступ. В результате этого модификация защищенных файлов и ключей реестра разрешена только сервису **TrustedInstaller** (%WinDir%\servicing\TrustedInstaller.exe). При установке обновлений Windows сервис Windows Update обращается к сервису **TrustedInstaller**, который и выполняет обновление системы. Надо ли говорить, что **TrustedInstaller** установит лишь обновления, имеющие цифровую подпись?

ПРИМЕЧАНИЕ

Следует иметь в виду, что если попытку доступа к системному ресурсу, защищенному механизмом WRP, с целью его изменения осуществит программа-инсталлятор (например, приложения или драйвера), то в доступе ему отказано не будет. Система определит, что в данном случае она имеет дело с программой-инсталлятором, запрос будет принят и обработан, и система даже вернет код успеха. Однако на самом деле ресурс изменен не будет, потому что в дело вступит виртуализация реестра, и изменение будет перенаправлено из ключа **HKLM** (защищенные общесистемные ресурсы) в ключ **HKCU** (пользовательская область).

³ Напомним, что в локализованных версиях название этой учетной записи должно быть введено на том самом языке, на который эта версия Windows локализована, о чем уже говорилось в *главе 4*, где этот вопрос уже обсуждался.

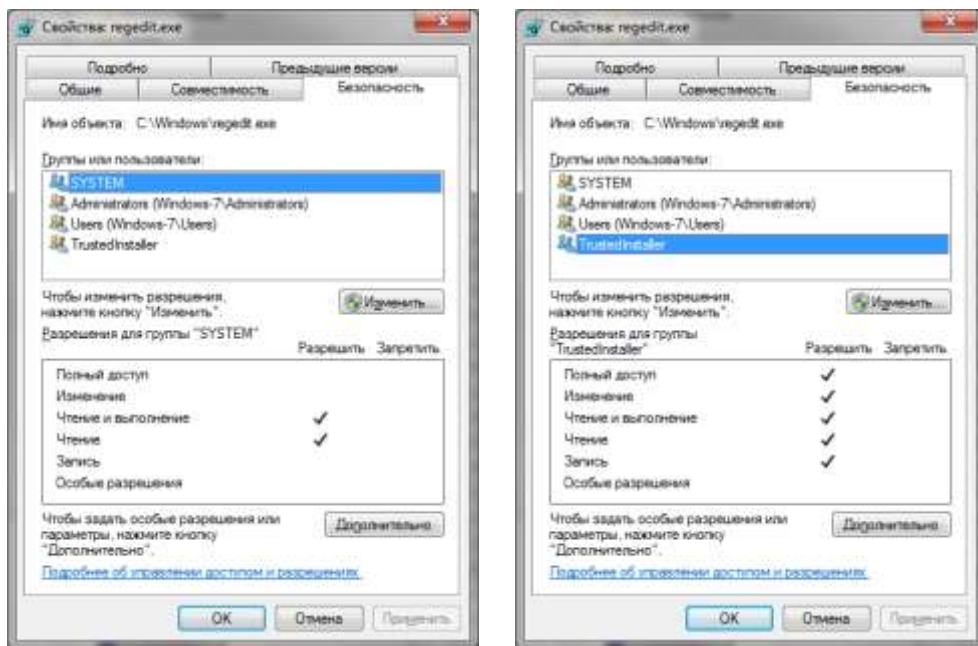


Рис. 9.7. Права доступа по умолчанию к файлу Редактора реестра Regedit.exe

4. Чтобы получить возможность редактирования прав доступа к файлу, защищенному WRP, вам необходимо присвоить себе права его владельца. Для этой цели нажмите кнопку **Дополнительно** (Advanced) в нижней части вкладки **Безопасность** (Security) окна свойств защищенного файла (см. рис. 9.7), а затем перейдите на вкладку **Владелец** (Owner). По умолчанию владельцем защищенного файла является учетная запись **TrustedInstaller** (рис. 9.8).
5. Нажмите кнопку **Изменить** (Modify) и из списка пользователей и групп выберите пользователя **Администратор** (или одного из пользователей, наделенных административными правами). На экране откроется диалоговое окно, показанное на рис. 9.9. Выполните двойной щелчок мышью на имени нужного пользователя или нажмите кнопку **Другие пользователи или группы** (Other users and groups) и замените владельца файла. Нажмите кнопку **Применить** (Apply), затем — кнопку **ОК**, и на экране откроется окно, показанное на рис. 9.10.

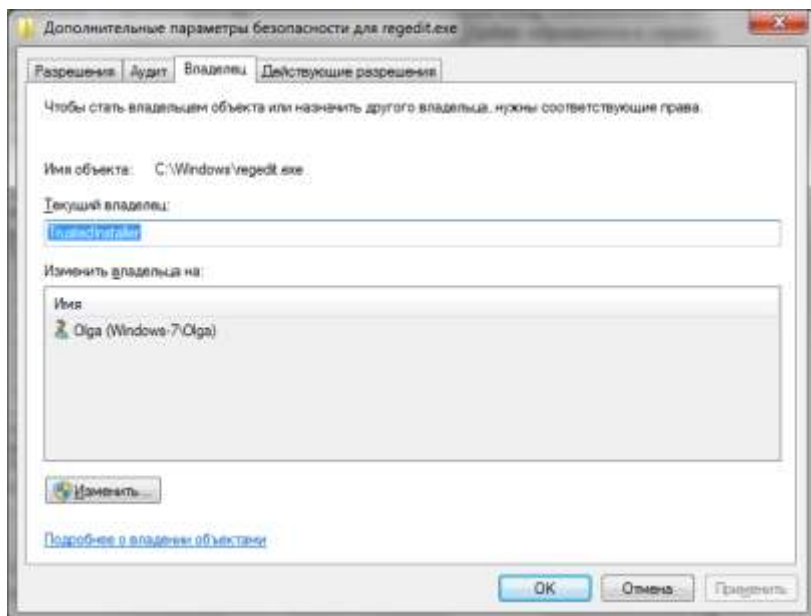


Рис. 9.8. По умолчанию владельцем файла, защищенного WRP (в данном случае файла Regedit.exe), является учетная запись **TrustedInstaller**

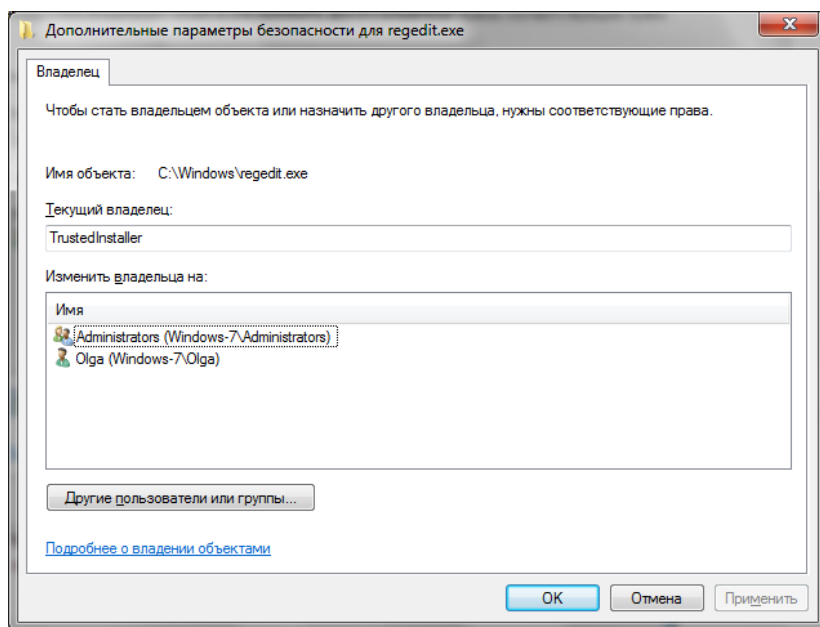


Рис. 9.9. Изменение владельца файла Regedit.exe

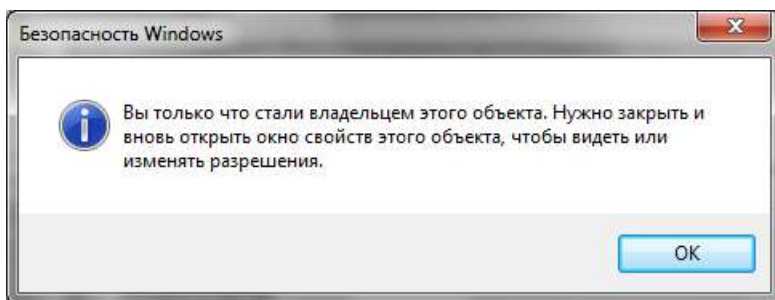


Рис. 9.10. Диалоговое окно подсистемы безопасности Windows, информирующее о смене владельца объекта

6. Нажмите кнопку **ОК**, откройте и закройте окно свойств объекта, а затем отредактируйте права доступа к нему требуемым образом. Например, вы можете предоставить полный доступ пользователю **Администратор** (Administrator) и одному из пользователей из группы администраторов. У рядовых пользователей можно отобрать все права доступа к файлу реестра, тогда все их попытки запустить Редактор реестра закончатся сообщением, показанным на рис. 9.11.

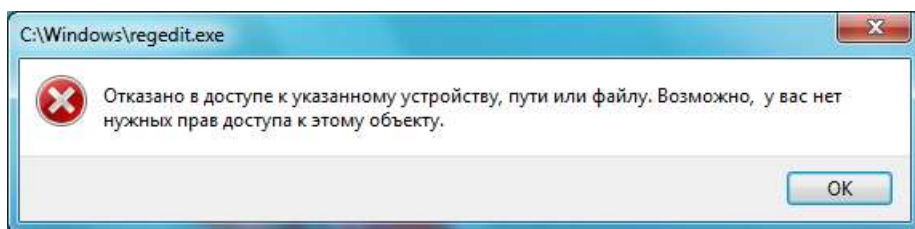


Рис. 9.11. Запрет на доступ к Редактору реестра для пользователей без административных прав вошел в силу

ВНИМАНИЕ!

Имейте в виду, что категорически не рекомендуется без крайней необходимости присваивать себе или даже пользователю **Администратор** (Administrator) права доступа к системным ресурсам, защищенным механизмом WRP. Дело в том, что после внесения таких изменений WRP больше не будет защищать модифицированный ресурс. Таким образом, вы, считая, что решаете одну проблему, потенциально создаете себе новую. В любом случае, оставив все "как есть", вы создаете брешь в системе безопасности. Например, в данном случае (речь о файле Regedit.exe), файл перестает быть защищенным, и теперь может быть модифицирован (в том числе — заражен вирусом). Поэтому, выполнив ту задачу, которую хотели, не забудьте восстановить права владельца в исходное состояние (верните права владельца учетной записи **TrustedInstaller**).

Итак, ваша цель достигнута. Пользователи, не имеющие административных прав, не могут получать доступ к Редактору реестра. Теперь, как было только что сказано в предшествующем примечании, необходимо восстановить для редактора реестра защиту WRP, вернув права доступа учетной записи **TrustedInstaller**.

Для этого действуйте следующим образом:

1. Щелкните по файлу Regedit.exe правой кнопкой мыши, и из раскрывшегося контекстного меню выберите команду **Свойства** (Properties).
2. Перейдите на вкладку **Безопасность** (Security), щелкните мышью по кнопке **Дополнительно** (Advanced) и в раскрывшемся окне перейдите на вкладку **Владелец** (Owner). И вот здесь мы натолкнемся на проблему — смотрите, учетной записи **TrustedInstaller** (как показано на рис. 9.12) нет в списке **Изменить владельца на:** (Change owner to:).

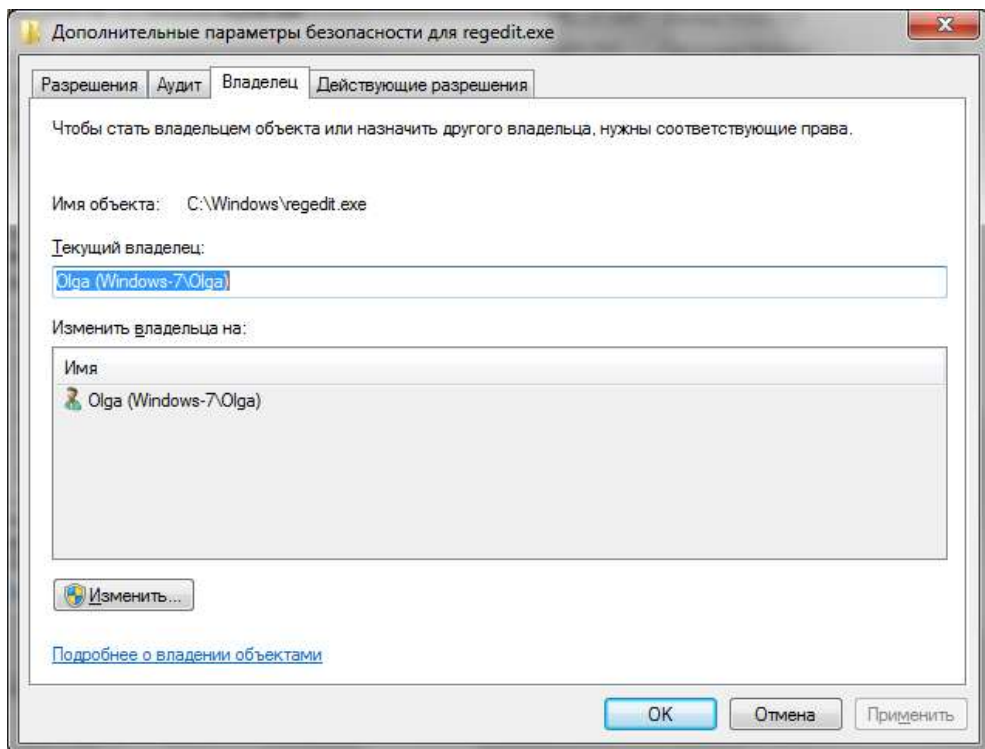


Рис. 9.12. Обратите внимание, учетной записи **TrustedInstaller** нет в списке **Изменить владельца на:** (Change Owner to:)

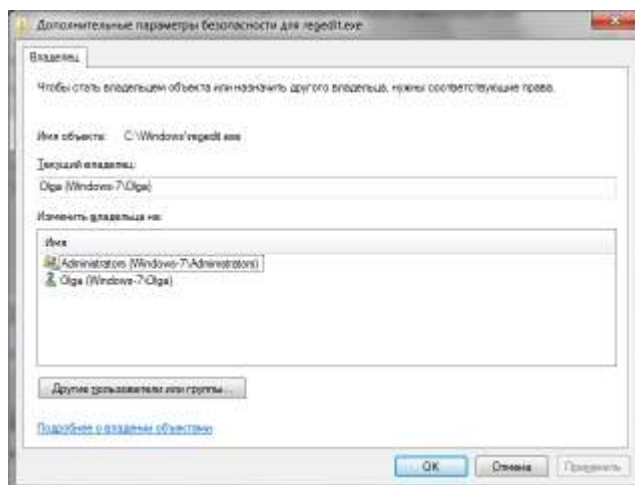


Рис. 9.13. И здесь учетной записи **TrustedInstaller** в списке пользователей нет!

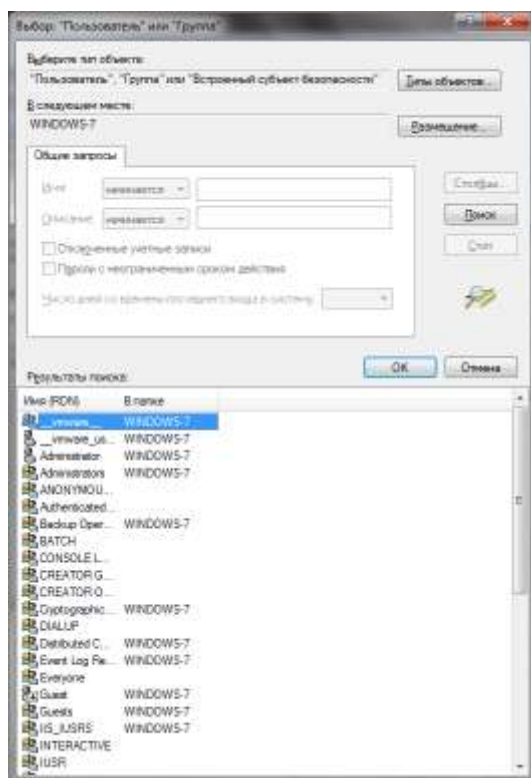


Рис. 9.14. Даже в длинном списке всех учетных записей пользователей и групп учетной записи **TrustedInstaller** нет!

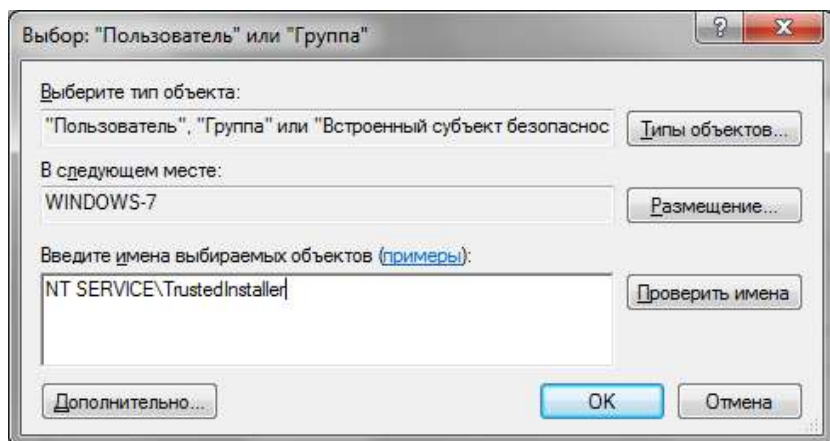


Рис. 9.15. Ручной ввод строки NT SERVICE\TrustedInstaller

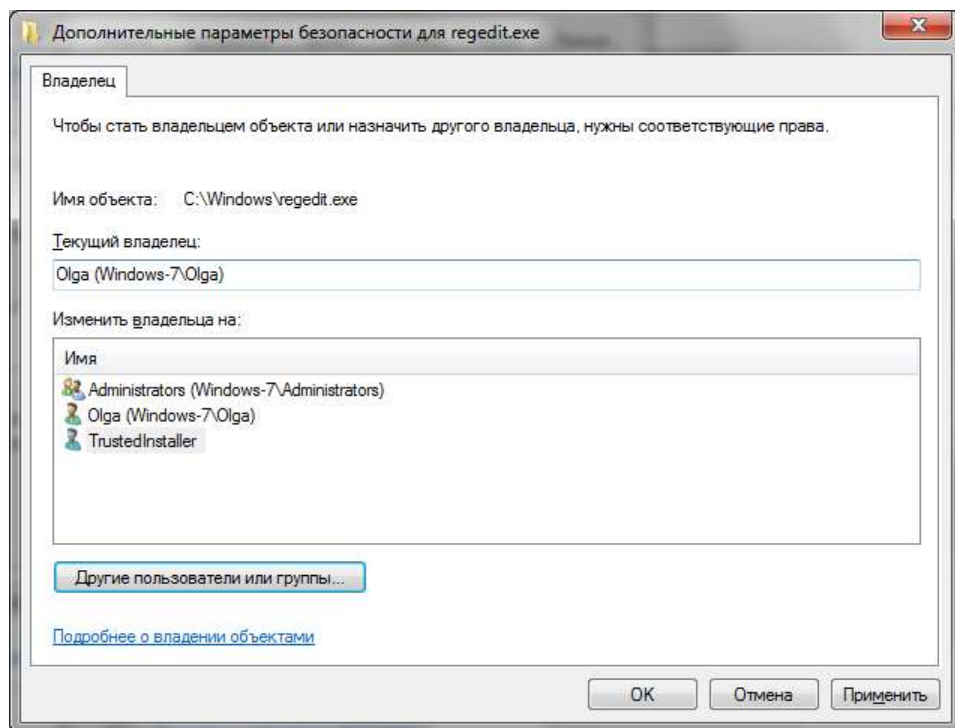


Рис. 9.16. Имя TrustedInstaller появилось в списке имен, доступных для выбора

3. Ну, что же, давайте поищем ее в списке других учетных записей. Нажмите кнопку **Изменить** (Edit). И здесь ее нет (рис. 9.13).
4. Нажмем кнопку **Другие пользователи или группы** (Other users and groups). Но и в раскрывшемся окне (рис. 9.14), как ни прокручивай длинный список результатов поиска, учетной записи **TrustedInstaller** вы не найдете!
5. В чем же дело? А вот в чем: учетная запись **TrustedInstaller** не принадлежит видимым пользователям и группам, а фактически работает в режиме сервиса NT (NT SERVICE). Поэтому для восстановления **TrustedInstaller** в качестве владельца файла, вам следует вернуться в окно, показанное на рис. 9.13, нажать кнопку **Другие пользователи или группы** (Other users and groups) и в поле **Введите имена выбираемых объектов** (Enter the object name to select) вручную ввести строку NT SERVICE\TrustedInstaller, как показано на рис. 9.15.
6. Нажмите кнопку **ОК**, и тогда имя **TrustedInstaller** появится в списке учетных записей, доступных для выбора (рис. 9.16).
7. Выберите имя **TrustedInstaller**, нажмите кнопку **Применить** (Apply), а затем нажмите кнопку **ОК** во всех диалоговых окнах, которые будут появляться.

Редактирование прав доступа к ключам реестра

Если у вас есть некоторый опыт работы в Windows NT/2000/XP, то вам будут знакомы пусть не все, но многие функциональные свойства Windows Vista и Windows 7, относящиеся к безопасности.

Например, идентификация пользователей и групп осуществляется с помощью *идентификаторов безопасности* (security identifiers, Security ID, SID). Они представляют собой длинные последовательности букв и цифр и, что важнее всего, уникальны для каждого пользователя (даже с учетом пользователей, зарегистрированных в других системах). Если вы сначала удалите учетную пользовательскую запись на локальном компьютере или в домене, а затем создадите новую с тем же регистрационным именем, то система сгенерирует для нее новый SID. Существование двух одинаковых идентификаторов безопасности принципиально невозможно.

SID имеет следующий формат: S-1-XXXXX₁-YYYYY₂-...-RID, где: S-1 — идентификатор безопасности, версия 1; XXXXX — номер полномочия (authority number), YYYYY_n — дополнительные номера полномочия (subauthority

numbers), RID — относительный идентификатор (Relative ID). Обратите внимание, что Relative ID (RID) не обязательно должен быть уникальным для каждого компьютера.

ПРИМЕЧАНИЕ

Многие пользователи Windows NT/2000/XP/Vista/7, в том числе и те, кто считает себя "опытными" и "продвинутыми", нередко полагают, что система идентифицирует каждого пользователя по входному имени (login) и паролю (password). Они заблуждаются — это не так. Именно SID позволяет уникально идентифицировать каждого пользователя в системе. Пользовательские профили, которые будут подробно обсуждаться в *главе 10*, также идентифицируются по соответствующим SID.

Итак, SID пользователя является уникальным. Однако существуют так называемые *известные SID* (well-known SIDs), значения которых постоянны для всех систем. Перечислим некоторые идентификаторы, которые охватывают известные категории пользователей и групп:

- ❑ **Все пользователи** (Everyone) (S-1-1-0) — все пользователи компьютера, даже с анонимными гостевыми учетными записями. Значение номера полномочий данного идентификатора равно 1 — так называемые *мировые полномочия* (World Authority), а значение дополнительного уровня полномочий равно 0 (Null RID);
- ❑ **Создатель-Владелец** (Creator Owner) (S-1-3-0) — шаблон (placeholder) в наследуемом элементе управления доступом (Access Control Entry, ACE). При наследовании ACE замещает SID этой категории на SID текущего владельца объекта. Значение номера полномочий для данного SID равно 3 (Creator Authority). У него есть одно значение номера дополнительных полномочий — 0 (Null RID);
- ❑ **Права владельца** (OwnerRights) (S-1-3-4) — для управления правами доступа к защищаемому объекту. Данный SID отличается от **Создатель-Владелец** и был впервые введен в Windows Vista;
- ❑ **TrustedInstaller** (S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464) — фактически **TrustedInstaller** представляет собой сервис, а не пользователя. Реализованная в Windows Vista и Windows 7, эта функция повышения надежности сервисов (service hardening) позволяет назначать сервисам полномочия точно так же, как и пользователям⁴.

ПРИМЕЧАНИЕ

Просмотреть SID любого из сервисов можно, дав команду `sc showsid` (рис. 9.17).

⁴ См. <http://www.microsoft.com/technet/technetmag/issues/2007/01/SecurityWatch>.

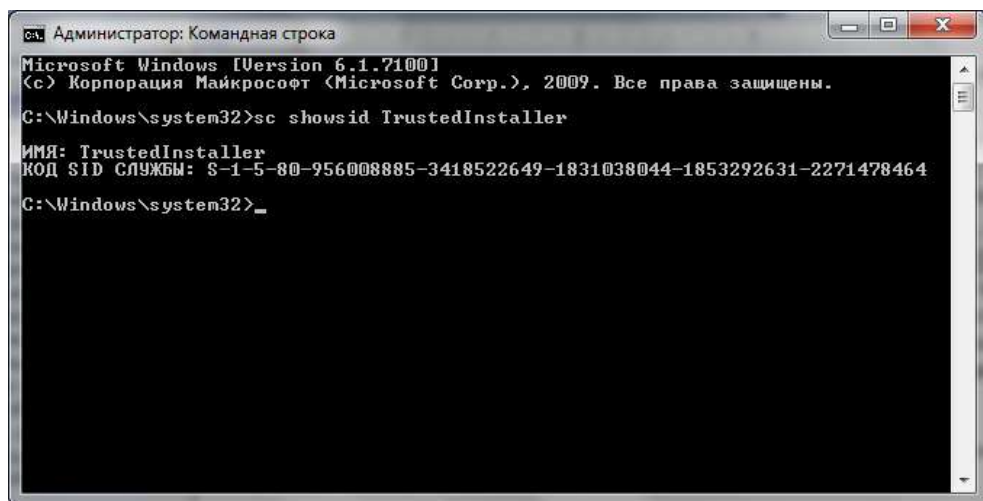


Рис. 9.17. Просмотр SID сервиса TrustedInstaller

ПРИМЕЧАНИЕ

Полный список известных SID в Windows 2000/XP приведен в статье Microsoft Knowledge Base Q243330 — "Well Known Security Identifiers in Windows 2000 and Windows XP" (<http://support.microsoft.com/kb/243330>). В Windows Vista в этот список были внесены изменения, которые в этой главе будут отмечены особо. Полный список известных SID в Windows Vista/7 можно найти по следующему адресу: http://www.windowsconfiguration.com/2007/04/well_known_sids.html. Кроме того, пользователям, желающим изучить данный вопрос углубленно, можно рекомендовать следующие источники информации:

<http://www.registrycleanersreviews.info/list-of-well-know-registry-sids>,
http://www.windowsconfiguration.com/2007/04/well_known_sids.html
<http://www.winzero.ca/WellKnownSIDs.htm>,
[http://msdn.microsoft.com/en-us/library/aa379649\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa379649(VS.85).aspx).

Windows Vista и Windows 7, как и их предшественницы, поддерживают *списки контроля доступа* (Access Control List, ACL) для реестра, которые могут использоваться для защиты ключей реестра. ACL представляют собой базу данных, которая поддерживает информацию о правах доступа к конкретным объектам операционной системы (в данном случае — к ключам реестра).

ПРИМЕЧАНИЕ

Подробные пошаговые инструкции по установке прав доступа к ключам реестра приведены в *главе 3*. В этой же главе основное внимание будет уделено не административным операциям, а практическим советам. В частности, здесь будут указаны наиболее важные ключи реестра, нуждающиеся в защите.

Когда вы работаете в Windows Vista/7 в составе рабочей группы или на компьютере, не подключенном к сети, и обладаете соответствующими административными правами, вам предоставляется доступ ко всем функциям обеспечения безопасности в операционной системе. Если ваш компьютер является участником домена, то эти характеристики будут определяться политикой, устанавливаемой ИТ-администратором.

Обзор стандартных прав доступа в Windows Vista/7

Стандартные настройки системы безопасности Windows Vista/7 определяются правами доступа по умолчанию, которые назначаются стандартным пользовательским группам. Перечислим наиболее важные пользовательские группы:

- **Администраторы (Administrators)** — в Windows NT/2000/XP пользователи из этой группы обладали полным набором прав на локальном компьютере или в домене. Так, по умолчанию администраторы в этих операционных системах могли получать доступ к любому ключу и параметру реестра, а также к любому объекту файловой системы. Начиная с Windows Vista, как уже упоминалось в *главе 4*, была введена новая функция — Контроль учетных записей пользователей (User Account Control, UAC), известная также как *принцип минимальных достаточных полномочий* (Least-Privileged User Account, LUA). В соответствии с этим принципом полного доступа ко всем объектам файловой системы, а также ключам и параметрам реестра, не имеет ни одна из учетных записей, включая даже учетную запись **SYSTEM**. Пользовательские учетные записи из группы **Администраторы** не являются исключением (кроме встроенной и по умолчанию заблокированной учетной записи **Администратор**). Это означает, что все процессы, запускаемые этими пользователями (включая установку программного обеспечения, запись информации в состав ключа реестра `HKKEY_LOCAL_MACHINE`, запуск драйверов и сервисов и т. п.), работают лишь с минимально необходимым уровнем полномочий. Если программа требует, администратор может этот уровень повысить (эта процедура известна как *privilege elevation*).

ПРИМЕЧАНИЕ

Запуск программы с неограниченным уровнем полномочий осуществляется одним из методов, которые будут рассмотрены чуть далее в этой главе, пока же отметим, что в этом случае на экране будет появляться хорошо известное всплывающее окно, запрашивающее согласие пользователя на выполнение данной операции.

По умолчанию в группу **Администраторы** включаются пользовательские учетные записи, создаваемые в процессе установки операционной системы.

Если же вы осуществляете обновление системы с одной из предшествующих версий, то в эту группу будут включены члены группы **Администраторы** обновляемой системы. Если компьютер является участником домена, то в нее будут включены члены группы **Администраторы** (Administrators) вашего домена;

СОВЕТ

Независимо от того, в какой системе вы работаете, Windows 7 или одной из предшествующих версий (например, Windows XP), настоятельно рекомендуется ограничивать количество пользователей, входящих в группу **Администраторы** (Administrators). Причина проста — чем многочисленнее эта группа, тем более уязвимой будет ваша система, поскольку все учетные записи этой группы (в особенности, если не соблюдается строгая парольная защита) могут потенциально быть использованы для получения неавторизованного доступа к компьютеру.

- **Администратор** (Administrator) — встроенная учетная запись администратора, имеющая относительный идентификатор (RID), установленный на 500, и по умолчанию заблокированная. Microsoft подразумевает, что эта учетная запись предназначена для исключительных ситуаций, когда все остальные средства устранения проблем не привели к успеху. В предшествующих версиях операционной системы пользователи часто использовали ее как стандартную административную учетную запись, нарушая тем самым целый ряд основополагающих принципов безопасности. По неподтвержденным слухам, Microsoft планирует в будущем ликвидировать эту учетную запись вообще, но пока что она просто заблокирована по умолчанию. При условии, что в группе **Администраторы** (Administrators) нет ни одной учетной записи, учетная запись **Администратор** активизируется в среде восстановления (WinRE) и безопасном режиме загрузки (safe mode);

ПРИМЕЧАНИЕ

В Windows XP встроенная учетная запись **Администратор** (Administrator) имела целый набор специальных прав и привилегий, которых не имели другие администраторы. Начиная с Windows Vista, эти различия устранены, за исключением двух:

- заблокированная учетная запись **Администратор** (Administrator) может использоваться при восстановлении системы, если в локальной системе нет других администраторов;
- на эту учетную запись не действует механизм UAC. Аналогичное утверждение справедливо и для учетной записи **Администратор домена** (Domain Administrator).

- **Опытные пользователи** (Power Users) — в Windows 2000/XP членам этой группы было разрешено устанавливать приложения, которые затем могли использоваться всеми членами группы **Пользователи** (Users), а также выполнять ограниченный набор задач по настройке системы, в том числе устанавливать системные дату и время, изменять параметры

настройки экрана, устанавливать принтеры, настраивать управление электропитанием и т. д. Членам группы **Опытные пользователи** разрешалось также запускать несертифицированные приложения, которые не могли успешно выполняться с полномочиями группы **Пользователи** (Users).

В Windows Vista/7 группа **Опытные пользователи** (Power Users) практически ликвидирована. Формально эта группа по-прежнему существует (рис. 9.18), но большинство полномочий, которые она имела в Windows XP, теперь у нее отобраны. Microsoft объясняет это тем, что фактически члены данной группы были администраторами, которые просто еще не успели присвоить себе полные административные права. При этом добиться данной цели было очень легко. Таким образом, группа **Опытные пользователи** (Power Users) сохранена исключительно в целях обратной совместимости с прежними версиями Windows. Если вам все же эта группа требуется, можно сделать новый административный шаблон в политиках безопасности (gpedit.msc) и присвоить данной группе права и полномочия, аналогичные прежним⁵. Тем не менее, если вы планируете масштабный переход на Windows 7, от группы **Опытные пользователи** (Power Users) следует постепенно отказываться;

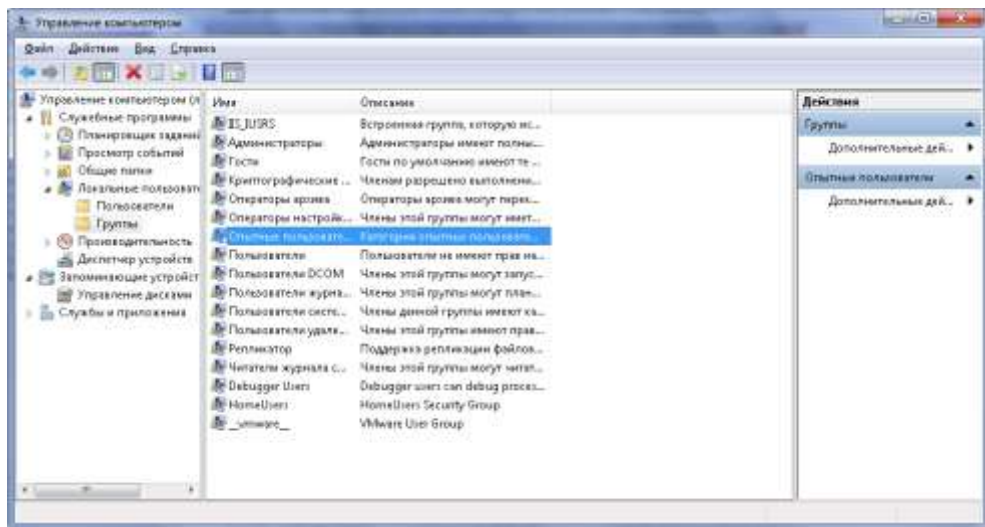


Рис. 9.18. Группа **Опытные пользователи** в Windows Vista и Windows 7 по-прежнему существует, но больше не обладает теми правами, которые присваивались ей в Windows 2000/XP

⁵ См. <http://technet2.microsoft.com/WindowsVista/en/library/00d04415-2b2f-422c-b70e-b18ff918c2811033.mspx?mfr=true>.

- ❑ **Пользователи (Users)** — теперь члены этой группы имеют ограниченные административные права. В частности, они не могут устанавливать или деинсталлировать приложения в папке %SystemRoot%, изменять настройки системы. Однако **Пользователи (Users)** получают право выполнять эти задачи при условии, что смогут по запросу системы предоставить корректную учетную информацию для одной из учетных записей из группы администраторов;

ПРИМЕЧАНИЕ

Если в системе активизирована функция UAC, то и пользователи из локальной группы **Администраторы (Administrators)** тоже работают с набором привилегий, типичным для членов стандартной группы **Пользователи (Users)**. Административные привилегии предоставляются только, когда пользователи подтверждают свое намерение выполнить программу с административными привилегиями.

- ❑ **Операторы архива (Backup Operators)** — могут выполнять резервное копирование и восстановление файлов компьютера, независимо от разрешений, которыми защищены эти файлы. Они могут также регистрироваться на компьютере, выключать его, но не могут менять параметры безопасности;
- ❑ **Репликаторы (Replicators)** — могут выполнять копирование файлов в домене;
- ❑ **Операторы настройки сети (Network Configuration Operators)** — имеют ограниченные административные полномочия, которые позволяют им конфигурировать возможности сети, например, назначать IP-адреса;
- ❑ **HelpServicesGroup** — могут запускать вспомогательные приложения для диагностики системных проблем. Данная учетная запись может использоваться членами группы Microsoft Help and Support Services для доступа к компьютеру по сети и локальной регистрации. Начиная с Windows Vista, эта группа была ликвидирована. Учетные записи **Support_XXXXXX** и **HelpAssistant** присутствуют только в системах, установленных как обновление одной из предыдущих версий;
- ❑ **Пользователи удаленного рабочего стола (Remote Desktop Users)** — имеют право на локальную регистрацию;
- ❑ **Криптографические операторы (Cryptographic Operators)** — члены этой группы могут выполнять криптографические операции;

- ❑ **Пользователи DCOM** (Distributed COM Users) — члены этой группы имеют возможность использовать Distributed COM (DCOM)⁶;
- ❑ **Гости** (Guests) — пользователи из этой группы могут получать доступ к собственным файлам и папкам, но не могут менять свой пароль;
- ❑ **IIS_USRS** — пользователи из этой группы могут работать с сервисом IIS (Internet Information Server);
- ❑ **Пользователи журналов производительности** (Performance Log Users) — могут пользоваться оснасткой **Стабильность и производительность** (Windows Performance Diagnostic Console) и вести мониторинг счетчиков и журналов производительности (как локально, так и удаленно);
- ❑ **Пользователи системного монитора** (Performance Monitor Users) — члены этой группы могут пользоваться оснасткой **Стабильность и производительность** (Windows Performance Diagnostic Console) и вести мониторинг только для счетчиков производительности (как локально, так и удаленно);
- ❑ **HomeUsers** — если вы сконфигурировали компьютер, как подключенный к домашней сети и присоединили его к домашней группе (HomeGroup), новой функциональной возможности, появившейся в Windows 7 (см. главу 8), то среди встроенных групп безопасности будет и группа **HomeUsers**. Как несложно догадаться, в ее состав будут включены все пользователи, являющиеся членами домашней группы.

Изменения параметров безопасности Windows Vista/7 по сравнению с Windows XP

В Windows Vista/7 были изменены многие стандартные настройки безопасности. Часть этих изменений касается локальных политик, которые могут быть модифицированы с помощью Редактора локальной групповой политики (Local Group Policy) или через групповую политику Active Directory. Рассмотрим наиболее важные изменения, коснувшиеся политики аудита (Audit Policy), назначения прав пользователя (User Rights Assignment) и параметров безопасности (Security Options).

⁶ COM (Component Object Model) — Объектная модель компонентов. Она представляет собой технологический стандарт Microsoft, предназначенный для создания программного обеспечения на основе взаимодействующих распределенных компонентов, каждый из которых может использоваться во многих программах одновременно. В 1996 году была выпущена технология DCOM (Distributed COM) — распределенная COM), позволяющая COM-компонентам взаимодействовать друг с другом по сети. Технология DCOM обеспечивает базовые установки безопасности, позволяя задавать, кто и из каких машин может создавать экземпляры объекта и вызывать его методы. Более подробную информацию по данному вопросу можно найти здесь: http://en.wikipedia.org/wiki/Distributed_Component_Object_Model.

Изменения политики аудита

Политика аудита используется для сбора информации в отношении доступа к ресурсам и использования привилегий. Активизируя аудит, вы можете вести журнал событий, имеющих отношение к безопасности системы, — таких как регистрация пользователя в системе или изменение параметров пользовательской учетной записи. Как и в Windows XP, аудит можно установить и на ключи реестра.

1. Чтобы установить политику аудита, сделайте следующее:
2. Нажмите кнопку **Пуск** (Start), выберите из меню опции **Все программы** (All Programs) | **Стандартные** (Accessories) и запустите сеанс командной строки с административными полномочиями (**Командная строка** (Command Prompt) | **Запуск от имени администратора** (Run as Administrator)).
3. Введите команду `gpedit.msc`. В левой панели раскрывшегося окна (рис. 9.19) разверните дерево **Параметры безопасности** (Security Settings).

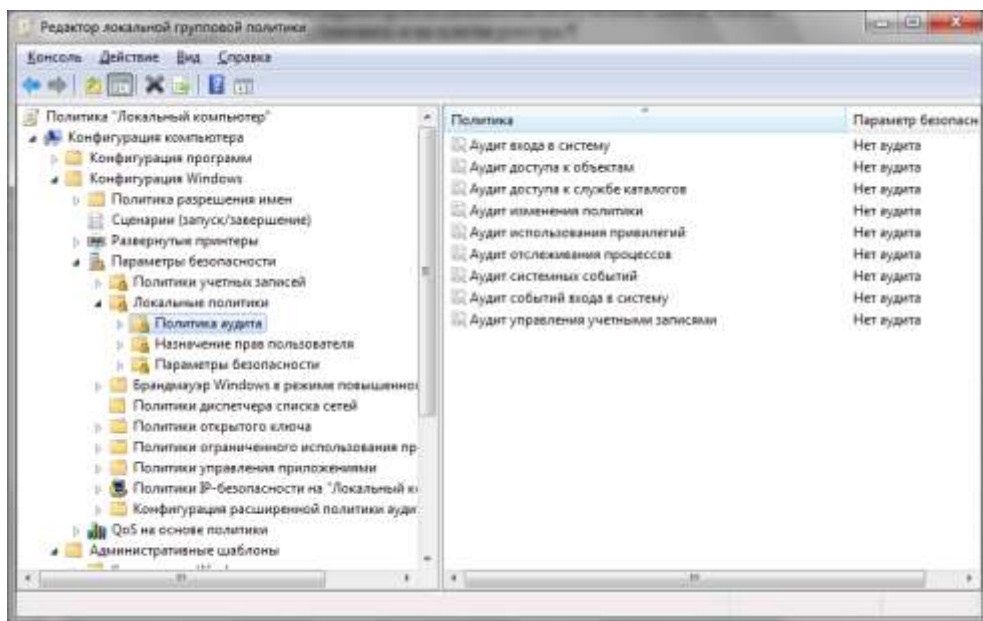


Рис. 9.19. Редактирование политики аудита

Значения политики аудита, установленные по умолчанию в Windows XP и Windows Vista/7, приведены в табл. 9.2. Можно видеть, что в Windows XP политика аудита по умолчанию не активизирована. В Windows Vista/7,

в отличие от XP, в журнале безопасности регистрируются все успешные попытки регистрации в системе для всех типов учетных записей.

Таблица 9.2. Установленные по умолчанию значения политики аудита

Политика	Значение по умолчанию для Windows XP	Значение по умолчанию для Windows Vista/7
Аудит событий входа в систему (Audit Account Logon Events)	Нет аудита (No auditing)	Успех (Success)
Аудит управления учетными записями (Audit Account Management)	Нет аудита (No auditing)	Нет аудита (No auditing)
Аудит доступа к службе каталогов (Audit Directory Service Access)	Нет аудита (No auditing)	Нет аудита (No auditing)
Аудит входа в систему (Audit Logon Events)	Нет аудита (No auditing)	Успех (Success)
Аудит доступа к объектам (Audit Object Access)	Нет аудита (No auditing)	Нет аудита (No auditing)
Аудит изменения политики (Audit Policy Change)	Нет аудита (No auditing)	Нет аудита (No auditing)
Аудит использования привилегий (Audit Privilege Use)	Нет аудита (No auditing)	Нет аудита (No auditing)
Аудит отслеживания процессов (Audit Process Tracking)	Нет аудита (No auditing)	Нет аудита (No auditing)
Аудит системных событий (Audit System Events)	Нет аудита (No auditing)	Нет аудита (No auditing)

ПРИМЕЧАНИЕ

Когда вы впервые откроете окно Редактора локальной политики (см. рис. 9.19), пусть вас не вводит в заблуждение установка значения **Нет аудита** (No auditing) на политики **Аудит событий входа в систему** (Audit Account Logon Events) и **Аудит входа в систему** (Audit Logon Events). На самом деле аудит по умолчанию активизирован и отслеживание событий ведется, в чем несложно убедиться, просмотрев журнал безопасности. Воистину, на самом деле тут все не так, как в действительности ;-)

Изменения в назначении прав пользователя

Политики в отношении назначения прав пользователя определяют, что конкретный пользователь или группа могут делать на компьютере. Чтобы опре-

дактировать стандартные права пользователя, назначенные по умолчанию, запустите сеанс командной строки с административными правами, введите команду `gpedit.msc` и разверните дерево **Параметры безопасности** (Security settings), как показано на рис. 9.20.

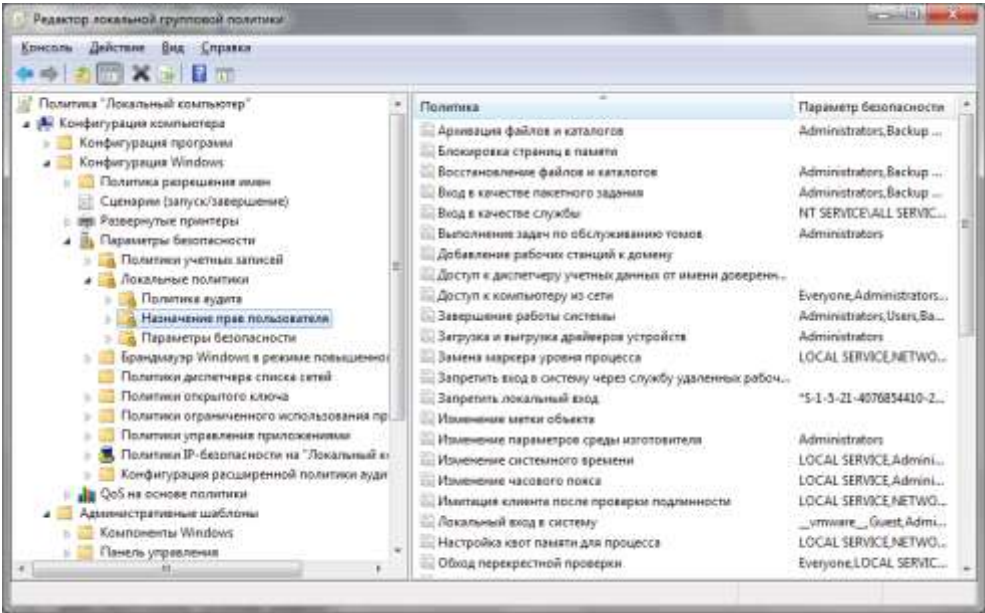


Рис. 9.20. Редактирование политики назначения прав пользователя

Значения политики назначения прав пользователя кратко перечислены в табл. 9.3. Отметим введение функции Контроля учетных записей пользователей (User Account Control, UAC), которая представляет собой дополнительный уровень защиты.

Таблица 9.3. Права, назначаемые пользователям и группам по умолчанию

Политика	Значение по умолчанию для Windows XP	Значение по умолчанию для Windows Vista/7
Доступ к диспетчеру учетных данных от имени доверенного вызывающего (Access Credential Manager As A Trusted Caller)	Не применимо	Настройки по умолчанию нет

Таблица 9.3 (продолжение)

Политика	Значение по умолчанию для Windows XP	Значение по умолчанию для Windows Vista/7
Доступ к локальному компьютеру через сеть (Access This Computer From The Network)	Все (Everyone), Администраторы (Administrators), Пользователи (Users), Опытные пользователи (Power Users), Операторы архива (Backup Operators)	Все (Everyone), Администраторы (Administrators), Пользователи (Users), Операторы архива (Backup Operators)
Работа в режиме операционной системы (Act As Part Of The Operating System)	Настройки по умолчанию нет	Настройки по умолчанию нет
Добавление рабочей станции к домену (Add Workstations To Domain)	Настройки по умолчанию нет	Настройки по умолчанию нет
Настройка квот памяти для процесса (Adjust Memory Quotas For A Process)	LOCAL SERVICE, NETWORK SERVICE, Администраторы (Administrators)	LOCAL SERVICE, NETWORK SERVICE, Администраторы (Administrators)
Разрешение локальной регистрации в системе (Allow Log On Locally)	Неприменимо	Гость (Guest), Администраторы (Administrators), Пользователи (Users), Операторы архива (Backup Operators)
Разрешение входа в систему через терминальные сервисы (Allow Logon Through Terminal Services)	Администраторы (Administrators), Пользователи удаленного рабочего стола (Remote Desktop Users)	Администраторы (Administrators), Пользователи удаленного рабочего стола (Remote Desktop Users)
Архивация файлов и каталогов (Back Up Files And Directories)	Администраторы (Administrators), Операторы архива (Backup Operators)	Администраторы (Administrators), Операторы архива (Backup Operators)
Обход перекрестной проверки (Bypass Traverse Checking)	Все (Everyone), Администраторы (Administrators), Пользователи (Users), Опытные пользователи (Power Users), Операторы архива (Backup Operators)	Все (Everyone), Администраторы (Administrators), Пользователи (Users), Операторы архива (Backup Operators)
Изменение системного времени (Change The System Time)	Администраторы (Administrators), Опытные пользователи (Power Users)	LOCAL SERVICE, Администраторы (Administrators)

Таблица 9.3 (продолжение)

Политика	Значение по умолчанию для Windows XP	Значение по умолчанию для Windows Vista/7
Изменение часового пояса (Change The Time Zone)	Неприменимо	LOCAL SERVICE, Администраторы (Administrators), Пользователи (Users)
Создание файла подкачки (Create A Pagefile)	Администраторы (Administrators)	Администраторы (Administrators)
Создание маркерного объекта (Create A Token Object)	Настройки по умолчанию нет	Настройки по умолчанию нет
Создание глобальных объектов (Create Global Objects)	Администраторы (Administrators), INTERACTIVE, SERVICE	Администраторы (Administrators), СЛУЖБА (SERVICE), LOCAL SERVICE, NETWORK SERVICE
Создание постоянных общих объектов (Create Permanent Shared Objects)	Настройки по умолчанию нет	Настройки по умолчанию нет
Создание символических ссылок (Create Symbolic Links)	Настройки по умолчанию нет	Администраторы (Administrators)
Отладка программ (Debug Programs)	Администраторы (Administrators)	Администраторы (Administrators)
Отказать в доступе к этому компьютеру из сети (Deny Access To This Computer From The Network)	SUPPORT, Гость (Guest)	Гость (Guest)
Отказать во входе в качестве пакетного задания (Deny Logon As A Batch Job)	Настройки по умолчанию нет	Настройки по умолчанию нет
Отказать во входе в качестве службы (Deny Logon As A Service)	Настройки по умолчанию нет	Настройки по умолчанию нет
Запретить локальный вход (Deny Logon Locally)	SUPPORT, Гость (Guest)	Гость (Guest)
Запретить вход в систему через терминальные сервисы	Настройки по умолчанию нет	Настройки по умолчанию нет

Таблица 9.3 (продолжение)

Политика	Значение по умолчанию для Windows XP	Значение по умолчанию для Windows Vista/7
Разрешение доверия к учетным записям пользователей и компьютеров при делегировании (Enable Computer And User Accounts To Be Trusted For Delegation)	Настройки по умолчанию нет	Настройки по умолчанию нет
Принудительное удаленное завершение работы (Force Shutdown From A Remote System)	Администраторы (Administrators)	Администраторы (Administrators)
Создание аудитов безопасности (Generate Security Audits)	LOCAL SERVICE, NETWORK SERVICE	LOCAL SERVICE, NETWORK SERVICE
Имитация клиента после проверки подлинности (Impersonate A Client After Authentication)	Администраторы (Administrators), СЛУЖБА (SERVICE)	Администраторы (Administrators), СЛУЖБА (SERVICE), LOCAL SERVICE, NETWORK SERVICE
Увеличение рабочего набора процесса (Increase A Process Working Set)	Настройки по умолчанию нет	Пользователи (Users)
Увеличение приоритета планирования (Increase Scheduling Priority)	Администраторы (Administrators)	Администраторы (Administrators)
Загрузка и выгрузка драйверов устройств (Load And Unload Device Drivers)	Администраторы (Administrators)	Администраторы (Administrators)
Блокировка страниц в памяти (Lock Pages In Memory)	Настройки по умолчанию нет	Настройки по умолчанию нет
Вход в качестве пакетного задания (Log On As A Batch Job)	SUPPORT, Администратор (Administrator)	Администраторы (Administrators), Операторы архива (Backup Operators)
Вход в качестве службы (Log On As A Service)	NETWORK SERVICE	Настройки по умолчанию нет

Таблица 9.3 (продолжение)

Политика	Значение по умолчанию для Windows XP	Значение по умолчанию для Windows Vista/7
Локальный вход (Log On Locally)	Гость (Guest), Администраторы (Administrators), Пользователи (Users), Опытные пользователи (Power Users), Операторы архива (Backup Operators)	Администраторы (Administrators), Пользователи (Users), Операторы архива (Backup Operators)
Управление аудитом и журналом безопасности (Manage Auditing And Security Log)	Администраторы (Administrators)	Администраторы (Administrators)
Изменение метки объекта (Modify An Object Label)	Неприменимо	Настройки по умолчанию нет
Изменение параметров среды изготовителя (Modify Firmware Environment Values)	Администраторы (Administrators)	Администраторы (Administrators)
Выполнение задач по обслуживанию томов (Perform Volume Maintenance Tasks)	Администраторы (Administrators)	Администраторы (Administrators)
Профилирование одного процесса (Profile Single Process)	Администраторы (Administrators), Опытные пользователи (Power Users)	Администраторы (Administrators)
Профилирование производительности системы (Profile System Performance)	Администраторы (Administrators)	Администраторы (Administrators)
Отключение компьютера от стыковочного узла (Remove Computer From Docking Station)	Администраторы (Administrators), Пользователи (Users), Опытные пользователи (Power Users)	Администраторы (Administrators), Пользователи (Users)
Замена маркера уровня процесса (Replace A Process Level Token)	LOCAL SERVICE, NETWORK SERVICE	LOCAL SERVICE, NETWORK SERVICE
Восстановление файлов и каталогов (Restore Files And Directories)	Администраторы (Administrators), Операторы архива (Backup Operators)	Администраторы (Administrators), Операторы архива (Backup Operators)

Таблица 9.3 (окончание)

Политика	Значение по умолчанию для Windows XP	Значение по умолчанию для Windows Vista/7
Завершение работы системы (Shut Down The System)	Администраторы (Administrators), Пользователи (Users), Опытные пользователи (Power Users), Операторы архива (Backup Operators)	Администраторы (Administrators), Пользователи (Users), Операторы архива (Backup Operators)
Синхронизация данных службы каталогов (Synchronize Directory Service Data)	Настройки по умолчанию нет	Настройки по умолчанию нет
Смена владельцев файлов и других объектов (Take Ownership Of Files Or Other Objects)	Администраторы (Administrators)	Администраторы (Administrators)

Основным отличием, как уже упоминалось, является то, что группа **Опытные пользователи** (Power Users) в Windows Vista и Windows 7 поддерживается исключительно для поддержания обратной совместимости с наследуемыми приложениями, и потому ей не присвоено никаких пользовательских прав.

Помимо этого, в Windows Vista/7 появились новые виды пользовательских прав:

- **Доступ к диспетчеру учетных данных от имени доверенного вызывающего** (Access Credential Manager As A Trusted Caller) — позволяет пользователю или группе устанавливать доверенные соединения с Диспетчером учетных данных (Credential Manager). В Windows Vista/7 Диспетчер учетных данных используется для управления учетной информацией пользователя. Учетная информация представляет собой набор данных, необходимых для регистрации в системе и аутентификации на конкретном сервере или конкретном сайте, — например, это может быть комбинация входного имени (user name) и пароля (password) или сертификата (certificate);
- **Разрешение локальной регистрации в системе** (Allow Log On Locally) — позволяет пользователю или группе регистрироваться в системе локально, используя для ввода клавиатуру. Изначально этот вид прав доступа носил наименование **Локальный вход в систему** (Log On Locally). В Windows Vista/7 существуют два вида этой привилегии:

Разрешение локальной регистрации в системе (Allow Log On Locally)

и **Запретить локальный вход** (Deny Log On Locally);

❑ **Изменение часового пояса (Change The Time Zone)** — позволяет пользователю или группе изменять часовой пояс. Так как члены стандартной группы **Пользователи (Users)** имеют это право по умолчанию, им для изменения часового пояса не нужны права администратора.

В Windows Vista/7 пользователи и запущенные ими процессы могут увеличивать рабочий набор процесса (working set), т. е. объем физической памяти, выделенной этому процессу операционной системой. Это изменение существенно влияет на работу приложений, использующих стандартную учетную пользовательскую информацию. Дело в том, что Windows Vista/7 ограничивает задачи, которые приложение может выполнять, и системные области, в которые приложение может выполнять запись. Если бы пользовательские права не позволяли увеличивать рабочий набор процесса, то приложения, запускаемые со стандартными пользовательскими привилегиями, часто страдали бы от недостатка памяти.

Изменения в параметрах безопасности

Параметры безопасности (Security Options) включают или отключают настройки безопасности для компьютера. Чтобы получить доступ к редактированию параметров безопасности, откройте консоль **Локальная политика безопасности (Local Security Policy)** и разверните дерево **Параметры безопасности (Security Settings)**, как показано на рис. 9.21.

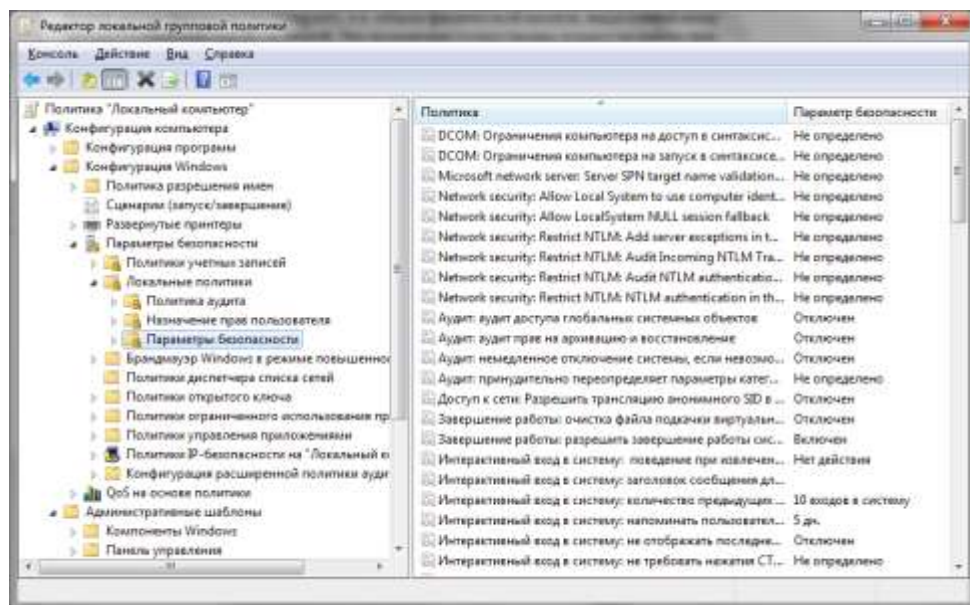


Рис. 9.21. Редактирование политики настроек безопасности

Сравнение типовых настроек безопасности в Windows XP и Windows Vista/7 приведено в табл. 9.4. Как и в предыдущих случаях, все изменения, в основном, являются следствием введения функции Контроля учетных записей пользователей (User Account Control, UAC).

Таблица 9.4. Типовые настройки безопасности в Windows XP и Windows Vista/7

Политика	Значение по умолчанию в Windows XP	Значение по умолчанию в Windows Vista/7
Учетные записи: Со- стояние учетной записи "Администратор" (Accounts: Administrator Account Status)	Неприменимо	Включен (Enabled)
Учетные записи: Со- стояние учетной записи "Гость" (Accounts: Guest Account Status)	Неприменимо	Отключен (Disabled)
Учетные записи: Раз- решить использование пустых паролей только при консольном входе (Accounts: Limit Local Account Use Of Blank Passwords To Console Logon Only)	Включен (Enabled)	Включен (Enabled)
Учетные записи: Пере- именование учетной записи "Администрато- р" (Accounts: Rename Administrator Account)	Администратор (Administrator)	Администратор (Administrator)
Учетные записи: Пере- именование учетной записи "Гость" (Accounts: Rename Guest Account)	Гость (Guest)	Гость (Guest)
Аудит: Аудит доступа глобальных системных объектов (Audit: Audit The Access Of Global Sys- tem Objects)	Отключен (Disabled)	Отключен (Disabled)
Аудит: Аудит прав на архивацию и восста- новление (Audit: Audit The Use Of Backup And Restore Privilege)	Отключен (Disabled)	Отключен (Disabled)

Таблица 9.4 (продолжение)

Политика	Значение по умолчанию в Windows XP	Значение по умолчанию в Windows Vista/7
Аудит: Немедленное отключение системы, если невозможно внести в журнал записи об аудите безопасности (Audit: Shut Down System Immediately If Unable To Log Security Audits)	Отключен (Disabled)	Отключен (Disabled)
DCOM: Ограничения компьютера на доступ в синтаксисе SDDL (Security Descriptor Definition Language) (DCOM: Machine Access Restrictions In Security Descriptor Definition Language (SDDL) Syntax)	Не определено	Не определено
DCOM: Ограничения компьютера на запуск в синтаксисе SDDL (Security Descriptor Definition Language) (COM: Machine Launch Restrictions In Security Descriptor Definition Language (SDDL) Syntax)	Не определено	Не определено
Устройства: Разрешать отстыковку без входа в систему (Devices: Allow Undock Without Having To Log On)	Включен (Enabled)	Включен (Enabled)
Устройства: Разрешить форматирование и извлечение съемных носителей (Devices: Allowed To Format And Eject Removable Media)	Администраторы (Administrators)	Не определено
Устройства: Запретить пользователям установку драйверов принтера (Devices: Prevent Users From Installing Printer Drivers)	Отключен (Disabled)	Отключен (Disabled)

Таблица 9.4 (продолжение)

Политика	Значение по умолчанию в Windows XP	Значение по умолчанию в Windows Vista/7
Устройства: Разрешить доступ к дисководам компакт-дисков только локальным пользователям (Devices: Restrict CD-ROM Access To Locally Logged-On User Only)	Отключен (Disabled)	Не определено
Устройства: Разрешить доступ к дисководам гибких дисков только локальным пользователям (Devices: Restrict Floppy Access To Locally Logged-On User Only)	Отключен (Disabled)	Не определено
Контроллер домена: Разрешить операторам сервера задавать выполнение заданий по расписанию (Domain Controller: Allow Server Operators To Schedule Tasks)	Не определено	Не определено
Контроллер домена: Требование цифровой подписи для LDAP-сервера (Domain Controller: LDAP Server Signing Requirements)	Не определено	Не определено
Контроллер домена: Запретить изменение пароля учетных записей компьютера (Domain Controller: Refuse Machine Account Password Changes)	Не определено	Не определено
Член домена: Всегда требуется цифровая подпись или шифрование потока данных защищенного канала (Domain Member: Digitally Encrypt Or Sign Secure Channel Data (Always))	Включен (Enabled)	Включен (Enabled)

Таблица 9.4 (продолжение)

Политика	Значение по умолчанию в Windows XP	Значение по умолчанию в Windows Vista/7
Член домена: Шифрование данных защищенного канала, когда это возможно (Domain Member: Digitally Encrypt Secure Channel Data (When Possible))	Включен (Enabled)	Включен (Enabled)
Член домена: Цифровая подпись безопасного канала, когда это возможно (Domain Member: Digitally Sign Secure Channel Data (When Possible))	Включен (Enabled)	Включен (Enabled)
Член домена: Отключить изменение пароля учетных записей компьютера (Domain Member: Disable Machine Account Password Changes)	Отключен (Disabled)	Отключен (Disabled)
Член домена: Максимальный срок действия учетных записей компьютера (Domain Member: Maximum Machine Account Password Age)	30 дней	30 дней
Член домена: Требовать стойкий ключ сеанса (Windows 2000 и выше) (Domain Member: Require Strong (Windows 2000 Or Later) Session Key)	Отключен (Disabled)	Отключен (Disabled)
Интерактивный вход в систему: не отображать последнее имя пользователя (Interactive Logon: Do Not Display Last User Name)	Отключен (Disabled)	Отключен (Disabled)

Таблица 9.4 (продолжение)

Политика	Значение по умолчанию в Windows XP	Значение по умолчанию в Windows Vista/7
Интерактивный вход в систему: не требовать нажатия Ctrl+Alt+Del (Interactive Logon: Do Not Require Ctrl+Alt+Del)	Не определено	Не определено
Интерактивный вход в систему: Текст сообщения для пользователей при входе в систему (Interactive Logon: Message Text For Users Attempting To Log On)	Не определено	Не определено
Интерактивный вход в систему: Заголовок сообщения для пользователей при входе в систему (Interactive Logon: Message Title For Users Attempting To Log On)	Не определено	Не определено
Интерактивный вход в систему: количество предыдущих подключений к кэш (в случае отсутствия доступа к контроллеру домена) (Interactive Logon: Number Of Previous Logons To Cache (In Case Domain Controller Is Not Available))	10	10
Интерактивный вход в систему: Напоминать пользователям об истечении срока действия пароля (Interactive Logon: Prompt User To Change Password Before Expiration)	14 дней	14 дней
Интерактивный вход в систему: Требовать проверки на контроллере домена для отмены блокировки компьютера (Interactive Logon: Require Domain Controller Authentication To Unlock Workstation)	Отключен (Disabled)	Отключен (Disabled)

Таблица 9.4 (продолжение)

Политика	Значение по умолчанию в Windows XP	Значение по умолчанию в Windows Vista/7
Интерактивный вход в систему: Требовать смарт-карту (Interactive Logon: Require Smart Card)	Не определено	Не определено
Интерактивный вход в систему: поведение при извлечении смарт-карты (Interactive Logon: Smart Card Removal Behavior)	Нет действия (No Action)	Нет действия (No Action)
Клиент сети Microsoft: Использовать цифровую подпись (всегда) (Microsoft Network Client: Digitally Sign Communications (Always))	Отключен (Disabled)	Отключен (Disabled)
Клиент сети Microsoft: Использовать цифровую подпись (с согласия сервера) (Microsoft Network Client: Digitally Sign Communications (If Server Agrees))	Включен (Enabled)	Включен (Enabled)
Клиент сети Microsoft: Посылать незашифрованный пароль сторонним SMB-серверам (Microsoft Network Client: Send Unencrypted Password To Third-Party SMB Servers)	Отключен (Disabled)	Отключен (Disabled)
Сервер сети Microsoft: Время бездействия до приостановки сеанса (Microsoft Network Server: Amount Of Idle Time Required Before Suspending Session)	15 минут	15 минут
Сервер сети Microsoft: Использовать цифровую подпись (всегда) (Microsoft Network Server: Digitally Sign Communications (Always))	Отключен (Disabled)	Отключен (Disabled)

Таблица 9.4 (продолжение)

Политика	Значение по умолчанию в Windows XP	Значение по умолчанию в Windows Vista/7
Сервер сети Microsoft: Использовать цифровую подпись (с согласия клиента) (Microsoft Network Server: Digitally Sign Communications (If Client Agrees))	Отключен (Disabled)	Отключен (Disabled)
Сервер сети Microsoft: Отключать клиентов по истечении разрешенных часов входа (Microsoft Network Server: Disconnect Clients When Logon Hours Expire)	Включен (Enabled)	Включен (Enabled)
Сетевой доступ: Разрешить анонимную трансляцию SID (Network Access: Allow Anonymous SID/Name Translation)	Отключен (Disabled)	Отключен (Disabled)
Сетевой доступ: Не разрешать перечисление учетных записей SAM анонимными пользователями (Network Access: Do Not Allow Anonymous Enumeration Of SAM Accounts)	Включен (Enabled)	Включен (Enabled)
Сетевой доступ: Не разрешать перечисление учетных записей SAM и общих ресурсов анонимными пользователями (Network Access: Do Not Allow Anonymous Enumeration Of SAM Accounts And Shares)	Отключен (Disabled)	Отключен (Disabled)

Таблица 9.4 (продолжение)

Политика	Значение по умолчанию в Windows XP	Значение по умолчанию в Windows Vista/7
Сетевой доступ: Не разрешать сохранение учетных данных или цифровых паспортов .NET Passports для сетевой проверки подлинности пользователя (Network Access: Do Not Allow Storing user credential of .NET Passports For Network Authentication)	Отключен (Disabled)	Отключен (Disabled)
Сетевой доступ: Разрешать применение Разрешений "для всех" к анонимным пользователям (Network Access: Let Bce (Everyone) Permissions Apply To Anonymous Users)	Отключен (Disabled)	Отключен (Disabled)
Сетевой доступ: Именованные каналы, доступные анонимным пользователям (Network Access: Named Pipes That Can Be Accessed Anonymously)	COMNAP, COMNODE, SQL\QUERY, SPOOLSS, LLSRPC, Browser	SQL\QUERY, SPOOLSS, Netlogon, Lsarpc, Samr, Browser
Сетевой доступ: Удаленно доступные пути реестра (Network Access: Remotely Accessible Registry Paths)	(Множество путей, определенных как доступные)	Не определено
Сетевой доступ: Удаленно доступные пути и вложенные пути реестра (Network Access: Remotely Accessible Registry Paths And Sub-Paths)	Не применимо	Не определено
Сетевой доступ: Запретить анонимный доступ к именованным каналам и общим ресурсам (Network Access: Restrict Anonymous Access To Named Pipes And Shares)	Включен (Enabled)	Включен (Enabled)

Таблица 9.4 (продолжение)

Политика	Значение по умолчанию в Windows XP	Значение по умолчанию в Windows Vista/7
Сетевой доступ: общие ресурсы, доступ к которым можно получить анонимно (Network Access: Shares That Can Be Accessed Anonymously)	COMCFG, DFS\$	Не определено
Сетевой доступ: Модель совместного доступа и безопасности для локальных учетных записей (Network Access: Sharing And Security Model For Local Accounts)	Только Гость (Guest Only) — Локальные пользователи аутентифицируются как гости (Local Users Authenticate As Guest)	Классическая (Classic) — Локальные пользователи аутентифицируются от своего имени (Local Users Authenticate As Themselves)
Сетевая безопасность: Не хранить хэш-значения LAN Manager при следующей смене пароля (Network Security: Do Not Store LAN Manager Hash Value On Next Password Change)	Отключен (Disabled)	Включен (Enabled)
Сетевая безопасность: Принудительный вывод из сеанса по истечении допустимых часов работы (Network Security: Force Logoff When Logon Hours Expire)	Отключен (Disabled)	Отключен (Disabled)
Сетевая безопасность: Уровень проверки подлинности LAN Manager (Network Security: LAN Manager Authentication Level)	Отправлять ответы LM и NTLM (Send LM & NTLM Responses)	Отправлять только ответ NTLMv2 (Send NTLMv2 Response Only)
Сетевая безопасность: Требование цифровой подписи для LDAP-клиента (Network Security: LDAP Client Signing Requirements)	Согласование цифровой подписи (Negotiate Signing)	Согласование цифровой подписи (Negotiate Signing)

Таблица 9.4 (продолжение)

Политика	Значение по умолчанию в Windows XP	Значение по умолчанию в Windows Vista/7
Сетевая безопасность: Минимальная сеансовая безопасность для клиентов на базе NTLM SSP (включая безопасный RPC) (Network Security: Minimum Session Security For NTLM SSP Based (Including Secure RPC) Clients)	Минимума нет (No Minimum)	Минимума нет (No Minimum)
Сетевая безопасность: Минимальная сеансовая безопасность для серверов на базе NTLM SSP (включая безопасный RPC) (Network Security: Minimum Session Security For NTLM SSP Based (Including Secure RPC) Servers)	Минимума нет (No Minimum)	Минимума нет (No Minimum)
Консоль восстановления: разрешить автоматический вход администратора (Recovery Console: Allow Automatic Administrative Logon)	Отключен (Disabled)	Отключен (Disabled)
Консоль восстановления: разрешить копирование дискет и доступ ко всем дискам и папкам (Recovery Console: Allow Floppy Copy And Access To All Drives And All Folders)	Отключен (Disabled)	Отключен (Disabled)
Завершение работы: Разрешить завершение работы системы без выполнения входа в систему (Shutdown: Allow System To Be Shut Down Without Having To Log On)	Включен (Enabled)	Включен (Enabled)

Таблица 9.4 (продолжение)

Политика	Значение по умолчанию в Windows XP	Значение по умолчанию в Windows Vista/7
Завершение работы: Очистка файла подкачки виртуальной памяти (Shutdown: Clear Virtual Memory Pagefile)	Отключен (Disabled)	Отключен (Disabled)
Системная криптография: Обязательное использование сильной защиты ключей пользователей, хранящихся на компьютере (System Cryptography: Force Strong Key Protection For User Keys Stored On The Computer)	Не применимо	Не определено
Системная криптография: Использовать FIPS-совместимые алгоритмы для шифрования, хэширования и подписывания (System Cryptography: Use FIPS Compliant Algorithms For Encryption, Hashing, And Signing)	Отключен (Disabled)	Отключен (Disabled)
Системные объекты: Владелец по умолчанию для объектов, созданных членами группы "Администраторы" (System Objects: Default Owner For Objects Created By Members Of The Administrators Group)	Создатель объекта (Object Creator)	Создатель объекта (Object Creator)
Системные объекты: Не учитывать регистр для подсистем, отличных от Windows (System Objects: Require Case Insensitivity For Non-Windows Subsystems)	Включен (Enabled)	Включен (Enabled)

Таблица 9.4 (продолжение)

Политика	Значение по умолчанию в Windows XP	Значение по умолчанию в Windows Vista/7
Системные объекты: Усилить разрешения по умолчанию для внутренних системных объектов (например, символических ссылок) (System Objects: Strengthen Default Permissions Of Internal System Objects (for example, Symbolic Links))	Включен (Enabled)	Включен (Enabled)
Параметры системы: Необязательные под-системы (System Settings: Optional Subsystems)	Не применимо	Posix
Параметры системы: Использовать правила сертификатов для исполняемых файлов Windows для политик ограниченного использования программ (System Settings: Use Certificate Rules On Windows Executables For Software Restriction Policies)	Не применимо	Отключен (Disabled)
Управление учетными записями пользователей: 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)	Не применимо	Запрос согласия (Prompt For Consent)

Таблица 9.4 (продолжение)

Политика	Значение по умолчанию в Windows XP	Значение по умолчанию в Windows Vista/7
Управление учетными записями пользователей: Поведение запроса на повышение прав для обычных пользователей (User Account Control: Behavior Of The Elevation Prompt For Standard Users)	Не применимо	Запрос учетных данных (Prompt For Credentials)
Управление учетными записями пользователей: Обнаружение установки приложений и запрос на повышение прав (User Account Control: Detect Application Installations And Prompt For Elevation)	Не применимо	Включен (Enabled)
Управление учетными записями пользователей: Повышение прав только для подписанных и проверенных исполняемых файлов (User Account Control: Only Elevate Executables That Are Signed And Validated)	Не применимо	Отключен (Disabled)
Управление учетными записями пользователей: Все администраторы работают в режиме одобрения администратором (User Account Control: Run All Administrators In Admin Approval Mode)	Не применимо	Включен (Enabled)

Таблица 9.4 (окончание)

Политика	Значение по умолчанию в Windows XP	Значение по умолчанию в Windows Vista/7
Управление учетными записями пользователей: Переключение к безопасному рабочему столу при выполнении запроса на повышение прав (User Account Control: Switch To The Secure Desktop When Prompting For Elevation)	Не применимо	Включен (Enabled)
Управление учетными записями пользователей: При сбоях записи в файл или реестр виртуализация в расположение пользователя (User Account Control: Virtualize File And Registry Write Failures To Per-User Locations)	Не применимо	Включен (Enabled)

Ряд наиболее важных изменений в настройках безопасности Windows Vista/7 связан со следующими настройками сетевой безопасности:

- ❑ **Удаленный доступ к реестру** (Remote registry access) — в Windows XP множество путей реестра доступны удаленно по умолчанию. В Windows Vista/7 никакие из путей реестра по умолчанию не указаны как доступные удаленно — это повышает защищенность. Кроме того, в состав Windows Vista и Windows 7 входит новая опция безопасности, позволяющая управлять доступом к вложенным ключам реестра — **Сетевой доступ: Удаленно доступные пути и вложенные пути реестра** (Network Access: Remotely Accessible Registry Paths And Sub-Paths);
- ❑ **Анонимный доступ к именованным каналам и общим ресурсам** (Anonymous access to named pipes and shares) — в состав Windows Vista и Windows 7 добавлена опция безопасности, ограничивающая анонимный доступ к именованным каналам и общим ресурсам. Это изменение блокирует такой анонимный доступ;
- ❑ **Модель совместного доступа и безопасности для локальных учетных записей** (Network Access: Sharing And Security Model For Local Accounts) — в Windows XP локальные пользователи по умолчанию аутентифицируют-

ся как гости (guests). В Windows Vista и Windows 7 локальные пользователи аутентифицируются от собственного имени. Это изменение повышает уровень безопасности за счет того, что пользователи, зарегистрировавшиеся в системе, гарантированно имеют необходимые разрешения на доступ ко всем областям файловой системы;

- ❑ **Хранение хэш-значений LAN Manager** (Network Security: Do Not Store LAN Manager Hash Value On Next Password Change) — в Windows XP, когда пользователь производит смену пароля, на компьютере можно сохранить хэш-значение LAN Manager, которое помогает в последующей аутентификации. Windows Vista гарантирует, что эти хэш-значения не хранятся на компьютере. Это повышает общую защищенность системы за счет того, что пользователь при каждой смене пароля должен получать новое хэш-значение;
- ❑ **Аутентификация LAN Manager** (LAN Manager authentication) — в Windows XP клиентские компьютеры используют аутентификацию LM и NTLM, а также более новую версию протокола NTLMv2. В Windows Vista/7 клиентские компьютеры используют только аутентификацию NTLMv2 и могут применять сеансовую защиту NTLMv2, если она поддерживается сервером. Таким образом, процесс аутентификации стал более защищенным.

Совместное использование файлов и полномочия доступа к ним в Windows Vista/7

Windows Vista/7 предоставляет возможность совместно с другими пользователями оперировать файлами в локальной системе и в сети. С выходом каждой новой версии в этой области появлялись различные усовершенствования. Основные отличия модели совместного доступа к файлам и принтерам, реализованной в Windows Vista/7, от модели Windows XP, сводятся к следующему:

- ❑ имя рабочей группы, используемое по умолчанию в Windows Vista/7, — WORKGROUP. В Windows XP Home Edition по умолчанию использовалось имя рабочей группы MSHOME. Если вы устанавливаете Windows Vista/7 как обновление Windows XP Home Edition, то имя рабочей группы, использовавшееся в Windows XP, сохранится и в Windows Vista/7;
- ❑ Windows Vista/7 использует папку **Общие** (Public) вместо папки **Общие документы** (Shared Documents) в Windows XP. Если активизирован совместный доступ, то любые папки и все объекты, вложенные в папку **Общие**, будут автоматически выделены в совместный доступ под именем

Общие. При этом конфигурировать совместный доступ к файлам для отдельных папок не требуется. Файл или папку, которую вы желаете предоставить в совместный доступ, будет достаточно скопировать в папку **Общие**;

- ❑ по умолчанию Windows Vista/7 не поддерживает модель простого общего доступа к файлам и папкам (simple file sharing). Доступ к общим папкам, в том числе к папке **Общие**, требует ввода пользовательского имени и пароля.

ПРИМЕЧАНИЕ

В Windows 7, в дополнение к этому, реализованы два дополнительных усовершенствования, а именно: домашняя группа (homegroup), которая была вкратце рассмотрена в *главе 8*, а также дополнительный механизм безопасности, позволяющий предотвратить случайное уничтожение файла или папки другими пользователями, не являющимися владельцами данных объектов (рис. 9.22). Таким образом, чтобы изменить права доступа к папке или файлу, необходимо сначала присвоить себе права владельца, а затем уже открывать общий доступ и устанавливать права для конкретных пользователей.

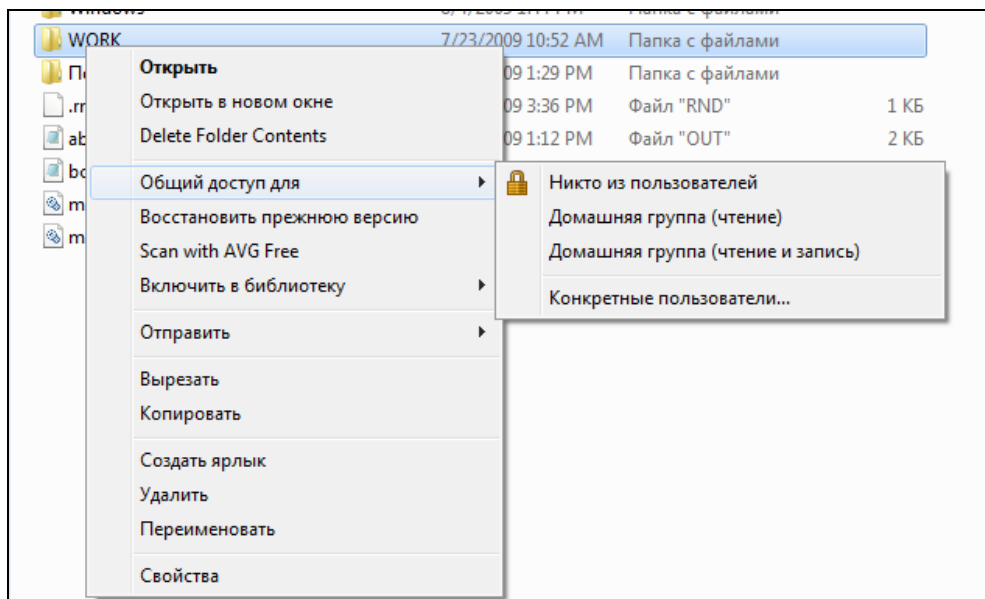


Рис. 9.22. Контекстное меню для предоставления общего доступа к папке в Windows 7

Конфигурирование совместного доступа к файлам и папкам в Windows Vista и Windows 7

Конфигурирование совместного доступа к файлам и принтерам в Windows Vista и Windows 7 состоит из следующих шагов:

1. Установка одинакового имени рабочей группы на всех принадлежащих к этой группе компьютерах.
2. Указание типа сети (network location type).
3. Включение общего доступа к файлам и принтерам.

Указание имени рабочей группы

Чтобы определить имя рабочей группы для компьютера, работающего под управлением Windows Vista или Windows 7, раскройте окно **Панель управления** (Control Panel) и выполните двойной щелчок по значку **Система** (System). Имя рабочей группы отображается в раскрывшемся окне (рис. 9.23) в группе опций **Имя компьютера, имя домена и параметры рабочей группы** (Computer name, domain, and workgroup settings).

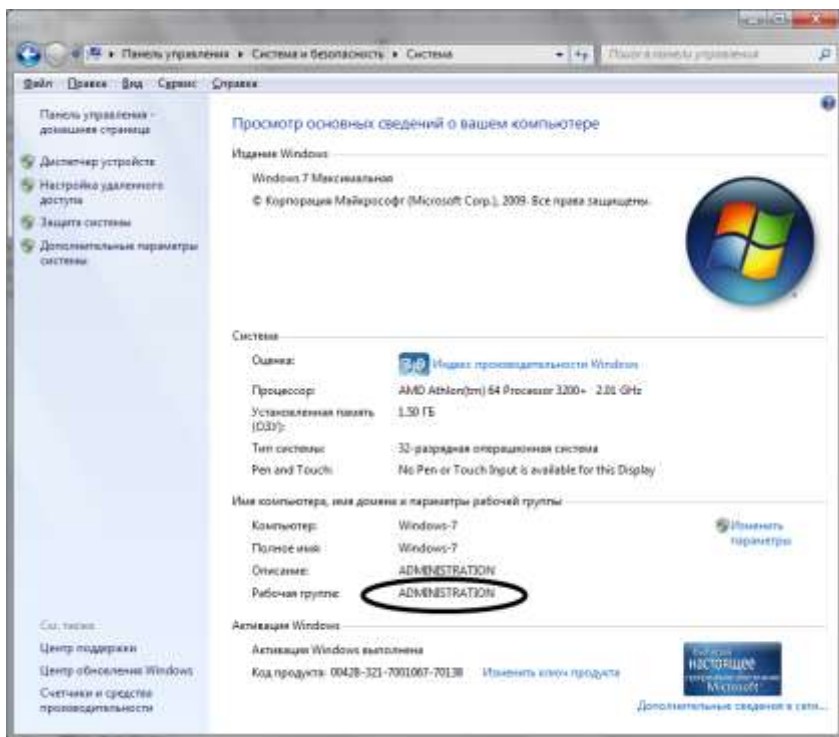


Рис. 9.23. Просмотр имени рабочей группы в Windows Vista/7

Чтобы сконфигурировать имя рабочей группы для компьютера Windows Vista/7, проделайте следующее:

1. Выполните щелчок мышью по ссылке **Изменить параметры** (Change settings) в группе опций **Имя компьютера, имя домена и параметры рабочей группы**.
2. На вкладке **Имя компьютера** (Computer Name) окна **Свойства системы** (System Properties) нажмите кнопку **Изменить** (Change).
3. Откроется окно **Изменение имени компьютера или домена** (Computer Name/Domain Changes), показанное на рис. 9.24. Введите нужное имя в поле **Имя компьютера**, при необходимости подключитесь к домену или введите нужное имя рабочей группы (по умолчанию — `Workgroup`), и нажмите кнопку **ОК**.
4. В диалоговом окне, которое откроется сразу же после этого, нажмите кнопку **ОК**.
5. Нажмите кнопку **Заккрыть** (Close). Чтобы внесенные изменения вошли в силу, вам потребуется перезагрузка.

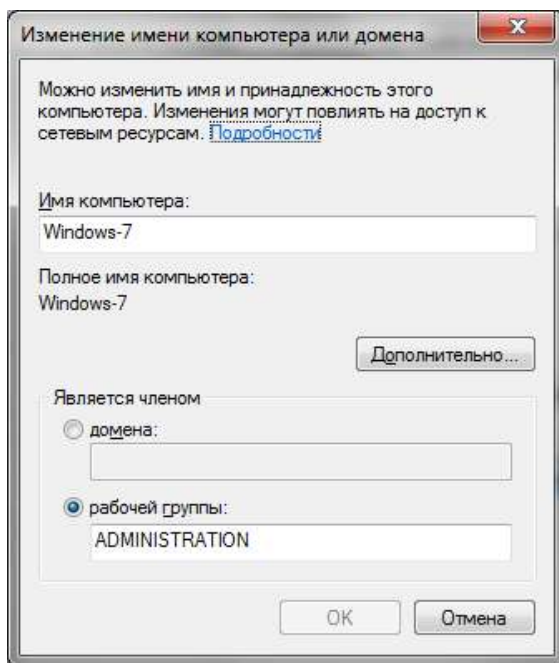


Рис. 9.24. Диалоговое окно **Изменение имени компьютера или домена**

Настройка сетевого размещения

Сетевое размещение (network location type) — это параметр Windows Vista/7, в соответствии с которым операционная система автоматически конфигурирует параметры безопасности и другие настройки, имеющие отношение к сетевому доступу. В Windows Vista и Windows 7 поддерживаются следующие типы сетевого размещения:

- ❑ **Домен (Domain)** — компьютер подключен к сети, управляемой контроллером домена Active Directory. Примером такой сети является интрасеть масштаба предприятия;
- ❑ **Общественная сеть (Public)** — компьютер подключен к сети, имеющей прямое соединение с Интернетом. Примерами таких сетей являются сети с доступом в Интернет, организованные в аэропортах, библиотеках, интернет-клубах и т. п.;
- ❑ **Частная сеть (Private)**, как в Windows Vista или **Домашняя сеть (Home)**, как в Windows 7, — компьютер подключен к сети, имеющей некоторый уровень защиты от вторжения из Интернета, и содержит в своем составе доверенные (trusted) компьютеры. Примерами таких сетей являются частные домашние сети или сети малых предприятий, защищенные брандмауэрами.

Чтобы просмотреть текущий тип сетевого соединения, нажмите кнопку **Пуск** (Start), щелкните правой кнопкой мыши по пункту **Сеть (Network)** и из контекстного меню выберите команду **Свойства (Properties)**. Раскроется окно Центра управления сетями и общим доступом (рис. 9.25 и 9.26), уже знакомое нам по *главе 8*.

СОВЕТ

Для сетей малых предприятий и домашних сетей рекомендуется выбирать сетевое размещение типа **Частная сеть (Private)**, если вы работаете в Windows Vista, или **Домашняя сеть (Home)**, если вы работаете в Windows 7.

Если у вас установлен какой-либо тип сетевого размещения (например, **Общественная сеть**) и требуется изменить его на другой, например, на домашнюю сеть, сделайте следующее:

1. В Windows Vista справа от имени сети (см. рис. 9.25) находится ссылка **Настройка (Customize)**, а в Windows 7 (рис. 9.26) — ссылка с указанием типа сетевого размещения (в приведенном примере — это сеть предприятия). Выполните щелчок мышью на этой ссылке.
2. На экране откроется окно **Настройка сетевого размещения (Set Network Location)**. Обратите внимание на различия в виде этого окна в Windows Vista (рис. 9.27) и в Windows 7 (рис. 9.28).
3. В любом случае, сделайте ваш выбор — это операция простая и самоочевидная.

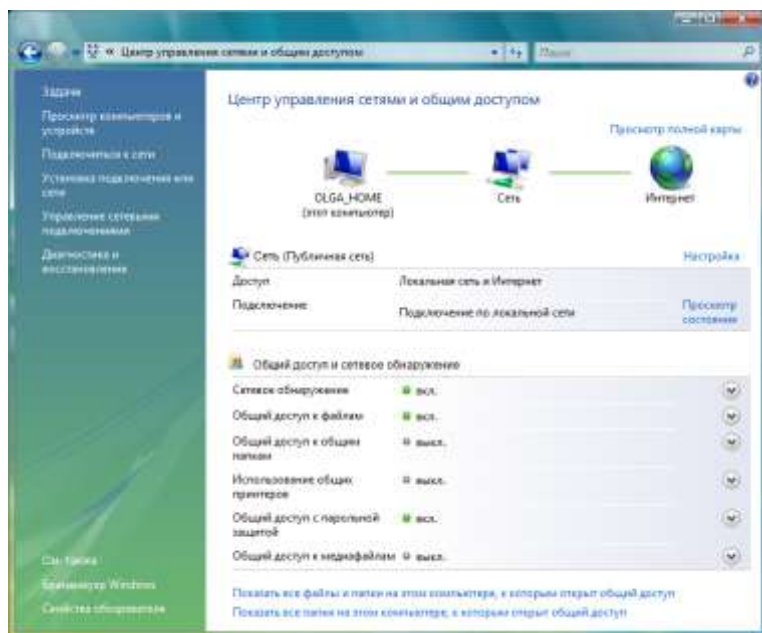


Рис. 9.25. Пример подключения к публичной сети (Windows Vista)

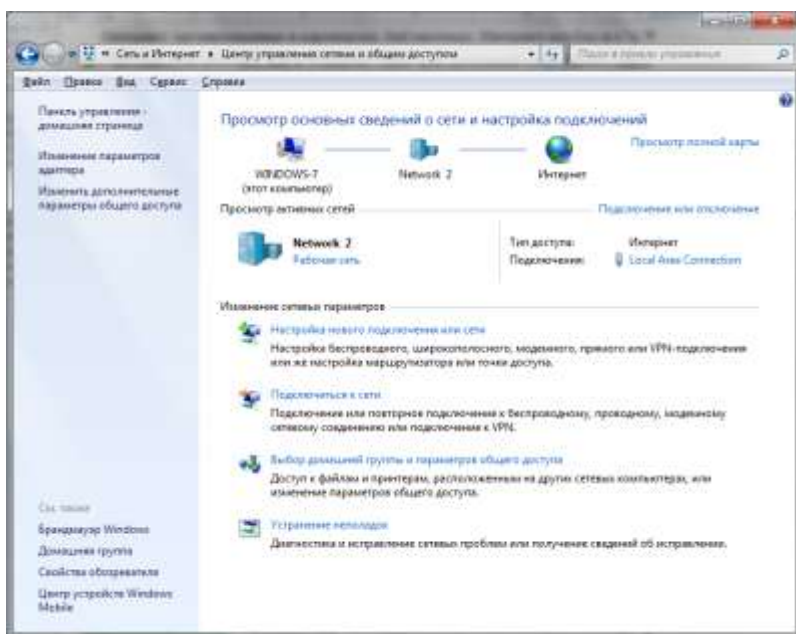


Рис. 9.26. Пример подключения к рабочей сети (Windows 7)

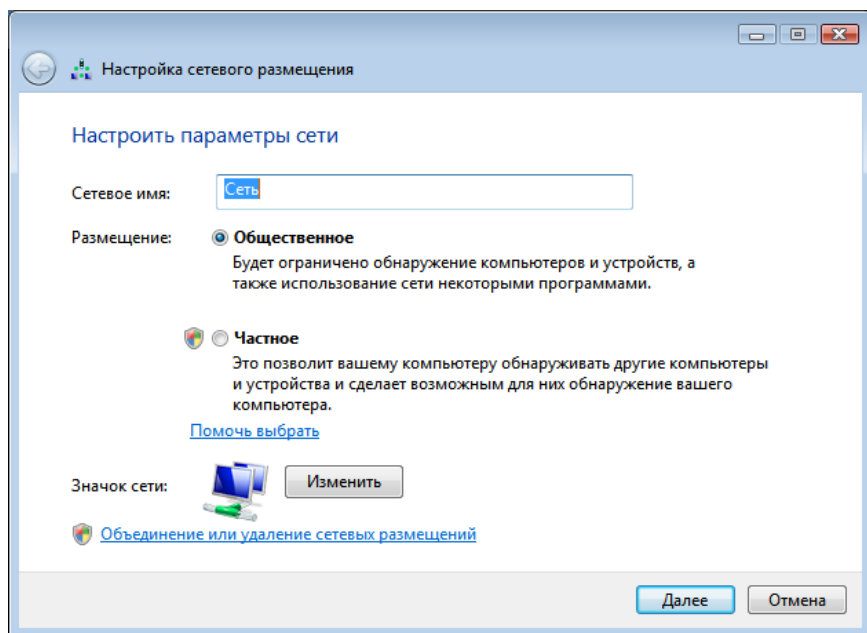


Рис. 9.27. Окно Настройка сетевого размещения (Windows Vista)

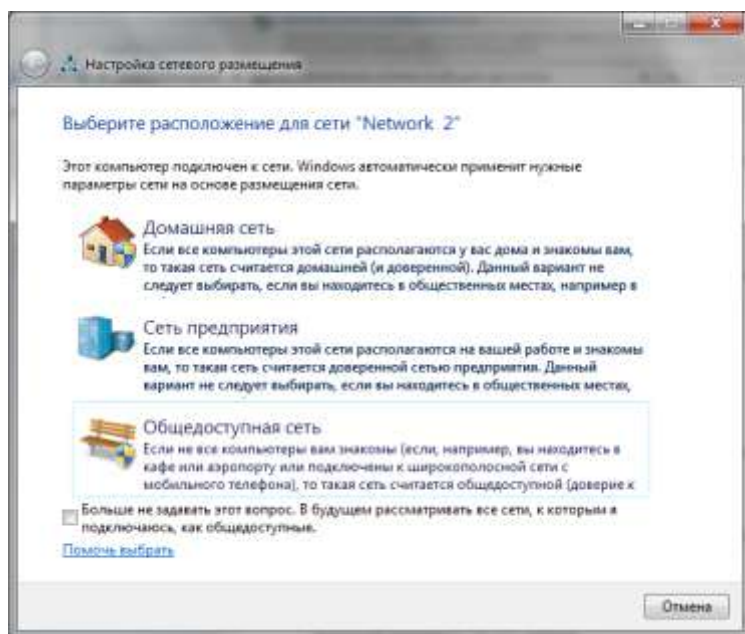


Рис. 9.28. Окно Настройка сетевого размещения в Windows 7

ПРИМЕЧАНИЕ

В Windows Vista вам требовалось настраивать опции совместного использования файлов и принтеров, вручную выбирая опции из группы **Общий доступ и сетевое обнаружение** (Sharing and Discovery) окна Центра управления сетями и общим доступом (см. рис. 9.25). В Windows 7 все нужные опции конфигурируются автоматически, и вы избавлены от этой необходимости.

Предоставление папки в общий доступ

Чтобы предоставить в общий доступ одну из папок на компьютере Windows 7, действуйте следующим образом:

1. Щелкните правой кнопкой мыши по папке, для которой требуется задать параметры общего доступа, и выберите из контекстного меню опцию **Общий доступ для** (Shared access for). В этом меню вам будут доступны следующие опции (см. рис. 9.22):
 - **Никто из пользователей** (Nobody);
 - **Домашняя группа (чтение)** (HomeGroup (Read));
 - **Домашняя группа (чтение и запись)** (HomeGroup (Read and Write));
 - **Конкретные пользователи** (Specific users).

СОВЕТ

Если вы выберете опцию **Никто из пользователей** (Nobody), то доступа к папке не будет иметь никто, кроме владельца. Чтобы изменить права доступа к такой папке или такому файлу, вам сначала потребуется забрать себе права владельца. О том, как это делается, было рассказано ранее в этой главе на примере файла Regedit.exe. Две следующих опции относятся к домашней группе (HomeGroup), которая вкратце была рассмотрена в *главе 8*.

2. Выберите опцию **Конкретные пользователи** (Specific users). На экране откроется окно, показанное на рис. 9.29. Если вы хотите прекратить общий доступ к папке, выберите опцию **Прекратить общий доступ** (Stop sharing). Чтобы модифицировать список пользователей, имеющих доступ к объекту, выберите вторую опцию — **Изменить разрешения на общий доступ** (Modify sharing permissions).
3. На экране откроется следующее окно, в котором вы сможете добавить в список тех пользователей, которым вы решили предоставить общий доступ к файлу или папке, и установить уровень прав доступа (рис. 9.30). Добавив в список нужных пользователей, нажмите кнопку **Общий доступ** (Sharing), и через несколько секунд ваша цель будет достигнута.

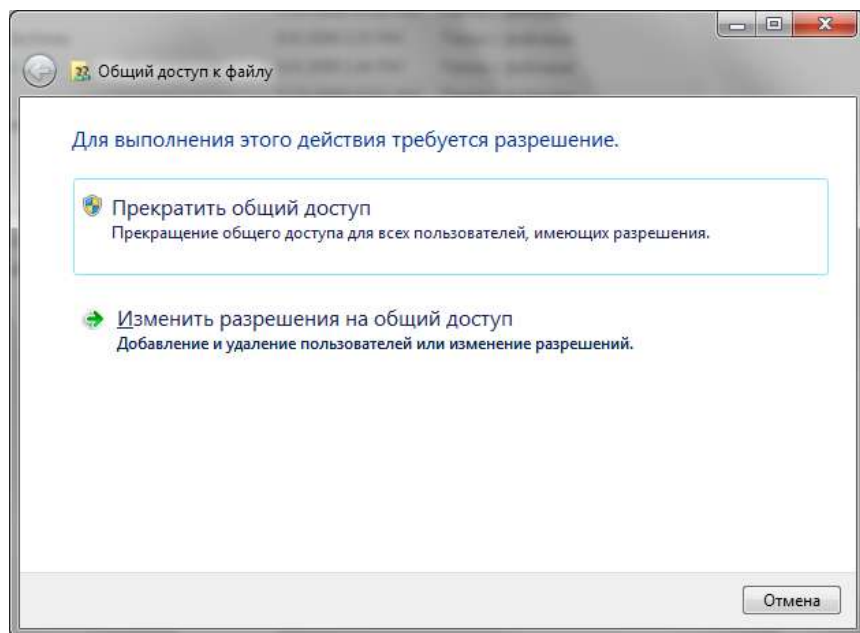


Рис. 9.29. Окно **Общий доступ к файлу**

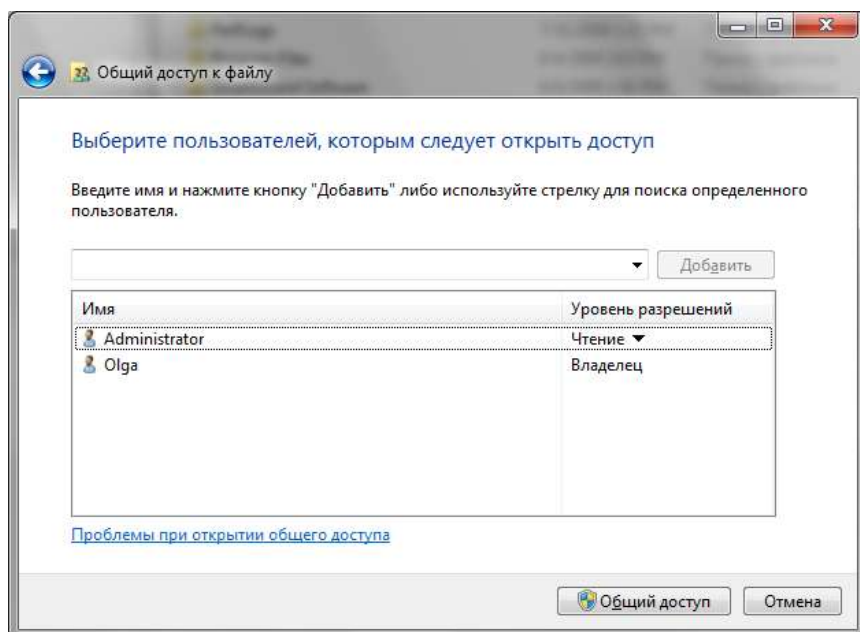
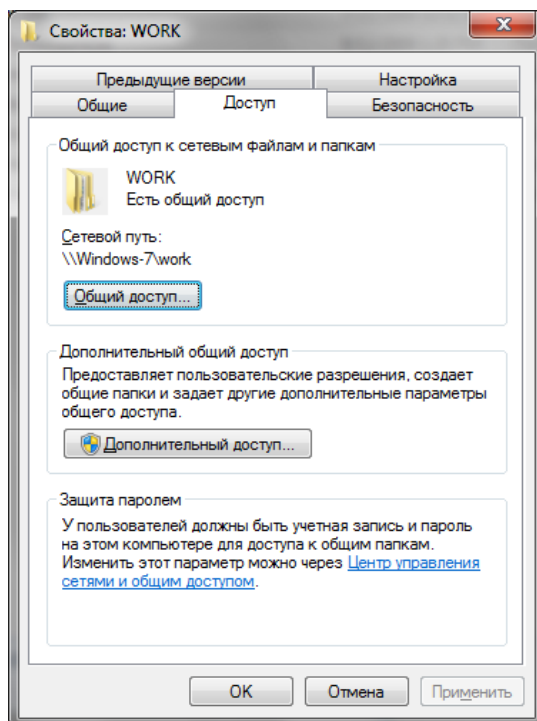
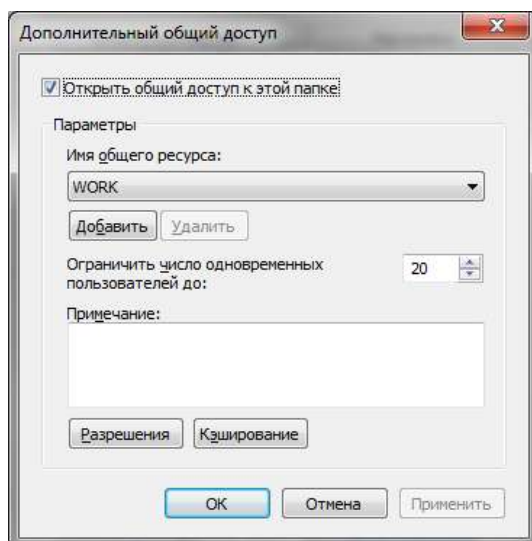


Рис. 9.30. Добавление пользователей в список контроля доступа к файлу или папке

Рис. 9.31. Вкладка **Доступ** окна свойств папкиРис. 9.32. Окно **Дополнительный общий доступ**

ПРИМЕЧАНИЕ

Обратите внимание, насколько упростилась эта процедура по сравнению с аналогичной в Windows Vista.

Предоставить папку в общий доступ можно и из окна свойств папки (рис. 9.31). Для этой цели проделайте следующее:

1. В окне **Компьютер** (Computer) найдите папку, которую требуется предоставить в общий доступ, и выполните на ней щелчок правой кнопкой мыши.
2. Из контекстного меню выберите команду **Свойства** (Properties) и перейдите на вкладку **Доступ** (Sharing).
3. Нажмите кнопку **Общий доступ** (Share), и на экране откроется уже описанное ранее окно **Общий доступ к файлу** (см. рис. 9.26). Чтобы сконфигурировать дополнительные опции совместного доступа, нажмите кнопку **Дополнительный доступ** (Advanced Sharing).
4. После нажатия кнопки **Дополнительный доступ** Windows Vista отобразит окно **Дополнительный общий доступ** (Advanced Sharing), показанное на рис. 9.32.

В этом окне можно проделать следующие операции:

- создать один или несколько разделяемых ресурсов для выбранной папки под разными именами;
- указать максимальное количество пользователей, которые могут одновременно подключиться к общей папке (от 1 до 20);
- добавить примечание, помогающее пользователям ориентироваться в общих папках;
- указать права доступа к разделяемой папке. Для этого следует нажать кнопку **Разрешения** (Permissions) и в окне **Разрешения для <имя папки>** (рис. 9.33) указать права доступа для отдельных пользователей и групп;
- указать, будет ли доступна общая папка в автономном режиме. Для этого следует нажать кнопку **Кэширование** (Caching) (см. рис. 9.32).

Чтобы убедиться в том, что папка действительно предоставлена в общий доступ, просмотрите сеть, найдите в ней свой компьютер, раскройте его и убедитесь, что в нем отображается и папка, которую вы только что сконфигурировали как предоставленную в общий доступ (рис. 9.34).

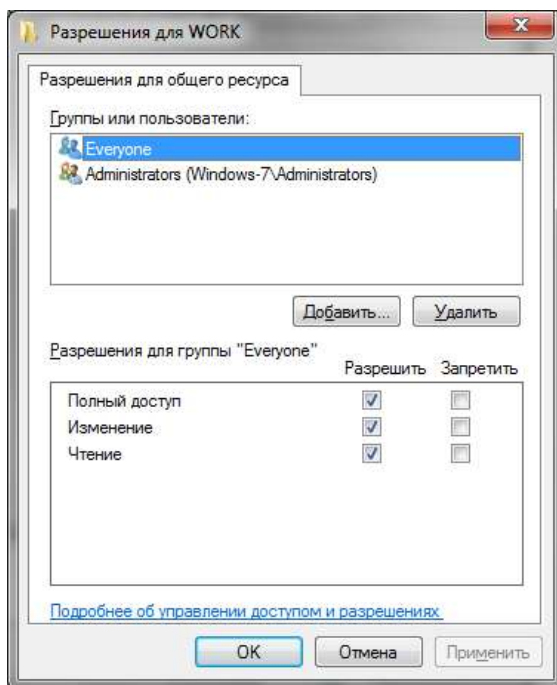


Рис. 9.33. Конфигурирование прав доступа для разделяемой папки

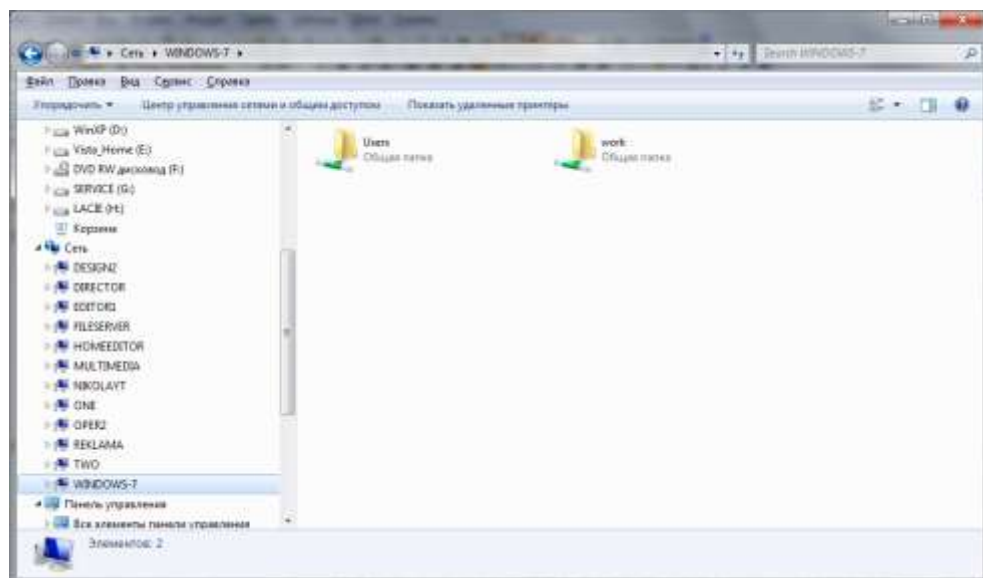


Рис. 9.34. Просмотр списка разделяемых папок и принтеров

Получение доступа к общим папкам и возможные проблемы

Если на компьютере Windows Vista/7, к разделяемым ресурсам которого вы пытаетесь получить доступ через сеть, установлена парольная защита, то при получении доступа возможны следующие варианты:

- ❑ при регистрации от имени пользователя, учетная запись которого была добавлена к списку пользователей, которым открыт доступ к папке, попытка соединения будет успешной;
- ❑ при регистрации от имени пользователя, чье имя не было добавлено в список пользователей, которым открыт доступ к разделяемой папке, вам будет предложено ввести входное имя и пароль одного из пользователей, имеющих к этой папке доступ;
- ❑ при регистрации от имени пользователя, учетная запись которого присутствует в списке пользователей на компьютере, где расположена общая папка, но не добавлена в список пользователей, которым открыт доступ к этому ресурсу, доступ к общей папке будет отклонен.

Если на компьютере, к которому вы пытаетесь подключиться, отключена парольная защита, в большинстве случаев попытка доступа к папке, предоставленной в общий доступ, завершится успехом, причем вводить входное имя и пароль не потребуется.

Тем не менее, если в список пользователей общей папки не внесены учетные записи **Гость** (Guest) или **Все** (Everyone), то доступ к папке, предоставленной в общее пользование, может завершиться неудачей даже после того, как пользователь введет входное имя и пароль. Чтобы исправить эту ситуацию, добавьте в список пользователей, которым разрешен доступ к разделяемой папке, учетную запись **Гость** (Guest) или группу **Все** (Everyone).

Обязательный контроль целостности в Windows Vista и Windows 7

В Windows Vista/7 реализована новая функциональная возможность, известная как *Обязательный контроль целостности* (Mandatory integrity control, MIC). Управление осуществляется с помощью элемента списка контроля доступа (access control entry, ACE) в системном списке контроля доступа (system access control list, SACL) защищаемого объекта (например, файла, процесса, ключа реестра и т. д.). Каждый процесс имеет уровень целостности (integrity level), и дочерние процессы наследуют уровень целостности от родительских. Прежде чем объяснять, что представляет собой обязательный

контроль целостности в действии, я предлагаю вам провести простой эксперимент.

1. Загрузитесь в Windows 7, войдите в систему, например, как пользователь из группы **Администраторы** (Administrators) и запустите любое приложение — например, простой текстовый редактор Блокнот (Notepad). Введите какой-нибудь текст и сохраните файл.
2. Запустите сеанс командной строки с административными полномочиями (рис. 9.35). Перейдите в папку, где был сохранен тестовый файл (в данном случае это файл C:\Users\Olga\Documents), и введите следующую команду:

```
icacls test.txt /setintegritylevel H
```

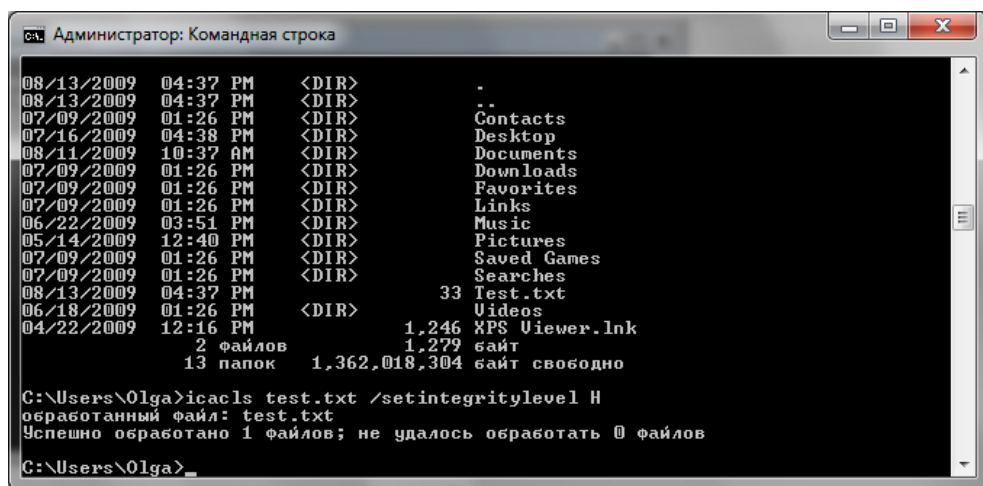


Рис. 9.35. Установка более высокого уровня целостности для тестового файла

3. Теперь снова запустите Блокнот (не из командной строки с административными правами, а обычным образом). Например, найдите наш тестовый файл на рабочем столе и выполните на нем двойной щелчок мышью.
4. Внесите в файл некоторые изменения и попробуйте его сохранить (рис. 9.36). Ну как, получилось?

Уровни контроля целостности активизируются и блокируются следующим ключом реестра: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\EnableMIC.

Остальные функции обеспечения безопасности, в том числе и защищенный режим Internet Explorer (Protected Mode), а также контроль учетных записей пользователей, о котором сказано уже немало, фактически основываются

на механизме обязательного контроля целостности. Поэтому рассмотрим этот механизм.

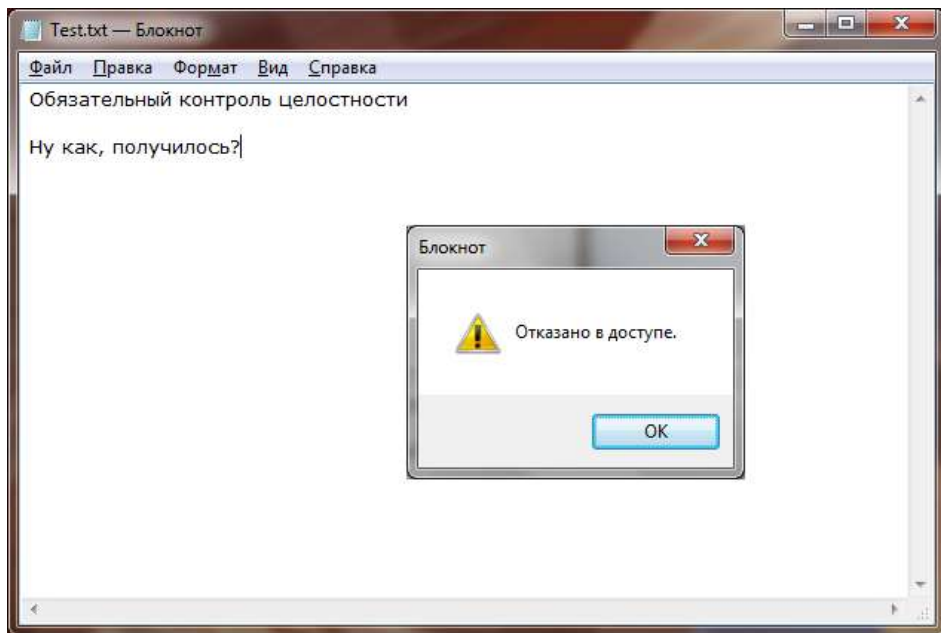


Рис. 9.36. Обязательный контроль целостности в действии

Когда пользователь входит в систему, Windows Vista/7 присваивает ему *идентификатор целостности* (integrity SID). Этот SID содержит метку целостности, которая определяет уровень доступа маркера пользователя (token), и, следовательно, указывает уровень полномочий, которых этот пользователь может достигнуть. Integrity SID имеет следующий формат: S-1-16-*<label>*, где *<label>* представляет уровень целостности. Во время проверки прав доступа Windows Vista/7 проверяет уровень целостности, присвоенный пользователю, и если он доминирует (то есть это число больше уровня целостности объекта или равно ему), пользователю разрешается модифицировать или удалять объект, в противном случае попытка доступа будет отклонена (как мы и видели в только что рассмотренном демонстрационном примере).

В Windows Vista/7 определено четыре уровня целостности: низкий (low), средний (medium), высокий (high) и системный (system). Обычные пользователи имеют средний уровень, при повышении уровня полномочий они получают высокий. Объекты, защищенные механизмом WRP, имеют такие ACL,

что доступ к ним имеет только сервис **TrustedInstaller**, а все остальные учетные записи, включая **SYSTEM**, имеют право только на чтение и исполнение. Краткая сводка уровней целостности приведена в табл. 9.5.

Таблица 9.5. Краткая сводка уровней целостности и их описание

Уровень целостности (Integrity Access Level)	Системные привилегии
Высокий (High)	Административные — можно устанавливать файлы в папку Program Files и вести запись в защищенные ключи реестра, например, в <code>HKEY_LOCAL_MACHINE</code>
Средний (Medium)	Пользовательские — можно создавать и модифицировать файлы в собственных папках и вести запись в ключи реестра в составе дерева <code>HKEY_CURRENT_USER</code>
Низкий (Low)	Недоверенные (Untrusted) — с таким уровнем привилегий можно вести запись только в папки наподобие <code>Temporary Internet Files\Low</code> и ключи реестра наподобие <code>HKEY_CURRENT_USER\Software\LowRegistry</code>

Как уже говорилось, на этом механизме основан и защищенный режим Internet Explorer (Internet Explorer Protected Mode, IEPM). Процесс IEPM и его расширения работают на низком уровне контроля целостности и потому имеют доступ только к папкам `Temporary Internet Files\Low`, `History`, `Cookies`, `Favorites`, а также к ключу `HKEY_CURRENT_USER\Software\LowRegistry` key. Поскольку эти ограничения могут мешать работе некоторых приложений, в режиме совместимости происходит виртуализация реестра, при которой доступ к ресурсам со средним (medium) уровнем контроля целостности перенаправляется в папки и ключи реестра с низким уровнем контроля целостности, `%userprofile%\LocalSettings\TemporaryInternet Files\Virtualized` и `HKEY_CURRENT_USER\Software\Microsoft\InternetExplorer\InternetRegistry`.

Защита реестра от несанкционированного удаленного доступа

Опция доступа к реестру удаленного компьютера представляет собой очень удобный метод, позволяющий администратору эффективно выполнять свои задачи по поддержке пользователей непосредственно с собственного рабочего места. Однако в ряде случаев эта возможность может быть источником проблем, поскольку удаленный доступ к реестру локального компьютера должен быть санкционированным.

Когда пользователь пытается установить соединение с реестром удаленного компьютера, действующий на этом компьютере сервис Server в первую очередь выполняет проверку существования ключа `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg` (рис. 9.37). Возможность получения удаленным пользователем доступа к реестру защищаемого компьютера определяется следующими факторами:

- ❑ если ключ `\winreg` не существует, то доступ к реестру сможет получить любой удаленный пользователь. Этот пользователь способен выполнять над реестром манипуляции в пределах, допускаемых списком контроля доступа (ACL);
- ❑ если ключ `\winreg` существует в реестре, то список контроля доступа, установленный для этого подключа, и будет определять, какие пользователи могут получать доступ к реестру с удаленного компьютера.

Если список контроля доступа (ACL) ключа `winreg` предоставляет удаленному пользователю доступ с правом чтения или записи (явно или как члену одной из групп), этот пользователь может подключиться к реестру. После установления такого соединения действия пользователя, манипулирующего реестром, будут ограничены только правами доступа к отдельным его ключам. Таким образом, даже если пользователь имеет только право на чтение ключа `winreg`, он сможет модифицировать другие ключи реестра, если их ACL это позволяют.

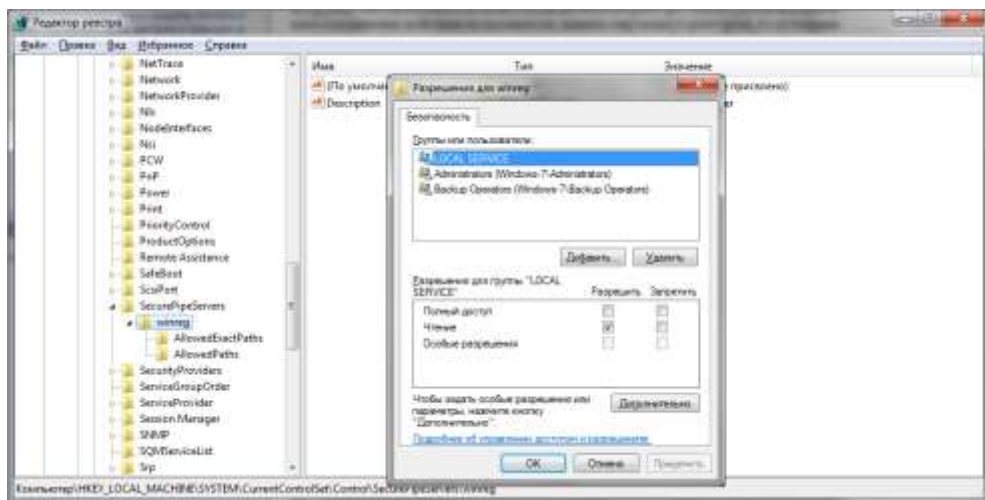


Рис. 9.37. Конфигурирование списка контроля доступа для `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg`

Защита ульев SAM и Security

Информация безопасности Windows Vista/7, как и в случае Windows NT/2000/XP, хранится в ульях реестра SAM (Security Accounts Manager) и Security. Улей SAM содержит пользовательские пароли в виде таблицы хэш-кодов, а улей Security — информацию о безопасности локального компьютера, в том числе права пользователей, политику в отношении паролей, членство пользователей в локальных группах.

ПРИМЕЧАНИЕ

Существует целый набор утилит, с помощью которых можно осуществить взлом улья SAM. Хорошую подборку таких утилит можно найти здесь: <http://www.openwall.com/passwords/microsoft-windows-nt-2000-xp-2003>.

Как защитить улей SAM

Microsoft официально утверждает, что лучший способ защиты Windows NT/2000/XP/Vista/7 — это защита административных паролей, но этого явно недостаточно. Доступ к ульям SAM и Security получают многие пользователи: например, пользователи из группы **Операторы архива** (Backup Operators), в обязанности которых входит резервное копирование реестра. А имея копии ульев SAM и Security, извлечь из них все пароли системы сможет даже не очень квалифицированный взломщик, что и будет показано далее.

По умолчанию ни один пользователь (даже администратор) не имеет необходимых прав доступа, которые позволили бы ему получить доступ или хотя бы просмотреть базу данных SAM Windows NT/2000/XP/Vista/7 с помощью редактора реестра. Но, тем не менее, ульи SAM и Security хранятся на диске точно так же, как и другие файлы, и единственное, что требуется для взлома — это раздобыть копии этих ульев. Обычным копированием этого не сделать — при попытке копирования реестра работающей системы из семейства Windows NT вы получите сообщение об ошибке (рис. 9.38).

Однако в составе программных продуктов имеются утилиты (Regback в Windows NT 4.0 Resource Kit, REG — в Windows 2000 Resource Kit, Reg и Regini — в составе Windows Vista/7), при помощи которых пользователи, принадлежащие к группам администраторов или операторов резервного копирования, могут получать копии реестра работающей системы.

Пользователь, желающий незаконно скопировать ульи SAM и Security, может воспользоваться утилитой NTFSDOS (<http://www.sysinternals.com/ntfs30.htm>), которая позволяет монтировать тома NTFS в DOS. Эта утилита и другие ее модификации (имеется также утилита NTFS for Windows 98) вызывают у многих

противоречивую реакцию (именно из-за потенциального риска для системы безопасности). После появления первых версий NTFSDOS корпорация Microsoft официально заявила, что истинная безопасность — это физическая безопасность. Тем не менее, эта утилита весьма полезна и может оказаться просто незаменимой при выполнении процедур аварийного восстановления (особенно если надо сделать такую работу быстро).

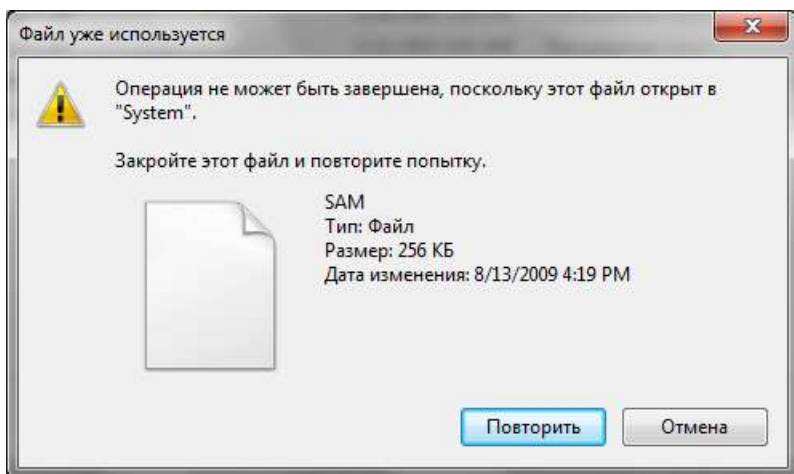


Рис. 9.38. Попытка копирования файлов реестра работающей системы из семейства Windows NT, включая Windows Vista и Windows 7, приводит к появлению сообщения об ошибке

Таким образом, для обеспечения должной защиты файлов SAM и Security от незаконного копирования и для предотвращения доступа рядовых пользователей домена к этим файлам необходимо установить защищаемые компьютеры в охраняемом помещении, а также лишить пользователей права на перезагрузку компьютера.

Подводя итоги, скажем, что следует:

- ☐ лишить конечных пользователей права локальной регистрации на серверах;
- ☐ в операционных системах, более ранних, чем Windows Vista/7, использовать файловую систему NTFS;

ПРИМЕЧАНИЕ

Как уже говорилось, Windows Vista/7 устанавливается только на томах NTFS, так что в данном случае этот совет уже утратил актуальность;

- ☐ обеспечить надлежащую физическую защиту для серверов;

- ❑ в системах, которые устанавливались как обновление предыдущих версий, следует ужесточить права доступа, особенно к %SystemRoot%\Repair;
- ❑ обеспечить безопасные условия хранения резервных копий системы в целом и реестра в частности.

Для взлома похищенных ульев SAM и Security больших усилий не требуется. Имея эти файлы в своем распоряжении, пользователь может в свободное время провести на них такое количество словарных атак, какое требуется для взлома паролей. Если в его распоряжении имеется утилита для взлома паролей (например, LCP — бесплатная альтернатива знаменитой утилите L0phtCrack, которая работает и в Windows 7), то успех проведенной атаки зависит, в основном, от качества используемого для взлома словаря — чем большее количество слов, дат, чисел, словосочетаний, используемых чаще всего в качестве пароля, содержится в этом файле, тем выше шансы успешного взлома (рис. 9.39). Скачать утилиту LCP можно по адресу <http://www.lcpsoft.com/english/download.htm>.

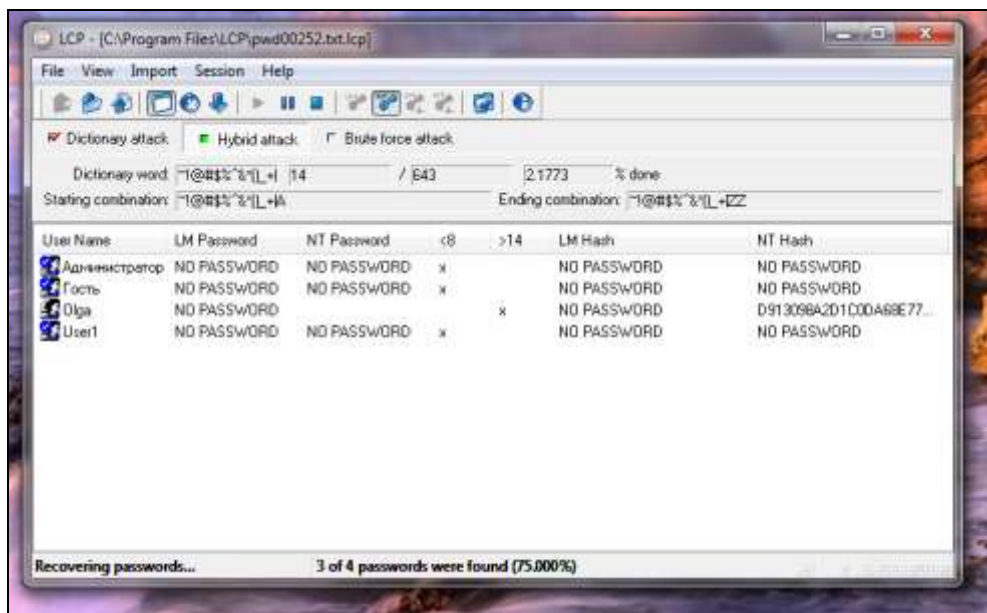


Рис. 9.39. Слабые пароли бесплатная утилита LCP вскрывает в течение нескольких минут

Таким образом, чтобы защитить систему, следует запретить пользователям использовать пустые пароли и задать системную политику в отношении паролей. Минимальная длина паролей в любом случае не должна быть меньше

8 символов. Помимо этого, в качестве пароля рекомендуется использовать произвольные комбинации букв и цифр, а также задать политику в отношении минимально допустимой сложности паролей.

СОВЕТ

Попробуйте представить себя на месте злоумышленника и взломайте свой собственный улей SAM (при этом учтите, что ваши задачи существенно проще, чем задачи, стоящие перед этим человеком — вам ведь не надо проводить удаленную атаку с целью похищения ульев SAM и Security). С пользователями, пароли которых будут вскрыты автоматически, следует провести разъяснительную работу. Помимо этого, рекомендуется установить правила периодической смены паролей.

Заключение

Завершая эту главу, считаю своим долгом сказать, что я вовсе не ставила перед собой задачу дать детальное и подробное рассмотрение модели безопасности Windows Vista/7. В рамках одной главы это невозможно чисто физически. Нерассмотренными остались многие вопросы, в том числе и такие важные, как обход цифровой подписи при загрузке драйверов, анализ существующих уязвимостей Windows Vist7 и тому подобное. Дополнительные источники информации, касающейся данного вопроса, можно найти в списке литературы в конце книги.

Глава 10



Реестр и пользовательские профили

Системы имеют тенденцию расти и, по мере роста, взаиморастворяться.

Обобщенный принцип неопределенности

Рабочая среда пользователя включает в свой состав элементы рабочего стола и параметры его настройки, в том числе и такие, как цветовая схема, параметры настройки мыши, размеры и расположение окон, сетевые соединения и соединения с принтерами, переменные окружения, параметры реестра и доступные для запуска приложения. Для управления рабочими средами пользователей в сетях Windows NT/2000/XP/Vista/7 традиционно применяются следующие возможности:

- ❑ *пользовательские профили* — содержат все параметры рабочей среды Windows, зависящие от конкретных пользователей, в том числе параметры настройки экрана и сетевые соединения;
- ❑ *регистрационные сценарии* (logon scripts) — командные (BAT) или исполняемые (EXE) файлы, которые запускаются каждый раз, когда пользователь регистрируется в сети с любой из рабочих станций. Регистрационный сценарий может содержать команды операционной системы — например, выполняющие установление сетевых соединений или осуществляющие запуск приложений. Регистрационные сценарии могут устанавливать *переменные окружения* (environment variables), например, пути (переменная PATH), указывать каталог для временных файлов (переменная TEMP) и т. д.;
- ❑ *системная политика* — применяется для управления настройками рабочих столов пользователей, а также для определения их прав в сети. Системные администраторы могут использовать системную политику для управления рабочими станциями в локальных и глобальных сетях.

В этой главе рассматриваются пользовательские профили и системная политика, а также даются указания по их использованию, например, для внесения

изменений в реестр. Помимо прочего, проблемы с загрузкой пользовательских профилей способны блокировать работу в системе и изрядно попортить вам кровь. Поэтому здесь пользовательские профили будут рассмотрены подробно. Кроме того, как и повсюду в этой книге, будет рассказано, как избежать проблем с их загрузкой.

Базовая информация о пользовательских профилях

Каждый пользователь современных операционных систем из семейства Windows NT/2000/XP/Vista/7 имеет в своем распоряжении множество настраиваемых параметров. В качестве примеров можно указать файлы *фоновых рисунков* (wallpaper), *экранных заставок* (screen savers), *настройки рабочего стола* (desktop) и параметры установленных в системе приложений. Перечисленные параметры представляют собой лишь незначительную часть настроек, которые пользователи могут устанавливать самостоятельно. Причины, по которым может потребоваться индивидуальная настройка, ничуть не меньше, чем пользователей, и все они отличаются друг от друга настолько же, насколько различны вкусы и предпочтения разных людей.

До введения концепции реестра основной проблемой с индивидуальной пользовательской настройкой всегда было то, что каждый раз, когда пользователь пересаживался за другой компьютер, ему приходилось выполнять ее заново.

На компьютерах, работающих под управлением операционных систем из семейства Windows NT/2000/XP/Vista/7, пользовательские профили (user profiles) создаются автоматически всякий раз, когда пользователь впервые регистрируется в системе. По умолчанию они поддерживают параметры настройки рабочего стола для пользовательской среды на локальном компьютере.

ПРИМЕЧАНИЕ

Необходимо отличать пользовательские профили (user profiles) от политик (policies). Профили не являются пользовательскими политиками, и у каждого пользователя есть профиль, даже если он не использует групповую политику (Group Policy).

Параметры, хранящиеся в пользовательском профиле

Пользовательский профиль содержит конфигурационные параметры и опции, индивидуально настроенные для каждого пользователя. Фактически пользовательский профиль представляет собой "моментальный снимок" рабочей среды пользователя.

Некоторые наиболее важные параметры, хранящиеся в пользовательском профиле, перечислены в табл. 10.1.

Таблица 10.1. Параметры, хранящиеся в пользовательском профиле

Элемент рабочей среды	Параметры, сохраняемые в пользовательском профиле
Графическая оболочка Windows (приложение Проводник (Explorer))	Все установленные пользователем параметры приложения Проводник (Explorer)
Панель задач и меню Пуск (Start)	Все личные программные группы и их свойства, все программные элементы и их свойства, все параметры настройки панели задач
Параметры настройки принтеров	Все соединения с сетевыми принтерами
Панель управления (Control Panel)	Все пользовательские настройки, выполненные в Панели управления (Control Panel)
Стандартные приложения (Accessories)	Все индивидуальные параметры настройки пользовательских приложений, влияющие на настройку пользовательской среды Windows. Сюда входят параметры настройки приложений Калькулятор (Calculator), Блокнот (Notepad), встроенного графического редактора Paint и др.
Параметры настройки приложений	Приложения могут отслеживать параметры своей настройки применительно к каждому конкретному пользователю. Если такая информация существует, она хранится в пользовательском улье реестра (HKEY_CURRENT_USER)
Закладки справочной системы (help bookmarks)	Все закладки, помещенные пользователем в справочную систему
Избранные ключи реестра	Все ключи реестра, отмеченные пользователем как избранные (Favorites)

Структура пользовательского профиля

Каждый пользовательский профиль состоит из улья реестра (файл NTUser.dat, который отображается на ключ реестра HKEY_CLASSES_ROOT при регистрации пользователя) и набора папок в файловой системе компьютера.

Рассмотрим более подробно местоположение пользовательских профилей, заданное по умолчанию, а также изменения, которые оно претерпевало с выходом каждой новой версии операционных систем из семейства

Windows NT/2000/XP/Vista/7. Эта информация особенно важна для администраторов, поскольку в сетях, к которым подключены компьютеры под управлением Windows 7, наверняка будут работать и компьютеры под управлением не только Windows Vista, но и более ранних версий Windows. При этом необходимости обеспечения обратной совместимости при централизованном управлении сетью еще никто не отменял.

ПРИМЕЧАНИЕ

Здесь и далее в этой главе для обозначения пути к папке, содержащей пользовательские профили, будет использоваться запись вида *%ProfilePath%*.

Хранение пользовательских профилей

Итак, все пользовательские профили Windows NT хранятся в папке *%SystemRoot%\Profiles*. Каждый новый пользовательский профиль создается в момент первой регистрации пользователя в системе на базе профиля Default User — стандартного пользовательского профиля. Папка \Default User и папки профилей всех пользователей содержат файлы Ntuser.dat и Ntuser.dat.log, а также каталоги ссылок на элементы рабочего стола.

В Windows 2000/XP местоположение пользовательских профилей претерпело изменения. Пользовательские профили стали храниться в папке *%SystemDrive%\Documents and Settings*, в составе которой имелись вложенные папки с именами, соответствующими входному имени каждого пользователя (учетной записи).

Причем в Windows XP расположение профилей зависит от способа, каким была установлена эта операционная система. Для начала рассмотрим местоположение пользовательских профилей для каждого типа инсталляции Windows XP (табл. 10.2), а затем перейдем к обсуждению изменений, внесенных в пользовательские профили в Windows Vista и Windows 7.

Таблица 10.2. Местоположение пользовательских профилей в Windows XP

Тип инсталляции Windows XP	Местоположение пользовательского профиля
"Чистая" инсталляция Windows XP (нет ранее установленных операционных систем)	<i>%SystemDrive%\Documents and Settings</i> ; например, C:\Documents and Settings
Обновление системы с Windows 2000	<i>%SystemDrive%\Documents and Settings</i> ; например, C:\Documents and Settings
Обновление системы с Windows NT 4.0	<i>%SystemRoot%\Profiles</i> ; например, C:\WinNT\Profiles
Обновление системы с Windows 9x/ME	<i>%SystemDrive%\Documents and Settings</i> ; например, C:\Documents and Settings

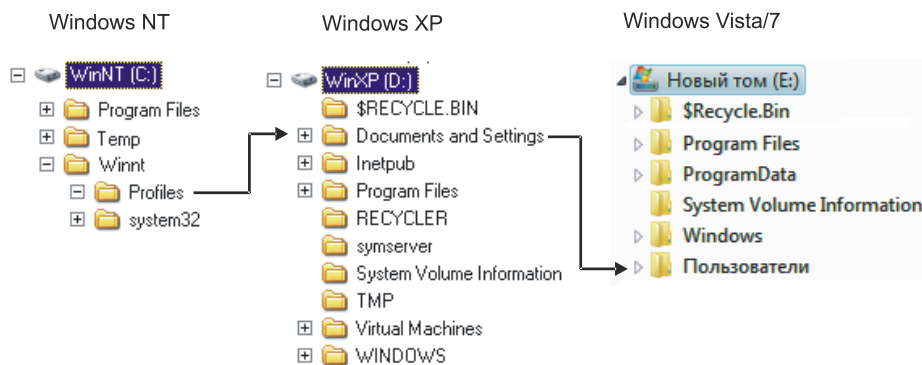


Рис. 10.1. Изменения в расположении папок пользовательских профилей от Windows NT до Windows Vista/7

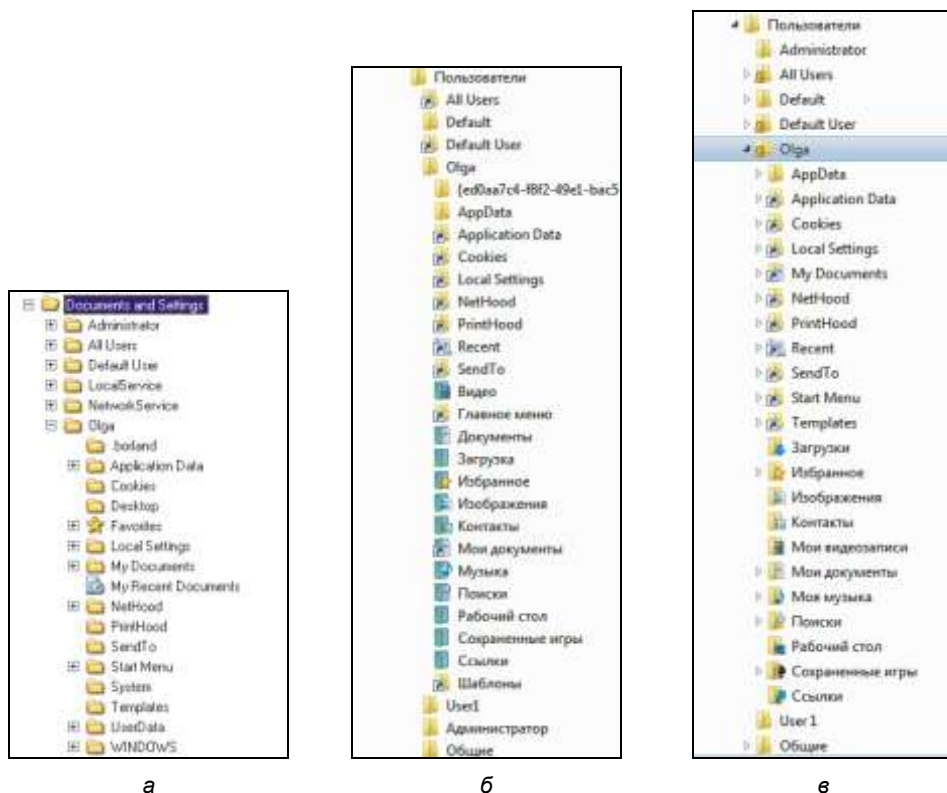


Рис. 10.2. Изменения в структуре пользовательских профилей в Windows Vista/7 по сравнению с Windows XP: а — структура пользовательского профиля в Windows XP; б — структура пользовательского профиля в Windows Vista, в — структура пользовательского профиля в Windows 7

В Windows Vista способ хранения пользовательских данных претерпел фундаментальные изменения. Папке Documents and Settings, хранившей пользовательские профили в стиле Windows XP, пришла на смену папка Users (Пользователи), которая хранится в корневом каталоге системного раздела. Эволюция размещения папок пользовательских профилей показана на рис. 10.1. Более того, на самом деле это даже не эволюция, а настоящая революция, поскольку структура пользовательских профилей тоже претерпела такие изменения, что профили в стиле Windows XP и Windows Vista/7 перестали быть совместимыми (рис. 10.2). С другой стороны, пользовательские профили в Windows Vista и Windows 7 очень похожи, несмотря на то, что различия имеются и между ними.

Конечным пользователям важна их персональная информация и личные настройки, поэтому об их переносе следует задумываться заранее. Это особенно важно в сетях предприятий, поскольку индивидуальная настройка рабочих сред пользователей после миграции отнимает много времени.

В Windows Vista/7, как и в Windows NT/2000/XP, пользовательский профиль создается автоматически, когда пользователь впервые регистрируется в системе. Для хранения этого профиля система создает вложенную папку в составе папки *%ProfilePath%* с именем, совпадающим с входным именем этого пользователя. Путь к этой папке будет записан в реестре и ассоциирован с *идентификатором безопасности* (Security ID, SID) этого пользователя.

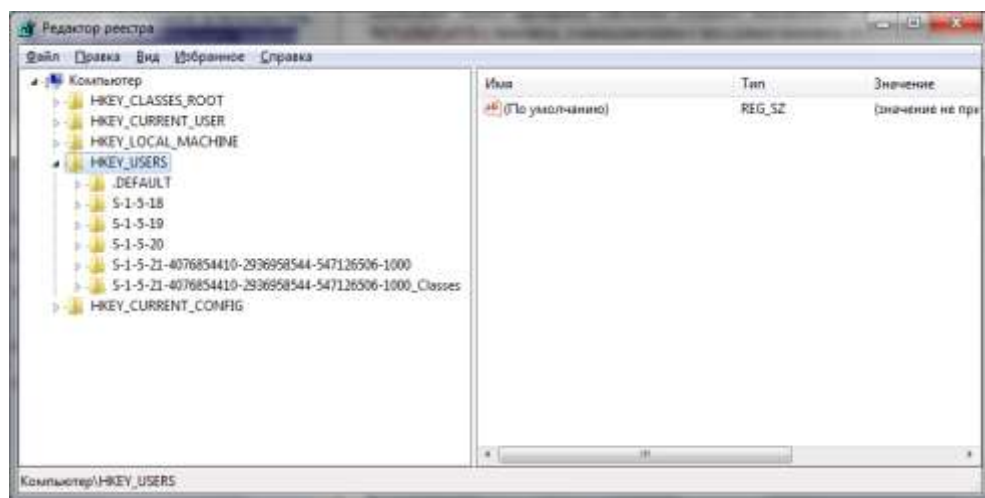


Рис. 10.3. Ключ реестра *HKEY_USERS* содержит список всех загруженных на данный момент (активных в памяти) пользовательских профилей, каждый из которых идентифицируется при помощи SID

ПРИМЕЧАНИЕ

Идентификаторы безопасности в Windows Vista/7 имеют довольно большую длину и уникальны для каждого пользователя даже на разных компьютерах. Причем в том случае, если учетную запись пользователя на компьютере или в домене сначала удалить, а затем вновь создать новую учетную запись с тем же именем, идентификатор безопасности, с которым она ассоциирована, будет другим. Среди пользователей Windows NT/2000/XP/Vista/7 очень широко распространено ошибочное мнение, что в системе пользователя идентифицируют регистрационные данные, т. е. входное имя (username или login name) и пароль (password). Это не так — каждый пользователь определяется в системе идентификатором безопасности (SID). Именно SID идентифицируют пользовательские профили (рис. 10.3).

Итак, когда пользователь регистрируется на локальном компьютере с использованием локальной учетной записи или учетной записи пользователя домена, если папка `%ProfilePath%` еще не содержит вложенной папки с именем, совпадающим с входным именем этого пользователя, такая папка будет создана, и путь к этой папке будет зарегистрирован в реестре и ассоциирован с SID этого пользователя. Например, если на компьютере Windows Vista или Windows 7 регистрируется пользователь Olga, то для хранения профиля этого пользователя будет создана папка с именем `%SystemDrive%\Users\Olga` (рис. 10.4 и 10.5).

Сравните иллюстрации, приведенные на рис. 10.4 и 10.5. Вы без труда заметите небольшие отличия в именовании папок пользовательского профиля:

- ❑ В Windows Vista: **Документы** (Documents), **Видео** (Videos) и **Музыка** (Music);
- ❑ В Windows 7: **Мои документы** (My Documents), **Мои видеозаписи** (My Videos) и **Моя музыка** (My Music).

ПРИМЕЧАНИЕ

Кстати, эти отличия заметны лишь на уровне графического пользовательского интерфейса. Если вы попытаете просматривать структуру пользовательских профилей через командную строку, то заметите два интересных момента: прежде всего вы обнаружите, что названия вложенных папок пользовательского профиля *не локализованы* (скорее всего — во избежание проблем с совместимостью различных локализованных версий). Кроме того, увидите, что все основные вложенные папки с пользовательскими данными в обеих системах называются одинаково (рис. 10.6).

Если впоследствии на этом компьютере регистрируется другой пользователь с таким же входным именем, но из другого домена, то будет создана еще одна папка пользовательского профиля, дополненная именем домена, в котором находится учетная запись зарегистрировавшегося в системе пользователя, например: `%SystemDrive%\Users\Olga [DOMAIN_NAME]`, где `[DOMAIN_NAME]` — имя домена, которому принадлежит учетная запись.

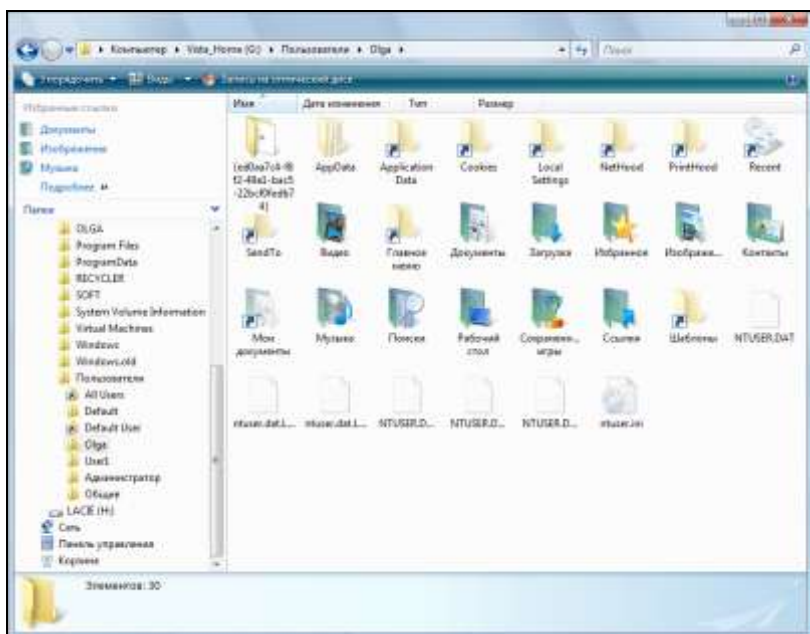


Рис. 10.4. Содержимое папки пользовательского профиля (Windows Vista)

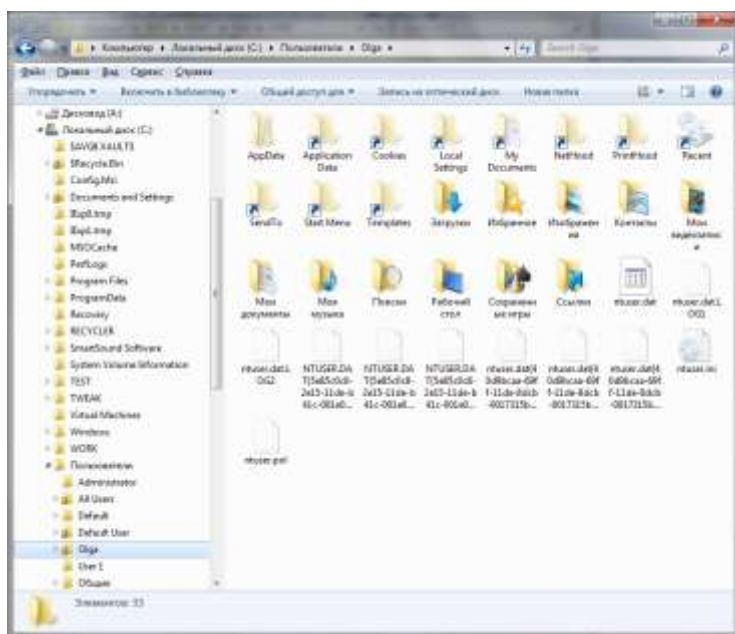


Рис. 10.5. Содержимое папки пользовательского профиля (Windows 7)

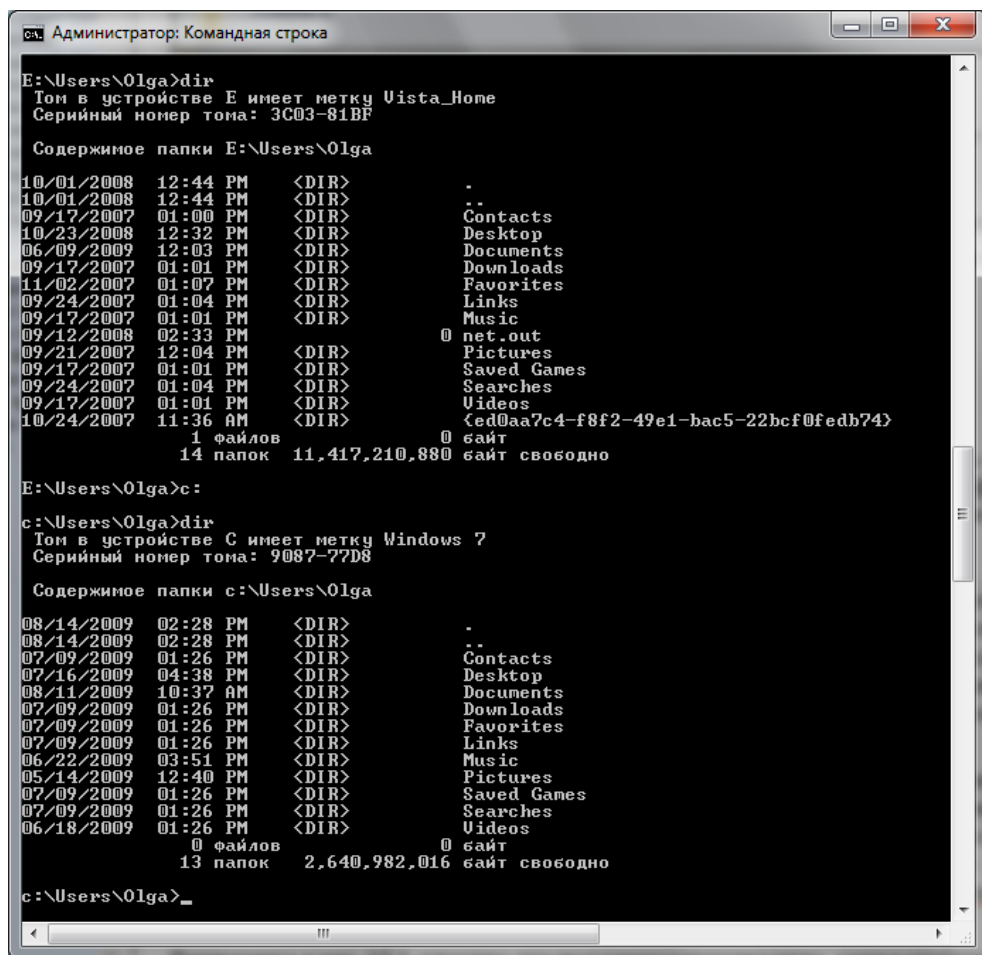


Рис. 10.6. Сравнение структур пользовательского профиля в Windows Vista и Windows 7

В том случае, если совпадают как пользовательское имя, так и имя домена, но при этом SID обоих учетных записей различаются (это как раз та ситуация, когда учетная запись пользователя была удалена, а затем повторно создана с тем же самым пользовательским именем), будут созданы новые папки пользовательских профилей следующего вида: %SystemDrive%\Users\Olga [DOMAIN_NAME].000, %SystemDrive%\Users\Olga [DOMAIN_NAME].001 и т. д.

Вернувшись к рис. 10.3, отметим, что под ключом реестра `HKEY_USERS` отображен не один пользовательский профиль, а несколько. Довольно часто люди думают, что эта часть реестра отображает все локальные профили (local profile) на данном компьютере. Так вот, это вовсе не так. Под ключом `HKEY_USERS`

представлен список только тех профилей, которые *на данный момент загружены в память*. Каждый раз, когда в системе регистрируется новый пользователь, под ключом `HKEY_USERS` появляется вложенный ключ с именем, совпадающим с `SID` соответствующей учетной записи (рис. 10.7). Когда пользователь выходит из системы, соответствующий улей выгружается из памяти.

Рассмотрим основные ульи пользовательских профилей, которые обычно загружены в память:

- ❑ `.DEFAULT` — профиль пользователя по умолчанию. Он представляет собой стандартный профиль, загружаемый даже тогда, когда еще ни один пользователь не зарегистрировался в системе. Именно поэтому он иногда называется еще *загрузочным профилем* (startup profile). Изменяя настройки в этом профиле, вы производите изменения, которые будут автоматически вноситься во все вновь создаваемые пользовательские профили;
- ❑ `S-1-5-18` — `SID` учетной записи **SYSTEM**;
- ❑ `S-1-5-19` — `SID` учетной записи **LocalService**;
- ❑ `S-1-5-20` — `SID` учетной записи **NetworkService**;
- ❑ `SID`, начинающийся на `S-1-5-21-` и оканчивающийся на `-500`, принадлежит встроенной учетной записи **Администратор** (Administrator), которая, как вы помните, в Windows Vista и в Windows 7 по умолчанию заблокирована.

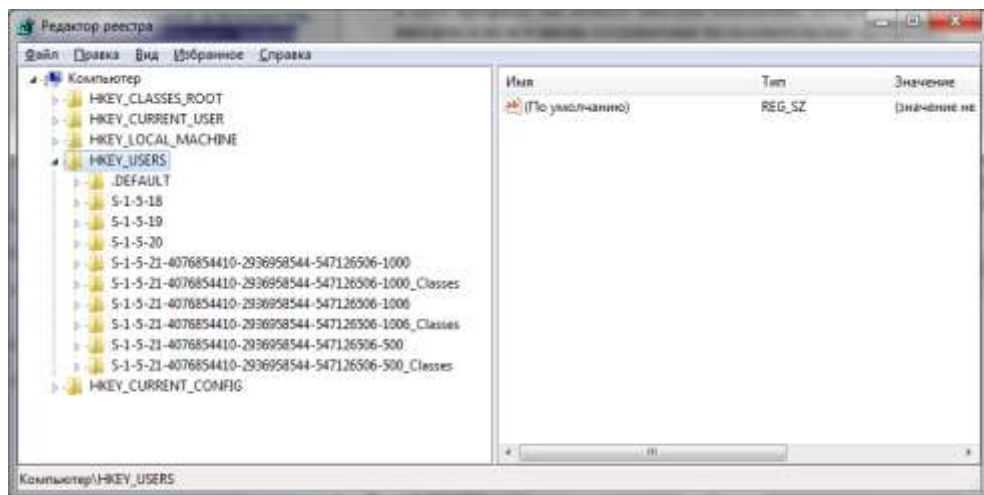


Рис. 10.7. Как только в системе регистрируется новый пользователь, под ключом реестра появляется новый вложенный ключ с именем, совпадающим с `SID` этого пользователя (сравните с рис. 10.3)

Все остальные записи под ключом реестра `HKEY_USERS` соответствуют прочим пользователям и служебным учетным записям, в настоящий момент зарегистрированным в системе.

Отличия структуры пользовательских профилей в Windows Vista/7 и Windows XP

Теперь рассмотрим параметры, хранящиеся в каталогах профиля, более подробно. Типичное содержимое папки пользовательского профиля было показано на рис. 10.2, 10.4 и 10.5. Настал момент более подробно обсудить структуру пользовательских профилей Windows Vista и Windows 7 и их отличия как друг от друга, так и от структуры пользовательского профиля Windows XP.

Сравнительный анализ структуры пользовательских профилей в Windows Vista и Windows XP приведен в табл. 10.3.

Таблица 10.3. Сравнение структур пользовательских профилей в Windows Vista и XP

Папка в составе пользовательского профиля Windows Vista/7	Описание	Аналог в Windows XP
AppData	По умолчанию применяется для хранения данных, относящихся к настройкам приложений (скрытая папка)	Не применимо
Application Data*	Данные, относящиеся к конкретному приложению, например собственный словарь для обработки текстов. Какие именно данные должны храниться в этом каталоге, определяют разработчики приложений	Documents and Settings\ %username%\Application Data
Cookies*	Cookie-файлы Internet Explorer	Documents and Settings\ %username%\Cookies
Local Settings*	Установки приложения, которые не перемещаются вместе с профилем, поскольку они, как правило, относятся к конкретной машине либо слишком велики	Documents and Settings\ %username%\Local Settings
NetHood*	Ярлыки на элементы сетевого окружения	Documents and Settings\ %username%\NetHood

Таблица 10.3 (окончание)

Папка в составе пользовательского профиля Windows Vista/7	Описание	Аналог в Windows XP
PrintHood*	Ярлыки, содержащиеся в папке принтера	Documents and Settings\ %username%\PrintHood
Recent*	Ярлыки на самые последние открываемые документы	Documents and Settings\ %username%\My Recent Documents
Main Menu*	Ярлыки, указываемые на программы	Documents and Settings\ %username%\Main Menu
SendTo*	Ярлыки, указывающие место сохранения копий документов и приложений	Documents and Settings\ %username%\SendTo
Templates*	Ярлыки, указывающие на шаблоны	Documents and Settings\ %username%\Templates
Contacts	Хранит информацию о контактах пользователя	Не применимо
Desktop	Элементы рабочего стола, включая файлы и ярлыки	Documents and Settings\ %username%\Desktop
Documents	Хранит все документы, созданные пользователем	Documents and Settings\ %username%\My Documents
Downloads	Предназначена для сохранения информации, загружаемой из Интернета	Не применимо
Favorites	Содержимое папки Favorites в Internet Explorer	Documents and Settings\ %username%\Favorites
Music	Предназначена для хранения музыкальных файлов пользователя	Documents and Settings\ %username%\My Music
Videos	Предназначена для хранения видеофайлов пользователя	Documents and Settings\ %username%\My Videos
Pictures	Предназначена для хранения графических файлов пользователя	Documents and Settings\ %username%\My Pictures
Searches	Предназначена для сохранения результатов поиска	Не применимо
Links	Предназначена для хранения ссылок на избранное содержимое (Windows Explorer Favorite Links)	Не применимо
Saved Games	Сохраненные игры	Не применимо

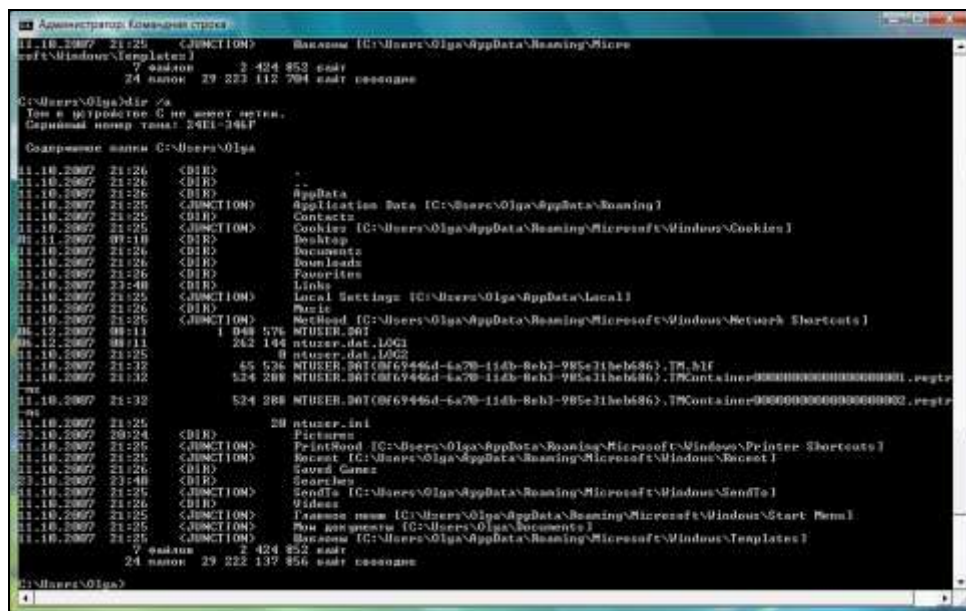


Рис. 10.8. Windows Vista использует точки разветвления NTFS для обеспечения обратной совместимости с предшествующими версиями операционных систем из семейства Windows 2000/XP

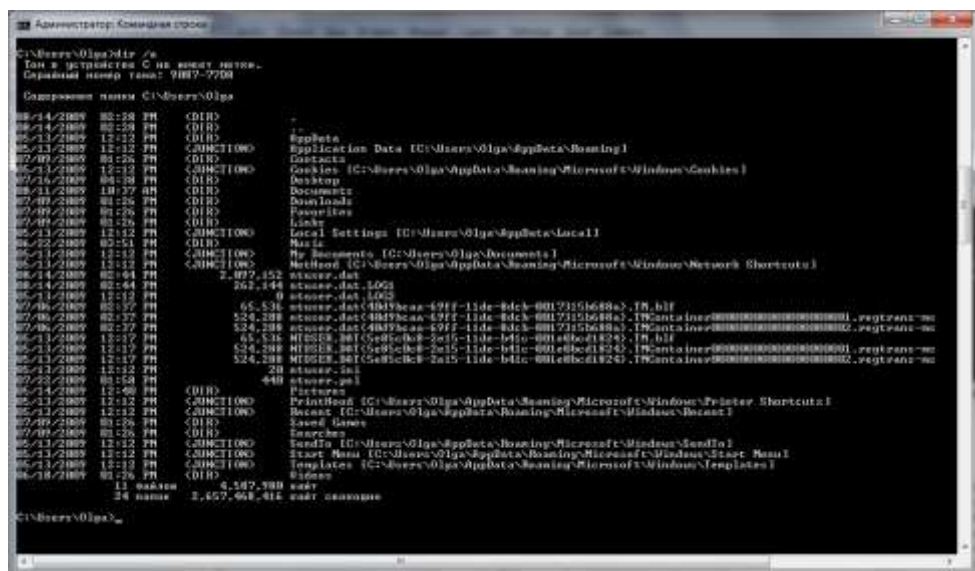


Рис. 10.9. Структура каталога пользовательского профиля Windows 7 содержит все те же самые точки разветвления, что и в Windows Vista

Звездочкой отмечены скрытые папки, представляющие собой *точки разветвления* NTFS (junction points), ссылающиеся на соответствующие вложенные папки пользовательских профилей, существовавших в Windows XP (рис. 10.8 и 10.9). Чтобы просмотреть структуру пользовательского профиля в таком виде, вам необходимо дать команду `dir /a`, которая выводит полный список всех файлов и папок, в том числе, и скрытых. Обратите внимание, что на рис. 10.8 и 10.9 точки разветвления NTFS помечены как **<JUNCTION>** (в отличие от обычных папок, помеченных как **<DIR>**).

Фактически, точки разветвления представляют собой функциональную возможность, предоставляемую файловой системой NTFS, которая с момента своей разработки прошла длительный путь эволюции. В настоящее время существуют пять версий NTFS:

- ❑ NTFS v1.0 — выпущена вместе с Windows NT 3.1;
- ❑ NTFS v1.1 — выпущена вместе с Windows NT 3.5;
- ❑ NTFS v1.2 — выпущена с Windows NT 3.51 и Windows NT 4.0 (иногда называется NTFS 4.0 — по версии операционной системы);
- ❑ NTFS v3.0 — выпущена с Windows 2000 (иногда называется NTFS V5.0 — по внутреннему номеру версии операционной системы);
- ❑ NTFS v3.1 — используется в Windows XP (иногда называется NTFS V5.1), Windows Server 2003 (иногда называется NTFS V5.2), Windows Vista (NTFS V6.0), Windows Server 2008 и Windows 7.

ПРИМЕЧАНИЕ

В Windows Vista появились такие новые функции, как NTFS на основе транзакций (Transactional NTFS, TxF), классические символические ссылки в стиле UNIX (symbolic links) и ряд функций по обеспечению повышенной надежности. Естественно, что они присутствуют и в Windows 7. Однако эти новые возможности в большей степени опираются на функциональность самой операционной системы, нежели на файловую систему NTFS. Таким образом, основной номер версии NTFS пока не изменился.

Всего в Windows Vista/7 поддерживаются четыре вида ссылок: ярлыки (shortcuts), жесткие ссылки (hard links), точки разветвления (junction points) и символические ссылки (новая возможность, доступная только еще в Windows Vista и Windows Server 2008):

- ❑ *ярлыки* — это хорошо вам известные файлы с расширением `lnk`. Если в оболочке Windows выполнить двойной щелчок мышью по файлу с таким расширением, то Windows откроет этот файл;

ПРИМЕЧАНИЕ

Во многих книгах по реестру очень часто можно встретить совет "как убрать стрелки с ярлыков". Лично я, в свете сказанного, считаю, что этот совет утратил

свою актуальность. "Стрелки" — это довольно удобно, потому что они сразу же позволяют понять, с каким видом ссылки вы имеете дело. Может, кого-то они и "бесят", поэтому вполне можете совету последовать, он вообще-то безобиден (но и бесполезен). Но вот меня эти стрелки теперь ни капельки не раздражают.

- ❑ *жесткие ссылки* — это новые записи в дереве каталогов для уже существующих файлов. За счет этого один и тот же файл может отображаться в нескольких папках (или в одной папке под разными именами). При этом все жесткие ссылки должны находиться на одном томе;
- ❑ *точки разветвления* — представляют собой указатели, ссылающиеся на папку с помощью абсолютного пути, а Windows автоматически перенаправляет запросы точки разветвления на целевую папку. Точки разветвления не обязаны находиться на одном томе;
- ❑ *символические ссылки* — эта новая возможность, появившаяся в Windows Vista, отличается от жестких ссылок тем, что может ссылаться и на файлы, и на папки (жесткие ссылки могут ссылаться только на файлы). От точек разветвления они отличаются тем, что используют относительные пути вместо абсолютных.

Как видно из табл. 10.3, а также рис. 10.8 и 10.9, точки разветвления и символические ссылки активно используются для организации связей между папками пользовательских профилей Windows XP и Vista/7, например:

- ❑ C:\Documents & Settings → C:\Users (Junction);
- ❑ C:\Users\All Users → C:\ProgramData (Symbolic Link);
- ❑ C:\Users\Default Users → C:\Users\Default (Junction).

В составе каждой папки имеются дополнительные вложенные папки и точки разветвления.

Для создания ссылок и управления ими предусмотрена утилита командной строки `mklink`. Она использует следующий синтаксис:

```
mklink [[/D] | [/H] | [/J]] link target
```

Здесь:

- ❑ `/D` — создает символическую ссылку на каталог. Если эта опция командной строки пропущена, то по умолчанию будет создана символическая ссылка на файл;
- ❑ `/H` — создает жесткую ссылку вместо символической;
- ❑ `/J` — создает точку разветвления, ссылающуюся на каталог;
- ❑ `link` — указывает имя новой символической ссылки;
- ❑ `target` — указывает путь (относительный или абсолютный), по которому выполняет перенаправление новая ссылка.

Кроме того, в Windows Vista/7 изменилась структура папки Application Data. В составе пользовательского профиля появилась отдельная папка AppData, внутри которой имеются три вложенных папки: Roaming, Local и LocalLow:

- папки Local и LocalLow используются для хранения данных приложений, которые не должны перемещаться по мере того, как пользователь переходит с компьютера на компьютер. Обычно эти данные или относятся к конкретному компьютеру, или слишком велики по объему, чтобы их можно было перемещать. Папка AppData\Local в Windows Vista/7 аналогична папке Documents and Settings\%username%\Local Settings\Application Data в Windows XP;
- папка Roaming используется для хранения данных, специфичных для приложений, например, индивидуальных словарей. Эти данные должны перемещаться вместе с пользовательским профилем. Папка AppData\Roaming в Windows Vista/7 аналогична папке Documents and Settings\%username%\Application Data в Windows XP.

В табл. 10.4 приведена подробная сводка соответствий между папками пользовательских профилей Windows Vista/7 и Windows XP. Эта информация важна для администраторов, желающих организовать работу пользователей в смешанной среде Windows XP и Windows Vista/7, избежав при этом проблем с совместимостью.

Таблица 10.4. Соответствия между папками пользовательских профилей Windows Vista/7 и Windows XP

Пользовательский профиль Windows Vista/7	Пользовательский профиль Windows XP
...\AppData\Roaming	Application Data
Не применимо	Local Settings
...\AppData\Local	Local Settings\Application Data
...\AppData\Local\Microsoft\Windows\History	Local Settings\History
...\AppData\Local\Temp	Local Settings\Temp
...\AppData\Local\Microsoft\Windows\Temporary Internet Files	Local Settings\Temporary Internet Files
...\AppData\Roaming\Microsoft\Windows\Cookies	Cookies
...\AppData\Roaming\Microsoft\Windows\Network Shortcuts	Nethood
...\AppData\Roaming\Microsoft\Windows\Printer Shortcuts	PrintHood
...\AppData\Roaming\Microsoft\Windows\Recent	Recent

Таблица 10.4 (окончание)

Пользовательский профиль Windows Vista/7	Пользовательский профиль Windows XP
...\AppData\Roaming\Microsoft\Windows\Send To	SendTo
...\AppData\Roaming\Microsoft\Windows\Start Menu	Start Menu
...\AppData\Roaming\Microsoft\Windows\Templates	Templates
...\Contacts	Не применимо
...\Desktop	Desktop
...\Documents	My Documents
...\Downloads	Не применимо
...\Favorites	Favorites
...\Music	My Music
...\Videos	My Videos
...\Pictures	My Pictures
...\Searches	Не применимо
...\Links	Не применимо
...\Saved Games	Не применимо

Файл *Ntuser.dat*

Файл *Ntuser.dat* представляет собой часть реестра, поддерживающую пользовательский профиль, и является кэшированной копией поддерева локального реестра `HKKEY_CURRENT_USER`. В составе этого ключа, структура которого показана на рис. 10.3 и 10.7, хранятся параметры, определяющие рабочую среду для пользователя, в текущий момент зарегистрированного в системе.

Кроме файлов *Ntuser.dat* и *Ntuser.dat.log* в каталоге пользовательского профиля могут находиться файлы *ntuser.pol* и *ntuser.ini*, определяющие настройки групповой политики для этого пользователя. Остальные файлы, начинающиеся со строки *Ntuser.dat* и имеющие длинные имена (см. рис. 10.5, 10.8 и 10.9), создаются Диспетчером транзакций (Transaction Manager) и представляют собой журналы транзакций (надеюсь, из главы 1 вы помните, что, начиная с Windows Vista, файловая система и реестр организованы на базе транзакций?).

ПРИМЕЧАНИЕ

Как и в случае с Windows Vista, групповые политики доступны не во всех вариантах поставки Windows 7.

Папка *Общие* (Public)

В Windows XP в составе папки Documents and Settings имелась папка для профиля Все пользователи (All Users). Наличие этой папки предоставляло возможность добавлять в пользовательские профили общие данные, не редактируя каждый пользовательский профиль индивидуально. Когда пользователь регистрируется в системе, Windows XP объединяет содержимое папок Desktop и Start Menu в составе профиля All Users с содержимым профиля пользователя, входящего в систему. Например, если добавить в состав папки All Users\Desktop ярлык, то этот ярлык будет появляться на рабочих столах всех пользователей.

В Windows Vista и Windows 7 папка Все пользователи (All Users) существует в целях обеспечения обратной совместимости (см. рис. 10.8 и 10.9). В действительности в Windows Vista/7 все ее функциональные возможности переданы папке Общие (Public), структура которой аналогична структуре всех остальных пользовательских профилей Windows Vista/7 (рис. 10.10 и 10.11). Windows Explorer объединяет содержимое вложенных папок профиля Общие (Public), в том числе Desktop и Start Menu, с содержимым обычных пользовательских профилей при регистрации пользователей в системе. Единственное отличие папки Общие (Public) от папки остальных пользовательских профилей состоит в том, что в ней нет улья реестра Ntuser.dat, поскольку Windows этого файла не загружает. Вместо него Windows Vista/7 записывает все параметры настройки, общие для всех пользователей, в соответствующие вложенные ключи в составе дерева `HKEY_LOCAL_MACHINE`.

Папка Общие (Public) введена специально для организации совместного доступа к файлам и принтерам, основные концепции которого в Windows Vista и Windows 7 были существенно переработаны. Новый механизм совместного доступа учитывает и основные концепции безопасности Windows Vista и Windows 7. Обратите также внимание, что в Windows 7 в составе этой папки появилась новая вложенная папка — **Libraries** (рис. 10.11). Эта папка поддерживает новую функциональную возможность Windows 7 — **Библиотеки** (Libraries).

ПРИМЕЧАНИЕ

Папка **CyberLink**, показанная на рис. 10.11, папкой по умолчанию не является — она была создана оценочной версией программы CyberLink PowerDirector, которая тестировалась на работоспособность под Windows 7.

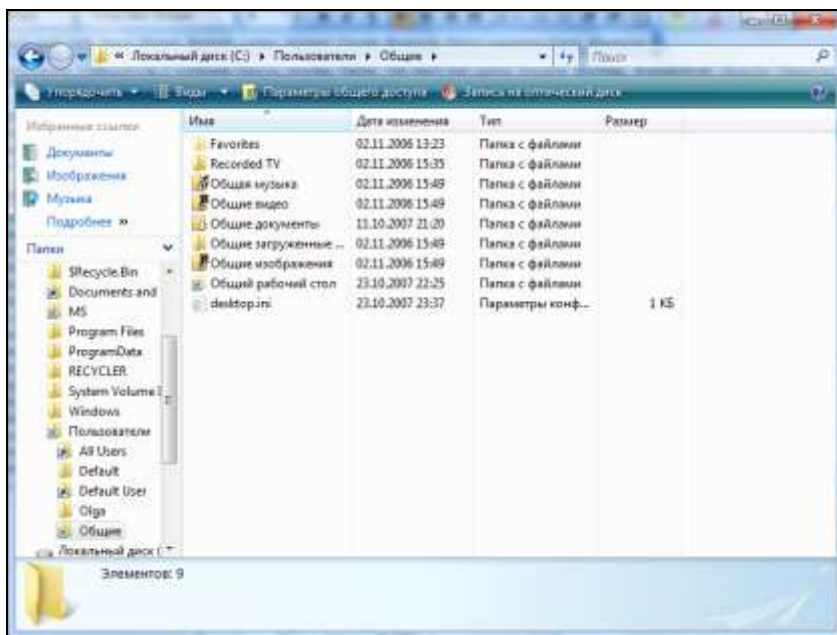


Рис. 10.10. Структура папки **Общие** в составе пользовательского профиля Windows Vista

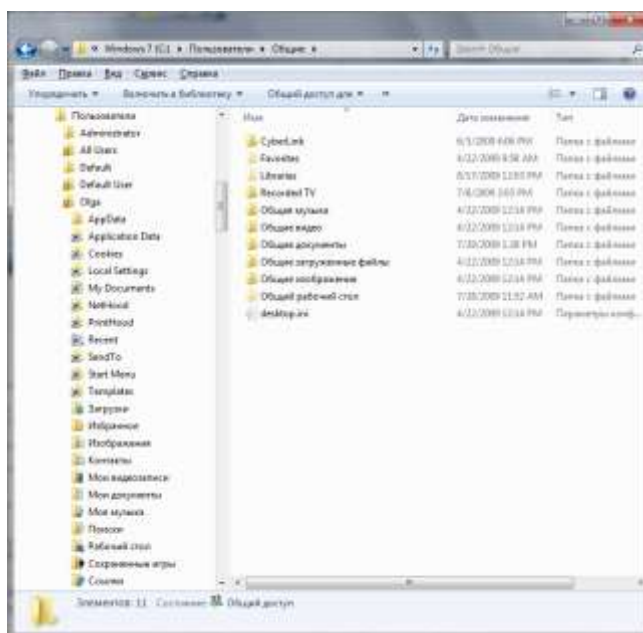


Рис. 10.11. Структура папки **Общие** в составе пользовательского профиля Windows 7

Перемещение пользовательского профиля в другую папку

Довольно часто встречаются такие ситуации, когда пользователи желают полностью переместить папку своего пользовательского профиля со всем ее содержимым, включая и настройки, задаваемые через реестр, например, на другой диск. Добиться нужного результата можно так:

1. Создайте полную резервную копию вашей системы.
2. Создайте абсолютно новую учетную запись пользователя с административными правами, но пока не входите под этим именем в систему.
3. Скопируйте содержимое профиля по умолчанию на другой диск (например, C:\Users\Default → D:\Users\Default).
4. Скопируйте на другой диск оригинальное содержимое общего профиля (например, C:\Users\Public → D:\Users\Public).
5. Запустите редактор реестра и найдите ключ `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList`. Измените значения параметров `Default`, `Public` и `ProfilesDirectory` следующим образом:
 - `Default` на `D:\Users\Default` (на рис. 10.12 показано редактирование параметра `Default`);
 - `Public` на `D:\Users\Public`;
 - `ProfilesDirectory` на `D:\Users`.

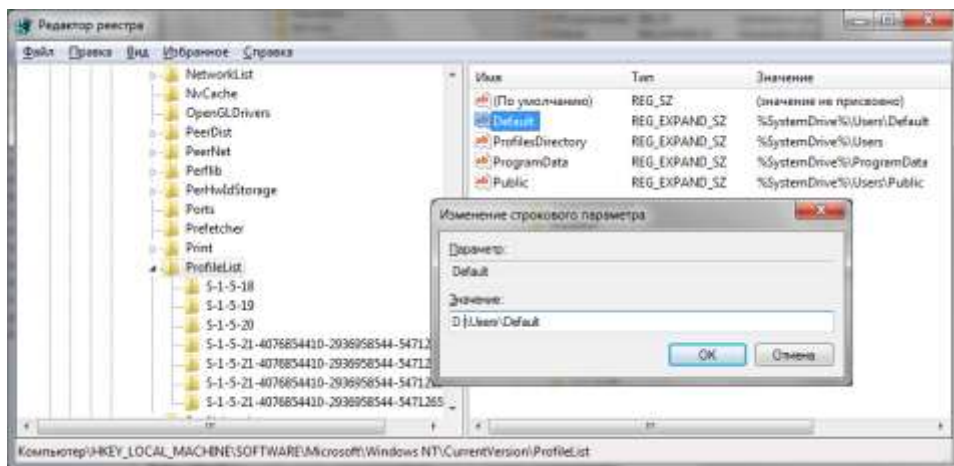


Рис. 10.12. Редактирование параметра `Default` в составе ключа реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList`

6. Перезагрузите Windows и войдите в систему от имени пользователя, который еще никогда не регистрировался в системе и, следовательно, еще не имеет пользовательского профиля. Например, если учетная запись **Администратор** (Administrator) на вашем компьютере еще не разблокирована, лучше всего будет сделать это сейчас и войти в систему с максимальными привилегиями. При первой регистрации в системе Windows создаст профиль для нового пользователя. Обратите внимание, что этот профиль будет создан уже на новом диске.
7. Зарегистрировавшись в системе, по возможности закройте все работающие приложения, которые только можно закрыть. Это позволит избежать блокировки файлов при их копировании.
8. Скопируйте все содержимое папки с пользовательскими профилями в новый каталог (например, C:\Users* → D:\Users\). Имейте в виду, что это будет довольно длительный процесс. Ускорить его можно, написав скрипт, запускаемый из командной строки.

СОВЕТ

Обратите внимание, что множество временных файлов (с расширением tmp) окажутся заблокированными и потому не смогут быть скопированы. Просто пропустите их копирование, нажимая клавиатурную комбинацию <Alt>+<S> (пропускать следует только файлы с расширением tmp).

СОВЕТ

Если некоторые другие файлы, помимо временных, все же не окажутся скопированными, попробуйте исследовать ситуацию с помощью утилиты Марка Руссиновича `groschex.exe`, которую можно загрузить с сайта <http://www.microsoft.com/technet/sysinternals/Processesandthreadsutilities.mspx?wt.svl=featured>. С ее помощью вы сможете определить, что за программа мешает копированию того или иного файла. Тем не менее, если вы закроете максимально возможное количество работающих программ, такая ситуация маловероятна.

9. Откройте редактор реестра, выполните поиск всех ключей и значений, задающих местоположение папки пользовательского профиля. Методично замените эти значения на новые (в рассматриваемом примере: C:\Users на D:\Users). Выполнение этой задачи вручную также отнимет много времени, поэтому, если вы планируете проводить эту операцию часто, лучше тоже написать для этой цели отдельный скрипт.
10. Выйдите из системы и снова зарегистрируйтесь от имени того же пользователя. Повторите предыдущий шаг, чтобы убедиться, что вы изменили все нужные ключи и значения. Эта рекомендация дается потому, что при выходе из системы некоторые программы обновляют реестр, используя прежние пути к папкам пользовательских профилей.

11. Выйдите из системы и вновь зарегистрируйтесь от имени пользователя, под учетной записью которого вы обычно работаете. Протестируйте конфигурацию, чтобы убедиться, что все работает корректно. Все программы должны работать нормально, за исключением тех, что используют "жестко закодированное" значение пути к папкам пользовательских профилей. Чтобы идентифицировать такие программы, подойдет уже упомянутая утилита Procexp.exe. Найдя программы, переконфигурируйте их настройки так, чтобы они указывали на новый каталог с пользовательскими профилями.

Совместимость с наследуемыми приложениями и профилями пользователей Windows 2000/XP

Как уже говорилось ранее, в Windows NT 4.0 все локально кэшированные пользовательские профили хранятся в папке %SystemRoot%\Profiles. Если установка Windows 2000/XP производилась как обновление предыдущей операционной системы, то эта папка по-прежнему будет использоваться для хранения пользовательских профилей. В случае, если при установке Windows 2000/XP была выбрана опция установки новой копии операционной системы, для хранения пользовательских профилей будет создана новая папка с именем Documents and Settings, расположенная на одном разделе с установленной операционной системой Windows 2000/XP.

Некоторые программы для поиска путей к локально кэшированным пользовательским профилям используют жестко закодированные пути. Таким образом, если пользователь попеременно работал на компьютерах под управлением Windows NT 4.0 и Windows 2000/XP, такие программы могут повести себя непредсказуемым образом, если попытка поиска локально кэшированного пользовательского профиля в каталоге %SystemRoot%\Profiles завершится неудачей.

Аналогично пользователи, регистрирующиеся с компьютеров Windows Vista и Windows 7, не могут загружать перемещаемые профили, созданные в Windows XP. Пути решения этой проблемы будут рассмотрены в последующих разделах.

Совместимость с приложениями

Многие приложения Windows активно пользуются существующими соглашениями об именовании папок в пользовательских профилях. Примером могут служить стандартные диалоговые окна **Открыть** (Open) и **Сохранить** (Save), автоматически находящие нужные папки в пользовательских профилях.

Приложения, обладающие возможностью запрашивать операционную систему о расположении папок пользовательского профиля (часто их называют

хорошо известными папками — well-known folders или shell folders), имеют возможность беспрепятственно находить нужные папки. Windows Explorer безошибочно укажет путь к изменившемуся местоположению папки в случае использования функции перенаправления папок (Folder Redirection). Поэтому изменения в пользовательских профилях Windows Vista/7 для них "прозрачны".

Однако наследуемые приложения часто используют другой метод отыскания папок пользовательских профилей. Они запрашивают Windows о расположении нужной папки и сохраняют эту информацию в своих настройках для дальнейшего использования. При переходе на Windows Vista/7 местоположение папки пользовательского профиля изменяется, в результате чего приложение начинает работать неправильно (например, не находит нужных данных).

Для обеспечения обратной совместимости с такими приложениями Windows Vista и Windows 7 используют *точки разветвления* (junction points) — ссылки на данные, хранящиеся в другом каталоге на жестком диске. Windows Vista создает точки разветвления для папок, вложенных в папки пользовательских профилей Windows XP (см. табл. 10.3 и рис. 10.8 и 10.9). Например, скрытая папка Send To в составе папки пользовательского профиля указывает на папку Documents and Settings\%username%\SendTo. На рис. 10.8 и 10.9 все точки разветвления помечены как <JUNCTION>, в отличие от нормальных папок пользовательского профиля Windows Vista/7, которые помечены как каталоги (<DIR>).

Наилучшей тактикой защиты персональной информации конечных пользователей при переходе на Windows Vista/7 является *перенос* (migration) этой информации на новую операционную систему с помощью специализированных утилит, выполняющих такой перенос корректно. Например, Microsoft предлагает для этой цели бесплатную (freeware) утилиту User State Migration Tool (USMT). USMT позволяет собрать информацию о существующих пользовательских профилях и корректно перенести ее на новое место, а также дает возможность просканировать компьютеры и определить, какие профили существуют и какие из них нуждаются в переносе.

СОВЕТ

Поставщики коммерческого программного обеспечения также предлагают средства переноса, причем, по сравнению с USMT, они предоставляют более широкие функциональные возможности. Если вы заинтересованы в масштабном переносе индивидуальной пользовательской информации, обратите внимание на такие продукты, как Altiris Deployment Solution (<http://www.altiris.com/Download.aspx>), Symantec Ghost Solution Suite (<http://www.symantec.com/themes/ghost/index.jsp>), LANDesk Management Suite (<http://www.landesk.com/Products/LDMS/index.aspx>) и Prism Deploy (<http://www.newboundary.com/products/prismdeploy/>).

Совместимость с пользовательскими профилями предыдущих версий операционной системы

Хотя теоретически в Windows 2000 и Windows XP структура профилей считается одинаковой, но это только в теории, а на самом деле администраторы имели много проблем и головной боли. Аналогичная проблема, но усугубившаяся несовместимостью пользовательских профилей предыдущих версий Windows 2000/XP, существует и в Windows Vista/7. Внесенные изменения не позволяют Windows Vista/7 загружать пользовательские профили предыдущих версий Windows, а предыдущие версии Windows не загружают профили пользователей Windows Vista/7. Пути решения этой проблемы будут рассмотрены в следующем разделе.

Работа с перемещаемыми профилями в Windows Vista/7

Чтобы создать перемещаемый пользовательский профиль, необходимо выполнить следующие операции:

1. На компьютере, являющемся контроллером домена, создайте учетную запись пользователя с правами администратора, а также разделяемый каталог для хранения профилей (учетную запись администратора профилей следует создавать в Active Directory Users and Computers).
2. Создайте учетную запись для пользователя с перемещаемым профилем. Запустите оснастку консоли MMC, управляющую пользователями и группами, выберите учетную запись вновь созданного пользователя и выполните на ней двойной щелчок мышью. Раскроется диалоговое окно **Свойства: <имя пользователя>** (User Properties). Перейдите на вкладку **Профиль** (Profile) и укажите путь к профилю пользователя в формате `\\server name\share name\%user name%`, где `server name` — имя сервера, `share name` — имя разделяемой папки, в которой хранятся пользовательские профили, а `user name` — имя пользователя с перемещаемым профилем (рис. 10.13).
3. Раскройте окно **Свойства системы** (System properties) и нажмите кнопку **Параметры** (Settings) в группе опций **Профили пользователей** (User Profiles) (рис. 10.14).
4. В раскрывшемся диалоговом окне **Профили пользователей** (User Profiles) выделите существующий локальный пользовательский профиль (рис. 10.15) и нажмите кнопку **Копировать** (Copy To).

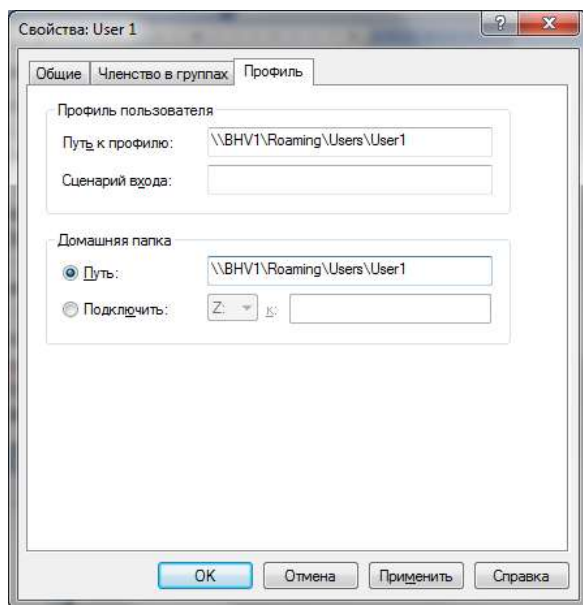


Рис. 10.13. Диалоговое окно свойств пользователя

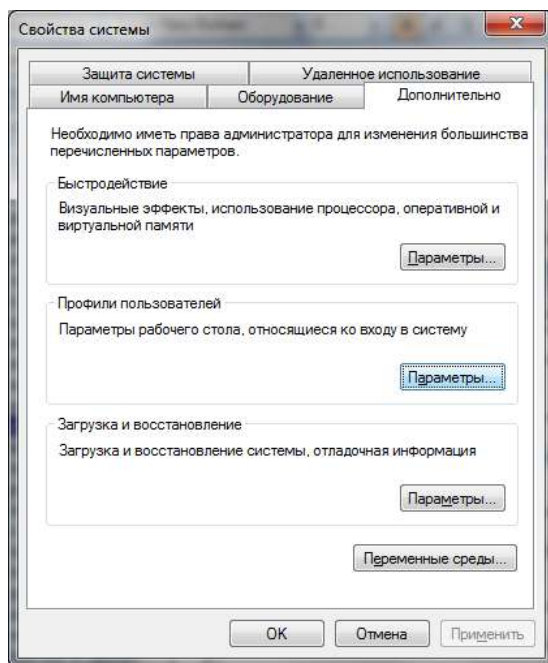


Рис. 10.14. Вкладка Дополнительно окна Свойства системы

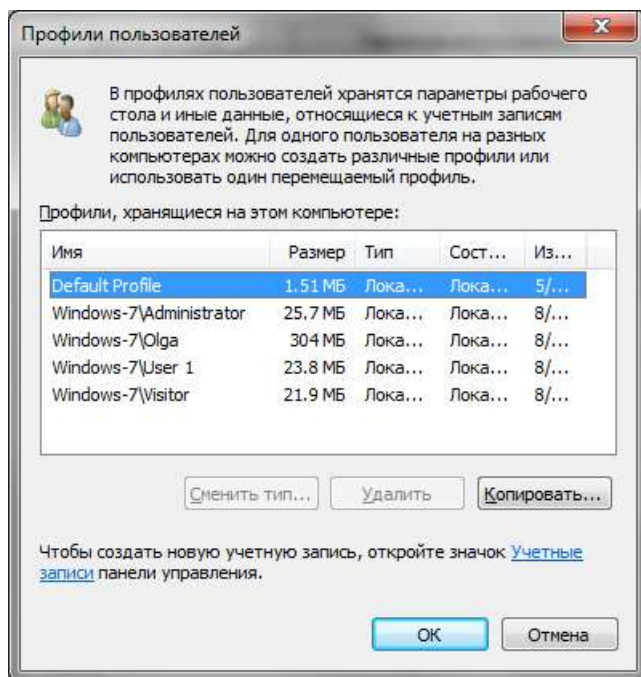


Рис. 10.15. Окно Профили пользователей

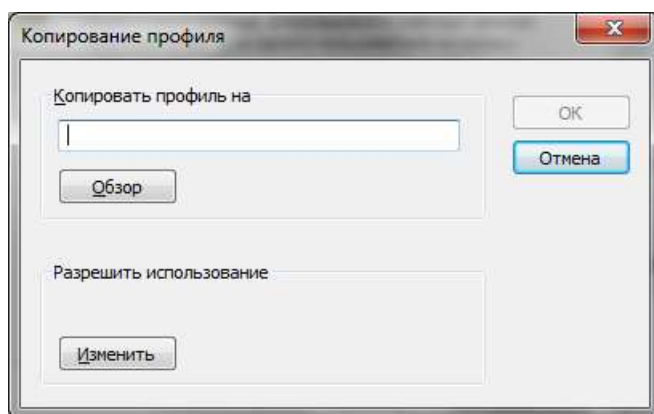


Рис. 10.16. Окно Копирование профиля

5. Раскроется окно **Копирование профиля** (Copy To), показанное на рис. 10.16. Укажите в соответствующем поле путь к разделяемой папке, в которой хранятся пользовательские профили. Указывать путь следует в формате

UNC (Universal Naming Convention), например: `\\server name\share name\user profile folder`.

ПРИМЕЧАНИЕ

Во всех версиях Windows, предшествовавших Windows 7 (Windows 2000/XP/Vista), вы легко могли скопировать любой незаблокированный пользовательский профиль. Начиная с Windows 7, эта возможность оказалась заблокированной. Скопировать можно только профиль по умолчанию (Default Profile), а если вы выберете любой другой из профилей, существующих в системе, то увидите, что кнопка **Копировать** (Copy To) будет заблокирована (рис. 10.17).

СОВЕТ

Обойти это ограничение можно при помощи ручного копирования и редактирования реестра (см. разд. "Перемещение пользовательского профиля в другую папку"). Есть и еще один вариант — перезаписать нужный вам пользовательский профиль поверх профиля по умолчанию (этот метод официально не поддерживается, но он работает). Я рассмотрю этот метод чуть далее в этой главе.

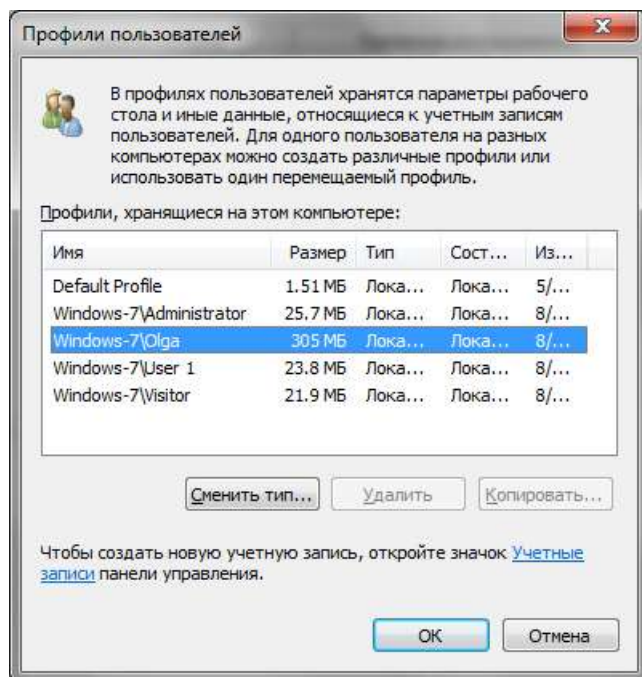


Рис. 10.17. В Windows 7 заблокирована возможность копирования любых локальных пользовательских профилей, кроме профиля по умолчанию (Default Profile)

6. Выберите пользователя, которому разрешается работать с указанным профилем, нажмите кнопку **ОК** для копирования профиля. Нажмите кнопку **ОК**, чтобы подтвердить внесенные изменения.
7. Зарегистрируйтесь в сети с клиентского компьютера Windows Vista/7 и откройте на нем окно **Профили пользователей** (User Profiles), показанное на рис. 10.18. Тип профиля пользователя с перемещаемым профилем должен иметь статус **Перемещаемый** (Roaming). Чтобы изменить тип профиля, нажмите кнопку **Сменить тип** (Change Type) и в следующем окне выберите нужный тип профиля.

ПРИМЕЧАНИЕ

Начиная с Windows 2000, стандартные права доступа к пользовательским профилям изменились. Так, администраторы больше не имеют прав доступа типа "Полный доступ" (Full Control) ко всем пользовательским профилям. Это означает, что если администратору требуется получить доступ к содержимому пользовательского профиля, он должен выполнить операцию присваивания прав владельца на объекты файловой системы (если пользовательские профили хранятся на разделе NTFS) и соответствующие ульи реестра. С точки зрения безопасности этот подход весьма логичен, поскольку операция присваивания прав владельца является событием, подлежащим аудиту. Кроме того, Windows Vista/7 добавляет к концу названия папки перемещаемого пользовательского профиля суффикс *v2*. Это делается для того, чтобы отличать перемещаемые профили пользователей Windows Vista и Windows 7 от перемещаемых профилей пользователей других операционных систем.

Как выполнить перезапись профиля по умолчанию нужным вам пользовательским профилем

Теперь рассмотрим обещанный чуть ранее совет по перезаписи профиля по умолчанию другим профилем, который вы впоследствии захотите использовать как перемещаемый. Действуем следующим образом:

1. Создайте пользовательскую учетную запись (в нашем примере назовем ее **Kokoreva**). Настройте пользовательский профиль в соответствии с вашими потребностями.
2. Зарегистрируйтесь в системе от имени пользователя с административными правами, но не **Kokoreva** (в противном случае файлы в вашем пользовательском профиле будут заблокированы).
3. Если этого до сих пор не было сделано, то настройте свойства папок (Folder Options) таким образом, чтобы отображались все скрытые и системные файлы. О том, как это делается, уже рассказывалось в *главе 1*.
4. Перейдите в каталог C:\Users и переименуйте папку Default в Default Backup (на тот случай, если что-то пойдет категорически не так, нам понадобится оригинальная папка Default).

5. Создайте копию вашего вновь созданного пользовательского профиля и переименуйте ее в *Default*.
6. Выполните щелчок правой кнопкой мыши на этой новой папке *Default* и отрегулируйте к ней права доступа следующим образом: группы **Everyone** и **Users** должны иметь к ней доступ с правами **Read & Execute**, **List Folder Contents** и **Read**. После этого можете при желании удалить папку **Kokoreva**.
7. Теперь попробуйте зарегистрироваться в системе от имени любой новой учетной записи, для которой еще не создавался пользовательский профиль. Если параметры рабочего стола и прочие настройки окажутся такими, какие вы создали для профиля, которым заменили **Default**, значит, все в порядке.

ВНИМАНИЕ!

Этот совет я нашла на сайте <http://www.irongeek.com/i.php?page=security/windows-7-copy-default-profile>, и его автор честно предупреждает о том, что ему пока неизвестно, какие проблемы следование этому совету может вызвать в дальнейшем. Microsoft вам никогда такого совета не даст. Однако я протестировала данный совет, и у меня все отлично работало. Проблем пока нет.

Политики пользовательских профилей

Начиная с Windows XP, Microsoft стала последовательно улучшать и развивать управление пользовательскими параметрами. Так, по сравнению с Windows 2000, роуминг параметров стал более надежным, был усовершенствован алгоритм объединения пользовательских профилей, а также добавлены новые параметры политики. В Windows Vista и Windows 7 все эти нововведения получили дальнейшее развитие.

ПРИМЕЧАНИЕ

Внесенные изменения настолько многочисленны, что описать их в полном объеме в рамках одной главы невозможно. Детальную информацию по данному вопросу можно найти в документе "Managing Roaming User Data Deployment Guide", который доступен для скачивания по адресу <http://technet2.microsoft.com/WindowsVista/en/library/fb3681b2-da39-4944-93ad-dd3b6e8ca4dc1033.mspx?mfr=true>. Однако далее здесь будет дано пояснение новых настроек политики в отношении пользовательских профилей, впервые появившихся в Windows Vista и Windows 7.

Политики пользовательских профилей в Windows XP и Windows Vista/7 имеют свой узел в Редакторе групповой политики (Group Policy), показанном на рис. 10.18. Кроме того, по сравнению с Windows 2000 в Windows XP было добавлено три новых политики, а в Windows Vista — еще пять. Для просмотр-

ра политик в отношении пользовательских профилей необходимо выполнить следующие действия:

1. Запустите сеанс Редактора групповой политики любым из уже описанных ранее способов. Напомним, что проще всего это сделать, введя из командной строки команду `GPedit.msc`.

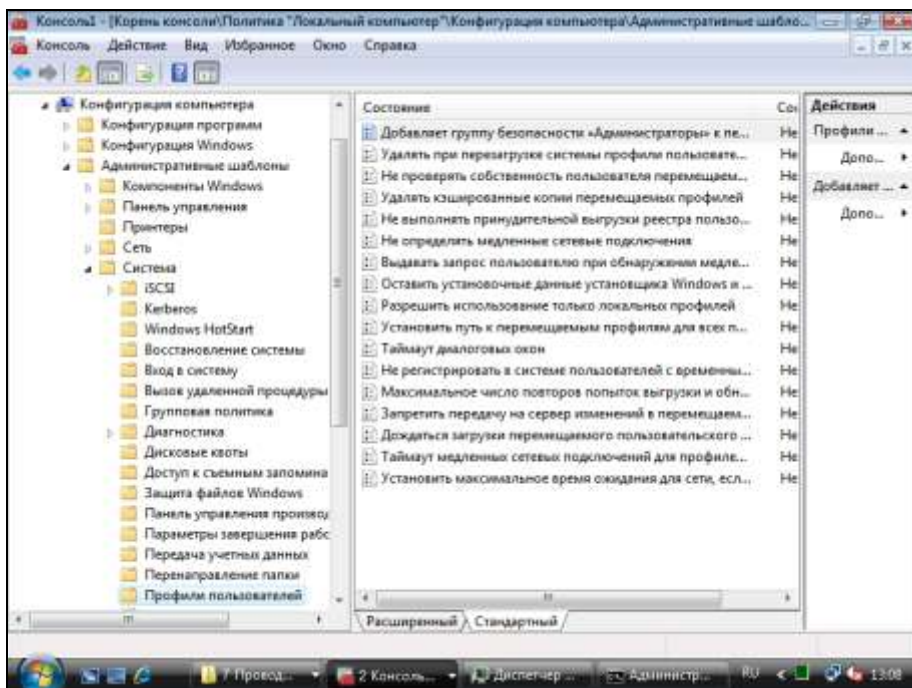


Рис. 10.18. Для политики **Профили пользователей** в окне Редактора групповой политики есть собственный узел

2. Разверните окно консоли, как показано на рис. 10.18: **Конфигурация компьютера** | **Административные шаблоны** | **Система** | **Профили пользователей** (Computer Configuration | Administrative Templates | System | User Profiles).

Новые политики Windows Vista и Windows 7 в отношении пользовательских профилей

Рассмотрим вкратце новые политики в отношении пользовательских профилей, которые появились в Windows Vista/7. Часть из них находится в составе узла **Конфигурация компьютера** | **Административные шаблоны** | **Система** |

Профили пользователей (Computer Configuration | Administrative Templates | System | User Profiles), а часть — по тому же пути, но в составе узла **Конфигурация пользователя** (User Configuration).

Все эти политики относятся только к компьютерам, работающим под управлением Windows Vista/7, однако они могут сосуществовать в объектах групповой политики (Group Policy Objects, GPO), управляющих клиентскими компьютерами, работающими под управлением операционных систем более ранних версий, нежели Windows Vista. При этом клиенты Windows 2000/XP будут эти политики игнорировать. Перечислим наиболее важные политики Windows Vista/7 в отношении пользовательских профилей:

- ❑ **Удалять при перезагрузке системы профили пользователей по истечении указанного числа дней** (Delete user profiles older than a specified number of days on system restart) — необходимо указать числовое значение, задающее требуемое количество дней. Если вы сконфигурируете эту политику, Windows Vista/7 будет удалять все пользовательские профили, просуществовавшие дольше указанного времени;
- ❑ **Не выполнять принудительной выгрузки реестра пользователя при его выходе из системы** (Do not forcefully unload the user registry at user logoff) — Windows Vista/7 всегда принудительно выгружает улей реестра соответствующего пользовательского профиля. Данная политика отменяет поведение Windows Vista/7 по умолчанию;
- ❑ **Установить путь к перемещаемым профилям для всех пользователей, входящих в систему на данном компьютере** (Set roaming user profile path for all users logging onto this computer) — следует иметь в виду, что Windows читает конфигурации профилей в предопределенном порядке и использует первый сконфигурированный параметр, который при этом встретится. Порядок обработки параметров следующий:
 - путь к перемещаемому профилю терминального сервиса (Terminal Services), задаваемый политикой в отношении терминальных сервисов;
 - путь к перемещаемому профилю терминальных сервисов, указанный для конфигурации пользователя;
 - путь к перемещаемому профилю терминальных сервисов, указанный для конфигурации компьютера;
 - путь к перемещаемому профилю конкретного пользователя, указанный для конфигурации пользователя;
- ❑ **Установить максимальное время ожидания для сети, если пользователь имеет перемещаемый профиль или удаленный домашний каталог** (Set maximum wait time for the network if a user has a roaming

user profile or remote home folder) — при входе пользователя в систему Windows Vista/7 обычно ожидает установления сетевого соединения в течение 30 секунд. В случаях, когда регистрация происходит через беспроводную сеть, может потребоваться более длительный интервал ожидания. Если активизировать эту политику, Windows будет ожидать установления сетевого соединения в течение указанного интервала времени. Windows не будет синхронизировать перемещаемый профиль или домашнюю папку, если регистрация произошла раньше установления активного сетевого соединения;

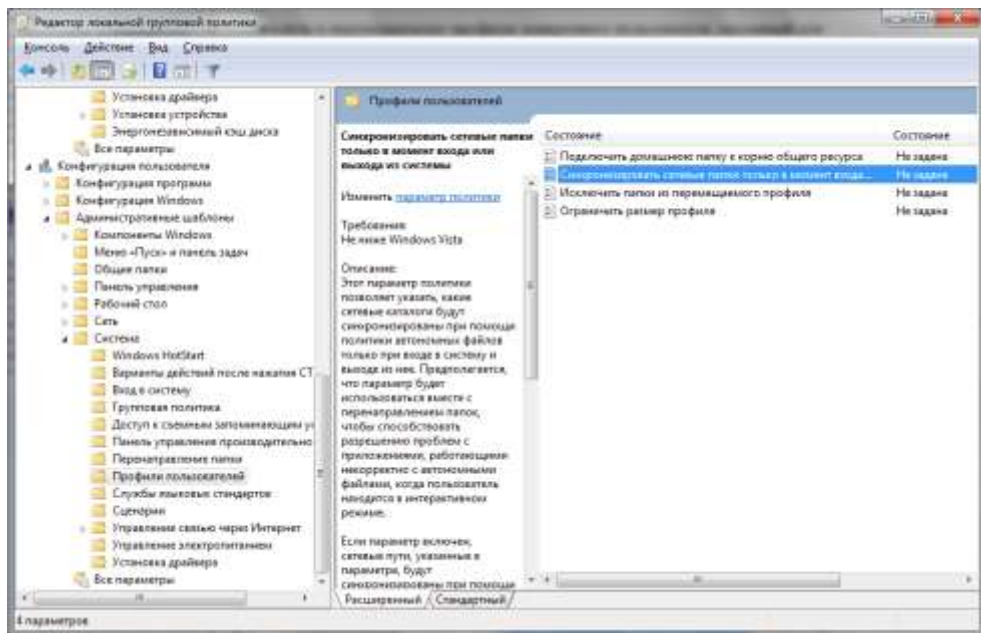


Рис. 10.19. Новые политики Windows Vista и Windows 7 в отношении пользовательских профилей в составе узла **Конфигурация пользователя | Административные шаблоны | Система | Профили пользователей**

- в составе узла **Конфигурация пользователя | Административные шаблоны | Система | Профили пользователей** (User Configuration | Administrative Templates | System | User Profiles) появилась еще одна новая политика (рис. 10.19) — **Синхронизировать сетевые папки только в момент входа или выхода из системы** (Network directories to sync at Logon/Logoff time only). Windows Vista/7 автоматически помечает все перенаправленные папки как доступные автономно, отслеживает их и синхронизирует их содержимое на локальном компьютере и в сетевом

каталоге. Этот процесс происходит при входе в систему, при выходе из системы, а также периодически в течение сеанса работы. Чтобы сконфигурировать эту политику, вы можете указать пути к сетевым папкам, синхронизация которых происходит только при входе в систему и при выходе из нее.

Способ получения пользовательского профиля и перенаправление папок

Способ получения пользователями своих профилей зависит от того, какой тип профиля установлен. Рассмотрим этот процесс подробнее.

- Для локальных профилей получение пользователями своих профилей выглядит следующим образом.

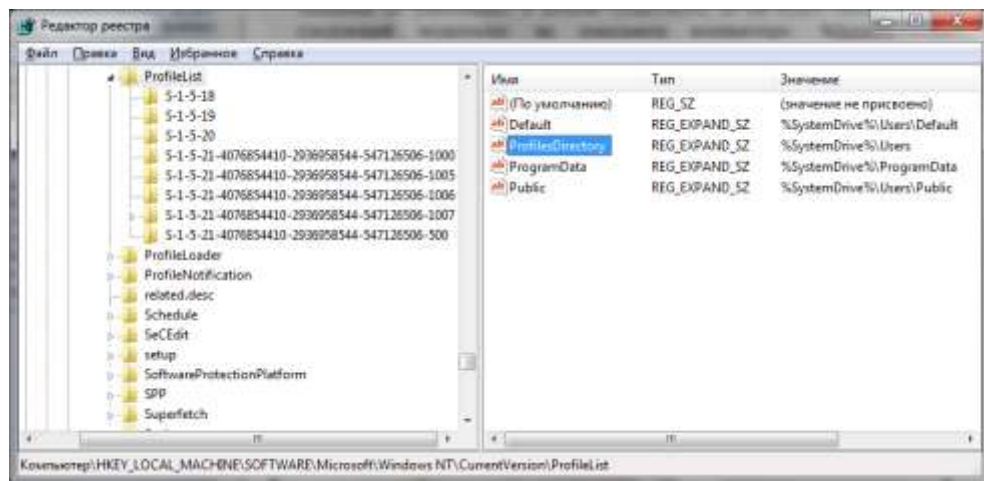


Рис. 10.20. Список пользовательских профилей хранится в реестре под ключом `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT \CurrentVersion\Profilelist`

Пользователь регистрируется в системе. Операционная система проверяет список пользовательских профилей, расположенный под ключом `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ProfileList` (рис. 10.20), чтобы определить, есть ли для данного пользователя локальный профиль. Если такой элемент существует, значит, локальный профиль используется. Если локальный профиль не найден, и компьютер является участником домена, то операционная система проверяет, есть ли такой профиль по умолчанию в домене (он должен быть расположен в разделяемой папке с именем NETLOGON контроллера домена, которая,

в свою очередь, находится в папке Default). Если пользовательский профиль, заданный по умолчанию, в домене существует, то он будет скопирован в следующий подкаталог на локальном компьютере: %SystemDrive%\Documents and Settings\Username (Windows XP) или %SystemDrive%\Users\Username (Windows Vista/7). Если же этот профиль не существует, то будет скопирован профиль, содержащийся в папке %SystemDrive%\Documents and Settings\Default User (Windows XP) или %SystemDrive%\Users\Default (Windows Vista/7).

Пользовательский улей реестра (Ntuser.dat) отображается в часть реестра HKEY_CURRENT_USER. Когда пользователь завершает сеанс, профиль сохраняется на локальном жестком диске компьютера.

- Для перемещаемых профилей этот процесс заключается в следующем.

Пользователь регистрируется, и Windows проверяет список пользовательских профилей, хранимых в реестре под ключом HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Profilelist, чтобы определить, существует ли копия профиля в кэше. Если локальная копия не найдена, а компьютер является частью домена, Windows проверяет, есть ли такой профиль, установленный по умолчанию, в домене (в папке NETLOGON контроллера домена, находящейся в папке Default). Если этот профиль существует, то он будет скопирован в следующий подкаталог локального компьютера. Если пользовательский профиль в домене не существует, то из каталога %SystemDrive%\Users\Default будет скопирован локальный профиль, заданный по умолчанию.

Пользовательский улей реестра (Ntuser.dat) копируется в локальную копию пользовательского профиля, хранящуюся в кэше, и отображается в часть реестра HKEY_CURRENT_USER. Локальный профиль, хранящийся в кэше, сравнивается с копией профиля на сервере, и оба файла объединяются.

Далее пользователь, как обычно, может запускать приложения и редактировать документы. Когда пользователь завершает сеанс, его локальный профиль копируется в местоположение, заданное администратором. Если профиль уже существует на сервере, то локальный профиль объединяется с копией, хранящейся на сервере.

ПРИМЕЧАНИЕ

В Windows NT 4.0 алгоритм соединения основывался на команде `xcopy` с поддержкой полной синхронизации. Это означает, что в любой момент времени существует лишь одна главная копия (master copy) профиля. При регистрации пользователя главный профиль расположен на локальном компьютере, а когда пользователь не регистрируется, главная копия его профиля находится на сервере. В большинстве случаев этот алгоритм работает хорошо, например, когда

пользователь регистрируется только на одном компьютере. Однако пользователь, одновременно зарегистрировавшийся на нескольких машинах, может столкнуться с непредсказуемым поведением.

Начиная с Windows XP, эта проблема устранена путем слияния профилей на уровне файлов. При обновлении документа или файла, новый алгоритм сравнивает временную метку файла-приемника с временной меткой файла-источника. Если файл-приемник оказывается более новым, то он не перезаписывается.

В Windows Vista/7 непереключаемые компоненты пользовательского профиля хранятся во вложенных папках пользовательского профиля AppData\Local и AppData\LocalLow.

С другой стороны, технология IntelliMirror включает в себя функциональную возможность *переадресации папок* (Folder Redirection), позволяющую администраторам осуществлять переадресацию определенных папок пользовательских профилей и размещать их в сети (с точки зрения пользователя, это почти то же самое перемещение (roaming), но при этом пользовательские установки хранятся в совместно используемой сетевой папке). Переадресация каталогов может использоваться в отношении всех типов профилей, включая локальные (local), перемещаемый (roaming) или обязательные (mandatory). Сочетание функции Folder Redirection с перемещаемыми профилями позволяет воспользоваться всеми преимуществами перемещаемых профилей и в то же самое время сократить сетевой трафик.

В Windows Vista/7 функция переадресации папок (Folder Redirection) была существенно улучшена и доработана и теперь позволяет администраторам переадресовать до 10 пользовательских папок. Фактически она является наиболее корректным методом преодоления путаницы и проблем, вызванных несовместимостью профилей Windows Vista с пользовательскими профилями Windows XP. В уже упомянутом документе "Managing Roaming User Data Deployment Guide" приведены готовые сценарии (case studies), иллюстрирующие пути преодоления возможных проблем.

Сценарии

Регистрационный сценарий (logon script) представляет собой командный (BAT) или исполняемый (EXE) файл, который запускается каждый раз, когда пользователь регистрируется в сети с любой из рабочих станций. Сценарий регистрации может содержать команды операционной системы, например, команды, выполняющие установление сетевых соединений или осуществляющие запуск приложений. Регистрационные сценарии могут устанавливать *переменные окружения* (environment variables): пути (переменная PATH), каталог для временных файлов (переменная TEMP) и т. д.

Начиная с Windows 2000, усовершенствование Windows Script Host (WSH) 2.0 позволяет системным администраторам создавать простые, мощные и гибкие *скрипты*. Для написания скриптов можно выбрать любой из языков, предпочитаемых администратором: Visual Basic Scripting Edition (VBScript), JScript, Perl. WSH поддерживает COM и позволяет использовать преимущества Windows Management Instrumentation (WMI) и Active Directory Services Interface (ADSI).

Использование WSH для написания регистрационных сценариев

Не углубляясь в детали, приведем небольшой пример фрагмента регистрационного сценария, который выполняет редактирование реестра. Поскольку многие пользователи просто боятся редактировать реестр, администратор может написать для них регистрационный сценарий, выполняющий настройку реестра. WSH предоставляет весьма удобный способ манипулирования реестром с помощью методов RegRead, RegWrite и RegDelete.

Приведенный далее фрагмент регистрационного сценария изменяет параметры настройки прокси-сервера. Как известно, они хранятся в реестре по адресу HKCU\Software\Microsoft\Windows\CurrentVersion\InternetSettings\ProxyServer, и сначала их следует прочитать с помощью метода RegRead. Затем, используя метод RegWrite, можно переписать существующее значение, заменив его на другое, например, NEWPROXY:80. Наконец, следует убедиться в правильности внесенных изменений, еще раз прочитав значение, сохраненное в реестре, с помощью метода RegRead:

```
...
sub regProxy
    prefix = _
        "HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\"
    WScript.Echo "Old ProxyServer settings: " & WshShell.RegRead(prefix & _
        "ProxyServer")
    WshShell.RegWrite prefix & "ProxyServer", "MYPROXY:80"
    WScript.Echo "New ProxyServer settings: " & WshShell.RegRead(prefix & _
        "ProxyServer")
end sub
...
```

ПРИМЕЧАНИЕ

К сожалению, многие из скриптов, написанных для предшествующих версий Windows, не могут применяться в Windows Vista/7 — по крайней мере, не могут

там применяться без доработки. Впрочем, это и не удивительно, поскольку в Windows Vista внесено много модификаций, и все они нашли отражение в реестре. Поэтому нельзя согласиться с утверждениями тех, кто заявляет о том, что "реестр Vista/7 на 90% остался неизменным".

Опытные администраторы, которые пишут скрипты, предназначенные для нескольких версий ОС, проверяют версии операционной системы. Казалось бы, для этой цели можно использовать переменную окружения `%os%`, но в Windows Vista она имеет такое же значение, как и в Windows XP.

Как временное решение, можно применить следующий подход:

```
if "%allusersprofile%"=="C:\ProgramData" goto WinVista
if %os%==Windows_NT goto WinXP
::
::if it gets here, assume 9x base
::
Exit
::Winvista
@Echo Windows Vista Operating System Detected
goto fin
::
:winxp
@Echo Windows XP Operating System Detected
::
:fin
```

Общие сведения о системной политике

Системная политика (System policy) представляет собой еще одно средство, которое системные администраторы могут использовать для централизованного управления доступом пользователей к сети и настройке рабочих столов, в том числе разделением данных и конфигурированием параметров системы. Системная политика представляет собой настройки реестра, автоматически устанавливаемые при регистрации пользователя на ПК. Основное отличие между системной политикой и пользовательскими профилями заключается в том, что системная политика применима к пользователям, группам пользователей и конкретным компьютерам. Для каждого из этих компонентов системные администраторы могут задавать, изменять и поддерживать настройки реестра. Комбинируя системную политику, присвоенную конкретному пользователю, компьютеру, на котором он зарегистрировался, и любым группам, к которым они могут принадлежать, вы получаете полный контроль

над типом пользовательской среды и правами пользователей. Для определения параметров каждой политики системные администраторы просто создают шаблоны системной политики.

Системная политика в Windows NT/2000/XP

В операционной системе Windows NT 4.0 впервые была введена утилита **Редактор системной политики** (System Policy Editor), которая позволяла задавать конфигурационные параметры для пользователей и компьютеров, хранящиеся в реестре Windows NT. С ее помощью администратор мог управлять рабочими средами пользователей и устанавливать конфигурационные параметры для всех компьютеров Windows NT 4.0 (Workstation или Server). В Windows 2000/XP для управления конфигурациями групп пользователей и компьютеров используется оснастка ММС **Групповая политика** (Group Policy), которая расширяет функциональные возможности Редактора системной политики (System Policy Editor) и предоставляет дополнительные возможности по управлению конфигурациями клиентских компьютеров, в том числе *опции политики в отношении реестра* (registry based policies), *параметры безопасности* (security settings), *параметры установки программного обеспечения, сценарии и перенаправление папок* (folder redirection). Параметры групповой политики, задаваемые администратором, содержатся в *объекте групповой политики* (Group Policy Object, GPO), который, в свою очередь, ассоциируется с одним из контейнерных объектов Active Directory — узлом, доменом или организационной единицей.

ПРИМЕЧАНИЕ

К сожалению, ограниченный объем данной книги не позволяет дать здесь подробное описание системной политики в Windows NT/2000/XP, но соответствующий фрагмент из моей книги о реестре Windows XP¹ приведен на сопроводительном компакт-диске.

Групповая политика в Windows Vista/7

В версиях, предшествующих Windows Vista, значения реестра, которые можно было задать через групповую политику, управлялись ADM-файлами. Если администратору требовалось контролировать через групповую политику дополнительные параметры реестра, помимо тех, которые управлялись стандартными ADM-файлами, поставлявшимися Microsoft, необходимо было создавать собственные ADM-файлы, что представляло собой непростую задачу.

¹ Кокорева О. И. Реестр Windows XP. — СПб.: БХВ-Петербург, 2004.

Вдобавок, ADM-файлы хранились в объектах групповой политики (GPO) в Active Directory, и каждый из этих GPO вместе с сопутствующими ADM-файлами реплицировался по всем контроллерам домена.

С выпуском Windows Vista ситуация изменилась в лучшую сторону. Во-первых, были внесены изменения в формат ADM-файлов. Теперь они имеют другой формат — ADMX, и хранятся по-другому.

Формат ADMX

Наиболее существенным отличием нового формата ADMX от формата ADM является то, что установка политик в отношении параметров реестра теперь базируется на стандарте XML. Этот подход предоставляет следующие преимущества:

- ❑ для редактирования файлов формата XML существует гораздо большее количество инструментальных средств;
- ❑ формат XML базируется на документированной схеме, что еще более упрощает разработку индивидуальных шаблонов;
- ❑ улучшенная многоязычная поддержка — для каждого из поддерживаемых языков можно создавать отдельные ADML-файлы без необходимости редактирования основных ADMX-файлов, фактически реализующих нужные политики. Стандартные ADMX-файлы, входящие в комплект поставки Windows Vista, содержатся в каталоге %SystemDrive%\Windows\Policydefinitions (рис. 10.21), а соответствующие файлы языковой поддержки — во вложенных папках этого каталога;
- ❑ еще одно радикальное отличие Windows Vista/7 от Windows NT/2000/XP состоит в том, что теперь ADMX-файлы структурированы по функциям. Объекты GPO, созданные в Windows XP, состояли из небольшого количества ADM-файлов (обычно — пяти), причем наиболее масштабным был файл System.adm. В Windows Vista/7 параметры настройки политики распределены по существенно большему количеству ADMX-файлов, каждый из которых определяет настройки политики в отношении конкретных компонентов Windows, включая апплеты Панели управления (Control Panel), Проводник (Windows Explorer) и т. п.

Файлы ADMX и ADML можно редактировать любым текстовым редактором (например, даже с помощью Блокнота, правда, для этой цели следует первоначально ознакомиться с синтаксисом XML).

ПРИМЕЧАНИЕ

Подробное описание спецификации XML, на которой базируются ADMX-файлы, можно скачать здесь: <http://www.w3.org/TR/xml/>, а описание схемы ADMX — по адресу <http://msdn2.microsoft.com/en-us/library/aa373476.aspx>. Кроме того,

Microsoft в сотрудничестве с FullArmor Corp. выпустила бесплатное средство ADMX Migrator (<http://www.microsoft.com/downloads/details.aspx?FamilyId=0F1EEC3D-10C4-4B5F-9625-97C2F731090C&displaylang=en>).

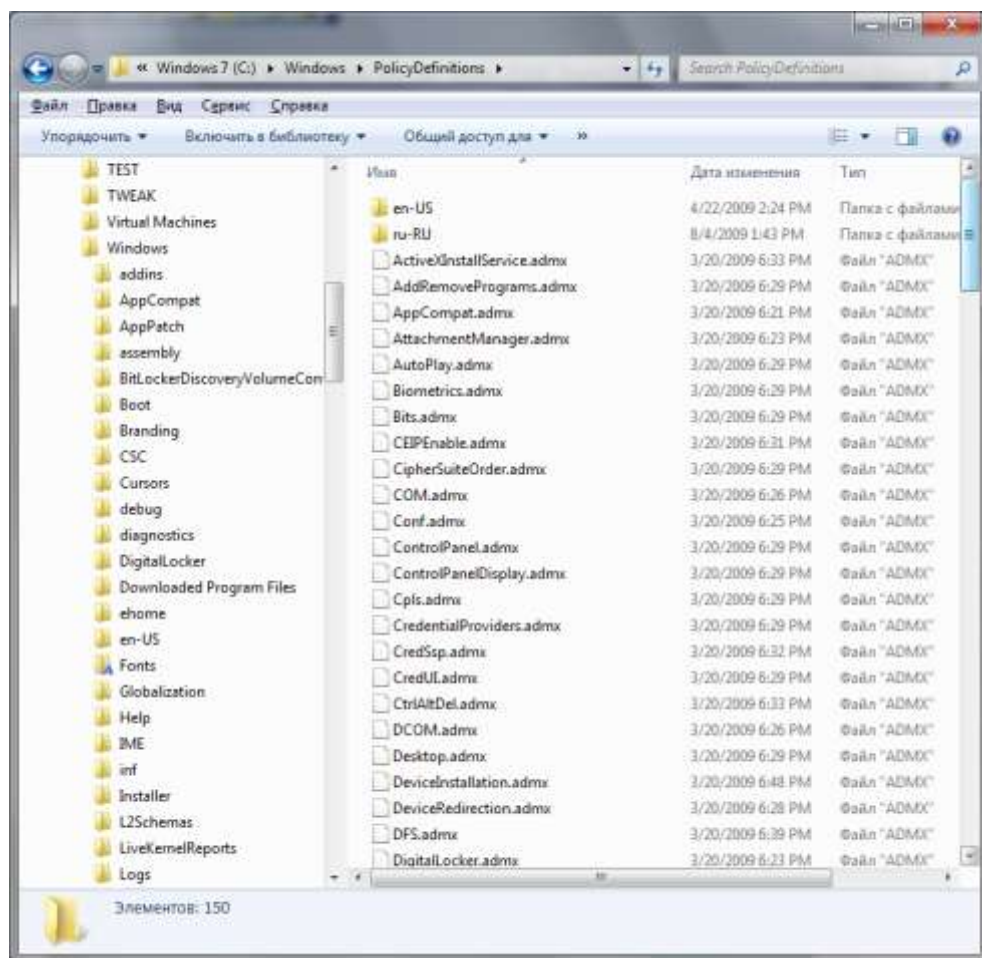


Рис. 10.21. Файлы ADMX, входящие в стандартный комплект поставки Windows Vista/7

Хранение шаблонов ADMX

В Windows NT/2000/XP при создании новых GPO файлы ADM автоматически копировались с локальной рабочей станции в разделяемый каталог SYSVOL на контроллере домена Active Directory. Затем эти ADM-файлы реплицировались на каждый из контроллеров домена, и для каждого из них

создавался GPO. Это приводило к существенному перерасходу сетевого трафика и дискового пространства, особенно в крупных сетях, насчитывавших десятки и сотни GPO.

В отличие от Windows NT/2000/XP, при создании объекта GPO на основе службы каталогов Active Directory на компьютере под управлением Windows Vista/7 отображающиеся в редакторе групповых политик политики административных шаблонов загружаются из папки `C:\windows\policydefinitions` на том же компьютере.

Файлы ADMX и ADML не копируются в сетевую папку SYSVOL, а используются локально. Это позволяет избежать нагрузки на сеть и системы хранения среды групповых политик, неизбежной при использовании файлов ADM. И это не единственный положительный момент. Windows Vista и Windows 7 также поддерживают центральное хранилище — базу данных административных шаблонов. Таким образом обеспечивается эффективное управление файлами ADMX, используемыми для редактирования объектов GPO, независимо от того, откуда производится редактирование. Это достигается путем копирования всех файлов ADMX и ADML официальной поставки и созданных пользователем в единое место в сети и последующего обращения к ним вместо локальных файлов при редактировании групповых политик с рабочих станций под управлением Windows Vista/7. Настройка центрального хранилища — несложная задача, которую достаточно выполнить один раз для данного домена.

Чтобы создать центральное хранилище, необходимо поступить следующим образом:

1. Зарегистрируйтесь на контроллере домена Active Directory как администратор.
2. Найдите разделяемый каталог SYSVOL на контроллере домена в роли эмулятора главного контроллера домена (PDC-emulator).

ПРИМЕЧАНИЕ

В принципе, можно использовать любой контроллер домена, но при выбранном подходе ваша работа будет эффективнее, так как изменения групповых политик обычно сконцентрированы на владельце роли PDC.

3. Раскройте разделяемую папку SYSVOL и создайте в ней новую папку PolicyDefinitions.
4. Скопируйте в новую папку PolicyDefinitions содержимое папки `C:\windows\policydefinitions` на вашей рабочей станции Windows Vista/7, не забыв о вложенной папке, содержащей языковые файлы ADML.

Как только файлы ADMX и ADML будут скопированы в папку центрального хранилища (Central Store), Редактор объектов групповой политики начнет ссылаться именно на них, а файлы ADMX и ADML, хранящиеся локально, будут игнорироваться.

Устранение проблем с загрузкой пользовательских профилей

Как уже ранее говорилось в этой главе, проблемы с загрузкой пользовательского профиля могут полностью блокировать работу пользователя. Даже если регистрация в системе пройдет успешно, в случае невозможности загрузки существующего пользовательского профиля и даже создания нового вы можете оказаться с набором очень ограниченных возможностей по выполнению каких бы то ни было задач. При этом вы загружаетесь с использованием временного пользовательского профиля, и все внесенные вами изменения теряются при выходе из системы. В данном разделе мы рассмотрим наиболее распространенные проблемы с загрузкой пользовательского профиля и пути их решения.

Сообщение о препятствиях для входа в систему

В некоторых ситуациях при попытке регистрации в системе Windows Vista/7 вы можете получить сообщение, гласящее:

Служба "Служба профилей пользователей" препятствует входу в систему. Невозможно загрузить профиль пользователя

(The user profile service service failed the login. User profile cannot be loaded).

Каким образом следует бороться с такой ситуацией? Действуйте следующим образом:

1. В первую очередь, если у вас на компьютере имеются и другие пользовательские профили (желательно административные), попробуйте зарегистрироваться с помощью одного из них.

ПРИМЕЧАНИЕ

Если пользовательский профиль, с загрузкой которого возникли проблемы, — это профиль единственной учетной записи пользователя с административными правами, попробуйте загрузиться в безопасном режиме (Safe Mode). О том, как это сделать, рассказано в *главе 7*. В безопасном режиме регистрация в системе автоматически произойдет с использованием встроенной учетной записи **Администратор** (Administrator).

2. Запустите сеанс командной строки с административными правами и дайте команду `eventvwr.msc`. В системном журнале приложений вы найдете сообщение о событии неудачного входа в систему, выглядящее примерно так, как показано на рис. 10.22. Итак, вы видите, что пользователь **User1** не смог зарегистрироваться в системе, поскольку сервису пользовательских профилей не удалось найти указанный файл. Как уже говорилось ранее в этой главе, критически важные пользовательские профили находятся в папке `\Users\<Username>` раздела, на котором установлена Windows Vista/7. Причем критическое значение имеют файлы `Ntuser.dat` и `Ntuser.dat.log`. Поэтому для начала следует проверить, действительно ли файл `Ntuser.dat` для указанного пользовательского профиля присутствует на своем месте.

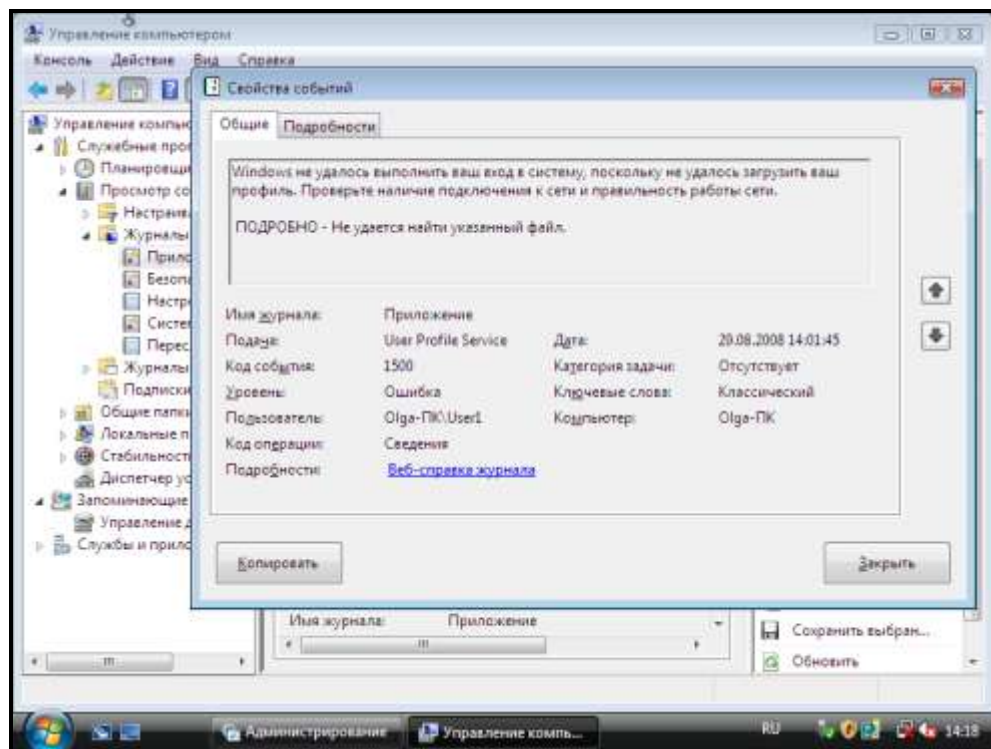


Рис. 10.22. Сообщение в системном журнале, содержащее информацию о неудавшейся попытке регистрации в системе

3. Фактически, файл `Ntuser.dat` представляет собой улей реестра, поэтому дальнейшее исследование проблемы мы будем производить с помощью Редактора реестра. Во-первых, можно попытаться загрузить этот улей

и посмотреть, действительно ли он поврежден. Во-вторых, просмотрите список профилей в составе ключа `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList` (рис. 10.23).

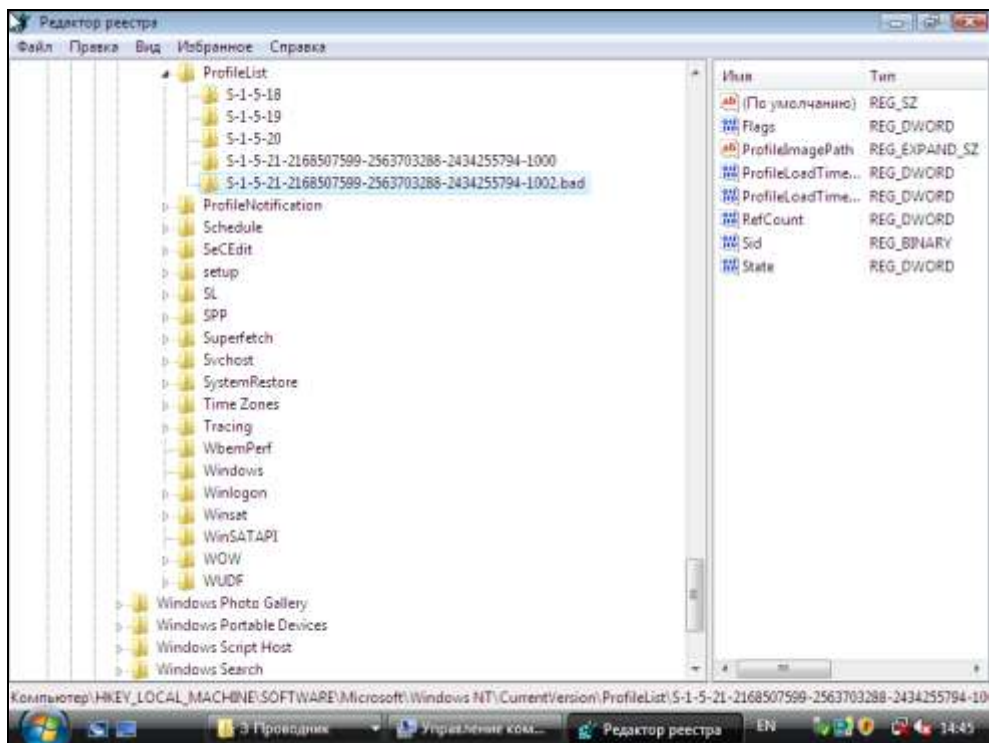


Рис. 10.23. Содержимое ключа реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList` показывает, что профиль пользователя все же действительно поврежден

4. Как уже говорилось ранее, для каждого пользовательского профиля в составе этого ключа имеется по одному подключу. Найдите подключ, соответствующий пользовательскому профилю, с загрузкой которого возникли проблемы. Если этот профиль действительно поврежден, то имя ключа будет заканчиваться на `.bad` (см. рис. 10.23). Кроме того, проверьте значения параметров `RefCount` и `State` в составе этого ключа. Если профиль не поврежден, они должны быть установлены на 0.
5. Если вы убеждены в том, что улей реестра повреждений не получил, и с профилем все в порядке, попробуйте для начала переименовать ключ и переустановить параметры `RefCount` и `State` на 0, после чего вы можете

попробовать повторить попытку регистрации в системе от имени данного пользователя.

6. В случае успеха можно считать, что задача решена. В случае неудачи вновь зарегистрируйтесь в системе от имени пользователя с административными правами, запустите редактор реестра и раскройте ключ `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList`. Найдите подключ для пользовательского профиля, с загрузкой которого возникли проблемы, и удалите его.
7. Затем запустите оснастку MMC `compmgmt.msc`, удалите учетную запись соответствующего пользователя, а затем вновь создайте учетную запись с тем же именем и теми же свойствами, что и удаленная учетная запись.
8. Попробуйте зарегистрироваться в системе от имени этого пользователя. В процессе регистрации будет создан новый пользовательский профиль с именем `\Users\<Username>`, а старый профиль будет переименован в `\Users\<Username>.old`.

Заключение

В этой главе рассмотрены файлы пользовательских профилей и системной политики. Кроме того, приведены инструкции по устранению проблем с загрузкой пользовательских профилей.

Глава 11



Диагностика и устранение проблем с загрузкой системы с помощью реестра

Если какая-нибудь неприятность может произойти, она случается.

Закон Мэрфи

Windows 7, безусловно, является наиболее надежной системой в семействе Windows — такого запаса прочности не было ни у одной из ее предшественниц, в том числе и у Windows Vista, не говоря уже о более ранних версиях, таких, как Windows XP. Означает ли это, что в Windows 7 не могут возникать проблемы с загрузкой? Вовсе нет. Любая операционная система может оказаться в таком состоянии, когда загрузка не выполняется, и Windows 7 — не исключение. Поэтому вы не должны испытывать чувство безысходности, столкнувшись с подобными проблемами. Считается, что проблемы такого рода носят самый сокрушительный характер (особенно, когда много срочной работы, а система не загружается). Что же делать в критической ситуации? Во-первых, не поддаваться панике. Во-вторых, постараться определить, что же именно препятствует загрузке системы.

Последовательность загрузки Windows Vista/7 была подробно описана в *главе 7*. Здесь же будут рассмотрены причины, по которым в процессе загрузки могут происходить неполадки и сбои, а также методика диагностики неполадок и пути решения возникшей проблемы.

В табл. 11.1 перечислены стадии загрузки Windows 7 и дано краткое пояснение процессов, происходящих на каждой из них при нормальном режиме загрузки.

Таблица 11.1. Краткое описание процесса загрузки Windows Vista/7

Стадия загрузки	Описание (для систем на базе процессоров x86)
Выполнение процедуры POST	Центральный процессор (Central Processor Unit, CPU) инициирует запуск встроенных подпрограмм POST самотестирования системной платы. После успешного завершения этих тестов, будут выполнены подпрограммы POST, осуществляющие тестирование отдельных адаптеров
Процесс начальной загрузки	Система осуществляет поиск загрузочного устройства в соответствии с установками порядка загрузки, хранящимися в CMOS. Если в качестве устройства загрузки указан жесткий диск, то системная BIOS считывает главную загрузочную запись (MBR) и загружает ее в память, а затем передает ей управление. Код, содержащийся в главной загрузочной записи, сканирует таблицу разделов в поисках системного раздела. Найдя системный раздел, MBR загружает в память его нулевой сектор и исполняет код, содержащийся в этом секторе. Сектор 0 на системном разделе, так называемый <i>загрузочный сектор раздела</i> (partition boot sector), содержит загрузочный код операционной системы — загрузочную запись раздела (Partition boot record, PBR). Этот код и осуществляет запуск операционной системы
Работа Менеджера загрузки bootmgr	На компьютерах x86 загрузочный сектор раздела Windows Vista/7 ищет Менеджер загрузки bootmgr и базу данных конфигурационной информации (BCD) в корневом каталоге системного раздела. Найдя Менеджер загрузки, код загрузочного сектора загружает его в память и передает ему управление. Менеджер загрузки выполняет две проверки целостности собственного кода, а затем проверяет, не находится ли компьютер в режиме сна или гибернации. Если это так, Менеджер загрузки находит загрузчик возобновления (Winresume.exe), загружает его в память и передает ему управление. Если компьютер не находился в состоянии сна или гибернации, то Менеджер загрузки находит базу данных BCD, читает хранящуюся в ней информацию и запускает остальные предзагрузочные приложения Windows (Windows pre-boot applications). Информация из системного хранилища BCD используется для отображения загрузочного меню. После того как пользователь выберет одну из опций загрузочного меню, bootmgr передаст управление загрузчику выбранной операционной системы — например, если выбрана одна из установленных копий Windows 7, будет вызван загрузчик Windows 7, расположенный в папке <code>%SystemRoot%\System32\WINLOAD.EXE</code>. Если на компьютере установлена еще одна операционная система, и пользователь выберет именно ее, управление будет передано загрузчику этой системы. Например, в случае с Windows Vista это будет загрузчик Windows Vista, расположенный в папке <code>%SystemRoot%\System32\WINLOAD.EXE</code>

Таблица 11.1 (продолжение)

Стадия загрузки	Описание (для систем на базе процессоров x86)
Работа Менеджера загрузки bootmgr	ПРИМЕЧАНИЕ Обратите внимание, что в данном случае %SystemRoot% обозначает каталог, в котором установлена копия Windows Vista, — в отличие от предыдущего случая, когда под тем же обозначением понимался каталог, в котором установлена копия Windows 7. Например, если Windows Vista установлена на первом разделе жесткого диска, а Windows 7 — на втором, то переменная окружения %SystemRoot% в каждом из случаев будет указывать на каталог \Windows в том разделе, где установлена копия системы, выбранной для загрузки. Наконец, если на компьютере установлена более ранняя версия Windows, например, Windows XP, то управление будет передано загрузчику этой операционной системы — в данном случае это будет файл NTLDR)
Загрузка операционной системы	Winload, новый загрузчик ядра, впервые появившийся в Windows Vista и, безусловно, присутствующий в Windows 7, загружает в память ядро операционной системы, файл %SystemRoot%\System32\ntoskrnl.exe, уровень аппаратных абстракций %SystemRoot%\System32\hal.dll и содержимое улья реестра %SystemRoot%\System32\config\system. Сразу же после загрузки улья реестра SYSTEM загрузчик Winload.exe выполняет проверку собственной целостности, а также наличие цифровых подписей у файлов, подлежащих загрузке. После этого Winload.exe загружает все драйверы устройств, которые должны загружаться на этой стадии запуска системы, а также все DLL режима ядра, импортируемые любыми из ранее упомянутых компонентов. После завершения этих операций управление передается ядру
Инициализация ядра	Ядро инициализирует систему в два этапа: сначала происходит инициализация самого ядра, а затем — инициализация всей системы. Ядро создает ключ HKEY_LOCAL_MACHINE\HARDWARE на основании информации, полученной от загрузчика, создает наборы управляющих опций и проверяет цифровые подписи всех драйверов, загружаемых на данном этапе, затем загружает и инициализирует сервисы и драйверы и запускает первый пользовательский процесс
Процесс регистрации пользователя в операционной системе	Сетевые компоненты (например, TCP/IP) загружаются асинхронно с другими службами, и на экране появляется приглашение зарегистрироваться. После успешной регистрации пользователя, Windows Vista и Windows 7 производят обновление конфигурационной информации из набора управляющих опций LastKnownGood

Таблица 11.1 (окончание)

Стадия загрузки	Описание (для систем на базе процессоров x86)
Обнаружение новых устройств посредством Plug and Play	Если Windows обнаруживает новые устройства, то им выделяются необходимые системные ресурсы. Windows Vista/7 извлекает требуемые файлы драйверов из архива Driver.cab. Если файл не найден, Windows сообщает пользователю о необходимости загрузки драйвера из другого источника. Определение нового устройства осуществляется асинхронно с процессом регистрации в системе

Диагностика неудачной загрузки

Как правило, проблемы, возникающие в процессе загрузки, более сложно устранять, нежели проблемы, возникающие в работающей системе, поскольку в первом случае в вашем распоряжении имеется лишь ограниченный набор диагностических средств, предоставляемых средой восстановления Windows (WinRE), а во втором — полный набор средств диагностики и мониторинга, предоставляемый операционной системой. К счастью, сбои в загрузке как Windows Vista, так и Windows 7 происходят редко, особенно, если вы регулярно выполняете техническое обслуживание и предупредительные действия. Однако вероятность возникновения проблемы существует. Точно так же, как и в других операционных системах, она может быть вызвана сбоями в работе аппаратных средств и ошибками программного обеспечения. Если возникший отказ носит серьезный характер, то загрузка системы прекращается, и на экране отображается сообщение об ошибке. Краткий перечень сообщений об ошибках и их значение представлены в табл. 11.2.

Таблица 11.2. Признаки неудачной загрузки

Признак (симптом)	Возможная причина и способ устранения
Программа POST выдает серию звуковых сигналов и отображает сообщения об ошибках, например: Hard disk error (Ошибка в работе жесткого диска) Hard disk absent/failed (Жесткий диск отсутствует или отказал)	Произошел останов программы самотестирования при включении (POST). Такой сбой называется <i>аппаратным</i> и возникает из-за неисправных или неверно установленных устройств
Не сохранены установки CMOS или NVRAM	Неисправность CMOS, повреждение данных или же необходимость замены внутреннего элемента питания

Таблица 11.2 (продолжение)

Признак (симптом)	Возможная причина и способ устранения
Сообщения об ошибках, связанные с главной загрузочной записью (Master boot record, MBR): Missing operating system (Операционная система отсутствует) Insert a system diskette and restart the system (Вставьте системную дискету и перезапустите систему)	MBR повреждена. Воспользуйтесь опцией Восстановление запуска (Startup Repair) среды восстановления Windows (WinRE)¹. Как вариант, можно воспользоваться режимом командной строки (Command Prompt). В опциях командной строки WinRE имеется команда <code>BootRec /FixMbr</code> — аналог команды <code>FIXMBR</code>, имевшейся в консоли восстановления (Recovery Console) Windows XP
Сообщения, связанные с ошибками таблицы разделов, например: Invalid partition table (Таблица разделов недействительна) A disk-read error occurred (Ошибка чтения диска)	Таблица разделов повреждена. В Windows Vista и Windows 7 сначала попытайтесь воспользоваться средой восстановления Windows (WinRE). Как и в предыдущем случае, простейший вариант заключается в использовании опции Восстановление запуска (Startup Repair). Как вариант, можно воспользоваться опциями командной строки, дав команды <code>BootRec /FixMbr</code> и <code>BootRec /FixBoot</code>
После установки еще одной операционной системы Windows Vista/7 не загружается	Загрузочный сектор Windows Vista/7 оказался перезаписан ("затерт") программой установки другой операционной системы. В Windows Vista/7 сначала попытайтесь воспользоваться средой восстановления Windows (WinRE). Как и в предыдущем случае, простейший вариант заключается в использовании опции Восстановление запуска (Startup Repair). Как вариант, можно воспользоваться опциями командной строки, дав команды <code>BootRec /FixMbr</code> и <code>BootRec /FixBoot</code>
Отсутствует какой-либо из файлов, необходимых для загрузки	Необходимые загрузочные файлы отсутствуют (утрачены) или повреждены, или же элементы (параметры), хранящиеся в базе данных BCD, указывают на неверный раздел

¹ О среде восстановления Windows (WinRE) и ее использовании для устранения проблем далее в этой главе будет рассказано подробно.

Таблица 11.2 (окончание)

Признак (симптом)	Возможная причина и способ устранения
Сообщение об ошибке загрузчика операционной системы <i>Winload.exe</i> : winload.exe..... is missing or corrupt.	Возможно, что файл загрузчика <i>Winload.exe</i> действительно отсутствует или получил повреждения. Кроме того, это же сообщение может быть вызвано некорректным изменением главной загрузочной записи (MBR) или базы данных загрузочной конфигурации (BCD), в результате чего Windows просто не может найти файл <i>Winload.exe</i> , который при этом может находиться на своем месте и быть вполне корректным. Поскольку Windows не находит загрузчика, процесс загрузки останавливается с выдачей этого сообщения
Сообщения об останове системы (STOP error , "синий экран смерти")	Существует множество возможных причин, вызванных неполадками программного и аппаратного обеспечения, которые будут рассмотрены далее в этой главе, а также в <i>главе 12</i>

В целом, проблемы с загрузкой Windows Vista/7 можно подразделить на следующие категории:

- ☐ проблемы на начальной стадии загрузки;
- ☐ проблемы, возникающие после прохождения тестов POST, но до появления индикатора загрузки ядра;
- ☐ проблемы, возникающие после появления индикатора загрузки ядра, но до появления окна интерактивного входа в систему;
- ☐ проблемы, возникающие после регистрации пользователя в системе.

Рассмотрим все эти проблемы более подробно.

Проблемы на начальной стадии загрузки и их устранение

Как правило, аппаратные проблемы, диагностируемые программой самотестирования при включении (POST), более сложны, нежели проблемы с конфигурацией программного обеспечения. Чтобы устранить проблемы, связанные с аппаратным обеспечением, следует внимательно ознакомиться с документацией, поставляемой с вашей системой, и выполнить основные проверки аппаратных средств. Необходимо тщательно проверить правильность подключения кабелей и внутренних адаптеров, убедиться, что все периферийные

устройства (например, клавиатура), от правильной установки и функционирования которых зависит нормальное выполнение программы POST, установлены и работают верно.

При необходимости проверьте правильность установки перемычек (джамперов) и DIP-переключателей. Это особенно важно в отношении установки жестких дисков. Запустите программу диагностики, позволяющую выявить неисправность в аппаратном обеспечении, и замените отказавшее устройство. Существенную помощь на этом этапе вам могут оказать следующие полезные информационные ресурсы:

- ☐ руководство BIOS Survival Guide: http://burks.bton.ac.uk/burks/pcinfo/hardware/bios_sg/bios_sg.htm;
- ☐ информация по диагностическим сигналам и сообщениям BIOS: <http://www.sysopt.com/tutorials/article.php/3552501>.

Если процедура POST прошла успешно, начнется процедура загрузки с использованием параметров, указанных в CMOS или NVRAM. В этом случае проверьте, правильно ли задана последовательность загрузки. На компьютерах на базе BIOS операционные системы могут запускаться со следующих устройств:

- ☐ CD/DVD-носители;
- ☐ жесткие диски и дискеты;
- ☐ флэш-накопители USB;
- ☐ сетевые адаптеры.

Типичное сообщение об ошибке, произошедшей на этой стадии загрузки, выглядит так:

Non-system disk or disk error

Replace and press any key when ready

Чаще всего эта проблема вызвана неправильной конфигурацией BIOS, проблемами с жесткими дисками или файловыми системами. Информацию о задании последовательности загрузки можно найти в сопроводительной документации к вашему компьютеру. Для этого войдите в программу BIOS Setup и убедитесь, что устройство, с которого требуется произвести загрузку операционной системы, указано первым в последовательности загрузки (Boot Sequence), а затем сохраните внесенные изменения.

ПРИМЕЧАНИЕ

Если вы желаете загружаться с накопителя флэш-USB (например, для выполнения аварийно-восстановительных работ), то имейте в виду, что в программе BIOS Setup этот накопитель должен быть виден как жесткий диск.

Учтите, что если сохранить изменения BIOS невозможно, то, скорее всего, проблема вызвана неисправностью CMOS, повреждением данных или же необходимостью замены внутреннего элемента питания. В этом случае проблема тоже является аппаратной, и проведение дальнейших работ будет невозможным без ее устранения. О замене микросхем CMOS хорошо рассказано в книге "BIOS: дизассемблирование, модификация, программирование"². Правда, стоит отметить, что если вы не обладаете достаточным опытом, не следует выполнять эту процедуру самостоятельно, лучше обратиться к квалифицированному специалисту по техническому обслуживанию.

Среда восстановления Windows

Основным средством устранения проблем, возникающих на начальной стадии загрузки, является среда восстановления Windows (Windows Recovery Environment, WinRE). Она, как правило, запускается с дистрибутивного DVD Windows 7. Кроме того, WinRE можно установить на жесткий диск, а также создать носители (CD или флэш-накопители USB) с копией WinRE.

ПРИМЕЧАНИЕ

О среде восстановления Windows вкратце уже говорилось в *главе 7*. Там упоминалось, что, начиная с Windows 7, среду восстановления Windows можно запускать из отладочного меню Windows 7, очень похожего на аналогичное меню Vista с одним лишь отличием — в нем первым пунктом является строка **Устранение неполадок компьютера** (Troubleshoot computer problems), которой в Windows Vista не было. Именно эта опция меню и запускает WinRE. Таким образом, в Windows 7 уже нет необходимости устанавливать WinRE на жесткий диск, потому что она может быть запущена из отладочного меню. Тем не менее, как будет показано далее, такой способ запуска WinRE имеет некоторые ограничения, так что пользователи мультizaгрузочных систем, а также специалисты по технической поддержке по-прежнему должны быть заинтересованы в дополнительных возможностях WinRE.

Рассмотрим дополнительные опции WinRE чуть более подробно, нежели это было сделано в *главе 7*.

Для этой цели нам потребуются:

- ☐ дистрибутивный DVD-диск с инсталляционной копией Windows 7;
- ☐ установочный диск с продуктом Windows Automated Installation Kit (WAIK)³.

² Дармаван Салихан. BIOS: дизассемблирование, модификация, программирование: Пер. с англ. — СПб.: БХВ-Петербург, 2007 (<http://www.bhv.ru/books/book.php?id=180728>).

³ Этот продукт можно бесплатно скачать здесь:

<http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=696dd665-9f76-4177-a811-39c26d3b3b34>.

Шаг 1. Установка Windows Automated Installation Kit (WAIK)

Чтобы создать носитель с WinRE или установить WinRE на жесткий диск, вам потребуется проделать следующее:

1. Скачать с сайта Microsoft продукт Windows Automated Installation Kit.
2. Поскольку Windows AIK поставляется в виде файла образа (ISO), после завершения загрузки необходимо "прожечь" образ на чистый носитель DVD.

СОВЕТ

Одной из долгожданных и очень удобных возможностей, появившихся в Windows 7, является непосредственная запись ISO-образов на носители CD и DVD. Таким образом, чтобы подготовить дистрибутивный носитель, вам больше не требуется никакое дополнительное программное обеспечение. Выполнив двойной щелчок мышью по имеющемуся ISO-файлу, вы раскроете окно, показанное на рис. 11.1. Воспользуйтесь этой новой возможностью, и подготовьте DVD-носитель с продуктом WAIK.

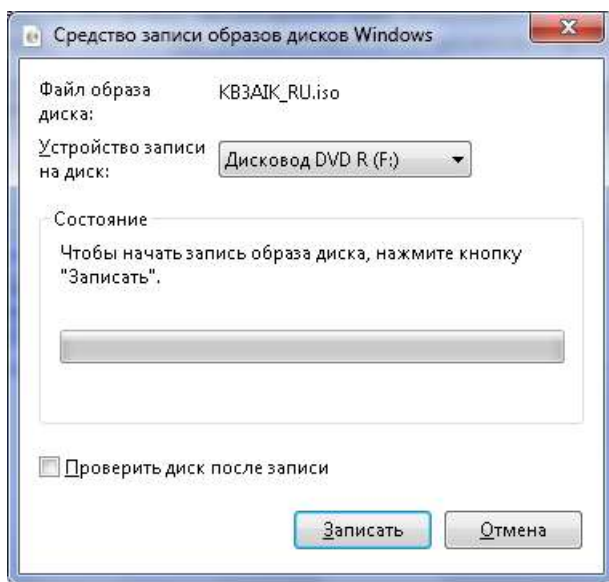


Рис. 11.1. Прожиг дистрибутивного DVD с WAIK с помощью встроенного средства записи образов дисков, появившегося в Windows 7

3. С подготовленного носителя установить Windows Automated Installation Kit на компьютер, работающий под управлением Windows 7, Windows Vista

с Service Pack 1 (SP1), Windows Server 2008 R2 или Windows Server 2008 (рис. 11.2).

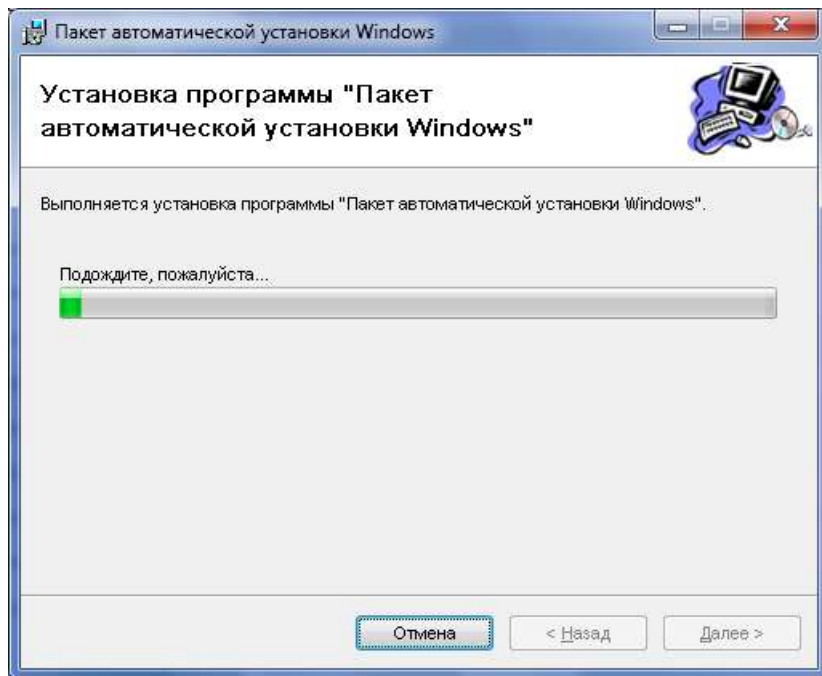


Рис. 11.2. Установка Windows Automated Installation Kit

ПРИМЕЧАНИЕ

Программный продукт Windows AIK предназначен для профессиональных специалистов в области ИТ. В комплекте с ним поставляется подробная документация, которую ответственным администраторам настоятельно рекомендуется внимательно изучить.

Шаг 2. Создание среды WinRE

На данном этапе вам потребуется дистрибутивный диск Windows 7 для копирования всех необходимых файлов среды восстановления Windows. Итак,

1. На компьютере, где установлен программный продукт WAIK, войдите в систему как пользователь **Администратор** (Administrator). Из меню **Пуск** (Start) выберите опции **Все программы** (All Programs) | **Microsoft Windows AIK** | **Командная строка средств развертывания** (Deployment Tools Command Prompt), как показано на рис. 11.3.

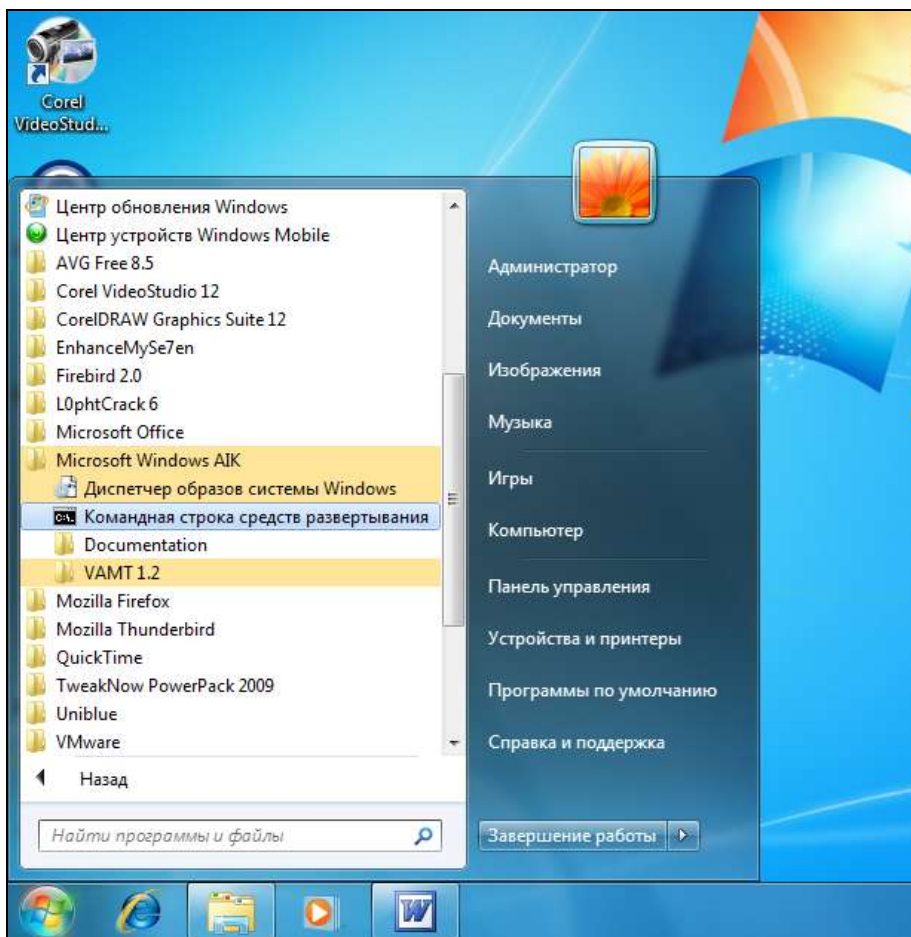


Рис. 11.3. Вызов командной строки для запуска средств развертывания

2. Создайте каталог для образа Windows Preinstallation Environments (Windows PE), точку монтирования и скопируйте в созданный каталог файл образа. Для этой цели дайте из командной строки следующую команду:

```
copyype.cmd <arch> <destination>
```

Здесь *<arch>* — имя архива, из которого должно производиться копирование, а *<destination>* — имя каталога, в который должны копироваться файлы. Параметр *<arch>* может принимать следующие значения:

- x86 — 32-разрядные версии Windows 7;
- Amd64 — 64-разрядные версии Windows 7;

- Ia64 — 64-разрядные версии Windows 7 для платформы Itanium.

Например (рис. 11.4):

```
copyre.cmd x86 c:\winre_x86
```

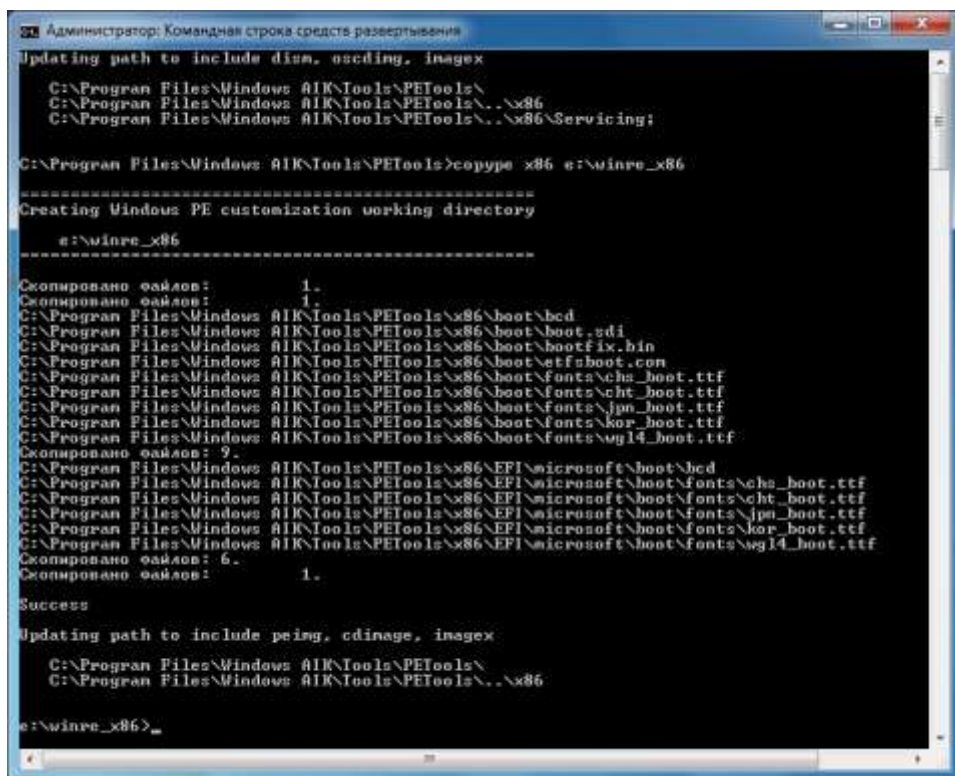


Рис. 11.4. Работа скрипта *copyre.cmd*

В результате работы скрипта будет создана следующая структура каталогов (рис. 11.5):

```
C:\winre_x86
```

```
C:\winre_x86\ISO
```

```
C:\winre_x86\mount
```

3. Вставьте в привод DVD дистрибутивный диск Windows 7 и дайте следующие команды:

```
imagex.exe /export /boot <DVD_Drive>\sources\boot.wim 2
c:\winre_x86\winre.wim "Windows Recovery Environment"
```

```
imagex.exe /mountrw c:\winre_x86\winre.wim 1 c:\winre_x86\mount
```

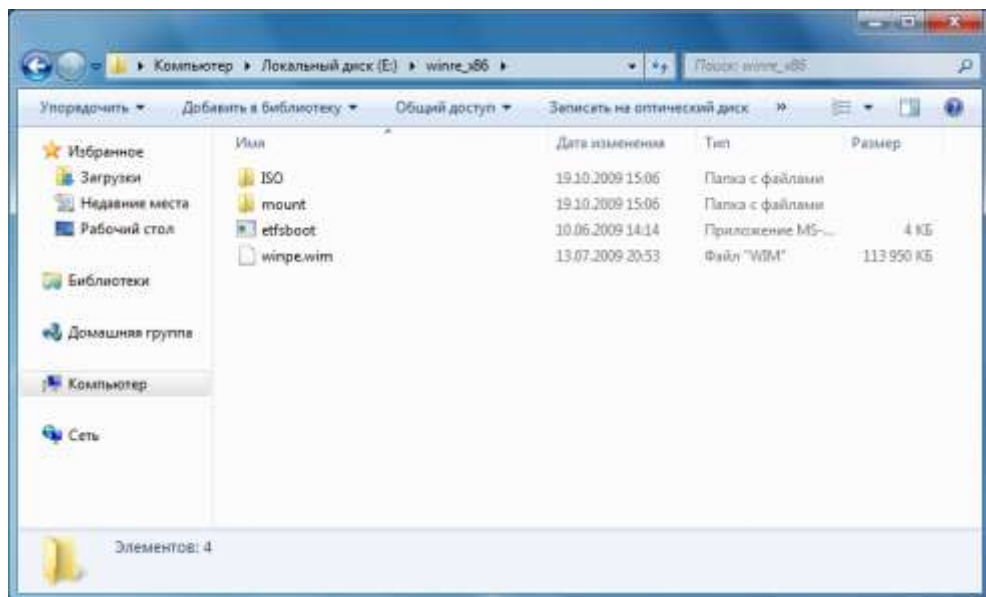


Рис. 11.5. Структура каталогов, создаваемая в результате работы скрипта *corrupt.cmd*

ПРИМЕЧАНИЕ

На данном этапе, пользуясь продуктом WAIK, вы можете добавить дополнительные скрипты WinRE, пакеты Windows PE и дополнительные драйверы, а также индивидуальные утилиты для среды восстановления Windows. Подробная информация по этому вопросу содержится в сопроводительной документации к продукту WAIK.

Шаг 3. Настройка среды WinRE

Теперь вы можете настроить различные варианты использования среды WinRE, в частности:

- ☐ создать образ DVD, содержащего среду WinRE. Это удобно, если у вас нет возможности постоянно носить с собой дистрибутивный диск Windows 7;
- ☐ скопировать WinRE на носитель флэш-USB — вы получите удобную USB-версию WinRE, которую можно будет постоянно иметь при себе и применять на большинстве современных компьютеров, поддерживающих загрузку с устройств USB;
- ☐ установить WinRE на жесткий диск компьютера, работающего под управлением Windows 7.

Рассмотрим все эти варианты более подробно.

Создание DVD для аварийного восстановления Windows 7

Чтобы создать DVD со средой восстановления Windows 7, проделайте следующее:

1. Создайте образ диска для восстановления незагружаемой системы Windows 7. Для этого скопируйте вновь созданный образ WinRE в каталог `ISO\Sources` и переименуйте этот файл в `boot.wim`, например:

```
copy c:\winre_x86\winre.wim c:\winre_x86\ISO\sources\boot.wim
```

2. Создайте образ загрузочного диска, запускающего среду WinRE. Это делается с помощью утилиты `oscdimg`, входящей в состав WAIK:

```
oscdimg -n -bc:\winre_x86\etfsboot.com c:\winre_x86\ISO  
c:\winre_x86\winre_x86.iso
```

3. Прожгите созданный образ на "болванку". Учтите, что если вы включите в состав создаваемого образа большое количество дополнительных драйверов и индивидуальных средств восстановления поврежденной системы, вам может потребоваться даже не CD, а DVD-носитель.

Создание USB-носителя для загрузки WinRE

Носители флэш-USB нашли самое широкое применение. Здесь будет рассказано еще об одном удобном варианте их использования для аварийного восстановления незагружаемых операционных систем Windows 7. Проделайте следующее:

1. Возьмите носитель флэш-USB 2.0 объемом не менее 512 Мбайт.

ВНИМАНИЕ!

Обратите внимание, что носитель должен быть именно USB 2.0, так как в противном случае ничего у вас не получится. Кроме того, лучше всего взять носитель большого объема (примерно 2–4 Гбайт), поскольку это очень удобно для переноса данных.

2. Отформатируйте USB-носитель, работая под управлением Windows 7. Для чего запустите сеанс командной строки и дайте следующие команды:

```
diskpart  
select disk 1  
clean  
create partition primary  
select partition 1  
active  
format fs=fat32  
assign  
exit
```

СОВЕТ

В приведенном примере команд USB-носитель — это disk 1. Если в системе установлено несколько жестких дисков, то этот номер будет другим (например, disk 2). Поэтому, прежде чем очищать и форматировать USB-носитель, проверьте, какой номер диска он имеет, иначе вы затрете свои важные данные. Увидеть номера дисков компьютера можно, отдав сразу после команды diskpart команду list disk.

3. Скопируйте в папку C:\winre_x86\iso все утилиты, доступ к которым вам требуется иметь в WinRE (например, imageh.exe, wimscript.ini).
4. Скопируйте файлы WinRE в корневой каталог USB-носителя:

```
xcopy c:\winre_x86\iso\*. * /s /e /f <USB-drive>:\
```

Теперь вы сможете загружать WinRE на любом компьютере, поддерживающем загрузку с USB-носителей.

ПРИМЕЧАНИЕ

Наиболее сложной задачей является установка WinRE на жесткий диск. Здесь основную проблему представляет собой выбор раздела, на который будет производиться установка. Читателям, всерьез заинтересовавшимся данным вопросом, рекомендуется внимательно прочесть официальную документацию Microsoft для Windows 7 и Windows Server 2008 (на русском языке) по следующему адресу: [http://technet.microsoft.com/ru-ru/library/dd744280\(WS.10\).asp](http://technet.microsoft.com/ru-ru/library/dd744280(WS.10).asp).

Запуск среды восстановления Windows

Для устранения проблем начальной стадии загрузки следует загрузить компьютер с инсталляционного DVD Windows 7 или заглавременно созданного загрузочного носителя с копией WinRE, выбрать нужный язык установки (рис. 11.6), нажать кнопку **Далее** (Next) и в следующем окне выполнить щелчок мышью на ссылке **Восстановление системы** (Repair Your Computer) в нижней части экрана (рис. 11.7). После этого запустится среда восстановления Windows (WinRE), и вам будет предложено выбрать операционную систему для восстановления (рис. 11.8).

ПРИМЕЧАНИЕ

Если запустить среду восстановления, выбрав первую строку из отладочного меню, выводимого по нажатию клавиши <F8>, то среда восстановления не будет предлагать выбрать операционную систему, которую вы хотите восстановить. Вам будет предложено только выбрать язык и раскладку клавиатуры, а затем ввести пароль (см. главу 7). Таким образом, восстановить можно будет только одну систему.

Когда вы выберете операционную систему, подлежащую восстановлению, на экране откроется окно с параметрами восстановления системы, показанное на рис. 11.9.



Рис. 11.6. Выбор устанавливаемого языка



Рис. 11.7. Для запуска WinRE следует выполнить щелчок мышью на ссылке **Восстановление системы** в нижней части окна **Установка Windows**

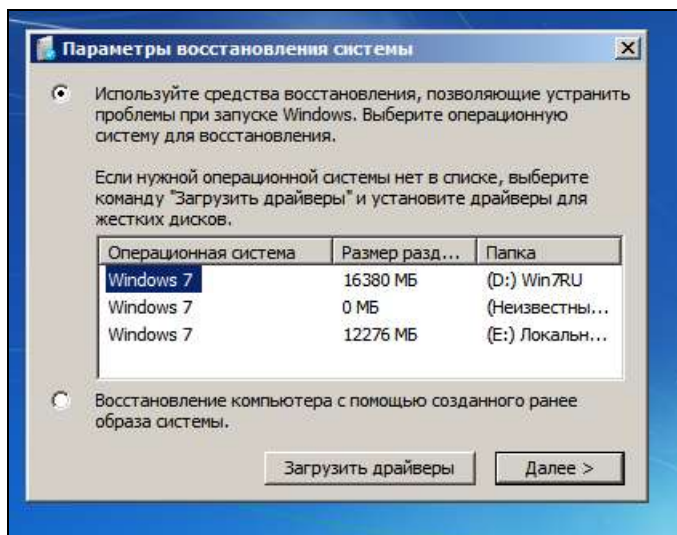


Рис. 11.8. В окне, выведенном WinRE, вам будет предложено выбрать копию Windows 7, подлежащую восстановлению

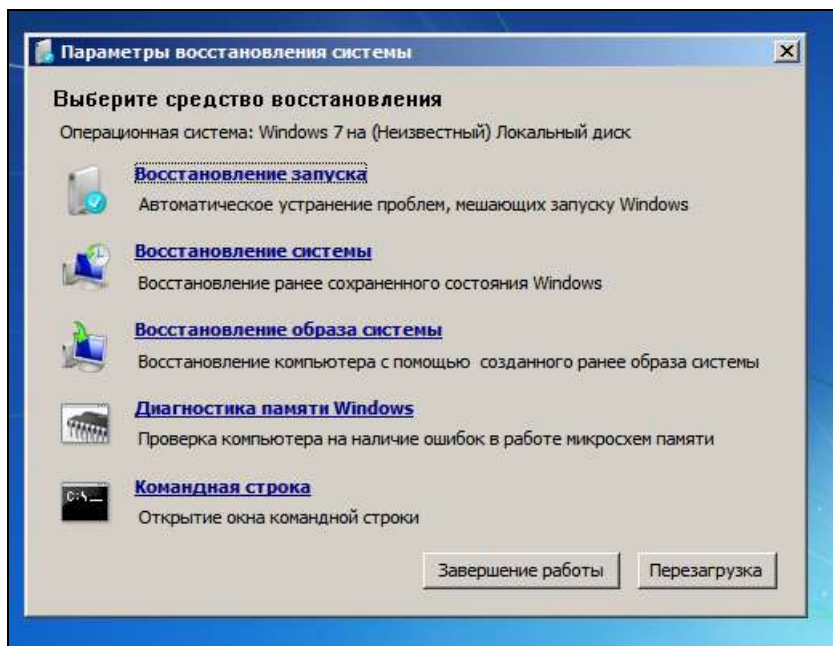


Рис. 11.9. Опции восстановления незагружаемой системы, предоставляемые средой восстановления Windows 7

Опции среды восстановления Windows

Опции среды восстановления Windows уже были вкратце рассмотрены в *главе 7*, поэтому здесь мы их просто перечислим, а более подробно остановимся на тех случаях, когда WinRE не справляется с поставленной задачей. Итак, среда восстановления WinRE предоставляет пять различных путей для восстановления системы после возникновения проблем, препятствующих загрузке (см. рис. 11.9):

- ☐ **Восстановление запуска** (Startup Repair);
- ☐ **Восстановление системы** (System Restore);
- ☐ **Восстановление образа системы** (System Image Restore);
- ☐ **Диагностика памяти Windows** (Windows Memory Diagnostics Tool);
- ☐ **Командная строка** (Command Prompt).

Опция *Восстановление запуска*

Опцию **Восстановление запуска** (Startup Repair) следует использовать для автоматического устранения проблем, препятствующих началу загрузки Windows. К их числу относятся проблемы, вызванные поврежденной главной загрузочной записью, затертым загрузочным сектором раздела, повреждениями загрузочного менеджера (bootmgr), а также отсутствующими или поврежденными файлами, необходимыми для загрузки Windows 7, список которых был приведен в *главе 7* (см. табл. 7.1). Например, на рис. 11.10 показан пример сообщения об ошибке, вызванного сбоем жесткого диска.

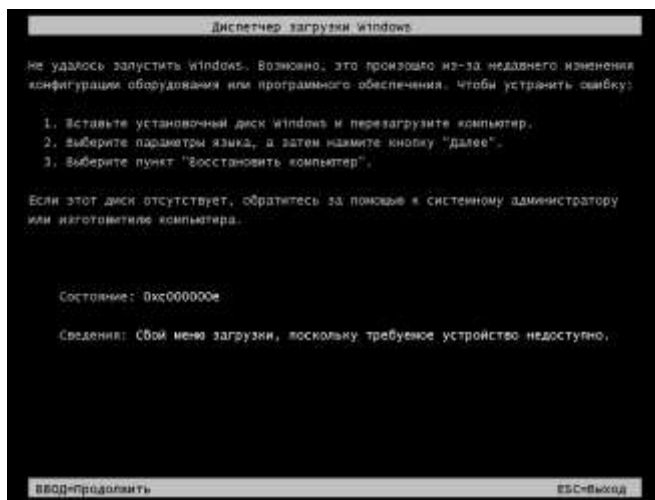


Рис. 11.10. Сообщение о невозможности загрузки Windows 7, вызванное сбоем жесткого диска

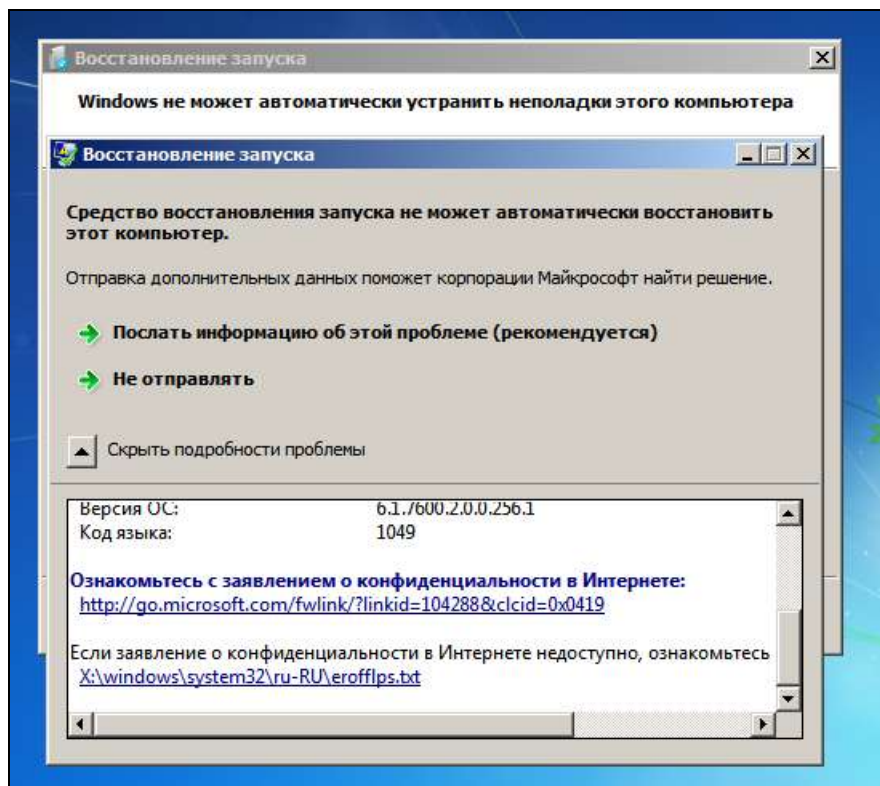


Рис. 11.11. Процесс автоматического восстановления незагружаемой системы хоть и редко, но может закончиться неудачей

В большинстве случаев ваши проблемы будут успешно решены. Но даже если этого не произойдет (рис. 11.11), в вашем распоряжении останутся и другие возможности восстановления. Стоит также отметить, что в случае неудачи рекомендуется повторить попытку.

Опция **Восстановление системы**

Опция **Восстановление системы** (System Restore) подобна аналогичной опции, имевшейся в Windows XP. Она используется для отката системы к состоянию, зафиксированному одной из предварительно созданных точек восстановления. Однако, начиная с Windows Vista, эта функция стала более удобной в использовании и может быть запущена из WinRE. Таким образом, даже если проблемы, возникшие в системе, настолько серьезны, что препятствуют загрузке, вы все же сможете выполнить откат к одной из имеющихся точек восстановления.

ВНИМАНИЕ!

Если у вас установлена система с двойной или даже тройной загрузкой, где кроме Windows Vista/7 существует еще и Windows XP или Windows Server 2003, то вы столкнетесь с проблемой несовместимости реализаций функции восстановления системы в Windows Vista/7 и более ранних версиях Windows. Результатом этого является затирание точек восстановления Windows Vista/7 после того, как вы загрузитесь и поработаете в Windows XP. Как уже неоднократно говорилось ранее, Windows XP не распознает точек восстановления, созданных более поздними версиями Windows: Vista и 7. Во избежание порчи точек восстановления она их просто удаляет. Спрячьте от Windows XP раздел, на котором установлены Windows Vista или Windows 7 – и проблема будет решена. Сделайте это сразу же, например, следующим способом: предположим, что Windows XP установлена на первом разделе жесткого диска (C:), а Windows Vista или Windows 7 — на втором (D:). Загрузитесь в Windows XP, запустите редактор реестра и найдите ключ `HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices\Offline`. В состав этого ключа добавьте параметр `\DosDevices\D:` с типом данных `REG_DWORD` и установите для него значение 1. Если подключ `HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices\Offline` не существует, его следует создать вручную.

Опция Восстановление образа системы

Опция **Восстановление образа системы** (System Image Restore) доступна только в Windows 7 Professional, Enterprise и Ultimate. Как явствует из ее названия, она предназначена для восстановления системы на основании предварительно созданной резервной копии образа диска. Резервная копия может храниться на внутренних или внешних жестких дисках, а также на одном или нескольких носителях DVD. В тех случаях, когда на компьютере уже нет установленной копии Windows 7 (так бывает в случаях отказа и последующей замены жесткого диска), ранее сохраненный образ может использоваться для запуска процедуры восстановления. При этом вам нет необходимости пользоваться отдельными утилитами для разбиения диска на разделы. Средство **Восстановление образа системы** (System Image Restore) автоматически разобьет и отформатирует жесткий диск.

ВНИМАНИЕ!

На эту опцию не следует рассчитывать любителям мультизагрузочных систем, в которых первый раздел жесткого диска отформатирован с использованием файловой системы FAT32, о чем тоже уже говорилось в *главе 2*.

Опция Диагностика памяти Windows

Опция **Диагностика памяти Windows** (Windows Memory Diagnostic Tool) предназначена для тестирования модулей памяти. Как известно, дефектные или несовместимые модули памяти могут приводить к сбоям как в Windows Vista, так и в Windows 7.

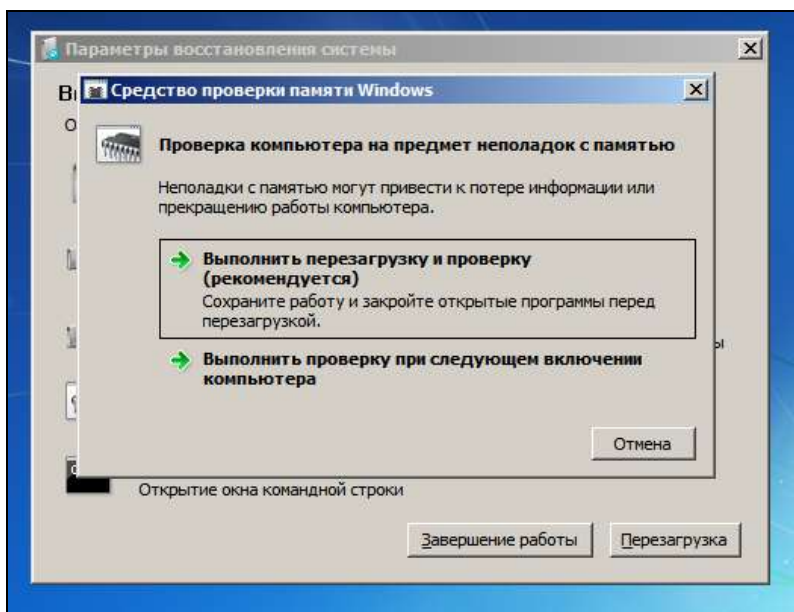


Рис. 11.12. Средство диагностики памяти Windows позволяет выполнить проверку компьютера на предмет неполадок с памятью

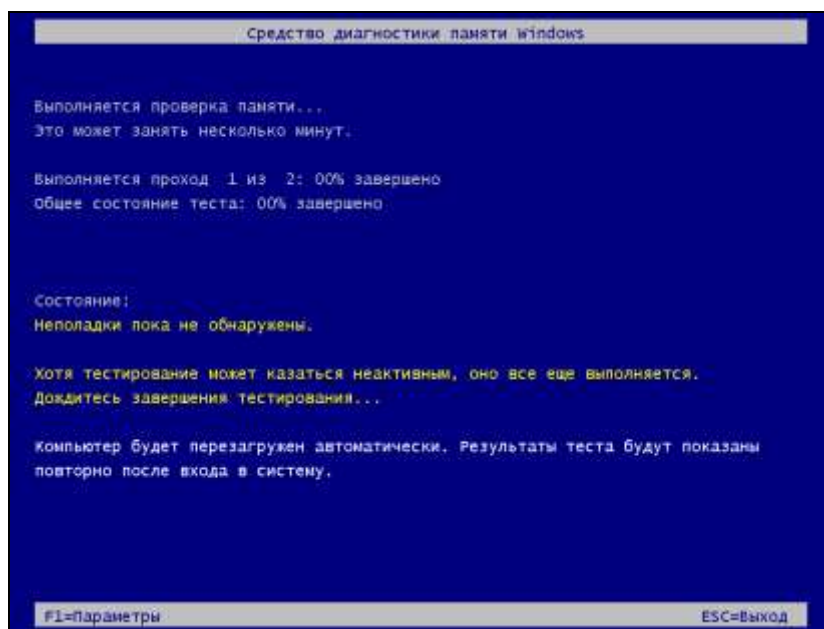


Рис. 11.13. Средство диагностики памяти Windows за работой

Чтобы выявить такие проблемы, запустите средство диагностики памяти Windows, выбрав опцию **Диагностика памяти Windows** (Windows Memory Diagnostics Tool) в окне WinRE (см. рис. 11.9). На экране появится окно, показанное на рис. 11.12. Выберите первую опцию из списка, и средство диагностики памяти Windows выполнит двукратную проверку памяти (рис. 11.13) — до и после запуска графической оболочки Windows.

Опция Командная строка

Опция **Командная строка** (Command Prompt), в отличие от консоли восстановления Windows XP, которая в основном была предназначена для ручного восстановления поврежденных системных файлов, позволяет запускать любые утилиты командной строки, в том числе программы для множественного копирования файлов (например, `xcopy` или `robocopy`). С ее помощью можно скопировать данные с поврежденной системы на другие диски, в том числе — на внешние носители USB, а также форматировать носители CD/DVD-RW и копировать на них данные. Наконец, из командной строки доступны аналоги многих команд, которые ранее были доступны через консоль восстановления. Краткий список аналогов команд, которые ранее были доступны из Recovery Console, приведен в табл. 11.3.

Таблица 11.3. Команды Recovery Console в Windows XP и их аналоги, доступные через опцию **Командная строка** в WinRE

Команда Консоли восстановления (Recovery console) в Windows XP	Аналог в Windows RE
BootCfg	BootRec /ScanOS BootRec /RebuildBcd bcdedit
FixBoot	BootRec /FixBoot
FixMBR	BootRec /FixMbr
Map	DiskPart
Logon	Не требуется
LISTSVC	Отсутствует
ENABLE	Отсутствует
DISABLE	Отсутствует
SYSTEMROOT	Не требуется

Все остальные команды, ранее доступные через Recovery Console, остались без изменений. Что касается отсутствующих команд, относящихся к управ-

лению сервисами (`listsvc`, `enable` и `disable`), то в WinRE вы можете вручную запустить из командной строки Редактор реестра и вручную загружать необходимые ульи.

Восстановление поврежденной системы с помощью опции **Восстановление запуска**

В первую очередь следует попытаться выполнить автоматическое восстановление поврежденной системы, выбрав опцию **Восстановление запуска** (Startup Repair). Однако в ряде случаев процедура восстановления запуска может не справиться с поставленной задачей и запуститься повторно (см. рис. 11.11).

Почему же могут произойти такие ситуации? Чтобы ответить на этот вопрос, следует знать, какие проблемы процедура восстановления запуска решать может, а какие, увы, нет. Итак, процедура восстановления при запуске автоматизирует устранение следующих проблем:

- ☐ повреждения реестра;
- ☐ отсутствующие или поврежденные системные файлы и файлы драйверов;
- ☐ поврежденные метаданные жесткого диска (MBR, таблица разделов, загрузочный сектор);
- ☐ поврежденные метаданные файловой системы;
- ☐ установка проблемных или несовместимых драйверов;
- ☐ установка несовместимых с Windows Vista/7 патчей или пакетов обновлений;
- ☐ поврежденные данные загрузочной конфигурации;
- ☐ аппаратные проблемы — дефектная память или физические повреждения жесткого диска (эти проблемы будут обнаружены, но исправить их с помощью WinRE, разумеется, не удастся).

При этом опция восстановления запуска принципиально не может устранить следующие проблемы:

- ☐ проблемы с микропрограммным обеспечением (BIOS или EFI), а также дефекты прочих аппаратных компонентов;
- ☐ проблемы, возникшие при первичной установке Windows Vista/7 или при попытке обновления Windows XP до Windows Vista/7;
- ☐ ошибки, связанные с регистрацией в системе;
- ☐ проблемы, вызванные заражением компьютера вирусами или другим вредоносным ПО.

После того как средство **Восстановление запуска** (Startup Repair) отработает, в каталоге %WINDIR%\System32\LogFiles\Srt будет создан текстовый файл журнала — SrtTrail.txt. В этом файле будет содержаться диагностическая информация, выявленная в ходе тестирования конфигурации, а также результаты (успех или неудача) выполненных восстановительных операций.

Анализ файла журнала SrtTrail.txt

Рассмотрим структуру этого файла более подробно, так как его внимательный разбор поможет выявить истинную причину ошибки. Пример содержимого первого раздела этого файла показан на рис. 11.14. Краткое описание полей файла приведено в табл. 11.4.

Следующий раздел файла журнала содержит описание выполненных диагностических процедур (рис. 11.16).

Поля этого раздела кратко описаны в табл. 11.5.

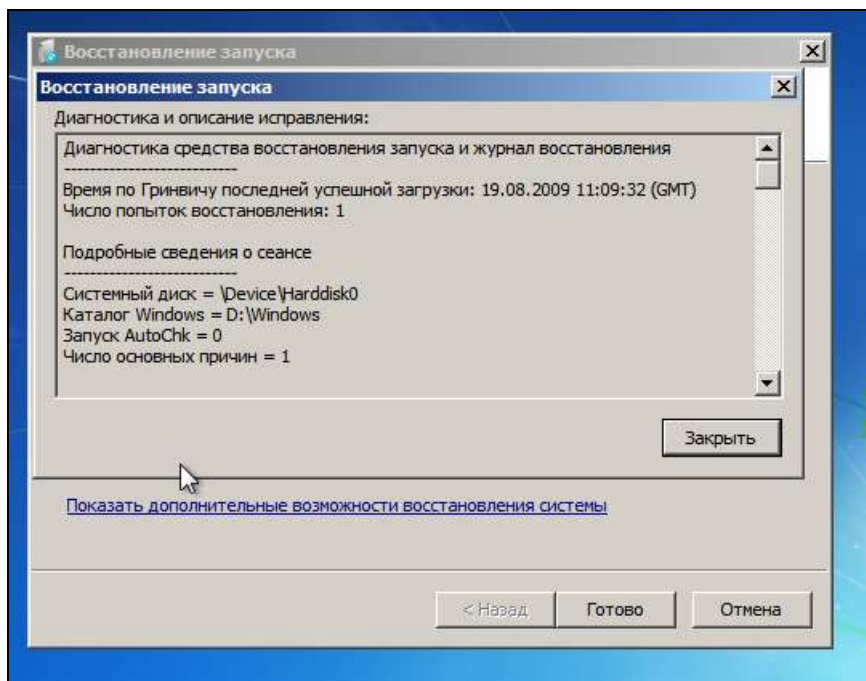


Рис. 11.14. Содержимое первого раздела файла журнала %WINDIR%\System32\LogFiles\Srt\SrtTrail.txt, протоколирующего процесс восстановления запуска

Таблица 11.4. Описание полей первой части файла журнала
%WINDIR%\System32\LogFiles\Srt\SrtTrail.txt

Поле	Описание
Системный диск (System Disk)	Путь к устройству для диска, на котором была обнаружена установленная копия Windows Vista/7, имеющая проблемы с запуском
Каталог Windows (WinDir)	Полный путь к каталогу, в котором установлена копия Windows Vista/7, попытка восстановления которой была предпринята
Запуск AutoChk (AutoChk Run)	Если в этом поле содержится значение 0, это значит, что программа AutoChk в процессе загрузки не запускалась (рис. 11.12). Если это поле имеет ненулевое значение, то в процессе загрузки Windows RE была запущена программа AutoChk (на рис. 11.15 она показана за работой)
Число основных причин (Root causes)	Количество основных проблем, препятствующих загрузке, обнаруженных в процессе выполнения диагностических процедур

```

Checking file system on F:
The type of the file system is NTFS.
Volume label is win7RU.

A disk check has been scheduled.
Windows will now check the disk.

CHKDSK is verifying files (stage 1 of 5)...
43264 file records processed.
File verification completed.
34 large file records processed.
0 bad file records processed.
2 EA records processed.
63 reparse records processed.
CHKDSK is verifying indexes (stage 2 of 5)...
14 percent complete. (44976 of 63270 index entries processed)

```

Рис. 11.15. Программа AutoChk за работой

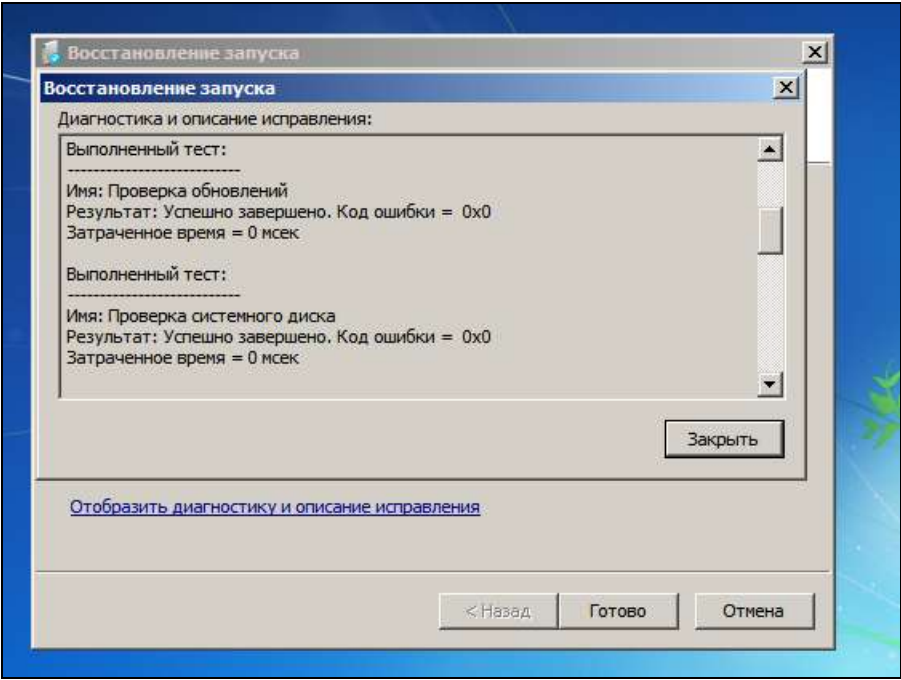


Рис. 11.16. Второй раздел файла журнала %WINDIR%\System32\LogFiles\Srt\SrtTrail.txt содержит описания выполненных диагностических процедур

Таблица 11.5. Поля второго раздела файла журнала %WINDIR%\System32\LogFiles\Srt\SrtTrail.txt

Поле	Описание
Имя (Name)	Наименование выполненного теста
Результат (Result)	Текстовое описание результата выполнения теста (например: Успешно завершено)
Код ошибки (Error code)	Код ошибки, возвращенный диагностической процедурой. Значение 0x0 указывает на то, что данный тест был успешно завершен
Затраченное время (Time taken)	Временной интервал (в миллисекундах), затраченный на выполнение данной диагностической процедуры

Краткий список тестов, выполняемых при выборе опции **Восстановление запуска** (Startup Repair), с краткими описаниями приведен в табл. 11.6.

Таблица 11.6. Краткий список тестов, выполняемых WinRE при выборе опции *Восстановление запуска*

Диагностическая операция	Описание
Тестирование метаданных диска (Disk metadata test)	Выполняется проверка целостности метаданных жесткого диска: главной загрузочной записи (MBR), таблицы разделов (partition table), а также загрузочного сектора (boot sector)
Определение целевой ОС (Determine target OS)	Цель данного теста — определение местоположения установленной копии Windows Vista/7 на основе базы данных загрузочной конфигурации (Boot Configuration Data, BCD)
Тестирование ульев реестра (Registry hives test)	Проверка целостности ульев реестра
Быстрое тестирование метаданных тома (Quick volume metadata test)	Проверка существования каталога, в который установлена операционная система Windows Vista/7
Диагностика журнала событий (Event log diagnosis)	Проверка журнала событий Windows Vista/7 и выявление важных событий, произошедших за последнее время
Проверка статуса загрузки (Boot status test)	Проверка флага, указывающего на успешность загрузки Windows Vista/7. В процессе запуска загрузчик Winload.exe устанавливает флаг статуса загрузки, сигнализируя таким образом о том, что загрузка ОС началась. Как правило, этот флаг сбрасывается при появлении экрана, приглашающего пользователя зарегистрироваться в системе. Если в процессе загрузки произошел сбой, флаг сброшен не будет, и при следующей попытке загрузки загрузчик будет подразумевать, что процесс запуска завершился неудачей
Проверка статуса установки (Setup state check)	Цель этого теста — выявление сбоев в процессе установки Windows
Анализ аварийных дампов (Bugcheck analysis)	Этот тест анализирует аварийные дампы, создаваемые при падении системы в "синий экран" в процессе загрузки
Диагностика журналов установки программного обеспечения (Software installation log diagnosis)	Данный тест проверяет, не производилась ли в последнее время установка нового программного обеспечения или пакетов обновлений
Диагностика сбоев жесткого диска (Disk failure diagnosis)	Данный тест проверяет статус SMART (Self-Monitoring, Analysis, and Reporting Technology) для жесткого диска
Chkdsk	Запуск Chkdsk с целью идентификации проблем с метаданными системы

Таблица 11.6 (окончание)

Диагностическая операция	Описание
Проверка целостности двоичных файлов (Binary file integrity test)	Проверка целостности двоичных файлов во время запуска системы
Тестирование списков контроля доступа (ACL test)	Данный тест проверяет корректность списков контроля доступа всех файлов, необходимых для загрузки системы

Основные причины сбоев при загрузке, отражаемые в файле журнала *SrtTrail.txt*

Если в процессе выполнения диагностики WinRE обнаруживает причину сбоя, эта причина будет отражена в файле журнала (рис. 11.17). Поля соответствующего раздела файла журнала описаны в табл. 11.7, а основные проблемы, препятствующие загрузке Windows Vista/7, которые могут быть обнаружены опцией WinRE **Восстановление запуска**, описаны в табл. 11.8.

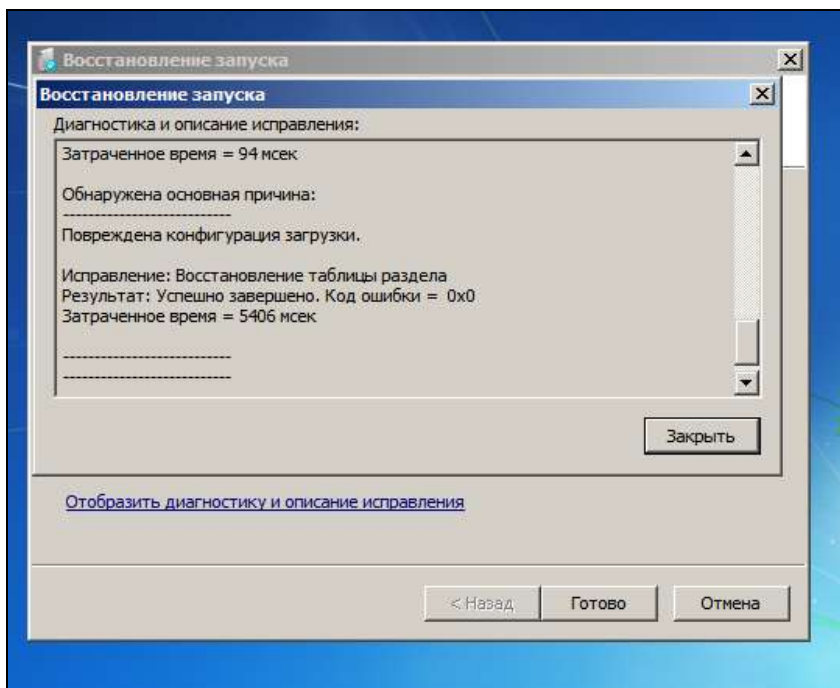


Рис. 11.17. Windows RE обнаружила и успешно исправила причину сбоя при загрузке

Таблица 11.7. Поля, описывающие выявленную проблему, препятствующую загрузке Windows Vista/7

Поле	Описание
Обнаружена основная причина (Root cause found)	Текстовое описание обнаруженной проблемы
Исправление (Repair action)	Название выполненной операции
Результат	Текстовое описание результата предпринятых действий (успех или неудача)
Код ошибки (Error code)	Код ошибки, возвращенный процедурой восстановления. Значение 0×0 указывает, что процедура была успешно выполнена

Таблица 11.8. Возможные причины, препятствующие загрузке Windows Vista/7

Причина сбоя	Описание
Менеджер загрузки не смог обнаружить загрузчик операционной системы (Boot manager failed to find OS loader)	Файл Winload.exe отсутствует или получил повреждения. Как уже упоминалось в главе 7, в данном случае вполне возможна и такая ситуация, когда Winload.exe вполне исправен и находится на своем месте, а появление ошибки вызвано повреждением MBR
Поверждена загрузочная конфигурация (Boot configuration is corrupt)	Файл загрузочной конфигурации (BCD) поврежден или содержит некорректные данные
Отсутствует файл <имя файла>, необходимый для загрузки (Boot critical file <filename> is missing)	Файл, имя которого указано в сообщении, отсутствует
Необходимый для загрузки файл <имя файла> поврежден	Файл, имя которого указано в сообщении, поврежден
Несколько файлов, необходимых для загрузки, получили повреждения (Several boot critical files are corrupt)	Повреждения получили сразу несколько файлов, необходимых для загрузки
Поврежден реестр (Registry is corrupt)	Улей реестра не загружается
Неизвестный код ошибки (Unknown bugcheck <code>. Parameters = <param1>, <param2>, <param3>, <param4>)	Во время загрузки появился "синий экран смерти" с указанным кодом ошибки
Драйвер <имя драйвера> препятствует запуску системы (Driver <drivername> is preventing the system from starting)	Драйвер с именем, указанным в сообщении, отсутствует или поврежден

Таблица 11.8 (продолжение)

Причина сбоя	Описание
Установка или обновление драйвера препятствуют запуску системы (A recent driver installation or upgrade may be preventing the system from starting)	Незадолго до перезагрузки был установлен несовместимый драйвер, который и вызывает сбой при загрузке
Установленный патч не позволяет загрузить систему (A patch is preventing the system from starting)	Установленное обновление вызывает сбой при загрузке системы
Списки ACL файла <имя файла> неверны. Прежнее значение = <значение> (ACLs on file <filename> are not proper. Old value = <value>)	Указанный в сообщении файл недоступен из-за неправильно установленных списков контроля доступа (ACL)
Таблица разделов не содержит корректного системного раздела (The partition table does not have a valid System Partition)	Системный раздел, указанный в таблице разделов, не содержит необходимых системных файлов
Повреждена MBR (MBR is corrupt)	Повреждена MBR на системном диске
На диске <номер диска> повреждена таблица разделов (Partition table is corrupt on disk <drivenumber>)	Таблица разделов на указанном диске не содержит ни одного корректного элемента
Поврежден загрузочный раздел системного диска (Boot sector for system disk partition is corrupt)	Загрузочный сектор системного диска содержит некорректную информацию
Код загрузочного сектора системного диска поврежден (Boot sector code for system disk partition is corrupt)	Код загрузочного сектора не совпадает с загрузочным сектором по умолчанию
Системный том на диске поврежден	Системный том недоступен
На диске не найдено файлов ОС (No OS files found on disk)	Каталог %WINDIR% не содержит инсталляции Windows Vista/7
Отсутствует менеджер загрузки (Boot manager is missing)	На системном разделе нет файла bootmgr
Не обнаружен жесткий диск. Если диск установлен, он не отвечает (A hard disk could not be found. If a hard disk is installed, it is not responding)	Система не может обнаружить ни одного установленного жесткого диска. Это сообщение может появиться только при запуске Windows RE с CD или DVD
Параметры безопасности, установленные на этом компьютере, препятствуют запуску Windows (Security settings on this computer are preventing Windows from starting)	Windows Vista/7 на компьютере установлена, но параметры безопасности не позволяют выполнять аудит

Таблица 11.8 (окончание)

Причина сбоя	Описание
Неизвестный тип файловой системы на системном разделе (System partition has an unknown file system type)	Системный раздел отформатирован с использованием файловой системы, которую Windows Vista/7 не может распознать
Статус загрузки указывает на успешный запуск ОС (Boot status indicates that the OS booted successfully)	Windows Vista/7 была успешно загружена. Этот сценарий часто встречается, когда пользователь запускает WinRE вручную
Произошел сбой в процессе установки (Failure while setup is in progress)	Система не запускается, так как в процессе установки Windows Vista произошел сбой
Версия операционной системы несовместима с опцией Восстановление запуска (The operating system version is incompatible with Startup Repair)	Вы пытаетесь выполнить восстановление несовместимой версии Windows. Обратите внимание, что опция Восстановление запуска может применяться только для восстановления Windows Vista/7

На рис. 11.18 приведен пример ошибки, которая не может быть устранена с помощью опции **Восстановление запуска** (Startup Repair).

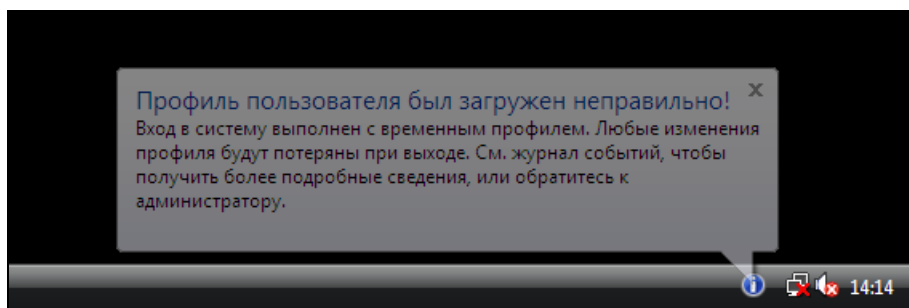


Рис. 11.18. Пример ошибки неправильной загрузки пользовательского профиля, также не устранимой при помощи опции **Восстановление запуска**

Восстановительные операции, выполняемые при выборе опции **Восстановление запуска**

Восстановительные операции, которые выполняются при выборе опции **Восстановление запуска**, кратко перечислены в табл. 11.9.

Таблица 11.9. Краткое описание восстановительных операций, выполняемых WinRE в автоматическом режиме

Восстановительная операция	Описание
BCDMD	Восстановление MBR, таблицы разделов или загрузочного сектора
ChkDsk	Запуск ChkDsk в режиме восстановления
Восстановление файлов (File Repair)	Замещение поврежденных системных файлов резервными копиями
BootCfg	Восстановление базы данных BCD
Восстановление системы (System Restore)	Откат состояния системы к одной из ранее созданных точек восстановления
Исправление ACL (ACLs fix)	Восстановление списков контроля доступа (Access Control Lists, ACL) для указанных файлов к значению по умолчанию
Откат реестра (Registry rollback)	Замещение поврежденных ульев реестра резервными копиями
Изменение параметра Crash on Audit (Change Crash on Audit Failure setting)	Блокирует аудит Windows. Только администратор сможет войти в систему
Диагностика памяти (Memory Diagnostics)	Запускает средство диагностики памяти memtest.exe

Возможные результаты выполнения восстановительных операций перечислены в табл. 11.10.

Таблица 11.10. Возможные результаты восстановительных операций

Результат	Описание
Успешно завершено. Код ошибки = 0x0 (Completed successfully. Error code = 0x0)	Процедура диагностики и восстановления завершилась без ошибок
Завершено неудачно. Код ошибки = <код> (Failed. Error code = <errorcode>)	Процедура диагностики и восстановления завершилась неудачно
Процедура начата, но не завершена (Started but not completed)	Либо процесс диагностики, либо процесс восстановления был прерван пользователем

Приведенная в этом разделе информация ни в коем случае не претендует на полноту. Однако она четко показывает, что несмотря на усовершенствован-

ную среду восстановления WinRE, устранение проблем с загрузкой Windows Vista/7 не всегда может пройти гладко. В последующих разделах будет приведено несколько примеров восстановления незагружаемой системы Windows Vista/7, иллюстрирующих сказанное.

Проблемы с мультизагрузочными конфигурациями

У пользователей, активно применяющих мультизагрузочные конфигурации, часто возникает следующая проблема: Windows Vista/7 перестает загружаться после установки более ранней версии операционной системы. При этом возможны следующие варианты:

- ❑ при установке более ранней версии (например, Windows XP) будет запускаться только она, а Windows Vista и Windows 7 просто не будут отображаться в меню загрузки;
- ❑ при установке дополнительной копии Windows XP в систему с двойной загрузкой, где уже есть одна копия Windows XP и одна копия Windows Vista/7, меню загрузки может принять такой вид, как показано на рис. 11.19. Попытка выбрать опцию **Unidentified operating system on drive C** приведет к результату, показанному на рис. 11.20.

Причины возникновения этой проблемы очевидны, и они обсуждались в *главе 7*, так что здесь мы не будем останавливаться на них подробно. Лучше рассмотрим пути ее решения, так как они не столь уж очевидны, как может показаться на первый взгляд, — ведь простое восстановление главной загрузочной записи Windows Vista/7 с помощью опции **Восстановление запуска** (Startup Repair) в WinRE приведет к тому, что перестанет загружаться и Windows XP.

Чтобы решить проблему, действуйте следующим образом:

1. Если вы только что установили Windows XP, и теперь у вас загружается только она, то загрузите Windows XP и войдите в систему как пользователь с административными правами.
2. Вставьте в привод дистрибутивный диск с копией Windows Vista/7 (в зависимости от того, какая из них присутствовала в системе раньше). Восстановите главную загрузочную запись Windows Vista/7, дав следующую команду:

```
<DVD_drive>:\boot\Bootsect.exe /NT60 All
```



```

Please select the operating system to start:

Microsoft Windows XP Professional
Unidentified operating system on drive C.

Use the up and down arrow keys to move the highlight to your choice.
Press ENTER to choose.
Seconds until highlighted choice will be started automatically: 23

For troubleshooting and advanced startup options for Windows, press F8.

```

Рис. 11.19. Unidentified operating system on drive C — это Windows Vista/7, и попытка ее загрузить не приведет ни к чему хорошему

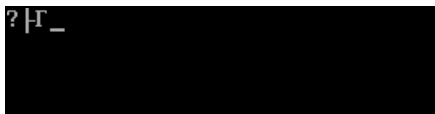


Рис. 11.20. Вот что вы увидите на экране, попытавшись загрузить "неидентифицированную операционную систему"

ПРИМЕЧАНИЕ

В этой команде *<DVD_drive>* — это диск, на котором находятся установочные файлы системы Windows Vista/7.

- После восстановления вы сможете загружать Windows Vista/7, но Windows XP загружаться перестанет. Чтобы восстановить возможности загрузки Windows XP вручную, воспользуйтесь программой Bcdedit.exe. Для этого введите в командной строке следующие команды:

```
<диск>:\Windows\system32\Bcdedit /create {ntldr} -d "Описание предыдущей версии системы Windows"
```

ПРИМЕЧАНИЕ

В этой команде и следующих *<диск>* — это диск, на котором установлена система Windows Vista/7.

```
<диск>:\Windows\system32\Bcdedit /set {ntldr} device partition=x:
```

ПРИМЕЧАНИЕ

В этой команде *x:* — это буква диска активного раздела.

```
<диск>:\Windows\system32\Bcdedit /set {ntldr} path \ntldr
```

```
<диск>:\Windows\system32\Bcdedit /displayorder {ntldr} -addlast
```

4. Перезагрузите компьютер.**ПРИМЕЧАНИЕ**

Если у вас на компьютере установлено несколько копий Windows XP, не забудьте отредактировать файл Boot.ini так, чтобы в нем были правильно указаны пути к каждой из них. Если же на компьютере имеется только одна копия Windows XP, то этот файл просто не нужен.

Проблемы с запуском, возникающие после загрузки ядра

Как говорилось в *главе 7*, если процедура загрузки дошла до появления индикатора загрузки (см. рис. 7.12 и 7.13), это означает, что ядро Windows Vista/7 успешно загрузилось. Если после этого в ходе запуска ОС происходит сбой, то, вероятнее всего, он вызван несовместимым или некорректно работающим драйвером или сервисом.

В данном случае ваша задача сводится к выявлению и блокированию проблемных программных компонентов с целью обеспечения успешной загрузки Windows. После того как Windows успешно запустится, вы сможете выполнить дальнейшие процедуры по устранению неполадок. Последовательность шагов, которые следует предпринять с этой целью, должна быть следующей:

1. Для начала попробуйте воспользоваться инструментом **Восстановление запуска** (Startup repair), так как его использование наиболее безопасно. Этот инструмент позволяет автоматически устранять не только проблемы с запуском, возникающие на начальных этапах загрузки, но и проблемы, возникающие после загрузки ядра. Если после запуска инструмента **Восстановление запуска** Windows запустится нормально, то ваша цель достигнута. Если проблему решить и не удастся, проанализируйте файл журнала %WINDIR%\System32\LogFiles\Srt\SrtTrail.txt, как было описано ранее в данной главе.
2. Попробуйте загрузиться с помощью опций отладочного меню, выводимого по нажатию клавиши <F8>. Краткое описание доступных опций отладочного меню и рекомендации по их применению были приведены в *главе 7*. При этом при загрузке в безопасном режиме вам будут доступны все стандартные графические средства по устранению неполадок.

ПРИМЕЧАНИЕ

При запуске Windows Vista/7 производится считывание информации из файла журнала `%windir%\Bootstat.dat`. Если Windows Vista/7 обнаружит, что последняя попытка запуска была неудачной, то отладочное меню загрузки появится автоматически, и нажимать клавишу <F8> вам не придется.

3. Проанализируйте журнал `%Windir%\Ntbtlog`, чтобы выявить драйвер, вызывающий сбой. Для этого сравните список драйверов, загружаемых в обычном режиме, и драйверов, загружаемых в безопасном режиме. Драйвер, который вызывает сбой системы, в режиме загрузки обычного режима помечается как **Loaded driver**, а в безопасном режиме — как **Did not load driver**. Кроме того, в безопасном режиме вы можете заблокировать или откатить потенциально опасные драйверы.
4. Поочередно блокируйте сервисы, которые загружаются только в обычном режиме, до тех пор, пока вы не сможете загрузить компьютер нормальным образом.
5. Если вы не можете загрузиться в безопасном режиме, попробуйте запустить WinRE и воспользоваться опцией **Командная строка** (Command Prompt). Запустите из командной строки программу Notepad (Блокнот) и сравните файлы Ntbtlog, созданные при успешной и неудачной попытках загрузки в безопасном режиме. Выявив проблемный драйвер, из командной строки замените его работоспособной версией. Повторяйте этот процесс до тех пор, пока система не начнет запускаться в обычном режиме.

Устранение неполадок, возникающих сразу же после входа в систему

Если сбой происходит сразу же после регистрации в системе, то он, скорее всего, вызван одним из приложений, загружающихся автоматически. Чтобы выявить проблемные приложения, действуйте следующим образом:

- при регистрации в системе нажмите клавишу <Shift> и удерживайте ее в этом положении в течение всего времени входа в систему (до тех пор, пока на экране не появится рабочий стол Windows Vista/7). Эта процедура влияет лишь на текущий сеанс работы с системой. Если вам удастся ус-

пешно зарегистрироваться, значит, проблема действительно вызвана приложениями автозагрузки;

- если сбой начал происходить сразу же после установки нового приложения, то удалите это приложение.

Заключение

Если вы имеете предварительный опыт работы с предшествующими версиями Windows, то вы обнаружите, что процесс устранения неполадок в процессе загрузки Windows Vista/7 стал гораздо удобнее и предоставляет намного больше возможностей. Вы сможете устранить большинство наиболее распространенных проблем, не прилагая чрезмерных усилий.

Глава 12



"Синий экран смерти"

"there was an error processing your error"¹

Фольклор

Windows NT crashed.
I am the Blue Screen of Death
No one hears your screams.²

Фольклор

Почти все, кто уже успел достаточно поработать с операционными системами из семейства Windows NT, наверняка знают, хотя бы понаслышке, о том, что такое BSOD (Blue Screen Of Death, в буквальном переводе с английского — "Синий экран смерти"). Это выводимое на синем фоне системное сообщение (называемое еще "сообщение **STOP**" или "ошибка **STOP**"), свидетельствующее о крахе системы, после которого система сбрасывает дамп памяти и (обычно) уходит на перезагрузку, теряя все несохраненные данные.

Особо неприятно то, что возникать "синий экран" может в самых неожиданных местах и при самых неожиданных обстоятельствах. Так, например, он появился на церемонии открытия Олимпийских игр в Пекине — в течение некоторого времени огромное изображение "синего экрана смерти" Windows XP проецировалось на крышу Национального стадиона³. Что примечательно и, действительно, заслуживает упоминания, так это то, что организаторы Олимпиады пошли на поводу у общественного мнения и отказались от использования Windows Vista, сославшись на ее нестабильность (а ведь

¹ "В процессе обработки ошибки произошла еще одна ошибка".

² "Windows NT рухнула. Я — синий экран смерти. Никто не слышит ваших воплей".

³ См.: <http://gizmodo.com/5035456/blue-screen-of-death-strikes-birds-nest-during-opening-ceremonies-torch-lighting>.

вполне возможно, что с Vista, что бы о ней ни говорили, такого конфуза не приключилось бы).

ПРИМЕЧАНИЕ

Между прочим, довольно обширная коллекция разнообразных BSOD, возникших при различных обстоятельствах в разных системах, находится здесь: <http://www.dognoodle99.cjb.net/bsod/> и здесь: <http://daimyo.org/bsod> — правда, эти сайты давно не обновлялись, поэтому там нет картинок с изображением синего экрана для Windows Vista и, уж тем более, для Windows 7. Впрочем, хотя и Windows Vista, и Windows 7 действительно надежнее и стабильнее, чем их предшественницы, "синие экраны" появляются и у них (см., например, <http://gizmodo.com/5129919/what-a-windows-7-bsod-looks-like>).

Так давайте разберемся, что же представляет собой "синий экран" и как с ним бороться. Фактически, BSOD появляется всякий раз, когда в системе возникает состояние ошибки, которую она не может обработать — например, выполнение заведомо некорректной операции (скажем, такой, как деление на нуль или попытка освобождения уже освобожденной памяти). Во всех этих случаях работа системы завершается в аварийном режиме, при этом система отображает для пользователя код ошибки (если успевает это сделать) и сбрасывает на жесткий диск так называемый *дамп* ("моментальный снимок") памяти, поковырявшись в котором, можно определить причину сбоя. Аварийно завершить работу системы, выбросив "синий экран", — это самое простое и надежное, что только можно сделать при крахе системы. Microsoft неспроста пошла по этому пути, так как это — путь наименьшего сопротивления. В сущности, BSOD представляет собой своего рода "предохранитель", ведь если бы его не было, то разрушение данных могло бы зайти еще дальше.

Итак, когда операционные системы из семейства Windows NT выявляют серьезную ошибку, которую не могут самостоятельно устранить, они, в зависимости от типа ошибки, генерируют соответствующие системные сообщения, которые известны под собирательным названием "синих экранов смерти". "Синий экран" может появиться, в том числе, и в ситуациях, когда операционная система останавливается в процессе загрузки. Система генерирует такие сообщения с тем, чтобы предотвратить дальнейшее разрушение данных. Типичные образцы таких экранов показаны на рис. 12.1 ("синий экран" в Windows Vista, появившийся в процессе загрузки вследствие повреждения улья реестра COMPONENTS) и 12.2 ("синий экран в Windows 7, появившийся в процессе работы вследствие того, что пользователь вручную создал состояние ошибки).

```
STOP: c0000218 {Registry File Failure}
The registry cannot load the hive (file):
\SystemRoot\System32\Config\COMPONENTS
or its log or alternate.
It is corrupt, absent, or not writable.

Collecting data for crash dump ...
Initializing disk for crash dump ...
Beginning dump of physical memory.
Dumping physical memory to disk: 95
```

Рис. 12.1. Типичный вид "синего экрана" в Windows Vista, появляющегося в процессе загрузки вследствие повреждения одного из ульев реестра

```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

The end-user manually generated the crashdump.

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x000000E2 (0x00000000,0x00000000,0x00000000,0x00000000)

Collecting data for crash dump ...
Initializing disk for crash dump ...
Beginning dump of physical memory.
Dumping physical memory to disk: 90
```

Рис. 12.2. Типичный пример "синего экрана" в Windows 7, появляющегося в ходе работы вследствие искусственного сброса аварийного дампа

Типичный "синий экран" в Windows Vista и Windows 7 содержит информацию кода ошибки (bugcheck information), рекомендации пользователю (recommended user action) и информацию отладочного порта (debug port information). При этом выяснение истинных причин ошибки все равно остается

сложной задачей. Тем не менее, в ряде не слишком сложных случаев опытному пользователю вполне по силам самостоятельно решить возникшую проблему.

Если **STOP**-сообщение ("синий экран") появляется в процессе загрузки операционной системы, то, как правило, события развивались по одному из описанных далее путей:

- ❑ произведена установка программного обеспечения, которое разрушило часть информации системного реестра, хранящейся под ключом `HKEY_LOCAL_MACHINE` — это может происходить при попытках прикладной программы установить новую службу или драйвер. Результатом будет появление "синего экрана", на котором выведена информация о невозможности загрузки реестра или одного из его файлов;
- ❑ пользователь некорректно изменил конфигурацию аппаратных средств, что привело к разрушению или перезаписи критически важных системных файлов;
- ❑ произведена установка нового сервиса или системного драйвера, который не является совместимым с аппаратными средствами компьютера, что и вызывает ошибку при перезагрузке (более конкретно: загрузка некорректного файла приводит к разрушению исправного системного файла, который был загружен в память до момента сбоя).

СОВЕТ

Активное применение обсуждавшихся в *главе 5* средств защиты системных файлов Windows представляет собой надежный метод предотвращения подобных ситуаций. Именно поэтому они и рассматривались там настолько подробно. Пользуйтесь этими средствами и не дожидайтесь возникновения проблемы. Поверьте, эта рекомендация надежна!

Однако что же делать, если проблема все же возникла? Иногда сообщения, выводимые в случае возникновения проблем с загрузкой, явным образом ссылаются на поврежденный файл реестра (возьмем, например, сообщение о поврежденном или отсутствующем файле улья `COMPONENTS`, приведенное на рис. 12.1). Однако, к сожалению, так бывает не всегда. Если имеются основания подозревать, что проблемы с загрузкой связаны именно с реестром, можно начать восстановление с использованием варианта загрузки последней удачной конфигурации (Last Known Good Configuration).

Для этой цели следует воспользоваться загрузочным меню с дополнительными отладочными опциями, появляющимся при нажатии клавиши <F8>. Опции этого меню были подробно описаны в *главе 7*.

Если вы имеете опыт работы с Windows NT/2000/XP, то наверняка знаете, что проблемы с загрузкой чаще всего вызывались некорректно работающими драйверами устройств. Такие несовместимые драйверы могли привести

к краху системы либо сразу же после инсталляции, либо даже через некоторое время, в течение которого их работа на первый взгляд казалась корректной. Причем вторая ситуация, когда драйвер в течение некоторого времени все же работал, не вызывая никаких проблем, всегда была более труднообъяснимой (а в самом-то деле, что же могло вдруг вызвать ошибку, когда все, вроде бы, работало нормально?). Дело тут, по-видимому, в том, что как программная, так и аппаратная конфигурация компьютера со временем могут меняться, и эти изменения способны вызвать к жизни ошибки, допущенные при проектировании драйвера и оставшиеся до того незамеченными. Системы Windows Vista и Windows 7 также могут быть выведены из строя установкой некорректного драйвера. В этом случае вам могут помочь опции загрузки системы в безопасном режиме, безопасном режиме с поддержкой сети или в безопасном режиме с интерфейсом командной строки.

Если несовместимый драйвер вызывает проблему при первой же перезагрузке, то вам очень повезло, потому что, как правило, в этом случае действительно помогает опция **Последняя удачная конфигурация (дополнительно)** (Last Known Good Configuration (Advanced)). Система при загрузке использует информацию ключа реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet` и восстановит всю конфигурационную информацию, сохраненную после предыдущей успешной загрузки компьютера. В ряде случаев, если использование этой опции не помогло, но вам известен драйвер, вызвавший проблему (список таких драйверов можно получить с помощью утилиты `sigverif`, описанной в главе 5), то вы можете попробовать другие способы быстрого восстановления. Например, попытаться применить такие опции меню безопасного режима, как **Безопасный режим** (Safe Mode), **Безопасный режим с загрузкой сетевых драйверов** (Safe Mode with Networking) или **Безопасный режим с поддержкой командной строки** (Safe Mode with Command Prompt), при выборе которых Windows загружается с минимальным набором драйверов и сервисов. После загрузки в одном из этих режимов проблемный драйвер можно будет удалить из системы штатными средствами Windows, такими как Мастер установки оборудования (Hardware Wizard) или Диспетчер устройств (Device Manager).

Если приведенные выше рекомендации не помогли решить проблему, вспомните о методах восстановления поврежденного реестра, подробно описанных в главе 2.

ПРИМЕЧАНИЕ

Наиболее безопасным местом хранения резервных копий реестра может служить раздел диска, отличный от загрузочного (а лучше всего вообще хранить их на другом физическом диске, что поможет добиться максимальной защиты от аппаратных сбоев, которые могут сделать полученные копии файлов реестра недоступными).

Вы никогда не видели "синего экрана" и хотите на него посмотреть

Вы никогда в жизни не видели "синего экрана"? Многие люди, которые видели, вам позавидуют и скажут, что вы — счастливчик. Что? Вам хочется увидеть, что это такое? Пожалуйста!

Как в Windows 2000/XP, так и в Windows Vista/7 имеется функция, которая позволяет сбросить систему в "синий экран смерти" и создать файл аварийного дампа Memory.dmp. Экран сообщения **STOP**, который появится при использовании этой возможности, будет содержать следующее сообщение:

```
*** STOP: 0x000000E2 (0x00000000,0x00000000,0x00000000,0x00000000)
```

The end-user manually generated the crashdump.

По умолчанию эта возможность заблокирована, и для ее активизации следует вручную отредактировать реестр и перезагрузить компьютер. Редактором реестра раскройте ключ реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\i8042prt\Parameters` и добавьте в состав этого ключа параметр `CrashOnCtrlScroll` с типом данных `REG_DWORD`. Присвойте этому параметру значение 1.

После перезагрузки вы сможете посмотреть на "синий экран". Для этого следует, удерживая правую клавишу `<Ctrl>`, дважды нажать клавишу `<Scroll Lock>`.

ПРИМЕЧАНИЕ

Кстати, приведенная здесь рекомендация по ручной генерации состояния ошибки — это не просто забавный "трюк", позволяющий удовлетворить ваше (впрочем, вполне законное) любопытство. Он может оказаться довольно полезным при устранении текущих проблем в работе системы, потому что с его помощью можно получить дамп памяти в заданный момент. Иначе, спрашивается, зачем бы Microsoft предоставляла такую возможность?

Методы борьбы с "синим экраном смерти" в Windows Vista и Windows 7

Как уже говорилось, в Windows Vista/7 ошибки **STOP** возникают, когда ядро или драйвер устройства, работающий в режиме ядра, встречает ошибку, после которой система не может восстановиться самостоятельно. Единственное действие, которое она может выполнить в этой ситуации, чтобы предотвратить дальнейшее разрушение данных — это перезагрузка. В результате данные, не сохраненные пользователем, могут быть потеряны.

Установка параметров запуска операционной системы

Чтобы бороться с "синими экранами", необходимо настроить поведение системы при их появлении. Рассмотрим эти возможности более подробно.

1. Для указания параметров загрузки откройте окно **Панель управления** (Control Panel), выберите опцию **Система** (System), а в раскрывшемся окне щелкните по ссылке **Дополнительные параметры системы** (Advanced System Properties).
2. На экране появится окно **Свойства системы** (System Properties), раскрытое, как показано на рис. 12.3, на вкладке **Дополнительно** (Advanced). Нажмите кнопку **Параметры** (Settings) в группе **Загрузка и восстановление** (Startup and Recovery).

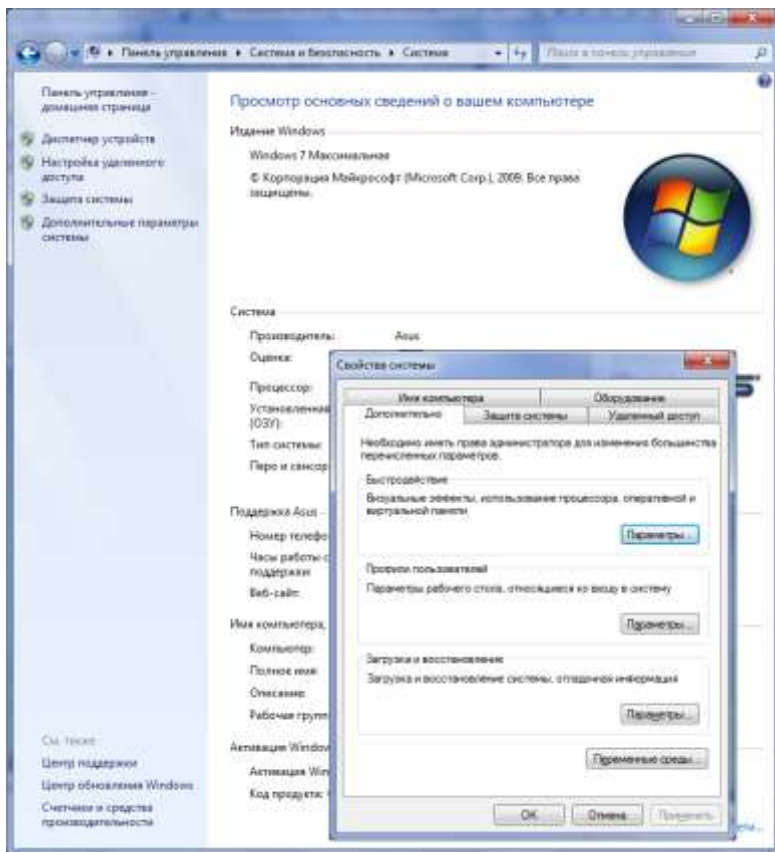


Рис. 12.3. Вкладка **Дополнительно** окна **Свойства системы**

Откроется окно **Загрузка и восстановление** (Startup and Recovery), показанное на рис. 12.4.

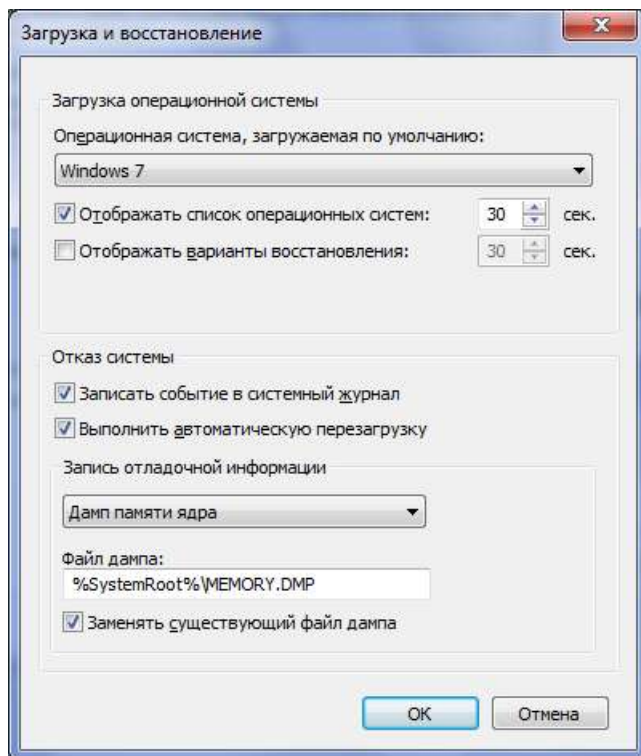


Рис. 12.4. Окно **Загрузка и восстановление**

В верхней части этого окна имеется группа опций **Загрузка операционной системы** (System Startup), позволяющая указать операционную систему, загружаемую по умолчанию (в случае, когда на компьютере установлено несколько операционных систем), и задать временной интервал, в течение которого на экране будет отображаться меню загрузки.

ПРИМЕЧАНИЕ

В Windows XP в группе опций **Загрузка операционной системы** (System Startup) была предусмотрена возможность ручного редактирования файла Boot.ini. Для того чтобы выполнить ее, достаточно было нажать кнопку **Правка** (Edit). Поскольку начиная с Windows Vista на смену файлу Boot.ini пришла сложная база данных загрузочной конфигурации BCD, представляющая собой улей реестра, этой возможности больше нет. Как уже говорилось в *главе 4*, для ручного редактирования конфигурационной информации улья реестра BCD предназначается даже не Редактор реестра, а утилита командной строки BCDedit.exe.

В данном случае нас интересует группа опций **Отказ системы** (System Failure), позволяющая определить поведение системы в случае возникновения ошибок **STOP**. Опции из этой группы заслуживают более подробного обсуждения.

Системный журнал событий является очень хорошим источником информации, которая может позволить выяснить причину возникновения ошибки. Именно поэтому в любом случае рекомендуется установить флажок **Записать событие в системный журнал** (Write an event to the system log). Если этот флажок установлен, то при каждом возникновении ошибки **STOP** в системном журнале событий будет делаться соответствующая запись.

Наконец, если компьютер, на котором происходит указанная ошибка, необходимо как можно скорее привести в рабочее состояние, то, вероятно, вы захотите, чтобы он автоматически перезагружался в случае возникновения ошибок **STOP**. Для этого установите флажок **Выполнить автоматическую перезагрузку** (Automatically reboot).

ПРИМЕЧАНИЕ

В конференциях можно встретить рекомендацию по редактированию реестра Windows таким образом, чтобы система автоматически перезагружалась при возникновении ошибок **STOP**. Эта рекомендация сводится к тому, чтобы раскрыть ключ `HKKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl\` и задать значение параметра `Autoreboot` в составе этого ключа, равным 1. Хотя эта рекомендация в целом правильна, данную задачу можно выполнить гораздо более простым способом — установкой флажка **Выполнить автоматическую перезагрузку** (Automatically reboot) окна **Загрузка и восстановление** (Startup and Recovery).

Если ошибки, приводящие к отображению "синего экрана", появляются систематически, то наилучшим источником информации о причине их возникновения будет отладочный дамп. Для конфигурирования системы таким образом, чтобы при ее крахе содержимое оперативной памяти сбрасывалось в файл на жестком диске, используются опции из группы **Запись отладочной информации** (Write Debugging Information). Поле **Файл дампа памяти** (Dump File) предназначено для ввода имени файла, в который будет сбрасываться эта информация, а установка флажка **Заменять существующий файл дампа** (Overwrite any existing file) приводит к тому, что содержимое существующего файла дампа каждый раз будет замещаться новой информацией. Эти опции используются точно так же, как и в ранних версиях Windows NT.

Начиная с Windows 2000, компания Microsoft включила в систему расширенную функцию для сохранения отладочного дампа. Если вы имеете предварительный опыт работы с Windows NT, то наверняка помните, что в Windows NT 4.0

в отладочный дамп можно было сбросить только все содержимое физической памяти компьютера. Объем файла, который при этом генерирует система, всегда имеет размер, несколько больший, нежели объем оперативной памяти, установленной на компьютере, и при этом значительный объем данных, содержащихся в файле дампа, практически бесполезен. Поскольку ошибки **STOP** представляют собой ошибки ядра, именно информация ядра (состояние системы на момент возникновения ошибки, сведения об активных приложениях, загруженных драйверах устройств и т. д.) и представляет практический интерес при анализе дампа. Данные о режиме пользователя обычно просто увеличивают размер файла дампа и не предоставляют полезной информации.

Именно поэтому, начиная с Windows 2000, в диалоговом окне **Загрузка и восстановление** (Startup and Recovery) появилась новая опция, позволяющая регулировать размеры файла аварийного дампа.

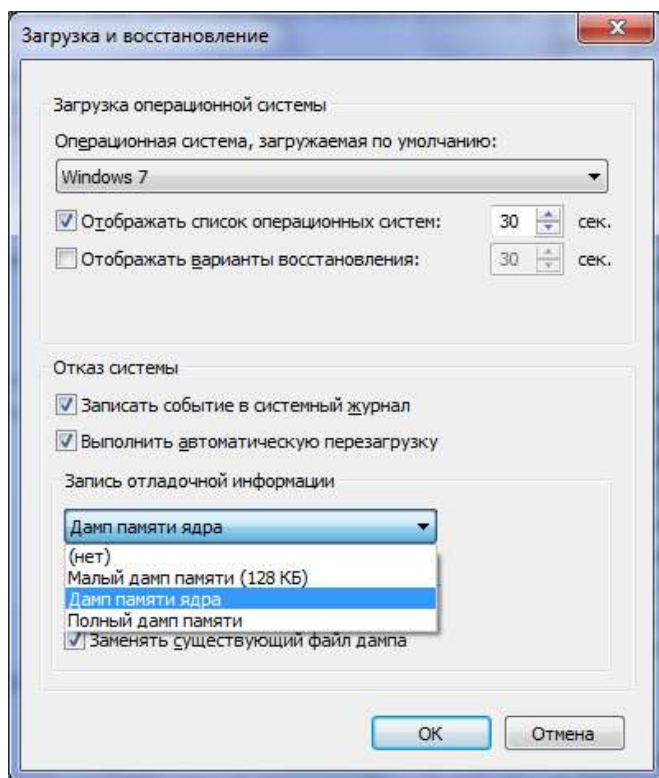


Рис. 12.5. Варианты записи отладочной информации дампа памяти, создаваемого при возникновении ошибок **STOP**

Список из группы **Запись отладочной информации** (Write Debugging Information) позволяет выбрать режим сохранения дампа. Наряду с возможностью сохранения полного дампа (как в Windows NT 4.0) Windows 2000/XP и Windows Vista/7 имеют опцию **Дамп памяти ядра** (Kernel Memory Dump), при которой в файле дампа будет сохранена только информация ядра. Новые версии средств анализа аварийного дампа, в том числе dumpexam и WinDbg, будут интерпретировать этот файл корректно. Экономия дискового пространства, которой можно добиться с помощью этой опции, может быть разной в различных системах (и даже зависеть от типа возникающих ошибок).

ПРИМЕЧАНИЕ

Обратите особое внимание и на дополнительную опцию — **Малый дамп памяти (64 КБ)** (Small Memory Dump), которая позволяет ограничить размер дампа до значения в 64 Кбайт (см. рис. 12.5). Эта возможность активно используется сервисом отчета об ошибках (Error reporting).

Наиболее распространенные ошибки STOP в Windows Vista и Windows 7

Ошибки типа **STOP** в Windows Vista и Windows 7 могут проявляться на любом этапе — как при загрузке, так и в процессе работы операционной системы. Иногда они даже появляются и в процессе установки ОС на компьютер. При этом наиболее неприятной является ситуация, когда перезагрузка начинается практически мгновенно, так что вы просто не успеваете разглядеть информацию, выводимую на "синий экран". Если такая ситуация наблюдается уже в процессе запуска, то действовать рекомендуется следующим образом:

1. Включите компьютер, выберите загружаемую копию Windows Vista или Windows 7 (если у вас — мультизагрузочная система) и нажмите клавишу <F8>. Если на компьютере установлена только одна копия Windows Vista/7, нажмите эту клавишу сразу же, как только на экране появится логотип BIOS, и не отпускайте ее, пока на экране не будет выведено меню с дополнительными вариантами загрузки.
2. Когда на экране появится расширенное меню загрузки, выберите опцию **Отключить автоматическую перезагрузку при отказе системы** (Disable automatic restart on system failure), как показано на рис. 12.6.

Загрузка операционной системы начнется, но на этот раз автоматической перезагрузки при появлении ошибки не произойдет, и вы сможете подробно рассмотреть отображенный синий экран (рис. 12.7).

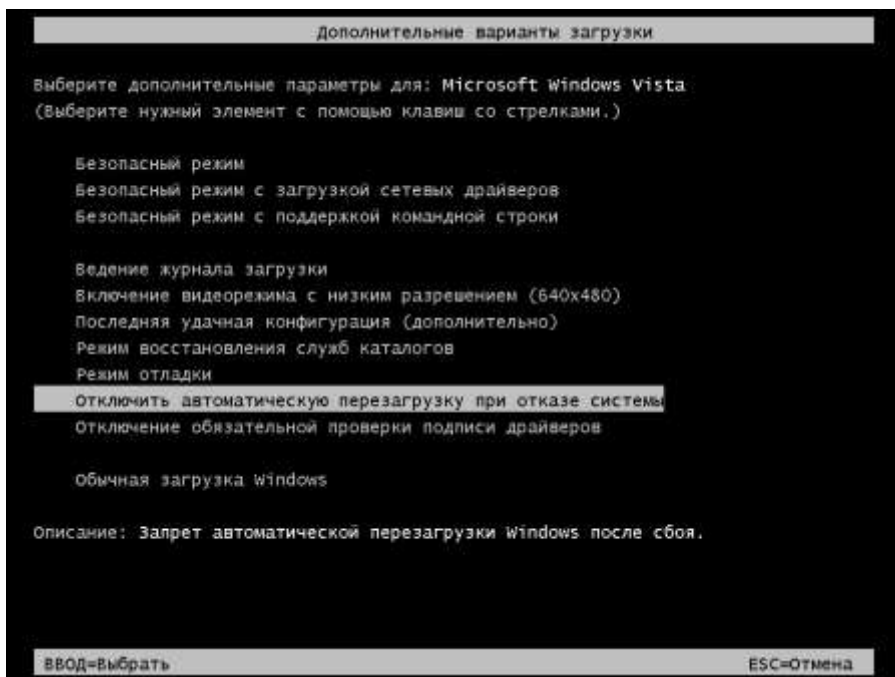


Рис. 12.6. Отключение опции автоматической перезагрузки при отказе системы

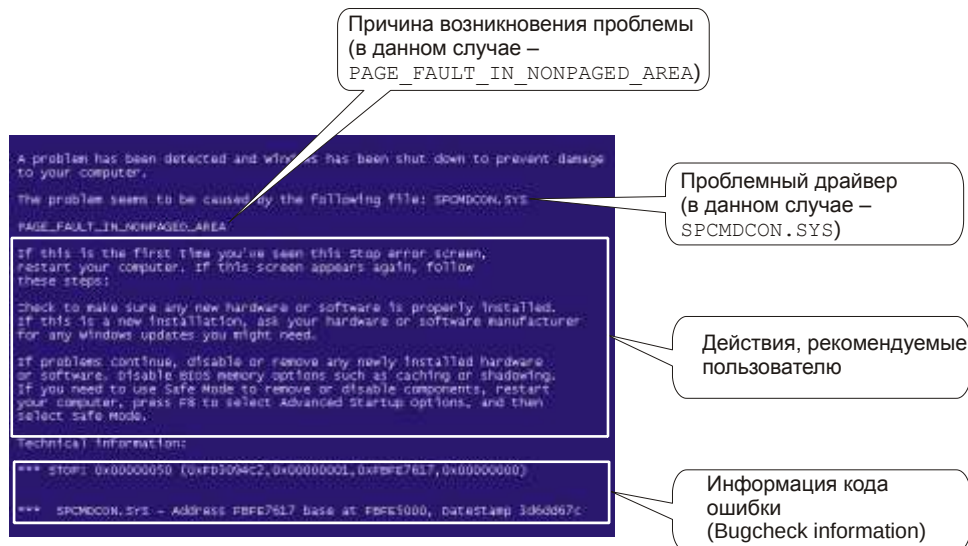


Рис. 12.7. Пример "синего экрана" (информация, наиболее важная для дальнейших шагов по устранению неполадки, выделена)

Как показано на рис. 12.7, в верхней части экрана содержится информация о причине возникновения проблемы, даются указания на проблемный сервис или драйвер (если эта информация доступна). Следующая часть экрана содержит инструкции для пользователя касательно того, какие действия надо произвести, чтобы устранить проблему. Как правило, эти инструкции сводятся к установке/удалению драйверов, проверке конфликтов аппаратных средств или программного обеспечения, отключению недавно добавленных в систему аппаратных устройств, блокированию опций разгона (если вы разгоняли компьютер через настройки BIOS) и т. д. Для выяснения истинных причин возникшей проблемы наибольший интерес представляет собой последний раздел — **Technical Information**, в котором приводятся следующие сведения:

- ❑ код ошибки и его символьное имя (например, **0x0000001E, KMODE_EXCEPTION_NOT_HANDLED**);
- ❑ четыре параметра, поясняющие ошибку и предназначенные для отладочного ПО (значение параметров зависит от кода ошибки);
- ❑ адрес места ошибки (если его возможно указать);
- ❑ название драйвера, в котором произошла ошибка (если его возможно указать).

Ошибки **STOP** идентифицируются префиксом **0x**, за которым следует восьмизначный код в шестнадцатеричном формате. Хотя для записи кодов ошибок и может использоваться сокращенная форма (например, можно написать вместо **STOP 0x0000000A** код **STOP 0xA**), но для полноценного ведения отчетности используются полные восьмизначные коды. За основным кодом ошибки может идти до четырех восьмизначных шестнадцатеричных чисел (параметров), которые, как правило, будут уникальны для вашего компьютера в конкретной ситуации.

Наконец, кроме кода ошибки и параметров указывается конкретное сообщение об ошибке, например, **IRQL_NOT_LESS_OR_EQUAL**.

Рассмотрим ошибки **STOP**, наиболее часто встречающиеся в новейших версиях операционных систем Microsoft: Windows Vista и Windows 7.

INACCESSIBLE_BOOT_DEVICE (STOP 0x0000007B)

Эта ошибка чаще всего встречается в процессе установки Windows Vista/7, если загрузочный диск SATA (Serial Advanced Technology Attachment) сконфигурирован неправильно, и сам драйвер SATA блокирован (disabled).

Обычно это происходит, если в программе BIOS Setup вы установите для загрузочного диска режим использования спецификации AHCI (Advanced Host

Controller Interface), и при этом драйвер AHCI (Msahci.sys) в Windows Vista/7 заблокирован (в процессе установки Windows Vista/7 все неиспользуемые драйверы накопителей блокируются, чтобы ускорить процесс запуска операционной системы). В этом случае после перезагрузки вы получите "синий экран" с кодом ошибки:

STOP 0x0000007B INACCESSIBLE_BOOT_DEVICE

ПРИМЕЧАНИЕ

Это поведение отмечается только для загрузочных дисков. Если диск, для которого вы меняете режим SATA в программе BIOS Setup, не является загрузочным, то ошибки не возникнет.

Чтобы избежать появления этой проблемы, сделайте следующее:

1. Работая в Windows Vista/7, закройте все ненужные приложения и запустите Редактор реестра.
2. Раскройте следующий ключ реестра: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Msahci`. В составе этого ключа найдите параметр с именем `Start` и установите для него значение 0.
3. После этого можете входить в программу BIOS Setup и менять режим SATA для загрузочного диска.

СОВЕТ

Если проблема уже возникла, запустите WinRE, выберите опцию **Командная строка** (Command Prompt) и дайте команду `Regedit.exe`. Теперь вы сможете устранить ошибку.

Следует иметь в виду, что появление этого "синего экрана" может быть вызвано и другими причинами, такими как:

- ☐ неправильное подключение жесткого диска или его физическая неисправность;
- ☐ несовместимость BIOS или другого оборудования с Windows Vista/7;
- ☐ заражение загрузочного сектора вирусом.

ПРИМЕЧАНИЕ

Подробное описание и рекомендации по устранению этих проблем описаны в статье из Microsoft Knowledge Base (<http://support.microsoft.com/kb/935806/en-us>).

PAGE_FAULT_IN_NONPAGED_AREA (STOP 0x00000050)

Это сообщение **STOP** чаще всего встречается на самых ранних стадиях процесса загрузки. В частности, оно может появиться, когда система пытается

загрузить драйвер i8042prt.sys. Проблема возникает лишь в некоторых аппаратных конфигурациях, и чтобы ее разрешить, необходимо установить обновление (hotfix), описанное в следующей статье из Microsoft Knowledge Base: "Error message when you start a Windows Vista-based computer:

STOP: 0x00000050 PAGE_FAULT_IN_NONPAGED_AREA"

(<http://support.microsoft.com/kb/939720/en-us>).

Кроме того, эта ошибка может появляться, если на компьютере имеется адаптер Card Bus, и в него вставлена карта Secure Digital (SD) или Compact Flash (CF), или же к компьютеру подключен внешний жесткий диск SATA (eSATA), работающий в режиме AHCI. В этом случае вам также потребуется установить обновление (hotfix), описанное в следующей статье из Microsoft Knowledge Base: "Error message on a Windows Vista-based computer that has a storage device inserted into a card bus adapter:

STOP: 0x00000050" (<http://support.microsoft.com/kb/938239/en-us>).

IRQL_NOT_LESS_OR_EQUAL (STOP 0x0000000A)

Эта ошибка обычно происходит в одном из следующих случаев:

- ☐ на компьютере установлено более 3 Гбайт RAM;
- ☐ компьютер применяет систему хранения данных, использующую драйвер мини-порта Storport;
- ☐ на компьютере установлен контроллер, использующий 32-разрядный режим прямого доступа к памяти (DMA);
- ☐ компьютер имеет чипсет NVIDIA.

Чтобы устранить эту ошибку, установите обновление, описанное в следующей статье из Microsoft Knowledge Base: "Error message when you try to install Windows Vista on a computer that uses more than 3 GB of RAM: STOP 0x0000000A" (<http://support.microsoft.com/kb/929777/en-us> 929777).

Кроме того, это сообщение может появляться, если вы запускаете или перезагружаете портативный компьютер Windows Vista/7 при закрытой крышке. В этом случае ситуацию также можно поправить путем установки обновления. Это обновление описано в следующей статье из Microsoft Knowledge Base: "Stop error message when you start a portable Windows Vista-based computer that has the lid closed:

STOP: 0x0000000A" (<http://support.microsoft.com/kb/941507/en-us>).

KERNEL_MODE_EXCEPTION_NOT_HANDLED (STOP 0x0000008E)

Это сообщение обычно свидетельствует о неправильно сконфигурированном драйвере устройства. Кроме того, появление этой ошибки часто говорит о том, что компьютер инфицирован вирусами или другим вредоносным программным обеспечением. Метод, рекомендованный Microsoft — применение средства удаления вредоносных программ Microsoft Malicious Software Removal Tool (<http://support.microsoft.com/kb/890830/ru>).

REGISTRY_ERROR (STOP 0x00000051)

В сущности, это сообщение об ошибке встречается редко, если только вы не занимаетесь экспериментами с реестром по несколько раз в день. Вызвано оно тем, что система в процессе загрузки не может корректно прочитать один из ульев реестра с жесткого диска. Совершенно очевиден тот факт, что с реестром что-то случилось. Простейшим путем устранения данной проблемы будет восстановление реестра с заблаговременно созданной резервной копии. О том, как это делается, было рассказано в *главе 2*. Данная ошибка могла быть вызвана проблемой с оборудованием или тем, что сама система повреждена. Также это может означать, что ошибка вызвана операцией обновления, которую использует только система безопасности и только, когда ресурсы на исходе.

PFN_LIST_CORRUPT (STOP 0x0000004E)

Обычно этот код ошибки вызывается установкой в компьютере дефектных модулей RAM.

MACHINE_CHECK_EXCEPTION (0x0000009C)

Причина возникновения этой ошибки аппаратная ("Urecoverable hardware error has occurred"). Чаще всего она возникает в результате перегрева компьютера, сбоя RAM, процессора, блока питания. Наиболее вероятной первопричиной является некорректный разгон (overclocking).

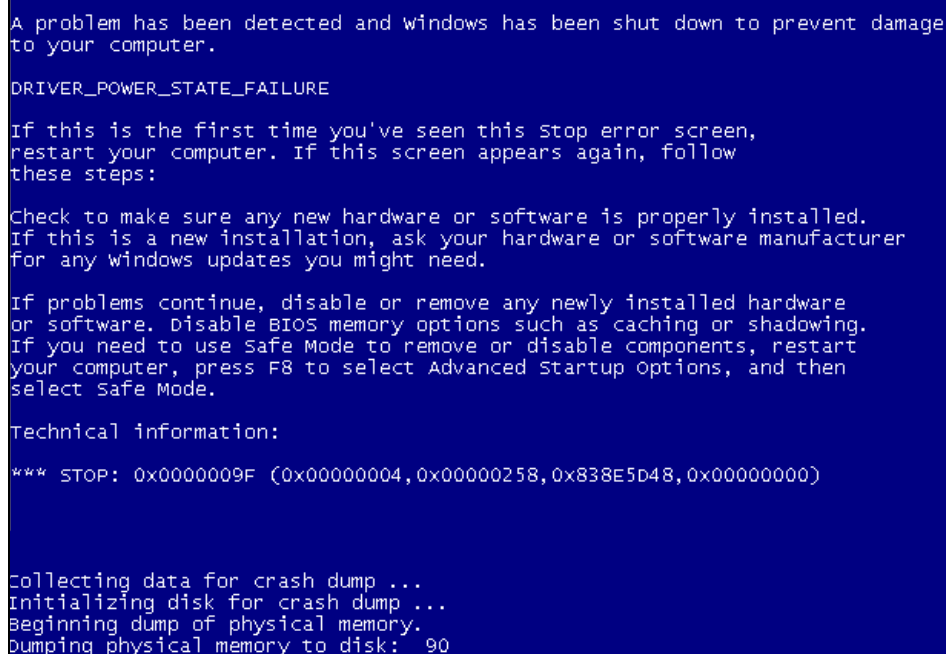
MULTIPLE_IRP_COMPLETE_REQUESTS (0x00000044)

Эта ошибка означает дефект программирования драйвера. Также может возникать в системах, работающих со значительной перегрузкой.

DRIVER_POWER_STATE_FAILURE (0x0000009F)

Драйвер находится в нестабильном режиме энергопотребления. Обычно это происходит в переходных режимах — например, при выключении компью-

тера или при переводе компьютера в режимы сна, гибридного сна и гибернации. Надо заметить, что такую ошибку умудрилась получить я сама, экспериментируя на очень старом компьютере с очень древними устройствами (рис. 12.8).



```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

DRIVER_POWER_STATE_FAILURE

If this is the first time you've seen this stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x0000009F (0x00000004, 0x00000258, 0x838E5D48, 0x00000000)

collecting data for crash dump ...
initializing disk for crash dump ...
beginning dump of physical memory.
dumping physical memory to disk: 90
```

Рис. 12.8. Вот мой первый "синий экран" в Windows 7
(получен в эмуляторе на очень старом компьютере)

Другие распространенные ошибки **STOP**

В этой главе были кратко перечислены распространенные ошибки **STOP**, чаще всего встречающиеся на практике. На самом деле их гораздо больше, и устранение каждой из возникающих проблем требует интуиции и творческого подхода. Если вы столкнетесь с ошибкой **STOP** и решите устранять проблему самостоятельно, то основная рекомендация, которую можно дать на этот случай, состоит в следующем: выполните поиск по базе знаний Microsoft (<http://support.microsoft.com/search>), используя в качестве ключевого слова код соответствующей ошибки (например, **0x0000007B**).

Общие рекомендации по устранению ошибок BSOD

Обычно, когда вы видите "синий экран", он остается на экране несколько секунд прежде, чем начнется перезагрузка компьютера, давая вам возможность рассмотреть код ошибки. Очень хорошие и детальные рекомендации по решению проблем с "синим экраном смерти" можно найти здесь:

<http://www.sun.com/desktop/products/sunpci/bsod.pdf>

и здесь: <http://aumha.org/a/stop.htm>.

Если это не поможет, вам следует обратиться по адресу сайта Microsoft Online Crash Analysis (<http://oca.microsoft.com/en/winddiag.asp>). Вы можете отправить в Microsoft отчет об ошибке и файлы дампов памяти. Местоположение дампов памяти и другие параметры отладочного режима можно найти в реестре под ключом `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl` (рис. 12.9).

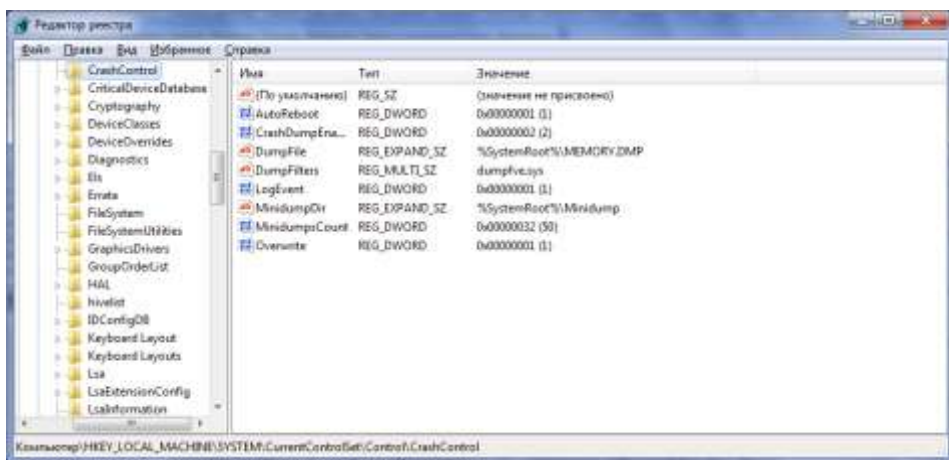


Рис. 12.9. Ключ реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl` содержит все параметры настройки отладочного режима

Заключение

В данной главе рассмотрены методы устранения некоторых ошибок **STOP** при помощи реестра. На практике их, разумеется, гораздо больше. Любопытный читатель найдет множество собственных методов решения возникающих проблем путем редактирования реестра. Автор желает вам успехов на этом сложном и долгом, но очень интересном пути.

Глава 13



Настройка производительности системы с помощью реестра

Вы уже дошли до состояния, когда у вас нет времени, чтобы разрешить те проблемы, которые отнимают у вас все время?

А. Блох, "Законы Мэрфи"

Теперь, когда мы обсудили наиболее общие проблемы, перейдем к рассмотрению тонкой настройки системы и решению некоторых частных задач. Возможно, кое-какие приведенные здесь рекомендации уже вам знакомы — в том числе и по предыдущим главам этой книги. Но здесь им будет уделено более пристальное внимание. К тому же, недаром говорят, что "можно верить лишь тому, что сказано трижды".

Настройка производительности Windows 7

Несмотря на то, что разработчики Microsoft в свое время приложили максимум усилий, чтобы повысить как скорость загрузки Windows Vista, так и ее производительность, многие пользователи продолжали сетовать, что их ожидания в этом отношении не оправдались. Часто можно было услышать, что "Windows XP SP3 существенно быстрее, чем Vista". Даже появление продуктов Service Pack 1 и 2 для Windows Vista этого разочарования не уменьшили. Именно поэтому при разработке Windows 7 производительность была поставлена, так сказать, во главу угла. Уже ранние бета-версии Windows 7 и загружались существенно быстрее, и в процессе работы демонстрировали значительно более высокую производительность, чем Windows Vista и Windows XP.

За счет чего же это было достигнуто? В основном — за счет сведения к минимуму количества сервисов, стартующих при запуске системы, количества дисковых операций, операций чтения и записи в реестр и индексируемых

файлов. Что еще важнее, Windows 7 не только серьезно повышает производительность, но и отличается от своих предшественниц гораздо более эффективным энергопотреблением. Начиная с Windows 7, у системных сервисов появилась возможность *триггерного запуска* (triggered startup). Это означает, что теперь для сервиса нет необходимости постоянно работать в фоновом режиме с целью мониторинга событий, как это было в более ранних версиях Windows. В Windows 7 сервисы могут стартовать только при наступлении определенных событий. Разработчики программного обеспечения имеют возможность конфигурирования триггеров и разработки своих сервисов в соответствии с этими новыми требованиями¹.

К настоящему времени в Интернете уже появилось множество статей, предлагающих обзоры и сравнительный анализ производительности Windows 7, Windows Vista и Windows XP². И с каждым днем появляются все новые и новые обзоры, которые в большинстве своем подтверждают сказанное — да, Windows 7 действительно является самой быстрой из всех операционных систем Microsoft, существующих на сегодняшний день. Но значит ли это, что вы, как пользователь, не можете дополнительно повысить производительность своего компьютера, работающего под управлением Windows 7? Конечно, нет! Оптимальная настройка и конфигурирование системы позволят вам заставить ее работать еще быстрее и буквально "выжать" из нее максимум. Давайте рассмотрим, как этого можно добиться.

Оценка общей производительности аппаратной конфигурации

Хотя Windows 7, как уже упоминалось ранее, действительно серьезно превосходит своих предшественниц по производительности, даже от нее не стоит ожидать фантастических результатов на компьютере, удовлетворяющем лишь минимальным аппаратным требованиям. Так, если в вашей системе физически присутствует только 1 Гбайт оперативной памяти, следует задуматься об установке дополнительных модулей RAM.

Как же оценить производительность аппаратной конфигурации? Начиная с Windows Vista, в состав операционной системы была введена новая встроенная функциональная возможность — Индекс производительности Windows (Windows Experience Index, WEI), предназначенная специально для того, чтобы помочь потребителям определить, чего можно ожидать от конкретной аппаратной конфигурации.

¹ Более подробную информацию по этим вопросам можно найти в блоге разработчиков Microsoft: <http://blogs.msdn.com/e7/archive/2008/08/29/boot-performance.aspx>.

² См., например: <http://blogs.zdnet.com/BTL/?p=22006>.

Если вы откроете Панель управления (Control Panel) и выберете опцию **Система** (System), то в раскрывшемся окне вы увидите основную информацию о вашей системе, в том числе — версию Windows, сведения о процессоре и памяти, сведения об имени компьютера и его членстве в домене или рабочей группе и, наконец, тот самый Индекс производительности Windows (рис. 13.1).

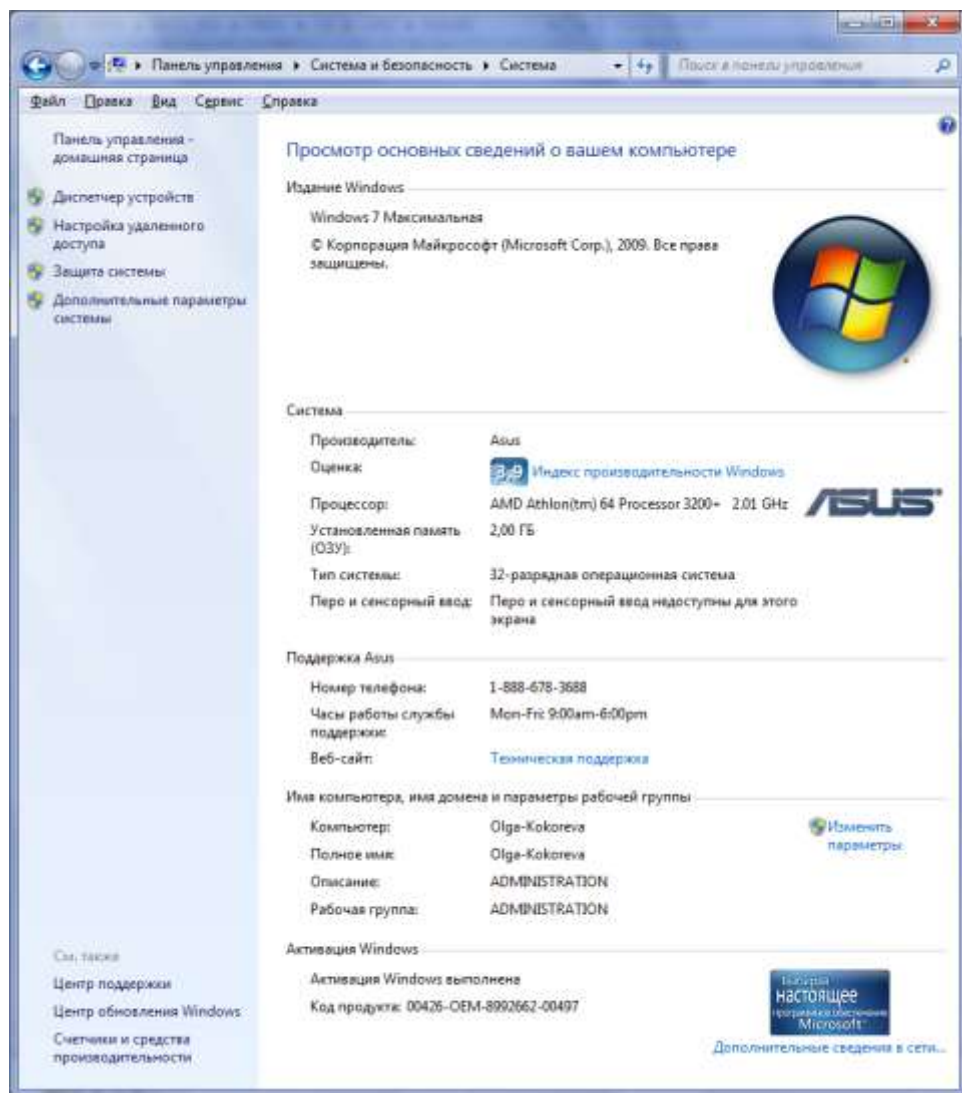


Рис. 13.1. Основная информация о системе включает Индекс производительности Windows (кстати, в данном случае он совсем не плох — в этой системе поддерживается интерфейс Windows Aero и все, связанные с ним "полезности")

Индекс производительности Windows вычисляется индивидуально для каждой конкретной аппаратной конфигурации и базируется на оценках, выставляемых по каждой из следующих категорий: **Процессор** (Processor), **Память** (RAM), **Графика** (Graphics), **Графика для игр** (Gaming Graphics) и **Основной жесткий диск** (Primary Hard Disk). Как будет показано чуть далее, окончательная оценка выставляется не на основе осредненной оценки по всем компонентам (что можно было бы предположить), а по самой низкой оценке, выставленной по любой из перечисленных категорий. Целая часть индекса производительности представляет собой так называемый *базовый уровень* (base score) — например, две аппаратные конфигурации с индексами 4.5 и 4.9 представляют системы базового уровня 4.

Для Windows Vista были определены следующие базовые уровни производительности:

- ❑ **уровень 1** — самая низкая из возможных оценок, которую может получить компьютер, способный работать под этой операционной системой. В данной ситуации, как бы вы ни старались, а высокой производительности добиться нельзя, и без радикальной модернизации обойтись просто невозможно;
- ❑ **уровень 2** — на этом компьютере можно использовать знаменитый интерфейс Windows Aero, но время от времени на нем будут возникать серьезные проблемы с производительностью, особенно если при включенном Windows Aero запустить большое количество приложений;
- ❑ **уровень 3** — стандартный и достаточно неплохой уровень. Его обычно получают компьютеры, имеющие логотип Windows Premium Logo (с предварительно установленной Windows Vista Home Premium). На таких машинах интерфейс Aero включается автоматически и хорошо работает при использовании одного монитора. При работе с двумя мониторами (особенно с высоким разрешением) время от времени могут возникать проблемы с производительностью;
- ❑ **уровень 4** — так называемый уровень *хай-энд* (High End). Высокопроизводительная конфигурация, обычно с двухъядерными процессорами, быстрой памятью и дисками. Позволяет играть в трехмерные игры и хорошо работает с трехмерной графикой;
- ❑ **уровень 5** — действительно мощная конфигурация. Наиболее высокий уровень из доступных для Windows Vista.

Таким образом, в Windows Vista индексы производительности Windows могли варьироваться от 1.0 до 5.9. В Windows 7 диапазон значений WEI был расширен. Изменились и правила присвоения базового уровня, которые теперь более точно отражают реально существующую ситуацию. Общие пра-

вила ранжирования систем, существовавшие в Windows Vista, в основном, применимы и к Windows 7. Но, как только что было сказано, в Windows 7 добавились новые уровни: 6.0 и 7.0. Это означает, что на текущий момент Windows 7 может выставить максимальную оценку 7.9. Эти новые уровни отражают технологический прогресс, достигнутый в области ключевых технологий, а именно: твердотельных носителей (solid state disks), многоядерных процессоров и графических адаптеров нового поколения.

По официальным сведениям Microsoft, вновь введенные в Windows 7 уровни характеризуются так:

- **уровень 6** — модный игровой компьютер с поддержкой графики DX10 и высоких скоростей смены кадров при высоких экранных разрешениях (например, 40–50 кадров в секунду при разрешении 1280×1024);
- **уровень 7** — еще более высокие скорости смены кадров при еще более высоких экранных разрешениях. Такие компьютеры можно отнести к классу рабочих станций, рекомендуемых для эффективной работы с приложениями CAD, видео высокой четкости (HD video) и фотографиями.

В соответствии с информацией, приведенной на сайте Softpedia (<http://news.softpedia.com/news/Hardware-Configuration-for-the-Perfect-7-9-Windows-7-Score-102349.shtml>), компьютер, работающий под управлением Windows 7, получит максимально возможный индекс производительности, если он имеет восьмиядерный процессор, 8 Гбайт RAM, сверхскоростные твердотельные накопители и, наконец, видеоадаптер с поддержкой DirectX 10, для которого установлены драйверы, совместимые с моделью WDDM 1.1.

ПРИМЕЧАНИЕ

В свежееустановленных системах индекс производительности Windows определяется не совсем точно, как и в случае с системами, только что подвергшимися модернизации (рис. 13.2).

Чтобы получить точную оценку, щелкните по ссылке **Индекс производительности Windows**. Раскроется окно, показанное на рис. 13.3. Нажмите в этом окне кнопку **Обновить** (Update) — она появляется в том случае, когда в системе обнаруживается новое оборудование, или щелкните по ссылке **Повторить оценку** (Update My Score). В приведенном примере самую низкую оценку получил процессор (3,9), а самую высокую — основной жесткий диск (5,7). Общая оценка данной системы — всего лишь 3.9 (по компоненту, получившему наиболее низкую оценку).

Увеличить индекс производительности можно различными способами. Например, разыскать и установить новейшие драйверы и обновления, попы-

таться оптимальным образом настроить систему, а затем выполнить тест повторно. Таким путем удастся незначительно повысить общую оценку (на одну или несколько десятых). Но радикального повышения производительности можно добиться только серьезным обновлением оборудования — в частности, в рассмотренном примере слабым местом всей системы является процессор (который, впрочем, получил не такую уж и плохую оценку).

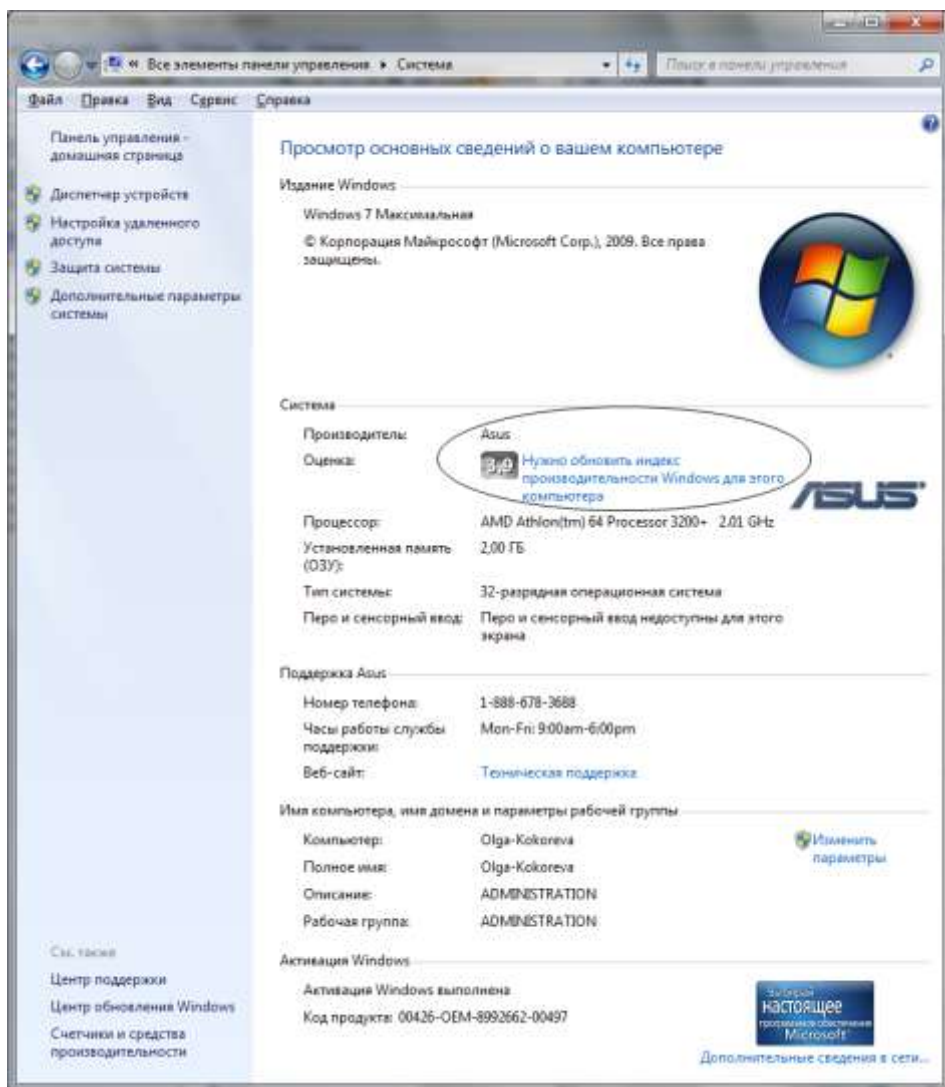


Рис. 13.2. После модернизации компьютера индекс производительности Windows нуждается в обновлении

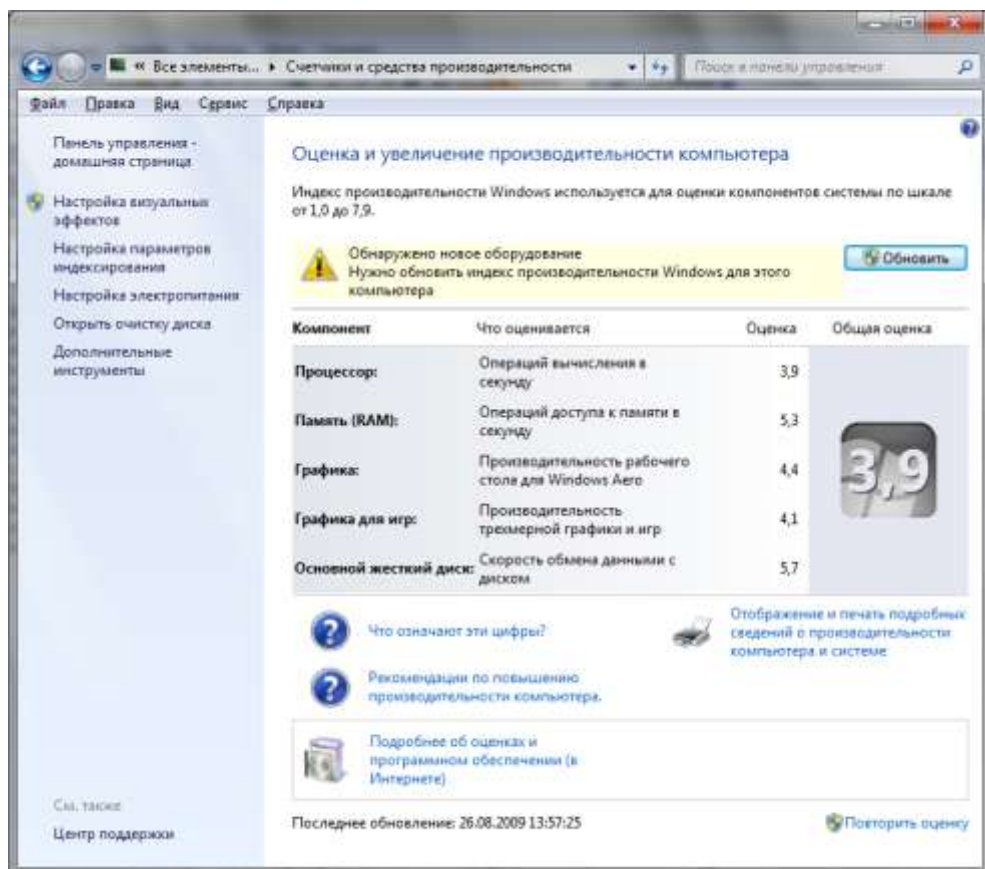


Рис. 13.3. Общая оценка уровня производительности компьютера выставляется не на основе усредненной оценки по всем компонентам, а по самой низкой оценке, выставленной по какой-либо одной из категорий

ПРИМЕЧАНИЕ

В Интернете имеется множество "твиков" и "хаков" (см., например, здесь: <http://www.mydigitallife.info/2007/08/29/modify-and-cheat-windows-vista-experience-index-rating-with-systempoint/>), позволяющих "подкрутить" индекс WEI. Мы рассмотрим их чуть далее в этой главе, но имейте в виду — фактически, они ничего вам не дадут — это просто будет "дутая" оценка, а реального повышения производительности вы не получите.

Интерпретация подуровней индекса производительности Windows

Кроме базового уровня (base score), у индекса производительности Windows существуют и *подуровни* (subscores). Умение интерпретировать эти подуров-

ни особенно важно для тех пользователей, которые планируют модернизацию (upgrade) компьютера или устраняют проблемы с производительностью операционной системы. По этой причине подуровни WEI заслуживают подробного рассмотрения³. Подразделяются они на пять категорий:

- ☐ подуровень индекса производительности процессора (Processor subscore);
- ☐ подуровень производительности по RAM (memory subscore);
- ☐ подуровень производительности графической подсистемы (Graphics subscore);
- ☐ подуровень графики для игр (Gaming graphics subscore);
- ☐ подуровень производительности основного жесткого диска.

Подуровень индекса производительности процессора

Этот подуровень оценивает производительность процессора при его загрузке задачами, типичными для большинства компьютеров, работающих под управлением Windows, в том числе:

- ☐ сжатие и распаковка данных с применением стандартного алгоритма LZW;
- ☐ сжатие и распаковка данных с применением встроенного алгоритма Windows, использующегося для файлов гибернации, ReadyBoost и других функций;
- ☐ шифрование и расшифровка;
- ☐ вычисление хэш-функций;
- ☐ кодирование видео.

Для получения окончательной оценки результаты нормализуются, после чего осуществляется их средневзвешенная оценка.

Для тестов производительности центрального процессора в Windows Vista было установлено три границы:

- ☐ процессоры с частотой 850 МГц, одноядерные AMD Athlon (K7) или Intel Pentium 4 соответствовали оценке 2.0. По мере роста производительности их оценка могла линейно возрасти до 4.7;
- ☐ оценки двухъядерных процессоров среднего ценового диапазона начинались с 4.8;
- ☐ высокопроизводительные двухъядерные процессоры из разряда High-End получали оценку от 5.8.

³ Более детальную и полную информацию о принципах оценки WEI в Windows 7 можно найти в следующих статьях:

<http://www.thevista.ru/page.php?id=10929> и <http://www.thevista.ru/page.php?id=11060>.

Как уже говорилось, в Windows 7 система оценки WEI поддерживает вплоть до 8 процессорных ядер (впрочем, она может без изменений использоваться и для 16-ядерных процессоров). В Windows 7 применяются следующие правила оценки процессоров:

- ☐ системы с производительностью, эквивалентной той, которую можно ожидать от CPU с одним или двумя физическими ядрами, могут получить оценку вплоть до 5.9;
- ☐ диапазон от 6.0 до 6.5 соответствует производительности системы с двухъядерным процессором из разряда High-End, который в Windows Vista мог получить оценку 5.9;
- ☐ диапазон от 6.3 до 6.9⁴ соответствует производительности систем с хорошим трехъядерным процессором. Оценка 6.9 определена исключительно для систем с производительным четырехъядерным процессором;
- ☐ оценки выше 7.0 соответствуют производительности четырехъядерного процессора среднего ценового диапазона;
- ☐ оценка 7.9 соответствует производительности восьмиядерного процессора с технологией SMT⁵.

ПРИМЕЧАНИЕ

В целом, оценка не строго привязана к числу ядер CPU. Скорее, она связана с уровнем производительности. Например, некоторые двухъядерные процессоры могут получить оценку выше, чем трехъядерные.

Подуровень производительности по RAM

Системная память является компонентом, играющим ключевую роль в оценке производительности системы. Этот подуровень основан на оценке общего объема памяти, установленной на вашем компьютере (исключая память,

⁴ Да-да, не стоит удивляться — в Windows 7 диапазоны действительно могут перекрываться, причем это перекрывание было сделано намеренно. Более подробную информацию по данному вопросу см. здесь: <http://www.techarp.com/showarticle.aspx?artno=622&pgno=0>, а перевод этой инсайдерской информации, полученной через <http://www.techarp.com>, на русский язык см. здесь: <http://www.thevista.ru/page.php?id=10929> и <http://www.thevista.ru/page.php?id=11060>.

⁵ SMT (Simultaneous Multi-Threading) — технология параллельной обработки потоков (SMT). Новая технология, идущая на смену Hyper-Threading. При ее использовании каждое ядро может одновременно обрабатывать два потока (таким образом, восьмиядерные процессоры смогут параллельно обрабатывать до 16 потоков). По предварительным данным это повышает производительность на 20–30% при выполнении таких задач, как мультимедийные приложения, базы данных, поисковые системы. Более подробную информацию можно найти по следующим адресам: http://en.wikipedia.org/wiki/Simultaneous_multithreading, <http://www.cs.washington.edu/research/smt/>, http://www.3dnews.ru/cpu/intel_dunnington_nehalem.

зарезервированную для графической подсистемы). Подуровни по оценке подсистемы памяти определены в табл. 13.1.

Таблица 13.1. Подуровни WEI по оценке подсистемы памяти

Объем памяти (RAM)	Наивысший подуровень производительности	Операционная система
< 256 Мбайт	1.0	Правила, действующие в Windows Vista и применимые для Windows 7
< 500 Мбайт	2.0	
≤ 512 Мбайт	2.9	
< 704 Мбайт	3.5	
< 960 Мбайт	3.9	
< 1,5 Гбайт	4.5	
< 3 Гбайт	5.5	Новые правила Windows 7
< 4 Гбайт	5.9 (только для 64-разрядных систем)	

ПРИМЕЧАНИЕ

Здесь следует отметить, что для высоких оценок (6+ и 7+) производительность памяти не будет определяющим фактором, кроме тех случаев, когда она окажется ниже результатов тестирования процессора. Вот основные причины, по которым это может произойти:

- подсистема памяти неправильно работает из-за ошибок (или неправильных настроек) BIOS;
- в систему были установлены неподдерживаемые модули памяти;
- вместо двухканальной системы доступа к памяти используется одноканальная;
- в систему — в ущерб производительности — была установлена более дешевая (и более медленная) память.

Подуровень производительности графической подсистемы

Этот подуровень указывает, насколько хорошо компьютер будет поддерживать Windows Aero и осуществлять воспроизведение видео. При выполнении данного теста оценивается полоса пропускания видеопамати (Мбайт в секунду), поэтому чем больший объем выделенной графической памяти установлен на вашем видеоадаптере, тем выше будет эта оценка. Графические адаптеры, не поддерживающие Microsoft DirectX 9, вне зависимости от каких бы то ни было прочих факторов, никогда не получают оценки выше, чем 1.0. Помимо этого, драйвер видеоадаптера, не соответствующий модели Win-

dows Vista Display Driver Model (WDDM)⁶, также не позволит выставить оценку выше, чем 1.9.

Подуровень графики для игр

Этот подуровень основывается на скорости обработки кадров (frames per second, кадров в секунду). Если видеоадаптер не поддерживает Microsoft Direct3D 9, он не получит оценки выше, чем 1.0. Видеоадаптер, поддерживающий Direct3D 9, DirectX 9 и WDDM автоматически получит оценку не ниже, чем 2.0.

В Windows 7 были добавлены новые наборы тестов DX10 — основные (или базовые) тесты DX10, а также тесты, основанные на новых функциях DX10. С точки зрения перспектив процедуры оценки, план состоит в том, чтобы скомбинировать оценки графических адаптеров класса DX10 и DX9 в соответствии со следующими правилами:

- ❑ оценка DX9-адаптеров будет ограничена 5,9;
- ❑ для достижения оценки 6.0 и выше требуется видеокарта DX10.

При этом правила оценки производительности видеоадаптеров в режиме DX9 остаются такими же, как для Windows Vista, а оценки для тестов DX10 выглядят следующим образом:

- ❑ <2.0 — система не поддерживает DX9 или DX10;
- ❑ 2.0–5.9 — так оцениваются адаптеры DX10, которые показывают в этом режиме производительность ниже, чем в режиме DX9, а также адаптеры, для которых установлены драйверы WDDM 1.0. В этом случае для таких адаптеров будет использоваться система оценки DX9 и будет игнорироваться производительность в режиме DX10;
- ❑ 4.0–4.9 — система показывает базовую производительность в играх DX10;
- ❑ 5.0–5.9 — хорошая производительность в играх DX10;
- ❑ 6.0–6.9 — пользователь может ожидать очень хороших показателей частоты кадров (40–50 кадров в секунду) в большинстве DX10-игр в разрешении 1280×1024 со всеми включенными функциями графики (кроме самых требовательных);
- ❑ 7.0+ — система показывает высокую частоту кадров (≥60 кадров в секунду) в требовательных играх в режиме 1280×1024. Во всех, кроме особо требовательных игр могут быть включены все доступные функции графики.

⁶ Дополнительную информацию о WDDM можно найти здесь: <http://msdn.microsoft.com/en-us/library/aa480220.aspx>.

Подуровень производительности основного жесткого диска

Этот подуровень оценивает скорость обмена данными с жестким диском (Мбайт/сек). Современные жесткие диски всегда получают оценку не ниже 2.0.

Инструмент WinSAT

Фактическая оценка производительности компьютера Windows Vista/7 осуществляется с помощью инструмента Windows System Assessment Tool (WinSAT). В состав Windows Vista и Windows 7 входит утилита командной строки Winsat.exe, которая запускается автоматически сразу же после установки Windows и перед тем, как во вновь установленной системе происходит первая регистрация пользователя. Результаты ее работы как раз и отображаются в окне информации о системе (см. рис. 13.1 и 13.2). При этом полученные результаты сохраняются в системном реестре в составе ключа HKLM\Software\Microsoft\Windows NT\Winsat (рис. 13.4) и в файлах XML, расположенных в составе папки %Systemroot%\performance\winsat\datastore (рис. 13.5). Для каждой оценки производительности создается отдельный файл, и каждый из таких файлов получает имя по дате и времени выполнения оценки. По умолчанию, в хранилище XML хранятся десять самых последних оценок.

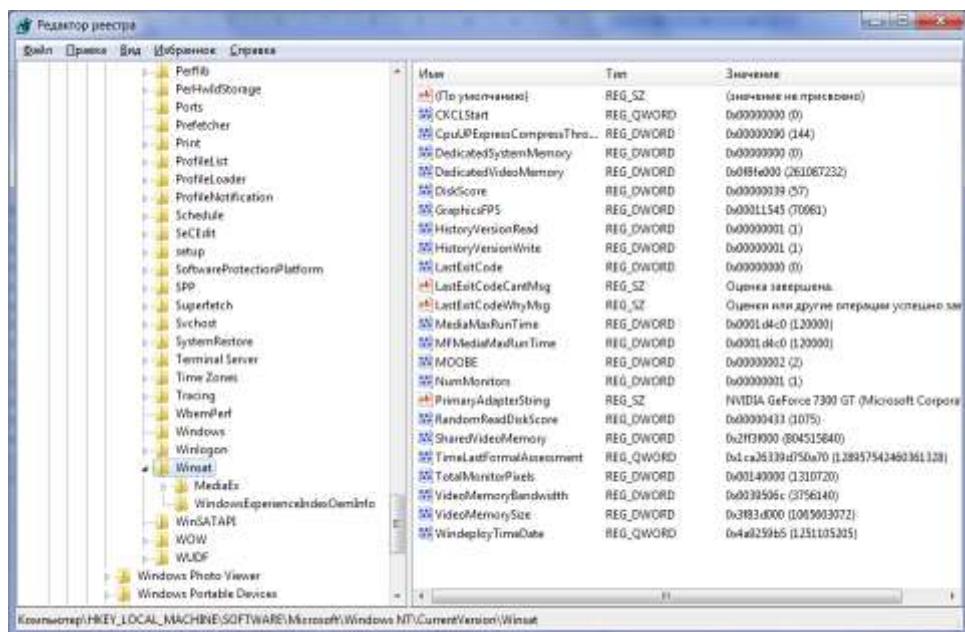


Рис. 13.4. Информация WinSAT в составе ключа реестра
HKLM\Software\Microsoft\Windows NT\Winsat

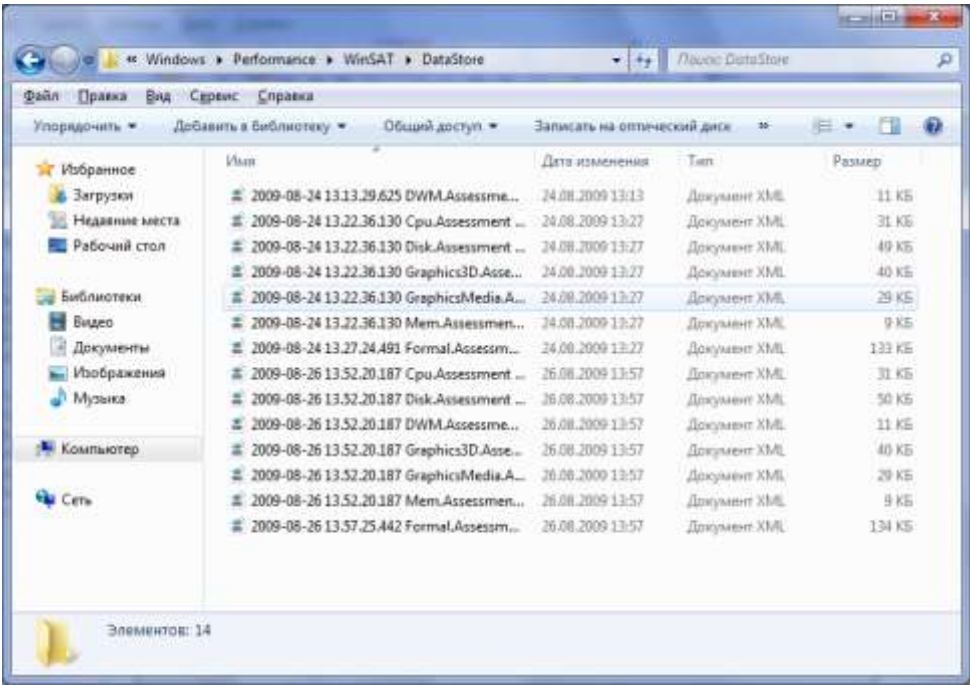


Рис. 13.5. Файлы данных WinSAT в хранилище данных XML

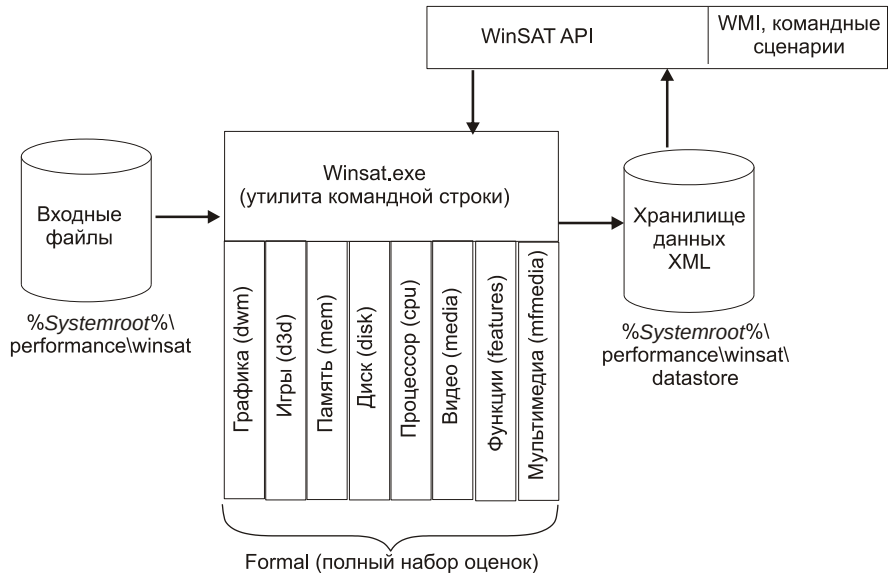


Рис. 13.6. Общая архитектура WinSAT

Кроме того, приложения могут получать доступ к индексу производительности Windows через специальный WinSAT API. Это позволяет разработчикам приложений реализовать в своих программах возможности самоконфигурации в соответствии с полученным значением WEI. За счет этой возможности приложения могут настраивать свои конфигурации так, чтобы их запуск не приводил к катастрофической потере производительности на слабых компьютерах. Наконец, утилита Winsat.exe может использоваться в командных сценариях. Общая архитектура WinSAT показана на рис. 13.6.

Запуск WinSAT из командной строки

Утилита Winsat.exe требует запуска из командной строки с административными привилегиями (рис. 13.7).

```

Администратор: Командная строка
Microsoft Windows [Version 6.1.7600]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.

C:\Windows\system32>winsat features
Средство оценки системы Windows
> DWM running... leaving it on
> Политика электропитания системного процессора сохранена и настроена на "Максимальную производительность"
> Поддержка: Перечисление возможностей
> Gathering System Information
> Operating System
      : 6.1 Build-7600
> Processor
      : AMD Athlon(tm) 64 Processor 3200+
> TSC Frequency
      : 0
> Number of Processors
      : 1
> Number of Cores
      : 1
> Number of CPUs
      : 1
> Number of Cores per Processor
      : 1
> Number of CPUs Per Core
      : 1
> Cores have logical CPUs
      : NO
> L1 Cache and line Size
      : 65536 64
> L2 Cache and line Size
      : 524288 64
> Intel physical mem available to the OS
      : 1.99 GB (2 145 902 592 bytes)
> Adapter Description
      : NVIDIA GeForce 7300 GT (Microsoft Corporation - WDDM)
> Adapter Manufacturer
      : NVIDIA
> Adapter Driver Version
      : 8.15.11.0693
> Adapter Driver Date (yy/mm/dd)
      : 2007/5/14
> Has DX9 or better
      : Yes
> Has Pixel Shader 2.0 or better
      : Yes
> Has LDM Driver
      : Yes
> Dedicated (local) video memory
      : 248.992MB
> System memory dedicated as video memory
      : 0MB
> System memory shared as video memory
      : 767.246MB
> Primary Monitor Size
      : 1200 x 1024 (1310720 total pixels)
> WinSAT is Official
      : Yes
> Время выполнения 00:00:00.00
> Остаток времени выполнения 00:00:01.05
> Восстановлена политика питания системного процессора

C:\Windows\system32>

```

Рис. 13.7. Пример вывода команды Winsat features

Утилита Winsat.exe в Windows Vista и Windows 7 использует следующий синтаксис:

```
winsat <test_name> [options]
```

Здесь [options] — поддерживаемые опции командной строки, а <test_name> — имя оценки, которое может принимать одно из следующих значений (см. рис. 13.6):

- ❑ dwm (Desktop Window Manager) — графика. Цель этой оценки заключается в выяснении возможности данной системы поддерживать комбинирован-

ный рабочий стол Windows Vista (Aero Glass). Запускать эту оценку можно только на системах, где установлены видеодрайверы с поддержкой WDDM;

- ❑ `d3d` (Direct 3D) — определяет игровые возможности системы;
- ❑ `mem` (Память) — оценка системной памяти;
- ❑ `disk` (Диск) — оценка возможностей дисковой подсистемы;
- ❑ `cpu` (Процессор) — оценка вычислительных возможностей процессора;
- ❑ `media` (Видео) — оценка производительности при кодировании и декодировании видео;
- ❑ `features` (Функции) — оценка производительности системных функций;
- ❑ `mfmedia` (Мультимедиа) — оценка производительности инфраструктуры мультимедиа;
- ❑ `formal` — полный набор оценок с сохранением результата.

Утилита `Winsat.exe` поддерживает следующие опции командной строки:

- ❑ `-help` или `-?` — вывод справки;
- ❑ `-v` — вывод подробной информации о выполнении и состоянии, а также об ошибках, если они имели место;
- ❑ `-xml <filename>` — имя файла, в котором должны быть сохранены результаты.

Рассмотрим примеры использования утилиты `Winsat.exe` из командной строки:

- ❑ вывод справочной информации: `winsat -help`;
- ❑ выполнение полного набора тестов (не поддерживается в Windows XP):
`winsat formal`;
- ❑ вывод информации об аппаратных средствах, включая количество процессоров и ядер, размер и другие характеристики кэша процессора L1 и L2, графическую память, разрешение и т. д.: `winsat features`;
 - эту команду лучше всего использовать с параметром `-xml <имя_файла>` для сохранения данных;
 - параметр `-eef` можно использовать для перечисления дополнительных компонентов, таких как оптические диски, модули памяти и другие элементы;
- ❑ запуск оценки диспетчера окон рабочего стола для создания оценки графики WinSAT: `winsat Dwmformal`;
- ❑ запуск оценки ЦП для создания оценки процессора WinSAT: `winsat Cpuformal`;

- ❑ запуск оценки памяти для создания оценки памяти (RAM) WinSAT:
`winsat Memformal;`
- ❑ запуск оценки графики для создания оценки графики для игр WinSAT:
`winsat Graphicsformal;`
- ❑ запуск оценки диска для создания оценки основного жесткого диска WinSAT: `winsat Diskformal;`
- ❑ тестирование процессора:
 - `winsat cpu -encryption` (шифрование AES256);
 - `winsat cpu -compression` (сжатие LZW);
 - `winsat cpu -encryption2` (вычисление хэша с использованием алгоритма SHA1);
 - `winsat cpu -compression2` (сжатие с использованием алгоритма Vista);
 - `winsat media -input {winsatencode.wmv} -encode {winsat.prx}` и `winsat mfmedia -input {winsat.wmv} -nopmp` (кодирование и декодирование видео, не поддерживается в WindowsXP);

ПРИМЕЧАНИЕ

Здесь `winsatencode.wmv` — рекомендованный видеоклип для оценки производительности декодирования видео, `winsat.prx` — файл, рекомендованный для оценки конфигурации кодирования медийных файлов, и `winsat.wmv` — рекомендованный видеоклип для оценки производительности инфраструктуры мультимедиа. Все эти файлы находятся в каталоге `%systemroot%\performance\winsat`.

- ❑ оценка памяти: `winsat mem;`
- ❑ оценка дисковой подсистемы:
 - `winsat disk -seq -read -n 0;`
 - `winsat disk -flush -n 0;`
- ❑ оценка графики и графики для игр:
 - `winsat dwm;`
 - `winsat graphicsformal -wddm` (не поддерживается в WindowsXP);
 - `winsat d3d -objs c(30) -alushader -totalobj 20` (пример теста Direct3D).

В число новых параметров для предварительного заполнения результатов оценки WinSAT, появившихся в Windows 7, входят следующие:

`Winsat prepop [-datastore <каталог>] [ -graphics | -cpu | -mem | -disk | -dwm ]`

Это приводит к созданию XML-файлов WinSAT, имена которых содержат строку `prepoper`, например:

0008-09-26 14.48.28.542 Cpu.Assessment (Prepop).WinSAT.xml

Чтобы создать полный набор итоговых XML-файлов, используйте команду `winsat prepoper`.

Также возможно произвести предварительное заполнение результатов для подсистемы, например, для ЦП. При этом имеются следующие зависимости:

- ☐ оценка ЦП имеет вторичную зависимость от оценки памяти;
- ☐ оценка памяти имеет вторичную зависимость от оценки ЦП;
- ☐ оценка графики имеет вторичную зависимость от оценок памяти и ЦП;
- ☐ оценка диспетчера окон рабочего стола может выполняться отдельно;
- ☐ оценка диска может выполняться отдельно.

Если оценка для вторичной зависимости не существует, то WinSAT запустит вторичную оценку вместе с запрошенной первичной оценкой. Например, команда `winsat prepoper -cpu` запустит тест ЦП и памяти, если XML-файл теста памяти отсутствует.

Как "подкрутить" индекс производительности в Windows 7

Сразу следует предупредить, что этот "трюк", несмотря на его внешнюю эффективность, на практике бесполезен. Результат будет поддельным, и реального повышения производительности вы не получите. Зато он довольно поучителен с образовательной точки зрения, потому что позволяет понять, как же формируется результат WEI. Поэтому выполним эту процедуру, понимая, что на самом деле она ни на что не влияет, а уже после этого займемся реальным повышением производительности Windows 7. Итак, проделаем следующее:

1. Запустите Windows Explorer и раскройте папку `%Windir%\Performance\WinSAT\DataStore`.
2. Найдите XML-файл, созданный последним — в нашем случае это будет файл `2009-09-11 12.52.54.571 Formal.Assessment (Recent).WinSAT.xml` (рис. 13.8). Присвойте себе права владельца на этот файл, а затем отредактируйте права доступа, дав себе возможность выполнения всех операций с данным файлом (подробно эти процедуры рассматривались в *главе 9*).
3. Откройте этот файл с помощью приложений Notepad.exe или Wordpad.exe и найдите тег `<WinSPR>` (рис. 13.9).
4. Отредактируйте этот фрагмент, как показано в листинге 13.1.

Листинг 13.1. Фрагмент XML-файла с оценкой индекса производительности, "подкрученный" так, чтобы система показывала фальшивый индекс

```
<WinSPR>
<SystemScore>7.9</SystemScore>
<MemoryScore>7.9</MemoryScore>
<CpuScore>7.9</CpuScore>
<CPUSubAggScore>7.9</CPUSubAggScore>
<VideoEncodeScore>7.9</VideoEncodeScore>
<GraphicScore>7.9</GraphicScore>
<GamingScore>7.9</GamingScore>
<DiskScore>7.9</DiskScore>
</WinSPR>
```

5. Теперь снова откройте окно **Система** (System) — посмотрите, как изменился индекс производительности Windows (рис. 13.10)!

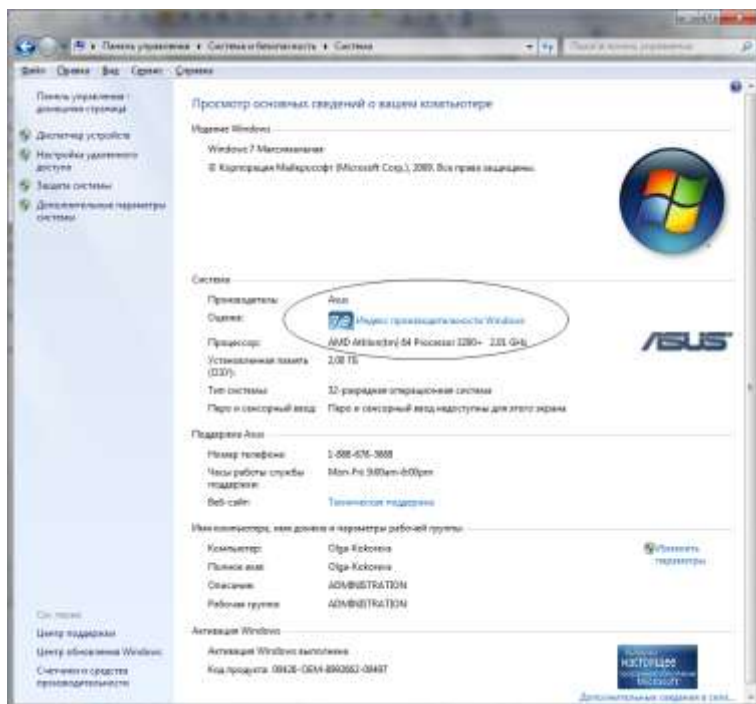


Рис. 13.10. Фальшивый индекс производительности Windows — это то же самое, что и "дутые" результаты ЕГЭ некоторых школьников

Что ж, индекс производительности мы подделали — но много ли от этого пользы? Во-первых, если вы внимательно прочли начальные разделы этой главы, вы сразу же увидите, что наш индекс "дутый" — достаточно обратить внимание на то, какой в системе процессор и какой в ней установлен объем памяти, а потом сравнить их с показателями, приведенными в разд. *Интерпретация подуровней индекса производительности Windows*, — работать быстрее и лучше ваш компьютер от этого "твика" все равно не станет. Наконец, индекс производительности Windows, носит чисто рекомендательный характер и предназначен для того, чтобы помочь пользователям определить, какие системные компоненты в первую очередь нуждаются в модернизации с тем, чтобы добиться от компьютера такой производительности, которая необходима им для решения конкретных задач, а вовсе не для того, чтобы бахвалиться им друг перед другом. Так что хватит баловства, а лучше давайте разберемся, как реально повысить производительность вашей системы, тем более, что резервов для этого более чем достаточно.

Настройка системы на оптимальную производительность

Классическим симптомом невысокой производительности является низкая скорость инициализации системы. Все операции, имеющие отношение к загрузке, происходят медленно, после регистрации в системе вам приходится долго ждать, прежде чем вы сможете нормально работать, а запускаемые приложения стартуют медленно. Программы зависают при выполнении операций чтения/записи на диск и т. д.

Однако при выполнении диагностики производительности имейте в виду, что выяснение истинных причин низкой производительности, как и устранение проблем с загрузкой (см. главу 11) требует творческого подхода. Здесь тоже возможны ситуации, когда общее впечатление обманчиво, и возникшая проблема просто маскирует другую, которая и представляет собой корень зла. Классический пример — медленные дисковые операции. На первый взгляд вам может показаться, что проблему вызывает жесткий диск, в то время как на самом деле проблема может быть вызвана нехваткой памяти!

Еще один характерный пример — ситуации, когда один процесс "поглощает" все ресурсы процессора, замедляя работу всех приложений. Это может происходить и в системах, имеющих более 2 Гбайт RAM, и наращивать память в этой ситуации попросту бесполезно. Гораздо лучше выявить приложение или драйвер, ведущий себя таким образом. Чаще всего оказывается, что проблема вызвана драйверами устройств, разработанными для Windows XP, или старым антивирусным программным обеспечением. Наконец, если вы пре-

небрегаете защитой системы и не установили совместимого антивирусного ПО, такое поведение системы с высокой степенью вероятности может быть вызвано и вирусной инфекцией, о чем тоже не стоит забывать.

Диагностика проблемы нехватки памяти

Рекомендованным методом выявления проблем производительности является использование встроенных средств Windows — Диспетчера задач Windows (Windows Task Manager) и Монитора надежности и производительности (Reliability and Performance Monitor). Как и в предыдущих версиях Windows, самым простым способом запустить Диспетчер задач является клавиатурная комбинация <Ctrl>+<Shift>+<Esc>. Для выявления проблем с производительностью после появления окна **Диспетчер задач Windows** (рис. 13.11) перейдите на вкладку **Быстродействие** (Performance).

Обратите внимание на следующие счетчики памяти:

- ❑ **Всего** (Total) — общий объем RAM, установленный на данном компьютере;
- ❑ **Кэшировано** (Cached) — чем выше это значение, тем лучше (например, если в системе установлено 2 Гбайт RAM, то для этого счетчика значение 1300 Мбайт будет вполне нормальным);

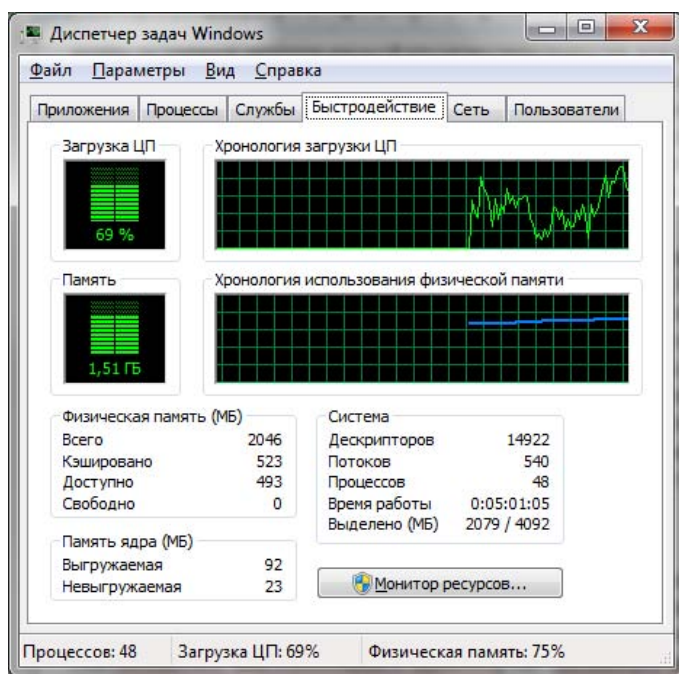


Рис. 13.11. Вкладка **Быстродействие** окна **Диспетчер задач Windows**

- **Свободно** (Free memory) — это новый счетчик, впервые введенный в Windows Vista. Низкое значение здесь, на самом деле, вполне нормально (обратите внимание на предыдущий счетчик — Windows использует большую часть доступной памяти под кэш именно для повышения производительности). Чуть далее в этой главе будет пояснено, почему в Windows Vista и Windows 7 "свободная память — это память, которая тратится впустую".

Пошаговая процедура оптимизации Windows 7

В отличие от "твика" с фальсификацией индекса производительности Windows 7, подборка советов, приведенных в этом разделе, действительно поможет вам оптимизировать производительность системы даже без радикальной модернизации аппаратных средств компьютера. Сначала рассмотрим приемы, которые можно выполнить с помощью пользовательского интерфейса, а затем — настройки, которые задаются только путем редактирования реестра. Пошагово выполните следующие операции:

1. Щелкните правой кнопкой мыши по значку **Компьютер** (Computer) на рабочем столе или в меню **Пуск** (Start). Из раскрывшегося контекстного меню выберите команду **Свойства**. Затем щелкните мышью по ссылке **Дополнительные параметры системы** (Advanced system settings). Откроется окно **Свойства системы** (System Properties), в котором перейдите на вкладку **Дополнительно** (Advanced), как показано на рис. 13.12. Обратите внимание, что есть и более простой и короткий метод открыть это окно непосредственно. Для этого можно ввести команду `sysdm.cpl` в поле поиска в меню **Пуск** (Start).
2. Теперь щелкните мышью по кнопке **Параметры** (Settings) в группе опций **Быстродействие** (Performance). На экране появится окно **Параметры быстродействия** (Performance Options), раскрытое на вкладке **Визуальные эффекты** (Visual Effects) (рис. 13.13). Установите в этом окне переключатель **Обеспечить наилучшее быстродействие** (Adjust for best performance). В этом случае окажутся отключены все визуальные эффекты, и пользовательский интерфейс будет настроен в стиле Windows XP.

Если вы хотите оптимизировать производительность Windows 7, но при этом не скатываться до упрощенного уровня Windows XP, а использовать наиболее интересные из новых возможностей пользовательского интерфейса Windows 7, установите флажки, соответствующие следующим опциям:

- **Включение композиции рабочего стола** (Enable desktop composition) — если вы хотите использовать одну из тем оформления рабочего стола в стиле Windows Aero;

- **Включить эффект прозрачности** (Enable transparent glass) — если вы хотите использовать эффекты полупрозрачности;
- **Отображать эскизы вместо значков** (Show thumbnails instead of icons) — если вы хотите отображать миниатюры при работе с Проводником (Explorer);
- **Отображать содержимое окна при перетаскивании** (Show window contents while dragging) — если вы хотите, чтобы содержимое окон отображалось при их перетаскивании;
- **Сглаживать неровности экранных шрифтов** (Smooth edges of screen fonts) — если вы хотите, чтобы экранные шрифты были настроены на максимальное удобство чтения с экрана;
- **Отбрасывание теней значками на рабочем столе** (Use drop shadows for icon labels on the desktop) — если вы хотите, чтобы значки на рабочем столе отбрасывали тени;
- **Использование стилей отображения для окон и кнопок** (Use visual styles on windows and buttons) — если вы хотите, чтобы рабочий стол и все остальные элементы рабочего стола были оформлены именно в стиле Windows Vista/7, а не Windows XP.

При использовании этих настроек все избыточные визуальные эффекты будут отключены, производительность оптимизирована, и при этом вы сможете пользоваться всеми преимуществами нового пользовательского интерфейса Windows 7 (если, конечно, они вам нравятся). С другой стороны, если вы привыкли к пользовательскому интерфейсу Windows XP, от своих привычек отказываться не хотите, и при этом компьютер у вас достаточно слабый, то смело блокируйте абсолютно все визуальные эффекты.

3. Откройте окно Проводника и на инструментальной панели выберите опции **Упорядочить** (Organize) | **Параметры папок и поиска** (Folder and Search Options). Перейдите на вкладку **Вид** (View), как показано на рис. 13.14.

Чтобы добиться максимальной производительности, сохранив при этом основные выигрышные черты пользовательского интерфейса Windows 7, на этой вкладке можно смело блокировать следующие опции:

- **Отображать сведения о размере файлов в подсказках папок** (Display file size information in folder tips);
- **Скрывать расширения для зарегистрированных типов файлов** (Hide extensions for known file types);
- **Отображать сжатые или зашифрованные файлы NTFS другим цветом** (Show encrypted or compressed NTFS files in color);

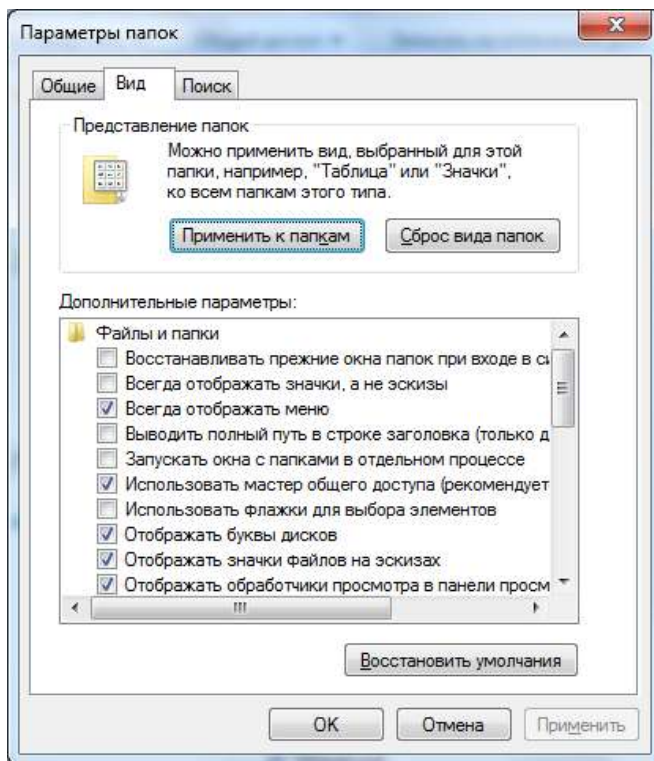


Рис. 13.14. Вкладка Вид окна Параметры папок

- **Отображать описания для папок и элементов рабочего стола** (Show pop-up description for folder and desktop items).
4. Щелкните правой кнопкой мыши по значку **Компьютер** на рабочем столе или в меню **Пуск**. Из раскрывшегося контекстного меню выберите команду **Управление** (Manage). В раскрывшемся окне выберите опцию **Службы и приложения** (Services & Applications), затем выполните двойной щелчок мышью по опции **Службы** (Services). Раскроется окно, показанное на рис. 13.15. Еще быстрее этого же результата можно добиться, введя команду `services.msc` в поле поиска меню **Пуск** или из сеанса командной строки. В раскрывшемся окне **Службы** вы можете перевести в режим ручного запуска (Manual) те сервисы, которые существенно замедляют процесс запуска операционной системы.

ПРИМЕЧАНИЕ

В Windows 7 нет необходимости в блокировке сервисов — достаточно перевести их в режим ручного запуска (Manual) — об этом уже упоминалось в главе 7.

Это очень удобно и абсолютно безопасно — в случае, если Windows потребует один из таких сервисов, операционная система сможет автоматически его запустить благодаря уже упоминавшейся возможности триггерного запуска. С другой стороны, если вы полностью блокируете какой-либо сервис, установив для него тип запуска **Disabled**, то система не сможет его запустить, и вы получите сообщение об ошибке. Список сервисов, которые безбоязненно можно перевести в режим ручного запуска, можно найти здесь: <http://www.askvg.com/windows-7-services-that-can-be-safely-set-to-manual/>.

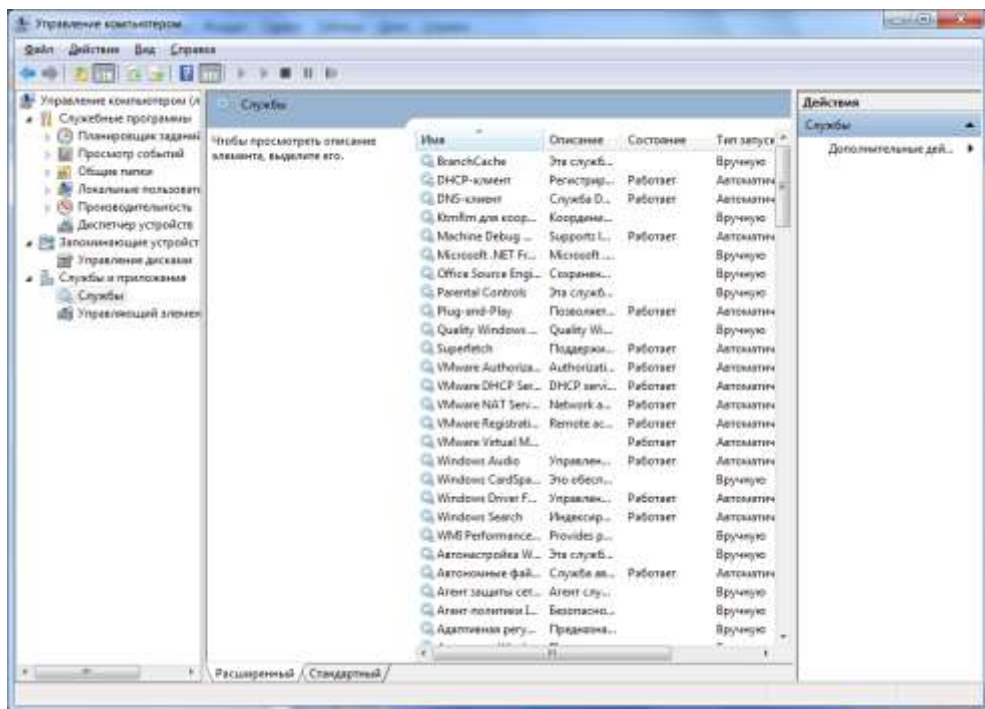


Рис. 13.15. Окно, позволяющее управлять работой служб Windows 7

- Из командной строки или через меню **Пуск** (Start) запустите утилиту *msconfig.exe*. Перейдите на вкладку **Автозагрузка** (Startup) и блокируйте все программы, автоматически стартующие при запуске системы, кроме тех, которые действительно абсолютно необходимы. В частности, вы без риска можете блокировать автоматический запуск утилит, управляющих дополнительными возможностями графических адаптеров и звуковых карт (рис. 13.16).

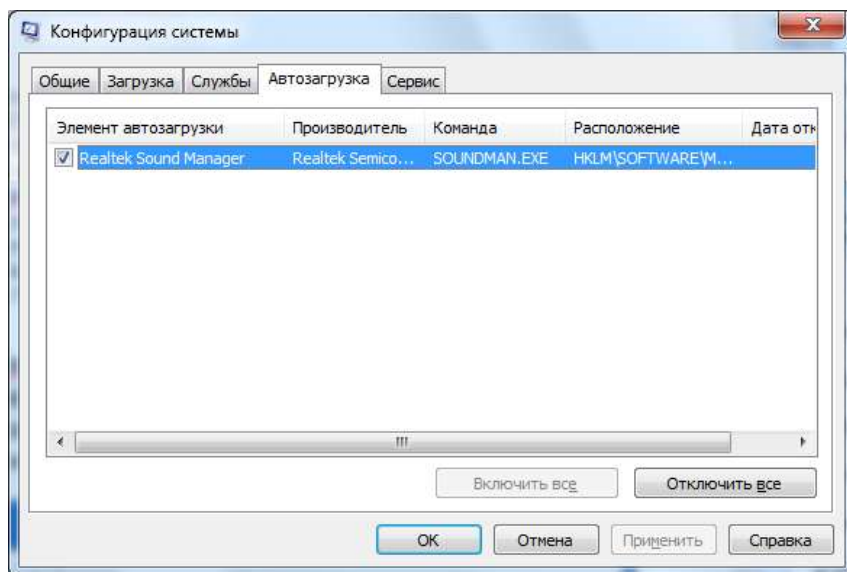


Рис. 13.16. Блокировка элементов автозагрузки

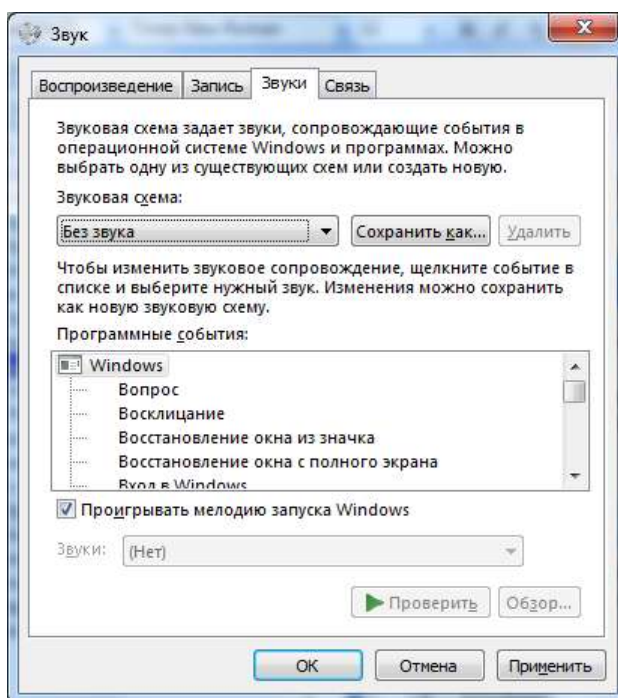


Рис. 13.17. Вкладка Звуки диалогового окна Звук

6. Запустите апплет **Звук** (Sound) Панели управления. Быстрее всего это можно сделать, дав команду `mmsys.cpl` из меню **Пуск** (Start) или из сеанса работы с командной строкой. Перейдите на вкладку **Звуки** (Sounds) и выберите из раскрывающегося списка **Звуковая схема** (Sound Scheme) опцию **Без звука** (No Sounds), как показано на рис. 13.17. Впрочем, вы можете избирательно блокировать некоторые системные звуки, оставив нужные вам.
7. Наконец, выполняйте следующие рекомендации:
 - регулярно производите дефрагментацию жесткого диска;
 - устанавливайте только то дополнительное ПО, с которым вы действительно будете работать;
 - устанавливайте новейшие драйверы для ваших устройств;
 - не игнорируйте установку важных обновлений Windows.

Использование возможностей ReadyBoost и SuperFetch

Так какой же объем памяти требуется для нормальной работы с Windows 7? Однозначный и простой ответ — одного гигабайта, рекомендуемого минимальными требованиями к аппаратной конфигурации, явно мало (хотя по личному опыту могу сказать, что даже при 1 Гбайт RAM Windows 7 ведет себя намного лучше, чем Vista). Как минимум, я бы рекомендовала иметь систему, в которой установлено 2 Гбайт RAM. Кроме того, если вы хотите преодолеть проблему нехватки памяти, обратите внимание на такие возможности Windows Vista/7, как ReadyBoost и SuperFetch.

Эти средства повышения производительности были рассмотрены в *главе 7*, здесь же будут просто сделаны некоторые замечания и рекомендации по их использованию.

ReadyBoost

Функция ReadyBoost — это фактически еще один способ "добавить памяти" в вашу систему! Использование кавычек объясняется просто — на самом деле вы не добавляете в систему физическую RAM, а просто даете системе указание использовать носитель USB 2.0 Flash в качестве сверхбыстрого виртуального кэша. Это решение довольно экономично, поскольку хотя физическая RAM и лучше подходит для кэширования, но и ее стоимость выше, чем стоимость флэш-памяти. При этом время произвольного доступа у флэш-памяти примерно на порядок меньше, чем у жесткого диска. К числу поддерживаемых устройств относятся устройства USB Flash, флэш-карты Secure Digital, Compact Flash, а также внутренние карты PCI Express. Именно поэтому,

если вас интересует экономный метод повышения производительности, и рекомендуется обратить внимание на данный метод "наращивания памяти".

Параметры реестра и настройки функции ReadyBoost были описаны в *главе 7*, так что не будем здесь на них останавливаться. Ответим только на ряд распространенных вопросов, которые могут у вас возникнуть, если вы заинтересуетесь этой возможностью:

- ❑ использование части пространства носителя USB автоматически уменьшит объем пространства, доступного для хранения файлов. Кроме того, наилучшим соотношением между физической RAM и памятью, отведенной для использования на носителе Flash USB, является пропорция 1:1. Если объем памяти на носителе Flash USB превысит объем RAM, физически установленной в системе, производительность снова начнет падать;
- ❑ в системе можно иметь не более одного устройства ReadyBoost, и MP3-плееры для этой цели использовать нельзя — они с данной технологией несовместимы;
- ❑ если вы внезапно удалите носитель Flash USB, используемый как устройство ReadyBoost, ничего ужасного не произойдет, так как все страницы, находящиеся на устройстве, присутствуют и в файле подкачки на диске;
- ❑ "трюк", описанный в *главе 7*, рекомендуется опробовать только в качестве эксперимента. Если же вы всерьез заинтересовались функцией ReadyBoost и захотели ее применять в своей повседневной работе, выберите устройство Flash USB, полностью удовлетворяющее требованиям ReadyBoost⁷, в противном случае вы можете быть разочарованы полученным результатом.

Реабилитация SuperFetch

Одной из наиболее популярных жалоб на Windows Vista была следующая: "Куда подевалась вся моя свободная память?" Такие пользователи обычно говорят: "Вот в Windows XP ее было так много! А в Vista сколько памяти ни добавь, все будет мало!" Причина этих жалоб — банальное непонимание принципа, заложенного в основу функции SuperFetch. Хуже того, любители "трюков" с реестром очень любят блокировать SuperFetch через параметры реестра, которые были описаны в *главе 7*. А еще они любят удалять все файлы с расширением pf, хранящиеся в каталоге %Windir%\Prefetch, чтобы "освободить дисковое пространство". Имейте в виду — эти "трюки" не только бесполезны, а попросту вредны, и сейчас я объясню почему.

⁷ Подробную информацию об устройствах, подходящих для ReadyBoost, можно найти здесь: <http://blogs.msdn.com/tomarcher/archive/2006/06/02/615199.aspx>.

Прежде всего, сама технология SuperFetch ориентирована на то, чтобы ускорить загрузку приложений с диска, преодолев таким образом "узкое место", вызванное медленным дисковым вводом/выводом. В Windows Vista/7 вся свободная оперативная память используется как кэш — а не как ресурс — именно для того, чтобы быстрее загружать нужные приложения в нужное время.

Чтобы лучше понять эту идею, вспомним, как обращалась с памятью Windows XP. Когда ей требовалось больше памяти, она вытесняла данные в файл подкачки. Таким образом, если пользователь на время отлучался от компьютера, а в это время на машине запускался другой процесс, все запущенные пользователем приложения и их данные вытеснялись в файл подкачки. При этом, по завершении фонового процесса, данные, которые были вытеснены в файл подкачки, не загружались обратно в память автоматически. И когда пользователь возвращался обратно и снова приступал к работе, система "тормозила", поскольку данные, вытесненные в файл подкачки, необходимо было снова загрузить в память.

Функция SuperFetch была разработана именно с тем, чтобы избежать такой проблемы и услужливо предоставлять приложениям все необходимые им данные без необходимости вновь загружать их из файла подкачки. Именно поэтому — чем больше памяти использовано под кэш (см. рис. 13.11) и чем меньше осталось "свободной" — тем лучше. В Windows Vista/7 ситуация обстоит так: свободная память — это выброшенная память! Что же касается папки %Windir%\Prefetch, то эти данные используются функцией SuperFetch, и удалять их тоже не следует (в любом случае, "экономия" дискового пространства будет ничтожной, а вот в производительности вы проиграете). И блокировка функции SuperFetch только снизит производительность.

Единственный случай, когда блокировка SuperFetch может вам помочь, — это если вы хотите поиграть в какую-нибудь старую игру, которой требуется много свободной памяти. Как заблокировать SuperFetch, вы, видимо, уже догадались и сами — ведь параметры реестра, управляющие настройками этой функции, были описаны в *главе 7*. Напомним, что это параметры EnablePrefetcher и EnableSuperfetch в составе ключа HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\MemoryManagement\PrefetchParameters.

Эти параметры могут принимать следующие значения:

- ☐ 0 — функция заблокирована;
- ☐ 1 — упреждающая выборка при запуске приложений;
- ☐ 2 — упреждающая выборка при загрузке;
- ☐ 3 — упреждающая выборка при загрузке и запуске приложений.

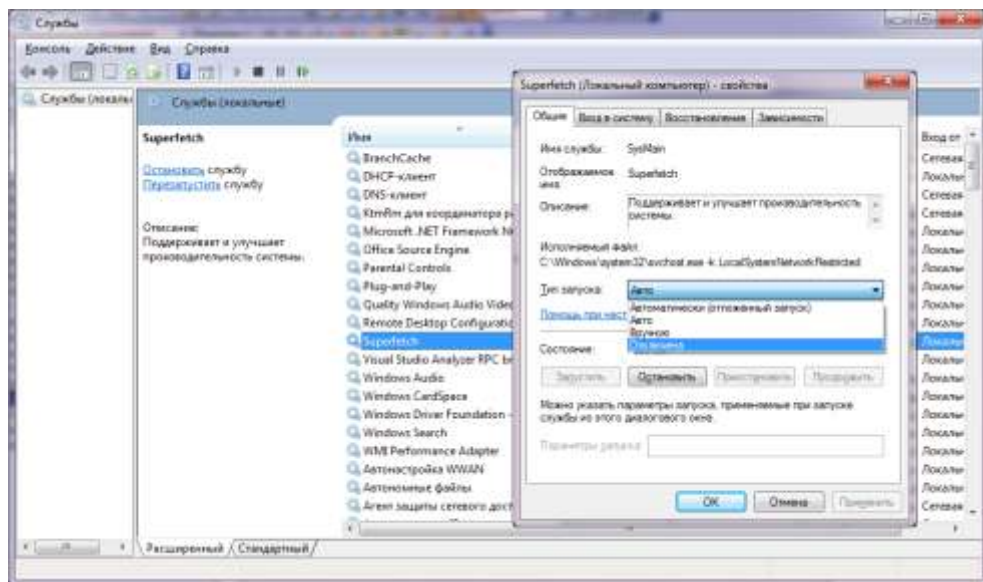


Рис. 13.18. Блокировка сервиса SuperFetch

Еще один (еще более простой) метод блокировки SuperFetch — остановить соответствующий сервис (рис. 13.18). Если хочется блокировать — блокируйте, но не ждите никакого выигрыша в производительности!

В заключение обсуждения функций ReadyBoost и SuperFetch развенчаем один популярный миф, а именно — что функцию SuperFetch можно активизировать в Windows XP, добавив в состав ключа `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\MemoryManagement\PrefetchParameters` параметр `EnableSuperFetch`.

Абсурдность этого совета должна быть очевидна каждому, кто хоть немного понимает принципы работы упреждающей выборки. В Windows XP нет такого сервиса, и в ядре Windows XP нет такой строки. Раз команда не существует, она и не может быть выполнена.

Настройка файла подкачки

Если Windows Vista/7 сталкивается с проблемами нехватки адресного пространства в физической памяти (RAM), она, как известно, использует файл подкачки на жестком диске. Использование файла подкачки — это не самоцель, а скорее, просто неизбежное зло. Однако в отношении файла подкачки тоже существует множество легенд и мифов, и некоторые из них развенчать я далее и постараюсь.

Чтобы посмотреть настройки файла подкачки в вашей системе, откройте окно **Панель управления** (Control Panel), запустите апплет **Система** (System), выполните щелчок по ссылке **Дополнительные параметры системы** (Advanced System Settings), на вкладке **Дополнительно** (Advanced) раскрывшегося окна **Свойства системы** (System Properties) в группе опций **Быстродействие** (Performance) нажмите кнопку **Параметры** (Settings). На экране появится окно **Параметры быстродействия** (Performance options), раскрытое на вкладке **Визуальные эффекты** (Visual Effects) — см. рис. 13.13. Раз уж мы озабочены проблемой производительности на слабом компьютере, то задержитесь на этой вкладке и установите переключатель **Обеспечить наилучшее быстродействие** (Adjust for best performance). Все визуальные эффекты будут отключены. Большого выигрыша вы, правда, не получите, но это все же лучше, чем ничего (уж этот совет, по крайней мере, безвреден).

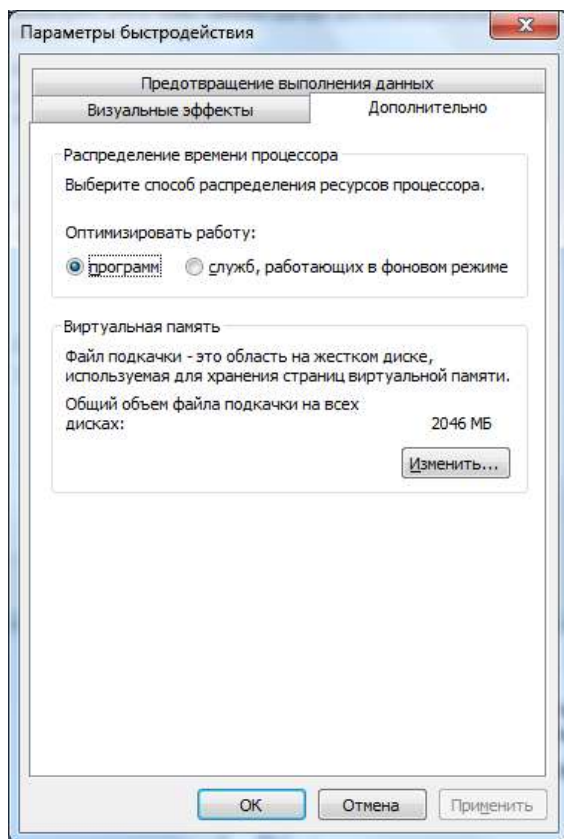


Рис. 13.19. Вкладка **Дополнительно** (Advanced) окна **Параметры быстродействия** (Performance options)

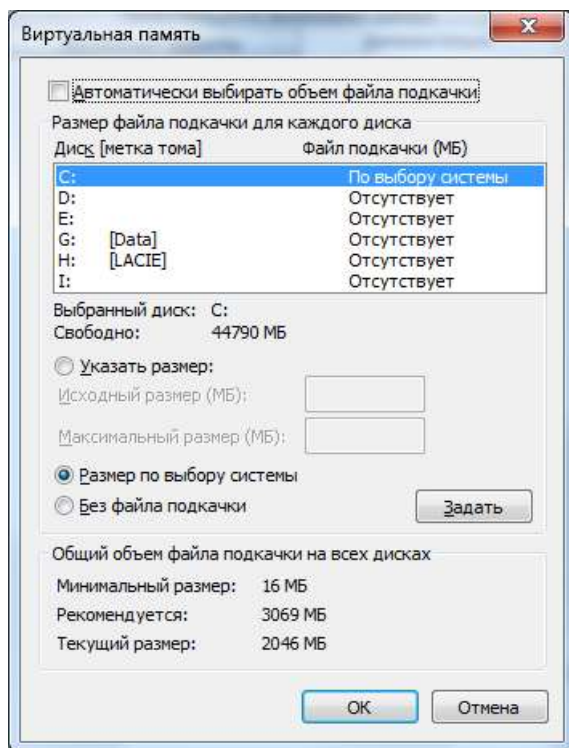


Рис. 13.20. Окно Виртуальная память (Virtual Memory)

Затем перейдите на вкладку **Дополнительно** (Advanced), показанную на рис. 13.19. В группе опций **Виртуальная память** (Virtual memory) нажмите кнопку **Изменить** (Change), после чего на экране откроется окно **Виртуальная память** (Virtual Memory), показанное на рис. 13.20.

При нормальных условиях размер файла подкачки должен составлять от 1 до 1,5 от объема физически установленной в системе памяти.

А теперь развенчаем самый популярный миф в отношении файла подкачки, который гласит, что производительность системы можно повысить, если файл подкачки (pagefile.sys) переместить в другой раздел физического жесткого диска. Это — чепуха, и никакого повышения производительности вы такой манипуляцией не добьетесь. На самом деле вы ее только уроните, потому что в этом случае система будет лихорадочно позиционировать считывающие головки жесткого диска, прыгая между разделом Windows и разделом, на котором расположен файл подкачки. Если вы действительно хотите повысить производительность, то лучшее, что вы сможете сделать — это переместить файл подкачки не просто в другой раздел, а на другой физический

жесткий диск. В этом случае Windows действительно будет обрабатывать запросы на ввод и вывод быстрее. Так что, если файл подкачки находится в загрузочном разделе, то Windows будет выполнять запросы на чтение и запись как системной папки, так и файла подкачки. При перемещении же файла подкачки на другой физический жесткий диск конкуренция между запросами на чтение и запись будет уменьшена.

Очистка файла подкачки при выходе из системы

Некоторые программы третьих фирм могут временно хранить незашифрованные пароли или другую важную информацию в памяти в простом текстовом формате (plain-text). Эта информация может оставаться в файле подкачки, представляя потенциальную угрозу для безопасности системы. Таким образом, для пользователей, реально заинтересованных в обеспечении безопасности, было бы желательно, чтобы в процессе завершения работы системы файл подкачки pagefile.sys системы регулярно очищался и не содержал бы в себе потенциально опасных данных.

ПРИМЕЧАНИЕ

Эта рекомендация применима для всех версий Windows, начиная с Windows NT 3.51. Очень важно иметь в виду, что очистка файла подкачки не подменяет собой меры по обеспечению физической защиты компьютера, а лишь помогает обеспечить безопасность данных, в то время, когда операционная система не запущена. Кстати, существует и еще одно распространенное заблуждение, а именно: очистка файла подкачки повышает производительность. В действительности дело обстоит как раз наоборот: очистка файла подкачки при завершении работы системы не повышает ее производительность, а напротив, замедляет процесс останова. Тем не менее, пользователи, всерьез озабоченные проблемой безопасности, могут пойти на этот шаг и пожертвовать производительностью во имя защиты данных.

Для организации очистки файла подкачки во время завершения работы, выполните следующие действия:

1. Запустите редактор реестра и откройте следующий ключ (рис. 13.21):

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management
```

2. Найдите параметр `ClearPageFileAtShutdown` (тип данных — `REG_DWORD`). Именно этот параметр позволяет управлять очисткой файла подкачки во время останова системы (записывать или нет нули поверх данных, которые могут содержаться в файле подкачки). Этот параметр может принимать следующие значения:

- 0 (по умолчанию) — в этом случае перезапись файла подкачки нулями не производится (рекомендуется для пользователей домашних ПК, озабоченных проблемой производительности);

- 1 — в этом случае при останове системы содержимое файла подкачки будет затерто нулями (рекомендуется в производственной среде, где важно обеспечение безопасности).

ПРИМЕЧАНИЕ

Внесенные вами изменения вступают в силу только после перезагрузки компьютера.

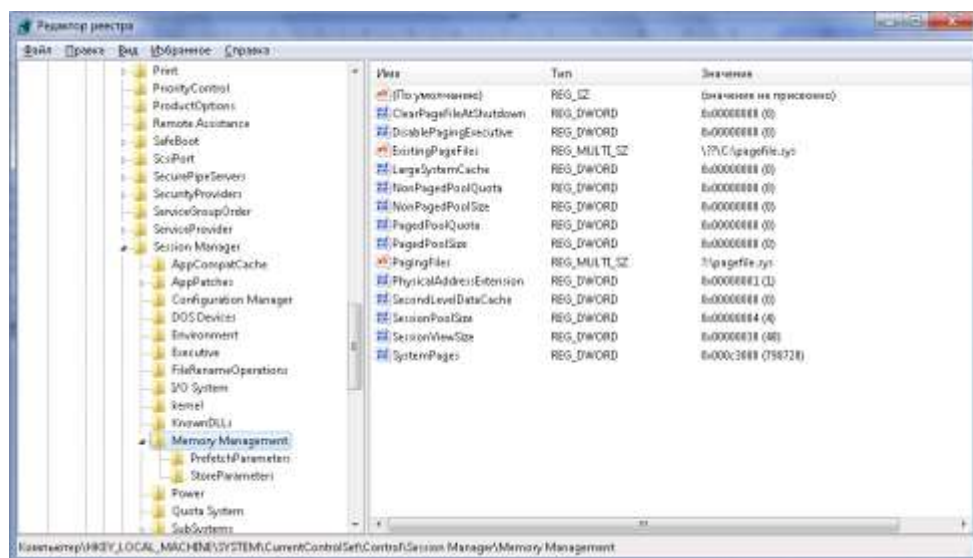


Рис. 13.21. Содержимое ключа реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management

Кроме того, в составе этого же ключа реестра есть еще парочка параметров, которыми можно воспользоваться для настройки подсистемы работы с памятью. Рассмотрим вкратце эти параметры:

- **DisablePagingExecutive** (тип данных REG_DWORD) — управляет тем, как подсистема памяти обращается с неактивными драйверами и системным кодом, работающими в режиме ядра. Этот параметр может принимать следующие значения:
 - 0 (по умолчанию) — говорит о том, что неактивные драйверы и системный код, работающие в режиме ядра, будут вытесняться из памяти в файл подкачки;
 - 1 — указывает, что неактивные драйверы и системный код, работающие в режиме ядра, будут оставаться в памяти резидентно и никогда не будут вытесняться в файл подкачки;

ПРИМЕЧАНИЕ

Следует отметить, что изменение значения этого параметра с нуля на единицу даст выигрыш в производительности только в одном случае — если требуется восстановить процесс, который был вытеснен из памяти в файл подкачки. В большинстве случаев редактировать значение по умолчанию не рекомендуется. Однако если у вас нет проблем с нехваткой памяти, то установка этого значения в 1 может ускорить работу системы при повторной активизации приложений, которые в течение определенного периода времени были неактивны.

- `LargeSystemCache` (тип данных `REG_DWORD`) — управляет размером кэша файловой системы. Этот параметр может принимать следующие значения:
- 0 (значение по умолчанию) — под кэш файловой системы выделяется стандартный объем RAM (менее 10 Мбайт). Это значение рекомендуется для обеспечения наилучшей производительности работающих в системе приложений;
 - 1 — будет использоваться большой кэш файловой системы (он может занять практически всю доступную файловую систему за вычетом 4 Мбайт). Эта опция подходит только в том случае, когда Windows Vista/7 работает в качестве сервера, а не рабочей станции или игрового компьютера. Имейте в виду, что установка этого значения на компьютерах, использующихся в качестве рабочих станций, может привести к существенному падению производительности.

Заключение

В этой главе в общих чертах были рассмотрены вопросы, связанные с тонкой настройкой и устранением неполадок в системе. Автор искренне надеется, что они помогут наиболее эффективно использовать возможности операционной системы Windows 7 и при необходимости разрешить возникшие технические проблемы. Все приемы, изложенные здесь, могут быть выполнены при помощи встроенных средств операционной системы. Однако существует также множество ценных инструментальных средств и утилит, разработанных сторонними фирмами, и эти средства, безусловно, могут оказать большую помощь в каждодневной работе с Windows 7.

Глава 14



Коллекция "твиков"

Любое устройство, требующее наладки и регулировки, обычно не поддается ни тому, ни другому.

*Универсальный закон
для молодых инженеров*

Вот теперь, когда мы обсудили наиболее общие принципы организации реестра, рассмотрели проблемы, которые могут быть вызваны его повреждениями и научились с ними бороться, можно попробовать осуществить некоторые настройки системы с помощью реестра.

Вы не забыли обо всех необходимых мерах предосторожности, упомянутых в *главе 2*? Если забыли, то перечитайте эту главу заново, выполните все предписанные там операции, создайте точку восстановления, выполните резервное копирование и только тогда приступайте! Я прочла немало книг о реестре практически всех вариаций Windows — начиная с Windows 9x и заканчивая Windows Vista, в названиях которых фигурировали слова "трюки" и "секреты". И вот что хочу вам сказать — ни один профессиональный трюкач не будет выполнять трюки без надлежащей страховки. Считайте, что выполнение всех процедур, предписанных в *главе 2*, — это ваша страховка и есть.

Настройка интерфейса

Многие пользователи просто обожают настраивать интерфейс нестандартным образом — "под себя", и понять их можно — этим они хотят как бы "выделиться из толпы". Причем подобное поведение характерно не только для пользователей Windows — приверженцы других операционных систем тоже очень любят заниматься индивидуальной настройкой интерфейса. Такие настройки называются *твиками* (tweaks), и как раз для любителей нестандартных интерфейсов создано множество утилит, называемых *твикерами*

и предназначенных менять как внешний вид, так и функциональные возможности операционной системы. Некоторые из таких утилит будут рассмотрены в *главе 15*, а здесь мы сосредоточимся именно на "ручном" твикинге. Эта информация будет вам полезна также, если впоследствии вы захотите самостоятельно создать подобную утилиту.

Сначала рассмотрим несколько полезных настроек пользовательского интерфейса (UI). Здесь, конечно, как всегда — часть настроек можно выполнить и с помощью встроенных административных утилит или инструментов графического интерфейса. Однако основное внимание мы уделим настройкам, которые возможно выполнить только путем редактирования реестра.

Изменение фонового изображения экрана регистрации в Windows 7 без применения сторонних инструментов

О настройке процесса регистрации в системе мы немного уже говорили в *главе 4*. Вернемся к этой теме и попробуем изменить экран регистрации (logon screen) в Windows 7. Экран регистрации — это тот самый экран, где вам предлагается выбрать пользователя, от имени которого вы желаете войти в систему, и ввести пароль. Стандартный экран регистрации в Windows 7 выглядит так, как показано на рис. 14.1.



Рис. 14.1. Стандартный экран регистрации в Windows 7

Но что, если нам хочется изменить этот экран, заменив, например, фоновое изображение? В Windows 7 это — элементарная операция, которая требует лишь внимательности и некоторых навыков редактирования реестра.

Итак, приступим. Для получения желаемого результата потребуется выполнить следующие шаги:

1. Запустите редактор реестра и раскройте ключ `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\Background`. Этот ключ разработчики Microsoft предназначили специально для OEM-производителей и энтузиастов твикинга. В составе этого ключа создайте параметр `OEMBackground` (тип данных — `DWORD`). Установите для него значение, равное 1. Это говорит о том, что вы хотите использовать нестандартный фоновый рисунок (рис. 14.2).

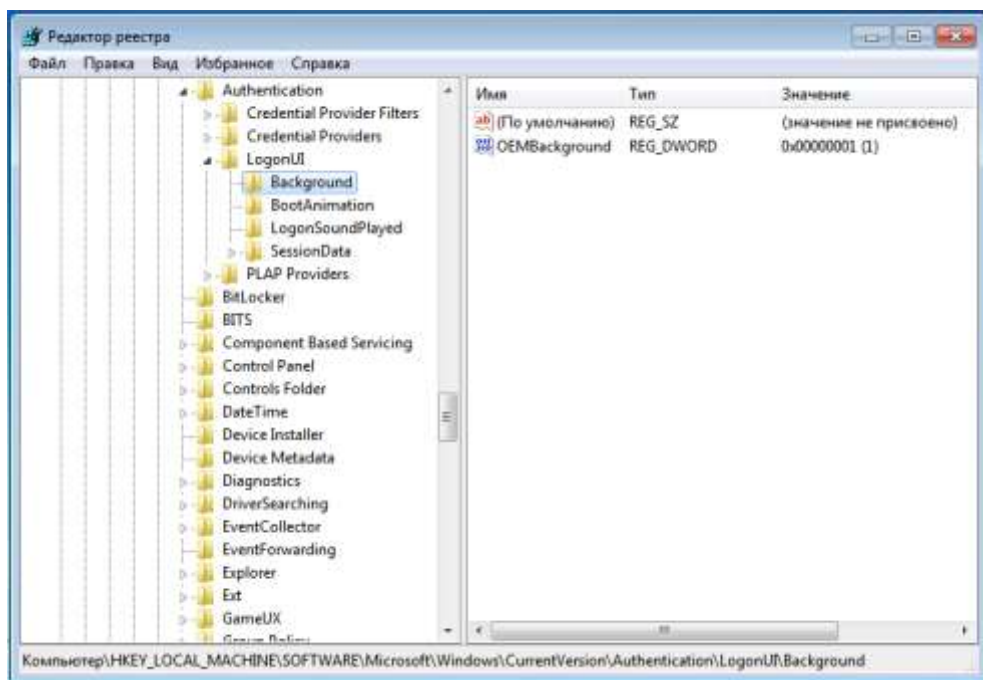


Рис. 14.2. Содержимое ключа реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\Background`

2. После создания ключа раскройте папку `%windir%\system32\oobe` и создайте в ней вложенную папку с именем `info`, а в ней — еще одну вложенную папку `backgrounds`. Полный путь к нужной нам папке будет выглядеть следующим образом: `%windir%\system32\oobe\info\backgrounds`.

3. В созданную папку `backgrounds` скопируйте изображение, которое вы хотите использовать в качестве фона для экрана регистрации в системе. Изображение должно быть представлено файлом в формате JPEG с разрешением, равным используемому вами экранному разрешению. Размер файла не должен превышать 256 Кбайт. Переименуйте файл изображения, присвоив ему имя `BackgroundDefault.jpg`.
4. Кроме того, рекомендуется с помощью любого из предпочитаемых вами графических редакторов создать на основе этого файла еще несколько файлов *JPEG* для самых распространенных экранных разрешений. Назовите эти файлы именами следующего вида: `BackgroundВысота×Ширина.JPG`. Имена файлов для самых распространенных видеорежимов могут выглядеть следующим образом:

- `Background768×1280.jpg`;
- `Background900×1440.jpg`;
- `Background960×1280.jpg`;
- `Background1024×1280.jpg`;
- `Background1280×1024.jpg`;
- `Background1024×768.jpg`;
- `Background1280×960.jpg`;
- `Background1600×1200.jpg`;
- `Background1440×900.jpg`;
- `Background1920×1200.jpg`;
- `Background1280×768.jpg`;
- `Background1360×768.jpg`.

В случае если система не может найти файла с именем, соответствующим текущему экранному разрешению, в качестве фона будет применено изображение из файла `BackgroundDefault.jpg`. При необходимости это изображение будет растянуто или сжато таким образом, чтобы полностью покрывать экран.

ПРИМЕЧАНИЕ

Если размер файла превышает 256 Кбайт, то изменение в силу не войдет. Кроме того, если вы смените тему оформления Windows 7, ваш нестандартный экран регистрации может быть отключен, потому что используемая тема оформления рабочего стола включает в себя, в том числе, и настройки экрана регистрации.

5. Чтобы проверить, вошло ли изменение в силу, достаточно выйти из системы. Если все операции были выполнены правильно, то экран регистра-

ции изменится на нестандартный. Вот, например, то, что получилось у меня (рис. 14.3).

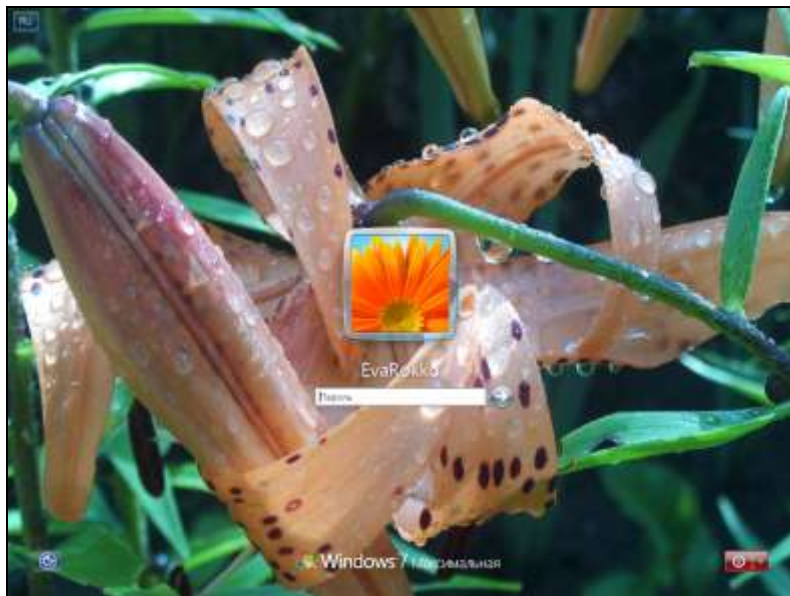


Рис. 14.3. Модифицированный экран регистрации в Windows 7

ПРИМЕЧАНИЕ

Оригинальный фон, по умолчанию используемый при отображении экрана регистрации, можно найти в файле `C:\Windows\System32\oobe\background.bmp`. При желании вы можете его отредактировать, а затем сохранить полученное изображение в папке `%windir%\system32\oobe\info\Backgrounds` под именем `BackgroundDefault.jpg`.

- Чтобы отменить внесенное изменение, достаточно установить значение параметра `ОЕМBackground` в составе ключа `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\Background` на 0 или просто удалить этот параметр.

Дальнейшие модификации экрана регистрации в Windows 7

Если вам понравился эффект, описанный в предыдущем разделе, знайте, что совершенно необязательно ограничиваться только им. Давайте продолжим наши упражнения и модифицируем текст, отображаемый на экране регистрации,

а также вид кнопок, представляющих существующие в системе учетные записи пользователей¹.

Модификация картинки пользователя

Для начала давайте изменим картинку, представляющую вашу учетную запись. Сделать это не просто, а очень просто, причем для этой цели даже не нужно редактировать реестр. Вполне достаточно стандартных средств пользовательского интерфейса. Прodelайте следующее:

1. Откройте окно Панели управления и выберите опцию **Учетные записи пользователей и семейная безопасность** (User Accounts and Family Safety) — вы очень быстро увидите, что среди опций, позволяющих управлять учетными записями пользователей, есть и опция, позволяющая изменить рисунок, представляющий выбранного пользователя (рис. 14.4).

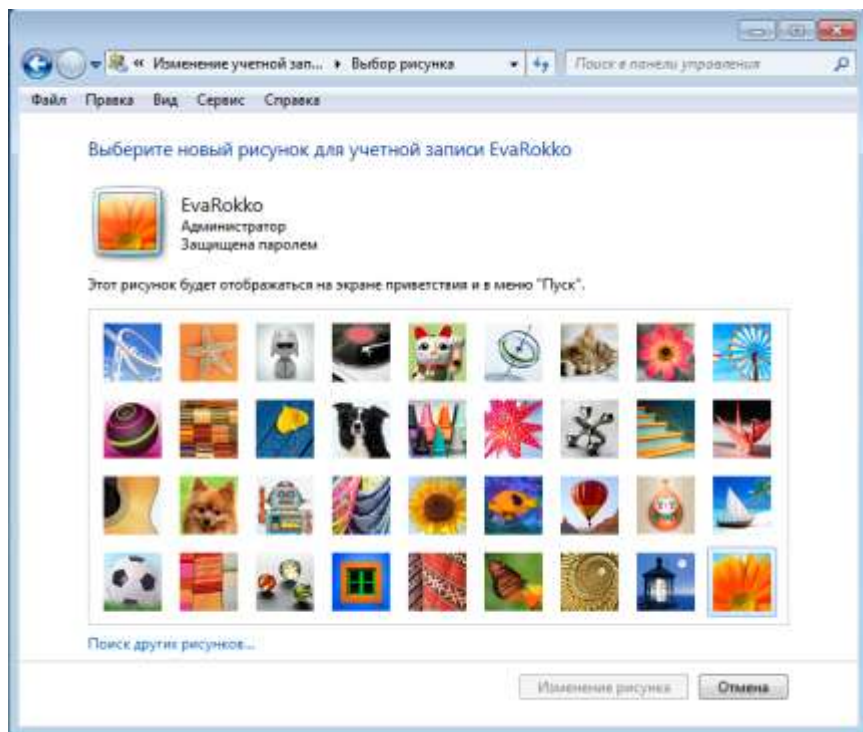


Рис. 14.4. Встроенные административные средства Windows 7 позволяют легко изменить рисунок, представляющий учетную запись пользователя

¹ Оба этих совета можно найти на множестве различных сайтов, посвященных "твикам" Windows 7, но впервые они были представлены Рафаэлем Риверой (Rafael Rivera) — см. <http://www.withinwindows.com/2009/06/13/tweak-your-windows-7-login-ui-button-set/>.

2. Обратите внимание, что в нижней части экрана имеется ссылка **Поиск других рисунков** (Search for other pictures). Пройдите по этой ссылке и выберите себе любой понравившийся рисунок. По умолчанию поиск предлагается начать с библиотеки изображений (рис. 14.5).

ПРИМЕЧАНИЕ

Выполнять поиск по библиотекам гораздо удобнее, чем бродить традиционным способом по файловой системе. Это, кстати, мой ответ на полемику, разгоревшуюся у меня с одним из других авторов, пишущих для нашего издательства (не будем указывать пальцем, кто конкретно это был). В ходе дискуссии с его стороны прозвучал такой тезис: "Про новые средства Windows 7 я пишу на протяжении всей книги. В частности, и про библиотеки там сказано. Но, должен заметить, ничего такого принципиально нового в них не видно". Да и вообще все эти вещи были им названы "сомнительными инновациями". Я ему ответила вполне конкретно: "А вы пользоваться ими пробовали?" Вот, попробуйте и убедитесь, что это действительно УДОБНО.

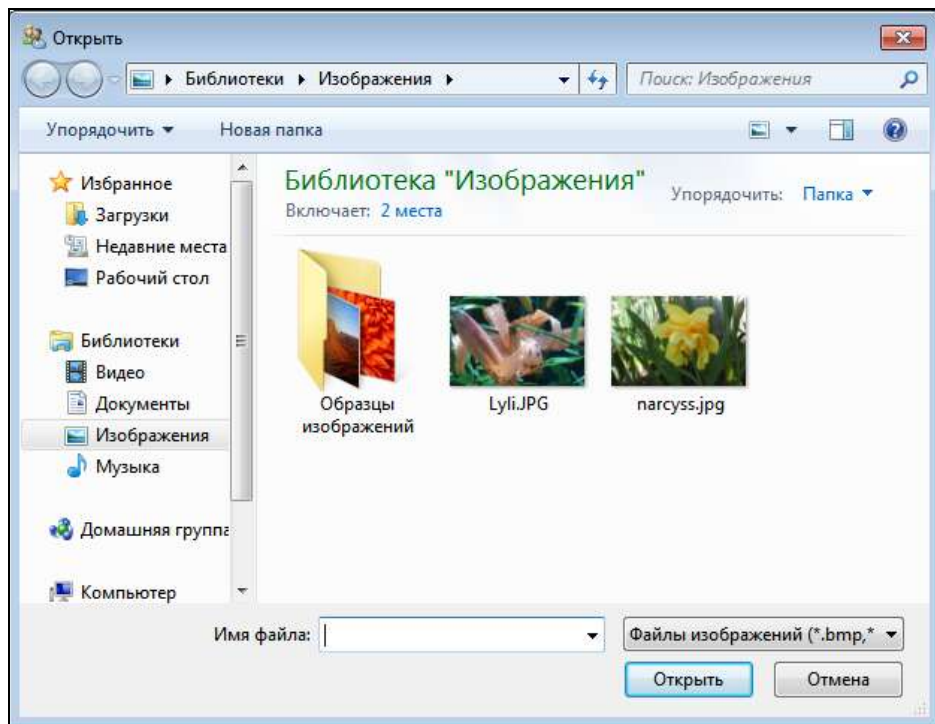


Рис. 14.5. По умолчанию поиск предлагается начать с библиотеки изображений

3. Итак, выберите понравившийся рисунок, нажмите кнопку **Открыть** (Open) и подтвердите внесенное изменение. Чтобы проверить, вошла ли

модификация в действие, выйдите из системы и посмотрите на полученный эффект (рис. 14.6).



Рис. 14.6. Изменение рисунка, представляющего пользователя

Модификация изображения кнопок, представляющих пользователей на экране регистрации

Теперь немного усложним задачу. Если вы измените стандартный фон на индивидуально подобранное изображение, у вас могут возникнуть небольшие проблемы с отображением самой экранной кнопки. Так, если вы выберете слишком светлый фон, то и сама кнопка, и входное имя пользователя могут отображаться недостаточно четко. Аналогичная ситуация возникнет и в случае, если вы выберете слишком темный фон, — и кнопка, и имя пользователя могут просто "потеряться".

Чтобы этого не случилось, давайте чуть-чуть изменим вид самой кнопки. Для этого проделайте следующие шаги:

1. Запустите редактор реестра и откройте ключ:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI
```

2. Создайте новый параметр с типом данных REG_DWORD, дайте ему имя ButtonSet, а затем присвойте ему одно из следующих значений:

- 0 — текст отбрасывает светлую тень, кнопка — более темную (это вариант, используемый Windows по умолчанию);
- 1 — текст отбрасывает более темную тень, кнопка полупрозрачна (этот вариант настройки удобен для светлого фона);
- 2 — текст не отбрасывает никакой тени, кнопка непрозрачна (этот вариант будет удобен для темного фона).

Старые рецепты по-прежнему работают

Старые-престарые рецепты по модификации процесса регистрации в системе, работавшие еще в Windows XP, по-прежнему действуют и в Windows 7.

Замаскируем в окне регистрации имя последнего зарегистрировавшегося пользователя

Вы можете настроить систему таким образом, чтобы в ней не отображалось имя пользователя, зарегистрировавшегося последним. Так же, как и в предыдущих версиях Windows, это делается с тем, чтобы повысить безопасность системы, усложнив угадывание паролей для тех, кто пытается получить к системе несанкционированный доступ. Экран регистрации при этом будет выглядеть так, как показано на рис. 14.7.

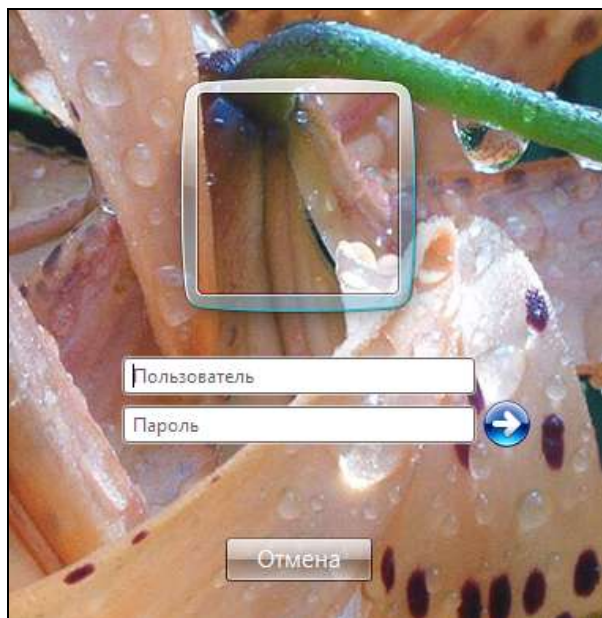


Рис. 14.7. Экран регистрации в системе, сконфигурированной так, чтобы не отображать имя пользователя, зарегистрировавшегося последним (как, впрочем, и других пользователей системы)

Как и ранее, это можно сделать различными способами. Первый из них заключается в использовании локальных политик безопасности. Чтобы выполнить эту задачу, сделайте следующее:

1. В меню **Пуск** (Start) выберите опцию **Панель управления** (Control Panel). Далее выберите опции **Система и безопасность** (System and Security) | **Администрирование** (Administrative Tools) | **Локальная политика безопасности** (Local Security Policy). Впрочем, наиболее простой и быстрый метод запуска этой оснастки MMC заключается в том, чтобы дать команду `secpol.msc` из командной строки или через поле поиска меню **Пуск**.

В левой части окна MMC разверните иерархический список **Параметры безопасности** (Security Settings), выбрав опции **Локальные политики** | **Параметры безопасности** (Local Policies | Security Options). В правой части окна MMC появится список правил, которые можно задать для локального компьютера.

2. Выполните двойной щелчок мыши, указав опцию **Интерактивный вход в систему: не отображать последнее имя пользователя** (Interactive logon: Do not display last user name) или же выберите из контекстного меню, выводимого по нажатию правой кнопки мыши, команду **Свойства** (Properties). На экране появится окно **Интерактивный вход в систему: не отображать последнее имя пользователя** (Interactive logon: Do not display last user name), показанное на рис. 14.8.
3. Чтобы имя пользователя, последним зарегистрировавшегося в системе, не отображалось на экране регистрации, установите в этом окне переключатель **Включен** (Enabled).
4. Чтобы проверить действие внесенного изменения, выполните выход из системы. Вы увидите, что экран регистрации будет выглядеть так, как было показано на рис. 14.7.

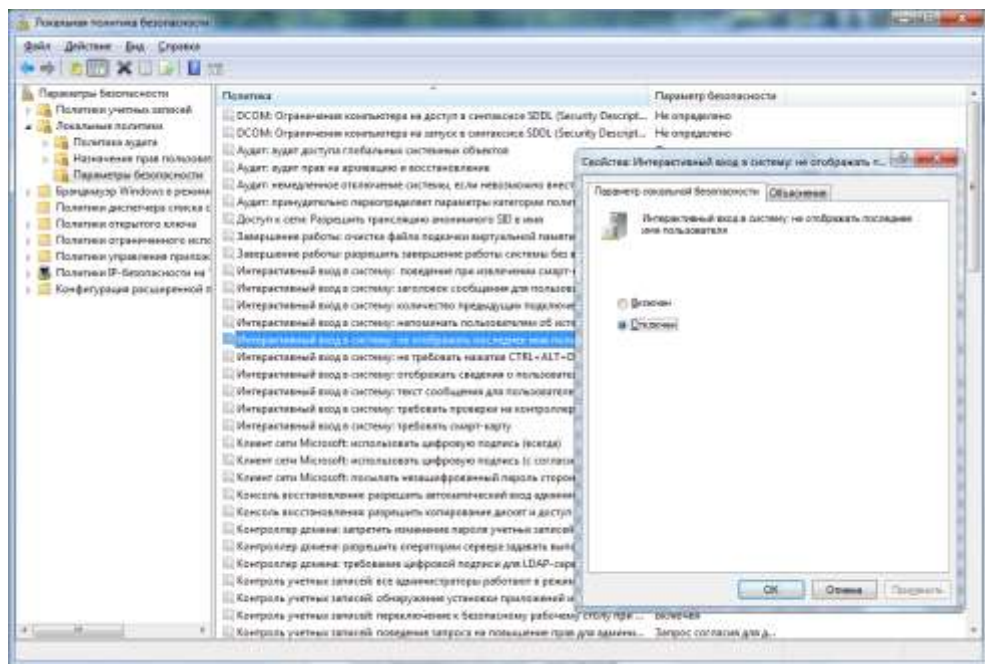


Рис. 14.8. По умолчанию политика **Интерактивный вход в систему: не отображать последнее имя пользователя** отключена

Пользователям вариантов поставки Windows 7, в которых отсутствует возможность работы с локальными политиками безопасности, придется вносить это изменение через реестр. Для этой цели вам потребуется выполнить следующее:

1. Запустите редактор реестра и раскройте ключ `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion`. В составе этого ключа найдите вложенные подключи `\Policies\System` (если эти подключи отсутствуют, то их следует создать).
2. Найдите в составе ключа `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Policies\System` параметр `dontdisplaylastusername` (тип данных `DWORD`), как показано на рис. 14.9. Если такого параметра нет, его следует создать. Присвойте параметру значение 1.

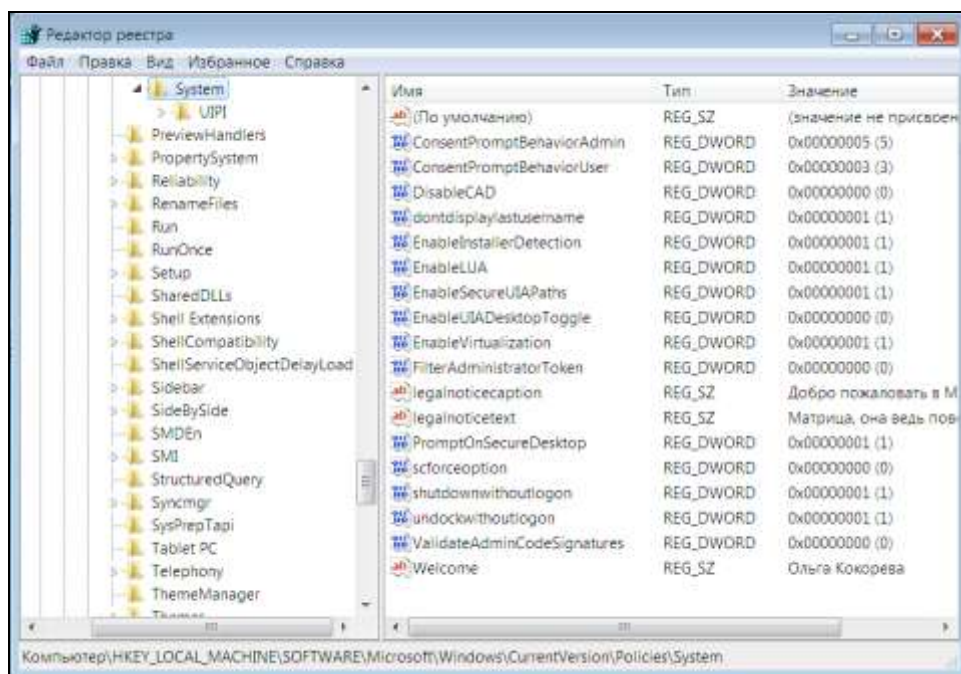


Рис. 14.9. Содержимое ключа реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`

Дополнительная защита компьютера от несанкционированного доступа

Чтобы дополнительно усилить защиту компьютера от несанкционированного доступа, можно потребовать, чтобы перед регистрацией пользователем необходимо было нажать клавиатурную комбинацию `<Ctrl>+<Alt>+<Del>` (рис. 14.10).



Рис. 14.10. Windows 7 можно настроить так, чтобы перед регистрацией пользователь должен был нажать клавиатурную комбинацию <Ctrl>+<Alt>+<Del>

ПРИМЕЧАНИЕ

Люди, сильно озабоченные безопасностью, обычно устанавливают такое требование, чтобы исключить возможность перехвата паролей.

Чтобы задать это требование, в составе того же ключа (HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Policies\System) найдите DWORD-параметр `DisableCAD` и установите для него значение 0.

ПРИМЕЧАНИЕ

Как и в предыдущем случае, эту задачу можно выполнить двумя способами: через локальные политики безопасности и через реестр.

Информационное сообщение для пользователей, регистрирующихся в системе

Наконец, как и в предшествующих версиях Windows, в Windows 7 можно создать информационное сообщение для пользователей, пытающихся зарегистрироваться на компьютере. Раз уж мы сосредоточились на редактировании реестра, то посмотрите еще раз на рис. 14.9. Обратите внимание на два параметра с типом данных `REG_SZ` — `legalnoticecaption` и `legalnoticetext`. Первый из них задает заголовок индивидуального сообщения, а второй — собственно сам текст.

ПРИМЕЧАНИЕ

Как и в Windows XP, в Windows Vista и Windows 7 для всех только что описанных настроек аналогичные параметры с теми же именами можно создавать и под ключом `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon`. Однако следует помнить, что параметры под ключом `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System` имеют приоритет, и если они установлены, то значения под ключом `Winlogon` не действуют.

Автоматическая регистрация в системе

Как и в предыдущих версиях Windows, в Windows 7 процедуру регистрации в системе можно автоматизировать, исключив необходимость вводить регистрационную информацию (входное имя, пароль и домен, которому он принадлежит).

ПРИМЕЧАНИЕ

Несмотря на то, что возможность автоматической регистрации выглядит весьма удобной, ее использование представляет определенный риск с точки зрения безопасности, поскольку каждый, кто имеет физический доступ к компьютеру, может также получить доступ как к хранящейся в нем информации, так и потенциально ко всем сетям, к которым он подключен.

Для того чтобы добавить регистрационную информацию с помощью Редактора реестра Regedit.exe:

1. Запустите Regedit.exe и найдите следующий подключ реестра:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon`

2. Найдите параметр `DefaultUserName` и установите его значение равным имени пользователя, который должен автоматически регистрироваться в системе.
3. Если значение `DefaultPassword` не существует, создайте новый значимый элемент, относящийся к типу данных `REG_SZ`, переименуйте его в `DefaultPassword` и в качестве его значения укажите пароль по умолчанию.
4. Если значимый элемент `AutoAdminLogon` не существует, создайте новое значение типа `REG_SZ`, переименуйте его в `AutoAdminLogon`, а затем установите его значение равным 1.
5. Сохраните ваши изменения и затем выйдите из программы Редактор реестра.
6. Закройте систему и перезагрузите компьютер.

После перезагрузки пользователь, заданный по умолчанию, будет автоматически зарегистрирован.

ПРИМЕЧАНИЕ

`AutoAdminLogon` представляет собой значимый элемент типа `REG_SZ`, а не элемент типа `REG_DWORD`. Обратите также внимание — чтобы активизировать автоматическую регистрацию, вам необходимо сбросить локальные установки безопасности (Local Security Setting) — **Свойства: Интерактивный вход в систему: не требовать нажатия CTRL+ALT+DEL** (Interactive logon: Do not require CTRL+ALT+DEL) — рис. 4.14.

Добавляем часто используемые приложения в контекстное меню рабочего стола

Совет, приведенный в этом разделе, действует не только для Windows 7, но и для Windows Vista. Если вы часто пользуетесь каким-либо приложением,

то можете не только прикрепить его к меню **Пуск** (Start) или вывести на Панель задач, но и добавить в контекстное меню рабочего стола.

На рис. 14.11 в качестве примера показано контекстное меню, в которое добавлены два дополнительных приложения: Windows Media Player и Process Monitor — утилита Марка Руссиновича (Mark Russinovich), которая будет более подробно рассмотрена в *главе 15*.

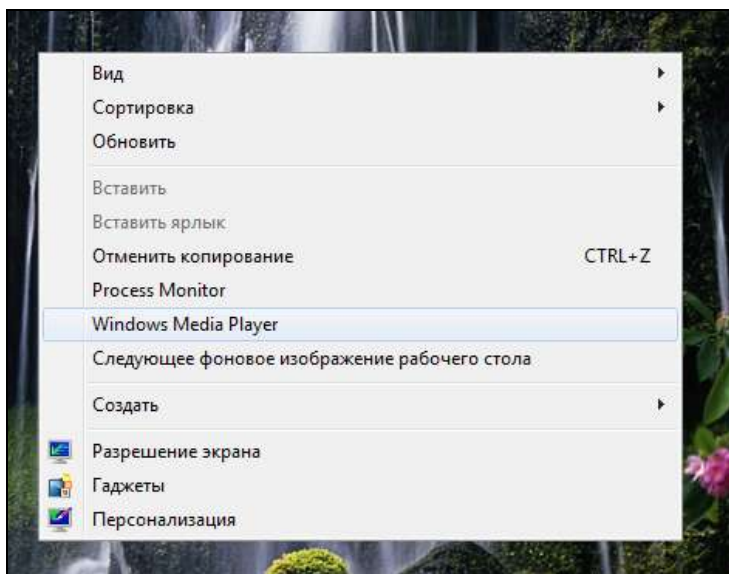


Рис. 14.11. Модифицированное контекстное меню, включающее команды для запуска часто используемых вами приложений

Чтобы добавить в контекстное меню рабочего стола какие-либо приложения, сделайте следующее:

1. Запустите Редактор реестра (Regedit.exe) и раскройте ключ: `HKEY_CLASSES_ROOT\Directory\Background\shell`.
2. В составе этого ключа создайте еще один ключ с именем, отражающим название вашего любимого приложения, которое вы хотите запускать через контекстное меню, например, WMP (Windows Media Player), Winamp, Firefox и т. п. Параметру По умолчанию (Default) в правой панели окна Редактора реестра присвойте значение, соответствующее названию команды, которое должно появляться в контекстном меню.
3. В составе этого ключа создайте еще один вложенный ключ с именем `command`. Для параметра По умолчанию (Default) в правой панели окна за-

дайте значение, отражающее полный путь к исполняемому файлу вашего приложения, например:

C:\Program Files\Windows Media Player\wmplayer.exe

C:\Program Files\Winamp\winamp.exe

C:\APP\Procmon\Procmon.exe

На рис. 14.12 показано, как должны выглядеть описываемые ключи.

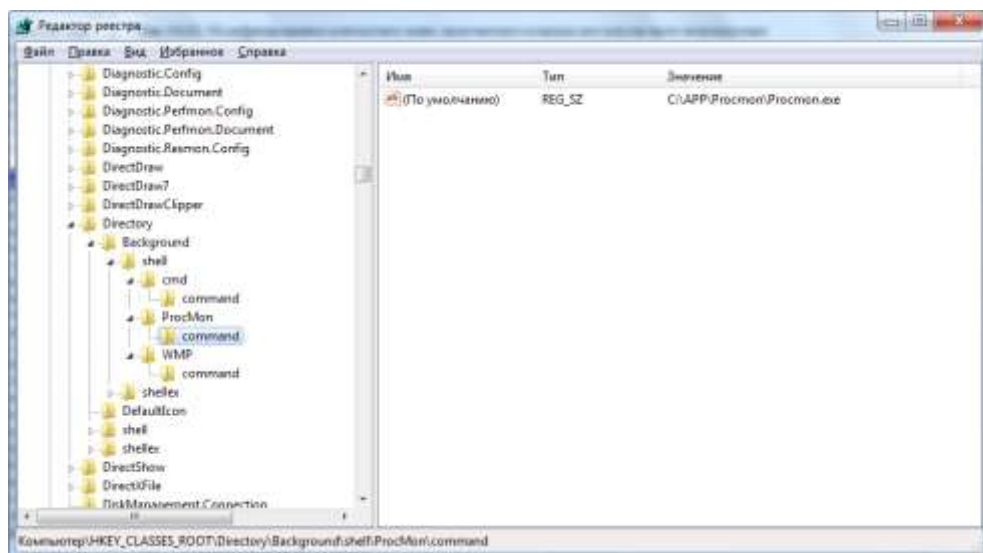


Рис. 14.12. Структура вложенных ключей реестра, добавляющих в контекстное меню рабочего стола команды для запуска приложений Windows Media Player и Process Monitor

4. Теперь протестируйте результат — раскройте контекстное меню рабочего стола и поочередно запустите добавленные в контекстное меню приложения.

ПРИМЕЧАНИЕ

При желании вы можете добавить в контекстное меню любое количество приложений.

5. Если вы не хотите перегружать стандартное контекстное меню, то можете добавить в состав всех ключей с именами приложений пустое строковое значение с именем `Extended` (рис. 14.13). В этом случае дополнительные команды будут отображаться в контекстном меню, если вы будете выполнять щелчок правой кнопкой мыши при нажатой клавише `<Shift>`.

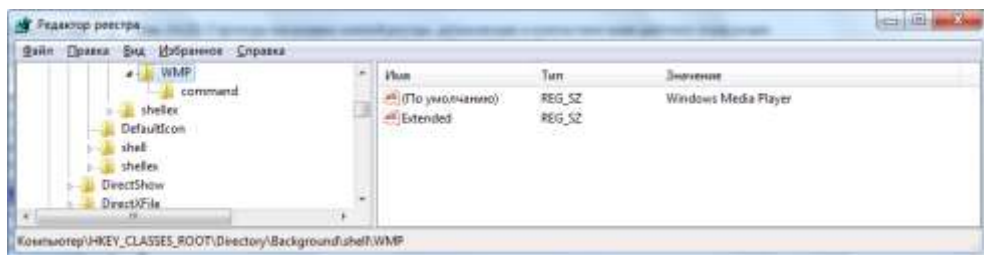


Рис. 14.13. Добавление пустого строкового значения с именем `Extended` приведет к тому, что дополнительная команда будет появляться в контекстном меню только при щелчке правой кнопкой мыши при нажатой клавише <Shift>

Скрываем значки библиотек в навигационной панели Проводника

По умолчанию при запуске Проводника Windows **Библиотеки** (Libraries) являются при навигации отправной точкой (рис. 14.14), что — да, действительно, нравится не всем пользователям. И предлагаемый рецепт подойдет как тем, кто считает, что присутствие значков библиотек при просмотре через Проводник — это излишество, так и тем, кто вообще обожает что-то прятать от пользователей.

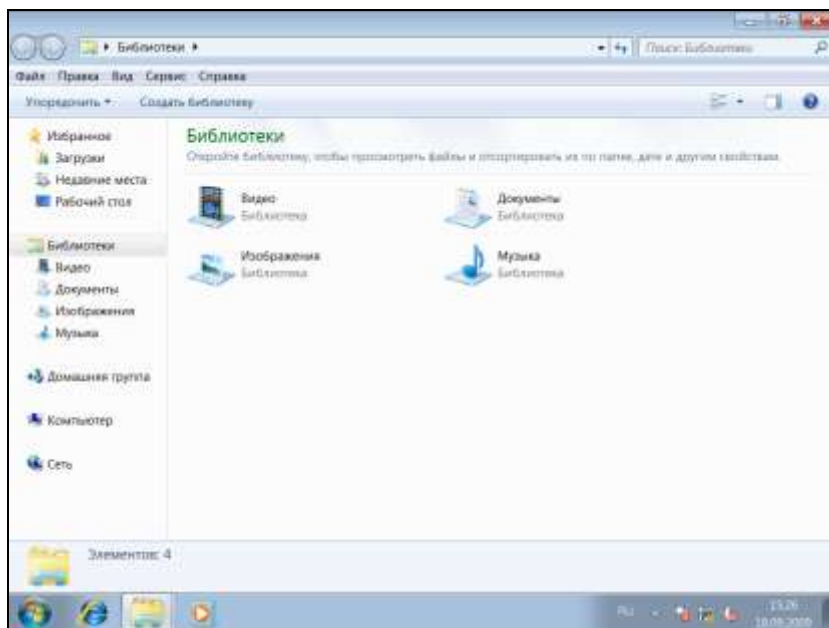


Рис. 14.14. По умолчанию при запуске Проводника Windows **Библиотеки** являются отправной точкой

Если вы тоже предпочитаете работать "по старинке", то можете убрать библиотеки из навигационной панели Проводника. При этом вы не блокируете библиотеки совсем — они по-прежнему будут вам доступны в составе вашего пользовательского профиля.

Итак, выполните следующее:

1. Запустите Редактор реестра и найдите ключ: `HKEY_CLASSES_ROOT\CLSID\{031E4825-7B94-4dc3-B131-E946B44C8DD5}\ShellFolder`.
2. Присвойте себе права владельца на этот ключ (как было описано в *главе 9*), а затем присвойте себе полный доступ к этому ключу реестра.
3. Вновь раскройте ключ реестра `HKEY_CLASSES_ROOT\CLSID\{031E4825-7B94-4dc3-B131-E946B44C8DD5}\ShellFolder` и измените значение шестнадцатеричного параметра `Attributes c` `b080010d` на `b090010d`, нажмите кнопку **ОК**, а затем выйдите из системы и зарегистрируйтесь повторно.
4. Обратите внимание — библиотеки исчезнут из навигационной панели Проводника (рис. 14.15), но при этом, они по-прежнему будут вам доступны, так что при желании вы сможете ими пользоваться (рис. 14.16).

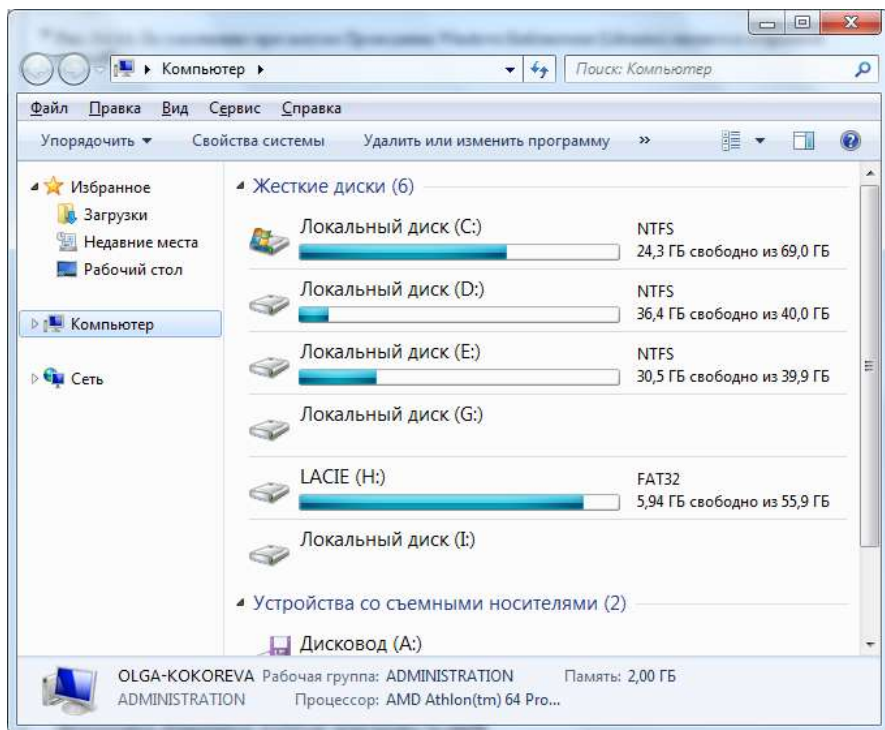


Рис. 14.15. Библиотеки исчезли из навигационной панели Проводника

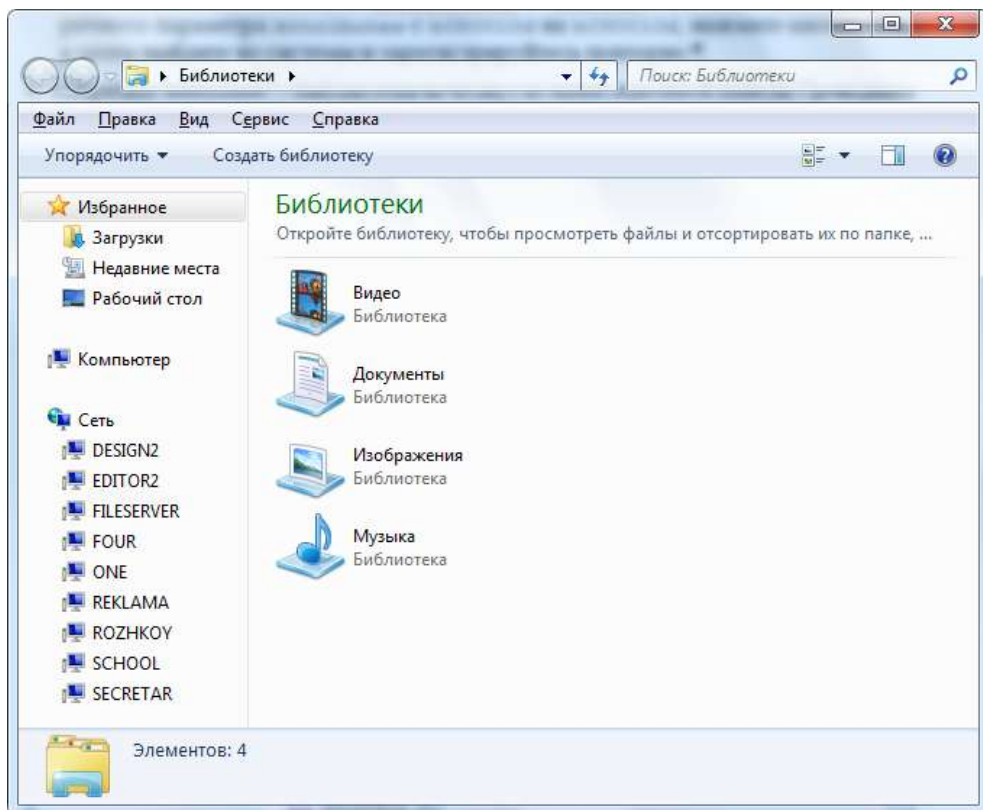


Рис. 14.16. Но, тем не менее, они по-прежнему остаются доступными, так что при желании ими можно пользоваться

5. Если полученный результат вас устраивает, на этом можно и остановиться. Не забудьте восстановить исходные права доступа к ключу реестра `HKEY_CLASSES_ROOT\CLSID\{031E4825-7B94-4dc3-B131-E946B44C8DD5}\ShellFolder` и вновь (как и было описано в *главе 9*) передать права владельца сервису `TrustedInstaller`.

ПРИМЕЧАНИЕ

Значок **Домашняя группа** (HomeGroup) исчезнет сам по себе, если вы не создавали домашней группы или блокировали поддерживающие ее сервисы (см. *главу 8*).

6. Внесенное изменение можно в любой момент отменить, если восстановить исходное значение параметра `Attributes(b080010d)` в составе ключа `HKEY_CLASSES_ROOT\CLSID\{031E4825-7B94-4dc3-B131-E946B44C8DD5}\ShellFolder`.

Впрочем, вы можете и полностью блокировать библиотеки, раз не хотите ими пользоваться. Для этой цели вам потребуется запустить Редактор реестра и внести следующие изменения:

1. Удалить следующие ключи реестра:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\
Desktop\NameSpace\{031E4825-7B94-4dc3-B131-E946B44C8DD5}
```

```
HKEY_CLASSES_ROOT\CLSID\{031E4825-7B94-4dc3-B131-E946B44C8DD5}
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{031E4825-7B94-4dc3-B131-
E946B44C8DD5}
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\
FolderDescriptions\{2112AB0A-C86A-4ffe-A368-0DE96E47012E}
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\
FolderDescriptions\{491E922F-5643-4af4-A7EB-4E7A138D8174}
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\
FolderDescriptions\{7b0db17d-9cd2-4a93-9733-46cc89022e7c}
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\
FolderDescriptions\{A302545D-DEFF-464b-ABE8-61C8648D939B}
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\
FolderDescriptions\{A990AE9F-A03B-4e80-94BC-9912D7504104}
```

2. Кроме того, необходимо раскрыть ключ: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\HideDesktopIcons\NewStartPanel`, в составе этого ключа найти параметр `{031E4825-7B94-4dc3-B131-E946B44C8DD5}` и установить его значение на нуль.

СОВЕТ

Соответственно, если вы вдруг решите снова пользоваться библиотеками, вам потребуется воссоздать все эти ключи и параметры. Проще всего это сделать, если заранее сделать их резервные копии.

Помощь в устранении неполадок

Если вам это действительно интересно, то вы можете найти массу рекомендаций и трюков, связанных с редактированием реестра, главным образом позволяющих настроить пользовательский интерфейс по своему вкусу. К сожалению, все эти настройки невозможно рассмотреть полностью, и даже в книгах, специально посвященных данному вопросу, показана только вершина айсберга. Однако ряд методик, связанных с редактированием реестра, могут оказать помощь в устранении неполадок. В этом разделе мы рассмотрим некоторые из них, представляющие наибольший практический интерес.

Настройка программы архивации данных

Казалось бы, темам резервного копирования и восстановления как операционной системы, так и отдельных файлов, в этой книге уже было уделено достаточно внимания. Теперь настало время рассмотреть дополнительные возможности настройки встроенной в Windows Vista/7 программы архивации данных. Как это можно сделать? Как всегда — при помощи реестра.

Наверняка многие пользователи заметили, что Windows 7, как и все ее предшественницы, поддерживает список файлов и папок, которые по умолчанию исключаются из процессов резервного копирования и восстановления, выполняемых с помощью встроенной утилиты резервного копирования и других программ архивации, совместимых с конкретной версией операционной системы. В обычных условиях, вероятно, эти файлы действительно должны быть исключены из процедур резервного копирования и восстановления. Тем не менее, вполне возможна ситуация, когда опытный пользователь Windows захочет их в эти процедуры включить. Именно для таких случаев и предназначены инструкции, приведенные в данном разделе.

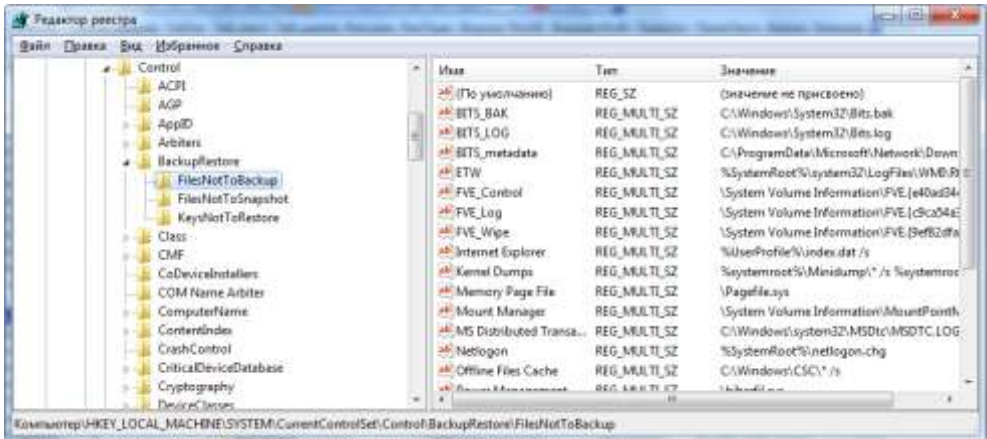


Рис. 14.17. Содержимое ключа реестра
HKLM\SYSTEM\CurrentControlSet\Control\BackupRestore

Приложения, запрашивающие или выполняющие операции резервного копирования и восстановления, используют следующие ключи реестра, расположенные в составе ключа HKLM\SYSTEM\CurrentControlSet\Control\BackupRestore (рис. 14.17):

- ❑ `FilesNotToBackup` — этот ключ реестра содержит параметры с типом данных `REG_MULTI_SZ`, указывающие имена файлов и каталогов, которые

приложения архивации должны исключать из процессов резервного копирования и восстановления;

- ❑ `FilesNotToSnapshot` — сервис теневого копирования тома (Volume Shadow Copy Service) поддерживает этот новый ключ реестра, появившийся в Windows Vista. Приложения и сервисы используют этот ключ, чтобы указать файлы, которые должны быть удалены из вновь создаваемых моментальных снимков тома. Отметим, что в Windows Server 2003 и Windows XP/2000 этот ключ не поддерживается;
- ❑ `KeysNotToRestore` — этот ключ реестра содержит параметры, указывающие имена подключей и параметров реестра, которые приложения архивации не должны восстанавливать при выполнении восстановления;
- ❑ `LastInstance` — новый ключ реестра, впервые появившийся в Windows Vista и не поддерживаемый в Windows 2000/XP и Windows Server 2003. Присутствие этого ключа в реестре указывает, что была выполнена операция аварийного восстановления с использованием сервиса теневого копирования тома и среды WinRE;
- ❑ `LastRestoreId` — новый ключ реестра, появившийся в Windows Vista SP1 и Windows Server 2008. В более ранних версиях этот ключ не поддерживается. В Windows Vista SP1 и более поздних версиях приложение архивации, выполняющее восстановление системных данных (system state data), должно будет создавать этот ключ в составе ключа реестра `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\BackupRestore\SystemStateRestore`, чтобы указать на выполнение этой операции;
- ❑ `DisableMonitoring` — новый параметр реестра, впервые появившийся в Windows 7 и не поддерживаемый ни в одной из предшествующих операционных систем. Как вы уже знаете, в Windows 7 пользователям предлагается сконфигурировать функцию резервного копирования (Windows Backup). Такие предложения начинают появляться при запуске системы на седьмой день после установки Windows 7 (если пользователь не выполнил эту задачу сразу же). Кроме того, они будут появляться и в тех случаях, когда пользователь подключит новый жесткий диск. Если вы пользуетесь не встроенной программой Windows Backup, а, например, решением от стороннего разработчика, вы можете использовать параметр `DisableMonitoring`, чтобы блокировать эти предупреждения.

По умолчанию параметр `DisableMonitoring` в реестре отсутствует, поэтому, чтобы воспользоваться функцией блокировки, его необходимо создать в составе следующего ключа реестра:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsBackup
```

Этот параметр должен иметь тип данных `REG_DWORD`, а его значения интерпретируются следующим образом:

- 1 — автоматические уведомления о необходимости сконфигурировать архивацию отключены;
- 0 — автоматические уведомления не отключены.

Описание ключа *FilesNotToBackup*

Файлы, исключаемые из процессов резервного копирования и восстановления Windows Vista/7, перечислены в составе ключа `HKLM\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup`.

Чтобы отредактировать список файлов, исключаемых из процессов резервного копирования и восстановления в масштабах всей системы, требуется выполнять редактирование реестра.

Формат каждого из параметров в составе ключа `FilesNotToBackup`, которые указывают на файлы, не включаемые в процесс резервного копирования, описан в табл. 14.1.

Таблица 14.1. Формат параметров в составе ключа *FilesNotToBackup*

Параметр	Тип данных	Значение
<i>Component</i> — имя параметра	REG_MULTI_SZ	<i>[drive][path]filename [/s]</i> Здесь: • <i>Drive</i> — буквенное обозначение диска (необязательно), например: <code>c:</code>. • <i>Path</i> — путь к файлу (необязательно), при указании которого можно использовать символы шаблона (wildcard characters). • <i>Filename</i> — имя файла (указывается обязательно), которое может содержать символы шаблона. • <i>/s</i> — этот ключ указывает, что в список включаются и все вложенные каталоги указанного пути

Краткое описание параметров, находящихся в составе этого ключа, приведено в табл. 14.2.

Таблица 14.2. Параметры реестра в составе ключа FilesNotToBackup

Параметр	Значение
ASR error file*	%SystemRoot%\repair\asr.err
ASR log file*	%SystemRoot%\repair\asr.log
Digital Rights Management (DRM) folder*	%SystemDrive%\Documents and Settings\All Users\DRM* /s
Catalog database*	%SystemRoot%\System32\CatRoot2* /s
Client Side Cache	%SystemRoot%\csc* /s
ComPlus	%SystemRoot%\Registration*.crmlog /s
Internet Explorer	%UserProfile%\index.dat /s
Memory Page File	\Pagefile.sys
Microsoft Writer (Bootable state)*	%SystemRoot%\Registration*.clb *.crmlog /s
Microsoft Writer (Service state)*	%SystemRoot%\system32\NtmsData*
MS Distributed Transaction	%SystemRoot%\System32\DTCLog\MSDTC.LOG
Netlogon*	%SystemRoot%\netlogon.chg
NtFrs	%SystemRoot%\ntfrs\jet* /s %SystemRoot%\debug\NtFrs* %SystemRoot%\sysvol\domain \DO_NOT_REMOVE_NtFrs_PreInstall_Directory* /s %SystemRoot%\sysvol\domain \NtFrs_PreExisting___See_EventLog* /s %SystemRoot%\sysvol\staging\domain\NTFRS_*
Power Management	\hiberfil.sys
VSS Default Provider	\System Volume Information*{3808876B-C176-4e48-B7AE-04046E6CC752} /s
Temporary Files	%TEMP%* /s

Таблица 14.2 (окончание)

Параметр	Значение
Entry	Default Value
Client Side Cache	%Systemroot%\csc* /s
ComPlus	%Systemroot%\registration*.clb
Internet Explorer	%UserProfile%\index.dat /s
Memory Page File	\Pagefile.sys
MS Distributed Transaction Coordinator	%Systemroot%\WINNT\System32\DTCLog\MSDTC.LOG
Power Options	\hiberfil.sys
Single Instance Storage	\SIS Common Store*.* /s
Temporary Files	%TEMP%* /s

* Начиная с Windows Vista, больше не используется.

Описание ключа *FilesNotToSnapshot*

Сервис теневого копирования тома (VSS) может удалять файлы из теневой копии тома в процессе ее создания. Для этой цели используется ключ реестра:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot

В составе этого ключа хранятся параметры с типом данных REG_MULTI_SZ для каждого из приложений, файлы которых должны быть исключены из процесса теневого копирования. При указании этих файлов необходимо указывать полный путь (можно использовать символ шаблона *). Если полный путь указать невозможно, следует применять переменные окружения, например:

\$UserProfile\$Directory\Subdirectory\FileName.*

\$AllVolumes\$TemporaryFiles*.*

Чтобы указать, что параметр действует и применительно ко всем вложенным папкам, используется ключ /s , например:

\$UserProfile\$Directory\Subdirectory\FileName.* /s

\$AllVolumes\$TemporaryFiles*.* /s

Параметр в любом случае игнорируется, если по указанному пути нет файлов.

Администраторы могут блокировать использование переменной окружения \$UserProfile\$ за счет использования следующего ключа реестра:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Vss\Settings

В составе этого ключа необходимо создать параметр DisableUserProfileExpansion с типом данных REG_DWORD и присвоить ему нулевое значение.

Описание ключа *KeysNotToRestore*

Еще более сложная ситуация возникает с ключами реестра, исключаемыми из процесса резервного копирования. Эти ключи не перечислены на вкладке **Исключение файлов** (Exclude Files) диалогового окна **Параметры** (Options), и, следовательно, пользователю даже не предоставляется возможность редактирования их списка. Сам этот список хранится в составе ключа HKLM\SYSTEM\CurrentControlSet\Control\BackupRestore\KeysNotToRestore (рис. 14.18).

Список параметров, которые по умолчанию присутствуют в составе этого ключа, и их значений приведен в табл. 14.3.

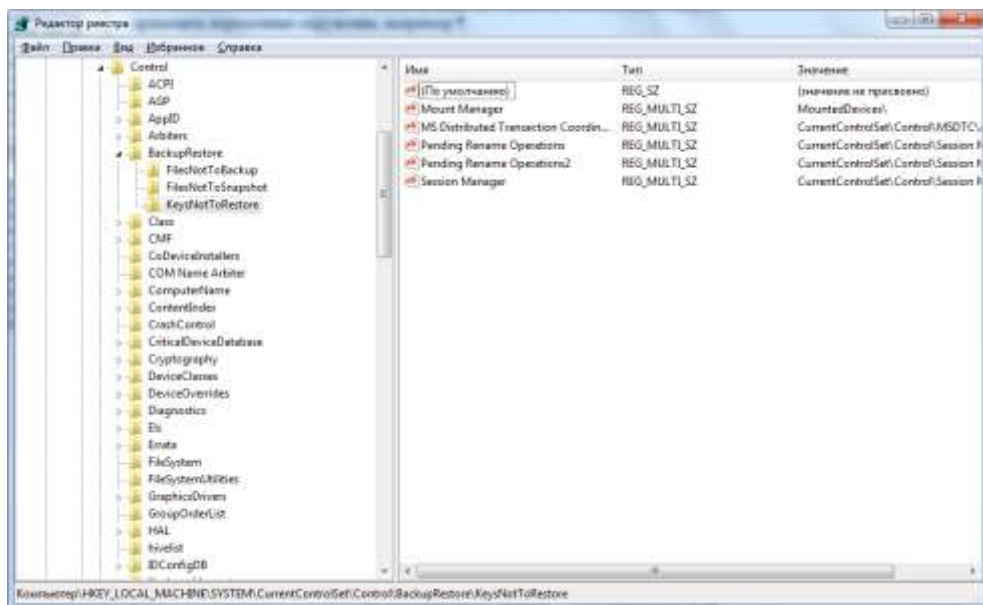


Рис. 14.18. Содержимое ключа реестра
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
BackupRestore\KeysNotToRestore

Таблица 14.3. Список параметров ключа реестра

HKLM\SYSTEM\CurrentControlSet\Control\BackupRestore\KeysNotToRestore

Параметр	Значение
Active Directory Restore	CurrentControlSet\Services\NTDS\Restore In Progress\CurrentControlSet\Services\NTDS\Parameters\New Database GUID
ASR Information	CurrentControlSet\Control\ASR\
Fault Tolerance	Disk\
Installed Services	CurrentControlSet\Services*
LDM Boot Information	CurrentControlSet\Services\dmio\boot info\
LDM Boot Information (dmboot)	CurrentControlSet\Services\dmboot\
Mount Manager	MountedDevices\
Pending Rename Operations	CurrentControlSet\Control\Session Manager\PendingFileRenameOperations
Plug and Play	CurrentControlSet\Enum\CurrentControlSet\Control\CriticalDeviceDatabase\
Removable Storage Manager	CurrentControlSet\Control\NTMS\ImportDatabase
Session Manager	CurrentControlSet\Control\Session
Windows Setup	Setup\SystemPartition

Запуск регистрации работы Windows Installer

Для диагностики функционирования компонента Windows Installer в Windows предусмотрено несколько сервисов регистрации, которые могут быть активизированы посредством реестра. После включения в него и запуска необходимых элементов вы можете вернуться к проблеме, возникшей во время инсталляции, и в дальнейшем компонент Windows Installer будет отслеживать выполнение данного процесса. Файлы регистрационных журналов снабжены стандартным расширением имен — log. Эти файлы хранятся в папке Temp, причем каждому из них присвоено случайное имя, начинающееся с префикса Msi.

Для того чтобы включить регистрацию работы компонента Windows Installer, запустите Редактор реестра (Registry Editor) и создайте новый значимый элемент Logging типа REG_SZ под ключом HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer. Присвойте ему значение, состоящее из перечисленных далее символов (например, "voicewarmupx").

Буквы, входящие в это значение, могут следовать в произвольном порядке. Каждая из них служит для включения соответствующего режима регистрации, применимого для инсталлятора MSI версии 1.1:

- ☐ i — сообщения о статусе (Status messages);
- ☐ w — предупреждения об ошибках, не являющихся фатальными (Non-fatal warnings);
- ☐ e — все сообщения об ошибках (All error messages);
- ☐ a — запуск действий (Start up of actions);
- ☐ r — записи, относящиеся к конкретным действиям (Action-specific records);
- ☐ u — запросы пользователей (User requests);
- ☐ c — исходные параметры пользовательского интерфейса (Initial UI parameters);
- ☐ m — информация о нехватке памяти или аварийном завершении (Out-of-memory or fatal exit information);
- ☐ o — информация о нехватке дискового пространства (Out-of-disk-space messages);
- ☐ p — терминальные свойства (Terminal properties);
- ☐ v — подробные выходные данные (Verbose output);
- ☐ + — присоединение к существующему файлу (Append to existing file);
- ☐ ! — выравнивание строк в журнале (Flush each line to the log);
- ☐ * — запись всей информации, за исключением режима, заданного опцией v. Для того чтобы включить опцию v, укажите "/1*v";
- ☐ x — вывод дополнительной отладочной информации.

СОВЕТ

Этой функцией следует пользоваться лишь в диагностических целях и рекомендуется не оставлять ее активизированной, поскольку она оказывает неблагоприятный эффект на производительность системы и заполняет дисковое пространство. Всякий раз при запуске утилиты **Установка и удаление программ** (Add/Remove Programs) в Панели управления (Control Panel) создается новый файл Msi*.log.

Запуск программ установки с повышенным уровнем привилегий

Вполне возможно, что вам захочется запускать процедуры установки приложений с повышенным уровнем привилегий. Для этого можно отредактировать реестр следующим образом:

1. Запустите редактор реестра и раскройте ключ: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer` (рис. 14.19).

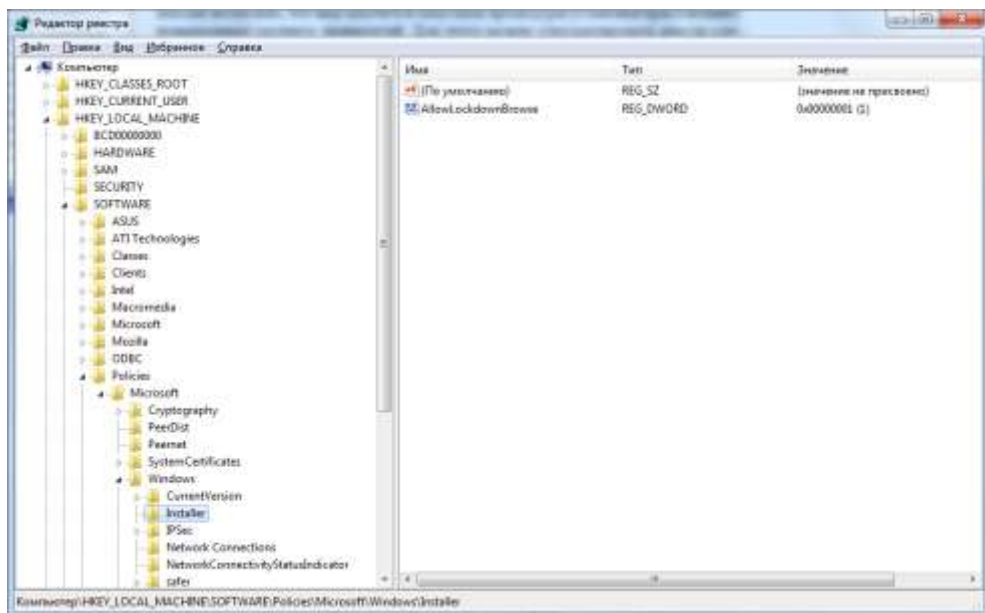


Рис. 14.19. Содержимое ключа реестра

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer

2. Создайте новый параметр с типом данных REG_DWORD и присвойте ему имя AlwaysInstallElevate.
3. Присвойте этому параметру значение 1.

Конфликт гаджетов и UAC

Как наверняка известно многим из вас, блокировка UAC приводит к тому, что в Windows 7 перестают работать некоторые гаджеты (gadgets). Почему это происходит? Дело в том, что нововведения в систему безопасности требуют, чтобы гаджеты не могли работать с повышением уровня привилегий. Поэтому если отключить UAC, то гаджеты прекратят работать. Чтобы решить эту проблему, сделайте следующее:

1. Запустите редактор реестра и откройте ключ HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Sidebar\Settings.
2. В составе этого ключа создайте параметр с типом данных REG_DWORD и назовите его AllowElevatedProcess.
3. Установите для этого параметра значение 1.
4. Закройте редактор реестра. Чтобы изменение вошло в силу, перезагрузки не потребуется.

Заключение

В этой главе в общих чертах были рассмотрены вопросы, связанные с тонкой настройкой и устранением неполадок в системе. Автор искренне надеется, что они помогут наиболее эффективно использовать возможности операционной системы Windows 7 (и при необходимости разрешить возникшие технические проблемы). Обратите внимание, что все приемы, изложенные здесь, могут быть выполнены при помощи встроенных средств операционной системы. Однако существует также множество ценных инструментальных средств и утилит, разработанных сторонними фирмами, и эти средства, безусловно, могут оказать большую помощь в повседневной работе. Именно о них и пойдет речь в следующей главе.

Глава 15



Дополнительные утилиты

Должен ли я отказываться от обеда только потому, что недостаточно хорошо понимаю процесс пищеварения?

Оливер Хэвисайд

Каждая новая версия операционных систем Microsoft из семейства Windows NT — и Windows 7 не является исключением из этого правила — предлагает пользователям множество новых конфигурационных или административных утилит, которые предоставляют пользователям более простой и удобный метод редактирования реестра, чем применение штатных средств его изменения — Редактора реестра Regedit.exe и утилит командной строки, описанных в *главе 3*. Тем не менее, многие (хотя и не все) из приемов, описанных в этой книге, нельзя выполнить, не прибегая к прямому редактированию реестра. Справедливости ради стоит отметить, что фирма Microsoft весьма активно реагирует на пожелания пользователей, и с выходом очередной версии Windows все большую часть таких функций реализует как стандартные возможности Панели управления (Control Panel) или в виде других системных утилит и программ-мастеров. Не отстают от Microsoft и сторонние производители.

Если вы хорошо знаете, где искать, то найдете в достаточном количестве всевозможные полезные утилиты из разряда shareware и freeware, которые помогут вам упростить поддержание реестра в работоспособном состоянии и разрешение наиболее часто возникающих проблем. Впрочем, нужно отметить, что не все из них одинаково полезны — в результате тестирования некоторых из них создается впечатление, что лучше бы их авторы вообще не брались за это дело. Ругать я ничего не буду, а просто приведу небольшой список утилит для Windows Vista и Windows 7, которые работают хорошо и действительно могут оказаться полезными.

Утилиты для индивидуальной настройки и управления работой Windows

В *главе 14* мы рассматривали варианты настройки, с помощью которых можно поменять фон регистрационного окна в Windows 7. Там же мы упоминали и о том, что в Интернете можно найти множество утилит, упрощающих эту задачу и избавляющих пользователей от необходимости вручную редактировать реестр. Давайте рассмотрим некоторые из них.

Утилиты для модификации регистрационного экрана Windows 7

Windows 7 Logon Background Changer

Первая из них — это утилита Windows 7 Logon Background Changer¹ от Жюльена Маничи (Julien Manici) — бесплатная утилита на основе открытого кода (open source), которая предоставляет очень простой и удобный путь для модификации регистрационного экрана Windows 7. Эту утилиту я успешно протестировала как на Windows 7 RC 7100, так и под управлением Windows 7 RTM.

Фактически, она делает в точности то, о чем и заявлено ее разработчиком, — меняет фон регистрационного экрана (рис. 15.1), позволяя выбрать либо один из фоновых рисунков обоев для рабочего стола, поставляемых в комплекте с Windows 7, либо один из файлов, подходящих для этой цели и хранящихся на вашем компьютере (напомним, что это должен быть файл формата JPG, и его размер не должен превышать 256 Кбайт).

Кроме того, утилита реализует и второй рецепт Рафаэля Риверы (Rafael Rivera)² — а именно позволяет преодолеть проблемы, вызванные отображением экранной кнопки при слишком светлом или слишком темном фоне. Наконец, она выполняет и административную задачу — позволяет вам, как администратору, предотвратить изменение регистрационного экрана самими пользователями (рис. 15.2).

Особую ценность этой программе придает то, что она основана на открытом исходном коде, который будет очень полезным тем из вас, кто желает приобрести навыки программирования под Windows 7. Приложение, как и заявлено его автором, может послужить хорошим иллюстративным примером использования Windows Presentation Foundation (WPF).

¹ См. http://www.julien-manici.com/windows_7_logon_background_changer/.

² См. разд. *Дальнейшие модификации экрана регистрации в Windows 7 главы 14*.



Рис. 15.1. Утилита Windows 7 Logon Background Changer



Рис. 15.2. Окно настроек утилиты Windows 7 Logon Background Changer

Как уже говорилось ранее, таких утилит существует множество — вот еще парочка: W7C Windows 7 UI Changer и Logon Changer for Windows 7.

W7C Windows 7 UI Changer

Первая из них, W7C Windows 7 UI Changer (рис. 15.3), разработана Windows7center³, требует запуска с правами администратора и, по сравнению с утилитой Windows 7 Logon Background Changer, обладает более скромными возможностями — она не позволяет улучшить вид экранных кнопок и текста на регистрационном экране. Однако со своей задачей она справляется, поэтому заслуживает упоминания, тем более, что тоже поставляется с исходным кодом, а это очень полезно для тех, кто желает изучать программирование под Windows 7.



Рис. 15.3. Утилита W7C LogonUI Changer

³ См. <http://windows7center.com/windows-7-news/download-our-windows-7-logonui-background-changer/>.

Logon Changer for Windows 7

Наконец, есть и еще одна утилита, которая хорошо справляется с поставленной задачей — это уже упомянутая Logon Changer for Windows 7 от Tweaks.com. Она поставляется хоть и бесплатно, но без исходных кодов. Зато предлагает довольно приятный и удобный пользовательский интерфейс — например, дает возможность протестировать результат и проверить, хорошо ли будет выглядеть новый регистрационный экран (рис. 15.4).

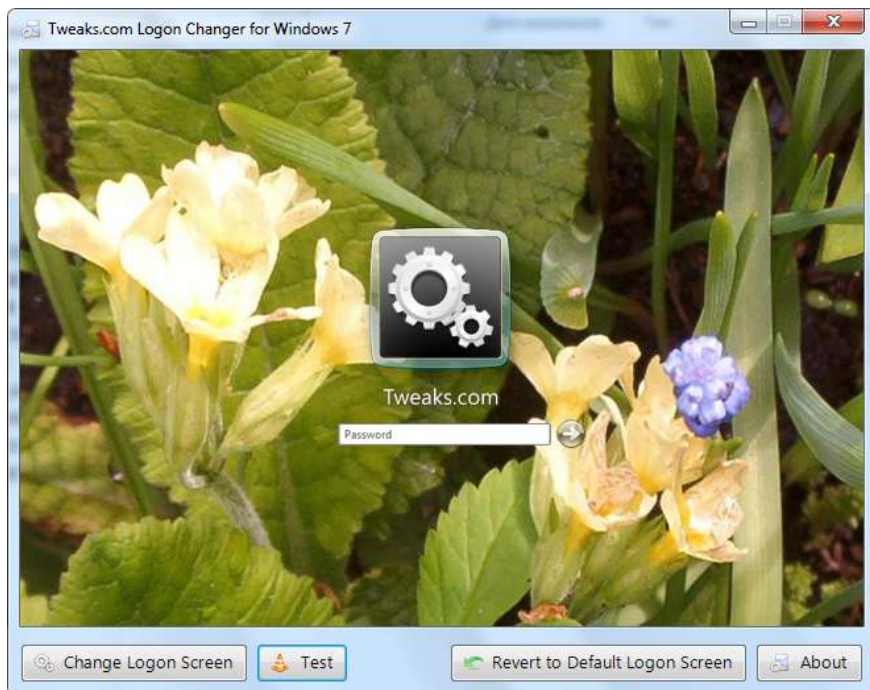


Рис. 15.4. Утилита Logon Changer for Windows 7

С моей точки зрения, лидером является утилита Жюльена Маничи, рассмотренная первой, но вот какую из них выбрать — решайте сами. Повторяю, со своей задачей справляются все три утилиты.

Универсальные утилиты: "твикеры" и не только!

В данном разделе будут рассмотрены несколько утилит, которые предоставляют не только "твики" и "трюки", но и огромное количество действительно полезных функций.

EnhanceMySe7en

Безусловным лидером среди такого рода утилит является бесплатная программа EnhanceMySe7en (рис. 15.5)⁴. Что особенно ценно — программа разработана специально для Windows 7, а это значит, что все ее функции работают корректно.

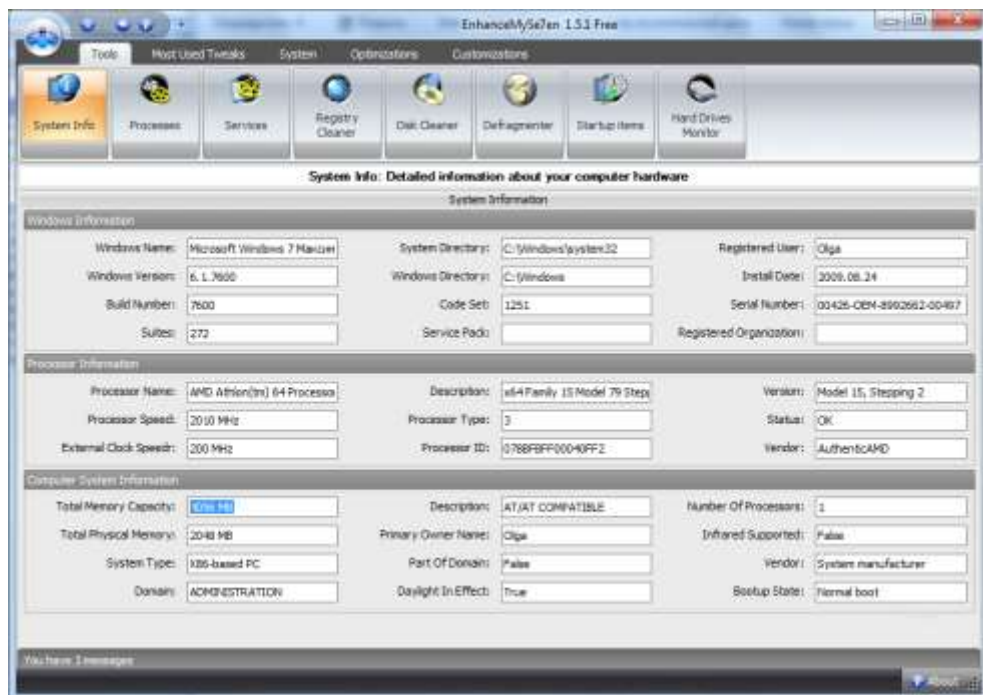


Рис. 15.5. Утилита EnhanceMySe7en — мощное и полезное средство, которое послужит вам отличным подспорьем в работе с Windows 7

ПРИМЕЧАНИЕ

Я особо хочу предостеречь тех пользователей, которые тестируют под Windows 7 различного рода "чистилки реестра" (registry cleaners), разработчики которых явным образом не указали, что программа поддерживает Windows 7. Старые "твикеры", хорошо работавшие под Windows XP или даже под Windows Vista, совершенно не обязательно будут работать точно так же корректно под Windows 7. Особенно это относится к утилитам, предназначенным для работы именно с реестром. Дело в том, что в каждой новой версии Windows в реестре появляются все новые и новые ключи, о которых такие программы "не знают" и интерпретируют их как ошибки. Соответственно, если вы решите следовать рекомендациям, кото-

⁴ См. http://www.seriousbit.com/tweak_windows_7/.

рые выдают такого рода программы, вы поступите в полном соответствии с известными законами Мэрфи, а именно:

- "Чтобы очистить что-то одно, придется запачкать что-то другое";
- "Но можно запачкать все, ничего не очистив".

Набор предоставляемых EnhanceMySe7en функций поистине впечатляет: это не просто "твикалка", а очень удобная и полезная программа, предоставляющая не просто набор популярных "твиков", но и множество полезных и даже уникальных в своем роде функций, в том числе:

- ❑ идентификация процессов (Process Identification), позволяющая выполнять идентификацию нераспознанных процессов, работающих в системе;
- ❑ управление программами, запускаемыми при запуске (Start-Up Management) — это аналог встроенной возможности Windows, позволяющей активизировать или блокировать программы, запускаемые при запуске системы;
- ❑ средство очистки реестра (Registry Cleaner) — функция очистки реестра, позволяющее удалить некорректные элементы и устранить другие ошибки (рис. 15.6). Впрочем, перед тем, как удалять элементы реестра, признанные некорректными, я настоятельно рекомендую выполнить резервное копирование реестра, нажав кнопку **Backup Registry**. Утилита создаст резервную копию в формате REG-файла (рис. 15.7);

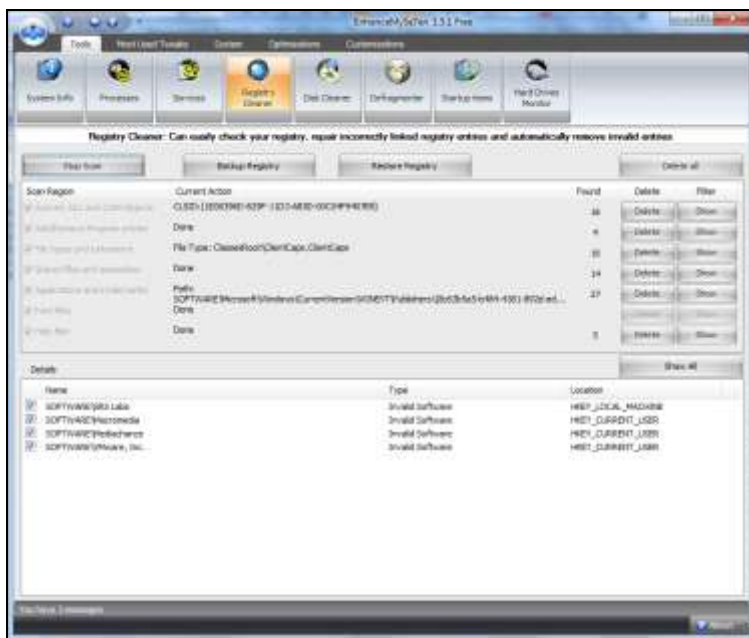


Рис. 15.6. Средство очистки реестра утилиты EnhanceMySe7en за работой

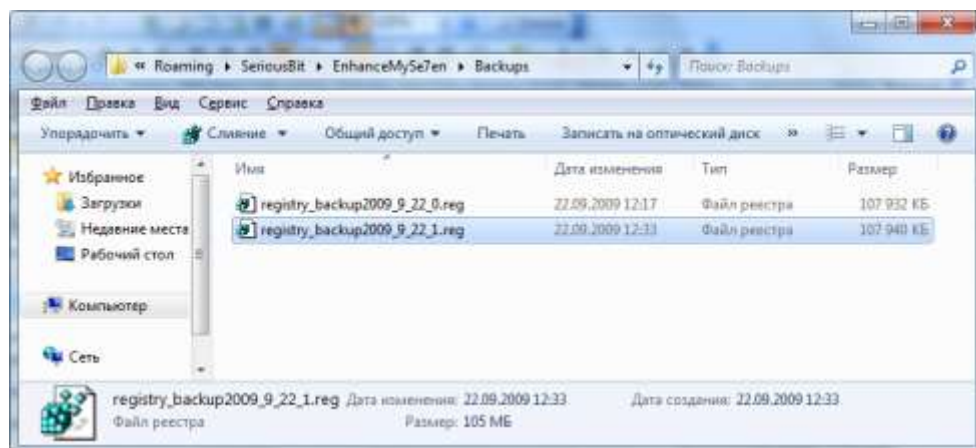


Рис. 15.7. Резервные копии реестра, созданные утилитой EnhanceMySe7

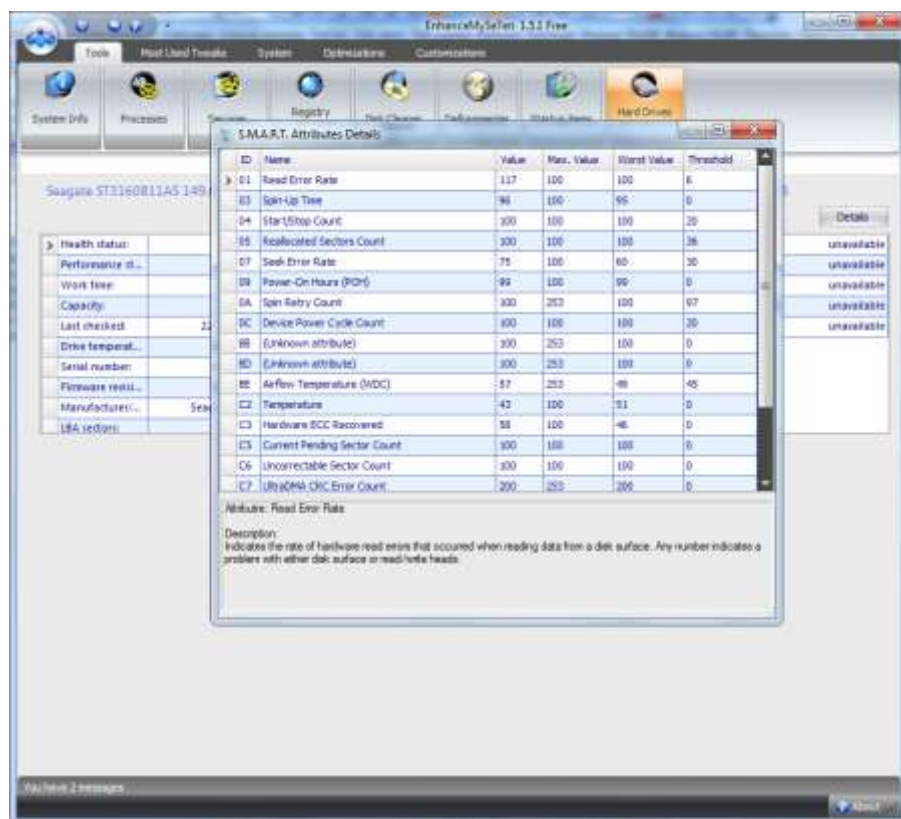


Рис. 15.8. Средства диагностики жестких дисков, встроенные в EnhanceMySe7

- ❑ средства очистки и дефрагментации жесткого диска и реестра (Disk Cleaner, Disk Defragmenter, Registry Defragmenter);
- ❑ монитор жестких дисков (Hard Drive Monitor) — подробные средства диагностики жестких дисков, аналогичные лучшим из сторонних утилит для диагностики аппаратных средств (рис. 15.8);
- ❑ возможности быстрого доступа ко всем встроенным административным средствам Windows 7 — попробуйте, вы очень быстро убедитесь, что они повышают удобство работы и позволяют выполнять многие операции быстрее, чем традиционный метод доступа к административным средствам через Панель управления (Control Panel);
- ❑ твики и настройки — на любой вкус (рис. 15.9).

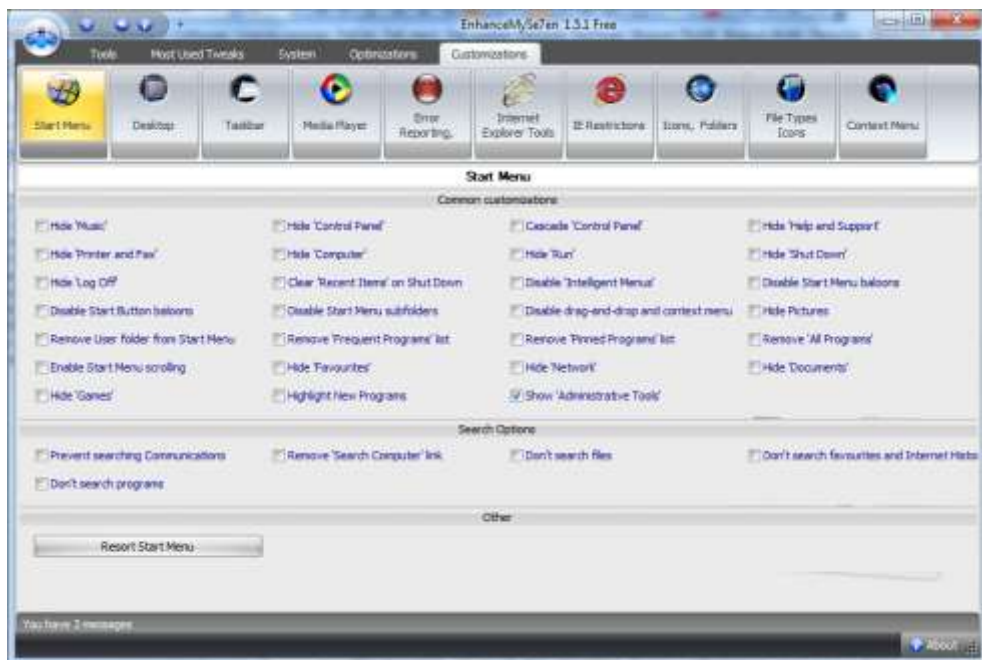


Рис. 15.9. EnhanceMySe7en предлагает "твики" на любой вкус — как "украшательские", так и весьма полезные — например, направленные на оптимизацию производительности и повышение уровня безопасности

В общем, это — отличное средство, которое рекомендуется иметь в системе каждому.

Little Tweaker

Little Tweaker⁵ — это небольшая и очень простая в использовании утилита, не требующая даже инсталляции (рис. 15.10). Конечно, Little Tweaker не идет ни в какое сравнение с только что описанным "монстром" EnhanceMySe7en. Однако, она будет хорошим выбором для тех пользователей, которые хотят получить возможность быстро, без риска и затруднений манипулировать контекстными меню, включением и отключением всплывающих предупреждений и т. п.

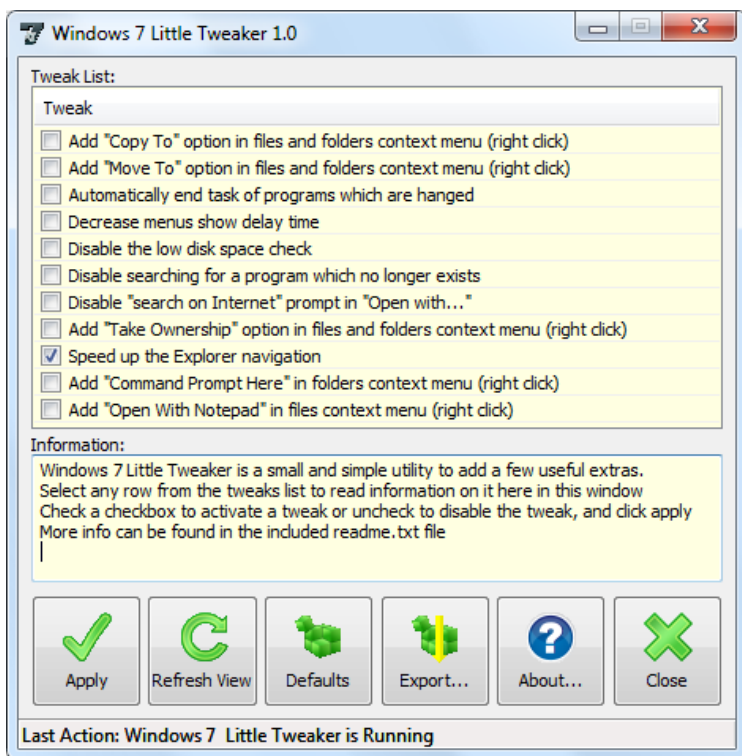


Рис. 15.10. Little Tweaker — это "говорящее название", потому что программа действительно представляет собой не что иное, как "маленький твикер"

ПРИМЕЧАНИЕ

Windows 7 Little Tweaker имеет ряд ограничений. Во-первых, это приложение предназначено исключительно для Windows 7 и не будет работать ни под какой другой версией Windows. Запускать приложение следует от имени администратора.

⁵ См. <http://leelusoft.blogspot.com/2009/05/windows-7-little-tweaker.html>.

тора, и при этом, чтобы вносимые ею изменения вошли в силу, необходима блокировка UAC (рис. 15.11). Кроме того, приложение предназначено для работы только в 32-разрядных версиях Windows 7 и не будет работать на 64-разрядной платформе. Тем не менее, я все же включила эту утилиту в данный обзор — во-первых, чтобы показать, что "твикеры" бывают разные, а во-вторых — из-за ее крайней простоты. Вполне возможно, что вам она может и понравиться.



Рис. 15.11. При активизированном UAC Windows 7 Little Tweaker не сможет внести в систему заявленные изменения

Ultimate Windows Tweaker

Программа Ultimate Windows Tweaker (UWT) изначально была разработана командой WinVista Club⁶ для Windows Vista. Однако ее разработчики выпустили новую версию, которая поддерживает и Windows 7⁷. Впрочем, бета-тестеры Windows 7 единодушно отмечали, что и первоначальная версия работала под новой системой достаточно хорошо, лишь изредка выдавая сообщения об ошибках, которые особого эффекта на работоспособность системы не оказывали. По этой причине данная утилита тоже заслуживает внимания (рис. 15.12).

UWT, как и рассмотренные в начале этой главы утилиты для модификации регистрационного экрана, позволяет выполнить эту задачу (рис. 15.13), базируясь на советах уже упомянутого Рафаэля Риверы (Rafael Rivera).

Но, в отличие от этих простейших "твикеров", UWT предоставляет и множество других возможностей индивидуальной настройки графического интерфейса Windows самыми разнообразными способами — от настроек панели задач и меню **Пуск** (Start) до параметров безопасности, поведения системы при завершении работы и конфигурации Internet Explorer. Особенно удобна опция **Show "Take Ownership"** (рис. 15.14), добавляющая в контекстное меню команду **Take Ownership**, позволяющую присвоить себе права владельца на выбранный объект (вы ведь помните, в *главе 9* было показано, какая это громоздкая процедура, если выполнять ее вручную).

⁶ См. http://www.winvistaclub.com/Ultimate_Windows_Tweaker.html.

⁷ См. <http://www.downloadsquad.com/2009/02/10/ultimate-windows-tweaker-updated-works-on-windows-7/>.

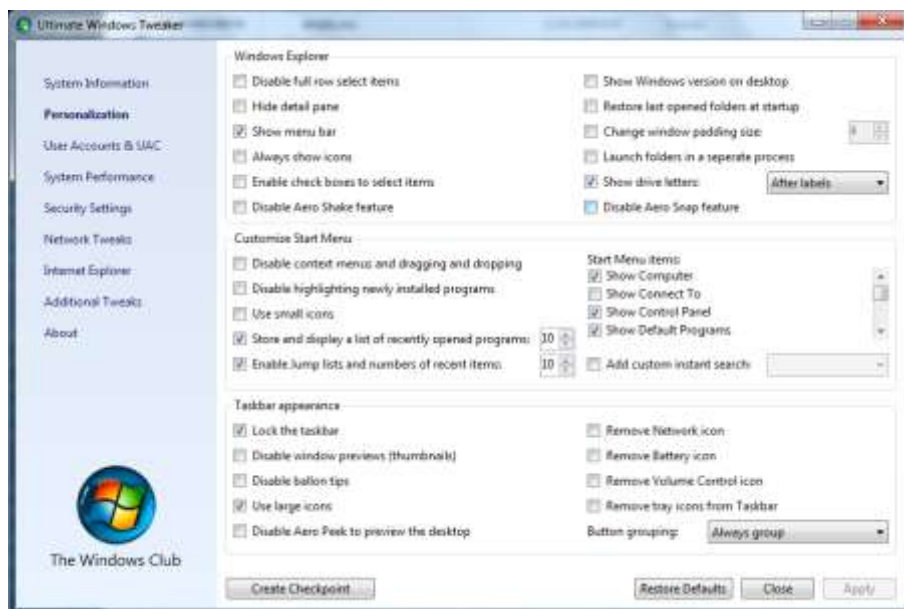


Рис. 15.12. Новая версия Ultimate Windows Tweaker от команды WinVista Club поддерживает Windows 7

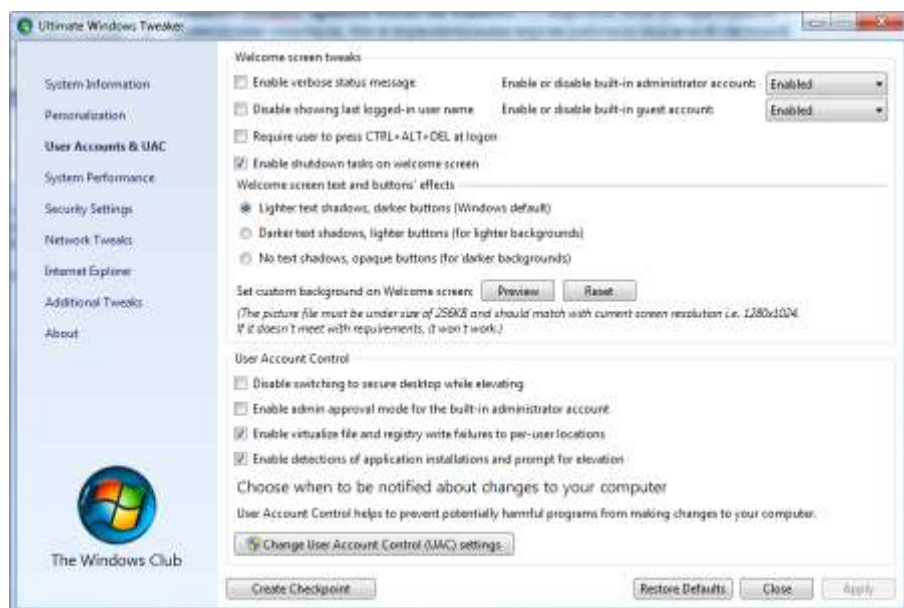


Рис. 15.13. Программа Ultimate Windows Tweaker позволяет модифицировать регистрационный экран Windows

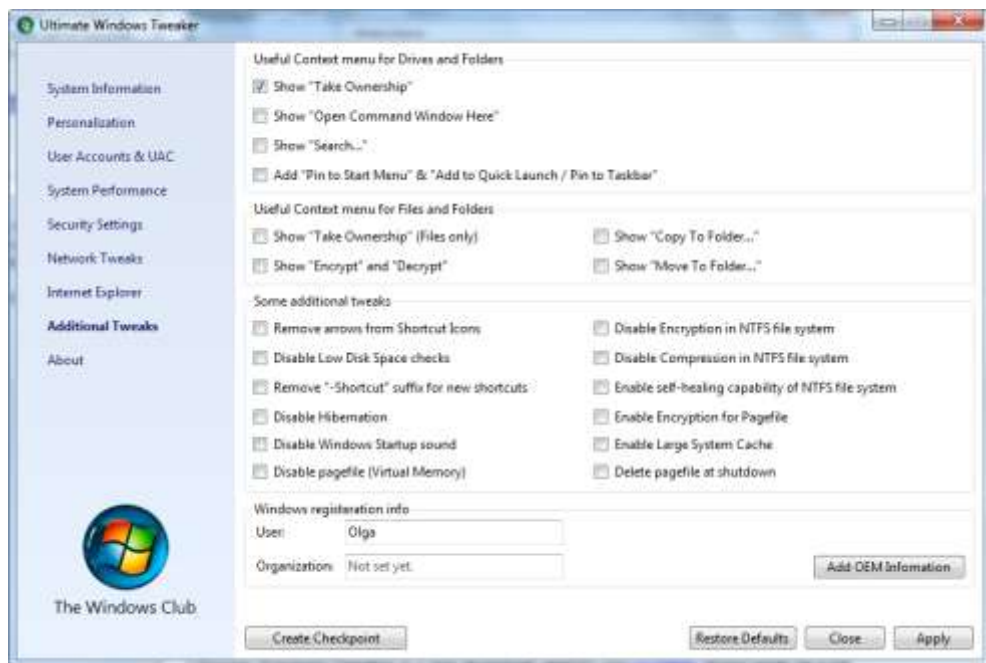


Рис. 15.14. Программа Ultimate Windows Tweaker работает под Windows Vista и Windows 7 и предоставляет множество полезных опций

Достоинством Ultimate Windows Tweaker, как и описанной в предыдущем разделе утилиты Little Tweaker, является портативность — программа не требует инсталляции и отлично работает, например, с носителей Flash USB. Учитывая ее довольно широкий набор возможностей, эта утилита должна занять достойное место в вашей коллекции полезных программ для Windows 7.

XdN Tweaker

Новая версия XdN Tweaker⁸ (рис. 15.15) от Николаса Кайто (Nicholas Caito) поддерживает практически все "живые" версии Windows, находящиеся в употреблении на текущий момент: Windows XP/Server 2003, Vista, Windows 7 и Server 2008. По обеспечиваемым функциональным возможностям она занимает промежуточное положение между Windows 7 Little Tweaker и Ultimate Windows Tweaker. XdN Tweaker будет хорошим выбором для пользователей, желающих выполнять базовые настройки простым и удобным способом. Достоинством программы является и то, что она поставляется и как инсталлируемое, и как портативное приложение.

⁸ См. <http://xenomorph.net/>.

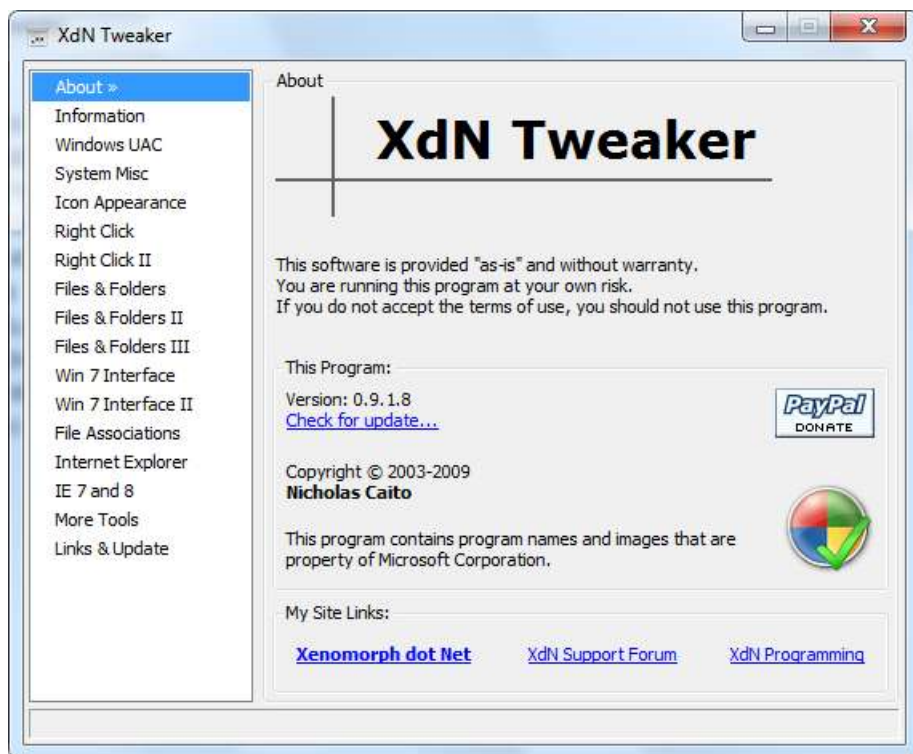


Рис. 15.15. Программа XdN Tweaker — отличный выбор для пользователей, ценящих простоту, удобство, портативность и универсальность

Windows 7 Manager

Утилита Windows 7 Manager от Yamicsoft позиционируется разработчиками не просто как "твикер", но и как полезная утилита, позволяющая управлять важными системными функциями. При первом запуске она сразу же предлагает создать точку восстановления системы (System Restore Point), что лично на меня произвело самое благоприятное впечатление (рис. 15.16). И она действительно оправдывает свое название — к числу предлагаемых ею функций относятся: очистка системы, средства защиты личной информации, мониторинг процессов, средство устранения проблем с деинсталляцией приложений, ставших ненужными, средство поиска дублирующихся файлов, а также набор инструментов по устранению неполадок. Разумеется, предлагается и "джентльменский набор" разнообразных "твиков" (рис. 15.17).

В целом, набор предлагаемых функций примерно соответствует набору, предлагаемому утилитой EnhanceMySe7en. Впрочем, в отличие от програм-

мы EnhanceMySe7en, которая представляет собой бесплатный продукт на основе открытого кода, Windows 7 Manager — это продукт коммерческий, и для тестирования на сайте производителей предоставляется 15-дневная оценочная версия⁹.

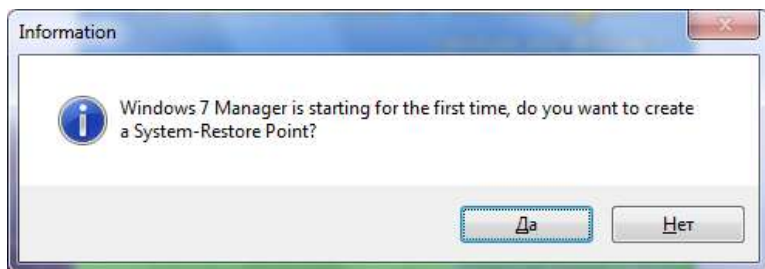


Рис. 15.16. При первом запуске программа Windows 7 Manager сразу же предлагает создать точку восстановления системы



Рис. 15.17. Windows 7 Manager предлагает "джентльменский набор" разнообразных "твиков"

⁹ См. <http://www.yamicsoft.com/windows7manager/index.html>.

TweakNow PowerPack 2009

TweakNow PowerPack¹⁰ — это бесплатный продукт, представляющий собой набор тесно интегрированных между собой утилит, предназначенных для индивидуальной настройки всех аспектов работы операционных систем Windows XP/Vista/7 (рис. 15.18). В состав продукта входит модуль Registry Cleaner, обеспечивающий возможность быстрой и безопасной очистки реестра Windows (рис. 15.19), а также модуль Registry Defragmenter, осуществляющий дефрагментацию реестра (рис. 15.20). Помимо этого, продукт позволяет задействовать более 100 скрытых настроек Windows, что позволит удовлетворить запросы самых придирчивых "твикеров".

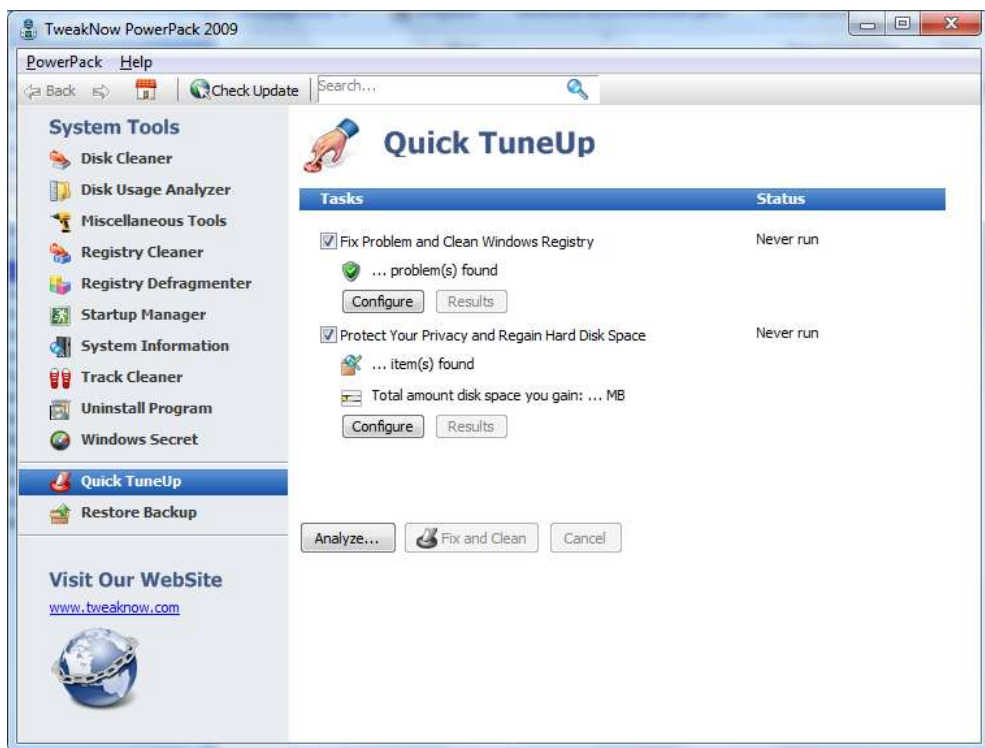


Рис. 15.18. TweakNow PowerPack — это бесплатный продукт, обеспечивающий множество дополнительных утилит для оптимизации Windows XP/Vista/7 — в том числе, и предназначенных для работы с реестром

¹⁰ См. <http://www.tweaknow.com/powerPack.html>.

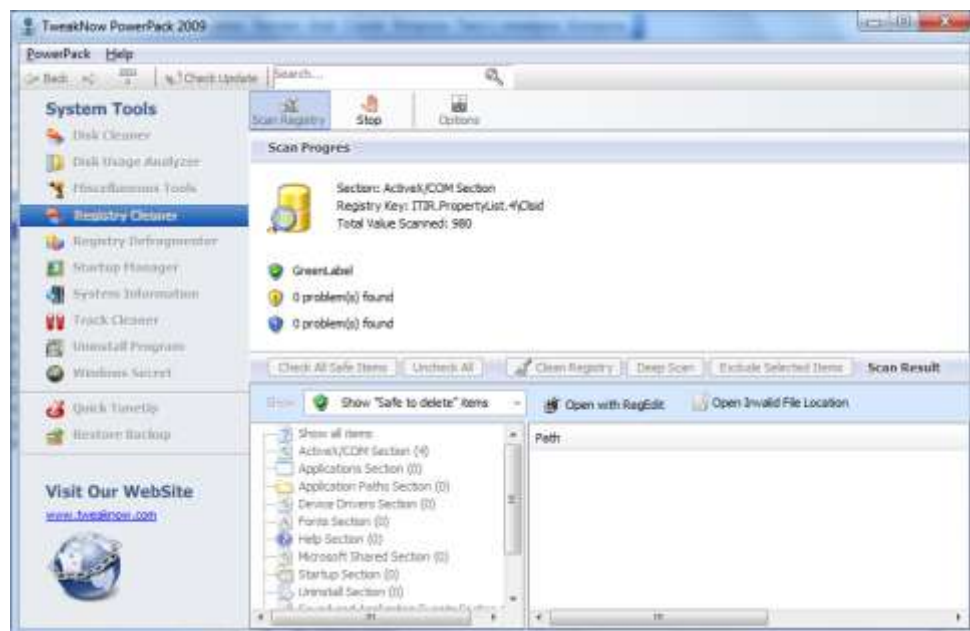


Рис. 15.19. Модуль Registry Cleaner за работой

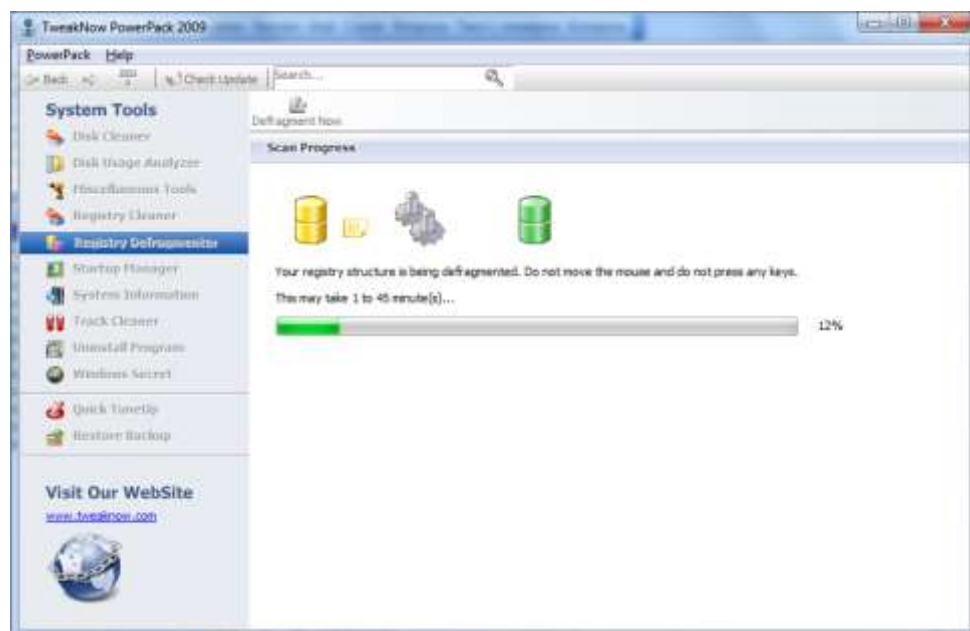


Рис. 15.20. Модуль Registry Defragmenter за работой

В составе программы имеется модуль Virtual Desktop, который позволяет вам иметь одновременно до четырех индивидуально настроенных конфигураций рабочего стола, между которыми вы можете мгновенно переключаться, в зависимости от вашего настроения или текущих потребностей (рис. 15.21). Наконец, эта программа тоже предоставляет полный, тесно интегрированный набор приложений и утилит, позволяющих вам получать детальную информацию об аппаратных средствах вашего компьютера и управлять всеми аспектами работы Windows.

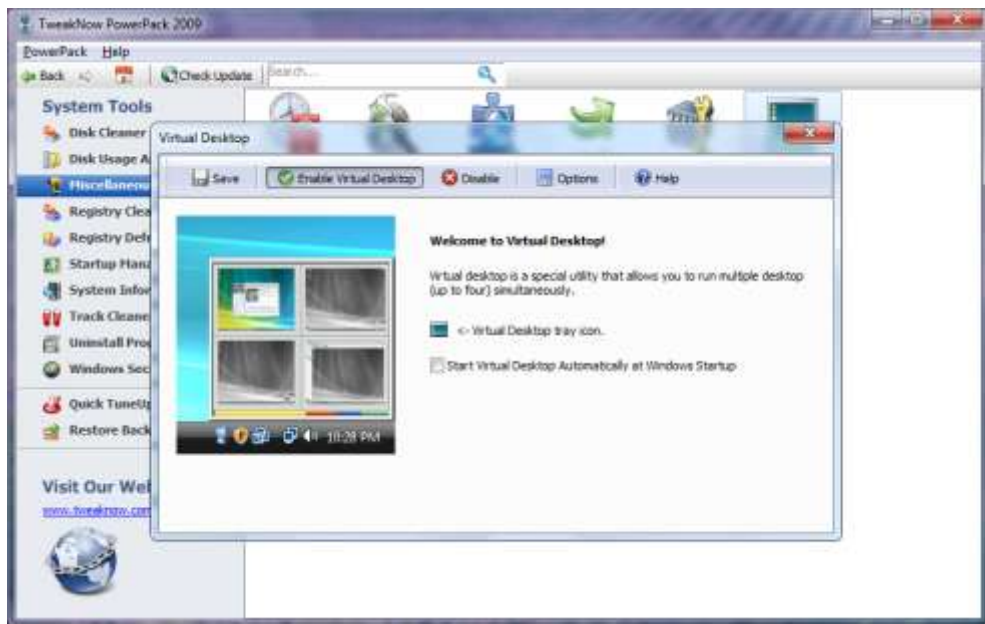


Рис. 15.21. Модуль Virtual Desktop позволяет иметь до четырех индивидуально настроенных конфигураций рабочего стола одновременно

Uniblue DriverScanner

Еще одна очень полезная утилита — это Uniblue DriverScanner (рис. 15.22) от Uniblue¹¹. Как вы помните, в *главе 5* этой книги мы говорили о том, как реестр хранит данные об аппаратных устройствах, подключенных к вашему компьютеру, и о том, какую важную роль играют драйверы аппаратных средств и правильность их конфигурации в реестре. Так вот, DriverScanner позволяет сканировать ваш компьютер и искать драйверы устройств, для ко-

¹¹ См. <http://www.liutilities.com/products/driverscanner/>.

торых соответствующие производители выложили на свои сайты обновленные версии драйверов, в которых, возможно, были уже исправлены существующие ошибки или реализованы новые функции. Если вы не выполняете эту задачу регулярно, то существует риск возникновения проблем — от относительно незначительных (хотя, например, низкую производительность "незначительным недостатком" никто не назовет) до серьезных, таких, как аппаратные конфликты или даже сбои в работе операционной системы.

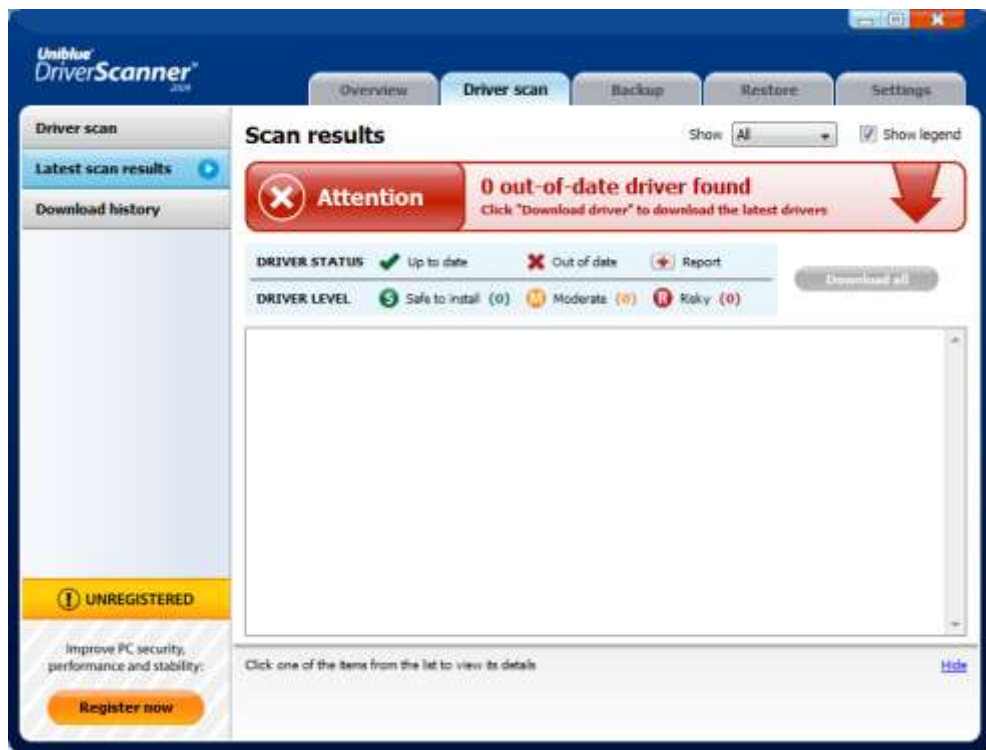


Рис. 15.22. Утилита Uniblue DriverScanner — средство поддержания всех драйверов в актуальном состоянии

При том, что база данных драйверов в вашей системе и так весьма обширна (и растет с подключением все новых и новых устройств), управлять драйверами с помощью стандартных средств Windows становится все сложнее и сложнее. Именно для упрощения решения этой задачи и разработано средство DriverScanner, позволяющее автоматически отслеживать, для каких драйверов появились обновления. Кроме того, DriverScanner помогает устанавливать обновления для всех драйверов, признанных устаревшими, а также

дает возможность выполнять резервное копирование всех установленных в системе драйверов на внешнее устройство. Это позволит существенно упростить ваши задачи по поиску и установке необходимых драйверов на тот случай, если вам по той или иной системе потребуется переустановить операционную систему.

Другие полезные программы для Windows 7

В предыдущих разделах этой главы мы рассмотрели несколько утилит, предназначенных для индивидуальной настройки Windows — как чисто "украшательских", так и универсальных, предоставляющих широкий набор полезных функций, включая и работу с реестром, в том числе — его резервное копирование, восстановление, сканирование и поиск ошибок, а также дефрагментацию.

В этом разделе мы рассмотрим еще несколько полезных инструментов, которые пригодятся вам для работы с реестром, и не только с ним.

Утилита Process Monitor от Марка Руссиновича

Если вы имеете опыт работы с предыдущими версиями Windows, то наверняка помните, какое огромное количество восторженных отзывов собрала утилита Regmon.exe, авторами которой являются известные исследователи Windows Марк Руссинович (Mark Russinovich) и Брюс Когсвелл (Bryce Cogswell).

Приложение Regmon.exe представляло собой утилиту, предназначенную для мониторинга реестра и позволявшую отображать на экране и сохранять в файле журнала всю информацию о доступе к реестру в масштабах всей системы (рис. 15.23). Эта уникальная по своим возможностям утилита была реализована как комбинация драйвера устройства и GUI и являлась просто незаменимым средством для всех пользователей как при изучении работы операционных систем Windows NT/2000/XP, так и при поиске проблем, вызванных неправильной конфигурацией реестра. Утилита Regmon позволяла задавать фильтры процессов и путей, управлять просмотром списка, сохранять содержимое полученного списка в файле формата ASCII, а также вести мониторинг доступа к реестру в процессе загрузки операционной системы.

Утилита Regmon.exe стала поистине легендарной, но в настоящее время она уже не поддерживается разработчиками, поскольку на смену ей пришло новое аналогичное приложение — Process Monitor (Procmon.exe) — гораздо более мощное средство мониторинга для Windows, поддерживающее все версии этой ОС, начиная с Windows 2000 SP 4 и заканчивая Windows 7 и Server 2008.

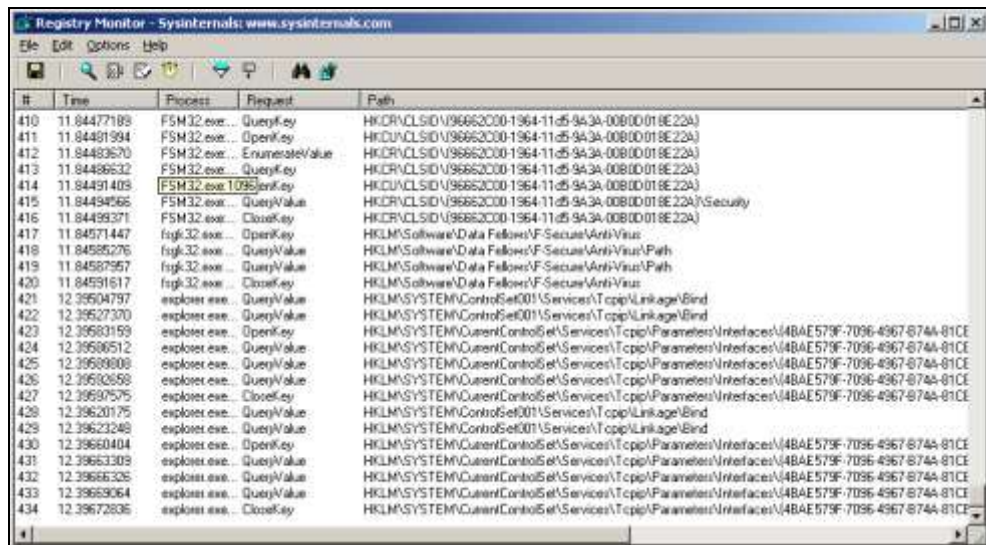


Рис. 15.23. Утилита Regmon в процессе работы

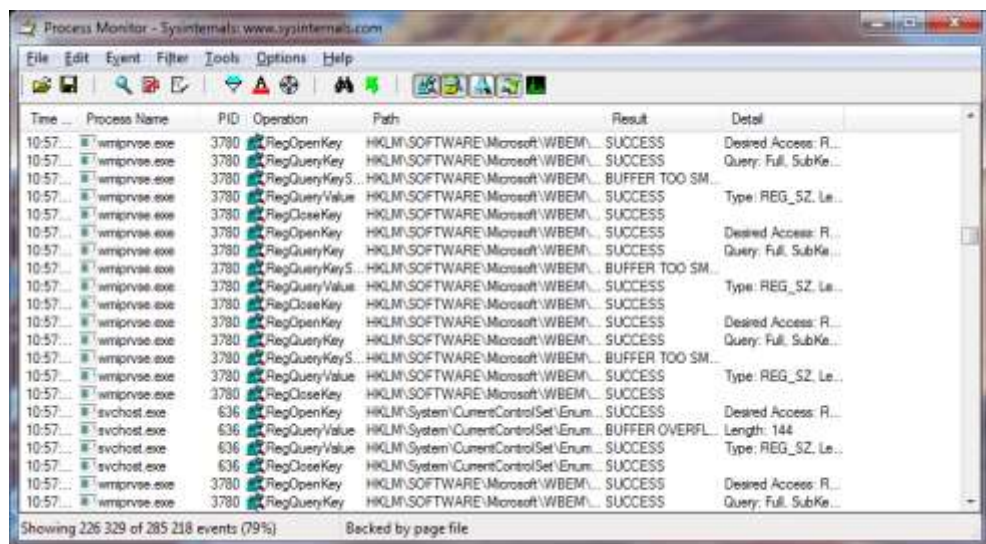


Рис. 15.24. Утилита Process Monitor пришла на смену знаменитой программе Regmon.exe

Process Monitor работает в режиме реального времени (рис. 15.24) и отслеживает все операции, имеющие место в Windows, включая доступ к файловой системе, реестру, а также все процессы (processes) и нити управления

(threads). Этот новый инструмент комбинирует возможности устаревших утилит Regmon.exe и Filemon.exe, разработанных авторами ранее, а также добавляет ряд новых возможностей, что делает ее незаменимым инструментом при исследованиях внутренних механизмов работы Windows, а также при устранении неполадок (например, при ручном удалении вирусов и другого вредоносного ПО).

Утилиты для взлома паролей

В главе 9 этой книги мы говорили о взломе паролей Windows, а также о том, что для взлома похищенных ульев SAM и Security больших усилий не требуется. Там было вполне убедительно показано, что если в вашем распоряжении имеется одна из утилит для взлома паролей, то успех атаки зависит от качества используемого для взлома словаря. Да и в любом случае — на атаку по методу "грубой силы" (Brute Force) можно на досуге потратить любое количество свободного времени.

В качестве примера для иллюстрации была приведена бесплатная утилита LCP¹². Кстати, слова "взлом паролей" ни у кого не должны вызывать глубокого возмущения. Ни одна из технологий не хороша и не плоха сама по себе — важно лишь, с какой целью она используется. Например, администраторы, всерьез озабоченные безопасностью, могут периодически производить аудит паролей и, найдя учетные записи, вообще не защищенные паролем или защищенные слабо, провести с соответствующими пользователями разъяснительную работу. Да наконец, утилиты этого рода могут использоваться для того, чтобы помочь пользователям, забывшим свои пароли, восстановить их и, таким образом, зарегистрироваться в системе. В любом случае, использование утилит для взлома паролей администраторами, преследующими вполне благородные цели, — это абсолютно законная практика!

ПРИМЕЧАНИЕ

Конечно, вы можете возразить, что пользователи должны создавать себе так называемую "дискету сброса пароля" (password recovery disk), тем более, что такие средства предоставляются операционными системами Windows XP, Windows Vista и, разумеется, Windows 7. Но многие ли это делают? К тому же, возможны ситуации, когда пользователь потеряет эту дискету (или носитель Flash USB), она окажется поврежденной, или же, например, создание таких носителей противоречит принятым у вас правилам безопасности. А выручить пользователя все-таки надо...

Рассмотрим еще одну популярную программу, которая может использоваться в данных целях — L0phtCrack. Эта легендарная утилита, к сожалению, про-

¹² См. <http://www.lcpsoft.com/english/download.htm>.

пала с рынка после того, как компания @stake, основанная разработчиками L0phtCrack (L0pht Heavy Industries), была приобретена Symantec. Однако в начале текущего года команда L0phtCrack выкупила права на свой инструмент у Symantec и выпустила новую версию — L0phtCrack 6 (рис. 15.25).

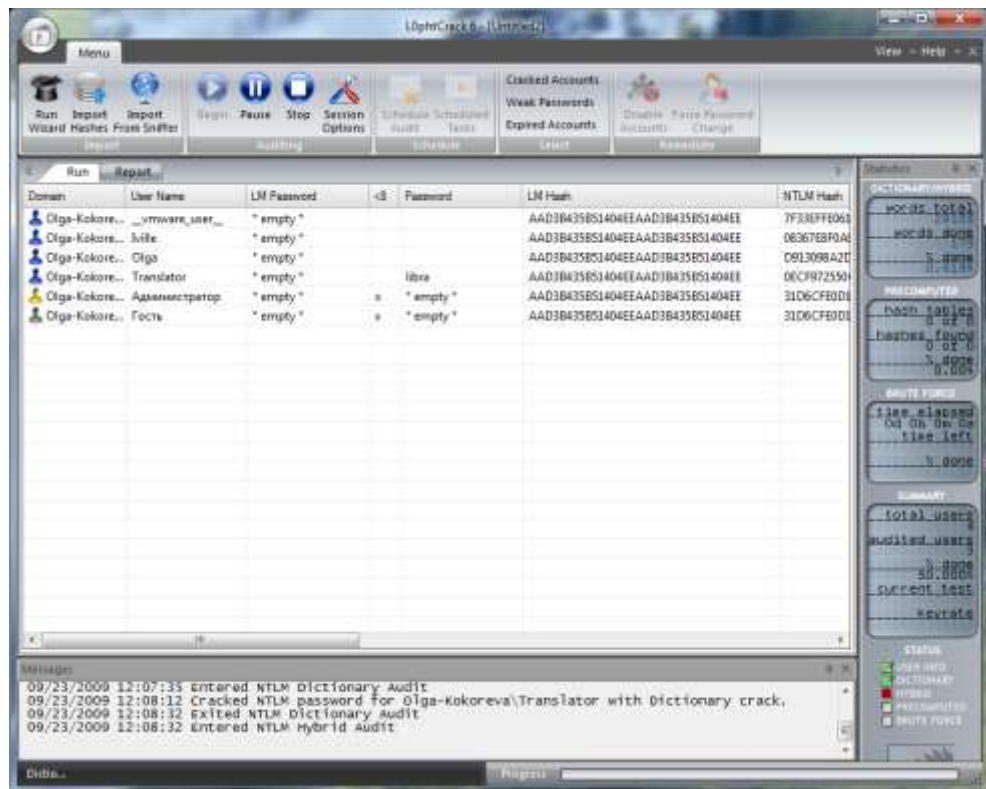


Рис. 15.25. Знаменитая утилита L0phtCrack вновь доступна!

Обратите внимание — пустые и слабые пароли она взламывает за считанные секунды!

ПРИМЕЧАНИЕ

Эта иллюстрация (рис. 15.25) приведена исключительно в демонстрационных целях. Не надо думать, что это я использую такие слабые пароли! У меня подобных дыр в системе нет.

Скачать утилиту L0phtCrack 6 можно по адресу: <http://www.l0phtcrack.com/download.html>. Правда, следует отметить, что для скачивания доступна только оценочная версия с 15-дневным сроком использования.

Если вас интересуют именно бесплатные утилиты для взлома паролей, обратите внимание на уже упомянутую LCP или еще один бесплатный аналог — Ophcrac (<http://ophcrack.sourceforge.net/>).

Заключение

Итак, вот всего лишь несколько из великого множества утилит, предназначенных для настройки Windows 7 и работы с реестром. Автор уверенно может рекомендовать их всем читателям. С остальными утилитами этого обширного класса читатель может ознакомиться, воспользовавшись адресами, приведенными в *приложении 1*.



ПРИЛОЖЕНИЯ



Приложение 1

Ресурсы Интернета

В условиях, когда операционные системы постоянно развиваются, появляются их новые версии и выходят самые разнообразные сервисные пакеты (Service Packs), недостаток любой книги становится очевидным — она неизменна. Автор и редактор тщательно проверяли все приводимые в книге материалы, советы и рекомендации, но...

Лучшим источником информации о Windows NT/2000/XP/Vista и, безусловно, Windows 7 является, конечно же, Интернет, поэтому в данном приложении я привожу наиболее интересные, информативные и, самое главное, надежные ссылки.

❑ <http://www.microsoft.com/>

Официальный сайт компании Microsoft, разумеется, знают все, и он всегда был и останется одним из самых надежных и полных источников информации о любых программных продуктах Microsoft. Здесь вы найдете множество сведений, в том числе и о реестре, огромное количество статей из Knowledge Base, официальные публикации и т. д., и возможно, отыщете ответы на те вопросы, которые вас интересуют. Что касается реестра, то вам следует обратиться по адресу Microsoft Downloads Center (<http://www.microsoft.com/downloads/search.aspx>), выбрать операционную систему, с которой вы работаете, и ввести запрос по ключевому слову Registry. Здесь вы найдете большое количество патчей реестра, утилит и инструментальных средств (некоторые из них — с исходными кодами).

❑ <http://msdn.microsoft.com/en-us/magazine/default.aspx>

MSDN Journal — неоценимое средство для всех, кто хочет знать операционные системы из семейства Windows NT не поверхностно, а углубленно.

❑ <http://www.microsoft.com/security/default.msp>

Официальный источник информации по безопасности Windows — Microsoft Security Advisor. Всем, кто реально озабочен безопасностью своих сетей Windows NT/2000/XP/Vista/7, рекомендуется регулярно посещать этот сайт (еще лучше — подписаться на рассылку).

❑ <http://labmice.techtarget.com/>

Этот ценнейший ресурс содержит информацию по всем версиям Windows, более ранним, чем Windows 7. Несмотря на внесенные в систему радикальные изменения и усовершенствования, Windows 7 все же выросла не на пустом месте! Для правильного понимания архитектуры и принципов работы Windows 7 предшествующие версии, особенно Windows Vista, тоже необходимо знать. А по широте охвата материала мало какой сайт может сравниться с этим. Особо ценно то, что здесь есть огромное количество ссылок самой разнообразной тематики.

❑ <http://www.osr.com>

Сайт для истинных профессионалов! Автор — консалтинговая фирма OSR Open Systems Resources, Inc. Сайт целиком посвящен разработке программного обеспечения для Windows NT/2000/XP/Vista/7, включая разработку файловых систем, драйверов устройств и т. п. Что особенно ценно, здесь вы можете подписаться на журнал "NT Insider" (<http://www.osronline.com/section.cfm?section=17>). Подписка бесплатная (free), а журнал при этом очень хорош и содержит огромное количество полезной информации. Если вы NT-программист — подписывайтесь, не раздумывая, и вы не пожалеете.

❑ <http://www.wugnet.com/>

Сайт Windows Users Group Network (WUGNET), содержащий массу информации обо всех версиях Microsoft Windows, включая и Windows Vista/7. На этом сайте вы можете найти информацию по технической поддержке, относящуюся к различным аспектам операционных систем Windows, e-mail-клиентов, shareware-продуктов, аппаратного обеспечения, игр, разработке программного обеспечения, создания систем подсказок, мультимедиа, изделиях Microsoft и многое другое.

❑ <http://www.winplanet.com/winplanet/>

Этот сайт содержит все, что относится к Windows: новости, обзоры, приемы работы, материалы для скачивания, а также бесплатные еженедельные бюллетени Windows. Много информации по всем версиям Windows, а не только Windows Vista/7.

❑ <http://technet.microsoft.com/en-us/sysinternals/default.aspx>

Авторами сайта Systems Internals являются Марк Руссинович (Mark Russinovich) и Брюс Когсвелл (Bryce Cogswell), и имена его создателей говорят сами за себя. На этом сайте вы найдете множество полезных утилит для Windows NT/2000/XP/Vista/7, а также технической информации, объясняющей принципы их функционирования. Это — мой любимый сайт.

❑ <http://www.windowsitlibrary.com/>

Как следует из названия, это свободная онлайн-библиотека технических справочников для профессионалов ИТ в Windows. Прекрасный ресурс, охватывающий практически все вопросы, относящиеся к операционным системам из семейства Windows NT.

❑ <http://www.theeldergeekvista.com/> и <http://www.theeldergeek.com/>

Множество полезной информации по Windows Vista и Windows XP. Правда, последнее время сайты, к сожалению, давно не обновлялись. Как уже говорилось, Windows 7 не выросла на пустом месте, поэтому предшествующие версии тоже необходимо тщательно изучать.

❑ <http://www.annoyances.org/>

Обширная коллекция статей, отрывков из книг, ценных советов по работе с Microsoft Windows. Отдельный раздел посвящен системному реестру, в том числе — реестру Windows Vista/7. Имеется отдельный форум, посвященный Windows 7.

❑ <http://www.msfn.org/>

Сайт, где обсуждаются самые актуальные новости из мира Windows, новейшие сервисные пакеты, вопросы бета-тестирования, модификации дистрибутивов и многое другое!

❑ <http://www.toutwindows.com>

Интересный сайт, содержащий множество полезной информации о Windows XP/Vista/7 и Windows Server 2008 (на французском языке).

❑ <http://www.computerperformance.co.uk/index.htm>

Полезнейший сайт, содержащий большое количество ценной информации по Windows Server 2003, Windows Vista и Windows Server 2008.

❑ http://www.petri.co.il/vista_tips.htm и <http://www.petri.co.il/windows-7.htm>

Внушительная подборка советов по настройке Windows Vista и Windows 7, статей и пошаговых руководств.

❑ <http://www.openwall.com/>

Если вы действительно заинтересовались паролями и их взломом, то вам — сюда. Приятного чтения и успехов в исследованиях!

❑ <http://lifehacker.com/tag/windows/>

Вот уж где раздолье для любителей "трюков", в том числе и трюков с реестром! А вот здесь: <http://lifehacker.com/tag/passwords/> — все, что вы хотели знать о паролях и их взломе, но боялись спросить.

❑ **<http://www.fas.org/irp/nsa/rainbow.htm>**

Официальный источник информации для всех, кто интересуется безопасностью компьютерных систем. Это — книги "Радужной серии".

❑ **<http://www.invisiblethings.org/>**

Сайт известной польской исследовательницы в области компьютерной безопасности Жанны Рутковской (Joanna Rutkowska), создавшей руткит по обходу цифровой подписи драйверов в Windows Vista ("Синяя пилюля"). Помимо текста презентации "Синей пилюли" здесь можно найти множество других полезных материалов и утилит.

❑ **<http://www.windowsreinstall.com/>**

Сайт, содержащий более 3000 страниц с ценнейшей информацией по установке, обновлению, переустановке, восстановлению и устранению неполадок, относящейся ко всем основным операционным системам из семейства Windows, которые когда-либо были выпущены Microsoft.

❑ **<http://www.windows7update.com/>**

Сайт, полностью посвященный Windows 7, где рассматриваются такие важные вопросы, как переход на использование Windows 7, установка, настройка, конфигурирование системы, вопросы миграции с более ранних версий и многое другое.

❑ **<http://www.techddi.com/>**

Сайт фирмы, специализирующейся на восстановлении данных. Предлагается множество специализированных утилит для восстановления поврежденных данных с различного рода носителей: жестких дисков, iPod, флэш-памяти, цифровых камер и т. п. Утилиты Windows NTFS Data Recovery Software и Windows FAT Data Recovery Software обеспечивает поддержку Windows Vista и Windows 7.

❑ **<http://www.xp-vista.com/category/troubleshooting/>**

Сайт, посвященный настройке и устранению неполадок в Windows XP и Windows Vista. Много ценной информации по вопросам безопасности. Сайт будет очень полезен тем, кто переходит на Windows 7, минуя Vista.

❑ **<http://www.insidetheregistry.com/content/home.aspx>**

Специализированный сайт, целиком и полностью посвященный реестру всех версий Windows.

❑ **<http://www.windows7hacker.com/>**

Сайт с "говорящим" названием — здесь много именно "хакерской" информации о Windows 7, которую вряд ли можно найти где-то еще.

❑ <http://www.hack7mc.com/>

Сайт, посвященный вопросам хакинга мультимедийных средств Windows 7 (Windows 7 Media Center).

❑ <http://www.downloadatoz.com/toplight/windows+7.html>

Здесь вы найдете разнообразные твики и трюки, связанные с Windows 7, но не в этом главная ценность данного ресурса. Что мне особенно в нем нравится — большое количество ценных рекомендаций по выбору утилит для Windows 7. Не просто как-то в ней работающих, а написанных специально для нее!

❑ <http://www.pctools.com/guides/registry/>

Здесь содержится большое количество "твиков" и "хаков" реестра (правда, для версий Windows, более ранних, чем Windows 7). Часть из них будет работать в Windows 7, а часть, к сожалению, нет. Поэтому относитесь к ним внимательно!

❑ <http://www.sevenforums.com/>

Краткие руководства по выполнению всех основных задач в Windows 7, а также дискуссионные форумы, посвященные этой операционной системе. Аналогичный сайт для Windows Vista — <http://www.vistaforums.com/>.

❑ <http://4sysops.com/archives/windows-7-all-4sysops-articles/>

Подборка статей, посвященных Windows 7 и предназначенных для системных администраторов.

❑ <http://www.askvg.com/category/windows-seven/>

Подборка "хаков" для Windows 7 (аналогичная подборка для Vista — <http://www.askvg.com/category/windows-vista/>).

Заключение

Естественно, что представленный список охватывает далеко не все ресурсы Интернета, посвященные Windows NT/2000/XP/Vista/7. Читатели, заинтересованные в обсуждаемой тематике, безусловно, найдут и множество других (и, вероятно, не менее интересных, чем приведенные здесь). Автор привел здесь только те, которые ему особенно понравились и оказались весьма полезны как в процессе повседневной работы, так и при поиске ответов на вопросы, которые у него возникали. Хочу особо отметить, что на момент написания данной книги все ссылки были рабочими.



Приложение 2

Список литературы

Разумеется, одна книга не может дать читателю ответы на все возникшие у него вопросы, как бы этого ни хотелось ее автору. Очень часто бывает, что с этой задачей не справляются даже энциклопедии (а эта книга энциклопедией не является). Автор считает необходимым привести список книг, в которых вы, скорее всего, найдете то, что вас интересует.

Как уже говорилось во введении, если вы проигнорировали Windows Vista, то в Windows 7 вас будет ждать множество неожиданностей, многое будет казаться вам непривычным и необычным, и у вас возникнет множество вопросов. И в этом нет ничего удивительного, потому что если между Windows XP и Windows Vista лежит пропасть, то от Windows Vista до Windows 7 — всего лишь один (но очень важный) шаг. Поэтому в данном списке литературы я и привожу ряд книг по Vista, поскольку они должны помочь вам понять многое из того, с чем вам предстоит познакомиться и в Windows 7. К сожалению, книг о Windows 7 на момент подготовки этой книги было очень мало, но есть и они. Не все эти книги мне понравились — временами у меня возникало впечатление, что их авторы просто взяли свои старые книги даже не по Vista, а по XP, и механически заменили буквосочетание "XP" на цифру "7". Их я в списке не упоминаю. Но есть и несколько достойных книг по Windows 7, и их я с удовольствием приведу. Итак:

Книги о Windows Vista

1. Брайан Ливингстон, Пол Таррот. "Секреты Windows Vista". — Диалектика, Вильямс, 2007.
2. Гралла П. "Windows Vista. Настольная книга пользователя и администратора" — СПб.: Питер, 2008.

3. Дэвид Пог. "Windows Vista. Недостающее руководство". — М.: "Русская Редакция", СПб.: БХВ-Петербург, 2008.
4. Кальп, Б. "Администрирование Windows Vista. Полное руководство". — М.: "Русская Редакция", СПб.: БХВ-Петербург, 2008.
5. Кокорева О. "Windows Vista. Решение проблем". — СПб.: БХВ-Петербург, 2009.
6. Майкл Ховард, Дэвид Лебланк. "Защищенный код для Windows Vista". — СПб.: Питер, 2008.
7. Мелбер Д. "Групповая политика Windows. Ресурсы Windows Server 2008, Windows Vista, Windows XP, Windows Server 2003 (+ CD-ROM)" — М.: "Русская Редакция", СПб.: БХВ-Петербург, 2009.
8. Пол Мак-Федрис. "Microsoft Windows Vista. Полное руководство". — Вильямс, 2007.
9. Таллоч М., Нортроп Т., Ханикатт Дж. "Ресурсы Windows Vista". — М.: "Русская Редакция"; СПб.: БХВ-Петербург, 2008.
10. Уильям Р. Станек. "Microsoft Windows Vista. Справочник администратора". — М.: "Русская Редакция", СПб.: БХВ-Петербург, 2008.
11. Чекмарев А. "Windows Vista для пользователей". — СПб.: БХВ-Петербург, 2007
12. Чекмарев А. "Windows Vista. Руководство администратора". — СПб.: БХВ-Петербург, 2008

Книги о Windows 7

1. Чекмарев А. "Windows 7 — это вам понравится!" — СПб.: БХВ-Петербург, 2009.
2. Paul McFedries. "Windows 7 Unleashed". — NY.: SAMS, 2009
3. Paul Thurrott, Rafael Rivera. "Windows 7 Secrets". — Wiley, 2009.
4. Ed Bott, Carl Siechert, Craig Stinson. "Windows 7 Inside Out". — Microsoft Press, 2009.



Приложение 3

Описание компакт-диска

На компакт-диске вы найдете сопроводительные материалы, призванные помочь в освоении принципов устранения неполадок и решения проблем Windows 7. Материалы для каждой главы сгруппированы по папкам, пронумерованным соответственно номерам глав.

Содержимое каждой папки выглядит следующим образом:

- ❑ Вложенная папка IMAGES — иллюстрации к соответствующей главе.
- ❑ Вложенная папка SUPPLEMENTARY — дополнительные материалы к соответствующей главе, не поместившиеся в печатную версию книги.

Предметный указатель

- "
- "super-hidden" files 406
- .
- .DEFAULT 480
- @
- @stake 661
- 6
- 6to4 391
- A
- Access Control Entry 420, 462
- Access Control List 128, 347, 421
- ACE 420, 462
- ACL 128, 347, 421, 466, 544, 546, 548
- ACM 255
- ACPI 215, 267, 274, 275
 - 2.0 217
 - 3.0 287
 - таблицы 278
 - уровни поддержки 276
 - уровни энергопотребления системы 293
- ACPI BIOS 237
- ACPI Machine Language 278
- Acronis True Image 81, 84
- Active Directory Services Interface (ADSI) 506
- Adaptive Display Brightness 279
- Add Hardware Wizard 213
- Add/Remove Hardware, утилита Control Panel 368
- Address Windowing Extensions 197
- ADE 255
- Administrative Tools 24
- Administrator
 - разблокирование учетной записи 172
 - учетная запись 45, 172, 412, 423, 480, 526
- Administrator Approval Mode 175
- Administrators
 - группа 45, 108, 128, 135, 422, 423
- ADML 509, 511
- ADMX 509, 511
- ADMX Migrator 510
- ADP 255
- Advanced Configuration and Power Interface 215
- Advanced Host Controller Interface 568
- Advanced Search 409
- Advanced Video Codec High Definition 206
- Aero 576
 - активация через реестр 171
 - причины, препятствующие работе 171
- AES256 588
- AHCI 567
- ALT 37
- Alternate Addressing 400
- AMD Athlon (K7) 580
- AML 278
- API:
 - для работы с реестром 333
 - ядра 336
- APIPA 398
- APP 255

Application manifests 15
ARP 400
ASA 255
ASCII 12, 13, 87, 103, 104, 658
ASP 255
ASPX 255
ATA 215
Authority number 419
AutoChk 541
Autoexec.bat 18
Automatic Private IP Addressing 398
AVCHD 206
AWE 197
AX 255

В

Backup Operators, группа 425
BAS 255
BAT 255
BCD 7, 21, 36, 84, 194, 195, 304,
308, 309, 312, 314, 315, 406, 518,
521, 543, 562
 объекты 196
 структура 197
 типы объектов 315
 типы стандартных
 приложений 316, 317
 улей реестра 33, 310, 312
 хранилища 195
BCD.LOG 36
BCDEdit 194, 198, 318, 319, 538, 562
 опции командной строки 319
BCD-Template 36
BCD-Template.log 36
BCD-Template.sav 36
Big endian 31
BIN 255
BIOS 194, 214, 216, 336, 518, 539, 565
 Setup 523, 568
 error codes 306
BitLocker Drive Encryption 65
Blue Screen of Death 327, 346
Bluetooth 205, 279, 359
Boot application 316

Boot Configuration Data 21, 194,
195, 543
Boot Configuration Database 304, 312
Boot manager phase 302
Boot partition 314
Boot sector 317
Boot sequence 307
Boot.ini 36, 194, 304, 309, 312,
319, 562
Boot\BCD, каталог 36, 304
Boot.ini 195, 197
Bootcfg.exe 319
Bootmgr 21, 84, 196, 304, 308, 309,
310, 312, 406, 518
BootRec /FixBoot 538
BootRec /FixMbr 538
BootRec /RebuildBcd 538
BootRec /ScanOS 538
Bootstrap 302
Boot-time programs 337
Bootvid.dll 331
Brute Force attack 660
BSOD 327, 346, 555, 556

С

C1, класс защищенности 404
C2, класс защищенности 404
Cache Manager 39, 335
CAD 577
CD 75, 79
 пишущий привод 79
Central Processor Unit 518
CER 255
ChkDsk 247, 337, 357, 543, 548
CHM 255
Ci.dll 331
Class installer 368
ClassGuid 369
CLB 255
CLFS 40
Clfs.sys 331
Client-Server Runtime SubSystem 343
CMD 255
CMOS 305, 518, 520, 523

CNT 255
CNV 255
COM 215, 255, 315
Command Prompt 45, 249, 358
Common Log File System 40
Compact Flash 338, 569, 600
Compaq 215
Complementary Metal Oxide
Semiconductor 305
COMPONENTS 36, 556
COMPONENTS.LOG 36
COMPONENTS.SAV 36
Config.sys 18, 24
Connect Network Registry 110
Control Panel 13, 24, 42, 43, 49, 50,
151, 152
Control set 333, 351
Control.ini 12
содержимое 13
Corel VideoStudio 58
CPL 255
CPU 518
CPX 255
Creator Owner, группа 420
Credential Providers 347, 405
CRT 255
CryptoAPI 253
Cryptographic Operators
группа 425
CSH 255
CSRSS 343, 346
Csrss.exe 144, 343, 345, 346

D

DAC 404
Debugging Mode 327
Default 34
Default.log 34
Default.sav 34
Delayed Start 353
Designed for Windows 7
логотип 208, 247
Desktop 472
Desktop Window Manager 171, 586

Device ID 21
Device Manager 42, 152, 210, 213, 223,
225, 262, 368
Devmgmt.msc 229
DEVMGR_SHOW_NONPRESENT_
DEVICES 229
DHCP 398
DID 21
Digital signature 236
Direct3D 205, 587
Direct3D 9 583
Directory Services Restore Mode 327
DirectX 10 577
Disable automatic restart on system
failure 327
Disconnect Network Registry 110
Discretionary access control 404
DiskPart 538
Distributed COM Users
группа 426
DLL 20, 243, 255, 330, 343, 519
режима ядра 21
уровня ядра 331
DMA 24, 213
DNS 401
Driver ranking scheme 236
Driver Rollback 230, 238, 248
Driver Staging 216, 235
Driver Store 236
DRV 255
DTD 255
Dumpexam 565
DV 206
DVD 75, 79
пишущий привод 79
DWM 171
Dwm.exe 144
DX10 583

E

EFI 194, 214, 306, 311, 314, 539
EFS 26
EMD 342
Enable Boot Logging 326, 329

Enable low resolution video
 (640×480) 326
 EnhanceMySe7en 644, 645, 648
 Environment variables 471
 ERD Commander 33
 Error Reporting 248, 358
 ErrorControl:
 параметр реестра 354
 eSATA 569
 Eventvwr.msc 267
 Everyone, группа 420
 EXE 255
 Executive 216, 335
 модуль 242
 Extensible Firmware Interface 194, 214
 External Memory Device 342

F

Fast Boot 338
 FAT 337, 406
 FAT32 84, 308, 536
 File Signature Verification 247,
 254, 258
 FileRepository 234
 Firefox 622
 Firmware 278, 306
 application 316
 boot manager 316
 Flash USB 660
 Folder Redirection 493
 FreeBSD 2
 Freeware 48, 639
 FSV 247
 FullArmor Corp 510
 FXP 255

G

Gaming graphics subscore 580
 GINA 347, 348, 405
 Globally Unique Identifier 295
 GPedit.msc 250, 382, 409, 424, 429
 GPO 501, 509
 Graphical Identification and
 Authentication 347, 405

Graphics subscore 580
 Group Policies 23
 Group Policy 288, 472
 Group Policy Objects 501
 GRP 255
 Guests:
 группа 426
 GUID 244, 245, 295, 298, 317, 369

H

HLS 255
 HAL 196, 313, 335
 Hal.dll 21, 313, 331
 Handle 28
 Hard links 484
 Hardware Abstraction Layer 196,
 313, 335
 Hardware Compatibility List 207, 254
 Hardware ID 245
 Hardware Profiles 24, 29
 HCL 207, 254
 HD video 577
 HDTV 206
 HDV 206
 HelpServicesGroup, группа 425
 H-HDD 339
 Hiberfil.sys 315
 Hibernate 293
 Hives 31
 HKCC 34, 136
 HKCR 136
 HKCU 34, 35, 136, 412
 HKEY_CLASSES_ROOT 27, 29, 115
 HKEY_CURRENT_
 CONFIG 27, 29, 115
 HKEY_CURRENT_
 USER 27, 29, 115, 148
 HKEY_LOCAL_MACHINE 27, 28, 31,
 107, 115, 148
 HKEY_LOCAL_
 MACHINE\BCD00000000 195
 HKEY_LOCAL_
 MACHINE\HARDWARE 214
 HKEY_LOCAL_MACHINE\
 HARDWARE\DESCRIPTION 214

HKKEY_PERFORMANCE_DATA 27
HKKEY_USERS 27, 29, 107, 115, 148
HKLM 136, 412
HKLM\BCD00000000 35, 304
HKLM\COMPONENTS 35
HKLM\HARDWARE\
 DEVICEMAP 214
HKLM\SAM 34, 35
HKLM\Security 34
HKLM\SECURITY 35
HKLM\Software 34
HKLM\SOFTWARE 35
HKLM\System 34
HKLM\SYSTEM 35
HKU\DEFAULT 34, 35
HLP 255
HomeGroup 362, 392, 397
HomeGroup Listener 398
HomeGroup Provider 397
HomeUsers 426
Hot-plug notification 232
HTA 255
Hybrid sleep 293

I

I/O Manager 216, 224
Icacs 463
IDE 307
IEEE 1394 207, 215, 218, 331
IEPM 465
IIS 426
IIS_USRS
 группа 426
IME 255
INF 232, 252, 255
INF-файлы 21, 48, 234, 369
 прекомпилированные 234
INI-файлы 12, 18, 24
INS 255
Integrity SID 464
Intel 215
Intel Pentium 4 580
IntelliMirror 505
Internet 49

Internet Explorer
 защищенный режим 465
Internet Explorer Protected Mode 465
Internet Information Server 426
IP Helper 389
IPHLPVC.DLL 389
IPv4 359
 поверх IPv6 392
IPv6 359, 360, 387
 поверх IPv4 388
IRP 221
IRQ 213
ISA 215
ISATAP 391
ISO-файлы 525
ISP 255
Itanium 304, 306, 311

J

JPEG 612
JPG 640
JS 255
JScript 506
JSE 255
Junction points 484, 493

K

Kd1394.dll 331
Kdcom.dll 331
Kdusb.dll 331
Kerberos V5 347
Kernel loading phase 304
Kernel Mode 233
Kernel Transaction Manager 23
Ksecdd.sys 331
KSH 255
KTM 23

L

L0phtCrack, утилита для взлома
 паролей 469, 660, 661
LANDesk Management Suite 493
Last Known Good Configuration
 (Advanced) 326, 333, 350, 352, 558

LastKnownGood 349, 352, 519
LCP 662
 утилита для взлома паролей 469
Least Privileged User Account 45,
 174, 422
Legacy devices 208
Libraries 397
Link Layer Topology Discovery 380
Linux 2, 84, 174, 406
Little Tweaker 648
Little-endian 30
LLTD 380, 381, 385
 настройки групповой
 политики 385
LM-аутентификация 450
LNK 255
Local Procedure Call 335
Local Security Authority SubSystem
 345, 348
Local user profile 24
LocalService 480
LocalSystem 343
 учетная запись 412
LOG 37
Logical Prefetcher 338
Logon Changer for Windows 7 642, 643
LPC 335
LPT 215
LSA 347
LSASS 348
Lsass.exe 314, 343
LUA 45, 174, 422
LZW 580, 588

M

Mac OS X 2
MAD 255
MAF 255
MAG 255
Malware 45
MAM 255
MAN 255
Mandatory integrity control 462
Mandatory user profile 24

MAN-файл 234
MAQ 255
MAR 255
MAS 255
Master Boot Record 307, 357
MAT 255
MAU 255
MAV 255
MAW 255
MBR 307, 357, 518, 543, 545
MDA 255
MDB 255
MDE 255
MDT 255
MDW 255
MDZ 255
Memory Manager 335
Memory Stick Pro 206
Memory subscore 580
Memory.dmp 560
Memtest.exe 318, 548
Memtest.exe 312, 321
MIC 462
Microkernel 335
Microsoft 1, 12, 32, 45, 50, 205, 215,
 556, 573
Microsoft DirectX 9 582
Microsoft Knowledge Base 50
Microsoft Malicious Software Removal
 Tool 570
Mklink 485
MMC 494
Mmsys.cpl 600
MRUList 13
MSC 255
Msconfig.exe 178, 194, 198, 598
MS-DOS 12, 24, 29
MSI 255, 635
MSP 255
MST 255
MUI 255

N

NAT 388
Native kernel API 336

Net 368
NetClient 369
NETLOGON 503
NetService 369
Netsh.exe 390
NetTrans 369
Network Address Translation 388
Network and Sharing Center 361
Network Configuration Operators,
 группа 425
Network Control Center 123
Network Diagnostics and
 Troubleshooting 364
Network Map 363
NetworkService 480
NLS 255
Nonpaged pool 332
Notify object 370
NSA 404
Nbtlog 552
Nbtlog.txt 326
Ntdetect.com 309
NTFS 84, 112, 124, 308, 337, 406,
 484, 498
 на базе транзакций 23, 248
 точки разветвления 484
NTFS v4.0 484
NTFS v1.0 484
NTFS v1.1 484
NTFS v1.2 484
NTFS v3.0 484
NTFS v3.1 484
NTFS v5.0 484
NTFS v5.2 484
NTFS v6.0 484
NTFSDOS 467, 468
Ntldr 197, 304, 308, 309, 312, 317, 318,
 321, 519
Ntldr-based loader object 316
NTLM 347
 аутентификация 450
Ntoskrnl.exe 21, 313, 329, 331, 336
Ntuser 36
Ntuser.dat 34, 35, 36, 473, 474, 487,
 488, 504

Ntuser.dat.log 34, 35, 36, 474, 487
Ntuser.ini 487
Ntuser.pol 487
NVRAM 339, 520, 523

O

Object Linking and Embedding 13
Object Manager 335
OCX 20, 255
OEM 252, 254, 275, 611
OLE 13, 18, 29
OnNow, промышленная
 инициатива 215
OpenBSD 2
Operating System-directed configuration
 and Power Management 275
Ophcrac 662
OPS 255
Orange Book 404
OSPM 275
OwnerRights 420

P

PAE 197
Paged pool 39
Pagefile.sys 605, 606
Paging 334
PAL 255
Partition Boot Record 307, 518
Partition Boot Sector 309
Partition Table 307
PBDA 206
PBR 307, 518
PC Card/CardBus 215
PC Tattletale 21
PCD 255
PCI 215, 216, 217
PCI Express 217, 338, 600
Performance Log Users 426
Performance Monitor Users
 группа 426
Perl 506
Physical Address Extension 197
PIF 255

Plug and Play 14, 18, 43, 121, 205, 207,
214, 349, 520
 архитектура 223
 краткая история 214
 распознавание устройств 230
 уровни поддержки 222
Plug and Play Manager 216, 220, 224,
225, 267
PNF-файлы 234
PnP 207, 222, 252
PnP Manager 21
PnP-X 225
Policy Manager 224
POSIX 336, 345
POST 302, 305, 306, 311, 357, 518,
520, 522
Power management 274
Power Manager 23, 216, 224
Power On Self Test 305
Power Options,
 утилита Control Panel 275
Power plans 279
Power Users, группа 423, 424
Power-on self test 302, 305, 306, 311,
357, 518, 520, 522
PPP 392
Previous versions 66
PRF 255
PRG 255
Prism Deploy 493
Private initialization files 13
Problem Reports and Solutions 265
Process Manager 335
Process Monitor 622, 658
Processor subscore 580
Procexp.exe 491, 492
Procmon.exe 658
Progman.ini 12
 содержимое 13
Protected Broadcast Driver
 Architecture 206
Protocol.ini 12
 содержимое 13
PST 255

Q

QoS 359, 381
Quality of Service 359, 381

R

Rainbow Series 404
RAR 213
ReadyBoost 338, 342, 580, 600
ReadyBoot 338, 339, 342
ReadyDrive 338, 339
Real-mode application 316
Recovery Console 16, 85, 538
REG 90, 467
Reg.dat 12, 13
 формат 13
Reg.exe 90, 93, 136, 147
 синтаксис 136
REG_BINARY 30, 115, 141
REG_DWORD 30, 141
REG_DWORD_BIG_ENDIAN 31
REG_DWORD_LITTLE_ENDIAN 30
REG_EXPAND_SZ 30, 101, 141
REG_FULL_RESOURCE_
 DESCRIPTOR 31, 118
REG_LINK 31
REG_MULTI_SZ 30, 101, 141
REG_NONE 31, 141
REG_QWORD 31
REG_QWORD_LITTLE_ENDIAN 31
REG_RESOUCE_REQUIREMENTS_
 LIST 31
REG_RESOURCE_LIST 31, 118
REG_RESOURCE_REQUIREMENTS_
 LIST 118
REG_SZ 30, 101, 141
Regback, команда 467
REGBACK
 папка 33
Regedit.exe 14, 87, 88, 90, 93, 94, 183,
407, 408, 412, 415, 622, 639
 загрузка и выгрузка ульев 106
 изменение прав доступа 412
 интерфейс 97
 клавиатурные комбинации 99
 меню Избранное 122

описание интерфейса 98
подключение сетевого реестра 109
права доступа по умолчанию 413
присвоение прав владельца 414
редактирование многострочных значений 118
редактор двоичных значений 115
редактор значений DWORD и QWORD 117
удаление ключей и параметров 119
управление безопасностью реестра 123
форматы экспортированных файлов 104
функции поиска 112
Regedt32.exe 94, 123
Regini.exe 93, 136, 147
Registry database 12
Registry Editor 42, 50, 93
Registry virtualization 41
Regmon.exe 658
REG-файл 48, 645
 экспорт 104
Relative ID 420
Release to Manufacturing 153
Reliability and Performance Monitor 593
Reliability Monitor 269
Remote Desktop Users, группа 425
REPAIR,
 папка 33
Replicators, группа 425
Resource Kit 93, 136, 147
Restore points 51, 52
Resume loader 313
RID 420
Roaming user profile 24
Robocopy 538
RS232 331
RTM 153

S

SACL 462
Safe Mode 325, 248, 326, 357
 режим загрузки 423

Safe Mode with Command Prompt 326, 328
Safe Mode with Networking 326
Safe Removal 219
SAM 34, 467
 взлом улья реестра 467
 улей реестра 470
Sam.log 34
Sam.sav 34
SATA 567
SAV 37
Sc 386
Sc showsid 420
SCF 255
SCR 255
Screen savers 472
SCSI 215, 307
SCT 255
SDK 29
Secure Digital 338, 569, 600
Security 34, 467
 улей реестра 470
Security ID 419, 476
Security log 131
Security Reference Monitor 335
Security token 41
Security, улей реестра 467
Security.log 34
Security.sav 34
Self-Monitoring, Analysis, and Reporting Technology 543
Serial Advanced Technology Attachment 567
Service Packs 1
Services.exe 314, 343
Session Manager 313
Session Manager Subsystem 335
SFC 247
Sfc.exe 255
SFP 247
SHA1 588
Shareware 48, 639
SHB 255
Shell folders 493
Shortcuts 484

- SHS 255
 - SID 419, 476, 477
 - формат 419
 - Sigverif 257, 559
 - Simplified Universal Player Encoder and Renderer 113
 - Sleep 293
 - SLMGR 191
 - Small Memory Dump 565
 - SMART 543
 - Smart Network Power 279
 - SMSS 335, 336, 343, 345
 - Smss.exe 313, 337
 - SMT 581
 - Software 34
 - Software Licensing Manager 191
 - Software.log 34
 - Software.sav 34
 - Spldr.sys 331
 - Spyware 21
 - SrtTrail.txt
 - файл журнала восстановления системы 540
 - Standby 293
 - Start, параметр реестра 353
 - Start Windows Normally 327
 - Startup Repair 249, 358
 - STOP 558, 563
 - ошибки 261
 - SUPER 113
 - SuperFetch 338, 339, 600, 601, 602
 - Surprise removal 219
 - SVCHOST 389
 - Symantec 661
 - Symantec Ghost Solution Suite 493
 - SYS 255
 - System 34, 39, 480
 - улей реестра 519
 - System access control list 462
 - System auditing 404
 - System File Checker 247, 254, 255
 - System File Protection 247
 - System Image Restore 536
 - System initialization files 12
 - System partition 314
 - System policy 507
 - System Policy Editor 508
 - System Protection
 - активизация 55
 - System Reserved
 - раздел 309
 - System Restore 51, 58, 62, 246, 249, 356, 358
 - в Windows 7 53, 72
 - в Windows Vista 52, 72
 - в Windows XP 52, 72
 - запуск из WinRE 535
 - конфигурирование 72
 - обратимость операции 61
 - отмена операции восстановления 63
 - ручная активизация 72
 - ручное создание точки восстановления 54
 - сервис 69
 - System.alt 39
 - System.ini 12
 - содержимое 13
 - System.log 34
 - System.sav 34
 - SYS-файлы 234
- Т**
- Task Scheduler 52, 53
 - TCP/IP 359, 360, 398, 519
 - TCSEC 404
 - Teredo 387, 388, 392
 - блокировка 390
 - клиент 389
 - конфигурирование 390
 - реализация в Windows Vista 388
 - сервер 389
 - Timer Coalescing 279
 - TLB 255
 - Tpm.sys 331
 - Transactional NTFS 39, 248, 484
 - Trusted Computer Base 343
 - Trusted Computer System Evaluation Criteria, TCSEC 404

TrustedInstaller 255, 415, 420, 465

сервис 412

учетная запись 412

TSP 255

TUNMP.SYS 389

TUNNEL.SYS 389

TweakNow PowerPack 654

Tweaks 609

TweakUI 65

TxF 23, 39, 484

TxR 23, 39

Txtsetup.oem 372

U

U.S. National Security Agency 404

UAC 26, 41, 45, 97, 142, 407, 422, 425, 429, 436

блокировка через реестр 183

настройка через реестр 185

отключение только для

администраторов 183

принцип действия 26

разблокирование 175

UDP 388

Ultimate

Windows 7 Ultimate 536

Ultimate Windows Tweaker 649

UMPNPMPGR 252

UNC 147, 497

Uniblue DriverScanner 656

Unicode 31, 304

Universal Naming Convention 147, 497

UNIX 484

Unsafe Removal of Device 219

URL 255

USB 205, 207, 215, 218, 286, 315, 331, 523, 529, 538

носители 79

USB 2.0 530, 600

USB Flash 338, 529, 600

User Account Control 26, 106, 142, 174, 422, 429, 436

User profiles 24, 472

User State Migration Tool 493

Userdiff 34, 36

Userdiff.log 34

Userdifr 34

Userdifr.log 34

Userinit.exe 347

Users, группа 423, 425

USMT 493

Uuidgen.exe 244, 369

V

VB 255

VBE 255

VBS 255

Vendor ID 21

VGA 325

VHD 207

VID 21

Virtual hard disk 207

Visual Basic Scripting Edition
(VBScript) 506

Volsnap.sys 65

Volume Shadow Copy 52, 65

Volume Shadow Copy Service 73

Volume snapshots 75

Vsmacros 255

VSS 73, 75, 255

VSSAdmin.exe 73, 74

VST 255

VSW 255

W

W7C Windows 7 UI Changer 642

WAIK 524, 525, 529

Wallpaper 472

WBF 405

WDDM 168, 583

WDDM 1.1 577

WDF 217

WDM 217

Web-камера 206

WEI 574

фальсификация 579, 589

Well-known folders 493

- Well-known SIDs 420
- WFP 234, 254, 412
- WHL 238
- Wi-Fi 359
- WIM-файл 315
- Win.ini 12
 - содержимое 12
 - ограничение по размерам 12
 - ограничение по размеру 14
- Win32 343, 347
- Winamp 622
- WinDbg 565
- Windows 15
 - 64-разрядные версии 253, 527
 - Safe Mode 63
 - безопасный режим загрузки 63
 - загрузчик возобновления работы 304
 - защита ресурсов 247
 - индекс производительности 574
 - индекс стабильности 272
 - предзагрузочные приложения 312
 - ранние версии 12
 - среда восстановления 20
 - установка критического обновления 59
 - установка устройств 207
 - утилиты для взлома паролей 660
- Windows 2000 4, 21, 26, 94, 484
- Windows 2000/XP 205
 - консоль восстановления 85
 - схема ранжирования драйверов 236
- Windows 3.1 11
- Windows 7 4, 11, 13, 16, 19, 33, 48, 207, 270, 403, 525, 531, 616, 619, 620, 621, 644, 660
 - "синий экран" 557, 560
 - 32-разрядные версии 527
 - Action Center 270
 - Business 167
 - Enterprise 167
 - Home 185
 - Home Edition 165
 - Home Premium 185
 - pfuhepxdr 207
 - RC 2
 - Release Candidate 153
 - RTM 2, 153
 - UAC 176
 - Ultimate 167
 - автоматическая регистрация в системе 620
 - административные средства 24
 - бета-версии 153
 - библиотеки 624
 - восстановление системы 51
 - Диагностика и устранение проблем с загрузкой 517
 - диапазон WEI 576
 - диск аварийного восстановления системы 78
 - домашняя группа 392
 - загрузочная анимация 331
 - загрузочное меню 321
 - загрузочный DVD 310
 - запись ISO-образов на CD и DVD 525
 - запуск сервисов 574
 - инициализация ядра 334
 - конфигурирование совместного доступа к файлам и папкам 452
 - методы индивидуальной настройки 153
 - минимальные требования Aero 168
 - настройка UAC 176
 - настройка активации 188
 - настройка процесса регистрации 610
 - настройка экрана регистрации в системе 611
 - настройки пользовательского интерфейса 154
 - новые возможности резервного копирования 78
 - новые уровни WEI 577
 - оптимизация производительности 594
 - опции отладочного меню при загрузке 322
 - перемещаемые профили пользователей 498

- планы электропитания 280
- поддержка Plug and Play 205
- подключение к Интернету 362
- пользовательские профили 24
- популярные постинсталляционные настройки 153
- пример неработающего твика 164
- производительность 573
- простейший способ настройки загрузки 192
- процесс загрузки 192, 301
- регистрационная информация сетевых адаптеров 372
- роль и место реестра 16, 18
- сетевые компоненты 26
- сетевые параметры в реестре 368
- сетевые технологии 359
- система оценки WEI 581
- системные сервисы 597
- слияние таймеров 279
- совместимые устройства 22
- создание диска аварийного восстановления системы 79
- создание образа системы 81
- создание точки восстановления 53
- схема процесса загрузки 302
- темы оформления 612
- ули реестра 33
- условия успешной загрузки 305
- установка сетевых компонентов 360
- файлы, необходимые для запуска 312
- Центр архивации и восстановления 75
- Центр поддержки 270
- Центр управления сетями и общим доступом 361
- энергосберегающие режимы 275
- этапы загрузки 302
- Windows 7 Enterprise 536
- Windows 7 Logon Background Changer 640, 642
- Windows 7 Manager 652
- Windows 7 Professional 536
- Windows 7 Setup 19
- Windows 95 11, 15, 94
- Windows Aero 164, 168, 582
 - активация темы 172
 - минимальные требования 168
- Windows AIK 525
 - установка 526
- Windows Automated Installation Kit 524, 525
 - установка 525
- Windows Biometric Framework 405
- Windows boot loader 315, 317
- Windows boot manager 21, 304, 315, 316
- Windows Display Driver Model 168
- Windows Experience Index 574
- Windows Explorer 43, 488
- Windows File Protection 234, 254, 412
- Windows Firewall 26, 359, 389
- Windows for Workgroups 3.1x 13
- Windows Genuine Advantage 188
- Windows Hardware Quality Lab, WHQL 372
- Windows image file 315
- Windows Installer 634
- Windows Logo v. 3.0 20
- Windows Management Instrumentation 217
- Windows Management Instrumentation (WMI) 506
- Windows Media Center 206
- Windows Media Player 622
- Windows Memory Diagnostic 321
- Windows Memory Diagnostic Tool 536
- Windows Memory Diagnostics Tool 249, 358
- Windows memory tester 317
- Windows Memory Tester 197
- Windows Mobile Device Center 22, 59
- Windows network class installer 368
- Windows NT 205, 312
- Windows NT 3.1 484
- Windows NT 3.5 15, 484
- Windows NT 3.51 484
- Windows NT 4.0 36, 484
- Windows NT/2000/XP/Vista 403

- Windows NT 16
- Windows operating system loader 304
- Windows PE 527, 529
- Windows Platform SDK 244, 369
- Windows pre-boot applications 518
- Windows Preinstallation Environments 527
- Windows Premium Logo 576
- Windows Presentation Foundation 640
- Windows Recovery Environment 16, 20, 51, 52, 78, 85, 358
- Windows reliability index 272
- Windows Resource Protection 234, 247, 254, 356, 412
- Windows resume application 317
- Windows resume loader 304
- Windows Script Host (WSH) 2.0 506
- Windows Server 2003 330
- Windows Server 2003 R2 40
- Windows Server 2008 32, 526, 531
- Windows Server 2008 R2 526
- Windows System Assessment Tool 584
- Windows Task Manage 593
- Windows Task Manager 144
- Windows Update 58, 248
 - сервис 412
- Windows Update Center 59, 210
- Windows Vista 1, 2, 4, 15, 16, 18, 23, 26, 32, 33, 84, 154, 188, 221, 269, 270, 372, 535, 660
 - "синий экран" 557, 560
 - BSOD 556
 - Home 185
 - Home Premium 185
 - SP1 573
 - SP2 573
 - UAC 175
- Windows Security Center 270
 - активация 187
 - аппаратные профили 239
 - базовые уровни WEI 576
 - взаимодействие с компьютерами Windows XP 387
 - возможности по защите системы 123
 - встроенные средства по управлению надежностью 246
 - диапазон WEI 576
 - дистрибутивный DVD 310
 - загрузка с дискеты 310
 - загрузочная анимация 331
 - загрузочное меню 321
 - защита драйверов цифровой подписью 252
 - защита системных файлов 249
 - известные SID 421
 - изменения групповой политики 508
 - изменения пользовательских профилей 474
 - несовместимость пользовательских профилей с Windows XP 476
 - новые виды пользовательских прав 434
 - новые политики в отношении пользовательских профилей 500
 - обязательный контроль целостности 462
 - описание корневых ключей 28
 - особенности MBR 308
 - отложенный автоматический запуск служб 350
 - перемещаемые профили 498
 - планы энергопотребления системы 278
 - поддержка Plug and Play 205
 - политики аудита 427
 - проблемы в мультизагрузочных системах 549
 - проблемы нехватки памяти 594
 - процесс загрузки 192, 301, 302
 - ранжирование драйверов 237
 - распространенные ошибки STOP 565
 - регистрация пользователя в системе 304
 - сервисы с отложенным запуском 354
 - сетевые возможности 359
 - система оценки WEI 580
 - скрытая учетная запись Администратора 45

- стандартные настройки
 - безопасности 422
 - типовые настройки
 - безопасности 436
 - усовершенствования реестра 39
 - файлы, необходимые
 - для запуска 312
 - Центр обеспечения
 - безопасности 269
 - Центр управления сетями и общим доступом 361
 - централизованное хранилище драйверов 231
 - энергосберегающие
 - режимы 274, 288
 - Windows Vista Business 84, 288
 - Windows Vista Display Driver Model 583
 - Windows Vista Enterprise 288
 - Windows Vista Home Basic 288
 - Windows Vista Home Premium 288
 - Windows Vista Pre-boot eXecution Environment 321
 - Windows Vista Ultimate 51, 84
 - Windows Vista с Service Pack 1 526
 - Windows Vista/7
 - Home Edition 184
 - сетевое размещение 454
 - Windows Vista Ultimate 288
 - Windows XP 1, 4, 15, 36, 65, 197, 235, 238, 406, 519, 535, 587, 616, 660
 - Recovery Console 86
 - аппаратные профили 24
 - консоль восстановления 521, 538
 - политики аудита 427
 - процесс загрузки 301
 - типовые настройки
 - безопасности 436
 - Windows XP Home Edition 288
 - Windows XP Professional 288
 - Windows XP Service Pack 2 330
 - WindowsXP 588
 - Winfile.ini 12
 - содержимое 13
 - Wininit.exe 345
 - Winload.exe 21, 196, 304, 308, 309, 312, 319, 330, 331, 519, 522, 543, 545
 - Winlogon 313, 343, 345, 347, 348, 405
 - WinRE 16, 20, 51, 52, 78, 85, 323, 324, 358, 423, 520, 521, 524, 529, 531, 568
 - Command Prompt 86
 - Startup Repair 86
 - System Restore 86
 - Windows Memory Diagnostic Tool 86
 - запуск 531
 - настройка среды 529
 - опции 85
 - опции командной строки 538
 - установка на жесткий диск 531
 - Winreg 466
 - Winresume.exe 196, 197, 304, 313, 518
 - WinSAT 584
 - хранилище данных 585
 - WinSAT API 586
 - Winsat.exe 584, 586
 - синтаксис 586
 - Winsat.prx 588
 - Winsat.wmv 588
 - Winsatencode.wmv 588
 - Winternals 33
 - Wireless USB 205, 360
 - WMI 217
 - WPF 640
 - WRP 234, 247, 254, 255, 356, 412, 415, 464
 - WS 255
 - WSC 255
 - WSF 255
 - WSH 255
 - WUSB 205
- X, Z**
- x86 304, 306, 518
 - xcopy 538
 - XdN Tweaker 651
 - XML 273, 509, 584
 - xsd 255
 - xsl 255
 - zip 213

А

Автозагрузка 350
Автоматическое обновление 248
Адаптивное управление яркостью
дисплея 279
Администратор
встроенная учетная запись 423
разблокирование учетной
записи 172
учетная запись 172, 412, 480, 526
Администраторы
группа 108, 123, 128, 135, 422, 423
Аппаратные конфликты 213, 214
Аппаратные профили 24, 29
Аудит 131
Аутентификация 404

Б

Безопасный режим загрузки 248, 357

В

Ветвь реестра
экспорт 103
Восстановление архива Windows
Complete PC 358
Восстановление запуска 249, 358
Восстановление образа системы 536
Восстановление системы 51, 246, 249,
356, 358
в Windows XP 52
в Windows 7 51
запуск из WinRE 535
Виртуализация реестра 41
Все пользователи, группа 420

Г

Гибернация 293
Гибридный жесткий диск 339
Гибридный сон 286, 293
Главная загрузочная запись 307
Гости
группа 426
Групповые политики 23, 472

Д

Дамп памяти 556
Дескриптор 28
Диспетчер Plug and Play 216, 224
PnP 21, 23
ввода/вывода 216, 224
локальных сеансов 345
питания 23
политики 224
сеансов 342
транзакций ядра 23, 39
устройств 42, 152, 210, 213, 223,
226, 262, 263, 368
электропитания 224
Домашняя группа 362
Домашняя сеть 454
Домен 454
Драйвер 21, 207
обновление 263
поиск обновлений 208
установка в автоматическом
режиме 207
установка и удаление 58
Драйверы устройств 23

Ж

Ждущие режимы 293
Жесткие ссылки 484
Жесткий диск
гибридный 339
Журнал безопасности 131

З

Загрузка и инициализация драйверов
и сервисов 304
Загрузка ядра 304
Загрузочное приложение 316
Загрузочный раздел 314
Загрузочный сектор 309, 317
Загрузчик 317
Загрузчик возобновления 317
Значимые элементы реестра 98

И

Идентификатор безопасности (security identifier, Security ID, SID) 419
Идентификация 404
Известные SID 420
Имена файлов
 расширения 18
Индекс производительности
 Windows 574
 базовый уровень 576
 вычисление 576
Индекс стабильности Windows 272
Инициализационные файлы
 приложений 12, 13
Инсталлятор класса 368
Интеллектуальное управление
 энергопотреблением сетевых
 устройств 279

К

Карта сети 363
Классическое меню Пуск
 имитация 155
Ключи реестра 27, 97
 опции аудита 135
 присвоение прав владельца 128
Командная строка 45, 249, 358
Консоль Восстановления 16
Контроль учетных записей
 пользователей 26, 45, 174, 422
КПК 21
Криптографические операторы
 группа 425

Л

Локальная политика
 безопасности 131

М

Манифесты приложений 15
Маркер безопасности 41
Мастер установки нового
 оборудования 213

Менеджер загрузки 33, 309
 загрузки EFI 316
 кэша 39
Меню Пуск (Start)
 классическое 154
Микропрограммное приложение 316
Моментальные снимки тома 75
Монитор стабильности системы 269
Мультизагрузочные конфигурации 549

Н

Набор управляющих параметров 351
 в реестре 350
Настройки рабочего стола 472
Нерезидентный пул 39
Носители
 твердотельные 577

О

Обновления
 с цифровой подписью 412
 установка 58
Общественная сеть 454
Объект на основе NTLDR 316
ООП 218
Операторы архива, группа 425
 настройки сети, группа 425
Операция восстановления
 отмена 63
Опытные пользователи, группа 423
Оранжевая книга 404
Откат драйвера 230, 238, 248
Отладочный дамп 563
Отчеты о проблемах и их решениях 265
Очистка файла подкачки 606
Ошибки реестра 49

П

Панель задач
 в Windows 7 163
 настройка 163
Панель управления 13, 24, 42, 43, 49,
 151, 152

- Параметры реестра 27
 - типы данных 30
 - Параметры управления электропитанием
 - для ноутбуков 284
 - для настольных компьютеров 284
 - настройка 281
 - установка через групповую политику 288
 - Пароль
 - требования к стойкому паролю 174
 - Переменные окружения 471
 - Перемещаемый пользовательский профиль 494
 - Планы электропитания 279, 295
 - высокая производительность 280
 - сбалансированный 280
 - экономия энергии 280
 - Подкачка 334
 - Подключи реестра 97
 - Подсистема диспетчера сеансов 335
 - Подуровень индекса производительности:
 - RAM 580, 581
 - графики для игр 580, 583
 - графической подсистемы 580, 582
 - процессора 580
 - основного жесткого диска 580
 - Пользователи,
 - группа 423, 425
 - Пользователи DCOM
 - группа 426
 - Пользователи журналов производительности
 - группа 426
 - Пользователи системного монитора
 - группа 426
 - Пользователи удаленного рабочего стола, группа 425
 - Пользовательские профили 24, 471
 - локальные 24
 - обязательные 24
 - перемещаемые 24
 - Пользовательский профиль
 - параметры 472
 - перемещение в другую папку 490
 - структура 473
 - Последовательность загрузки 307
 - Права владельца 420
 - Права доступа к ключам реестра
 - типы 125
 - Предзагрузочные приложения Windows 518
 - Предыдущие версии 66
 - Приложение Memtest.exe 317
 - Приложение реального режима 316
 - Приложения,
 - установка и удаление 14
 - Принцип минимальных достаточных полномочий 174
 - Проводник 43
 - Программа проверки подлинности Windows 188
 - Программы:
 - вредоносные 45
 - установка и удаление 58
 - Профили
 - аппаратные 24
 - Процесс:
 - начальной загрузки 302, 518
 - уровень целостности 462
 - Процессоры
 - двухъядерные 580
- Р**
- Работа менеджера загрузки 302
 - Радужная серия 404
 - Разграничительный контроль доступа 404
 - Раздел на диске
 - скрытый 33
 - Расширения имен файлов 18
 - Регистрционная база данных 12, 13
 - Регистрационный сценарий (logon script) 505
 - Редактирование реестра
 - альтернативы 42
 - Редактор реестра 14, 24, 42, 50, 87, 93
 - блокировка доступа через реестр 411

- блокировка доступа через
 - системные политики 409
- ограничение доступа 412
- Редактор системных правил 508
- Реестр 18, 472
 - альтернативные методы редактирования 49
 - архитектура 18
 - атомарность 37
 - виртуализация 142, 146
 - возникновение ошибок 49
 - иерархия 99
 - изменение прав доступа к ключам 123
 - концепция 12
 - корневые ключи 27
 - на базе транзакций 23, 39
 - резервное копирование 50, 151
 - ульи 32, 313
 - установка прав доступа 405
 - утилиты для очистки 645
 - параметры 27
- Режим административного подтверждения 175
- Режим ядра 233
- Репликатор, группа 425

С

- Самотестирование при включении питания 302
- Связь и внедрение объектов 13
- Сервис теневого копирования тома 73
- Сетевые протоколы канального уровня 380
- Символические ссылки 484
- Синий экран смерти 555
- Системная политика 471, 507
 - отличие от пользовательских профилей 507
 - шаблоны 508
- Системные инициализационные файлы 12
- Системные компоненты
 - взаимодействие с реестром 18

- Системный аудит 404
- Системный журнал событий 266
- Системный планировщик 52
- Системный раздел 307, 314
- Создатель-Владелец, группа 420
- Сон 293
- Список контроля доступа 128
- Спящий режим
 - параметры 281
- Средство восстановления системы усовершенствования Windows 7 70
- Сценарий
 - регистрационный 471

Т

- Таблица разделов 307
- Твики 609
- Телевидение высокой четкости 206
- Теневая копия тома 52, 53, 65
- Теневое копирование 51, 52, 65
- Точки восстановления 51, 52
 - автоматическое создание 52
 - рекомендации по выбору 58
 - типы 52
- Точки восстановления 51, 52
- Точки разветвления 484, 493

У

- Уведомление о внезапном подключении 232
- Удаленный доступ к реестру 449
- Ульи 32
 - отличие от других ключей 32
- Уникальный идентификатор устройства (Device ID, DID) 227
- Управление
 - электропитанием 274
- Управляющие наборы 349
- Упреждающая выборка 602
- Установка и удаление программ, утилита 368
- Устройства
 - скрытые 228

Ф

Файл подкачки 605
настройка 603
очистка 606
Файловые системы 26
Файлы:
"суперскрытые" 406
восстановление предыдущих
версий 66
резервное копирование
и восстановление 51
Файлы фоновых рисунков 472
Флэш-USB
использование для загрузки
WinRE 530

Ц

Центр архивации и восстановления
в Windows 7 78
в Windows Vista 78
Центр обновления Windows 59, 210
Центр управления сетями и общим
доступом 123

Центр устройств Windows Mobile 59
Цифровая подпись 236

Ч

Частная сеть 454

Ш

Шаблоны системной политики 508
Шифрующая файловая система 26

Э

Экран регистрации
стандартный 610
Экранные заставки 472
Экспорт реестра как метод резервного
копирования 87
Электропитание, утилита 275
Энергосберегающие режимы 274

Я

Ядро 313
инициализация 336, 519