Денис Колисниченко

СЕКРЕТЫ, НАСТРОЙКА И ОПТИМИЗАЦИЯ РЕЕСТРА Windows 7

Санкт-Петербург
«БХВ-Петербург»
2010

УДК 681.3.06
ББК 32.973.26-018.2
К60

Колисниченко Д. Н.

К60 Секреты, настройка и оптимизация реестра Windows 7. — СПб.: БХВ-Петербург, 2010. — 320 с.: ил.

ISBN 978-5-9775-0488-1

Рассмотрено устройство, настройка и оптимизация реестра, секреты и трюки при работе с ним, параметры популярных Windows-приложений. Описаны программы для мониторинга, чистки и быстрой настройки реестра, которые пригодятся каждому пользователю. Для администраторов систем даны приемы управления реестром (политики, списки доступа), использования Windows Installer, тонкая настройка системы и приложений, примеры действий в различных нештатных ситуациях. Некоторые настройки реестра, приведенные в этой книге, будут работать не только в Windows 7, но и в Windows Vista и Windows XP.

Для широкого круга пользователей Windows

УДК 681.3.06
ББК 32.973.26-018.2

Группа подготовки издания:

Главный редактор	*Екатерина Кондукова*
Зам. главного редактора	*Евгений Рыбаков*
Зав. редакцией	*Григорий Добин*
Редактор	*Ольга Кокорева*
Компьютерная верстка	*Ольги Сергиенко*
Корректор	*Зинаида Дмитриева*
Дизайн обложки	*Елены Беляевой*
Зав. производством	*Николай Тверских*

Лицензия ИД № 02429 от 24.07.00. Подписано в печать 30.10.09.
Формат 70×100$^{1}/_{16}$. Печать офсетная. Усл. печ. л. 25,8.
Тираж 1500 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 978-5-9775-0488-1

Оглавление

Введение

Тема данной книги — реестр популярных операционных систем от Microsoft — Windows Vista и Windows 7. Реестр (registry) — это важнейший компонент операционной системы Windows, который хранит как параметры самой операционной системы, так и настройки пользовательских программ.

Знание системного реестра Windows пригодится как обычному пользователю, так и системному администратору. Изменить параметры рабочего стола и пользовательских программ, сетевые настройки, параметры, влияющие на производительность, — все это можно сделать с помощью редактора реестра, который мы рассмотрим в этой книге.

В данной книге введение не будет скучным. Вместо краткого описания каждой главы ("Как читать эту книгу"), которое все равно никто не читает, мы поговорим о новшествах Windows 7. Думаю, данный материал будет интересен всем пользователям.

Новые возможности Windows 7

Как пользователь, работавший со всеми версиями Windows, начиная с Windows 3.0, могу ответственно заявить: до последнего времени лучшей версией Windows была XP. Ключевое слово здесь "была", потому что новая версия Windows — Windows 7 — по всем параметрам превосходит как Windows XP, так и Windows Vista.

Вкратце позволю себе охарактеризовать все версии Windows. Первую из них, Windows 3.0, сложно было назвать операционной системой, скорее, она представляла собой "надстройку" над MS-DOS. То же самое можно сказать и о Windows 3.1*x*. Потом появилась Windows 95, в основе которой тоже лежала MS-DOS (версии 7.0). Однако Windows 95 уже представляла собой полноценную 32-разрядную операционную систему. Впрочем, ядро Windows 95

было до такой степени незащищенным, что вытеснить его из памяти было под силу даже пользовательской программе. Кстати, в те времена я запускал программу loadlin для загрузки Linux, которая выгружала ядро Windows из памяти и загружала ядро Linux. В следующей версии, Windows 98, такой трюк уже не проходил, но все равно Windows оставалась слабо защищенной ОС, что подтверждалось огромным количеством вирусов, написанных специально для нее.

Параллельно разработке пользовательских версий Windows 9*x* велась разработка защищенной операционной системы для рабочих станций и серверов — Windows NT. Windows NT обладала гораздо более серьезными системными требованиями, но зато была более защищенной, благодаря как своему ядру, так и файловой системе NTFS (NT File System).

Затем, после выпуска Windows ME, Microsoft отказалась от ядра, используемого в Windows 9*x*: все новые версии Windows разрабатывались на основе ядра NT. В 1998 году появилась Windows 2000 — пятая версия NT, в которую вошли некоторые технологии из Windows 98, например, активный рабочий стол (active desktop) и новая версия браузера Internet Explorer. Windows 2000 представляла собой хорошую операционную систему, но почему-то не прижилась[1]. Может быть, это произошло потому, что она оказалась промежуточным звеном эволюции, и в 2001 году ей на смену пришла Windows XP.

Кстати, версии ядра Windows NT нумеровались так:

- 3.1 — Windows NT 3.1 Workstation, Advanced Server (1993 год)
- 3.5 — Windows NT 3.5 Workstation и Server (1994 год)
- 3.51 — Windows NT 3.51 Workstation и Server (1995 год)
- 4.0 — Windows NT 4.0 Workstation и Server (1996 год)
- 5.0 — Windows 2000 (1998 год)
- 5.1 — Windows XP (2001 год)
- 5.2 — Windows 2003 Server (2003 год)
- 6.0 — Windows Vista (2006 год), Windows Server 2008 (2008 год)
- 6.1 — Windows 7, Windows Server 2008 R2 (2009 год)

[1] Это высказывание довольно спорно, потому что очень многие люди довольно долго продолжали пользоваться Windows 2000, даже после выхода Windows XP (возможно, потому что она не требовала активации). На момент выпуска Windows 2000 именно она была лучшей среди всех ОС из семейства Windows, и в ней появилось множество прогрессивных нововведений. Так что сказать, что она "не прижилась", не совсем справедливо. Свою заслуженную долю популярности она все-таки получила. — *Прим. ред.*

Windows XP оказалась довольно удачной операционной системой — она была быстрой, надежной и вполне защищенной. Однако спустя 5 лет эта операционная система устарела. Она уже не поддерживала новые компьютеры (вспомните, как вы устанавливаете Windows — сначала вы устанавливаете операционную систему как таковую, а затем — драйверы устройств с диска производителя, т. к. Windows по умолчанию обеспечивает поддержку только базовых устройств). За время существования Windows XP для нее было написано огромное количество вирусов. Да и Microsoft с момента выпуска этой ОС давно не обновляла свое детище. Возникла потребность в повышении прибыли, а для этого нужна была новинка. В 2006 году такая новинка появилась — ею стала Windows Vista. Впрочем, широко разрекламированная система не оправдала ожиданий пользователей. В ней было множество недостатков, да и системные требования оставляли желать лучшего. Для 2006 года эта операционная система была настоящим "тяжеловесом". Ее даже назвали "провалом года" и самой худшей операционной системой от Microsoft (см., например, **http://ru.wikipedia.org/wiki/Windows_Vista**, **http://www.point.ru/news/stories/19316/**).

В апреле 2009 года вышел "релиз-кандидат" (RC) Windows 7, а 22 июля появилась окончательная версия (Release To Manufacturing, RTM)[1]. Кстати, оба этих релиза и использовались при написании данной книги. По заявлению Microsoft, в RC уже были включены все функции, присутствующие и в финальном релизе Windows 7. Это значит, что новых функций в тех версиях Windows 7, которые будут доступны конечным пользователям, уже не появится, а существующие просто будут "доведены до ума".

В Windows 7 появилось большое количество новых функций, и рассмотреть их все в этом кратком введении не представляется возможным. Некоторые из них просто неочевидны и обычному пользователю с первого взгляда даже незаметны. Например, знаете ли вы, что теперь в Windows 7 можно выбирать уровень уведомлений UAC (User Account Control)? Многие начинающие пользователи даже не обратят на это внимание, а профессионалы — совсем отключат UAC[2].

Рассмотрим основные нововведения, которые должны вызвать наибольший интерес именно у конечных пользователей.

---

[1] См. **http://en.wikipedia.org/wiki/Development_of_Windows_7**. — *Прим. ред.*

[2] Это тоже довольно спорное высказывание — ведь в Vista эта функция вызывала наиболее сильное раздражение у пользователей, так что многим из них возможность регулировки уровней UAC может показаться интересной. — *Прим. ред.*

Производительность

Windows 7 больше не кажется неповоротливым монстром, пожирающим системные ресурсы вашего компьютера. Тому есть две причины. Первая причина — в Microsoft действительно уделили самое пристальное внимание оптимизации системы. Так, она загружается и работает значительно быстрее, чем Vista, да и места занимает тоже меньше, чем Vista (Windows 7 Ultimate занимает всего 8 Гбайт дискового пространства сразу же после установки).

Вторая причина — за три года (с 2006-го) комплектация компьютеров "подросла". Если в 2006 году далеко не на каждом компьютере устанавливался 1 Гбайт оперативной памяти (обычно меньше), то сейчас компьютер с 1 Гбайт "оперативки" тоже встречается редко, но совсем по другой причине — обычно объем установленной RAM превышает это значение. Сегодня 2 Гбайт — это норма для нового компьютера. Выходит, что современные компьютеры уже достаточно давно соответствуют системным требованиям Vista. Тем не менее, многие пользователи все еще продолжают работать с Windows XP — уж так сильно не понравилась им Vista в 2006 году.

Новая панель задач

В Windows 7 более нет необходимости в использовании панели быстрого запуска (Quick Launch)[1], поскольку приложения, которые вы часто используете, можно закрепить прямо на панели задач (Taskbar). Чтобы закрепить приложение на панели задач, запустите приложение, щелкните правой кнопкой мыши по его значку на панели задач и выберите команду **Закрепить программу в панели задач** (Pin this program to taskbar), как показано на рис. В.1.

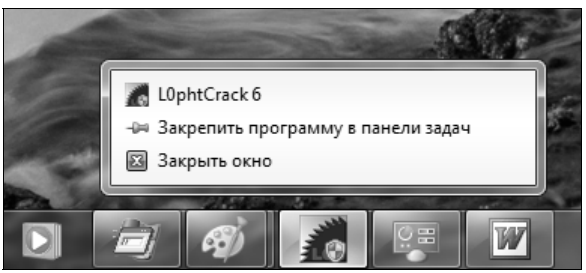


Рис. В.1. Привязка приложения к панели задач

Кроме того, новая панель задач выводит миниатюрные изображения окон программ, что позволяет быстро найти нужное окно. Далее, миниатюра мо-

[1] Хотя при желании восстановить ее можно — см. **http://www.sevenforums.com/tutorials/888-quick-launch-enable-disable.html**. — *Прим. ред.*

жет содержать список действий, например, для Windows Media Player — это могут быть кнопки переключения между композициями или кнопки управления воспроизведением видеоролика (рис. В.2). Выходит, чтобы сменить композицию или выполнить другое действие, соответствующее той или иной программе, не нужно даже переключаться в окно этой программы — достаточно нажать кнопку требуемого действия.

Рис. В.2. Миниатюры панели задач

К тому же новая панель задач стала полупрозрачной — сквозь нее просвечивает фон рабочего стола. Таким образом, она стала не просто более привлекательной, но и более функциональной.

Расширенное управление окнами

В предшествующих версиях Windows управление окнами было не очень удобным. В Windows 7 для этой цели можно использовать следующие клавиатурные комбинации (keyboard shortcuts):

- <Win>+<Up> — развернуть окно;
- <Win>+<Down> — восстановить/минимизировать окно;
- <Win>+<Left> — прикрепить окно к левому краю экрана;
- <Win>+<Right> — прикрепить окно к правому краю экрана;
- <Win>+<Shift>+<Up> — развернуть окно до максимального размера по вертикали;

- <Win>+<Shift>+<Down> — восстановить исходный размер по вертикали;
- <Win>+<Home> — минимизировать/восстановить все неактивные окна;
- <Win>+<D> — минимизировать/восстановить все окна;
- <Win>+<T> — выбрать первый элемент в панели задач. Для этого нажмите клавиатурную комбинацию <Win>+<T> еще раз и выберите следующий элемент;
- <Win>+<G> — отобразить гаджеты (gadgets) поверх всех окон;
- <Win>+<P> — отобразить дополнительные опции дисплея;
- <Win>+<X> — запустить приложение Mobility Center;
- <Win>+<N> — запустить приложение с панели задач (где *N* — номер приложения);
- <Win>+<+> — увеличить масштаб;
- <Win>+<-> — уменьшить масштаб;
- <Win>+<Shift>+<Left> — переключиться на левый монитор (если подключено два монитора);
- <Win>+<Shift>+<Right> — переключиться на правый монитор;
- <Win>+<Space> — показать рабочий стол.

Библиотеки

Впервые библиотеки (виртуальные папки) появились еще в Windows Vista Beta 1, но почему-то эту функцию не включили в состав релиза Vista. В Windows 7 эта функция появилась вновь (рис. В.3). Виртуальная папка (библиотека) объединяет несколько обычных папок, возможно, расположенных на разных дисках, в единое целое по общей тематике — музыка, видео и т. д. Вы можете использовать стандартные библиотеки или создавать собственные.

Слайд-шоу на рабочем столе

Наконец-то и в Windows появилась эта функция, а именно, автоматическая смена обоев рабочего стола. Теперь-то вам больше не придется устанавливать стороннюю программу для смены обоев — все, что нужно, Windows 7 уже "умеет" по умолчанию. Все, что вам необходимо для этого сделать — выбрать временно́й интервал, по истечении которого изображение на рабочем столе должно меняться (рис. В.4).

Рис. В.3. Библиотеки

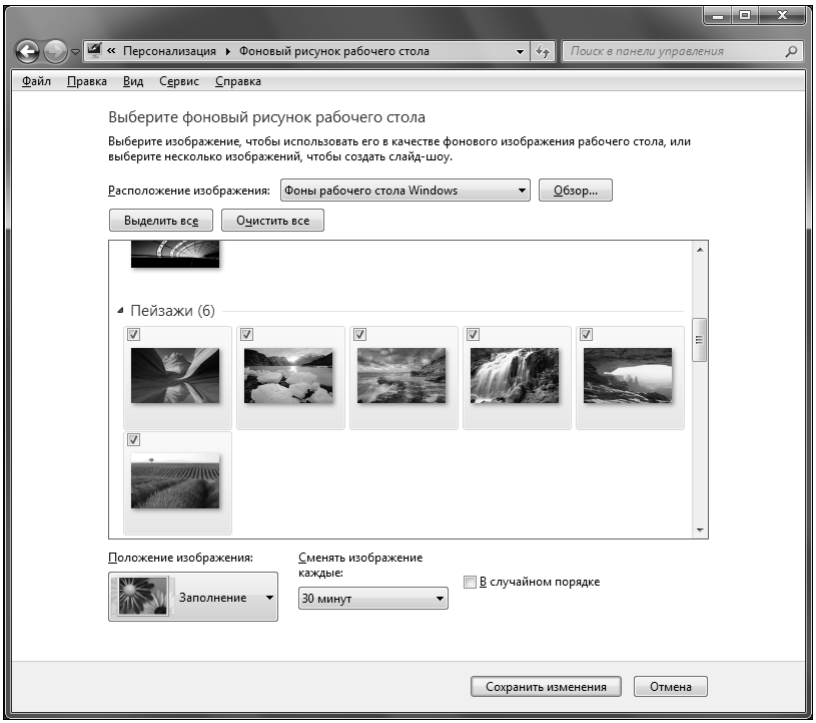


Рис. В.4. Слайд-шоу на рабочем столе

DirectX 11

В Windows 7 входит новейшая версия DirectX — 11[1]. Это означает, что Windows 7 обеспечивает поддержку самых новых видеокарт и новые возможности в играх. Вот только еще не все игры поддерживают DirectX 11. Одиннадцатая версия DirectX построена на базе 10-й версии, но собрана на самом последнем "железе" — многопроцессорных машинах и самых новых видеокартах, что обещает повышение производительности в играх (по сравнению с DirectX 10).

Подключение к большому экрану

Вам приходится подключать компьютер или ноутбук к большому монитору (LCD-телевизору) или проектору? Если да, то Windows 7 существенно облегчает эту процедуру. В Windows 7 появилась очень удобная утилита, позволяющая переключаться между основным монитором и подключенным большим экраном (рис. В.5).

Рис. В.5. Переключение между монитором и большим экраном

Запись ISO-образов

Windows Vista уже обеспечивала встроенные возможности записи файлов на носители CD/DVD, но не "умела" осуществлять запись ISO-образов. В Windows 7 такая возможность появилась (рис. В.6), причем поддерживается запись даже на диски Blu-Ray.

Федеративный поиск

Отныне можно производить поиск не только по локальному компьютеру, но и по удаленным файловым репозиториям (file repositories) в локальной сети или Интернете, например, по Sharepoint-сайтам. Изначально федеративный поиск (federated search) задумывался как инструмент корпоративного поиска,

[1] Дополнительную информацию см. здесь: **http://directx10.org/news/2009-08-29-1**. — *Прим. ред.*

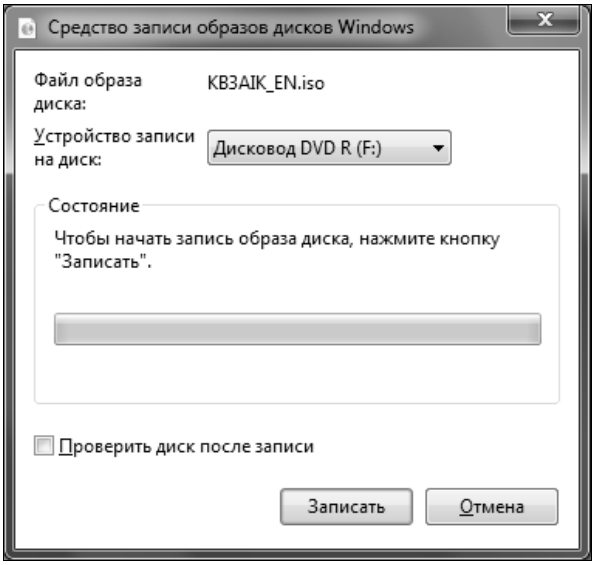


Рис. В.6. Запись ISO-образа

а потом перерос в нечто большее, поэтому он будет полезен не только офисным, но и домашним пользователям.

В этом кратком введении описаны далеко не все новые возможности, появившиеся в Windows 7. Однако с моей личной точки зрения они представляют собой наиболее важные функции Windows 7, которые будут интересны большинству пользователей, в том числе и домашних. Подробно вы сможете ознакомиться со всеми нововведениями по следующим адресам:

- **http://www.thevista.ru/page.php?id=10814**;
- **http://www.thevista.ru/page.php?id=10906**;
- **http://www.winblog.ru/win7/1147766072-kovarsky21010902.html**.

Совместимость реестра

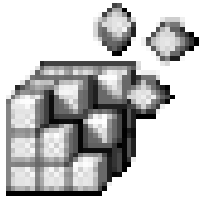
Вы когда-нибудь задавали себе вопрос, почему Windows занимает так много дискового пространства? Не только потому, что разработчики добавили большое количество новых возможностей и поддержку новых устройств. Каждая новая версия Windows должна обеспечивать и обратную совместимость с предыдущими (по мере возможностей). Старые программы должны по-прежнему работать в новой версии Windows. А чтобы старые программы могли нормально работать в новой версии Windows, реестр новой операци-

онной системы должен быть обратно совместим с предыдущей версией Windows. Это означает, что настройки реестра, работающие в Windows XP, будут, скорее всего, работать в Windows Vista и Windows 7[1], но не наоборот. Некоторые из настроек реестра, приведенные в этой книге, будут работать не только в Windows 7, но и в Windows Vista и Windows XP, но не всегда это будет так. Это и понятно: ведь в Windows XP, например, нет интерфейса Aero, поэтому все настройки, относящиеся к Aero, никак не повлияют на поведение Windows XP.

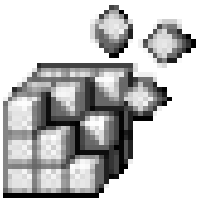
Вот теперь самое время приступить к чтению книги!

[1] Впрочем, это не обязательно будет так, и по ходу изложения я постараюсь обратить внимание читателей на эти моменты. — *Прим. ред.*

ЧАСТЬ I



Для пользователей



ГЛАВА 1

Основы реестра

1.1. Что такое реестр и для чего он используется?

Все версии Windows, начиная с Windows 95, хранят как свои собственные настройки, так и настройки большинства приложений в реестре. Реестр можно рассматривать как конфигурационную базу данных Windows.

Многие пользователи считают, что реестр — далеко не самая важная часть системы, поскольку она им не видна. Однако это не так. Да, на первый взгляд роль реестра по отношению к пользователям пассивна: они не замечают его работы и поэтому не осознают его важности.

Действительно, редактируя документы или бороздя просторы Интернета, пользователь непосредственно не сталкивается с реестром. Зато операционная система с ним работает непрерывно. Если запустить программу мониторинга реестра (в этой книге мы рассмотрим такие программы), то вы увидите, что практически при любом действии — будь то запуск программы или переход в другую папку в окне Проводника (Windows Explorer) — происходит обращение к реестру.

Опытные пользователи, знакомые со структурой реестра, могут очень тонко настраивать свою систему, потому что путем редактирования реестра можно выполнить многие настройки, недоступные через графический интерфейс пользователя (Graphical User Interface, GUI). Например, через Панель управления (Control Panel) вы никак не сможете скрыть те или иные вкладки окна параметров Internet Explorer, не сможете отключить дефрагментацию загрузочных файлов, которая выполняется при каждой загрузке компьютера, тормозя запуск системы, и т. д.

Вы можете спросить: а зачем обычному пользователю вообще нужно знать о реестре? Ведь не зря разработчики Windows "убрали" его подальше от глаз пользователей. Действительно, в Windows можно работать, не обращая внимания на реестр, а при настройке системы довольствоваться Панелью управления (Control Panel). Но в один не очень прекрасный момент Windows может дать сбой из-за повреждения реестра: записи в него некорректной информации или удаления необходимых данных (например, вирусом). Что делать? Можно переустановить Windows и все приложения, потратив на это целый день, а можно просто восстановить реестр, что займет не более получаса (разумеется, если у вас есть под рукой все, что для этого необходимо). Выходит, не только программистам и системным администраторам, но и обычным пользователям нужно знать, как минимум, что такое реестр и как выполнять его резервное копирование и восстановление в случае сбоя. Но если мы знаем, что такое реестр, то можно не останавливаться на полпути, а освоить хотя бы минимальные навыки работы с ним. Мне, например, намного удобнее запустить программу regedit.exe, найти раздел `Run`, отвечающий за автозапуск программ, и удалить из него все ненужное, чем использовать для этой цели какую-то специальную программу, будь то встроенная программа Windows Msconfig.exe или, например, какая-нибудь сторонняя утилита наподобие Starter (**http://codestuff.tripod.com/products_starter.html**). При этом вашей любимой программы от стороннего производителя может просто не оказаться под рукой, так же, как и доступа в Интернет, откуда можно было бы ее скачать. А вот редактор реестра regedit.exe, который мы рассмотрим в *главе 2*, входит в состав операционной системы, предоставляет более широкие возможности, нежели встроенные графические утилиты, и в умелых руках может творить чудеса.

Но редактирование раздела `Run` — это лишь самое тривиальное действие, которое можно выполнить с помощью приложения regedit.exe. Пользователи, по долгу службы занимающиеся администрированием компьютерных систем или желающие стать администраторами, наверняка оценят политики безопасности, о которых мы тоже поговорим в этой книге.

1.2. Краткая история реестра

Как мы помним, первой операционной системой для персональных компьютеров от Microsoft была MS-DOS. В этой операционной системе было два основных конфигурационных файла: config.sys и autoexec.bat. Первый из этих файлов содержал инструкции по загрузке драйверов и резидентных программ. В autoexec.bat указывались команды, которые выполнялись при загрузке MS-DOS, например, устанавливались переменные окружения, а также вызывались оболочки наподобие Norton Commander.

Кроме config.sys и autoexec.bat в MS-DOS не было ни других общесистемных конфигурационных файлов, ни реестра. Каждое приложение хранило свои настройки в отдельном файле, формат и местонахождение которого был известен только самому этому приложению. У одних приложений конфигурационные файлы были текстовыми (их можно было редактировать вручную в любом текстовом редакторе), у других — двоичными (такие файлы можно было редактировать только с помощью самого приложения, которое "знало" формат файла).

MS-DOS не устраивала пользователей своей однозадачностью и отсутствием дружественного пользовательского интерфейса. Многие сторонние разработчики выпускали свои *оболочки* для MS-DOS, облегчающие для пользователя процесс работы с операционной системой. Microsoft тоже не осталась в стороне, разработав собственную оболочку, которая получила название Windows. Первые версии Windows, по мнению многих довольно авторитетных пользователей, вообще не заслуживали внимания. Более или менее удачной стала только третья версия Windows — Windows 3.0. В этой версии для хранения настроек системы использовались INI-файлы, которые, однако, имели массу недостатков. Главным среди них была так называемая "плоская" структура — в INI-файлах не допускалось создание вложенных разделов (в отличие от современного реестра Windows, имеющего иерархическую древовидную структуру). Во-вторых, INI-файлы были текстовыми, что затрудняло хранение в них двоичной информации. С другой стороны, это позволяло редактировать INI-файлы в любом текстовом редакторе, чего нельзя сделать с современным реестром. Нужно отметить также, что INI-файлы имели единый формат для хранения настроек Windows-приложений. Ведь намного проще использовать уже известный формат и готовые API-функции для работы с ним, чем заново "изобретать велосипед", придумывая собственный формат конфигурационных файлов. Некоторые программы и до сих пор используют не реестр, а INI-файлы.

В Windows 3.1 впервые появилось некое подобие реестра, но он использовался только для хранения настроек механизма OLE (Object Linking and Embedding), а все остальные настройки системы по-прежнему хранились в INI-файлах.

С появлением Widows 95 появился и реестр в сегодняшнем понимании этого слова. Конечно, в последующих версиях Windows (Windows 2000/XP/Vista) структура реестра была изменена. Тем не менее, реестр Windows 95 уже был максимально похож на современный, несмотря на то, что многие приложения по-прежнему использовали INI-файлы для хранения своих настроек.

Реестры современных версий Windows (2000, XP, Vista, Windows 7) в значительной степени схожи, но все же у каждого есть свои отличия. Данная книга

ориентирована на новейшие версии Windows — Vista и Windows 7, поэтому об отличиях в Windows 2000 мы говорить не будем. Далее будет указываться, к какой из версий — Windows Vista или Windows 7 — относится сказанное, если же версия не уточняется, то сказанное справедливо для обеих систем.

1.3. Что нужно знать для работы с реестром?

Работа с реестром заключается в редактировании значений параметров реестра, которые чаще всего представлены в виде текстовых строк, а также чисел в десятичной и других системах счисления. Кроме того, вам пригодятся знания идентификаторов безопасности (Security IDs, SIDs), глобальных идентификаторов (Globally Unique IDs, GUIDs) и некоторых других объектов реестра, которые будут рассмотрены в этом разделе.

1.3.1. Системы счисления

Помимо известной нам со школы десятичной системы счисления существует множество других систем счисления. В первую очередь нас будут интересовать те из них, которые получили широкое распространение в компьютерных технологиях: двоичная (binary), использующая только две цифры — `0` и `1`, восьмеричная (octal), использующая цифры от `0` до `7`, и шестнадцатеричная (hex), где применяются цифры от `0` до `9` и буквы латинского алфавита от `A` до `F`. В реестре Windows активно используются только две: десятичная и шестнадцатеричная. С первой системой мы все знакомы, тогда как вторая, вероятно, нуждается в некоторых пояснениях.

В десятичной системе используются десять цифр: от 0 до 9, поэтому она и называется десятичной. Если вы не прогуливали уроки математики, то должны знать, что любое N-значное десятичное число можно представить следующим образом:

$$A = A_1 \times 10^{N-1} + A_2 \times 10^{N-2} + ... + A_N \times 10^0$$

Исходя из этой формулы, можно написать более общее выражение, подходящее для любой системы счисления:

$$A = A_1 \times B^{N-1} + A_2 \times B^{N-2} + ... + A_N \times B^0,$$

где B (от base) — это основание системы счисления. В случае с десятичной системой B = 10.

Например, число 453 можно представить так:

$$453 = 4 \times 10^2 + 5 \times 10^1 + 3 \times 10^0 = 4 \times 100 + 5 \times 10 + 3 \times 1 = 400 + 50 + 3 = 453$$

Теперь поговорим о шестнадцатеричной системе. В этой системе шестнадцать цифр:

`0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F`

Цифры `A`, `B`, `C`, `D`, `E` и `F` соответствуют числам 10, 11, 12, 13, 14 и 15 десятичной системы.

Вернемся к только что рассмотренной формуле, позволяющей представить число в любой системе счисления. Используя ее, вы можете с легкостью преобразовывать шестнадцатеричные числа в десятичные. Рассмотрим, например, преобразование в десятичную систему числа `AF`:

$A \times 16^1 + F \times 16^0 = 10 \times 16 + 15 = 175$

Проверку можно выполнить при помощи обычного калькулятора Windows 7. Запустите приложение Калькулятор (Calculator) — кстати, обратите внимание, что даже это простейшее приложение в Windows 7 оказалось дополненным целым рядом приятных мелочей — а затем из меню **Вид** (View) выберите команду **Программирование** (Programmer). Установите переключатель системы счисления в положение **Hex** (шестнадцатеричная), с помощью кнопок калькулятора или клавиш клавиатуры введите число `AF`, после чего установите переключатель системы в положение **Dec** (десятичная). В результате выполненных действий получаем 175 (рис. 1.1).

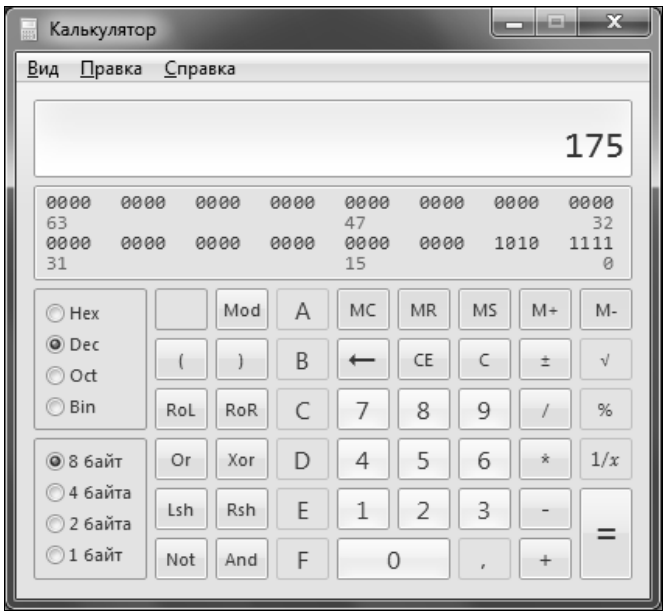


Рис. 1.1. Использование калькулятора для выполнения вычислений в шестнадцатеричной системе

Шестнадцатеричные числа часто записываются так: `0x`*число*. Например, запись `0x77` означает, что число 77 записано в шестнадцатеричной системе. Очевидно, что оно не равно числу 77 в десятичной системе: после преобразования `0x77` в десятичную систему мы получим число 119.

Иногда для указания того, что число записано в шестнадцатеричной системе вместо префикса `0x` добавляют суффикс `h`: `77h`.

Рассмотрим теперь порядок следования байтов в шестнадцатеричном числе. Для числа `0xA1FF` `0xA1` — это старший байт, а `0xFF` — младший байт. Левый байт называется старшим, поскольку вы умножаете его значение на более высокую степень числа 16.

В зависимости от архитектуры микропроцессора, для которой они изначально разрабатывались, одни программы хранят числа в таком порядке следования байтов, когда младший байт сохраняется по младшему адресу, а старший — по старшему (в англоязычной литературе он называется Little-Endian, или формат "остроконечников"), в то время как другие — в порядке Big-Endian, или формат "тупоконечников", иными словами, в порядке "от старшего к младшему". Если используется формат Big-Endian, то первыми сохраняются старшие байты, а затем — младшие. Предположим, что нам нужно сохранить в памяти число `0x00010203`. Если используется порядок "от старшего к младшему", то число будет сохранено в памяти таким образом:

```
0x00 0x01 0x02 0x03
```

Однако процессоры фирмы Intel, например, работают с обратным порядком следования байтов, в котором сначала сохраняются младшие байты, а потом — старшие. Следовательно, наше число `0x00010203` будет сохранено в памяти так:

```
0x03 0x02 0x01 0x00
```

Об этом нужно помнить при работе с программами редактирования реестра, хотя в большинстве случаев они корректно работают как с прямым, так и с обратным порядком следования байтов.

1.3.2. Идентификаторы безопасности

Уникальное имя какого-нибудь объекта называется *идентификатором* (identifier, ID). С помощью идентификаторов можно однозначно выделить объект из множества ему подобных. Например, идентификатором может быть имя пользователя, под которым он регистрируется в системе. Зная имя пользователя, например, `Dennis` (в данном случае строка `Dennis` — идентификатор), вы сможете произвести операции именно с этим пользователем, выделив его из числа других пользователей системы.

В Windows имена пользователей, компьютеров, принимающих участие в работе сети, групп пользователей и других объектов, подчиняются правилам безопасности. Для однозначного определения этих правил используются идентификаторы безопасности — SID (Security Identifier).

Каждый раз, когда создается объект, подчиняющийся правилам безопасности, Windows генерирует SID. Локальные SID (локальные идентификаторы, относящиеся только к данному конкретному компьютеру) генерируются локальными средствами защиты (LSA, Local Security Authority) и хранятся в локальной базе данных.

Кроме локальных средств защиты, есть еще средства защиты домена (Domain Security Authority). DSA генерируют идентификаторы безопасности для домена и сохраняют их не в локальной базе данных, а в Active Directory (службе каталогов) на контроллере домена.

Понятно, что локальные SID уникальны в пределах компьютера (в пределах локальной базы данных), а SID домена уникальны в пределах домена (базы данных Active Directory). Очевидно также, что локальные SID на разных компьютерах сети могут совпадать, так же как в разных доменах могут существовать одинаковые доменные SID.

Локальные SID никогда не повторяются. Предположим, в системе зарегистрирован пользователь `Dennis`. Его учетной записи будет сопоставлен некий SID. Если вы удалите эту учетную запись, а затем создадите новую учетную запись с таким же именем, то SID у этой учетной записи будет другой.

К учетной записи в Windows можно обратиться как по ее имени, так и по SID, поскольку SID однозначно идентифицирует учетную запись. Но обращаться по SID к учетной записи крайне неудобно, поскольку выражения SID достаточно громоздки, например:

```
S-1-5-21-2052111302-436374069-1343024091-1003
```

Очевидно, намного проще запомнить имя `Dennis`, чем приведенный SID, однако формат SID все равно нужно знать. SID всегда начинается с буквы `S`, после которой следует номер версии SID, обычно `1`. Далее, как правило, стоит число `5`, что означает систему NT (NT authority). Все последующие числа (`21-2052111302-436374069-1343024091`) являются идентификатором домена, а последнее число (`1003`) — идентификатором группы, к которой принадлежит данный пользователь.

Помимо персональных учетных записей пользователей в Windows есть постоянные или "короткие SID": они одинаковы на всех компьютерах. Знать эти SID просто необходимо, поскольку они часто встречаются в реестре. В табл 1.1 приведен список некоторых так называемых "широко известных" SID (well-known SIDs). Подробные списки "широко известных" SID и более

детальную информацию о них можно найти здесь: **http://support.microsoft.com/kb/243330**[1].

Таблица 1.1. *Некоторые постоянные SID*

SID	Пользователь или группа
S-1-0	Нет полномочий, "пустые" полномочия, соответствует имени пользователя "nobody" ("никто")
S-1-0-0	Тоже пустые полномочия, нет участника безопасности
S-1-1	Полномочия мира, так называемый "международный администратор"
S-1-1-0	Все. Группа, в которую входят все пользователи, даже анонимные пользователи и гости
S-1-2	Локальные полномочия, так называемый "локальный администратор"
S-1-3	Администратор-создатель (Creator)
S-1-3-0	Создатель/владелец (Creator/Owner)
S-1-3-1	Группа создателя
S-1-3-2, S-1-3-3	Создатель-владелец сервер и группа-создатель сервер соответственно. Используются в серверных версиях ОС Windows
S-1-3-4	Права владельца. Используется для управления правами владельца над объектом безопасности
S-1-4	Неуникальные полномочия
S-1-5	Администратор NT
S-1-5-1	Удаленный доступ. Группа, в которую входят все пользователи, вошедшие в систему с использованием удаленного доступа
S-1-5-2	Сеть. К этой группе относятся все пользователи, вошедшие в систему с использованием сетевого подключения
S-1-5-3	Партия. Группа, в которую входят все пользователи, вошедшие в систему с использованием средства пакетной очереди
S-1-5-4	Интерактивный. К этой группе относятся пользователи, вошедшие в систему с использованием интерактивного входа
S-1-5-5-*X*-*Z*	Сеанс входа в систему. Значения *X* и *Z* для этих идентификаторов SID меняются в каждом сеансе

[1] См. также следующие адреса, по которым можно найти подробную информацию для углубленного изучения:
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**. — *Прим. ред.*

Таблица 1.1 *(окончание)*

SID	Пользователь или группа
S-1-5-6	Служба (сервис)
S-1-5-7	Anonymous (анонимный пользователь)

1.3.3. Глобальные идентификаторы

Полное название глобальных идентификаторов — глобальные уникальные идентификаторы (Global Unique Identifier, GUID). GUID — это число, однозначно идентифицирующее какой-либо объект: компьютер, аппаратное устройство, программный компонент. GUID жестко привязывается к объекту: имя объекта можно изменить, а GUID — нет. GUID очень похожи на SID, но выполняют несколько иную роль: GUID никак не связаны с безопасностью и правами доступа.

Формат GUID, в отличие от формата SID, одинаков для всех объектов. GUID — это 16-байтное шестнадцатеричное число, разбитое на группы, состоящие из 8, 4, 4, 4 и 12 шестнадцатеричных цифр, соответственно. Группы в составе GUID отделяются друг от друга дефисами, а весь GUID заключен в фигурные скобки, например:

```
{645FF040-5081-101B-9F08-00AA002F954E}
```

Для создания GUID используется утилита guidgen.exe. Microsoft гарантирует, что сгенерированный GUID будет уникальным в пределах системы. Прочитать о том, как использовать guidgen.exe можно по следующему адресу:

http://msdn2.microsoft.com/en-us/library/ms241442(VS.80).aspx

1.3.4. Использование битовых масок

Как мы знаем, при использовании формата ASCII для представления одного символа используется один байт. Таким образом, слово "байт" занимает 4 байта (4 символа). В одном байте восемь битов, каждый из которых может принимать значение `0` или `1`.

Пойдем дальше. Возьмем любой символ, например, 1. В ASCII-таблице этому символу соответствует код 49. Переведем 49 в двоичную систему и получим вот такое число:

```
0011 0001
```

Зачем нам это все нужно знать? Дело в том, что некоторые простые настройки в реестре Windows хранятся в виде однобайтных значений.

Рассмотрим следующее число:

```
0000 0111
```

Первые четыре бита не используются, остальные, очевидно, используются для каких-то настроек: `0` — функция выключена, а `1` — включена. Хранить настройки в виде одного байта очень экономично: если нам нужно хранить четыре параметра, которые могут принимать только значения `0` или `1`, то намного проще хранить их в виде одного байта. Такое решение позволяет экономить до 7 байтов (при условии, что используются все восемь параметров).

Но есть небольшая проблема. Наше число `0111` будет просто отображаться как число 7. Как же установить определенный бит нашего байта с настройками? Можно, конечно, преобразовать число 7 в двоичную систему, получить число `0000 0111`, затем установить какой-то бит этого числа, а новое число (пусть это будет `1000 0111`) преобразовать обратно в десятичную систему (получится 135) и записать его в реестр. Но, согласитесь, это не очень удобно.

Намного проще использовать битовые маски, позволяющие выделить из байта бит, соответствующий маске. Разряды двоичного числа нумеруются *справа налево* (табл. 1.2).

Таблица 1.2. *Порядок нумерации разрядов*

Номер бита (с 0 до 7, справа налево)	7	6	5	4	3	2	1	0
Значение (0 или 1)	1	0	0	0	0	1	1	1

В верхней строке табл. 1.2 изображены номера разрядов (обратите внимание на порядок нумерации — от 0 до 7, справа налево), а во второй строке — наше число (135) в двоичном формате.

Битовая маска определяет, какой бит нужно установить (1) или, наоборот, сбросить. В этой книге вы можете встретить инструкцию, которая требует с помощью битовой маски `0x80` установить значение бита в `0`. Битовая маска `0x80` соответствует седьмому биту. Если мы сбросим этот бит, то наше число превратится обратно в число 7 (`0000 0111`).

В табл. 1.3 приведены битовые маски для байта.

Таблица 1.3. *Битовые маски*

Разряд	Битовая маска
7	0x80
6	0x40
5	0x20

Таблица 1.3 *(окончание)*

Разряд	Битовая маска
4	0x10
3	0x08
2	0x04
1	0x02
0	0x01

1.3.5. Кодировки и реестр

В знакогенераторы первых персональных компьютеров была загружена кодировка ASCII (American Standard Code for Information Interchange). Как уже говорилось чуть ранее, в этой кодировке один символ занимал один байт (8 битов), следовательно, максимально возможное количество символов для этой кодировки было ограничено числом 256.

Кодировка ASCII содержала специальные (управляющие) символы, цифры, символы пунктуации, символы латиницы, псевдографические символы, а также специальные символы некоторых европейских языков. Понятно, что ограничение в 256 знакомест не позволяло использовать символы всех европейских языков. Отечественные программисты разрабатывали русификаторы, загружающие в знакогенератор символы русского алфавита, перезаписывая уже существующие там символы.

Международная организация по стандартизации (ISO) разработала кодировку ISO Latin-1, которая несколько расширила ASCII, убрав из нее неиспользуемые символы и добавив некоторые национальные символы. Microsoft переработала Latin-1 и назвала ее ANSI. Но ANSI (American National Standards Institute) по-прежнему была 8-битной кодировкой, поэтому ограничение в 256 символов не было снято.

Тогда компании Apple, IBM и Microsoft создали некоммерческий консорциум, целью которого было создание универсальной кодировки, которая смогла бы содержать символы всех языков мира. Такой кодировкой стала Unicode, которая поддерживает 65 536 уникальных символов (один символ в этой кодировке занимает 16 битов). Такого количества знакомест хватило не только для представления символов всех используемых в мире алфавитов, но и для различных математических, географических символов, символов забытых языков (санскрит) и др.

Unicode является "родной" кодировкой как для Windows XP/Vista, так и для Windows 7. Тем не менее, Windows по-прежнему поддерживает кодировку

ANSI с целью обеспечения обратной совместимости с предыдущими версиями Windows. Имена объектов, файлов, каталогов, а также вся внутренняя информация Windows XP/Vista и Windows 7 представлена в Unicode.

1.4. Структура реестра

Знакомиться со структурой реестра лучше всего с помощью редактора реестра. Нажмите кнопку **Пуск** (Start), введите в поле поиска в нижней части этого меню команду `regedit` и нажмите клавишу <Enter>. Сначала на экране появится окно **Контроль учетных записей пользователей** (User Account Control, UAC), показанное на рис. 1.2. Функция UAC, впервые появившаяся в Windows Vista и присутствующая в Windows 7, запросит разрешение на запуск редактора реестра, поскольку это критически важное приложение, которое может нанести вред системе. Если вы дадите согласие, нажав кнопку **Да** (OK), то будет запущен редактор regedit.exe (рис. 1.3).

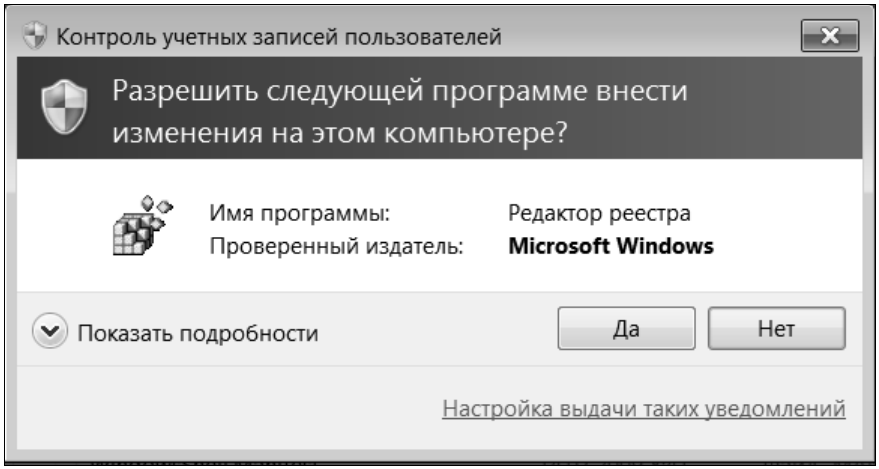


Рис. 1.2. Окно **Контроль учетных записей пользователей** (User Account Control) выводит запрос разрешения на запуск редактора реестра

Примечание

Функция UAC в Windows Vista вызывала сильное раздражение пользователей своей "навязчивостью", поэтому многие пользователи предпочитали ее просто блокировать. В Windows 7 появилась возможность регулирования уровней UAC, но, тем не менее, многие пользователи все равно предпочитают ее отключать.

Левая панель редактора реестра называется панелью разделов (ключей). На этой панели отображается иерархия разделов (которые также называются ключами) реестра. Правая панель — это панель параметров (она также назы-

вается панелью значений). В каждом разделе есть как минимум один параметр.

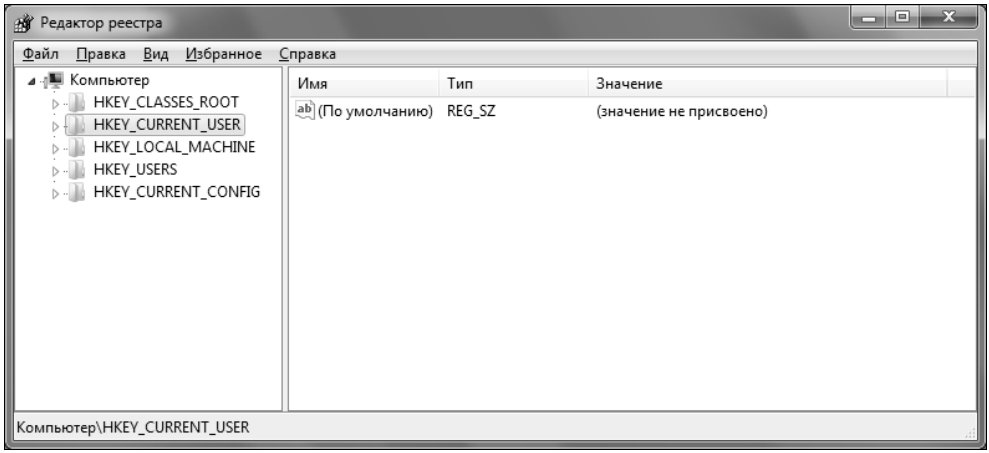


Рис. 1.3. Редактор реестра (regedit.exe)

Реестр имеет пять корневых разделов: `HKEY_CLASSES_ROOT`, `HKEY_CURRENT_USER`, `HKEY_LOCAL_MACHINE`, `HKEY_USERS`, `HKEY_CURRENT_CONFIG`. Названия корневых разделов (ключей) слишком длинные, поэтому для большего удобства приняты следующие сокращения:

- `HKEY_CLASSES_ROOT` — `HKCR`;
- `HKEY_CURRENT_USER` — `HKCU`;
- `HKEY_LOCAL_MACHINE` — `HKLM`;
- `HKEY_USERS` — `HKU`;
- `HKEY_CURRENT_CONFIG` — `HKCC`.

1.4.1. Разделы

Каждый раздел (ключ, в англоязычной литературе — key) может содержать, как уже отмечалось, несколько параметров (values). Кроме параметров раздел может содержать вложенные подразделы. Именно поэтому иерархическая структура реестра напоминает иерархическую структуру файловой системы. Ключи реестра аналогичны папкам, а параметры — файлам.

Примечание

В различной литературе ключи реестра называются как разделами, так и ключами. Такое разделение произошло потому, что в англоязычной литературе (да и в англоязычной версии редактора реестра) раздел называется key (что в пе-

реводе означает ключ), а в документации по реестру на русском языке (и в самом русскоязычном редакторе реестра) раздел называется так, как и должен — разделом. Отсюда и происходит некоторая путаница. Чтобы вы привыкли к обоим названиям, в книге я буду использовать оба эти названия с одинаковой частотой.

Длина имени ключа ограничена 16 383 Unicode-символами. Подробно об ограничении длины имени параметра можно прочитать по адресу: **http://support.microsoft.com/kb/256986**.

Ограничения, думаю, понятны: один символ в Unicode занимает в два раза больше памяти (16 битов), чем в ANSI (8 битов), поэтому длина имени ключа при использовании символов Unicode будет в два раза меньше.

Имя ключа может содержать любые символы, за исключением следующих:

```
? * \
```

Нельзя также создавать ключ с именем, которое начинается с точки, поскольку такие имена Windows резервирует для внутреннего использования.

Ключи могут быть связаны друг с другом. Связанные ключи похожи на ярлыки рабочего стола, которые используются для быстрого доступа к программе или документу. Аналогично, один ключ реестра может представлять собой ссылку на другой. Откройте раздел `HKLM\SYSTEM\CurrentControlSet\Hadrware Profiles`. В нем будет несколько подразделов `000`, `001` и т. д., которые содержат настройки профилей оборудования. Кроме того, здесь же присутствует раздел `Current`, представляющий собой ссылку на один из разделов в зависимости от выбранного при загрузке системы профиля оборудования. В свою очередь весь корневой раздел `HKCC` является ссылкой на раздел `HKLM\SYSTEM\CurrentControlSet\Hadrware Profiles\Current`. Обозначение ключей-ссылок ничем не отличается от обозначения других ключей. Главный признак того, что ключ является ссылкой, — появление в разных местах реестра одинаковых ключей с одними и теми же параметрами.

1.4.2. Параметры

Как уже отмечалось выше, в каждом разделе должен быть хотя бы один параметр. У каждого параметра есть три атрибута:

- *имя*, уникальное в пределах раздела, т. е. в одном и том же разделе не может быть двух параметров с одинаковыми именами. Имя раздела может содержать 16 383 Unicode-символов. Как и в случае с именем раздела, имя параметра не может содержать символы `\`, `*` и `?`. Имена параметров, которые начинаются с точки, зарезервированы для нужд Windows;
- *тип*, определяющий тип данных, которые может принимать параметр. Список допустимых типов параметров представлен в табл. 1.4;

- *значение* — это данные, которые содержит параметр. Если параметр не содержит значения, то считается, что он содержит пустое значение — null. Длина значения зависит от выбранного типа данных.

Все эти атрибуты для каждого параметра отображаются на панели параметров (см. рис. 1.2). В каждом разделе есть параметр по умолчанию — "(По умолчанию)" (в англоязычной версии Windows — "(Default)"). Список наиболее употребительных типов данных реестра приведен в табл. 1.4.

Таблица 1.4. *Типы параметров*

Тип	Кодовый номер	Описание
REG_BINARY	3	Двоичные данные. Параметр с таким типом может содержать все, что угодно. Редактирование таких данных (в том числе и ввод) выполняется в шестнадцатеричном виде
REG_DWORD	4	Целые числа. Длина этого типа — 32 бита (два слова). Напомню, что одно слово (word) равно 2 байтам и занимает 16 битов. Данный тип может использоваться для хранения чисел в диапазоне от –2 147 483 648 до +2 147 483 647. Данные этого типа можно просматривать как в десятичном, так и в шестнадцатеричном виде
REG_DWORD_BIG_ENDIAN	5	Целые значения, записанные в прямом порядке байтов. На Intel-совместимых компьютерах этот тип параметра присутствует редко
REG_DWORD_LITTLE_ENDIAN	4	Целые значения, записанные в обратном порядке байтов. На Intel-совместимых компьютерах этот тип аналогичен REG_DWORD
REG_EXPAND_SZ	2	Строка переменной длины, допускающая расширение. Такие строки представляют собой текст, который может содержать переменные, заменяемые конкретными значениями при вызове со стороны приложения
REG_FULL_RESOURCE_DESCRIPTOR	9	Дескриптор ресурса (устройства или его драйвера). Обычно данный тип используется системой Plug and Play. Редактор реестра не позволяет создавать параметры этого типа, допуская только их просмотр (см. HKLM\HARDWARE\DESCRIPTION)

Таблица 1.4 *(окончание)*

Тип	Кодовый номер	Описание
REG_LINK	6	Ссылка. Как и в предыдущем случае, редактор реестра не позволяет создавать параметры этого типа
REG_MULTI_SZ	7	Многострочное значение. Редактор реестра позволяет вам редактировать такие значения. Каждая строка в списке разделяется символом null (0x00), а весь список заканчивается двумя пустыми символами (0x00 0x00)
REG_NONE	0	Параметр без типа
REG_QWORD	11	Целое значение длиной 64 бита (4 слова). Тип аналогичен REG_DWORD, только длиннее его в два раза. Данный тип поддерживает 64-разрядные версии Windows XP/Vista/7
REG_QWORD_BIG_ENDIAN, REG_QWORD_LITTLE_ENDIAN	—	То же, что REG_DWORD_BIG_ENDIAN и REG_DWORD_LITTLE_ENDIAN, но для типа REG_QWORD
REG_RESOURCE_LIST	8	Список параметров типа REG_FULL_RESOURCE_DESCRIPTION. Редактор реестра не позволяет создавать параметры этого типа
REG_RESOURCE_REQUIREMENTS_LIST	10	Задает список ресурсов, которые используются устройством. Как и в предыдущем случае, редактор реестра не позволяет создавать параметры этого типа
REG_SZ	1	Строка постоянной длины. Наиболее часто используемый тип параметра реестра. Этот тип данных чаще всего присваивается значениям, которые представляют собой описания компонентов. Строка заканчивается пустым символом (0x00)

Если вы внимательно прочли эту таблицу, то уже поняли, что в основном вам придется работать с параметрами типов REG_SZ, REG_MULTI_SZ, REG_DWORD и REG_BINARY. Остальные типы данных используются реже, и не все они допускают редактирование с помощью редактора реестра.

В таблице есть столбец "кодовый номер". Как уже говорилось чуть ранее в этой главе, реестр представляет собой базу данных в двоичном формате, и

перечисленные в этой таблице "кодовые номера" как раз и являются внутренним представлением типов данных реестра, какой они имеют в двоичных файлов кустов или ульев, о которых речь пойдет далее в этой главе. Эти номера следует знать, если вы захотите "поковырять" реестр не с помощью предназначенных для этого приложений наподобие редактора реестра Regedit.exe, а, например, с помощью шестнадцатеричного редактора наподобие HIEW[1].

1.5. Корневые разделы реестра

Рассмотрим корневые ключи реестра, о которых мы только что упомянули в *разделе 1.4*:

- `HKEY_CLASSES_ROOT`;
- `HKEY_CURRENT_USER`;
- `HKEY_LOCAL_MACHINE`;
- `HKEY_USERS`;
- `HKEY_CURRENT_CONFIG`.

Из всех корневых разделов три фактически представляют собой ссылки на другие разделы реестра:

- `HKEY_CURRENT_USER` — ссылка на `HKU\<SID>`;
- `HKEY_CURRENT_CONFIG` — ссылка на `HKLM\SYSTEM\CurrentControlSet\Hardware Profiles\Current`;
- `HKEY_CLASSES_ROOT` — ссылка на `HKLM\SOFTWARE\CLASSES`.

---

[1] Вообще говоря, обычному пользователю вряд ли придет в голову "ковырять" реестр шестнадцатеричными редакторами, и он может даже задаться вопросом — а зачем вообще это нужно делать? Да и, кроме того, эти кодовые номера (иногда их еще называют API codes) в тексте книги никогда больше не встретятся. Но, раз уж автор затронул эту тему, скажу, что исследовать структуру реестра на таком низком уровне необходимо разработчикам ПО (например, если они решили написать собственный редактор реестра, превосходящий по своим возможностям встроенное приложение Regedit.exe), а также исследователям в области компьютерной безопасности и криминалистики (computer forensics). В общем-то, обе темы выходят далеко за рамки этой книги, и заинтересованным читателям, которые хотят изучить данный вопрос углубленно, можно порекомендовать следующие источники:
http://www.beginningtoseethelight.org/ntsecurity/index.php,
http://blogs.msdn.com/oldnewthing/archive/2009/02/05/9397154.aspx,
http://www.mdgx.com/reg.htm, **http://tinyurl.com/yczo2bs** и
http://www.sentinelchicken.com/research/.
На русском языке никаких источников по данной теме, заслуживающих внимания, мне обнаружить не удалось. — *Прим. ред.*

До сих пор мы говорили только о пяти корневых ключах реестра. 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.

1.5.1. *HKEY_CLASSES_ROOT* — корневые классы

Данный раздел содержит информацию об ассоциациях файлов и о регистрации классов для объектов COM (Component Object Model). В Windows можно каждому типу файла (*.doc, *.zip, *.txt) сопоставить программу, которая будет запускаться для обработки файла этого типа. Сведения об этих ассоциациях как раз и хранятся в данном ключе реестра.

Этот раздел реестра является наиболее интересным — он позволяет изменить много правил поведения системы. Не зря он является самым большим разделом реестра, хотя все зависит от конкретной системы: например, ключ HKLM может быть самым "маленьким", но потом очень быстро вырасти в размерах (по мере того, как в систему будут добавляться новые компоненты, устанавливаться дополнительные приложения и обновления Windows).

В ранних версиях Windows (до Windows 2000) раздел HKEY_CLASSES_ROOT был просто ссылкой на раздел HKLM\SOFTWARE\CLASSES, но с появлением Windows 2000 он стал намного сложнее.

Для создания HKEY_CLASSES_ROOT Windows объединяет два раздела:

- HKLM\SOFTWARE\Classes — содержит ассоциации типов файлов и регистрацию классов по умолчанию;
- HKCU\SOFTWARE\Classes — это ссылка на ключ HKU\<*SID*>_Classes (рис. 1.4), содержащий ассоциации типов файлов и регистрацию классов для пользователя, который в данный момент работает с системой.

Таким образом, в разделе HKCR содержится информация о глобальных ассоциациях типов файлов и регистрации COM-объектов (данная настройка одинакова для всех пользователей) и информация о пользовательских ассоциациях типов файлов и регистрации COM-объектов (разная для каждого пользователя, зарегистрированного в системе). Что это дает пользователю? Сплошные преимущества:

- пользователь может установить программу, которая лицензирована только для него, а не для всех пользователей компьютера. Типы файлов, с кото-

рыми работает эта программа, будут ассоциированы с ней только для текущего пользователя. Остальные пользователи при этом могут даже не подозревать, что в системе установлена программа для обработки файлов данного типа;

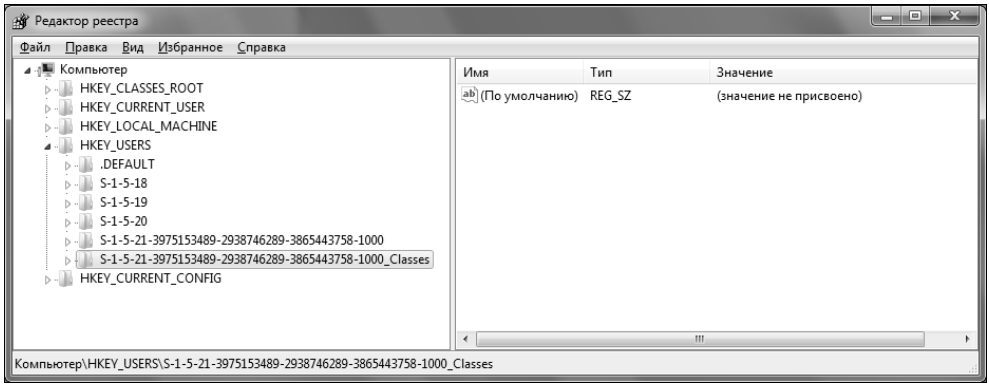


Рис. 1.4. Раздел `HKU\<SID>_Classes`

- каждый пользователь может использовать свою программу для обработки файлов одного и того же типа. Например, мне нравится видеопроигрыватель BSPlayer, который я ассоциировал с типами файлов *.avi и *.mpg, а кто-то любит просматривать фильмы с помощью стандартного проигрывателя Windows Media Player;
- пользователь может экспортировать свои ассоциации файлов в REG-файл и присоединить его к реестру другой системы (на другом компьютере). Ему не придется экспортировать весь глобальный список ассоциаций (а он огромен!);
- можно ограничить доступ к `HKLM\SOFTWARE\Classes`: пользователи смогут редактировать собственные ассоциации файлов, но не смогут редактировать общесистемные, что позволит повысить безопасность системы в целом.

Если вы создадите новый ключ в `HKCR`, то Windows создаст его в разделе `HKLM\SOFTWARE\Classes`. Иными словами, будет создана общесистемная ассоциация файла. Если вы хотите создать пользовательскую ассоциацию, то ее нужно явно создавать в разделе `HKCU\SOFTWARE\Classes`.

1.5.2. *HKEY_CURRENT_USER* — параметры текущего пользователя

В данном разделе реестра хранятся настройки текущего пользователя. По сути, этот раздел, как уже отмечалось, является ссылкой на раздел `HKU\<SID>` (SID — это ключ, который именуется по SID пользователя).

Настройки рабочего стола, параметры приложений пользователя, переменные окружения, сетевые соединения, установленные принтеры — вот краткий перечень настроек, хранящихся в этом разделе.

Некоторые подключи ключа `HKCU` представлены в табл. 1.5.

Таблица 1.5. *Некоторые подключи ключа HKCU*

Подключ	Описание
`AppEvents`	Сопоставляет звуки системным событиям. Параметры этого раздела обычно изменяются с помощью апплета **Звук** (Sound) Панели управления. Однако их можно изменять и вручную (с помощью редактора реестра)
`Console`	Содержит настройки консольной подсистемы (она используется для запуска приложений, не имеющих графического интерфейса, и для запуска старых DOS-приложений)
`Control Panel`	Содержит огромное количество настроек, которые можно изменить с помощью панели управления: параметры рабочего стола, региональные настройки, параметры клавиатуры и т. д. Однако в этом же разделе можно найти и такие параметры, которые нельзя изменить с помощью Панели управления. Для их изменения нужно использовать только редактор реестра
`Environment`	Содержит переменные окружения (Environment variables)
`EUDC`	Определенные пользователем символы (End-User-Defined Characters, EUDC)
`Identities`	В этом ключе хранятся параметры учетных записей Outlook Express, что позволяет разным пользователям использовать один и тот же почтовый клиент
`Keyboard Layout`	Содержит информацию о раскладках клавиатуры
`Network`	Используется для хранения информации о сетевых дисках. Каждый подраздел содержит настройки сетевого диска, который автоматически подключается при запуске системы. Имена подразделов совпадают с именами сетевых дисков
`Printers`	Используется для хранения пользовательских настроек принтеров
`Software`	Содержит пользовательские параметры приложений. Большая часть пользовательских настроек Windows хранится в этом разделе, вернее, в его подразделе `HKCU\Software\Microsoft\Windows\CurrentVersion`

Таблица 1.5 *(окончание)*

Подключ	Описание
System	Некоторые системные настройки и политики
Volatile Environment	Содержит переменные окружения, определенные при входе пользователя

1.5.3. *HKEY_LOCAL_MACHINE* — глобальные параметры

Корневой раздел HKLM содержит общесистемные параметры, влияющие на работу всех пользователей и на работу системы в целом. В этом разделе можно найти самые разнообразные параметры: от параметров драйверов до глобальных (или общих) параметров Windows. В табл. 1.6 приведены основные подразделы HKLM.

Таблица 1.6. *Подразделы HKLM*

Подраздел	Описание
BCD00000000	База данных загрузочной информации. Помимо всего прочего хранит описание загрузочного меню, отображаемого при запуске компьютера. В каталоге *%systemroot%*\System32\config существует шаблон данной ветви реестра — файл BCD-Template. Данный ключ впервые появился в Windows Vista, в XP и более ранних версиях его нет. Поскольку редактирование этого раздела требуется очень и очень редко, подробно мы его описывать не будем. Если кому-то интересно, дополнительную информацию можете найти по адресу: **http://www.geoffchappell.com/viewer.htm?doc=notes/windows/boot/bcd/objects.htm**
COMPONENTS	Содержит список всех компонентов, из которых состоит ваша операционная система. Данный ключ также впервые появился в Windows Vista, в XP и более ранних версиях его нет. В Windows 7 данный подраздел не отображается редактором реестра.
HARDWARE	Используется для хранения информации об аппаратных средствах компьютера
SAM	Менеджер безопасности учетных записей (Security Account Manager). Содержит локальную базу данных безопасности Windows. Данный раздел является ссылкой на HKLM\SECURITY\SAM. Этот раздел не может просмотреть даже администратор — это не позволяет сделать список управления доступом (ACL). ACL мы подробно рассмотрим далее в этой книге
SECURITY	Представляет собой еще одну часть базы менеджера безопасности SAM

Таблица 1.6 *(окончание)*

Подраздел	Описание
SOFTWARE	Содержит общесистемные параметры приложений, действительные для всех пользователей. Этот раздел организован следующим образом: все его подразделы первого уровня (относительно HKLM\SOFTWARE) — это названия производителей программного обеспечения, которое установлено на компьютере. Подразделы второго уровня — это названия программ. Подразделы третьего уровня — версии программ. Таким образом, иерархия имеет следующий вид: HKLM\SOFTWARE*Производитель**Программа**Версия*
SYSTEM	Используется для хранения управляющих наборов параметров (ControlSet). Подраздел CurrentControlSet указывает на текущий набор параметров. Содержимое данной ветви реестра определяет настройки аппаратных профилей компьютера, служб и драйверов и другую важную конфигурацию самой операционной системы

1.5.4. *HKEY_USERS* — пользовательские параметры

Раздел HKU содержит пользовательские настройки. В этом разделе вы найдете, как минимум, три подраздела:

- .DEFAULT — параметры по умолчанию. Windows их использует перед тем, как пользователь войдет в систему, например, для того, чтобы отобразить само окно, приглашающее к регистрации. Фактически этот профиль используется учетной записью LocalSystem и представляет собой ссылку на ключ HKEY_USERS\S-1-5-18. (S-1-5-18 — это как раз и есть SID учетной записи LocalSystem, см. табл. 1.1). Не нужно путать эти настройки с настройками по умолчанию, которые применяются перед первым входом в систему нового пользователя. На самом деле профиль для нового пользователя, который создается при его первой регистрации, генерируется на основе информации, которая хранится в файле C:\Documents and Settings\Default User\ntuser.dat (Windows XP) или C:\Users\Default\NTUSER.DAT (Windows Vista и Windows 7);
- <SID> — параметры безопасности пользователя с определенным SID. Раздел HKCU ссылается на этот раздел, о чем уже говорилось ранее в этой главе;
- <*SID*>_Classes — содержит ассоциации файлов пользователя и информацию о регистрации пользовательских COM-объектов. Как уже отмечалось, Windows объединяет этот раздел и HKLM\SOFTWARE\Classes в один большой корневой раздел HKCR.

Данный раздел содержит также настройки для постоянных SID (см. табл. 1.1): S-1-5-18, S-1-5-19, S-1-5-20.

1.5.5. *HKEY_CURRENT_CONFIG*

Раздел HKCC является ссылкой на раздел HKLM\SYSTEM\CurrentControlSet\Hardware Profiles\Current, который содержит параметры текущего профиля оборудования.

1.6. Кусты

Откройте Regedit.exe и посмотрите на структуру реестра. Вы увидите 5 корневых разделов и их подразделы. Это так называемая логическая структура реестра: так реестр представлен пользователю и программам. Но на самом деле все намного сложнее, и если вы думаете, что реестр хранится на диске в одном большом файле, то вы ошибаетесь.

На диске реестр организован в виде *кустов* (еще одно название — улей (hive)) — двоичных файлов специального формата. Для каждого куста Windows создает вспомогательные файлы, которые используются для восстановления основного файла куста, если при загрузке системы что-то пошло не так. Другими словами, вспомогательные файлы являются резервными копиями файла куста.

Кусты есть только для разделов HKLM и HKU. Остальные корневые разделы, как мы знаем, являются ссылками на подразделы этих двух разделов.

Файлы кустов для разделов HKLM расположены в каталоге *%SystemRoot%*\System32\config; обычно это — каталог C:\Windows\System32\config. Файлы кустов для HKU находятся в каталогах профилей пользователей (C:\Users\<*имя пользователя*>).

Вспомогательные файлы кустов имеют следующие расширения:

- .log — журнал изменений куста;
- .sav — исходная копия куста с момента установки Windows (обратите внимание на дату создания этого файла: вы вспомните, когда вы установили Windows)[1].

[1] Так было в Windows Vista. В Windows 7 вспомогательные файлы имеют расширения .log, .log1 и .log2. При этом файл с расширением .log — это журнал изменений, внесенных в улей, а файлы с расширениями .log и .log2 создаются при установке в Windows 7 и остаются неизменными в течение всего времени работы. — *Прим. ред.*

1.6.1. Кусты *HKLM*

Загляните в каталог %SystemRoot%\System32\config. В этом каталоге находятся файлы кустов и их вспомогательные файлы для раздела HKLM. В табл. 1.7 перечислены эти файлы.

Таблица 1.7. *Файлы кустов для HKLM*

Файл куста	Описание
BCD	Куст расположен в каталоге *%systemdrive%*\BCD. Содержит описание загрузочного меню Windows. В каталоге *%systemroot%*\System32\config находится шаблон этого куста — файл BCD-Template
COMPONENTS	Данный файл куста отсутствует в Windows XP и более ранних версиях Windows. Он есть только в Windows Vista и Windows 7. Файл куста хранится в каталоге *%systemroot%*\System32\config. Как уже было отмечено, куст COMPONENTS не отображается в редакторе реестра Windows 7, но файл куста присутствует на жестком диске
SAM	Содержит базу данных SAM, соответствует ключу реестра HLKM\SAM. Данный куст расположен в каталоге *%systemroot%*\System32\config
SECURITY	Соответствует ключу реестра HLKM\SECURITY. Данный куст находится в каталоге *%systemroot%*\ System32\config
SOFTWARE	Соответствует ключу реестра HLKM\SOFTWARE. Находится в каталоге *%systemroot%*\System32\config
SYSTEM	Соответствует ключу реестра HLKM\SYSTEM. Находится в каталоге *%systemroot%*\System32\config
DEFAULT	Хранится в каталоге *%systemroot%*\System32\config. Содержит настройки по умолчанию, которые будут применены для запуска процессов, стартующих от имени учетной записи LocalSystem, прежде, чем в системе зарегистрируется пользователь. Дополнительную информацию можно получить по адресу: **http://blogs.msdn.com/oldnewthing/archive/2007/03/02/1786493.aspx**

Наверное, вы заметили, что на диске нет файла куста HARDWARE. Его и не должно быть: раздел HKLM\HARDWARE создается каждый раз при запуске Windows, т. е. является динамическим. При выключении компьютера файл куста данного раздела реестра не сохраняется на диск. Без этого не смогла бы работать система Plug and Play.

Windows XP создает еще одну копию реестра в каталоге *%Systemroot%*\repair. Windows Vista и Windows 7 помещают копию реестра в каталог *%Systemroot%*\System32\config\RegBack. В данных каталогах сохраняется только системная часть реестра (общесистемные разделы). Резервную копию пользовательской части можно сделать с помощью специальных программ, которые будут рассмотрены в других главах этой книги.

Примечание

В каталоге *%Systemroot%*\System32\config\RegBack создается две копии реестра. Одна создается спустя 5 минут после входа пользователя в систему, а вторая — после последнего удачного входа в систему (файлы с расширением *.old). Напомню еще раз, что данный каталог существует только в Windows Vista и Windows 7, но не существует в более ранних версиях Windows[1].

Что еще можно найти в каталоге *%Systemroot%*\System32\config? Прежде всего это файлы журналов системных событий — они имеют расширение *.evt. Файл userdiff используется для преобразования профилей пользователей из более ранних версий Windows, например, Windows 2000 или Windows NT.

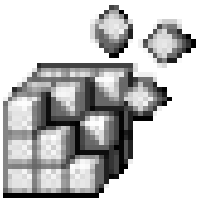
1.6.2. Кусты *HKU*

Каждый подраздел раздела HKU является кустом. Файл куста раздела HKU\.DEFAULT можно найти в каталоге *%Systemroot%*\System32\config (он так и называется — DEFAULT).

Пользовательские файлы кустов разделов HKU\<*SID*> и HKU\<*SID*>_Classes находятся в каталогах *%Userprofile%* и %Userprofile%\Local Settings\Application Data\Microsoft\Windows\ соответственно. Файл куста для HKU\<*SID*> называется Ntuser.dat, а файл куста для HKU\<*SID*>_Classes — UsrClass.dat.

В каталоге профиля пользователя кроме файлов Ntuser.dat и Ntuser.dat.log иногда имеются файлы ntuser.pol и ntuser.ini, определяющие настройки групповой политики для данного пользователя.

[1] В Windows 7 файлов с расширением .old нет, а есть файлы с расширениями .log1 и .log2. — *Прим. ред.*



ГЛАВА 2

Редактор реестра Registry editor

2.1. Знакомство с редактором реестра

В данной главе мы поговорим о программе Редактор реестра (Registry editor, Regedit.exe), позволяющей просматривать и редактировать реестр Windows. Даже если вы и не подозреваете об этом, вы изменяете реестр Windows каждый день: когда модифицируете параметры системы с помощью Панели управления (Control Panel), изменяете настройки программ или просто открываете документы (список последних использованных вами документов также заносится в реестр). Но все эти изменения неявные: вы просто выполняете нужные вам действия, а изменения в реестр вносит сама Windows. Regedit.exe позволяет изменять реестр непосредственно, что делает его очень мощным, но, вместе с тем, и опасным инструментом.

В неопытных руках редактор реестра — действительно опасный инструмент, именно поэтому вы не найдете ярлыка для его запуска в меню **Пуск** (Start). Вы только представьте себе, что было бы, если бы доступ к редактору был у каждого пользователя? Попытка внести изменения в реестр, не имея о нем четкого представления, может сделать систему неработоспособной, да так, что в некоторых случаях спасти ее поможет лишь полная переустановка.

Программа regedit.exe находится в каталоге *%Systemroot%*, обычно это — каталог C:\Windows. Для ее запуска в Windows XP нужно было выполнить команды **Пуск** (Start) | **Выполнить** (Run) или же нажать клавиатурную комбинацию <Win>+<R>, затем ввести в командную строку команду `regedit` и нажать клавишу <Enter>. В Windows Vista и Windows 7 для этой же цели просто нажмите кнопку **Пуск** (Start), введите в поле поиска в нижней части раскрывшегося меню строку `regedit` и нажмите клавишу <Enter>.

Примечание

Если за вашим компьютером работает кто-либо еще (коллеги, родственники), я настоятельно не рекомендую создавать ярлык для редактора реестра на рабочем столе (Desktop), в меню **Пуск** (Start) или же прикреплять этот ярлык на панель задач (Taskbar). Поступая таким образом, вы обеспечите всем, кто работает за компьютером, быстрый доступ к этой потенциально опасной программе.

Основные элементы пользовательского интерфейса редактора реестра изображены на рис. 2.1.

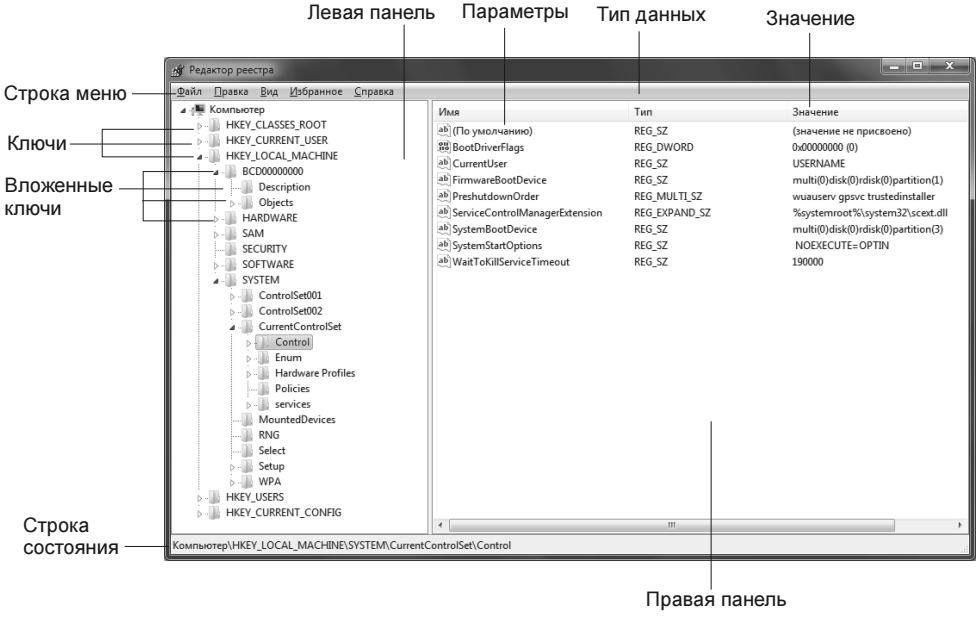


Рис. 2.1. Редактор реестра

Начиная с Windows XP, редактор реестра стал намного удобнее в использовании, нежели в предшествующих версиях Windows:

- появилась возможность добавления часто используемых ключей реестра в меню **Избранное** (Favorites);
- в Windows 2000 было два редактора реестра: Regedit.exe и Regedt32.exe[1]. Эти редакторы предоставляли различные наборы функций, поэтому иногда для

[1] Кстати, в regedt32 была очень хорошая функция — режим только для чтения. И этой функции нет в версии Regedit.exe, входящей в состав Windows XP и всех последующих версий, что не слишком хорошо. — *Прим. ред.*

достижения нужного эффекта приходилось использовать оба редактора. Начиная с Windows XP, функции этих двух редакторов совмещены в одном редакторе (Regedit.exe), что делает его использование еще более удобным;

- при запуске Regedit.exe возвращается к тому ключу реестра, с которым вы работали в прошлый раз;
- допускается экспорт любого раздела (а также всего реестра) в текстовый REG-файл;
- доступен ускоренный поиск по реестру.

2.2. Просмотр реестра

На левой панели редактора реестра (панель разделов) отображается иерархия всех разделов реестра. На правой панели окна редактора реестра (панель параметров) — параметры выбранного раздела реестра. Раздел вместе со всеми подразделами называется ветвью реестра.

Ваша работа с редактором реестра будет более эффективной, если вы изучите "горячие" клавиши (hotkeys) и комбинации клавиш (keyboard shortcuts), используемые для быстрого доступа к функциям редактора, представленные в табл. 2.1.

Таблица 2.1. *Клавиши быстрого доступа*

Клавиша/ комбинация клавиш	**Описание**
<↑>/<↓>	Позволяет перейти к предыдущему/следующему элементу (разделу на панели разделов или параметру на панели параметров)
<←> (или <->)	Если ветвь развернута, то нажатие стрелки влево приведет к ее сворачиванию. Если же ветвь не развернута, то будет выполнен переход к *родительскому* (а не предыдущему) разделу
<→> (или <+>)	Если ветвь свернута, то нажатие стрелки вправо приведет к ее разворачиванию, иначе будет выполнен переход к первому подразделу
<Home>	Позволяет вернуться к началу иерархии — элементу **Компьютер** (Computer)
<End>	Позволяет перейти к последнему видимому разделу
<Page Up>/<Page Down>	Выполняет переход вверх/вниз на одну страницу в панели разделов

Таблица 2.1 *(окончание)*

Клавиша/ комбинация клавиш	Описание
<Tab> (или <F6>)	Позволяет переключаться между панелями разделов и параметров
<Ctrl>+<F>	Открывает окно поиска — аналог команд меню **Правка** (Edit) | **Найти** (Find)
<F3>	Выполняет поиск с указанными ранее параметрами — аналог команд меню **Правка** (Edit) | **Найти далее** (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)

Рекомендую не забывать о возможности добавления часто используемых ключей в меню **Избранное** (Favorites). Например, одним из важнейших ключей реестра является `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`, в котором содержится информация о программах, автоматически стартующих при запуске системы. Помимо действительно нужных программ, этот ключ часто используется и различным вредоносным ПО. Кроме того, он является одной из излюбленных мишеней для атаки. В дальнейшем вы наверняка будете просматривать его очень часто, поэтому я рекомендую вам сразу же добавить его в избранное с помощью команд меню **Избранное** (Favorites) | **Добавить в избранное** (Add to Favorites), как показано на рис. 2.2.

Более подробно об автоматическом запуске мы поговорим в дальнейших главах книги, а сейчас данный раздел был упомянут исключительно для того, чтобы продемонстрировать метод добавления раздела в меню **Избранное** (Favorites). Получить доступ к разделу реестра после его добавления в меню **Избранное** (Favorites) можно через это же меню. В нашем случае в меню появится пункт **Run**, что соответствует имени добавленного раздела.

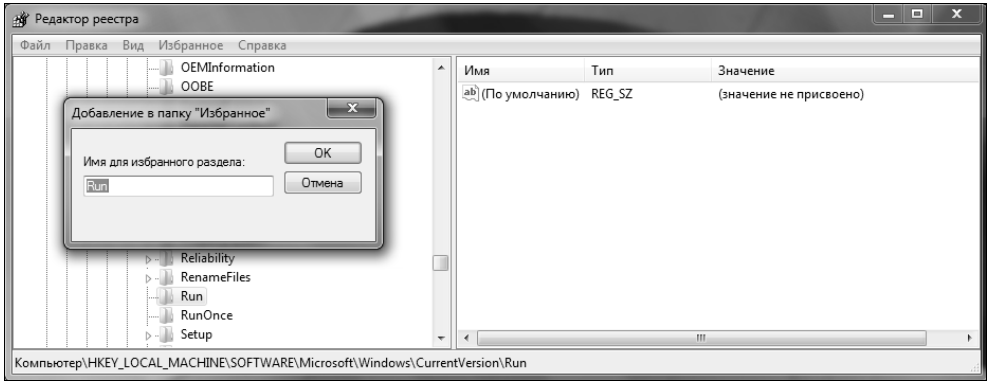


Рис. 2.2. Добавление раздела реестра в меню **Избранное** (Favorites)

2.3. Поиск данных в реестре

Для поиска значения в реестре выберите из меню команды меню **Правка** (Edit) | **Найти** (Find) или нажмите клавиатурную комбинацию <Ctrl>+<F>. В появившемся окне (рис. 2.3) нужно ввести искомое значение, а также указать, где его следует искать: в именах разделов, параметров или в значениях параметров. Обычно поиск производится по всем этим критериям, но для ускорения можно уточнить область поиска: если вам нужно найти, например, раздел, то незачем производить поиск в именах параметров и в их значениях. Чтобы повторить поиск, нажмите клавишу <F3>.

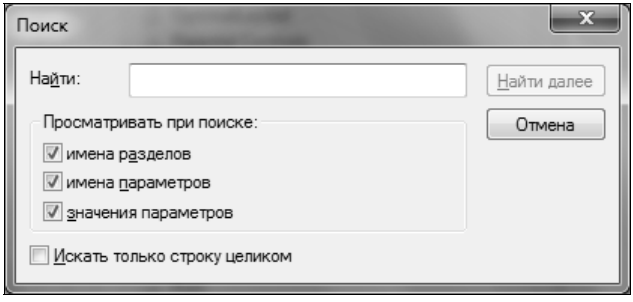


Рис. 2.3. Окно поиска

Другая возможность поиска — быстрый поиск — скорее всего, уже когда-либо использовалась вами. Она есть во многих программах и очень помогает при работе со списками. Смысл быстрого поиска заключается в том, что вы вводите начальные буквы элемента списка, а программа автоматически переходит к нужному вам элементу.

Точно такая же возможность есть и в редакторе реестра. Для выполнения поиска следует перейти к ветви, по которой будет осуществляться быстрый поиск, а затем ввести начальные буквы названия раздела, к которому вы хотите перейти. Например, вы находитесь в ветви HKLM\SOFTWARE и хотите быстро перейти к разделу Microsoft. В этом случае вам нужно ввести начальные буквы названия раздела, т. е. Mi. Если ввести только M, то редактор реестра переместит вас к первому разделу, который начинается на букву M, а это совсем необязательно будет Microsoft (например, у меня это Macromedia). Между вводом букв M и i должно пройти как можно меньше времени, иначе редактор реестра может посчитать, что вы уже ищите другой раздел, который начинается на букву I.

Функция поиска в редакторе реестра имеет следующие ограничения:

- нельзя выполнить поиск значений типа REG_DWORD и двоичных значений;
- редактор может искать только имена разделов, имена параметров и строковые данные.

Что делать, если все же нужно найти в реестре число? Можно экспортировать ветвь реестра, в которой предполагается выполнить поиск, в REG-файл, затем открыть его в Блокноте (Notepad) и произвести поиск числа. Как видите, все гениальное просто!

2.4. Редактирование реестра и создание новых объектов в реестре

Редактирование реестра заключается в создании новых разделов, новых параметров, удалении уже имеющихся параметров и разделов, а также редактировании значений параметров. Все эти операции мы и рассмотрим в этом разделе.

2.4.1. Создание нового раздела

Как уже было сказано, в реестре имеется пять корневых разделов. Вы не можете создать еще один корневой раздел, однако можете создать раздел в любом из имеющихся корневых разделов (он будет представлять собой раздел первого уровня по отношению к корневому). Для создания раздела проще всего щелкнуть правой кнопкой мыши по разделу, в котором вы хотите создать подраздел, а затем из контекстного меню выбрать команды **Создать** (New) | **Раздел** (Key), как показано на рис. 2.4.

После этого нужно ввести имя нового раздела и нажать клавишу <Enter> (рис. 2.5).

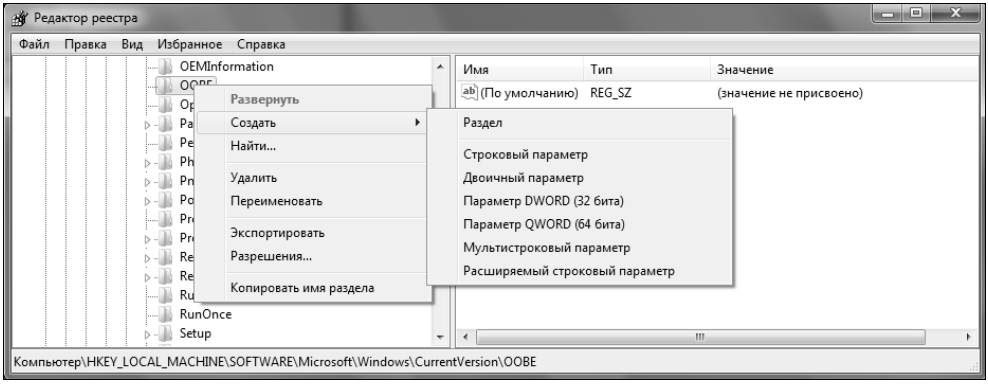


Рис. 2.4. Создание раздела

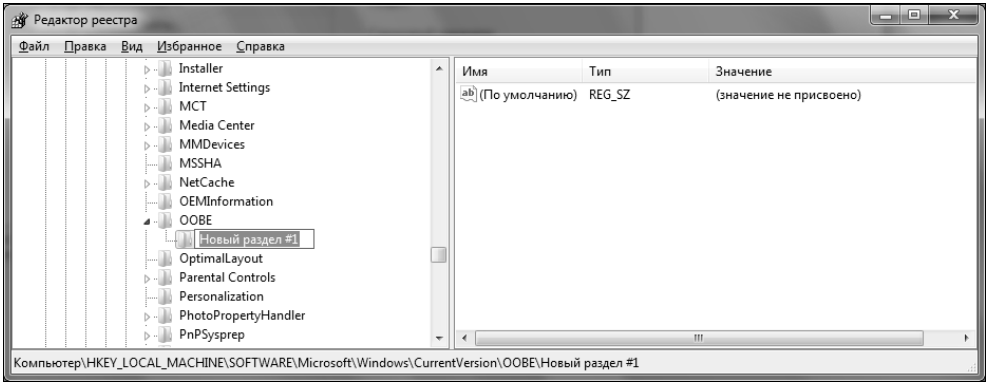


Рис. 2.5. Ввод имени раздела

Если вы не любите работать с правой кнопкой мыши, можно создать раздел при помощи следующих пунктов главного меню программы: **Правка** (Edit) | **Создать** (New) | **Раздел** (Key).

2.4.2. Удаление разделов и параметров

Удаление разделов или параметров может понадобиться, когда нужно сбросить настройки какой-нибудь программы. Иногда разработчики приложений забывают в окне настроек создать кнопку **По умолчанию** (Reset to Default), позволяющую сбросить параметры, поэтому пользователям приходится делать это вручную путем удаления из реестра разделов или параметров, принадлежащих программе.

Удалить раздел или параметр очень просто — выделите его и нажмите клавишу <Del>. Перед удалением я все же настоятельно рекомендую экспорти-

ровать удаляемые параметры (разделы) в REG-файл, чтобы в случае чего можно было выполнить откат.

2.4.3. Создание нового параметра

Редактор реестра позволяет создавать параметры следующих типов (см. рис. 2.4):

- `REG_SZ` — строковый параметр;
- `REG_BINARY` — двоичный параметр;
- `REG_DWORD` — параметр `DWORD`;
- `REG_QWORD` — параметр `QWORD`;
- `REG_MULTI_SZ` — мультистроковый параметр;
- `REG_EXPAND_SZ` — расширяемый строковый параметр.

Хотя уже в Windows Vista появились возможности редактирования параметров и остальных типов (см. табл. 1.3), например, параметров типа `REG_QWORD`, делать это через редактор реестра крайне нежелательно.

Для создания нового параметра перейдите в раздел, в котором нужно создать параметр, и выберите команды **Правка** (Edit) | **Создать** (New), после чего укажите тип создаваемого параметра.

2.4.4. Редактирование параметров

Для изменения значения параметра нужно выбрать команду **Правка** (Edit) | **Изменить** (Modify), но могу поспорить, что вам больше понравится раскрывать нужный параметр двойным щелчком мыши, чем выбирать команду **Изменить** (Modify) из меню **Правка** (Edit). В окне редактирования (рис. 2.6) вы сможете изменить только значение параметра.

Чтобы изменить имя параметра (переименовать параметр), нужно выделить его и нажать клавишу <F2>, после чего ввести новое имя и нажать клавишу <Enter>.

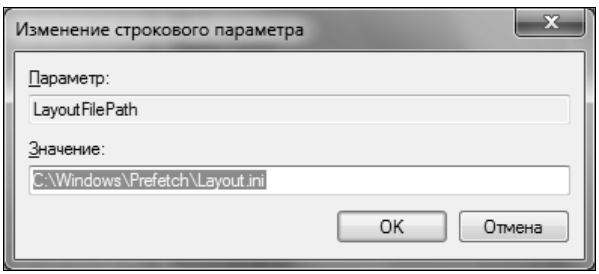


Рис. 2.6. Окно редактирования

А вот тип данных параметра вы изменить не можете. Единственный вариант — удалить параметр и создать новый с таким же именем, но другого типа. Правда, скорее всего вам никогда не понадобится изменять тип параметра.

Для редактирования двоичных данных гораздо удобнее использовать команду **Правка** (Edit) | **Изменить двоичные данные** (Modify Binary Data). На экране появится окно **Изменение двоичного параметра** (Edit Binary Value), показанное на рис. 2.7.

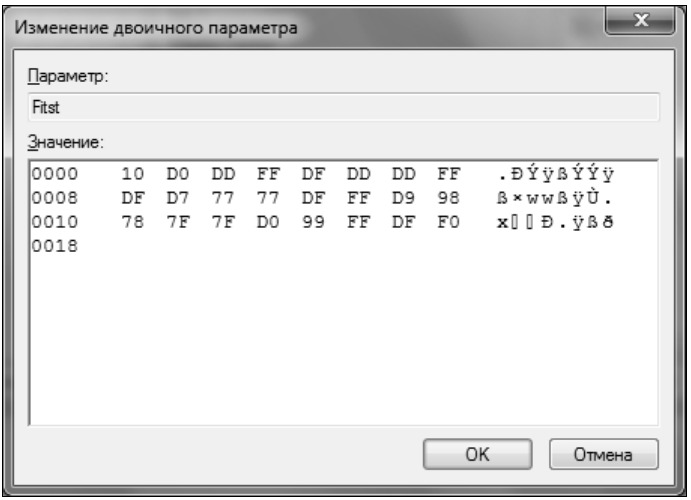


Рис. 2.7. Изменение двоичного параметра

2.4.5. Копирование имени раздела в буфер обмена

Наконец, не стоит забывать о командах **Правка** (Edit) | **Копировать имя раздела** (Copy Key Name). Данная команда копирует имя раздела реестра в буфер обмена (Clipboard). Далее вы можете вставить имя раздела (параметра) в любой текстовый документ, что очень удобно.

2.5. Импорт и экспорт разделов реестра

Иногда нужно выполнить экспорт того или иного раздела реестра, например, раздела, содержащего настройки определенной программы. Не всегда удобно делать резервную копию всего реестра, если нужно сохранить только один-

единственный раздел или даже параметр. В случае неудачного изменения реестра всегда можно восстановить настройки программы, импортировав ранее экспортированный раздел реестра. Вы можете выполнить экспорт раздела реестра либо в REG-файл, либо в файл куста реестра. Мы рассмотрим оба способа, а вы уже решите, какой из них и в каком случае вам больше подходит.

2.5.1. Экспорт параметров реестра в REG-файл

Смысл этого способа заключается в следующем. Вы выбираете раздел реестра, в котором требуется произвести изменения. Не обязательно выбирать весь корневой раздел, можно выбрать один из его подразделов (если выбрать весь корневой раздел, то получится очень большой REG-файл). После этого выполните команды **Файл** (File) | **Экспорт** (Export). Выберите тип файла **Файлы реестра (*.reg)** (Registry files (*.reg)), введите имя файла и нажмите кнопку **Сохранить** (Save). Обратите внимание: с помощью переключателей из группы опций **Диапазон экспорта** (Export range) вы можете сохранить сразу весь реестр, но тогда у вас получится очень большой REG-файл. Есть и еще один, намного удобный способ сохранять весь реестр целиком, и заключается он в создании точек восстановления системы (System Restore Points), о которых мы поговорим в следующей главе. С другой стороны, учитывая, что ни файлы кустов, ни файлы точки восстановления вы не можете перенести на другой компьютер, можно экспортировать в REG-файл весь реестр и записать его на сменный носитель (например, CD-ROM): так вы точно будете уверены, что резервная копия в целости и сохранности.

Преимущество этого способа заключается в том, что создается читаемый текстовый файл, который можно изменить с помощью любого текстового редактора.

Чтобы восстановить реестр из REG-файла, достаточно дважды щелкнуть на REG-файле в окне Проводника и согласиться добавить данные из него в реестр. REG-файлы очень удобно использовать для восстановления удаленных или неправильно измененных параметров реестра:

- Если в реестре нет параметра, который есть в REG-файле, то редактор реестра создаст такой же параметр в реестре.
- Если в реестре есть параметр с таким же именем, как в REG-файле, то редактор реестра восстановит значение параметра из REG-файла.

Более подробно о REG-файлах мы поговорим в *части II* этой книги, а пока перейдем к следующему разделу.

2.5.2. Экспорт параметров реестра в файл куста

REG-файлы довольно удобны, но у них есть один и очень большой недостаток, из-за которого их лучше не использовать для резервного копирования всего реестра. Предположим, что вы экспортировали реестр в REG-файл. А после этого "вражеская" программа добавила в реестр какой-то параметр, из-за которого нарушилась работа всей системы. Если данного параметра нет в REG-файле, но он есть в реестре, при обработке REG-файла этот параметр не будет изменен. То есть он останется и система будет по-прежнему "глючить".

Выход из этой ситуации есть: экспорт реестра в файл куста. Преимущество очевидно. Например, вы экспортировали весь ключ HKLM в файл куста. Когда вы будете импортировать файл куста, то весь ключ HKLM будет удален (со всеми параметрами, созданными "вражеской" программой), а на его месте будет восстановлен ключ HKLM из выбранного вами файла куста. Улавливаете разницу?

Для экспорта реестра в файл куста выберите команды **Файл** (File) | **Экспорт** (Export), в качестве типа файла выберите **Файлы кустов реестра (*.*)** (Registry hive files (*.*)), затем нажмите кнопку **Сохранить** (Save).

Для восстановления файла куста выберите из меню команды **Файл** (File) | **Импорт** (Import), в качестве типа файла выберите **Файлы кустов реестра (*.*)** (Registry hive files (*.*)), выберите файл куста и нажмите кнопку **Открыть** (Open).

Обратите внимание: в меню **Файл** (File) есть команды **Загрузить куст** (Load Hive) и **Выгрузить куст** (Unload Hive). Не нужно путать их с командами импорта и экспорта реестра.

При импорте файла куста происходит изменение рабочей части реестра. При загрузке файла куста в реестре создается полностью новая ветвь, которую можно просматривать и редактировать, но которая при этом никак не влияет на работу системы. Эта операция аналогична открытию еще одного документа в окне Word — точно так же, как открытие нового документа никак не отображается на уже открытых документах, так и загрузка в реестр нового куста никак не влияет на уже существующие.

Выгрузка куста удаляет ссылку на него из реестра. Чтобы выгрузить куст, выделите его, а затем выберите команду **Выгрузить куст** (Unload Hive). Вы можете выгружать только те файлы кустов, которые загрузили сами. Вы не можете выгрузить файл куста, который загрузила сама Windows.

> ***Примечание***
>
> Обратите внимание, что команды **Загрузить куст** (Load Hive) и **Выгрузить куст** (Unload Hive) применимы лишь к ключам, которые соответствуют ульям реестра, а в остальных случаях эти опции меню недоступны.

2.5.3. Когда и какой способ выбрать?

Первый способ можно использовать, если вам нужно экспортировать один-два раздела реестра. Как уже было отмечено выше, REG-файлы нельзя использовать для экспорта всего реестра.

Если нужно сохранить корневые разделы реестра (или весь реестр), намного удобнее и правильнее будет использовать экспорт в файлы кустов. У этого способа есть еще одно огромное преимущество. Файлы кустов, которые находятся в каталоге *%Systemroot%*\system32\config и *%Userprofile%*, нельзя скопировать, если Windows запущена. При обращении к файлу вы получите сообщение о том, что файл не существует, хотя он виден в оглавлении каталога. Чтобы скопировать эти файлы, нужно загрузиться с другой версии Windows, которая параллельно установлена на компьютере, или с загрузочного CD: вот тогда Windows не будет мешать копированию этих файлов. Но, согласитесь, не у каждого установлены две версии Windows, да и загрузочный диск не всегда есть под рукой. Поэтому намного удобнее экспортировать весь реестр в файлы кустов, а затем восстановить, когда это будет нужно. Файлы кустов, которые были созданы вами (например, путем экспорта реестра), вы можете свободно копировать, записывать на сменные носители и т. д.

2.6. Печать реестра

Мне трудно себе представить ситуацию, когда может понадобиться функция печати реестра. Тем не менее, она существует, и вы всегда можете распечатать любой раздел реестра. Лучше, конечно, не пытаться напечатать целиком ветвь `HKLM` и уж тем более — весь реестр. Я даже не могу предположить, что закончится раньше: тонер в принтере или бумага.

Для печати реестра нужно выделить нужную ветку и выполнить команды **Файл** (Файл) | **Печать** (Print). Далее все операции выполняются как обычно — выбираем принтер (рис. 2.8) и нажимаем кнопку **Печать** (Print).

Ради интереса я распечатал уже знакомый нам раздел `Run` и получил на листе бумаги следующий вывод (листинг 2.1):

Листинг 2.1. Фрагмент распечатанного содержимого раздела HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

```
Раздел: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Название класса: <Класс отсутствует>
Последнее время записи: 12.06.2007 — 7:44
```

```
Параметр 0
        Название:       NvCplDaemon
        Тип:            REG_SZ
        Значение:       RUNDLL32.EXE C:\WINDOWS\System32\NvCpl.dll,NvStartup

Параметр 1
        Название:       nwiz
        Тип:            REG_SZ
        Значение:       nwiz.exe /install

Параметр 2
        Название:       NeroFilterCheck
        Тип:            REG_SZ
        Значение:       C:\WINDOWS\system32\NeroCheck.exe

...
```

Не буду приводить результат целиком: из приведенного в листинге 2.1 отрывка вы и так уже поняли, что получите в результате. Хочу лишь отметить, что при печати раздела реестра будут распечатаны не только его параметры, но и его подразделы, поэтому следите за бумагой в принтере: ее может не хватить!

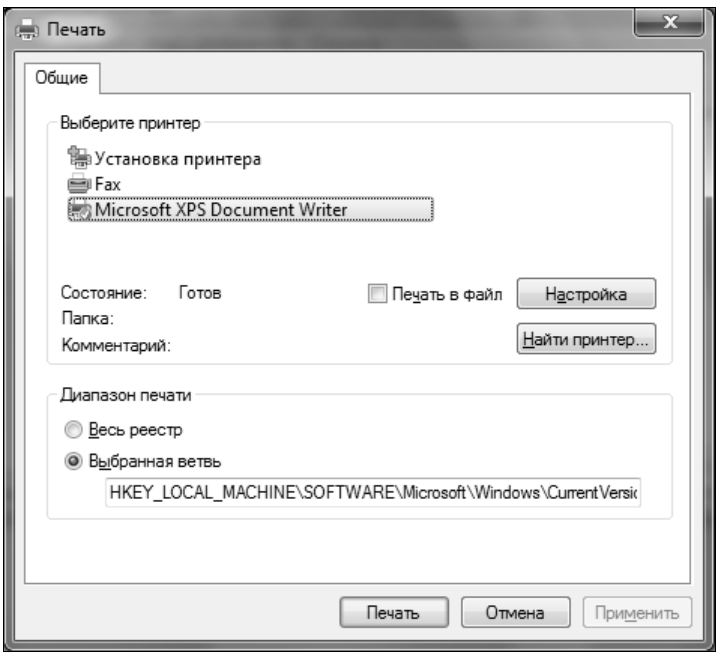


Рис. 2.8. Окно печати реестра

2.7. Работа с реестром удаленного компьютера

Начиная с Windows XP, вы можете подключаться к удаленному реестру. Иными словами, вы можете удаленно редактировать реестр другого компьютера, не покидая своего рабочего места. Согласитесь, что это очень удобно, если вы — администратор сети. Все, что вам для этого потребуется — это удостовериться в том, что на всех компьютерах сети запущена служба **Удаленный реестр** (Remote Registry).

> ***Примечание***
>
> Правда, следует помнить и о том, что это — потенциально опасная служба, поэтому держать ее включенной постоянно не рекомендуется. Кстати, в Windows 7 для этой службы по умолчанию предусмотрен именно ручной тип запуска (т. е. она не стартует автоматически при запуске системы).

Если вы решили воспользоваться возможностью удаленного редактирования реестра, убедитесь в том, что соблюдены следующие условия:

- на всех компьютерах, к которым вы будете пытаться подключиться, должна быть запущена служба **Удаленный реестр** (Remote Registry). Проверить это позволяет оснастка MMC services.msc. Доступ к ней можно получить традиционным путем — через Панель управления (Control Panel). Но быстрее всего добиться нужного результата можно, нажав кнопку **Пуск** (Start) и введя в поле поиска в нижней части меню команду `services.msc`;
- подключение к реестру удаленного компьютера должно производиться от имени учетной записи с правами администратора или даже от имени учетной записи `Администратор` (`Administrator`).

> ***Примечание***
>
> Начиная с Windows Vista, в систему безопасности был внесен ряд изменений, направленных на повышение общей защищенности системы. Так, учетная запись `Администратор` (`Administrator`) по умолчанию блокирована и сделана скрытой. Естественно, та же самая ситуация имеет место и в Windows 7. Поэтому, если вы хотите воспользоваться этой учетной записью, ее необходимо сначала разблокировать. Для этого запустите сеанс работы с командной строкой от имени администратора и дайте следующую команду: `net user Administrator /active:yes`. Разблокировав эту учетную запись, не забудьте сразу же защитить ее паролем. Выполнив все необходимые операции, не забудьте вновь заблокировать учетную запись `Администратор` (`Administrator`). Для этой цели дайте следующую команду:
> `net user Administrator /active:no`.

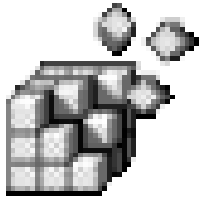
Выполните команду **Файл** (File) | **Подключить сетевой реестр** (Connect network registry). Далее нужно ввести имя компьютера, к которому вы пытае-

тесь подключиться. После этого вы сможете подключиться к его реестру и работать с ним, как со своим локальным реестром. Для отключения сетевого реестра выполните команду **Файл** (File) | **Отключить сетевой реестр** (Disconnect network registry).

2.8. Установка прав доступа к разделам реестра

Вы можете определить права доступа к тому или иному ключу (разделу) или параметру реестра. Выделите ключ или параметр реестра и выполните команду **Правка** (Edit) | **Разрешения** (Permissions). Далее процесс установки разрешений к разделу реестра не отличается от установки разрешений для доступа к сетевому каталогу.

ГЛАВА 3



Секреты пользовательского интерфейса

3.1. О чем эта глава?

В этой главе мы поговорим об изменении настроек рабочего стола (Desktop), корзины (Recycle Bin), меню **Пуск** (Start) и панели задач (Taskbar). Часть настроек, приведенных в этой главе, можно выполнить и с помощью пользовательского интерфейса[1], но есть и целый ряд таких, которые можно осуществить только путем редактирования реестра. Отметим, что настройки, которые вполне можно осуществить и стандартными средствами Windows, в общем-то не должны называться полноценными "хаками". Но, тем не менее, мы их рассмотрим "для общего развития": а вдруг вы когда-то захотите написать собственный "твикер" для реестра? Тогда после прочтения этой книги у вас под рукой будет все необходимое. Вам останется лишь разработать пользовательский интерфейс.

Далее при создании нового параметра реестра я буду называть раздел, в котором нужно его создать, после чего указывать имя параметра и его тип данных в следующем виде:

[тип] [имя]

Например:

```
REG_DWORD NoDesktop
```

[1] В частности, большинство из настроек, рассмотренных в этой главе, могут быть выполнены с помощью оснастки MMC GPEdit.msc. Впрочем, надо отметить, что эта оснастка недоступна пользователям таких вариантов поставки Windows 7, как Home Basic и Home Premium, а ведь именно они, предположительно, будут предустановлены на большинстве новых компьютеров. Таким образом, для пользователей таких систем описанные в данной главе "хаки" действительно будут актуальны, и выполнять их придется именно так, как здесь описано — путем редактирования реестра. — *Прим. ред.*

Далее будут указаны возможные значения этого параметра.

В этой главе мы будем изменять пользовательские настройки, хранящиеся в корневом разделе реестра HKEY_CURRENT_USER (или HKCU). Чтобы после внесения изменений в реестр они вступили в силу, нужно выйти из системы и снова зайти. А вот при изменении глобальных параметров (чего мы не будем делать в этой главе), т. е. раздела HKEY_LOCAL_MACHINE (HKLM), придется перезагружать компьютер.

3.2. Параметры рабочего стола

3.2.1. Отключение рабочего стола

С помощью всего лишь одного параметра реестра вы можете полностью блокировать функционирование рабочего стола: все пиктограммы будут скрыты и станет недоступным контекстное меню. Честно говоря, даже не знаю, зачем может понадобиться такая возможность, но одно могу сказать точно: порядок на рабочем столе вам гарантирован.

Итак, для отключения рабочего стола откройте следующий раздел реестра:

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

В этом разделе создайте параметр:

```
REG_DWORD NoDesktop
```

Возможные значения параметра:

- 1 — отключить рабочий стол;
- 0 — нормальная работа рабочего стола.

> ***Примечание***
>
> Если в разделе реестра HKCU\Software\Microsoft\Windows\CurrentVersion\Policies нет подраздела Explorer, то его придется создать самостоятельно.

Данный параметр работает во всех ОС Windows: XP, Vista, Windows 7. На рис. 3.1 изображен рабочий стол Windows 7: отображение пиктограмм отключено и выводится номер сборки Windows 7 (см. совет в следующем разделе).

> ***Примечание***
>
> Следует отметить, что изменения не вступают в силу сразу же после добавления нового параметра, однако перезагрузки компьютера тоже не требуется. В данном случае нужно выйти из системы (Logout), а затем повторно в ней зарегистрироваться.

3.2.2. Вывод версии Windows на рабочем столе

Если вы фанат Windows и созерцание номера версии Windows в правом нижнем углу рабочего стола доставляет вам удовольствие, тогда этот трюк для вас. В разделе `HKCU\Control Panel\Desktop` найдите следующий параметр и установите для него значение `1`:

```
REG_DWORD PaintDesktopVersion
```

Данный параметр работает как в Windows XP, так и в Windows Vista/Windows 7 (рис. 3.1). В дальнейшем, если параметры можно применять для обеих версий операционных систем, то подобные комментарии я делать не буду. Если же какой-то параметр работает только в Windows 7, Vista или только в XP, об этом будет сказано явно.

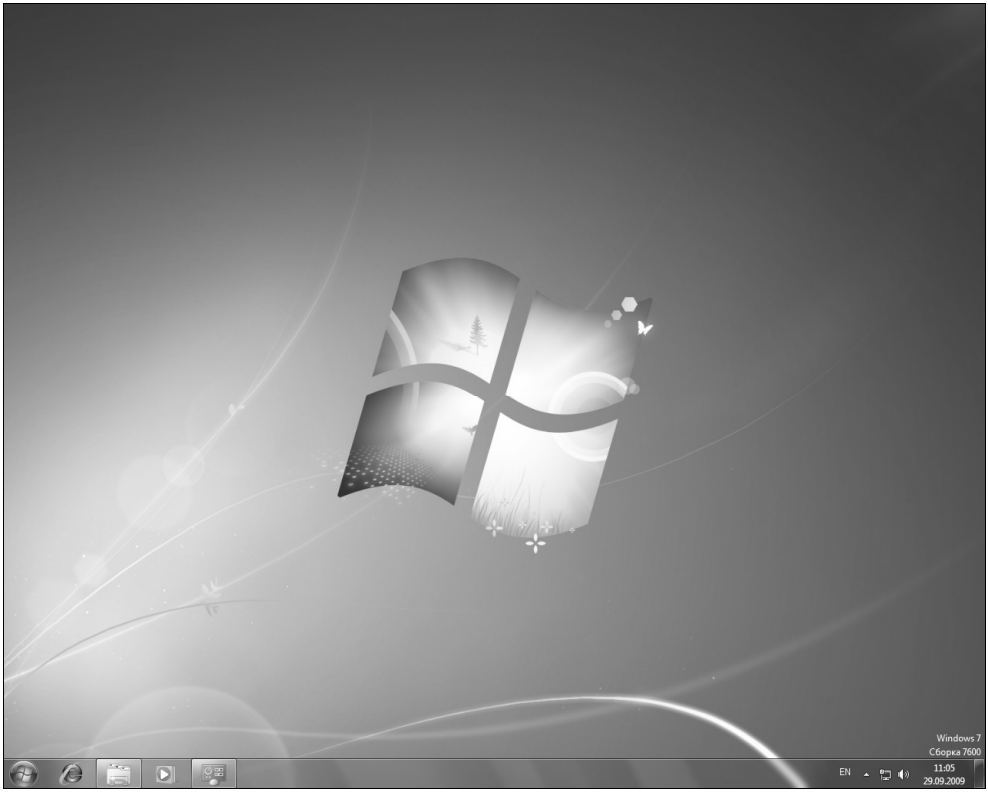


Рис. 3.1. Отключенный рабочий стол и вывод номера сборки Windows 7

3.2.3. Запрет команды *Изменение значков рабочего стола*

С помощью команды **Изменение значков рабочего стола** (Change desktop icons) в окне **Персонализация** (Personalization) пользователь может выбрать, какие стандартные пиктограммы, например, **Компьютер** (Computer), **Корзина** (Recycle Bin) и т. д., должны отображаться на рабочем столе, а какие — нет. Запретить команду **Изменение значков рабочего стола** (Change desktop icons) можно с помощью параметра `NoDispBackgroundPage` (тип данных — `REG_DWORD`) в разделе `HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System`.

Данный параметр может принимать следующие значения:

- `1` — исключить возможность изменения картинки пользователя (рис. 3.2);
- `0` — разрешить пользователям изменять картинку учетной записи.

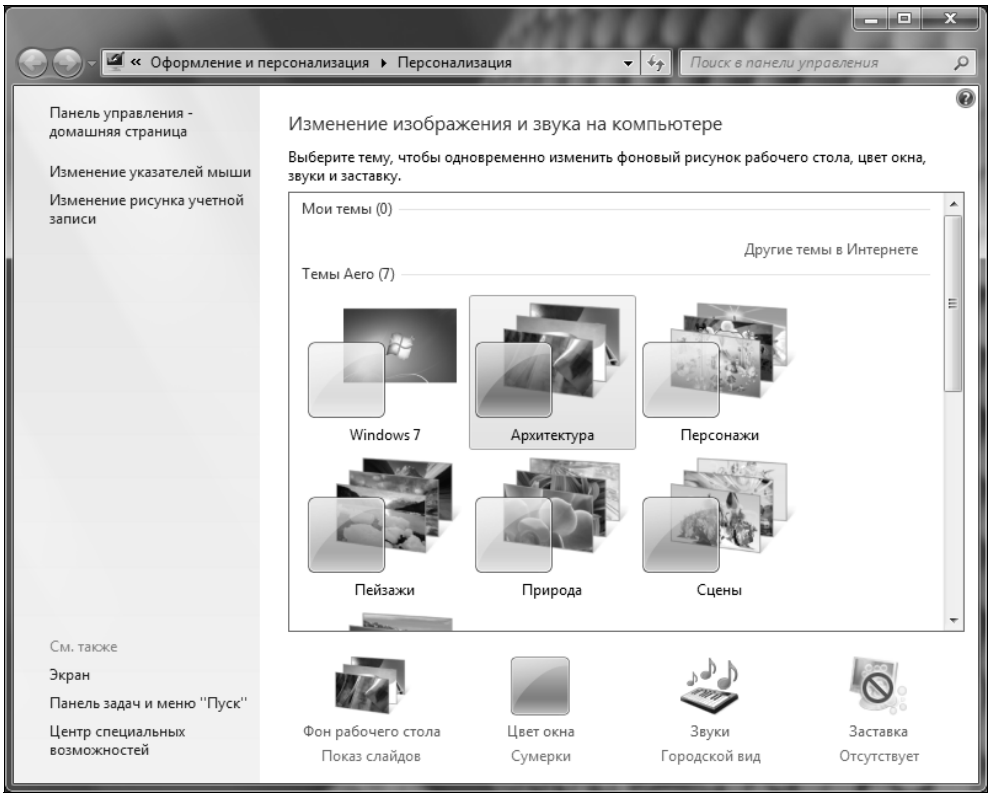


Рис. 3.2. В окне персонализации нет команды **Изменение значков рабочего стола**

Интересно, что в Windows XP параметр `NoDispBackgroundPage` использовался для запрета отображения вкладки изменения рисунка рабочего стола.

3.2.4. Запрет изменения обоев рабочего стола

Чтобы запретить пользователю менять обои рабочего стола, создайте в разделе `HKCU\Software\Microsoft\Windows\CurrentVersion\Policies` подраздел `ActiveDesktop`, создайте в нем параметр с типом данных `REG_DWORD`, назовите его `NoChangingWallPaper` и присвойте ему значение `1`. После этого при попытке изменения обоев будет выводиться сообщение о том, что данная возможность отключена системным администратором (рис. 3.3).

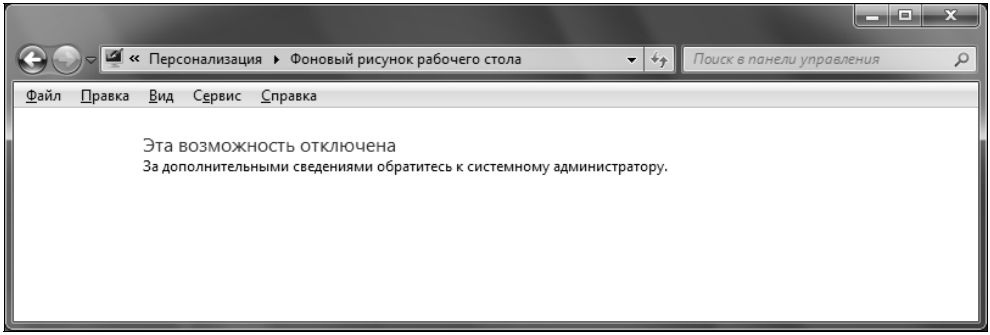


Рис. 3.3. Возможность изменения обоев рабочего стола теперь отключена

3.2.5. Запрет изменения параметров экранной заставки (Screensaver)

Иногда полезно отключить возможность изменения настроек экранной заставки. Нет, даже не потому, что вы хотите, чтобы у всех была одинаковая экранная заставка. А для того, чтобы у всех были одинаковые параметры экранной заставки, а именно — интервал ожидания, после которого она выводится на экран. Некоторые пользователи вообще отключают экранную заставку, другие устанавливают этот интервал слишком большим, что нежелательно с точки зрения безопасности. Чтобы запретить изменение пользователями параметров экранной заставки, в уже знакомом нам разделе `HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System` нужно создать параметр:

```
REG_DWORD NoDispScrSavPage
```

Если установить для него значение `1`, то из окна свойств экрана исчезнет вкладка **Заставка** (XP), а из окна **Персонализация** — ссылка **Заставка**

(Vista). В Windows 7 ссылка **Заставка** никуда не исчезнет, но работать просто не будет (рис. 3.4).

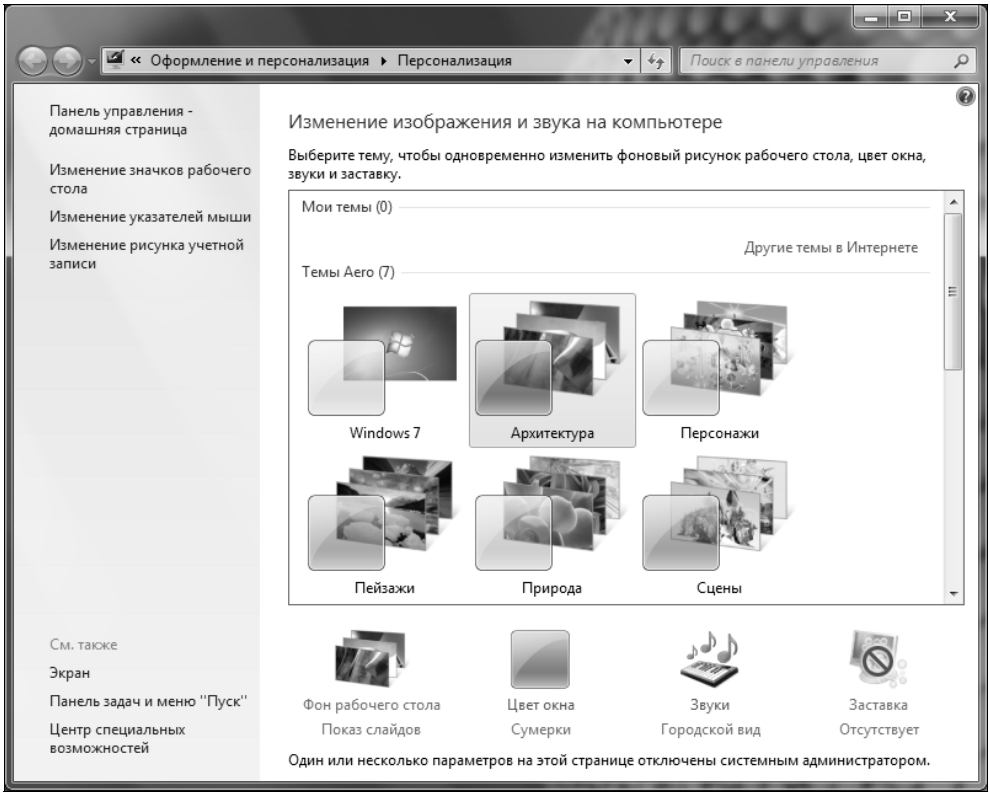


Рис. 3.4. Кнопка изменения хранителя экрана недоступна

3.2.6. Добавление значка *Корзина* в окно *Компьютер*

Сейчас мы разберемся, как добавить значок **Корзина** (Recycle Bin) в окно **Компьютер** (Computer). Перейдите в следующий раздел:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\MyComputer
\NameSpace
```

В этом разделе создайте подраздел с именем:

```
{645FF040-5081-101B-9F08-00AA002F954E}
```

После этого в окне **Компьютер** (Computer) появится значок **Корзина** (Recycle Bin), как показано на рис. 3.5.

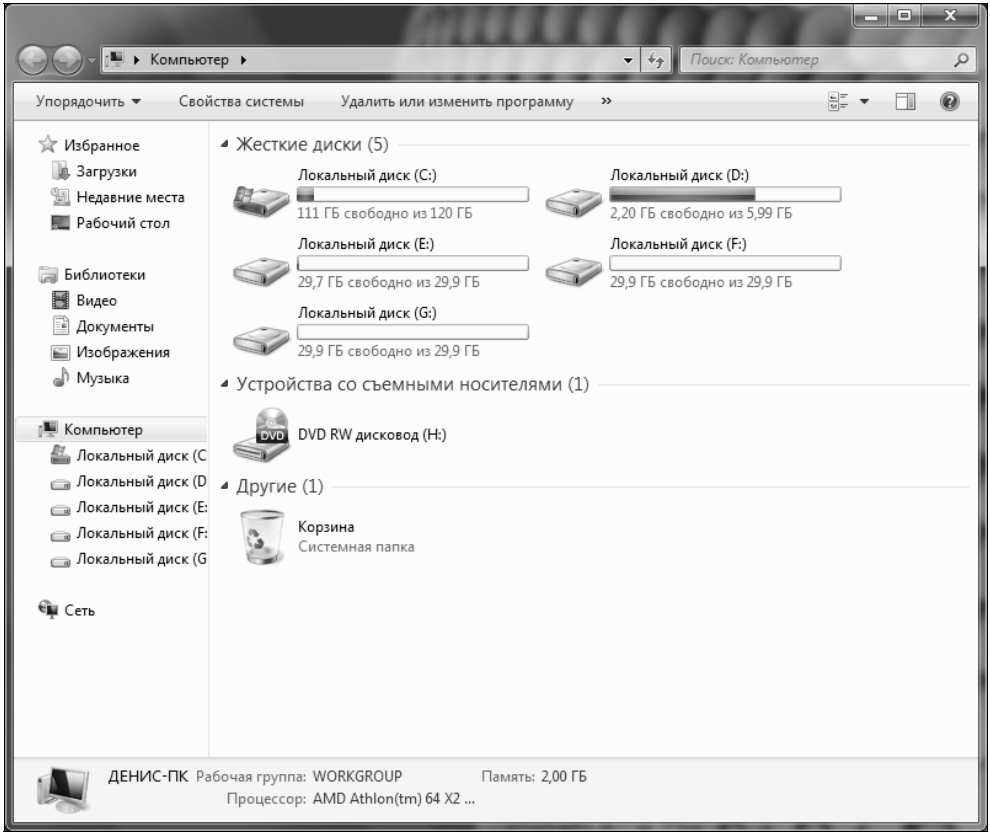


Рис. 3.5. Значок **Корзина** в окне **Компьютер**

Чтобы удалить значок **Корзина** (Recycle Bin) из окна **Компьютер** (Computer), достаточно удалить созданный вами раздел.

3.2.7. Добавление новых команд в контекстное меню *Компьютер*

Если щелкнуть правой кнопкой мыши на значке **Компьютер** (Computer), вы увидите контекстное меню. В это меню можно легко добавить свои команды. Для этого перейдите в раздел `HKCR\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell`. В этом разделе нужно создать новый раздел с любым именем, например, `Notepad`. А в разделе `Notepad` нужно создать подраздел `command` и создать параметр по умолчанию типа `REG_SZ`, и в качестве значения ввести команду, которую нужно выполнить, например, `c:\windows\notepad.exe`. Обратите внимание, что нужно указывать полный путь к программе, которую вы хотите выполнить.

3.2.8. Удаление стрелок с ярлыков

Не знаю, как вам, а мне жутко не нравятся стрелки на пиктограммах ярлыков на рабочем столе. Перейдите в раздел `HKCR\lnkfile` и удалите параметр `IsShortcut`.

3.3. Параметры панели задач

3.3.1. Сокрытие часов на панели задач

Скрыть вывод даты и времени на панели задач можно путем добавления параметра `REG_DWORD HideClock` в раздел реестра `HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`. Параметр может принимать следующие значения:

- `1`, если вы хотите скрыть часы;
- `0`, если вам нужно снова отобразить часы.

Установить формат времени можно с помощью параметра `HKCU\Control Panel\International\sTimeFormat` (тип данных — `REG_SZ`). Значение по умолчанию: `h:mm:ss tt`.[1]

3.3.2. Параметры области уведомления

Все параметры, которые будут рассмотрены в этом разделе, можно установить в диалоговом окне параметров панели задач (рис. 3.6), вызываемого с помощью команды **Свойства** (Properties) контекстного меню панели задач.

3.3.2.1. Сокрытие неиспользуемых пиктограмм в области уведомлений

Если у вас много пиктограмм в области уведомлений (system tray), то полезно скрывать неиспользуемые. Для этого нужно создать такой параметр:

`REG_DWORD EnableAutoTray`

в разделе `HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer`. Если параметр включен (его значение равно `1`), то будет выполнено автоматическое сокрытие пиктограмм в области уведомлений. Данный параметр используется по умолчанию; отсутствие параметра равносильно присвоению ему значения `1`. Для принудительного выключения нужно создать параметр и присвоить ему значение `0`.

---

[1] Здесь `tt` — многосимвольная строка обозначения времени, например, AM или PM. — *Прим. ред.*

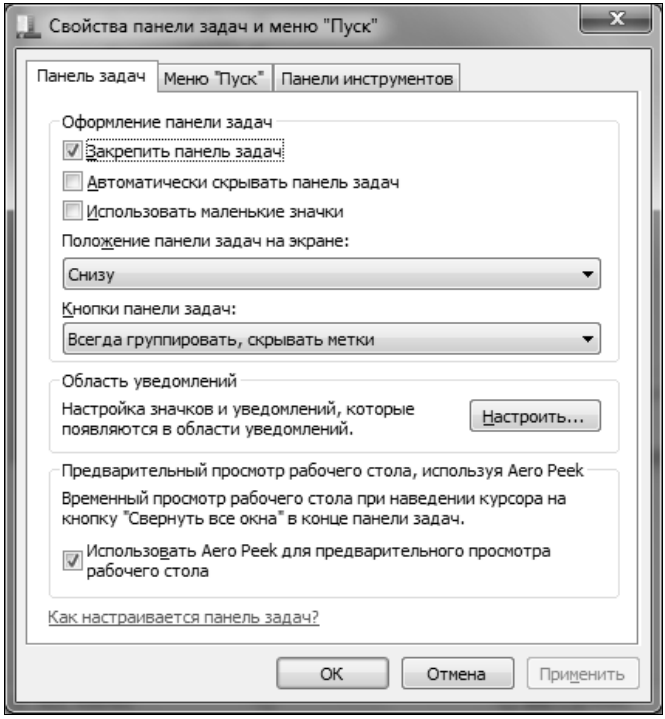


Рис. 3.6. Окно параметров панели задач

3.3.2.2. Сокрытие всех пиктограмм в области уведомлений

При желании можно вообще скрыть в области уведомлений все значки. Для этого перейдите в раздел `HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer` и создайте параметр:

```
REG_DWORD NoTrayItemsDisplay
```

Если параметр включен (его значение равно `1`), значки в области уведомлений отображаться не будут. Вы не сможете изменить значение данного параметра с помощью окна настройки панели задач, поэтому возьмите себе его на заметку.

3.3.3. Некоторые параметры панели задач

3.3.3.1. Автоматическая группировка схожих кнопок

Когда вы запускаете несколько экземпляров одного и того же приложения, например, открываете несколько окон Word, то Windows может сгруппиро-

вать подобные кнопки на панели задач. С одной стороны это удобно, поскольку кнопок на панели задач будет меньше, но чтобы добраться до нужного окна, придется дважды щелкать мышью — один раз для открытия меню окон, а второй — для выбора нужного окна. Поэтому мне не нравится автоматическая группировка сходных кнопок, которая включена по умолчанию. Если она вам тоже не нравится, то ее легко отключить (как с помощью реестра, так и с помощью окна параметров панели задач). Откройте раздел `HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced`. Найдите в нем параметр:

```
REG_DWORD TaskbarGlomming
```

Если такого параметра нет, его нужно создать. Для отключения группировки сходных кнопок присвойте этому параметру значение `0`.

Если вы все же включили группировку подобных кнопок, то можете ее настроить более гибко. Для этого используется следующий параметр, который находится в том же разделе:

```
REG_DWORD TaskbarGroupSize
```

Данный параметр может принимать следующие значения:

- `0` (по умолчанию) — кнопки будут группироваться в порядке их открытия и только в том случае, если на панели задач мало места;
- `1` — кнопки группируются в порядке, обратном их открытию, и только в том случае, если на панели задач мало места;
- `2` — кнопки будут группироваться в любом случае, при условии, что есть не меньше двух подобных;
- `3` — то же, что и `2`, но для группировки нужно как минимум три подобных кнопки.

3.3.3.2. Изменение уровня группировки кнопок в Windows 7

В Windows 7 (и только в Windows 7!) за группировку схожих задач на панели задач отвечает `DWORD`-параметр `TaskbarGlomLevel`. По умолчанию все схожие задачи, например открытые окна Internet Explorer, группируются в одну кнопку. Когда вы подводите указать мыши к этой кнопке, система отобразит несколько миниатюр окон и вы сможете выбрать нужное вам окно (рис. 3.7). Если вы присвоите параметру `TaskbarGlomLevel` значение `1`, для каждого окна будет своя кнопка на панели задач (рис. 3.8). Не знаю, но лично мне так больше нравится.

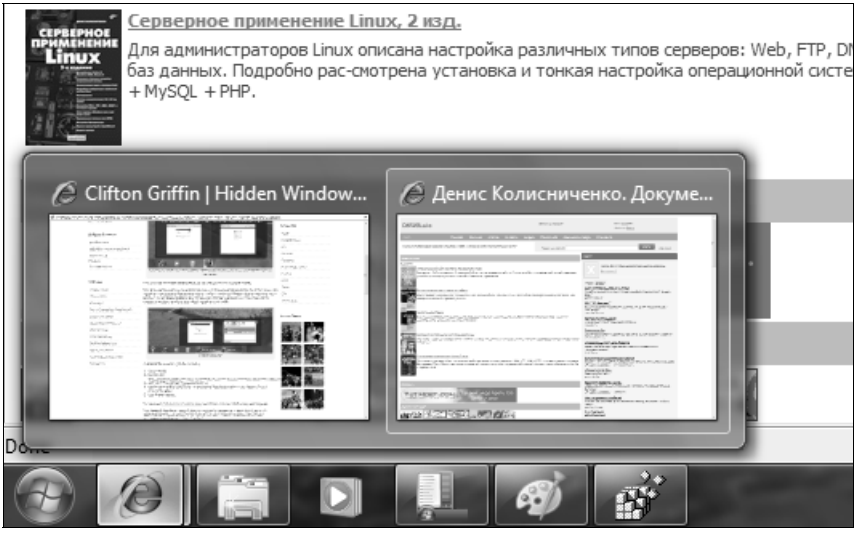


Рис. 3.7. Поведение панели задач Windows 7 по умолчанию

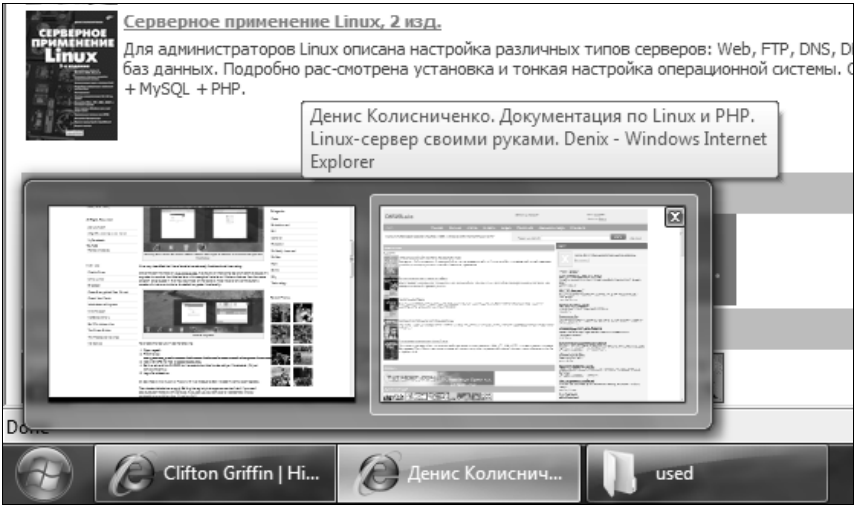


Рис. 3.8. Не группировать окна

3.3.4. Бесконечное мигание кнопок на панели задач

Если программа требует ввода данных, ее значок на панели задач будет мигать. Сколько раз будет мигать кнопка? Это зависит от следующего параметра:

```
REG_DWORD ForegroundFlashCount
```

Данный параметр вы найдете в разделе HKCU\Control Panel\Desktop. Если параметр равен 0, то кнопка будет мигать бесконечно.

В этом же разделе вы найдете еще один параметр, связанный с мерцанием кнопки окна. Как уже было сказано, если программа требует ввода данных, ее кнопка начнет мерцать на панели задач. По прошествии определенного времени (по умолчанию 200 секунд или 200 000 миллисекунд) окно программы "выскочит" поверх остальных окон (программе надоест ждать ввода, и она более настойчиво потребует внимания от пользователя). Сколько секунд будет ждать программа перед "выходом", определяется параметром ForegroundLockTimeout с типом данных REG_DWORD, значение которого измеряется в миллисекундах (а не в секундах!).

3.4. Меню *Пуск*

В реестре очень много параметров, влияющих на меню **Пуск** (Start), поэтому приготовьтесь читать — их действительно будет много. Еще раз напомню: для того чтобы внесенные изменения вступили в силу, вам нужно выйти из системы (завершить сеанс) и снова зарегистрироваться.

3.4.1. Как редактировать расширенное меню *Пуск* с помощью реестра

В этом разделе мы поговорим о расширенном меню **Пуск** (Start), которое впервые появилось в Windows XP. Настраивается данное меню с помощью параметров, которые также находятся в разделе реестра HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced. Однако если имена параметров реестра, настраивающих классическое меню[1], начинались со строки StartMenu*, то имена параметров расширенного меню начинаются строкой Start_, например, Start_AdminToolsRoot.

Существует два способа изменения расширенного меню. Первый заключается в редактировании раздела HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced.

Второй заключается в редактировании ключа HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer (изменяет настройки только для текущего пользователя) или такого же ключа в HKLM (изменяет настройки для всех пользователей).

---

[1] Обратите внимание, что если в Windows XP и Windows Vista имелась возможность переключения на использование классического меню **Пуск** (Start), то в Windows 7 этой возможности больше нет. И никакого "трюка" с реестром, позволяющего "вернуть" его, не существует. Единственное, что могут сделать пользователи, которым его не хватает, — это имитировать классическое меню, создав панель инструментов (Toolbar) на панели задач. — *Прим. ред.*

Отличие между ними заключается в следующем: если вы внесли изменения в раздел `HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced`, то они легко могут быть изменены с помощью стандартных средств Windows (имеется в виду окно настройки меню **Пуск** (Start)). Если же вы воспользовались вторым способом, то окно настройки меню **Пуск** (Start) будет бессильно — оно не сможет изменить параметры раздела `Policies\Explorer`, которые являются более приоритетными, чем параметры раздела `Explorer\Advanced`.

Параметров расширенного меню довольно много, но большинство из них управляет отображением определенных пунктов меню, поэтому большую часть параметров можно объединить в табл. 3.1. Все параметры из табл. 3.3, кроме `Start_ShowNetPlaces` и `Start_ShowHelp`, могут принимать одно из трех значений:

- `0` — не отображать соответствующий параметру пункт меню;
- `1` — отображать как ссылку;
- `2` — отображать как меню, т. е. в развернутом виде.

Параметры `Start_ShowNetPlaces` и `Start_ShowHelp` могут принимать только два значения:

- `0` — не отображать соответствующий параметру пункт меню;
- `1` — отображать соответствующий параметру пункт меню.

Таблица 3.1. *Параметры, влияющие на отображение пунктов расширенного меню* ***Пуск***

Пункт меню	**Параметр**
Выполнить (Run)	`REG_DWORD Start_ShowRun`
Избранное (Favorites)	`REG_DWORD StartMenuFavorites`
Документы (Documents)	`REG_DWORD Start_ShowMyDocs`
Изображения (Images)	`REG_DWORD Start_ShowMyPics`
Музыка (Music)	`REG_DWORD Start_ShowMyMusic`
Компьютер (Computer)	`REG_DWORD Start_ShowMyComputer`
Панель управления (Control Panel)	`REG_DWORD Start_ShowControlPanel`
Поиск (Search)	`REG_DWORD Start_ShowSearch`
Сетевые подключения (Network Connections)	`REG_DWORD Start_ShowNetConn`
Сеть (Network)	`REG_DWORD Start_ShowNetPlaces`
Справка (Help)	`REG_DWORD Start_ShowHelp`
Недавние документы (Recent Documents)	`REG_DWORD Start_ShowRecentDocs`
Администрирование (Administrative Tools)	`REG_DWORD Start_AdminToolsRoot`

Примечание

За отображение меню администрирования в меню **Пуск** (Start) отвечают два параметра: `REG_DWORD Start_AdminToolsRoot` и `REG_DWORD StartMenuAdminTools`. Первый параметр отвечает за отображение меню **Администрирование** (Administrative Tools) в меню **Пуск** (Start), а второй — в меню **Все программы** (All Programs). Второй параметр может принимать два значения: `1` — показывать меню администрирования, `0` — не показывать.

Кроме приведенных в табл. 3.3 параметров, есть еще два параметра:

- `REG_DWORD Start_LargeMFUIcons` — если параметр включен (его значение равно 1), то пункты меню **Пуск** (Start) будут представлены большими значками;
- `REG_DWORD Start_ScrollPrograms` — если этот параметр включен (его значение равно 1), то будет разрешена прокрутка меню **Все программы** (All Programs), если все пункты меню не помещаются на экране. Если же параметр выключен, то пункты меню будут отображены в несколько столбцов.

3.4.2. Другие параметры меню *Пуск*

3.4.2.1. Не отображать имя пользователя в меню *Пуск*

Чтобы имя пользователя не отображалось в меню **Пуск** (Start), нужно в раздел `HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer` добавить параметр `REG_DWORD NoUserNameInStartMenu` и присвоить ему значение `1`. Если присвоить ему значение `0` или вообще удалить этот параметр из реестра, имя пользователя будет отображаться.

3.4.2.2. Не отображать список часто используемых программ

Расширенное меню XP/Vista отображает часто используемые программы. Если вы не хотите видеть список часто используемых программ, перейдите в раздел `HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer` и найдите или создайте параметр `REG_DWORD NoStartMenuMFUprogramsList`. Если присвоить этому параметру значение `1`, Windows не будет отображать список часто используемых программ.

3.4.2.3. Список последних документов

Windows постоянно следит за вами и записывает имена файлов документов, с которыми вы работаете. На основании этих данных она формирует меню **Документы**. Это не всегда желательно.

Вы можете управлять функцией слежения с помощью двух параметров реестра:

- `REG_DWORD ClearRecentDocsOnExit` — если параметр включен (его значение равно `1`), то список последних документов будет автоматически очищен, как только вы выйдете из системы (или выключите/перезагрузите компьютер);
- `REG_DWORD NoRecentDocsHistory` — если параметр включен (его значение равно `1`), то история документов вообще вестись не будет.

Оба параметра находятся в разделе `HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`. Более удобным, конечно, является первый параметр, однако второй — более безопасный.

В разделе `HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer` есть еще один параметр, связанный со списком последних документов. Это — параметр с типом данных `REG_DWORD` и именем `MaxRecentDocs`. Его значение представляет собой максимальное количество последних документов, которое может запомнить Windows. По умолчанию используется значение 13.

3.4.3. Ускорение открытия меню

Если вам кажется, что ваше меню **Пуск** (Start) открывается слишком долго, попробуйте уменьшить задержку при открытии меню. По умолчанию она составляет 400 мс, но вы можете установить меньшее значение, скажем, 10 мс. Для этого откройте раздел реестра `HKCU\Control Panel\Desktop` и найдите параметр `REG_SZ MenuShowDelay`. Обратите внимание: этот параметр строкового типа, а не типа `REG_DWORD`.

Не нужно устанавливать для параметра `MenuShowDelay` значение 0, поскольку оно сильно нагружает процессор. Для минимальной задержки можно установить значение 1.

Также для ускорения открытия меню можно отключить выделение недавно установленных программ. Для этого в разделе `HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced` найдите или создайте параметр `REG_DWORD Start_NotifyNewApps` и установите для него значение `0`.

3.5. Включение технологии ClearType — сглаживание шрифтов

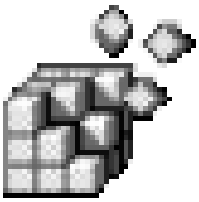
Сглаживание шрифтов (технология ClearType) значительно улучшает их отображение на экране. Существует два типа сглаживания: стандартное и ClearType. Последнее больше подходит для TFT-мониторов, на обычных шрифты будут выглядеть немного размыто.

Для установки типа сглаживания выполните следующие действия:

- перейдите в раздел `HKCU\Control Panel\Desktop` (для текущего пользователя) или в раздел `HKU\.DEFAULT\Control Panel\Desktop` (для всех пользователей);
- установите для параметра `REG_SZ FontSmoothing` значение `2` (использовать сглаживание). Если нужно отключить сглаживание, то установите для него значение `0`;
- для параметра `REG_DWORD FontSmoothingType` установите значение `1` для обычных мониторов или `2` для TFT-мониторов (сглаживание ClearType). Если установить для этого параметра значение 0, сглаживание будет отключено;
- для параметра `FontSmoothingOrientation` нужно установить значение `1`.

В следующей главе мы поговорим о параметрах Проводника Windows.

ГЛАВА 4



Параметры Проводника Windows

4.1. О параметрах Проводника

Параметры Проводника (Windows Explorer) довольно разнообразны и их очень много. Они разбросаны по всему реестру, поэтому нельзя однозначно сказать, как в случае с меню **Пуск** (Start)[1], в каком разделе их следует искать. В *главе 3* мы рассматривали все параметры — и те, которые можно настроить с помощью графического интерфейса Windows, и те, которые настраиваются только через реестр. В этой главе мы рассмотрим только те параметры Проводника, которые можно настроить через реестр.

4.2. Запуск отдельных процессов Проводника

Можно заставить Windows порождать отдельный процесс для каждого открытого окна Проводника. В этом случае системных ресурсов будет расходоваться больше, но система будет работать стабильнее.

Перейдите в раздел `HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced` и измените параметр `REG_DWORD SeparateProcess`. Если присвоить данному параметру значение `1` (значение по умолчанию — `0`), для каждого окна Проводника будет запускаться отдельный процесс.

---

[1] Хотя в Windows 7 (за исключением случаев, когда используется классическое оформление рабочего стола в стиле Windows XP) и нет уже надписи **Пуск** (Start), главное меню будем все равно называть меню **Пуск** (Start) — так проще и привычнее.

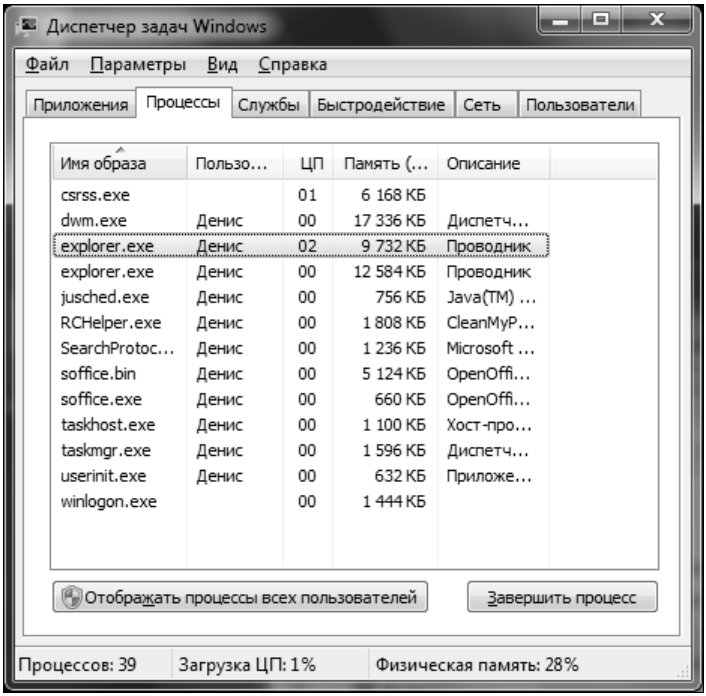


Рис. 4.1. Запущено две копии Проводника

4.3. Отключение уведомления о недостатке свободного пространства

По умолчанию, если на диске осталось меньше 10% свободного пространства, Проводник сообщит вам об этом. Иногда данная опция настолько раздражает, что пользователь готов удалить с диска все, что угодно, лишь бы уведомление о недостатке пространства больше не появлялось. Бороться с этим можно двумя способами: или снижением порога, при котором срабатывает функция уведомления, или же отключением этой функции.

Для отключения уведомления о недостатке свободного места выполните следующие действия:

1. Запустите командную строку (cmd.exe) с правами администратора. Для этого удерживайте нажатой клавиатурную комбинацию <Ctrl>+<Shift> при щелчке мышью на ярлыке cmd.exe или при запуске cmd.exe через поле поиска в нижней части меню **Пуск** (Start). После того, как вы увидите предупреждение UAC о том, что программа запускается с административными правами, разрешите запуск.

2. Введите команду `regedit`.
3. Перейдите в раздел реестра `HKEY_LOCAL_MACHINE\ OFTWARE\Microsoft \Windows Search\Gathering Manager`, щелкните на нем правой кнопкой мыши и выберите команду **Разрешения** (Permissions). Нажмите кнопку **Дополнительно** (Advanced). Перейдите на вкладку **Владелец** (Owner). Выберите учетную запись администратора и нажмите **OK**.
4. Перейдите в раздел реестра `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion \Policies\Explorer` и установите значение `1` для `REG_DWORD`-параметра `NoLowDiskSpaceChecks` (при необходимости создайте такой параметр).
5. В разделе `HKLM\SOFTWARE\Microsoft\Windows Search\Gathering Manager` измените `REG_DWORD`-параметр `BackOffLowDiskThresholdMB`: нужно присвоить ему значение `0`.
6. Перейдите в раздел `HKLM\SOFTWARE\Microsoft\Windows Search\Gather` и установите значение `0` для `REG_DWORD`-параметра `LowDiskMinimumMBytes`.

Надоедливых сообщений вы больше не увидите, однако помните, что:

- для работы системы восстановления нужно как минимум 200 Мбайт (или 300 Мбайт в Windows Vista/Windows 7) свободного места;
- для дефрагментации нужно минимум 10% свободного места.

4.4. Автоматическая перезагрузка Проводника

Это очень полезная функция, позволяющая автоматически перезагрузить процесс Проводника в случае сбоя. Откройте раздел `HKLM\Software \Microsoft\Windows NT\CurrentVersion\Winlogon` и найдите в нем параметр `REG_DWORD AutoRestartShell`. Установите для этого параметра значение, равное `1`. Для отмены этой функции нужно установить значение `0` для параметра `AutoRestartShell`. В Windows 7 автоматическая перезагрузка Проводника включена по умолчанию, но может по каким-то причинам вы пожелаете ее отключить, то будете знать, как это сделать.

4.5. Отключение записи состояния окна

По умолчанию Проводник запоминает координаты и размеры своего окна. При каждом последующем запуске окно Проводника будет иметь тот же размер и появится в том же месте, где оно располагалось на момент закрытия. Функция довольно удобная, но если вы хотите ее отключить, то это можно сделать в разделе `HKCU\Software\Microsoft\Windows\CurrentVersion\Policies`

\Explorer. Создайте параметр BINARY NoSaveSettings и задайте для него значение hex: 01 00 00 00 (рис. 4.2).

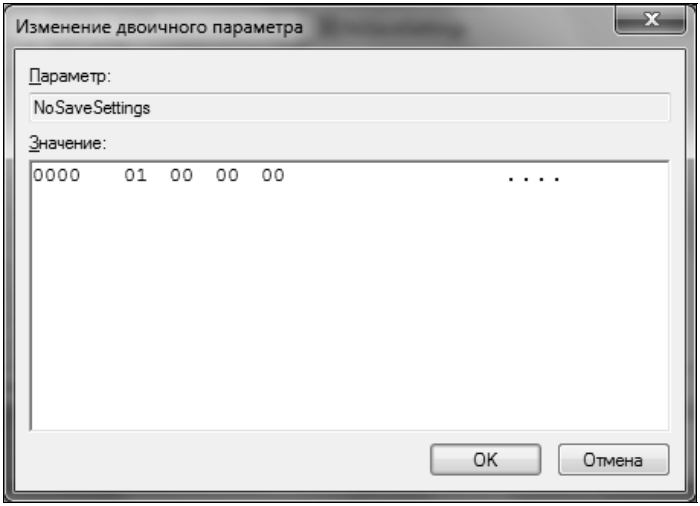


Рис. 4.2. Создание двоичного значения

4.6. Отключение кэширования изображений

Наверное, вы заметили, что в каждой папке, содержащей изображения, есть и скрытый файл thumbs.db. Windows создает такие файлы для кэширования миниатюр изображений, чтобы ускорить открытие папки в режиме **Эскизы страниц** (Page Thumbnails). Если вы хотите отключить эту возможность, тогда в разделе HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced создайте параметр REG_DWORD DisableThumbnailCache и присвойте ему значение 1.

4.7. Делаем ярлыки привлекательными

Вам нравятся стрелки в нижнем левом углу значка ярлыка? Мне тоже нет. Отключить их вывод можно очень просто. Перейдите в раздел HKLM\SOFTWARE\Classes\lnkfile и установите значение 0 для параметра REG_SZ IsShortcut (или вовсе удалите этот параметр). Об этом мы говорили в предыдущей главе, но чтобы вы лишний раз не листали книгу, решил напомнить вам об этом сейчас.

Для удаления стрелки с ярлыка DOS-программы перейдите в раздел HKLM\SOFTWARE\Classes\piffile и установите для параметра REG_SZ IsShortcut значение 0 (можно вообще удалить параметр).

При создании ярлыка к имени файла обычно добавляется строка "Ярлык для". Не каждому нравится эта строка, и многие ее удаляют. Проще вообще отключить функцию, добавляющую эту строку, чем каждый раз переименовывать ярлык. Итак, откройте раздел HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer и для параметра BINARY link установите значение hex:00,00,00,00.

4.8. Отображение содержимого окна при его перемещении по экрану

По умолчанию при перемещении окна по экрану при помощи левой кнопки мыши его содержимое продолжает отображаться в промежуточных положениях. На медленных компьютерах данную возможность можно отключить — в этом случае при перетаскивании будет отображаться только контур окна, а содержимое окна появится, когда вы отпустите левую кнопку мыши.

Перейдите в раздел HKCU\Control Panel\Desktop и установите для параметра REG_SZ DragFullWindows значение 0. Если такого параметра нет, его нужно создать. Обратите внимание на тип параметра: REG_REG_SZ, а не REG_DWORD.

4.9. Добавления команды удаления содержимого папки

Иногда нужно удалить все файлы из каталога, но не удалять сам каталог. Для этого нужно зайти в каталог, выделить все файлы, нажав клавиатурную комбинацию <Ctrl>+<A>, затем нажать клавишу <Delete>. Для упрощения данной процедуры можно создать в контекстном меню папки команду для удаления содержимого папки. Тогда вам нужно будет только щелкнуть по значку папки правой кнопкой мыши и выбрать эту команду.

Перейдите в раздел HKEY_CLASSES_ROOT\Directory\shell, создайте новый подраздел с именем Delete Folder Contents. В этом подразделе создайте еще один подраздел с именем command. Перейдите на правую панель редактора реестра и дважды щелкните на параметре по умолчанию для подраздела command. Присвойте ему следующее значение:

```
cmd /c "cd /d %1 && del /s /q *.*
```

Имейте в виду, что данная команда сразу же удаляет все содержащиеся в каталоге файлы, не помещая их в Корзину (Recycle Bin). После этого восстановить файлы можно только с резервной копии или с помощью специализированного программного обеспечения сторонних разработчиков, например, таких программ, как File Recover (**http://www.pctools.com/file-recover/**), которая поддерживает в том числе и Windows 7.

4.10. Отключение поиска подходящей программы в Интернете

Когда вы открываете файл неизвестного типа, который еще не сопоставлен ни с одной программой на вашем компьютере, Windows 7 отображает окошко, в котором предлагает вам либо найти подходящую программу в Интернете, либо выбрать программу из списка установленных программ (рис. 4.3). Вы обычно выбираете второй вариант, после чего появляется окно, изображенное на рис. 4.4.

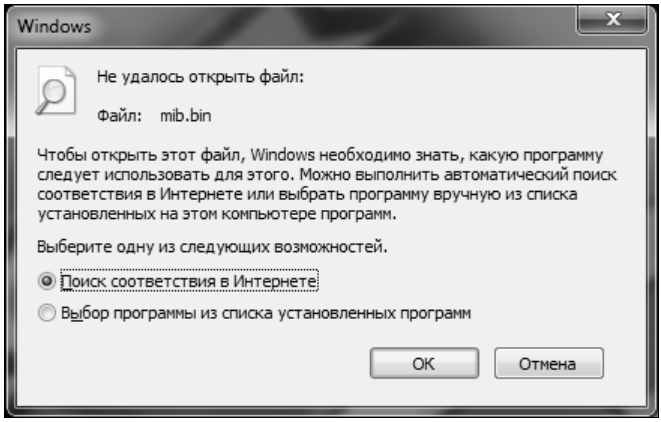


Рис. 4.3. Окно, предлагающее найти подходящую для открытия файла программу в Интернете

Вы можете отключить функцию поиска подходящей программы в Интернете, тогда вы сразу будете видеть второе окно, что в большинстве случаев более удобно. Для этого перейдите в раздел реестра `HKLM\SOFTWARE\Microsoft\Windows\ CurrentVersion\Policies\Explorer` и создайте `DWORD`-параметр `NoInternetOpenWith` со значением `1`. Чтобы вернуть все, как было, удалите этот параметр или присвойте ему значение `0`.

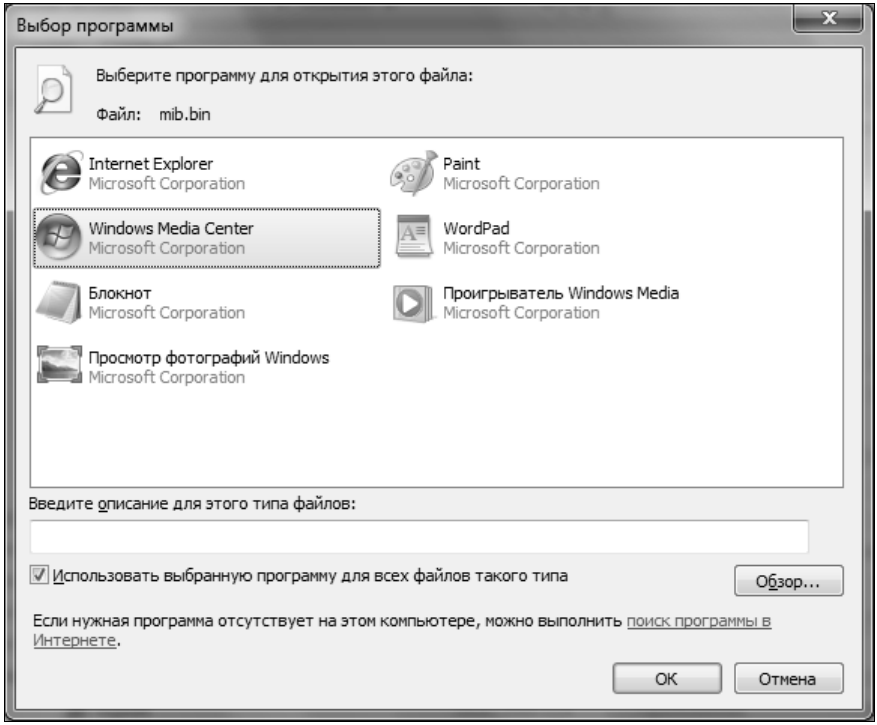


Рис. 4.4. Выбор подходящей программы из списка установленных программ

4.11. Изменение области предварительного просмотра в окне открытия файла (только для Vista)

В этом совете я покажу пример того, каким образом, редактируя реестр, можно исправить некоторые недостатки Windows Vista, чтобы хоть немного приблизить ее функциональные возможности к Windows 7.

В Windows 7 область предварительного просмотра отображает содержимое REG-файла, и вы можете с легкостью выбрать нужный вам REG-файл, например, для его редактирования в Блокноте (Notepad). В Windows Vista по умолчанию содержимое REG-файла не отображается, но путем редактирования реестра этот недостаток можно легко исправить.

Чтобы сразу было понятно, что мы собираемся сделать, взгляните на рис. 4.5 и 4.6. Первый рисунок иллюстрирует поведение Windows Vista "до", а второй — "после" модификации. На рис. 4.5 видно, что панель предварительного

просмотра не отображает содержимое REG-файла, а на рис. 4.6 панель предварительного просмотра ведет себя так же, как и в Windows 7 — вы можете просмотреть, какой REG-файл вам нужно открыть.

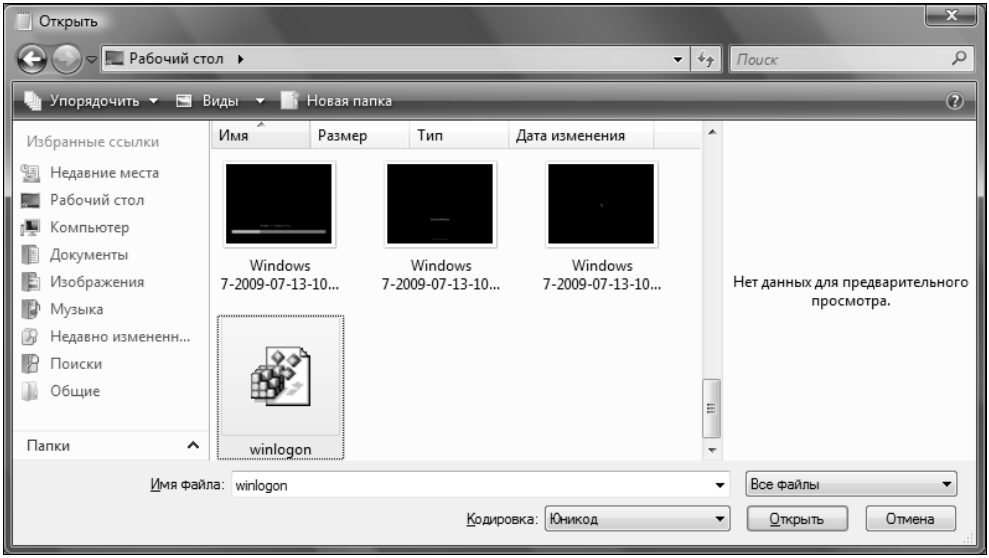


Рис. 4.5. Поведение Windows Vista до модификации

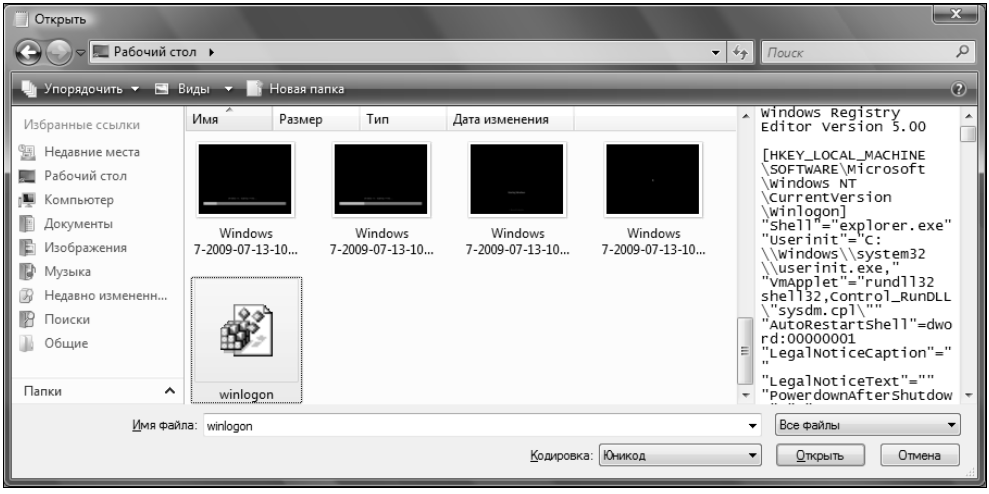


Рис. 4.6. После модификации Windows Vista тоже будет отображать в панели предварительного просмотра содержимое REG-файла

Теперь приступим к реализации задуманного. Перейдите в раздел реестра `HKEY_CLASSES_ROOT\regfile`. В этом разделе создайте новый подраздел и назовите его `shellex`.

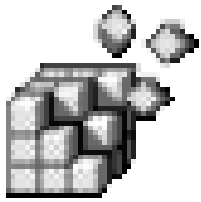
Далее в разделе `shellex` создайте подраздел `{8895b1c6-b41f-4c1c-a562-0d564250836f}`. Измените параметр по умолчанию для этого раздела. Его новое значение должно быть следующим:

```
{1531d583-8375-4d3f-b5fb-d23bbd169f22}
```

Последнее значение — это идентификатор средства предварительного просмотра текстовых файлов. Кроме этого идентификатора вы можете использовать следующие идентификаторы (возможно, вам захочется добавить предварительный просмотр для файла другого типа, а не только для REG-файла):

- `{031EE060-67BC-460d-8847-E4A7C5E45A27}` — используется для просмотра текста с форматированием (RTF);
- `{8a7cae0e-5951-49cb-bf20-ab3fa1e44b01}` — предварительный просмотр шрифтов;
- `{92dbad9f-5025-49b0-9078-2d78f935e341}` — просмотр MIME-почты.

Дополнительные обработчики предварительного просмотра могут быть найдены в разделе реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft Windows \CurrentVersion\PreviewHandlers`.



ГЛАВА 5

Активация Aero в Windows Vista/Windows 7

5.1. Что такое Aero?

Aero — это графический интерфейс пользователя (Graphical User Interface, GUI), разработанный специально для Windows Vista. Aero — это аббревиатура от Authentic, Energetic, Reflective and Open, что означает дословно "Подлинный, Энергичный, Рефлективный и Открытый". Относительно слов "Энергичный" и "Открытый" позволю себе усомниться. Исходных кодов Aero я не открывал и "бегает" Aero не очень энергично даже на современных компьютерах.

Минимальные системные требования для Aero следующие:

- процессор с частотой минимум 1 ГГц (вне зависимости от того, 32-разрядный он или 64-разрядный);
- 1 Гбайт оперативной памяти;
- видеокарта, совместимая с DirectX 9, с поддержкой Windows Display Driver Model (WDDM). На борту видеокарты должно быть не менее 128 Мбайт;
- 15 Гбайт свободного места на жестком диске;
- привод DVD-ROM;
- звуковой адаптер;
- доступ к Интернету.

Как можно видеть, предъявляемые требования довольно высоки, особенно к объему оперативной памяти и видеоадаптеру. Если ваш компьютер им не соответствует, можете даже не пытаться использовать Aero — скорее всего, у вас ничего не получится.

На мой взгляд, Aero — хороший графический интерфейс, но его системные требования явно завышены. В мире открытого программного обеспечения (Open Source) есть аналог Aero — графический интерфейс Compiz, который запускается под Linux. Так вот, Compiz мне удалось запустить на компьютере со следующей конфигурацией:

- Pentium III 833 МГц;
- 256 Мбайт RAM;
- 64 Мбайт Video.

Если интересно, вы можете увидеть Compiz в действии по следующему адресу **http://dkws.org.ua/files/video/compiz.flv**.

Для просмотра файла нужна программа FLV Player, которую можно скачать по адресу **http://rivavx.de/**.

Понятно, что без Aero вполне можно обойтись, но без него попросту не интересно. Как тогда оправдать деньги, потраченные на покупку новой версии Windows? Как оправдать деньги на покупку нового компьютера или модернизацию старого? Ведь приличный видеоадаптер стоит 100–150 долларов и дополнительно нужно 40–50 долларов на покупку еще одного модуля оперативной памяти объемом 512 Мбайт (при условии, что уже установлено 512). Выходит, нужно потратить 150–200 долларов на модернизацию компьютера, не считая затрат на приобретение новой ОС. Aero — это как раз и есть та изюминка, ради которой многие пользователи покупали Windows Vista. Других причин я не вижу — старая добрая Windows XP по-прежнему очень хорошо работает. Хочется попробовать что-то новенькое, вот и покупаются новые компьютеры — для запуска Aero, потому что без него Windows Vista, да и Windows 7, по крайней мере внешне, не намного отличается от Windows XP.

Чем же хорош Aero? Он стал более понятным, более мощным (что подтверждается в первую очередь системными требованиями), более эффектным — еще бы — "живые" пиктограммы, много анимации, добавлен эффект прозрачности окон и т. д.

Мне в Aero нравится больше всего прозрачность окон (рис. 5.1) и эффектное переключение между окнами (рис. 5.2 и 5.3).

Если вам интересно, вы можете прочитать о трехмерном кубическом виртуальном столе и даже просмотреть его в действии на этом сайте: **http://www.tweakvista.com/Article39150.aspx**.

На сайте **http://www.tweakvista.com** вы найдете полезные советы по работе с Windows Vista. Далеко не все они связаны с реестром и далеко не все полезны (некоторые из них просто очевидны, другие — читаешь и не понимаешь,

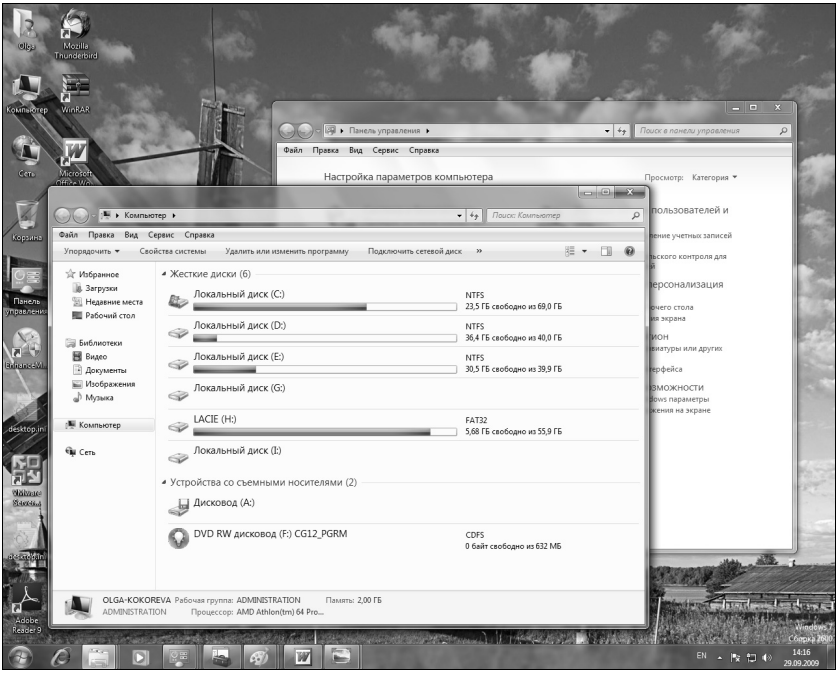


Рис. 5.1. Эффект прозрачности Aero

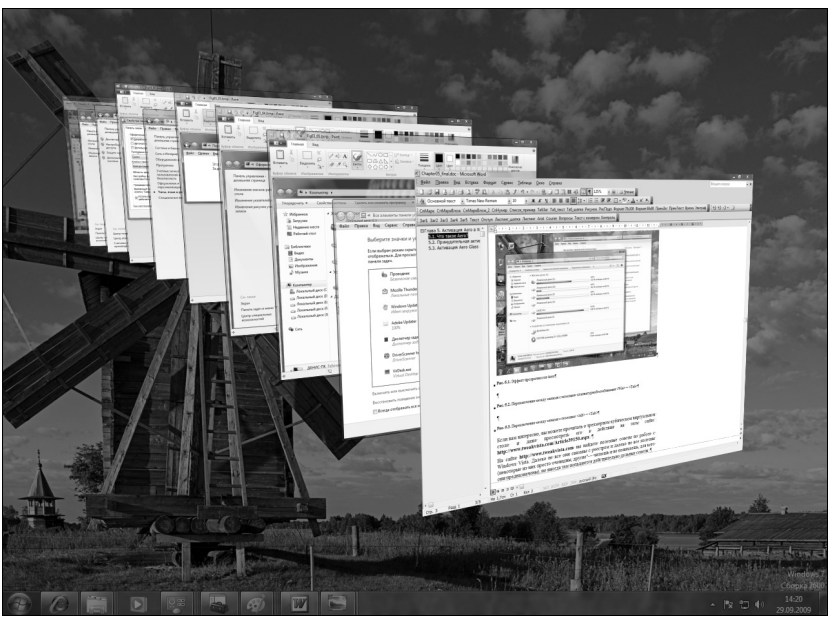


Рис. 5.2. Переключение между окнами с помощью клавиатурной комбинации <Win>+<Tab> (так называемая функция 3D Flip)

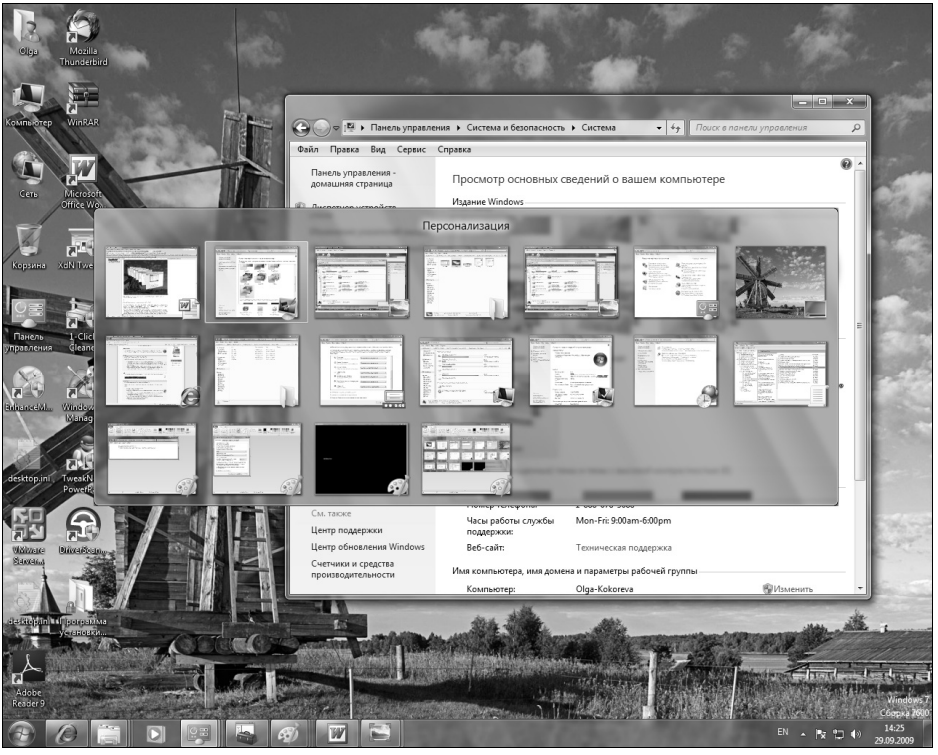


Рис. 5.3. Переключение между окнами с помощью <Alt>+<Tab>

для кого они предназначены), но иногда там попадаются действительно дельные советы.

5.2. Принудительная активация Aero в Windows 7

Windows 7 автоматически активирует Aero, если конфигурация вашего компьютера позволяет с ним комфортно работать. Однако не всегда конфигурация компьютера соответствует представлениям Windows о комфортной работе. К слову, если у вас меньше 1 Гбайт оперативной памяти, то Aero вы не активируете, но у вас может быть 1 Гбайт, но встроенная видеокарта "забрала" 128 Мбайт памяти, поэтому Aero не будет активирован по умолчанию.

По умолчанию, если индекс производительности Windows вашего компьютера равен 3.0 или превышает это значение, Windows активирует Aero. Чтобы проверить индекс производительности вашего компьютера, щелкните по кнопке **Пуск** (Start), выполните щелчок правой кнопкой мыши по пункту ме-

ню **Компьютер (**Computer) и из раскрывшегося контекстного меню выберите команду **Свойства** (Properties). На экране появится окно свойств системы, показанное на рис. 5.4. Для обновления индекса производительности Windows (Windows Experience Index, WEI) или его вычисления (если рейтинг еще ни разу не вычислялся) щелкните по ссылке **Индекс производительности Windows** (Windows Experience Index), в раскрывшемся окне нажмите кнопку **Обновить** (Update) или щелкните по ссылке **Повторить оценку** (Re-run the assessment), см. рис. 5.5.

Примечание

Кнопка **Обновить** (Update) будет присутствовать в этом окне, только если на компьютере обнаружено новое оборудование. Если этого не произошло, то в вашем распоряжении всегда остается ссылка **Повторить оценку** (Re-run assessment).

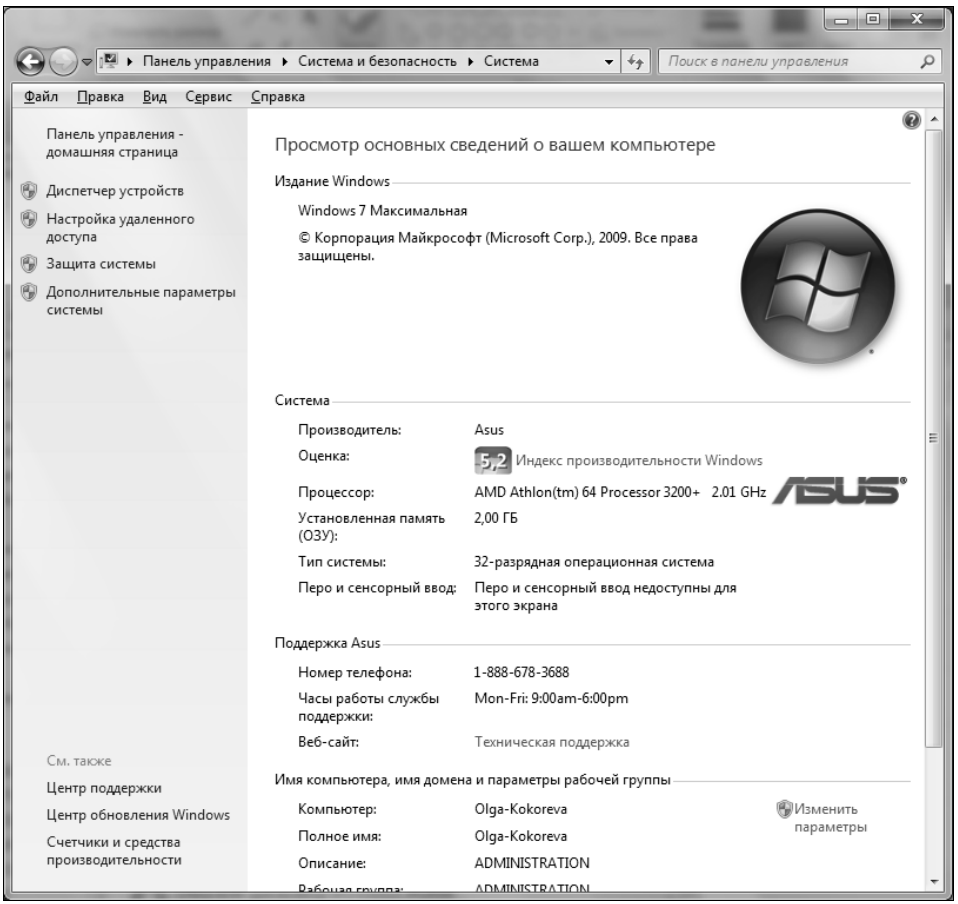


Рис. 5.4. Рейтинг компьютера больше 3.0

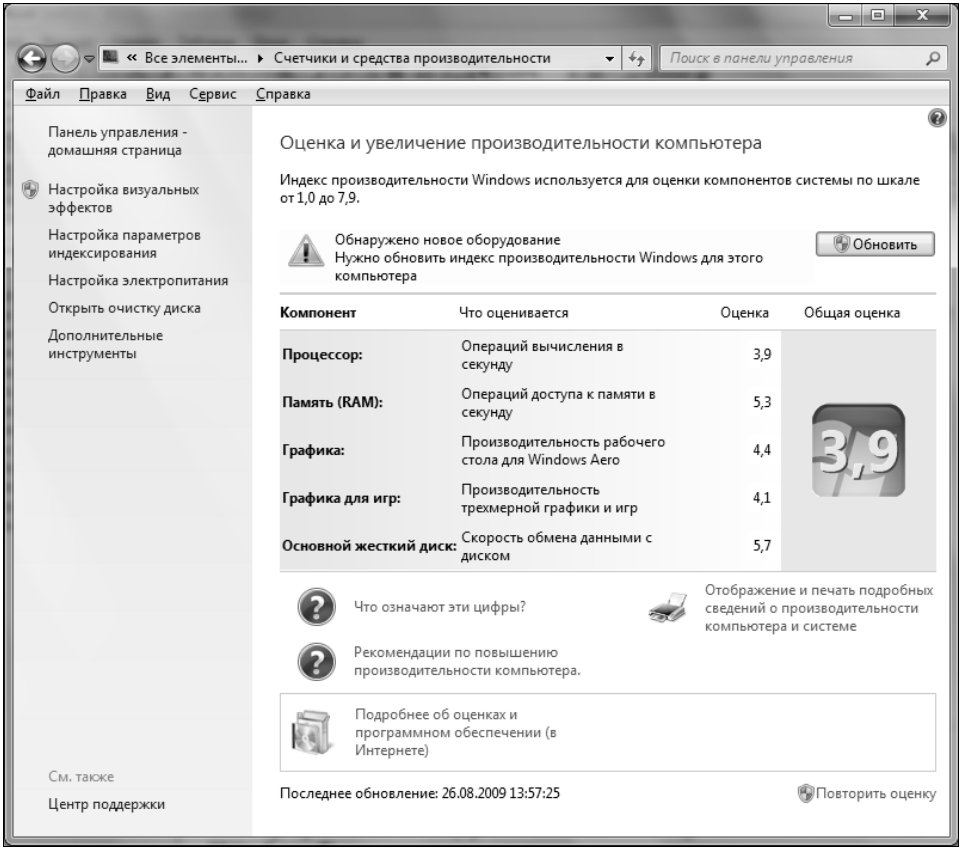


Рис. 5.5. Вычисление рейтинга компьютера

Чтобы Windows менее сурово "придиралась" к аппаратным средствам вашего компьютера, запустите редактор реестра, перейдите в раздел `HKCU\Software\Microsoft\Windows\DWM` и создайте три `DWORD`-параметра:

- `UseMachineCheck`
- `Blur`
- `Animations`

Для всех параметров нужно установить значение `0`. Нажмите кнопку **Пуск**, введите команду `cmd` и нажмите клавишу<Enter>. Введите следующие команды (вы должны зарегистрироваться в системе от имени пользователя с правами администратора):

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

Примечание

Для запуска командной строки с правами администратора нужно запустить cmd.exe, удерживая в нажатом состоянии клавиатурную комбинацию <Ctrl>+ +<Shift>, а потом подтвердить запуск программы для UAC.

Данные команды перезапустят менеджер рабочего стола (Desktop Window Manager, DWM). После этого щелкните правой кнопкой мыши на рабочем столе, выберите команду изменения свойств рабочего стола и активируйте одну из тем Windows Aero.

5.3. Активация Aero Glass в Windows Vista

Если ваша система соответствует системным требованиям Aero, то Windows Vista должна по умолчанию его активировать. Если же этого не произошло, вы можете попытаться активировать Aero самостоятельно.

Если у вас полноценная версия Vista, то вам нужно перейти в раздел реестра `HKCU\Software\Microsoft\Windows\DWM` и установить следующие параметры:

- `REG_DWORD Composition` равным `1`;
- `REG_DWORD CompositionPolicy` равным `2`.

После этого нужно перезагрузить компьютер, а после перезагрузки выполнить команды:

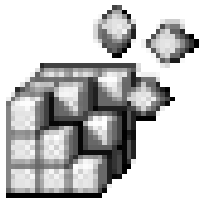
- `net stop uxsms`
- `net start uxsms`

Далее следует еще раз перезагрузить компьютер. Данный совет поможет, если ваш компьютер соответствует требованиям Aero, но Windows почему-то его не активировала.

Примечание

Если у вас есть какие-то проблемы с Windows Vista (совсем не обязательно с Aero), рекомендую обратиться на форум Microsoft — вам там обязательно помогут. Адрес форума **http://forums.microsoft.com/TechNet-RU/ShowForum.aspx?ForumID=953&SiteID=40**.

ГЛАВА 6



Повышение производительности локальной сети и интернет-соединения

6.1. Повышение производительности Интернета

На производительность интернет-соединения непосредственное влияние оказывает размер передаваемого блока данных.

Максимальный размер пакета задается параметром MTU (Maximum Transmit Unit). По умолчанию данное значение может быть установлено автоматически, но это не всегда оптимально. Если размер пакета превысит значение, допускаемое маршрутизатором провайдера, то пакет будет разделен на несколько пакетов, что, естественно, скажется на скорости и пропускной способности вашего соединения. Если размер пакета будет меньше, чем положено — это тоже нехорошо, потому что канал будет использован нерационально, ведь по нему будут передаваться полупустые кадры.

По умолчанию Windows использует размер MTU, равный 1500 байт. Это значение не очень хорошо подходит для DSL-соединений, линий T1, кабельных модемов, локальной сети и совсем не годится для обычных модемных соединений. Давайте разберемся, почему. ADSL и RadioEthernet-соединения обычно используют технологию PPPoE (PPP over Ethernet), обеспечивающую передачу PPP-кадров по Ethernet-сети. При использовании PPPoE нужно учитывать несколько факторов. Максимальный размер кадра Ethernet составляет 1518 байт, из которых 18 предназначается для заголовка и контрольной суммы, поэтому для полезных данных остается 1500 байт. Данное значение и указывается по умолчанию для Ethernet, но ведь мы собираемся передавать пакеты PPP, причем PPPoE отбирает еще 6 байт, а PPP — 2 байта. Получает-

ся, что для PPPoE значение MTU должно быть равно 1492. При установке TCP-соединения каждая сторона получает параметр MSS (Maximum Segment Size), максимальный размер TCP-сегмента. По умолчанию его размер равен MTU минус размер заголовков TCP/IP, которые занимают еще 40 байт. То есть размер MMS для PPPoE равен 1452 байта.

Как видите, значение 1500 байт не всегда соответствует действительности. Вот корректные значения MTU в зависимости от способа соединения:

- ADSL, RadioEthernet (PPPoE) — 1452;
- обычный модем — 576.

Для задания MTU перейдите в раздел `HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters`, создайте параметр с типом данных `REG_DWORD` и назовите его `MTU`. Установите для него значение, соответствующее используемому вами типу соединения (1452 или 576). Будьте внимательны: не забудьте переключить редактор реестра в десятичный вид (рис. 6.1).

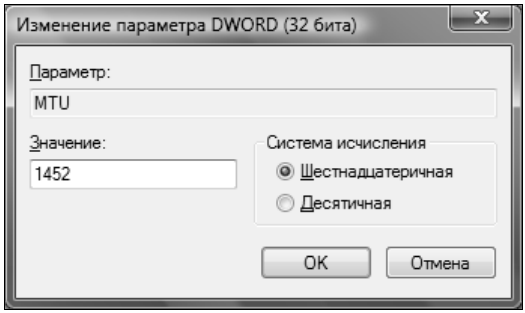


Рис. 6.1. Установка значения MTU

Если у вас не PPPoE и не обычный модем, вы можете заставить Windows автоматически вычислить значение MTU. Для этого в разделе `HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters` создайте параметр `REG_DWORD EnablePMTUDiscovery` и присвойте ему значение `1`. Если соединение начнет работать медленнее, то вы всегда можете удалить этот параметр.

Для высокоскоростных сетей с большой пропускной способностью можно включить поддержку TCP-окон размером больше 64 Кбайт. Для этого в разделе `HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters` создайте параметр `REG_DWORD Tcp1323Opts` и установите для него значение `1`.

Примечание

Чтобы описанные параметры вступили в силу, нужно перезагрузить компьютер.

6.2. Повышение производительности локальной сети

Обычно Windows самостоятельно сканирует сеть в поисках сетевых принтеров и назначенных заданий системного планировщика (Scheduled Tasks). Если отключить поиск сетевых принтеров и заданий планировщика, то можно повысить производительность локальной сети, а именно скорость доступа к компьютерам, присутствующим в сети.

Перейдите в раздел `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RemoteComputer\NameSpace`. В нем вы найдете два подраздела:

- `{2227A280-3AEA-1069-A2DE-08002B30309D}`;
- `{D6277990-4C6A-11CF-8D87-00AA0060F5BF}`.

Удаление первого раздела отключит поиск сетевых принтеров, а второго — поиск заданий планировщика.

6.3. Установка способа доступа к общим ресурсам

В разделе `HKLM\System\CurrentControlSet\Control\Lsa` содержится `DWORD`-параметр `RestrictAnonymous`, регулирующий способ доступа к общим ресурсам компьютера из локальной сети. Если этот параметр равен `1`, запрещен любой анонимный доступ. Пользователям сети не разрешено просматривать удаленно учетные записи и общие ресурсы компьютера.

Если параметр равен `2`, запрещен неявный доступ к системе. Это означает, что в сети компьютер виден не будет, но доступ к нему можно будет получить по его IP-адресу.

6.4. Другие полезные сетевые настройки

В реестре Windows можно найти множество сетевых параметров. Самые полезные сетевые параметры были собраны мною в табл. 6.1 (у всех параметров тип `REG_DWORD`).

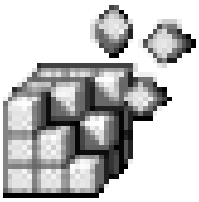
Таблица 6.1. *Самые полезные сетевые параметры*

Раздел!Параметр	Комментарий
`HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLastUserName`	Не отображать имя последнего пользователя при входе в систему (значение `1`). Значение по умолчанию — `0`

Таблица 6.1 *(окончание)*

Раздел!Параметр	Комментарий
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon \AutoAdminLogon	Автоматический вход в систему администратора (значение 1). Из соображений безопасности использовать этот параметр не рекомендуется
HKLM\System\CurrentControlSet\ Services\Tcpip\Parameters \EnableDeadGWDetect	Включить автоматическое определение "мертвых" сетевых шлюзов (значение 1)
HKLM\System\CurrentControlSet\ Services\Tcpip\Parameters \KeepAliveTime	Задает время жизни пакетов в миллисекундах. Значение по умолчанию 30 000 мс или 5 минут
HKLM\SOFTWARE\Policies\ Microsoft\Windows NT \DisablePasswordSaving	Запрещает (1) сохранение паролей
HKLM\Software\Policies\ Microsoft\Windows NT\Printers \DisableHTTPPrinting	Отключает (1) печать по http
HKLM\Software\Policies\ Microsoft\Windows NT\Printers \DisableWebPnPDownload	Запретить загрузку драйверов принтеров по HTTP (значение 1)
HKLM\Software\Policies\Microsoft\ Windows\DriverSearching \DontSearchWindowsUpdate	Отключить поиск драйверов по Windows Update (значение 1)

ГЛАВА 7



Параметры носителей данных

7.1. Сокрытие дисков

Возможно, у вас есть диски, содержимое которых вы не хотите показывать другим пользователям. Тогда можно их скрыть. Для сокрытия дисков используется параметр `REG_DWORD NoDrives` в разделе `HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`.

В качестве значения этого параметра нужно установить число, соответствующее имени диска (табл. 7.1).

Таблица 7.1. *Номера дисков*

Диск	Номер	Диск	Номер
A	1	B	2
C	4	D	8
E	16	F	32
G	64	H	128
I	256	J	512
K	1024	L	2048
M	4096	N	8192
O	16384	P	32768
Q	65536	R	131072
S	262144	T	524288
U	1048576	V	2097152
W	4194304	X	4194304
Y	16777216	Z	33554432

Если вам нужно скрыть несколько дисков, например `A` и `B`, в качестве значения параметра `NoDrives` нужно установить сумму номеров дисков, т. е. 1 + 2 = 3. Для сокрытия всех дисков используется значение 67108863.

Примечание

Как вы заметили, номер диска — это степень двойки, нумерация начинается с 0: $2^0 = 1$, $2^1 = 2$, $2^2 = 4$ и т. д. Табл. 7.1 я привожу, чтобы упростить вам вычисления.

В результате выбранные вами диски будут скрыты, но к ним все равно можно будет получить доступ, например, через Проводник (Windows Explorer), если знать имя диска. Просто введите имя диска, скажем, `D:\`, и вы получите к нему доступ. Это удобно, если за компьютером, кроме вас, работают не очень продвинутые пользователи: вы сможете работать со своими дисками без всяких проблем, а они их увидеть не смогут.

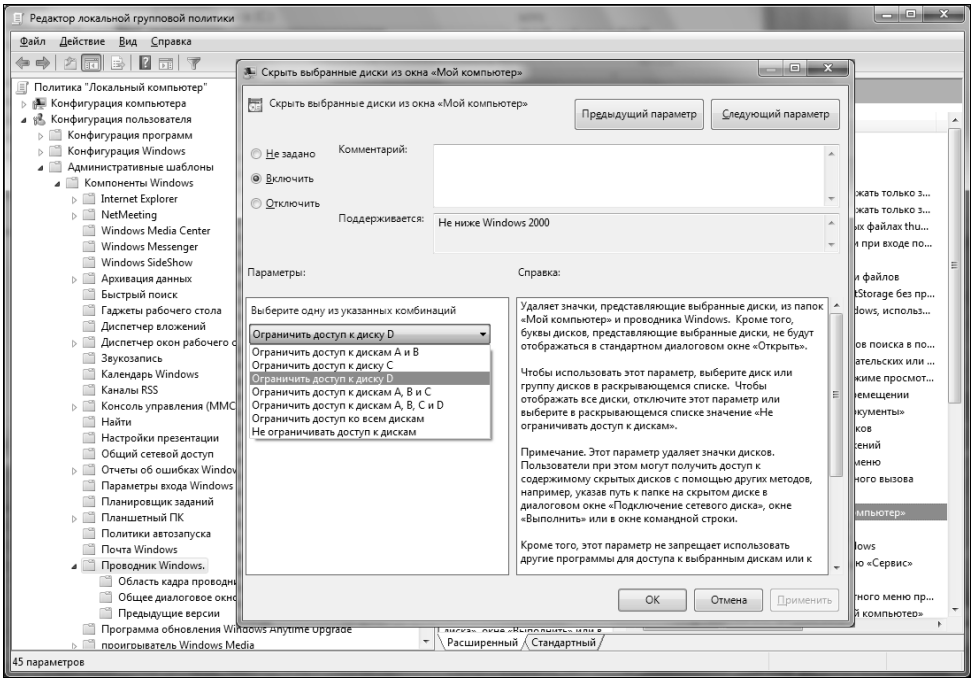


Рис. 7.1. Оснастка **Редактор локальной групповой политики** (Local Group Policy Editor) (GPEdit.msc)

Примечание

Приведенный здесь способ — далеко не единственный метод скрыть диски от глаз любопытных пользователей. Можно еще применять системные политики, но о них мы поговорим позже. Применение системных политик может быть да-

же проще, поскольку все действия выполняются через оснастку (графический интерфейс). Наиболее простой и быстрый способ запуска этой оснастки заключается в том, чтобы щелкнуть мышью по кнопке **Пуск** (Start), а затем в поле поиска ввести название оснастки — `GPEdit.msc`. Далее следует развернуть дерево консоли, как показано на рис. 7.1 — **Конфигурация пользователя** (User Configuration) | **Административные шаблоны** | (Administrative Templates) | **Компоненты Windows** (Windows Components) | **Проводник Windows** (Windows Explorer). Здесь имеются две интересующие нас политики — **Скрыть выбранные диски из окна "Мой компьютер"** (Hide these specified drives in My Computer) и **Запретить доступ к дискам через "Мой компьютер"** (Prevent access to drives from My Computer). Этот же метод работает и в предшествующих версиях Windows — Windows 2000/XP/Vista.

Можно также скрыть диск с помощью утилиты `diskpart`. Запустите сеанс работы с командной строкой с правами администратора (для этого при запуске сеанса работы с командной строкой нужно нажать и удерживать клавиатурную комбинацию <Ctrl>+<Shift>), а затем введите команду `diskpart`. Введите команду `list volume` для просмотра разделов жесткого диска. После этого нужно ввести команду `select volume [`*`номер диска`*`]` для выбора раздела диска. Для сокрытия буквы диска введите команду `remove letter [`*`буква диска`*`]`. Чтобы заново назначить диску букву, выполните те же действия, но вместо команды `remove letter` используйте команду `assign letter [`*`буква диска`*`]`.

7.2. Запрет доступа к дискам

Как быть, если за компьютером работают более продвинутые пользователи, которые если и не знают, как изменить параметр `NoDrives`, то, по крайней мере, догадаются, что нужно просто ввести букву диска, чтобы получить к нему доступ? Как они об этом догадаются? Если вы скрыли последний диск, например, `F:`, то, может, они и ничего не заметят. А вот если вы скрыли диск в "середине" списка, например, `D:`, то почти наверняка такие пользователи сообразят, что "что-то здесь не то". Как? Есть список дисков: `A:`, `C:`, `E:`, `F:`. Куда пропал диск `D:`? Давайте попробуем ввести `D:` в Проводнике... Вот и все! Поэтому можно запретить доступ без их сокрытия в списке дисков.

Для этого используется параметр `REG_DWORD NoViewOnDrive`, который находится в том же самом разделе реестра (см. *раздел 7.1*). Значение этого параметра вычисляется по табл. 7.1.

В результате выбранные вами диски будут отображаться в списке дисков, но никто (даже вы) не сможет получить к ним доступ. Чтобы диски не были видны в списке дисков, можно еще применить предыдущий параметр — так будет лучше.

Чтобы вы сами смогли получить доступ к дискам, нужно изменить параметр `NoViewOnDrive`. А чтобы ваши продвинутые пользователи не смогли запустить

редактор реестра, вам нужно создать соответствующую политику, которая будет рассмотрена далее в этой книге. Где именно она будет рассмотрена, не скажу намеренно — чтобы вы внимательнее читали книгу.

7.3. Создание виртуальных дисков средствами Windows

В Windows можно создать виртуальные диски с помощью утилиты `subst`. Для этого запустите сеанс командной строки с правами администратора и запустите команду `subst`. Данная команда использует следующий синтаксис:

```
subst имя_диска путь_к_папке
```

Например,

```
subst X: D:\disk1
```

После выполнения этой команды каталог disk1 станет корневым каталогом диска `X:`. Обратиться к файлам каталога disk1 можно будет или через каталог D:\disk1 или через диск `X:`.

Для чего это нужно? Некоторые программы установки правильно работают, только если они запущены с корневого каталога диска. Если вы скопировали программу установки и все необходимые ей файлы с компакт-диска на жесткий диск, она может работать некорректно. Вы же не скопируете ее в корневой каталог диска `C:` — некрасиво, а из подкаталога она запускаться не хочет. Записывать на компакт-диск программу установки — лень (или, как обычно, нет "болванки" под рукой), поэтому проще использовать программу `subst`. Однако имейте в виду: команда `subst` не эмулирует работу CD/DVD, так что использовать ее вместо Alcohol 120% или VirtualDrive не получится. Созданный программой `subst` диск воспринимается системой как раздел жесткого диска, а не как CD/DVD.

Для удаления виртуального диска используется параметр `/D`:

```
subst имя_диска /D
```

Если виртуальный диск вам нужен не на один раз, а на некоторое время и вы не хотите каждый день вводить команду `subst`, можно использовать реестр. Для этого добавьте в раздел `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` параметр `VirtualDrive` (тип данных — `REG_SZ`), а в качестве значения — команду вызова `subst`, например, `subst X: D:\disk1`.

Если добавить параметр `VirtualDrive` в раздел `HKLM\Software\Microsoft\Windows\CurrentVersion\Run`, то виртуальный диск будет доступен всем пользователям.

7.4. Отключение автозапуска

7.4.1. Стандартный способ

Автозапуск CD/DVD-диска — штука довольно приятная. Вы вставляете диск, Windows находит в его корневом каталоге файл autorun.inf, читает инструкции, содержащиеся в этом файле, и запускает необходимую программу-оболочку (ее имя указывается в файле autorun.inf). Программа-оболочка позволяет выполнить некоторые полезные действия, например, запустить программу установки игры или запустить демонстрационный ролик.

Так уж получается, что мы чаще работаем с дисками, которые записывали сами. А на них нет никакого файла autorun.inf. Но Windows этому не поверит и не успокоится, пока не пересмотрит все каталоги на вставленном диске. Одно дело, если это CD и файлов на нем немного, и совсем другое, если это DVD, на котором очень много файлов и каталогов. Лично мне не очень нравится наблюдать за окошком, в котором выводится индикатор поиска программы-автозапуска.

Функцию автозапуска можно отключить. Для этого перейдите в раздел `HKLM\SYSTEM\CurrentControlSet\Services\Cdrom`. В нем будет параметр `AutoRun`. Установите значение `0` для этого параметра. После этого автозапуск будет отключен.

7.4.2. Новый способ: только для Vista и Windows 7

Приведенный выше способ является стандартным. Он будет работать даже в Windows XP. Но в Windows Vista и Windows 7 используется другой способ отключения автозапуска. Перейдите в раздел реестра `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\AutoplayHandlers\CancelAutoplay\Files`. В нем находятся текстовые параметры, содержащие имя файлов. Если такие имена файлов имеются на компакт-диске, автозапуск работать не будет. Если вы добавите параметр со значением *.*, то отключите автозапуск.

7.5. Windows 7 не распознает мой DVD-привод

Если вы установили Windows 7, а она не распознает ваш DVD-дисковод и DVD-привод отмечен желтым треугольником в списке диспетчера устройств, это означает, что Windows не может контролировать цифровые подписи драйвера DVD-привода. Проблему можно решить несколькими способами.

Можно при запуске системы нажать клавишу <F8> и выбрать запуск без проверки цифровых подписей драйверов[1]. Но это не лучшее решение, ведь клавишу <F8> придется нажимать при каждой загрузке или перезагрузке системы.

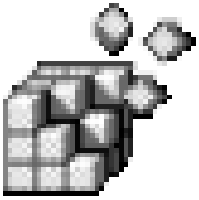
Осталось два способа. Первый заключается в редактировании реестра. Перейдите в раздел реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E965-E325-11CE-BFC1-08002BE10318}`. Удалите параметры `UpperFilters` и `LowerFilters`, после чего перезагрузите компьютер.

Второй способ заключается в следующем. Запустите сеанс командной строки (cmd.exe) с правами администратора и введите следующую команду:

```
bcdedit /set loadoptions DDISABLE_INTEGRITY_CHECKS
```

[1] Этот метод сработает только в 32-разрядных версиях Windows Vista и Windows 7, а в 64-разрядных версиях проверка цифровой подписи драйверов уже обязательна. Впрочем, исследователи уже достаточно давно научились обходить это препятствие — см. **http://bluepillproject.org/** и **http://www.invisiblethings.org**. На популярном уровне об этом рассказано в следующей книге: Касперски К., Рокко Е. Искусство дизассемблирования. — СПб.: БХВ-Петербург, 2007. — *Прим. ред.*

ГЛАВА 8



Системные параметры. Повышение производительности

8.1. Повышение производительности

Думаю, многие пользователи хотели бы сделать свою систему более быстрой и "отзывчивой" — иными словами, повысить ее производительность. В этой главе мы поговорим о параметрах реестра, позволяющих повысить производительность системы, а также о других параметрах, связанных с тонкой настройкой системы. Для вступления в силу большинства параметров, описанных в этой главе, необходима перезагрузка компьютера.

8.1.1. Ускорение работы с памятью

В реестре Windows (данный трюк подходит как для Windows XP, так и для Windows Vista/7) есть несколько параметров, влияющих на управление памятью. Сразу хочу предупредить: изменение этих параметров может существенно повысить производительность, может несущественно повысить производительность, может понизить производительность системы, а может вообще сделать систему неработоспособной. Поэтому отнеситесь к этим параметрам с особой осторожностью и внимательно читайте текст данной главы. И еще: упомянутые здесь параметры следует изменять, только если у вас большой объем оперативной памяти. Чтобы получить должный эффект, вам необходимо иметь более 512 Мбайт RAM для Windows XP и более 1 Гбайт для Windows Vista/7.

Параметры управления памятью находятся в разделе `HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management`. Вот эти параметры:

- `DisablePagingExecutive` (тип данных `REG_DWORD`) — по умолчанию выключен и его значение равно `0`. Если его включить (присвоить значение `1`),

система не будет записывать на диск при подкачке коды ядра и драйверов, а всегда будет держать их в оперативной памяти. Приложения будут быстрее реагировать на действия пользователей, поскольку не нужно будет загружать нужный приложению код ядра из файла подкачки. Но поскольку коды ядра и драйверов будут постоянно храниться в оперативной памяти, нужен большой объем физически установленной RAM;

- `LargeSystemCache` (тип данных `REG_DWORD`) — по умолчанию также выключен и его значение равно `0`. Если включить этот параметр (присвоить значение `1`), то ядро системы будет постоянно находиться в памяти, что ускорит доступ к ядру и повысит производительность всей системы. Этот параметр подойдет для машины, используемой в качестве сервера, а не для обычной рабочей станции или домашнего компьютера.

8.1.2. Выгрузка из памяти неиспользуемых DLL

Windows продолжает хранить в памяти однажды загруженные DLL, даже если они уже не используются программами. Это делается для ускорения доступа к библиотекам, но не очень экономно расходует оперативную память. Вы можете добавить параметр реестра, выгружающий неиспользуемые библиотеки из памяти. Если производительность системы, наоборот, понизится, его лучше удалить.

Параметр называется `AlwaysUnloadDll`, имеет тип `REG_DWORD` и находится в разделе `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer`. Параметру нужно присвоить значение `1`.

8.1.3. Автоматическое очищение файла подкачки

Вы можете включить параметр очистки файла подкачки (pagefile.sys) при перезагрузке (завершении работы) системы. С одной стороны, это позволит немного ускорить загрузку системы, но в то же время вы потеряете на времени завершения работы — компьютер будет выключаться медленнее. С другой стороны, в файле подкачки могут находиться конфиденциальные данные, в том числе и пароль в открытом виде, несмотря на очень тщательное шифрование файла с паролем. Поэтому файл подкачки по завершении работы лучше очищать.

Перейдите в раздел `HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management` и установите значение `1` для параметра `ClearPageFileAtShutdown`.

8.1.4. Повышение производительности системы путем запрета выгрузки драйверов

Если у вас достаточно оперативной памяти (хотя бы 2 Гбайт), можно увеличить производительность системы, запретив выгружать из оперативной памяти на жесткий диск код драйверов и другой служебный, но не используемый в данное время код. Перейдите в раздел `HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management` и создайте параметр `DisablePagingExecutive` (тип данных — `REG_DWORD`) со значением `1`.

8.1.5. Ускорение завершения работы системы

При завершении работы помимо всего прочего система завершает запущенные сервисы (службы). Если сервис не отвечает, то система выжидает некоторое время, а потом завершает службу.

Ускорить завершение работы можно путем уменьшения времени ожидания. Создайте в разделах реестра `HKLM\SYSTEM\CurrentControlSet\Control`, `HKLM\SYSTEM\CurrentControlSet001\Control` и `HKLM\SYSTEM\CurrentControlSet002\Control` строковый (`REG_SZ`) параметр `WaitToKillServiceTimeout`. Его значение — это время в миллисекундах, которое система будет ждать перед завершением службы. По умолчанию система ждет 20 секунд, т. е. 20 000 миллисекунд. Это слишком долго, вполне достаточно 10 секунд, т. е. 10 000 миллисекунд.

8.1.6. Отключение планировщика Windows

В Windows есть специальная программа — планировщик, выполняющая задания (другие программы) в определенное время. Обычно планировщиком никто никогда не пользуется, а поэтому его можно отключить, что сократит время загрузки Windows[1].

Чтобы отключить планировщик, перейдите в раздел `HKLM/SYSTEM/CurrentControlSet/Services/Schedule`, найдите параметр `Start` (тип данных — `REG_DWORD`) и установите для него значение `0`. Чтобы вернуть все в исходное состояние, нужно установить значение `2`.

---

[1] На самом деле от данного сервиса в Windows Vista и Windows 7 зависят такие важные системные задачи, как, например, резервное копирование, создание точек восстановления системы, регулярный запуск Windows Defender, сканирование системы антивирусными программами по расписанию и др. Сразу после блокирования сервиса ничего ужасного, конечно, не произойдет, зато потом могут начаться проблемы. А выигрыш по скорости загрузки был настолько ничтожным, что я его просто не заметила. — *Прим. ред.*

8.1.7. Увеличение производительности NTFS

Можно долго спорить о том, какая файловая система лучше — FAT32 или NTFS[1]. С моей точки зрения — однозначно NTFS. Она обеспечивает должный уровень безопасности и предоставляет возможности, которые не доступны в FAT32, кроме того, она поддерживает файлы больших размеров. В Windows XP максимальный размер файла для FAT32 — 4 Гбайт. А что делать, если вам нужно создать файл большего размера? Ведь рано или поздно вам придется создать образ DVD, а это уже 4,5 Гбайт!

Хотя у FAT32 также есть свои преимущества — она работает быстрее, чем NTFS. Но делу можно помочь. NTFS медленнее, чем FAT32, только потому, что:

- при каждом обращении к файлу или каталогу ей приходится обновлять метку последнего доступа. При большом количестве файлов или каталогов это снижает производительность системы;
- для совместимости со старыми приложениями в NTFS-разделе создается специальная таблица файлов, содержащая имена файлов в формате MS-DOS (как известно, это 8 символов для имени и 3 — для расширения файла). Не думаю, что вы до сих пор используете настолько древние приложения, поэтому можно смело отключить эту возможность, что положительно отразится на производительности.

Итак, для повышения производительности NTFS нужно перейти в раздел `HKLM\SYSTEM\CurrentControlSet\Control\FileSystem` и установить значение `1` для следующих параметров:

- `NtfsDisableLastAccessUpdate`;
- `NtfsDisable8dot3NameCreation`.

Первый параметр отключает запись последнего времени доступа, а второй — создание таблицы для совместимости со старыми приложениями. Для большей производительности можно дополнительно включить параметр `NtfsDisableEncryption`, но с точки зрения безопасности это не следует делать, потому что он отключает шифрование данных, обеспечиваемое файловой системой NTFS.

---

[1] Хотя многие пользователи (особенно те, кто создает мультизагрузочные системы) действительно продолжают пользоваться FAT32, Microsoft, со всей очевидностью, уже считает эту тему закрытой. Уже сейчас FAT32 поддерживается исключительно для обратной совместимости, а также всячески ущемляется и дискриминируется. Она даже не поддерживается средствами резервного копирования и восстановления, встроенными в Windows Vista и Windows 7, о чем не мешает помнить поклонникам мультизагрузки. — *Прим. ред.*

8.1.8. Включить поддержку UDMA-66 на чипсетах Intel

Внимание: данный трюк предназначен только для материнских плат, основанных на чипсетах Intel, и жестких дисков IDE (не SATA). Убедитесь также, что ваш жесткий диск поддерживает UDMA-66 и подключен к материнской плате с помощью кабеля 80-pin.

Если параметры вашего оборудования отвечают указанным требованиям, создайте в разделе `HKLM\System\ CurrentControlSet\Control\Class\{4D36E96A-E325-11CE-BFC1-08002BE10318}\0000` параметр с типом данных `REG_DWORD` и именем `EnableUDMA66`. Присвойте ему значение `1`.

8.1.9. Отключаем неиспользуемые сервисы

8.1.9.1. Зачем нужно отключать лишние сервисы?

Служба (или сервис, от англ. service) — это специальная программа, выполняющаяся в фоновом режиме и не имеющая пользовательского интерфейса. В большинстве случаев каждая служба представляет собой важный компонент операционной системы, без которого она не может функционировать. Значительно реже свои собственные службы добавляют программы посторонних разработчиков, например, Антивирус Касперского, Outpost Security Suite и другие программы.

Некоторые из служб можно отключить, однако к этому процессу следует подходить с осторожностью, чтобы случайно не отключить важную системную службу[1].

Каждая служба, даже если она просто находится в памяти и ничего не делает, занимает оперативную память и процессорное время. Следовательно, при отключении неиспользуемых служб мы оптимизируем работу оперативной памяти и процессорного времени, благодаря чему наш компьютер будет работать быстрее. Однако не нужно думать, что если вы отключите одну службу, то ваш компьютер сразу же начнет "летать". Одна служба ничего не решит. Нужно подойти к процессу отключения служб комплексно.

Надо понимать, что повышение производительности — далеко не единственная причина отключения неиспользуемых служб. Некоторые службы потенциально опасны, т. е. могут использоваться для атаки вашего компьютера

[1] Добавлю, что если вам хочется повысить производительность системы, блокировав некоторые неиспользуемые сервисы, то имеет смысл прочесть следующий источник: **http://www.computingunleashed.com/2009/02/list-of-services-in-windows-7-that-can.html**. — *Прим. ред.*

злоумышленником. Конечно, если установлен брандмауэр, то ваш компьютер находится в относительной безопасности, а вот если вы блокировали встроенный брандмауэр и не используете никакого стороннего, то желательно отключить некоторые службы.

Итак, рассмотрим отключение неиспользуемых служб, как средство повышения производительности компьютера и его защиты от атак.

8.1.9.2. Как отключить сервис?

Для управления службами используется специальная программа, для запуска которой нужно нажать кнопку **Пуск** (Start) и ввести в поле поиска, расположенное в нижней части меню, команду `services.msc`. Раскроется окно, показанное на рис. 8.1.

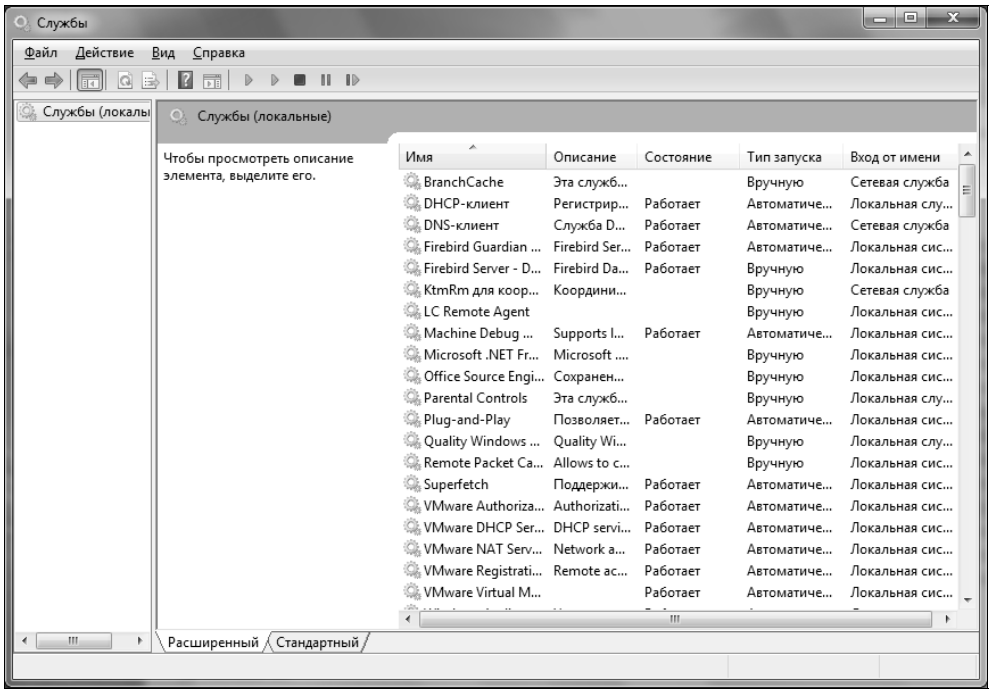


Рис. 8.1. Программа управления службами в Windows 7

В колонке **Имя** (Name) приводится название службы, в колонке **Описание** (Description) — описание функций, для выполнения которых она предназначена. Для более удобного просмотра описания можно щелкнуть по имени службы, а потом прочитать его в левой части окна.

Колонка **Состояние** (Status) отображает текущее состояние службы: если она работает, то вы увидите соответствующее сообщение.

Колонка **Тип запуска** (Startup Type) отображает способ запуска службы:

- **Автоматически** (Auto) — служба запускается автоматически при запуске Windows;
- **Автоматически (отложенный запуск)** (Automatic (Delayed Start)) — новый вид запуска служб, появившийся, начиная с Windows Vista, и, безусловно, применяющийся и в Windows 7. Он используется для тех сервисов, которые выполняют важные функции, но не нужны пользователю немедленно после регистрации в системе. Такие сервисы запустятся чуть позднее, и за счет этого система будет быстрее готова к регистрации пользователя;
- **Вручную** (Manual) — служба не запускается автоматически при запуске Windows, однако может быть запущена вручную пользователем или другой службой (т. е. это так называемый запуск по требованию);
- **Отключена** (Disabled) — служба вообще не запускается. Если данная служба понадобится, то сначала придется изменить тип запуска на автоматический, автоматический с отложенным запуском или ручной.

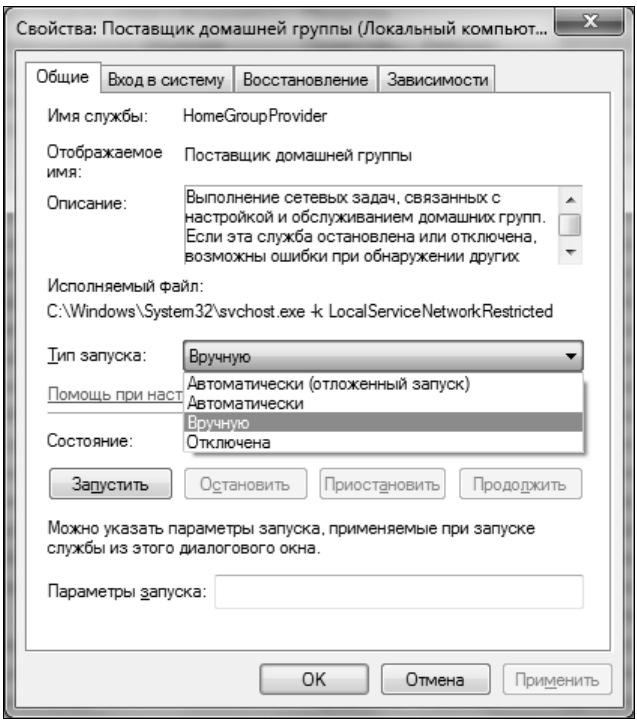


Рис. 8.2. Свойства службы

Для изменения типа запуска дважды щелкните по строке с нужной службой и выберите требуемый тип запуска, например, **Отключена** (Disabled) для полного отключения (рис. 8.2). Если служба запущена, то будет активна кнопка **Стоп** (Stop), которая используется для остановки службы. Останавливать службу перед ее отключением не нужно — Windows это сделает автоматически.

Для каждой службы приводится ее довольно подробное описание. Если вы знаете, что служба вам не нужна, ее можно отключить. Если вы не уверены, можно найти дополнительную информацию о службе в Интернете (поиск Гуглом еще никто не отменял)[1].

Лучше всего отключать службы поэтапно: отключите некоторые из них, запомните, что именно вы отключили. Затем немного поработайте, чтобы убедиться, что система работает корректно. Если какие-то нужные вам функции оказались недоступны, вновь включите ранее отключенные вами службы.

8.2. Настройка автозапуска программ

Для автоматического запуска программ используются следующие разделы реестра:

- `HKCU\Software\Microsoft\Windows\CurrentVersion\Run`;
- `HKCU\Software\Microsoft\Windows\CurrentVersion\Runonce`;
- `HKLM\Software\Microsoft\Windows\CurrentVersion\Run`;
- `HKLM\Software\Microsoft\Windows\CurrentVersion\Runonce`;
- `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx`.

Как мы уже говорили, разделы в `HKCU` содержат настройки для текущего пользователя, а в `HKLM` — для всех пользователей системы.

В разделы `Run` включены списки программ, которые автоматически запускаются при каждом входе пользователя в систему. В отличие от него, программы, содержащиеся в разделах `Runonce`, будут запущены только один раз при входе пользователя в систему, после чего этот список будет очищен. Раздел `RunonceEx` аналогичен `Runonce` с тем отличием, что программы из их списков будут выполнены один раз при загрузке системы, а не при входе определенного пользователя.

Теперь о том, как формируются списки автозапуска. Каждый список — это набор параметров типа `REG_SZ`. Имя параметра произвольное, а его значение — команда, которую нужно выполнить (рис. 8.3).

---

[1] Вот, например, очень хороший и заслуживающий доверия источник информации о службах Windows всех версий — начиная с Windows 2000 и заканчивая Windows 7: **http://www.blackviper.com/**. — *Прим. ред.*

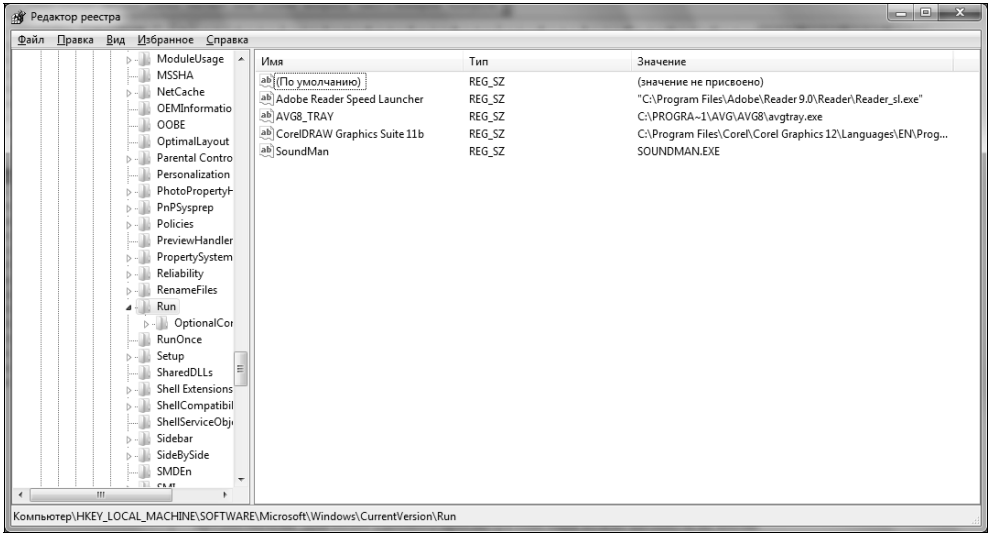


Рис. 8.3. Список автозапуска

Для добавления программы в список автозапуска нужно создать параметр типа `REG_SZ`, содержащий команду для запуска программы. Чтобы удалить программу из списка автозапуска, достаточно удалить соответствующий ей параметр из раздела (или разделов) `Run*`.

Для управления автозапуском также используются следующие параметры:

- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\` — параметр `DisableCurrentUserRun` — если параметр включен (его значение равно `1`), то пользовательский список `Run` из `HKCU` не будет выполнен;
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\` — параметр `DisableCurrentUserRunOnce` — отключает пользовательский список `RunOnce` из `HKCU`;
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\` — параметр `DisableLocalMachineRun` — отключает "общий" список автозапуска `Run` из `HKLM`;
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\` — `DisableLocalMachineRunOnce` — отключает "общий" список автозапуска `RunOnce` из `HKLM`.

8.3. Удаление программ из списка установленных (Uninstall своими руками)

Для удаления сведений об установке программы из реестра перейдите в раздел реестра `HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall`. В нем будут подразделы с именами, содержащими цифры и буквы, например, `{01B28B7B-EEC6-12D5-5B5A-5A7EBDF5EFBA}`, см. рис. 8.4.

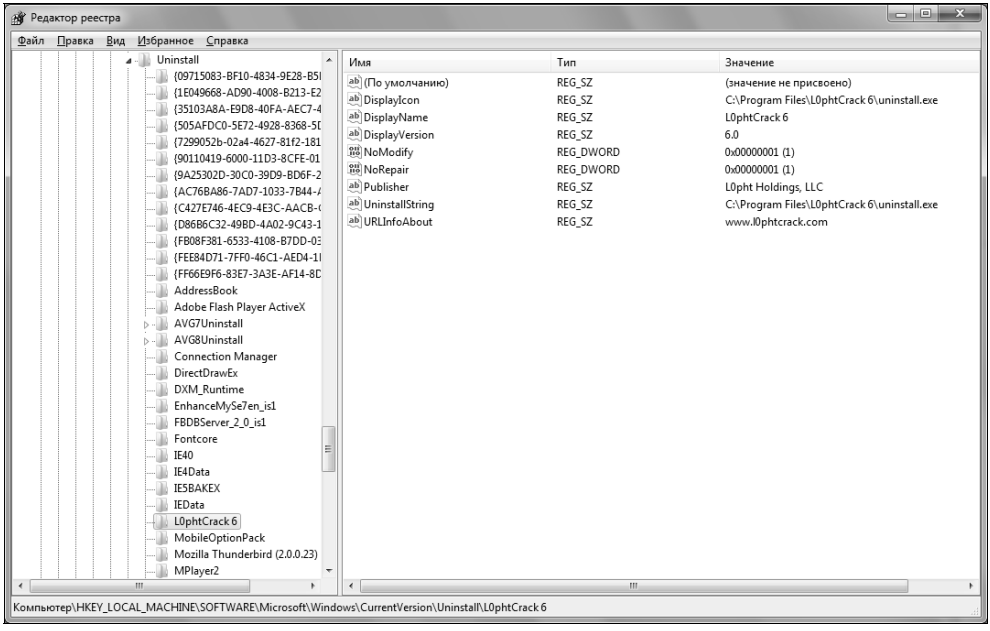


Рис. 8.4. Сведения об установленных программах

Каждый такой раздел соответствует какой-то программе. Какой именно? Имя программы содержится в параметре `DisplayName`. Например, у меня раздел `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{C427E746-4EC9-4E3C-AACB-C6BB1F714D7F}` соответствует программе Uniblue DriverScanner 2009.

Перед удалением раздела рекомендуется экспортировать этот раздел в REG-файл, чтобы в случае чего у вас была возможность его восстановить. Как только раздел будет экспортирован, можно его удалить.

8.4. Что делать с зависшими программами?

Иногда программы зависают, и их невозможно закрыть обычным образом. Тогда приходится открывать **Диспетчер задач** (Windows Task Manager), искать зависший процесс в числе работающих и вручную его завершать. Запустить Диспетчер задач (Windows Task Manager) проще всего одновременным нажатием клавиш <Ctrl>+<Shift>+<Esc>). Можно настроить Windows и таким образом, чтобы она автоматически завершала зависшие процессы. Для этого перейдите в раздел `HKCU\Control Panel\Desktop`. В этом разделе вы найдете следующие параметры:

- `AutoEndTasks` (`REG_DWORD`) — если присвоить этому параметру значение `1`, то Windows будет автоматически завершать зависшие задачи;
- `HungAppTimeout` (`REG_SZ`) — период, по прошествии которого можно считать приложение зависшим. Время отсчитывается с момента, когда приложение перестало отвечать на запросы операционной системы. По умолчанию оно равно 5000 мс или 5 с;
- `WaitToKillAppTimeout` (`REG_SZ`) — период ожидания перед завершением процесса (вдруг он "одумается"). По умолчанию это значение составляет 20 000 мс или 20 с.

Сложив значения параметров `HungAppTimeout` и `WaitToKillAppTimeout`, можно заметить, что по умолчанию Windows понадобится 25 с, чтобы завершить процесс.

А теперь немного практики. Чаще всего приложения зависают, ожидая ответа от какого-нибудь устройства или другого процесса. При этом бывает и так, что ожидаемое приложение не отзывается из-за большой загруженности процессора. Срок продолжительностью 5 секунд недостаточен для того, чтобы сделать вывод о том, что программа зависла. Нужно увеличить значение параметра `HungAppTimeout` до 10 000, т. е. 10 с. Если прошло 10 секунд, и нужное приложение не отзывается на запросы системы, его можно смело завершать. Вообще говоря, можно задать для параметра `WaitToKillAppTimeout` значение `0`, но лучше все-таки немного подождать, хотя бы 5 секунд, т. е. 5000 мс.

В целом, Windows 7 довольно хорошо справляется с зависшими программами, но на всякий случай лучше знать, где находятся параметры аварийного завершения программ. До недавнего времени я тоже думал, что Windows 7 неуязвима, но вчера попытался подключить свой телефон, чтобы скачать с него фотографии. Фотографии были успешно скачаны, но, когда я отключил телефон от компьютера, увидел синий экран смерти. В Windows 7 я его до этого не видел и искренне надеялся, что и не увижу.

8.5. Служба SuperFetch

Служба SuperFetch позволяет ускорить выполнение программ, с которыми вы часто работаете. Служба работает так: она помещает файлы программ, которые вы часто используете. За счет этого достигается ускорение запуска программ, ведь практически все необходимые файлы уже загружены службой SuperFetch.

Служба ведет себя довольно интеллектуально и запоминает, какие программы и когда вы запускаете. Скажем, если вы на выходных играете в Diablo II, а в будние дни преимущественно работаете с офисными приложениями, то файлы игры не будут загружены в будни, ровно как и файлы офисных приложений не будут загружены на выходных. Так достигается экономия оперативной памяти (понятно, что если загрузить в нее сразу все программы, с которыми вы работаете, то производительность будет оставлять желать лучшего).

Если оперативной памяти в компьютере мало (скажем, 1 Гбайт или меньше), то служба для ускорения работы системы может использовать флэш-память. Да, она медленнее оперативной памяти, но быстрее жестких дисков (правда, не все модели, а те, которые поддерживают технологию Windows ReadyBoost). Чтобы служба SuperFetch использовала флэш-носитель, подключите флэшку к компьютеру, а затем в окне автозапуска (AutoPlay) выберите команду **Ускорить работу системы** (Speed up my system) (рис. 8.5).

Настройки службы SuperFetch хранятся в разделе `HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters`. В этом разделе вы найдете три параметра типа `REG_DWORD`:

- `EnableBootTrace` — включает трассировку работы службы SuperFetch, значение по умолчанию — 0, т. е. трассировка выключена. Трассировка нужна только в том случае, если служба работает не так, как должна.
- `EnablePrefetcher` — определяет, будет ли включен механизм Prefetcher (механизм упреждающей выборки).
- `EnableSuperfetch` — определяет, будет ли включена служба SuperFetch.

Последние два параметра могут принимать четыре значения:

- `0` — функция выключена;
- `1` — функция включена, но только для загрузки системы;
- `2` — функция будет доступна только во время работы системы, но будет отключена при загрузке системы;
- `3` — функция будет доступна как во время загрузки, так и во время работы системы.

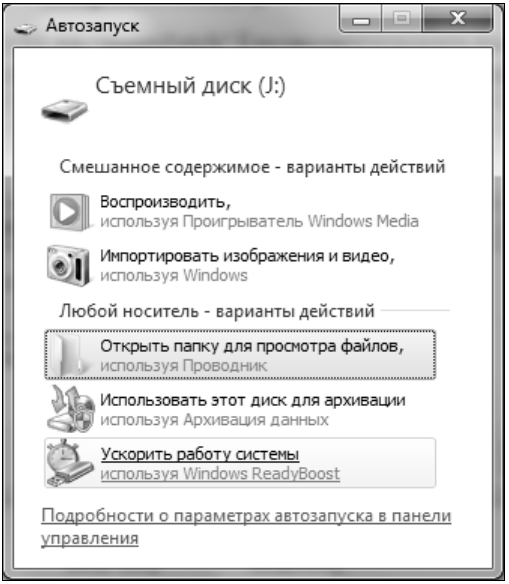


Рис. 8.5. Окно автозапуска для флэшки

8.6. Уменьшение фрагментации больших файлов

Параметр `ContigFileAllocSize` (тип `REG_DWORD`) раздела `HKLM\System\CurrentControlSet\Control\FileSystem` задает максимальный размер нефрагментируемого блока данных (в байтах). Этот параметр используется для того, чтобы система перед записью большого файла нашла сначала для него то место, на котором файл окажется в наименьшей степени фрагментированным. По умолчанию система начинает записывать файл на первый же обнаруженный фрагмент свободного пространства. Записав несколько частей файла, система обнаруживает, что следующие блоки заняты. Затем она начинает искать следующий свободный блок. Вполне может получиться и так, что первая часть файла физически записана в "начале" диска, вторая — в середине, а третья — в конце. Все это замедляет последующую работу системы с этим файлом — снижается скорость его чтения и записи. Когда же система будет последовательно (по возможности) располагать фрагменты файла, это снизит фрагментацию и повысит общую производительность системы.

Осталось только подобрать значение параметра `ContigFileAllocSize`. Для небольших жестких дисков (до 15 Гбайт) нужно установить значение `00000200`. Если объем жесткого диска 20–40 Гбайт — `00000400` или `00000600`. Для жест-

ких дисков размером 40 Гбайт и выше — `00001000`. Экспериментируйте со значением этого параметра, чтобы добиться максимальной производительности.

8.7. Выключение автоматического обновления Windows

По умолчанию Windows обновляет себя, не спрашивая об этом разрешения пользователя. Не верите? Установите брандмауэр Outpost Security Suite Pro и включите контроль компонентов. В среднем 2–3 раза в день вы будете видеть сообщение о том, что компоненты приложений изменены. Иногда приложения обновляют сами себя сами, а иногда "старается" именно служба автоматического обновления Windows.

В разделе `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update` находятся параметры автоматического обновления:

- `AUOptions` (`REG_DWORD`);
- `AUState` (`REG_DWORD`).

Отключить автоматическое обновление можно, присвоив следующие значения этим параметрам:

- `AUOptions` = `1`;
- `AUState` = `7`.

Если вы хотите только получать сообщения о возможности загрузки обновлений, измените данные параметры так:

- `AUOptions` = `2`;
- `AUState` = `2`.

Если нужно загружать обновления, а потом только уведомлять об их готовности к установке, то установите следующие значения указанных параметров:

- `AUOptions` = `3`;
- `AUState` = `2`.

8.8. Установка пути к дистрибутиву Windows

Вы скопировали дистрибутив на жесткий диск, а Windows по-прежнему его ищет на DVD? Измените параметр реестра `SourcePath` (`REG_SZ`) в разделе

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup. В качестве значения этого параметра укажите путь к дистрибутиву Windows.

8.9. Установка пути к каталогу *Program Files*

Путь к каталогу, в который по умолчанию устанавливаются все программы и по умолчанию называется C:\Program Files, задается строковым параметром ProgramFilesDir в разделе HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion (рис. 8.6).

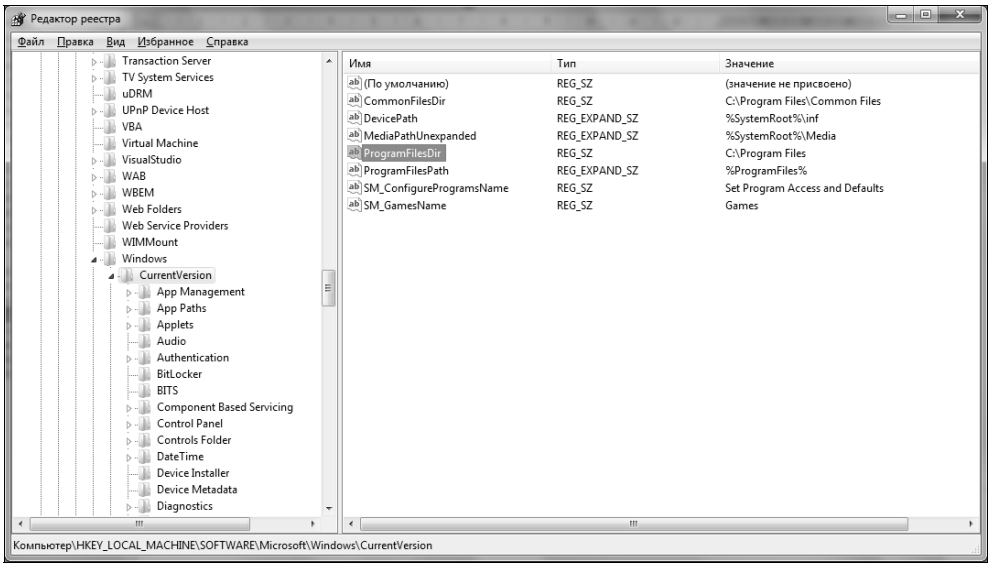


Рис. 8.6. Путь к каталогу Program Files

8.10. Настройка службы времени

Если вы используете службу времени, то можете настроить интервал синхронизации часов компьютера с сервером времени. Для этого перейдите в раздел HLKM\SYSTEN\CurrentControlSet\Services\W32Time\TimeProviders\NtpClient и установите значение параметра SpecialPollInterval (REG_DWORD). Его значение задается в секундах.

8.11. Что делать в случае отказа системы

В случае отказа системы Windows позволяет настроить выполнение следующих действий:

- автоматическая перезагрузка — параметр `AutoReboot` (`REG_DWORD`);
- запись события в системный журнал — параметр `LogEvent` (`REG_DWORD`);
- отправка административного сообщения — параметр `SendAlert` (`REG_DWORD`);
- запись отладочной информации `CrashDumpEnabled` (`REG_DWORD`).

Самым полезным является первый параметр, позволяющий перезагружать компьютер в случае отказа Windows. Запись события в системный журнал бессмысленна — от того, что в журнал будет записано сообщение об отказе системы, легче вам не станет, тем более что причина сбоя не указывается. Если хотите знать причину сбоя, то нужно включить последний параметр — запись дампа памяти, но чтобы понять причину по дампу памяти, нужно быть настоящим гением. Отправка административного сообщения тоже не нужна.

Итак, включим автоматическую перезагрузку компьютера в случае сбоя. Для этого перейдите в раздел `HKLM\SYSTEM\CurrentControlSet\Control\CrashControl` и присвойте параметру `AutoReboot` значение `1`.

8.12. Исправление ошибки инсталлятора в Windows 7

Некоторые приложения невозможно установить в Windows 7 — их установка приводит к краху инсталлятора Windows. Если при установке программы произошла ошибка (имеются в виду только MSI-инсталляторы), запустите редактор реестра и удалите раздел `HKLM\SOFTWARE\Microsoft\SQMClient\Windows\DisabledSessions`. После этого повторите попытку установки программы.

8.13. Комплексная доработка Windows 7

Рассмотрим REG-файл, выполняющий следующие действия:

- отключает уведомление о нехватке дискового пространства;
- ускоряет работу IE 8 путем отключения поиска сетевых принтеров и сетевых заданий;

- добавляет команды "**Move To**" (Переместить в) и "**Copy To**" (Копировать в) в контекстное меню;
- уменьшает время открытия меню;
- ускоряет завершение зависших процессов;
- добавляет команду "**Take Ownership**" (Изменить владельца) в контекстное меню каталога, что позволит быстро изменить владельца каталога.

Содержимое REG-файла приведено в листинге 8.1.

Листинг 8.1. Шесть трюков реестра в одном REG-файле

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies
\Explorer]
"NoLowDiskSpaceChecks"=dword:00000001
"LinkResolveIgnoreLinkInfo"=dword:00000001
"NoResolveSearch"=dword:00000001
"NoResolveTrack"=dword:00000001
"NoInternetOpenWith"=dword:00000001

[HKEY_CLASSES_ROOT\AllFilesystemObjects\shellex\ContextMenuHandlers
\Copy To]
@="{C2FBB630-2971-11D1-A18C-00C04FD75D13}"

[HKEY_CLASSES_ROOT\AllFilesystemObjects\shellex\ContextMenuHandlers
\Move To]
@="{C2FBB631-2971-11D1-A18C-00C04FD75D13}"

[HKEY_CURRENT_USER\Control Panel\Desktop]
"AutoEndTasks"="1"
"HungAppTimeout"="1000"
"MenuShowDelay"="8"
"WaitToKillAppTimeout"="2000"
"LowLevelHooksTimeout"="1000"

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control]
"WaitToKillServiceTimeout"="1000"

[-HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer
\RemoteComputer]
```

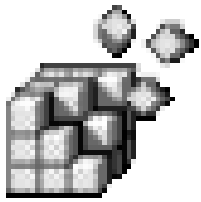
```
[HKEY_CLASSES_ROOT\*\shell\runas]
@="Take Ownership"
"NoWorkingDirectory"=""

[HKEY_CLASSES_ROOT\*\shell\runas\command]
@="cmd.exe /c takeown /f \"%1\" && icacls \"%1\" /grant administrators:F"
"IsolatedCommand"="cmd.exe /c takeown /f \"%1\" && icacls \"%1\" /grant
administrators:F"

[HKEY_CLASSES_ROOT\Directory\shell\runas]
@="Take Ownership"
"NoWorkingDirectory"=""

[HKEY_CLASSES_ROOT\Directory\shell\runas\command]
@="cmd.exe /c takeown /f \"%1\" /r /d y && icacls \"%1\" /grant
administrators:F /t"
"IsolatedCommand"="cmd.exe /c takeown /f \"%1\" /r /d y && icacls \"%1\"
/grant administrators:F /t"
```

ГЛАВА 9



Параметры Internet Explorer

9.1. Общие параметры IE

Очень много параметров Internet Explorer находится в разделе реестра `HKCU\Software\Microsoft\Internet Explorer\Main`, поэтому если в этой главе не будет явно указано, в составе какого раздела располагается тот или иной параметр, то подразумевается, что найти его можно именно в разделе `HKCU\Software\Microsoft\Internet Explorer\Main`.

9.1.1. Автоматическое изменение размера рисунков

Браузер Internet Explorer умеет автоматически изменять размер рисунков так, чтобы они полностью помещались на экране монитора, так, чтобы не появлялись полосы прокрутки. При желании вы можете отключить эту возможность. Для этого перейдите в раздел `HKCU\Software\Microsoft\Internet Explorer\Main` и присвойте параметру `REG_SZ Enable AutoImageResize` значение `no`. Регистр символов (как имен параметров, так и значений) важен, поэтому следите за ним!

Если такого параметра нет, то его нужно создать. Обратите внимание: в имени параметра есть пробел: `"Enable AutoImageResize"`. В дальнейшем имена параметров с пробелами будут заключаться в кавычки.

9.1.2. Отключение фоновых звуков

Некоторые Web-мастера устанавливают на Web-страницах фоновые звуки. В большинстве случаев эти звуки больше раздражают, чем придают нужный эффект. Запретить воспроизведение фоновых звуков можно с помощью па-

раметра REG_SZ Play_Background_Sounds, которому нужно присвоить значение no. Параметр находится в разделе HKCU\Software\Microsoft\Internet Explorer\Main.

9.1.3. Отключение автоматического обновления Internet Explorer

Internet Explorer (IE) является одним из наиболее часто обновляемых программных продуктов. Вы можете запретить его автоматическое обновление с помощью параметра REG_DWORD NoUpdateCheck, которому нужно присвоить значение 1.

Данный параметр находится в разделе HKCU\Software\Microsoft\Internet Explorer\Main.

9.1.4. Включение функции автозаполнения

С помощью параметра REG_SZ AutoSuggest в разделе HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\AutoComplete вы можете управлять автозаполнением строки адреса. Чтобы включить автозаполнение, присвойте этому параметру значение yes, а чтобы выключить автозаполнение — no.

9.1.5. Запрет автозаполнения форм

Параметр REG_SZ Use FormSuggest из раздела HKCU\Software\Microsoft\Internet Explorer\Main используется для автозаполнения форм. Автозаполнение форм можно отключить, если присвоить параметру значение no.

9.1.6. Запрет автозаполнения паролей

Если форма содержит поле для ввода пароля, то за ее работу отвечает параметр REG_SZ "FormSuggest Passwords" из того же раздела. Отключить запоминание пароля можно, присвоив этому параметру значение no.

Отключить запрос на сохранение пароля можно с помощью параметра "FormSuggest PW Ask" из того же раздела.

9.1.7. Удаление пароля на ограничение доступа к сайтам

IE позволяет установить пароль на ограничение доступа к сайтам по содержанию. Такие пароли обычно устанавливаются, чтобы дети не посещали сай-

ты "для взрослых". Но пароли имеют свойство забываться. Удалить пароль, если вы его забыли, можно в разделе `HKLM\Software\Microsoft\Windows \CurrentVersion\policies\Ratings`. Найдите параметр `REG_BINARY Key` и удалите пароль, при этом будет снято также и ограничение доступа.

9.1.8. Изменение стартовой страницы с помощью реестра

Адрес стартовой страницы хранится в параметре `REG_SZ StartPage`, который находится в разделе `HKCU\Software\ Microsoft\Internet Explorer\Main`.

9.1.9. Сокрытие редко используемых страниц в меню Избранное

Если включить параметр `REG_SZ FavIntelliMenus`, присвоив ему значение `yes`, то в меню **Избранное** (Favorites) будут отображаться только часто используемые пункты, а для доступа к редко используемым нужно будет нажать на стрелку, расположенную в самом низу меню.

9.1.10. Отключение автоматического дозвона

При просмотре Web-страниц, сохраненных на жестком диске, в автономном режиме (offline) IE пытается установить подключение с Интернетом и выводит окно **Подключение удаленного доступа**. Чтобы это окно больше не появлялось, нужно установить значение `0` для параметра `REG_DWORD EnableAutodial` в разделе `HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings`.

9.1.11. Изменение каталога для закачки файлов

С помощью параметра `REG_SZ "Download Directory"` вы можете изменить каталог, в который IE по умолчанию будет сохранять загружаемые файлы. Параметр находится в разделе `HKCU\Software\Microsoft\Internet Explorer`.

9.2. Параметры безопасности

9.2.1. Запрет изменения параметров IE

При включенном параметре с типом данных `REG_DWORD` и именем `NoBrowserOptions` (значение равно `1`) в разделе `HKCU\Software\Policies \Microsoft\Internet Explorer\Restrictions` пользователю запрещено изменять параметры IE. Все остальные параметры, приведенные в этом разделе книги, будут проигнорированы.

9.2.2. Отключение отображения вкладок окна настройки IE

Если же вы хотите частично запретить пользователю редактировать настройки браузера, то вам нужно изменить параметры, находящиеся в разделе `HKCU\Software\Policies\Microsoft\Internet Explorer\Control Panel` (этот раздел вам нужно создать самостоятельно):

- `GeneralTab` — управляет отображением вкладки **Общие** (General) окна настройки браузера;
- `SecurityTab` — управляет отображением вкладки **Безопасность** (Security);
- `PrivacyTab` — управляет отображением вкладки **Конфиденциальность** (Privacy);
- `ContentTab` — управляет отображением вкладки **Содержание** (Content);
- `ConnectionsTab` — управляет отображением вкладки **Подключения** (Connections);
- `ProgramsTab` — управляет отображением вкладки **Программы** (Programs);
- `AdvancedTab` — управляет отображением вкладки **Дополнительно** (Advanced);
- `Settings` — запретить изменение параметров временных файлов Интернета.

Чтобы скрыть вкладку окна настройки Internet Explorer, нужно создать соответствующий вкладке параметр и присвоить ему значение `1`.

> ***Примечание***
>
> Все только что перечисленные параметры имеют тип `REG_DWORD`.

9.3. Запрет доступа к Интернету. Установка IP-адреса прокси-сервера

Для запрещения доступа к Интернету достаточно указать неправильный IP-адрес прокси-сервера в настройках браузера. Для этого перейдите в раздел `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings` (если нужно запретить доступ к Интернету всем пользователям, то следует перейти в раздел `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings`).

Создайте (если не существует) `DWORD`-параметр `ProxyEnable` и присвойте ему значение `1`, если хотите запретить доступ к Интернету. Для разрешения доступа к Интернету нужно присвоить значение `0`.

Затем создайте строковый параметр `ProxyServer`, а в качестве значения установите несуществующий IP-адрес, например, `0.0.0.1:8080`.

Даже если вам не нужно запрещать доступ к Интернету, вы можете использовать приведенную выше последовательность действий для установки корректного адреса прокси-сервера. Если же вы хотите именно запретить доступ к Интернету, то кроме установки некорректного адреса прокси-сервера, нужно еще запретить пользователю самостоятельно изменять адрес прокси. Для этого перейдите в раздел реестра `HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel` (или в `HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet Explorer\Control Panel`) и создайте два `DWORD`-параметра:

- `Connwiz Admin Lock`
- `Connection Settings`

Чтобы запретить пользователю изменять параметры соединения с Интернетом, установите `1` в качестве значения обоих параметров. Значение `0` (для обоих параметров) разрешает изменение параметров соединения. После этого перезагрузите компьютер.

9.4. Ускорение работы браузеров Internet Explorer 7 и 8

Браузер Internet Explorer 7 работает медленнее, чем Firefox 3! У IE 8 с производительностью все в порядке — во всяком случае, на моем компьютере он работает быстрее, чем Firefox и Opera, но все трюки оптимизации, применимые к IE 7, можно применить и к IE 8, если его производительность чем-то вас не устраивает.

Повышение производительности IE 7 заключается в увеличении числа одновременных запросов, которые IE может осуществлять к Web-серверу, и в отключении проверки доступных сетевых ресурсов.

Для увеличения числа одновременных соединений перейдите в раздел реестра `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings` и создайте `DWORD`-параметр `MaxConnectionsPerServer` со значением `32`.

А чтобы отключить проверку сетевых ресурсов, нужно удалить следующий раздел реестра: `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\RemoteComputer\NameSpace\{D6277990-4C6A-11CF-8D87-00AA0060F5BF}`.

Для восстановления проверки сетевых ресурсов можно использовать REG-файл, приведенный в листинге 9.1.

Листинг 9.1. REG-файл, включающий проверку сетевых ресурсов

```
REGEDIT 5.00

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer
\RemoteComputer\NameSpace\{D6277990-4C6A-11CF-8D87-00AA0060F5BF}]
@="Scheduled Tasks"
```

Можно также отключить проверку доступных сетевых принтеров, удалив следующий раздел реестра:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer
\RemoteComputer\NameSpace\{2227A280-3AEA-1069-A2DE-08002B30309D}
```

Чтобы восстановить все, как было, используйте `REG`-файл из листинга 9.2.

Листинг 9.2. REG-файл, включающий проверку сетевых принтеров

```
REGEDIT 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer
\RemoteComputer\NameSpace\{2227A280-3AEA-1069-A2DE-08002B30309D}]
@="Printers"
```

9.5. Удаление Internet Explorer из реестра Windows

Если при попытке установки более новой версии IE происходит ошибка, рекомендуется удалить IE из реестра, но для этого нет необходимости удалять абсолютно все, что связано с IE. Просто перейдите в следующий раздел реестра:

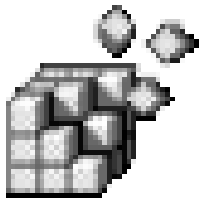
```
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components\
{89820200-ECBD-11cf-8B85-00AA005B4383}
```

Установите значение `0` для параметра `IsInstalled`. Перезагрузите компьютер.

Примечание

Перед выполнением этого действия создайте точку восстановления системы!

ГЛАВА 10



Параметры Windows Media Player

10.1. Автоматическая загрузка кодеков из Интернета

Кодек (англ. Codec — это сокращение от слов coder/decoder (кодировщик/декодировщик) или compressor/decompressor (компрессор и декомпрессор). Кодеки используются для сжатия и обратной распаковки мультимедиаданных (звук и видео). Мультимедийные данные занимают очень большой объем дискового пространства, что весьма затрудняет обмен ими. После обработки мультимедийной информации кодеком звуковой файл, который занимал, например, 100 Мбайт, сжимается до 10 Мбайт. Намного проще передать 10 Мбайт, чем 100 Мбайт, ведь так?

Кодек можно сравнить с архиватором с тем отличием, что архиватор сжимает (и, соответственно, распаковывает) данные любого типа, а кодеки предназначены для сжатия и распаковки только мультимедийных данных. Понятно, что при отсутствии архиватора мы не можем извлечь файлы, находящиеся в архиве. Аналогично, если нет кодека, то мы не можем просмотреть фильм или воспроизвести звуковой файл.

Если в системе нет нужного кодека для воспроизведения фильма (для звуковых файлов обычно все кодеки есть), любой проигрыватель (а не только Windows Media Player) сообщит вам о том, что данный формат файла не поддерживается. Для решения проблемы нужно определить, каким кодеком сжат фильм, найти в Интернете такой кодек и установить его.

Windows Media Player умеет загружать нужные для воспроизведения кодеки из Интернета. Это существенно упрощает установку кодеков — вам не придется самостоятельно определять тип кодека и искать его в Интернете: Media

Player все сделает сам, нужно только дать ему соответствующее разрешение. Для этого нужно перейти в следующий раздел реестра:

```
HKCU\SOFTWARE\Microsoft\MediaPlayer\Preferences
```

В этом разделе нужно создать параметр типа `REG_DWORD UpgradeCodecPrompt` и присвоить ему одно из значений:

- `0` — кодеки будут загружаться автоматически при наличии установленного соединения с Интернетом;
- `1` — перед загрузкой кодека проигрыватель спросит вас, согласны ли вы загрузить нужный кодек.

10.2. Отключение автоматического обновления

Windows Media Player периодически соединяется с Интернетом и проверяет, не появилась ли новая версия. Если новая версия доступна, то проигрыватель автоматически загружает ее. Такое поведение не может не раздражать некоторых пользователей, которые предпочитают самостоятельно устанавливать обновления программ. Процедуры отключения автоматического обновления в Windows Vista/7 и Windows XP отличаются. Сначала рассмотрим отключение автоматического обновления в Windows 7.

Перейдите в раздел `HKLM\SOFTWARE\Microsoft\MediaPlayer\PlayerUpgrade`. Создайте строковый параметр (`REG_SZ`) `AskMeAgain` и присвойте ему значение `NO`.

Для отключения автоматического обновления в Windows XP нужно перейти в раздел `HKLM\SOFTWARE\Policies\Microsoft\WindowsMediaPlayer` и добавить параметр `REG_DWORD DisableAutoUpdate` со значением `1`.

> ***Примечание***
>
> Отключить автоматическое обновление в Windows XP можно с помощью окна настройки Windows Media Player: **Сервис** (Tools) | **Параметры** (Options), вкладка **Проигрыватель** (Player), рамка **Автоматическое обновление** (Automatic updates). Там же можно включить опцию автоматической загрузки кодеков.

Помимо этого можно указать периодичность проверки наличия обновлений с помощью параметра `REG_DWORD UpgradeCheckFrequency` из раздела `HKCU\SOFTWARE\Microsoft\ MediaPlayer\Preferences`.

Параметр `UpgradeCheckFrequency` может принимать следующие значения:

- `0` — каждый день (один раз в день);
- `1` — раз в неделю;
- `2` — раз в месяц.

10.3. Удаление списка последних воспроизведенных файлов и URL

Последние воспроизведенные файлы хранятся в разделе `HKCU\Software\Microsoft\MediaPlayer\Player\RecentFileList`. Перейдите в этот раздел и удалите файлы, которые не должны быть в списке последних файлов.

Список последних воспроизведенных URL хранится в следующем разделе реестра:

`HKCU\Software\Microsoft\MediaPlayer\Player\RecentURLList`

10.4. Изменение заголовка окна проигрывателя

Перейдите в раздел реестра `HKCU\Software\Policies\Microsoft\WindowsMediaPlayer` и создайте в нем строковый параметр `TitleBar`. Присвойте ему любое значение — оно будет отображаться в заголовке окна проигрывателя.

10.5. Сокрытие компонентов проигрывателя

Вы можете скрыть радиопанель, панель избранных мультимедиафайлов и панель поиска новой станции. Для этого перейдите в раздел `HKCU\Software\Policies\Microsoft\WindowsMediaPlayer` и создайте в нем три параметра типа `REG_DWORD`:

- `NoRadioBar`
- `NoMediaFavorite`
- `NoFindNewStation`

Чтобы скрыть какой-то компонент проигрывателя, присвойте соответствующему параметру значение `1`. Когда компонент понадобится снова, установите значение `0` или просто удалите параметр.

10.6. Запрет изменения скина

Запретить пользователю изменять скин (графическое оформление) проигрывателя можно в разделе реестра `HKCU\Software\Policies\Microsoft\WindowsMediaPlayer`. Создайте строковый параметр `DefaultSkin` и присвойте

ему значение — имя скина, например, `Classic.wmz` (без кавычек). После этого создайте параметр `SetAndLockSkin` типа `REG_DWORD`. Если вы хотите запретить пользователю изменять скин, присвойте ему значение `1`. Для разблокировки скина, присвойте ему значение `1`.

10.7. Включение DVD-функций в Windows Media Player

Windows Media Player умеет воспроизводить диски, вот только по умолчанию возможность воспроизведения DVD отключена. Перейдите в следующий раздел реестра:

`HKCU\Software\Microsoft\MediaPlayer\Player\Settings`

Создайте строковый параметр `EnableDVDUI` и присвойте ему значение `Yes`. Перезапустите проигрыватель.

10.8. Включение MP3-кодирования в Windows XP

Как вам, должно быть, известно, дорожки Audio CD сохраняются на диске в файлах формата WMA (Windows Media Audio). Однако этот формат менее распространен, чем MP3, который знаком всем проигрывающим устройствам. Поэтому, возможно, вам захочется далее преобразовать WMA-файлы в формат MP3 при помощи какого-либо конвертера.

Было бы гораздо удобнее, если Media Player сразу записывал звуковые дорожки в формате MP3. Для включения встроенного MP3-кодека нужно в разделе `HKLM\SOFTWARE\Microsoft\MediaPlayer\Settings\` создать подраздел `MP3Encoding`, а в нем следующие параметры:

- `HightRate` типа `REG_DWORD` — максимальный битрейт, чем выше битрейт, тем качественнее MP3-файл. Он допускает установку значений 192000 (192 Кбит/с) или 256000 (256 Кбит/с), но на практике возможности встроенного кодека ограничены 128 Кбит/с, поэтому максимальное значение для этого параметра — 128000;
- `LowRate` типа `REG_DWORD` — минимальный битрейт. Чтобы получить гарантированные 128 Кбит/с, вполне достаточные для прослушивания MP3-файлов на компьютере и MP3-проигрывателе, нужно установить для этого параметра значение 128000;
- `MediumHighRate` типа `REG_DWORD` — "средневысокий" битрейт. Значение этого параметра также рекомендуется установить равным 128000;

- `MediumRate` типа `REG_DWORD` — средний битрейт, тоже устанавливаем равным 128000.

Значения битрейтов по умолчанию 128000, 56000, 112000, 64000 соответственно.

10.9. Отключение вкладки *Сеть* в Windows XP[1]

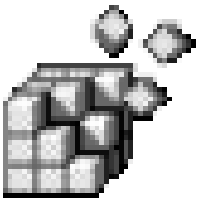
Для сокрытия вкладки **Сеть** (Network) окна настройки Windows Media Player, которое вызывается командами меню **Сервис** (Service) | **Параметры** (Settings), нужно в разделе `HKCU\Software\Policies\Microsoft` создать раздел `WindowsMediaPlayer`, а в нем — параметр `HideNetworkTab` (`REG_DWORD`) со значением `1`.

Примечание

Скрыть аналогичным образом другие вкладки не получится.

[1] Этот рецепт работает и в Windows 7. — *Прим. ред.*

ГЛАВА 11



Повышение привилегий процессов

11.1. Зачем это нужно?

Привилегии (process privileges) в мире информационных технологий — это очень тонкая вещь. Если предоставить пользователям минимальные привилегии, то мы обеспечим максимальную защиту системы от вредоносных программ, вирусов и необдуманных действий самих пользователей. Но минимальные привилегии — максимальное неудобство для администратора: пользователи будут обращаться к вам чуть ли ни при выполнении каждой операции.

С другой стороны, если предоставить пользователю максимальные полномочия, то придется гораздо чаще переустанавливать систему и восстанавливать данные...

Найти золотую середину достаточно сложно, но все-таки можно. Понимаю, что об административных политиках мы еще не успели подробно поговорить, но в этой главе мы обсудим несколько приемов настройки с использованием политики, а в *главе 19* рассмотрим политики Windows 7. В этой же главе мы сосредоточимся на повышении привилегий процессов.

11.2. Два способа повышения привилегий

Существует два способа запуска процессов с повышенными привилегиями. Первый из них заключается в использовании специальных политик (см. *главу 19*), а второй — в запуске программы от имени другого пользователя, обычно обладающего правами администратора.

При помощи первого из названных выше способов можно разрешить отдельным пользователям устанавливать программы, не добавляя их в группу Администраторы (Administrators). Второй способ полезен для самого администратора, если он работает с ограниченными полномочиями. Кстати, с точки зрения безопасности так и следует поступать: повседневные операции выполняются от имени простого пользователя, а операции, требующие повышенных полномочий, — от имени пользователя, обладающего правами администратора.

11.2.1. Политики

В *главе 24* мы познакомимся с политикой **Всегда производить установку с повышенными привилегиями** (Always install with elevated privileges). Данная политика позволяет обычным пользователям производить установку программ, даже если они находятся в группе Пользователи (Users), а не Опытные пользователи (Advanced Users) или Администраторы (Administrators). С одной стороны, если включить данную политику, "продвинутые" пользователи могут использовать ее для повышения своих полномочий и просмотра файлов и каталогов с ограниченным доступом. С другой стороны, вам не придется по просьбе каждого пользователя устанавливать нужные ему программы. Тут нужно выбирать, что для вас важнее — безопасность системы или собственный комфорт. Если среди пользователей нет диверсантов, то можно выбрать второй вариант.

> ***Примечание***
>
> Группа Опытные пользователи (Advanced Users), начиная с Windows Vista, пустая. Она оставлена из соображений обратной совместимости. Данная группа — недостаток Windows XP, но начиная с Vista, этот недостаток попытались исправить.

Чтобы данная политика работала, вы должны ее включить как в **Конфигурации компьютера** (Computer Configuration), так и в **Конфигурации пользователя** (User Configuration).

Применение этой политики возможно только на небольших предприятиях, где не используется Active Directory. В противном случае вам потребуется более гибкое средство — **Установка и поддержка программного обеспечения** (Software Installation snap-in), позволяющее устанавливать программы через GPO. Рассмотрение этого средства выходит за рамки данной книги, но вы можете узнать о нем больше по следующему адресу: **http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sag_adeconcepts_01.mspx?mfr=true**.

11.2.2. Запуск программ от имени другого пользователя

Для запуска программы от имени администратора нужно в окне Проводника (Windows Explorer) щелкнуть правой кнопкой по имени программы, которую вы хотите запустить, и из контекстного меню выбрать команду:

- **Запуск от имени администратора** (Run as Administrator) — данная команда есть только в Windows Vista/Windows 7 (рис. 11.1);

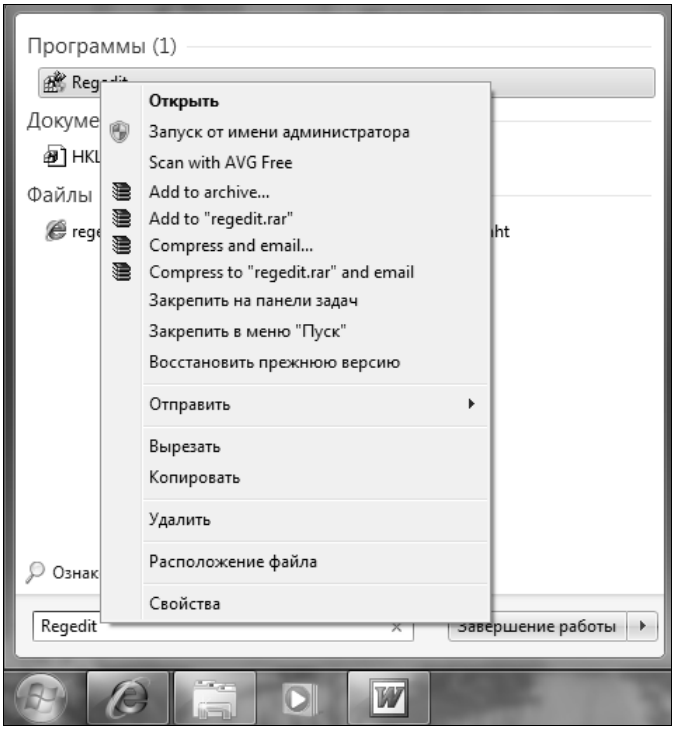


Рис. 11.1. Запуск программы от имени администратора в Windows Vista

- **Запуск от имени** (Run As) — данная команда есть в Windows XP. Вы увидите окно, в котором можно выбрать имя пользователя и ввести его пароль (рис. 11.2).

Кроме команды **Запуск от имени** (Run As) вы можете использовать команду `runas`, запускаемую из командной строки. Ее синтаксис следующий:

```
runas [/noprofile] [/profile] [/env] [/netonly] /user:имя_пользователя
программа
runas [/noprofile] [/profile] [/env] [/netonly] /smartcard
[/user:имя_пользователя] программа
```

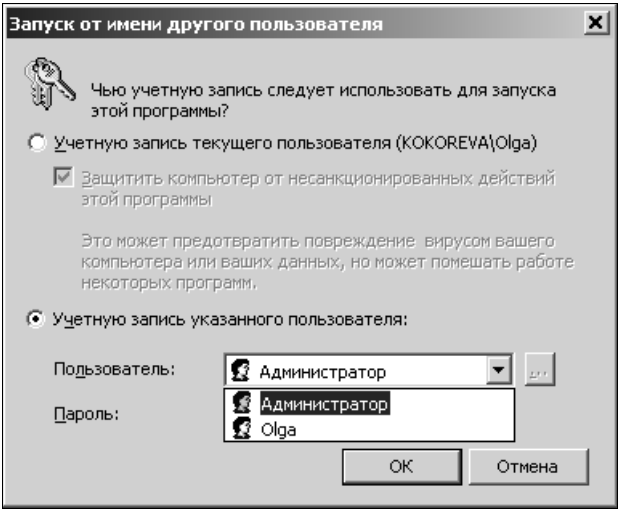


Рис. 11.2. Выбор имени пользователя и ввода его пароля в Windows XP

Допустимые параметры команды `runas` приводятся в табл. 11.1.

Таблица 11.1. *Параметры команды* `runas`

Параметр	Описание
`/noprofile`	Запускает программу `runas` без загрузки профиля пользователя. Некоторые программы, запущенные без загрузки профиля, могут работать некорректно
`/profile`	Загружает профиль пользователя, указанного с помощью параметра `/user`
`/env`	Позволяет использовать текущее окружение вместо окружения пользователя
`/netonly`	Если этот параметр указан, то имя пользователя и пароль предназначены только для удаленного доступа
`/savecred`	Использует имя пользователя и пароль, ранее сохраненные пользователем
`/smartcard`	Имя пользователя и пароль будут предоставлены через смарт-карту
`/user:`*имя_пользователя*	Задает имя пользователя, от имени которого будет запущена программа. Имя нужно указывать в формате *пользователь*`@`*домен* или *домен*`\`*пользователь*
программа	Программа, которую нужно запустить

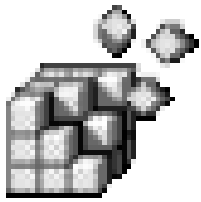
11.3. Приоритет: фоновым или активным приложениям

По умолчанию фоновые и активные приложения имеют почти одинаковый приоритет. Вы можете повысить производительность активных приложений. Тогда активное приложение, с которым вы в данный момент работаете, будет иметь более высокий приоритет, следовательно, будет работать быстрее.

Перейдите в раздел реестра `HKLM\SYSTEM\CurrentControlSet\Control\PriorityControl` и создайте параметр `Win32PrioritySeparation` типа `REG_DWORD` (или отредактируйте его значение, если он существует):

- `0` — приоритет фоновых и активных приложений одинаковый;
- `2` — чем выше значение параметра `Win32PrioritySeparation`, тем выше приоритет активных приложений перед фоновыми (тем больше ресурсов получат активные приложения). Значение 2 используется по умолчанию. Максимальное значение — 26;
- `6` — максимальное значение для слабых компьютеров;
- `10` — если у вас современный компьютер, можете попробовать установить значение 10 и посмотреть, как будет вести себя операционная система;
- `26` — максимальное значение параметра `Win32PrioritySeparation`.

ГЛАВА 12



Твикеры

12.1. Что такое твикер?

Твикер (от англ. tweaker) — это программа для тонкой настройки устройства или какой-либо другой программы. Существуют твикеры для тонкой настройки видеокарты и дисковых накопителей. В этой главе мы поговорим о программах-твикерах для настройки операционной системы. Таких программ много, но мы остановимся только на двух из них, которые, на мой взгляд, являются лучшими.

Мы не будем подробно рассматривать твикеры. Почему? Да потому, что основная задача твикера — это максимальное упрощение настройки Windows. Нужно отметить, что все твикеры отлично справляются с этой задачей: настроить Windows с помощью твикера может даже ребенок, а уж тем более квалифицированный пользователь. Зачем, спрашивается, мы тогда в этой книге так подробно рассматривали настройки реестра, если можно использовать твикер? А затем, чтобы вы стали квалифицированным пользователем и могли тонко настроить операционную систему и без твикера, ведь под рукой может не оказаться каких-либо дополнительных программ.

12.2. Твикеры для Windows Vista/Windows 7

Реестр Windows Vista имеет много общего с реестром Windows 7, поэтому большинство твикеров для Vista будут работать и в Windows 7, но некоторые опции, специфические только для Windows 7, эти программы изменять не смогут. Однако не забывайте посещать сайты разработчиков приведенных ниже программ — в скором времени должны появиться версии, полностью поддерживающие Windows 7.

12.2.1. Thoosje Vista Tweaker

Начнем с программы Thoosje Vista Tweaker (рис. 12.1). Она позволяет изменять около 60 настроек, влияющих как на "косметические" качества Vista, так и на производительность системы. Для работы с программой вам не нужны знания реестра — выбираете опцию и включаете или выключаете ее. Программа абсолютно бесплатна, вы можете скачать ее с сайта **http://www.thoosje.com/Windows-Vista-Tweaker.html**. На данный момент доступна вторая версия программы, а это указывает на то, что проект развивается, а не заброшен разработчиками.

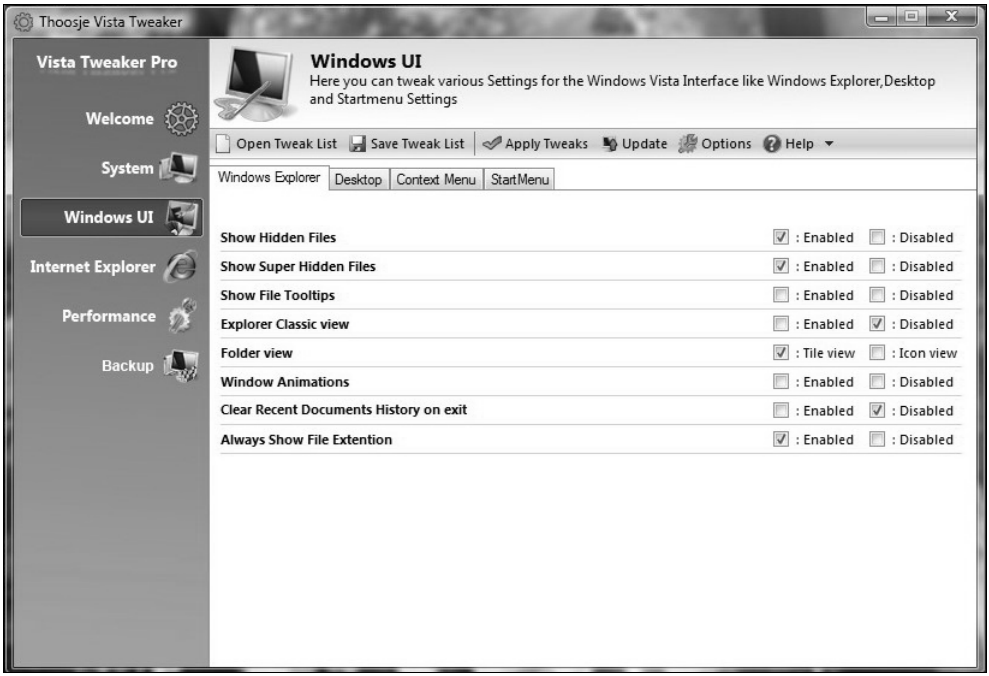


Рис. 12.1. Программа Thoosje Vista Tweaker

На сайте разработчиков этой программы вы найдете множество других бесплатных и полезных утилит, например, Thoosje Quick XP Optimizer. Посетите страничку утилит: **http://www.thoosje.com/Tools.html**.

12.2.2. VistaTweaker

VistaTweaker (рис. 12.2) — еще один твикер для Vista, позволяющий изменять системные настройки, настройки интерфейса пользователя, параметры Internet Explorer, параметры, влияющие на производительность, и т. д.

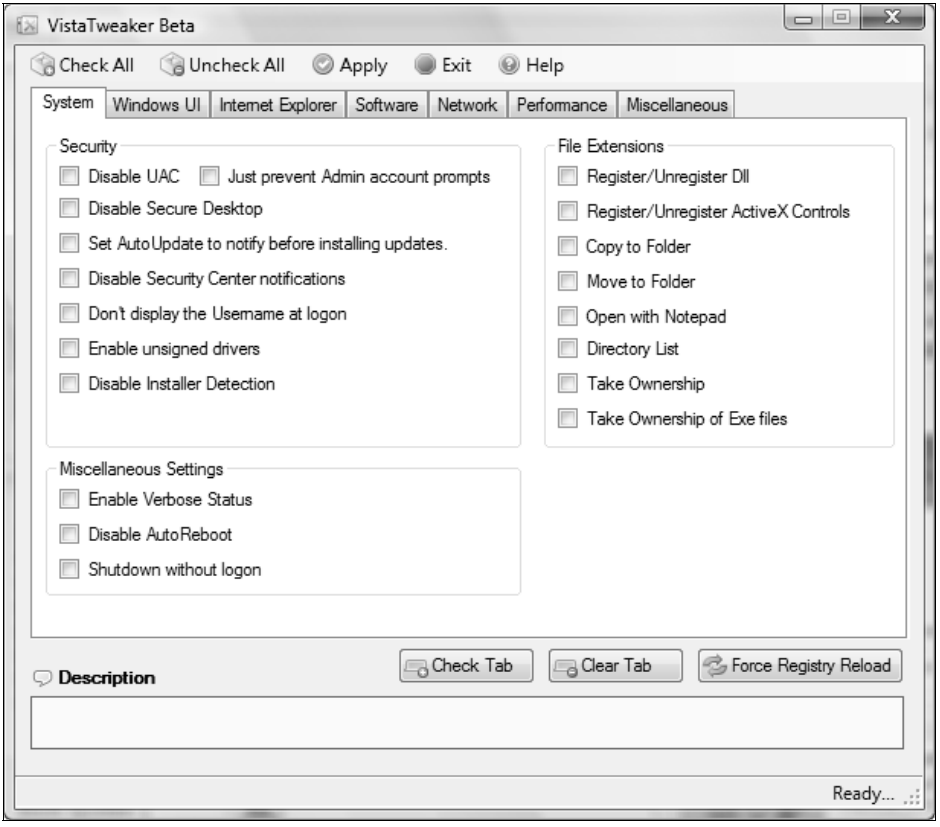


Рис. 12.2. Программа VistaTweaker

Программа является бесплатной, и ее можно скачать по адресу:

http://www.ajuaonline.com/downloads/

12.2.3. XdN Tweaker

Особенностью XdN Tweaker (рис. 12.3) является возможность установки параметров TCP/IP, изменения параметров Outlook и Vista UAC. Текущая версия программы поддерживает Windows 7 и Windows Vista. Скачать программу можно по адресу:

http://xenomorph.net/files-section/programming/visual-basic-programming/xdntweaker/

Рис. 12.3. Программа XdN Tweaker

12.2.4. Vista4Experts

Vista4Experts (рис. 12.4) — это не совсем обычный твикер. Это программа для IT-экспертов, желающих избавиться от надоедливых уведомлений центра безопасности, от окошек UAC, от автоматической установки обновлений и т. д. Скачать программу можно по адресу:

http://ntcore.com/vista4experts.php

12.2.5. Stardock TweakVista

Один из самых первых твикеров для Vista, который я стал использовать, — это Stardock TweakVista (рис. 12.5 и 12.6). Программу можно бесплатно скачать по адресу **http://www.tweakvista.com/ tweakvistautility/download.aspx**.

Существует две версии программы Stardock TweakVista: Free и Full. Первая — бесплатная, но с несколько ограниченными возможностями (доступны не все опции), а вторая — полная, но за нее нужно платить. Но на первое время вам хватит возможностей Free-версии.

У программы всего один недостаток: пока нет русскоязычной версии.

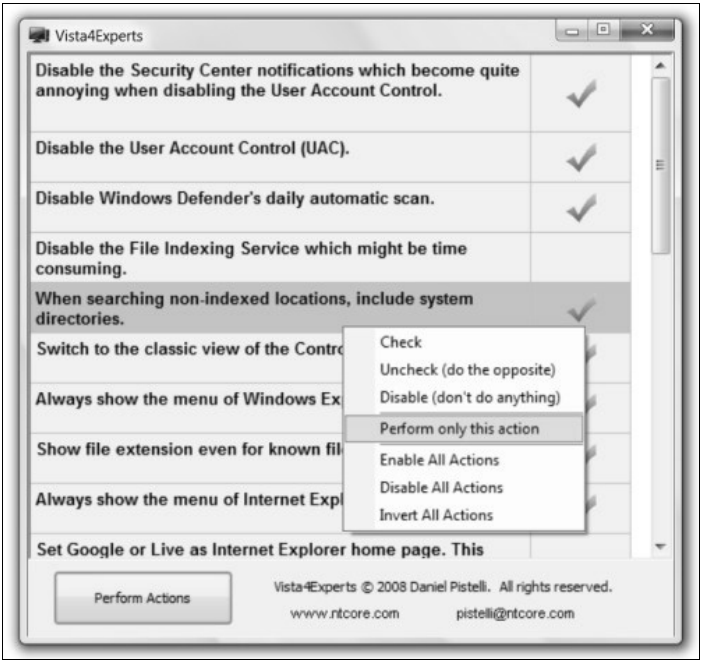


Рис. 12.4. Программа Vista4Experts

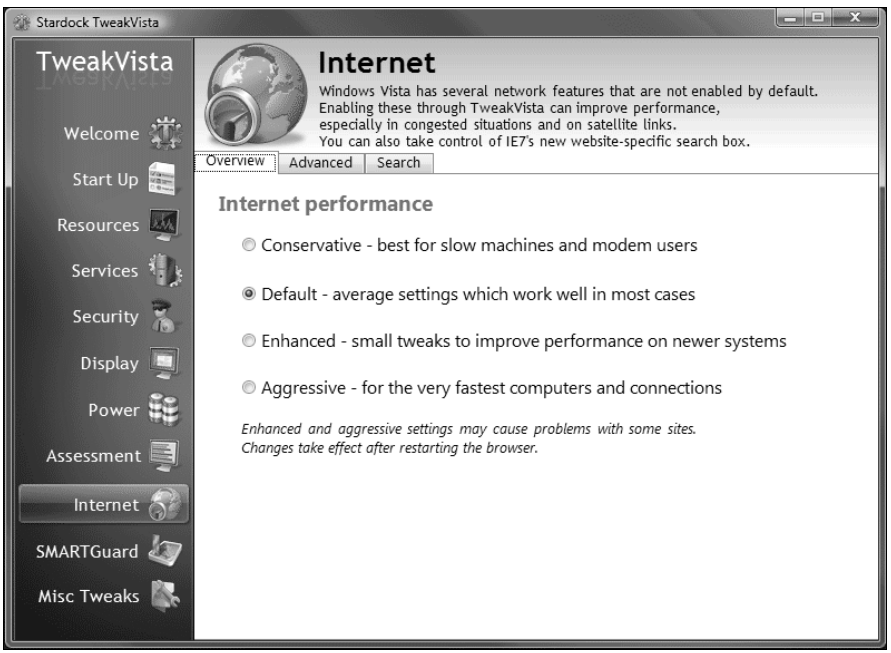


Рис. 12.5. Stardock TweakVista: Internet

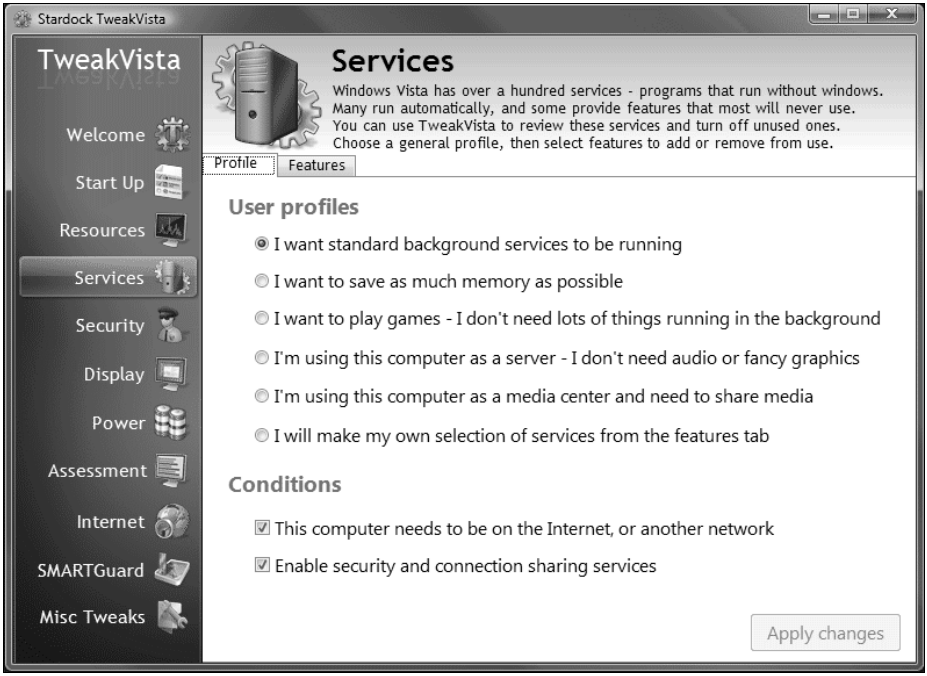


Рис. 12.6. Stardock TweakVista: Services

12.2.6. Windows 7 Manager

Программа Windows 7 Manager предназначена для тонкой настройки седьмой версии Windows. Она одинаково стабильно работает как с 32-, так и с 64-битной версией Windows 7. Программа сочетает в себе не только функции твикера, но и оптимизатора системы. В ней есть и "чистильщик", позволяющий удалить ненужные файлы, и менеджер процессов, и общий оптимизатор системы (рис. 12.7).

Программа не бесплатная. Скачать 15-дневную ознакомительную версию программы можно по адресу **http://www.yamisoft.com**.

Программа была протестирована мною: работает стабильно, но на всякий случай я бы не отказывался от возможности создать точку восстановления перед каждым применением этой программы. Благо, программа сама напоминает об этом при запуске.

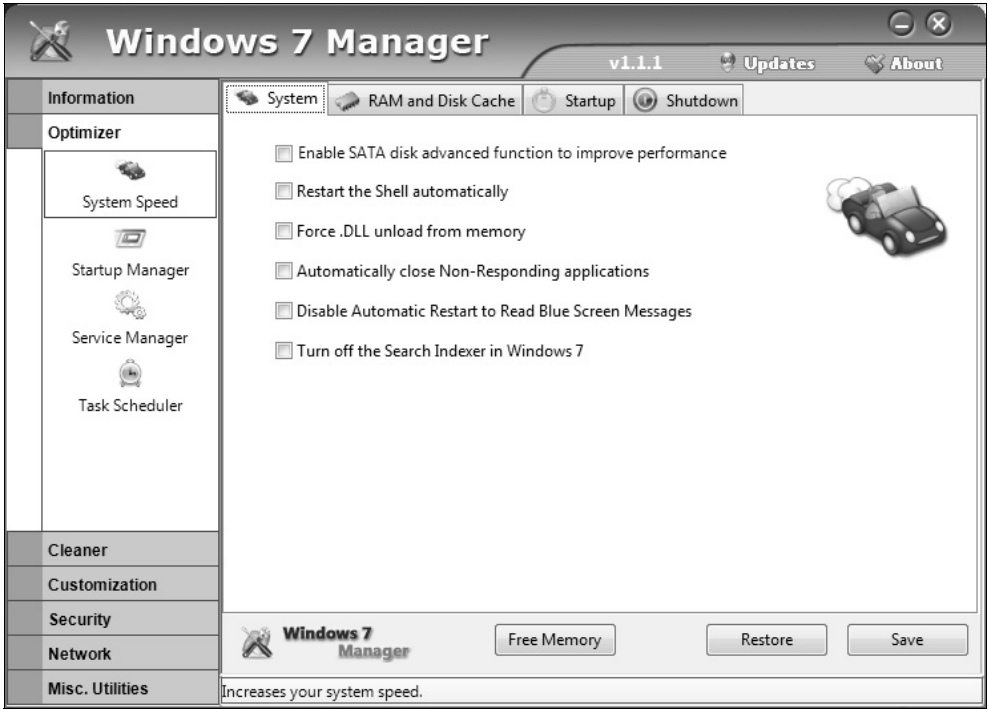


Рис. 12.7. Программа Windows 7 Manager

12.2.7. Ultimate Windows Tweaker v2, a Tweak UI for Windows 7 & Vista

Программа может использоваться как для настройки Windows 7, так и для настройки Windows Vista (рис. 12.8). У программы Ultimate Windows Tweaker v2 есть две особенности:

- программа абсолютно бесплатная;
- программа не требует установки, занимает мало места на диске (всего 350 Кб) и может запускаться с флэшки, что очень удобно.

> ***Примечание***
>
> Программа не умеет создавать точки восстановления, поэтому перед использованием программы создайте точку восстановления системы вручную — на всякий случай.

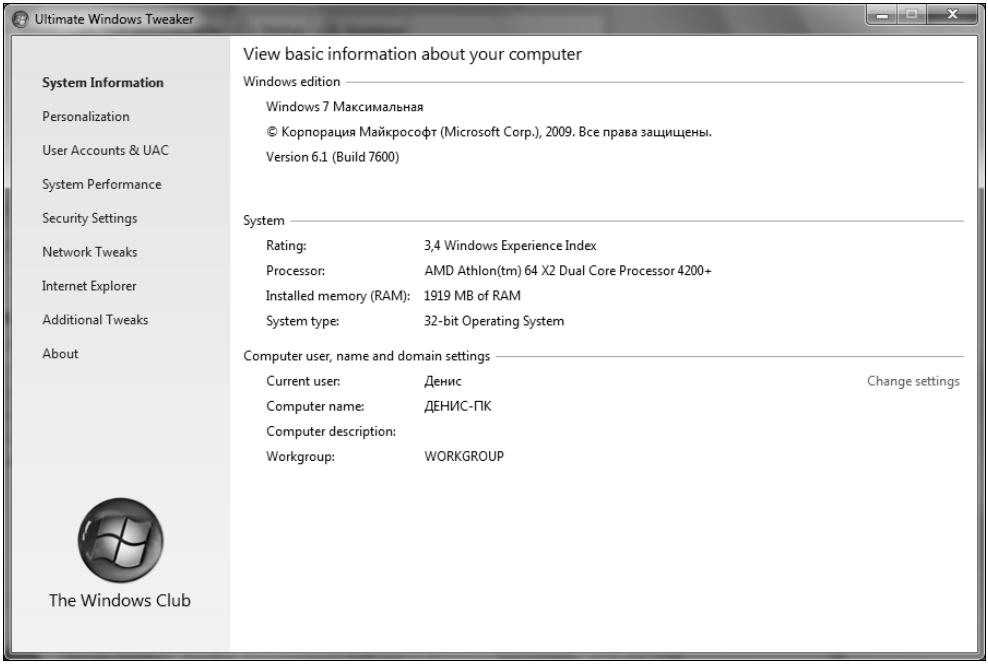


Рис. 12.8. Программа Ultimate Windows Tweaker v2

12.3. Твикер для Windows XP — XP Tweaker

Программа предназначена для тонкой настройки, защиты и оптимизации Windows XP. Поскольку программа разрабатывалась отечественными программистами, она учитывает особенности русских версий Windows XP и обладает очень удобным русскоязычным графическим интерфейсом, что дает возможность работать с ней даже неопытным пользователям (рис. 12.9).

Отличительной особенностью программы является наличие подробного справочника по реестру, в котором описаны все опции, которые умеет изменять программа. Используя этот справочник, вы можете написать аналог твикера — так сказать, "по образу и подобию", если, конечно, обладаете минимальными навыками программирования.

В разделе **Настройки** (рис. 12.10) вы можете сохранить все настройки в REG-файл для последующего быстрого восстановления настроек или для их переноса на другой компьютер.

Программа тестировалась в следующих операционных системах: Windows XP Professional, Windows XP Corporate Edition, Windows 2003 Server Enterprise Edition.

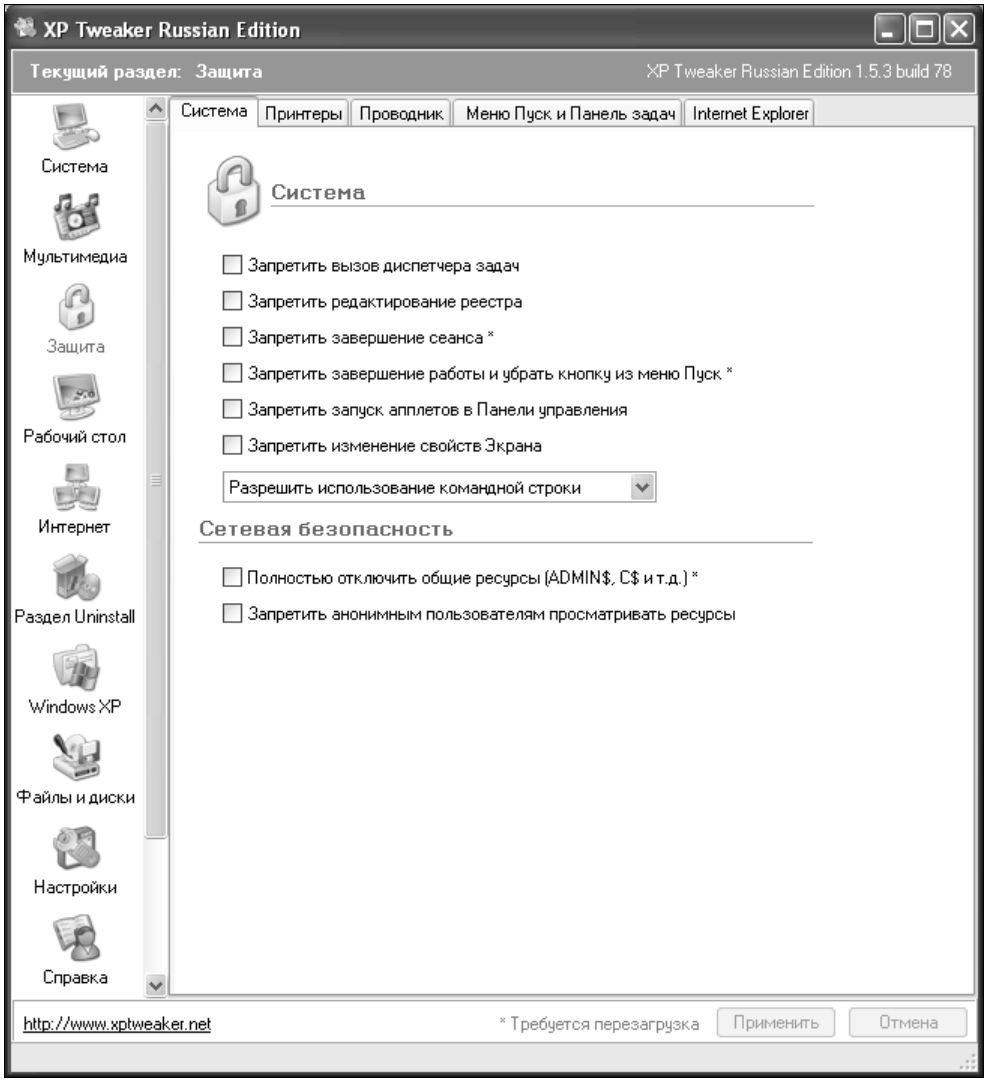


Рис. 12.9. Программа XP Tweaker

Теоретически есть возможность работы с этой программы и в Windows Vista: для этого нужно запустить ее с параметром `/nocheckver`. Однако я не рекомендую этого делать: хотя большинство параметров реестра Vista совместимы с параметрами Windows XP, но не все. В лучшем случае опции, которые вы пытались активировать, просто не будут работать, в худшем это может отразиться на стабильности всей системы. В частности, в Vista некорректно работает раздел **Uninstall**.

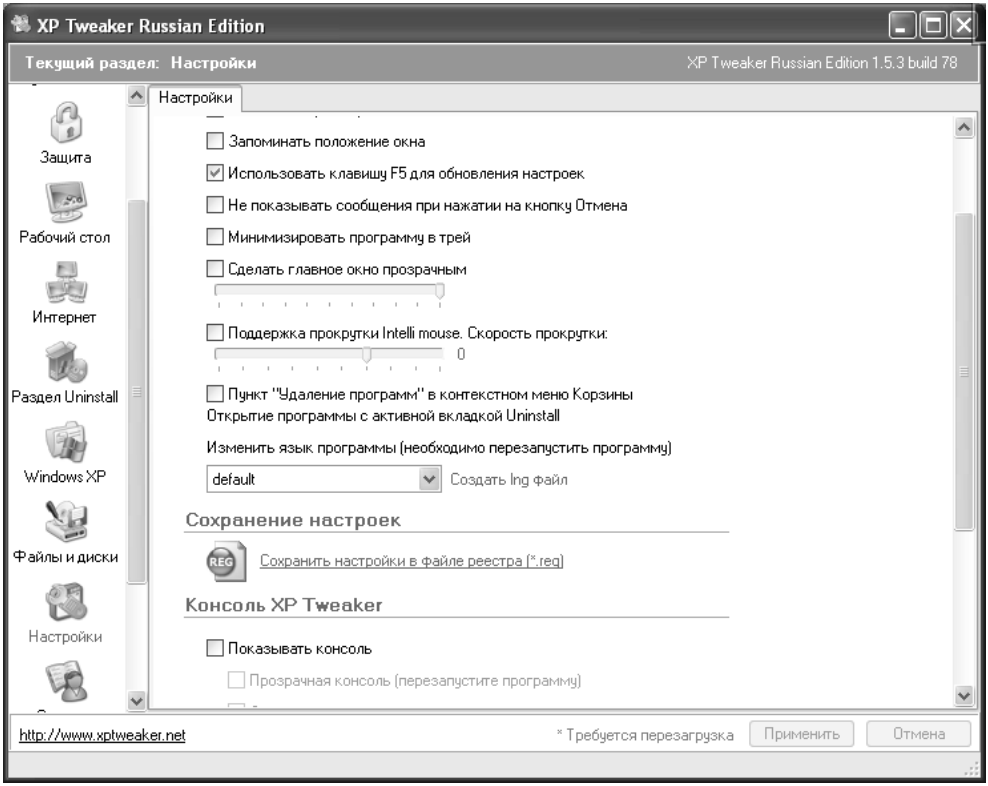


Рис. 12.10. Сохранение настроек

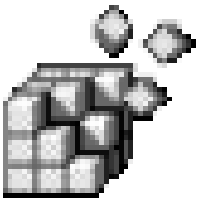
Если вы все же хотите использовать программу в Vista, скачайте и установите ее. Затем скачайте файл xpt200b81onlyexe.zip по следующей ссылке:

http://sourceforge.net/project/downloading.php?group_id=121008&use_mirror=osdn&filename=xpt200b81onlyexe.zip&98668826

В этом архиве находится немного модифицированная версия программы. Архив нужно распаковать в тот же каталог, в который вы установили твикер, после чего его можно использовать в Vista. Однако это не специализированная версия данной программы для Vista: из нее просто исключены опции, которые не совместимы с Vista или же неактуальны при ее использовании. Вследствие этого программа не умеет настраивать новые возможности Vista.

Для полноценной работы с программой XP Tweaker необходимо обладать правами администратора. Если вы запустили программу от имени обычного пользователя, большинство настроек не будут сохранены в реестре.

Скачать программу можно по адресу **http://xptweak.sourceforge.net**.



ГЛАВА 13

Программы для чистки и оптимизации реестра

13.1. Уход за реестром

Все современные прикладные программы хранят свои настройки в реестре. Если раньше часть программ хранила свои настройки в INI-файлах, то сейчас практически все они используют реестр. При удалении программ часто не удаляются ключи, принадлежащие этим программам, что приводит к появлению в реестре ненужных или неправильных записей (программа уже удалена, а ассоциацию файлов деинсталлятор удалить "забыл"). Все это в конечном итоге сказывается на размере реестра (он становится неприлично большим) и на производительности системы — чем больше реестр, тем больше ее времени уходит на работу с ним.

Чистить реестр вручную — дело неблагодарное: всегда есть опасность допустить ошибку, да и времени уйдет очень много, тогда как программа для чистки реестра все сделает безошибочно и это займет максимум 5 минут. В Интернете можно найти множество программ, предназначенных для чистки и оптимизации (дефрагментации) реестра. В этой главе мы как раз и поговорим о таких программах. Все программы позволяют быстро и безопасно (создается файл отката) очистить реестр от ненужных или некорректных ключей и параметров.

13.2. Программа *CleanMyPC Registry Cleaner*

Однако не все программы хороши для чистки реестра, особенно для чистки реестра Windows 7. В моей книге "Секреты реестра Windows XP/Vista"[1] опи-

[1] Колисниченко Д. Секреты реестра Windows XP/Vista. — СПб.: БХВ-Петербург, 2008.

сывалась довольно неплохая программа RegSeeker. Она превосходно работала в Windows XP, но вот работать в Windows 7 отказалась. Точнее, запуститься-то она запустилась, но вот дальше функциональность программы мне не понравилась. Начнем с того, что программа споткнулась при попытке отобразить список автоматически запускаемых программ. Но это мелочи по сравнению с тем, что программа нашла 1340 (!) ошибок в реестре свежеустановленной Windows 7 (рис. 13.1)! Это свидетельствует только об одном: программа не имеет понятия о реестре Windows 7. Если вы до сих пор используете Windows XP, то эта программа может вам пригодиться: она лучше ищет в реестре данные, чем стандартный Regedit.exe, умеет корректно удалять установленные программы, умеет чистить историю браузера IE, и, конечно же, чистит реестр и позволяет создавать его резервную копию. Скачать программу (она абсолютно бесплатна) можно по адресу: **http://www.hoverdesk.net/freeware.htm**.

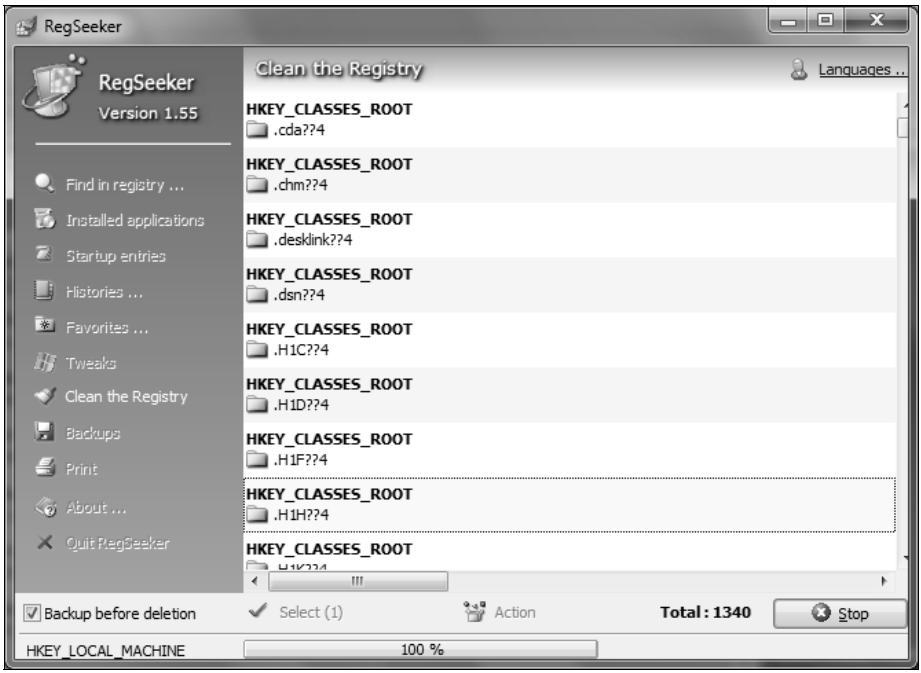


Рис. 13.1. RegSeeker не предназначен для реестра Windows 7

Второй рассмотренной в выше упомянутой книге программой была программа CleanMyPC Registry Cleaner. Данная программа, как указано на сайте разработчика, поддерживает следующие версии Windows:

- Windows 7 (32 и 64 бит)
- Windows Vista (32 и 64 бит);

- Windows XP (32 и 64 бит);
- Windows Server 2003 (32 и 64 бит);
- Windows Server 2008 (32 и 64 бит);
- Windows 2000;
- Windows ME;
- Windows 98.

Скачать программу можно по адресу:
http://www.registry-cleaner.net/windows-7-registry-cleaner.htm

Программа условно-бесплатная. Это означает, что имеете право использовать ее бесплатно на протяжении 15 дней, после чего должны будете ее или удалить, или зарегистрировать (регистрация стоит 29,95 долларов).

Новая версия программы (4.23) полностью поддерживает Windows 7. Предыдущая версия программы (4.22) поддерживает Vista, но я ее тестировал в Windows 7 и она превосходно работала. Однако если есть возможность, настоятельно рекомендую скачать последнюю версию программы — разработчики протестировали ее и заверяют, что она полностью совместима с Windows 7.

При запуске программа предлагает создать резервную копию реестра. Думаю, отказываться от этого не стоит. Отказаться можно только, если вы перед ее запуском создали точку восстановления системы. Зачем создавать резервную копию, должно быть понятно. После создания резервной копии вы увидите основное окно программы (рис. 13.2).

> ***Примечание***
>
> При создании резервной копии реестра программа создает CAB-файл, в который помещает все файлы, относящиеся к реестру (SAM, NTUSER.DAT и др.). Чтобы восстановить реестр из такой резервной копии, нужно запустить программу, перейти в раздел **Backup & Restore**, нажать кнопку **Restore Registry** и выбрать сохраненный ранее CAB-файл. Ничего сложного в этом нет. Однако я все равно рекомендую помимо такого резервного копирования создавать еще и точку восстановления системы.

Кнопки позволяют быстро выбрать необходимое действие:

- **Check Registry** — проверить реестр и "почистить" его в случае необходимости;
- **Backup Registry** — создать резервную копию реестра;
- **Defrag Registry** — дефрагментировать реестр, этим вы уменьшите его размер и увеличите производительность системы (обычно дефрагментацию реестра нужно выполнять не реже одного раза в полгода, хотя все зависит от интенсивности использования компьютера: если вы часто уста-

навливаете и удаляете программы, то можно дефрагментировать реестр раз в три месяца);

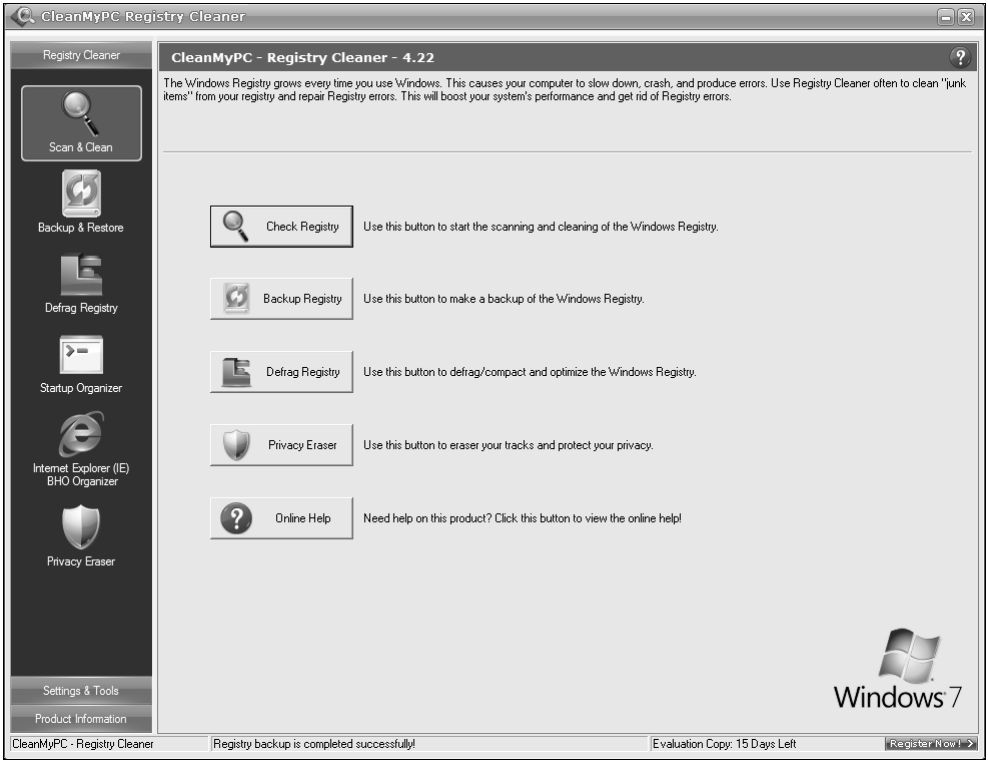


Рис. 13.2. Программа CleanMyPC

- **Privacy Eraser** — удалить приватную информацию (рис. 13.3): историю и Cookies браузера, список последних документов и компьютеров. Что мне понравилось в этой программе, так это поддержка не только браузера IE, но и других часто используемых браузеров — IE, Firefox, Opera, MSN, AOL. Ведь другие программы поддерживают только IE, а остальные браузеры приходится "чистить" самостоятельно — средствами браузера, что не очень удобно. А удалить список недавно использовавшихся документов можно не только из меню **Пуск** (Start) | **Документы** (Documents), но из меню **Файл** (File) программ MS Office (и других программ, например, WinZip, Windows Media Player, см. рис. 13.3);
- **Online Help** — вызов справочной системы.

Первым делом я решил "почистить" реестр, чтобы испытать программу. Нажмите кнопку **Scan & Clean** на панели слева (рис. 13.4), затем нажмите кноп-

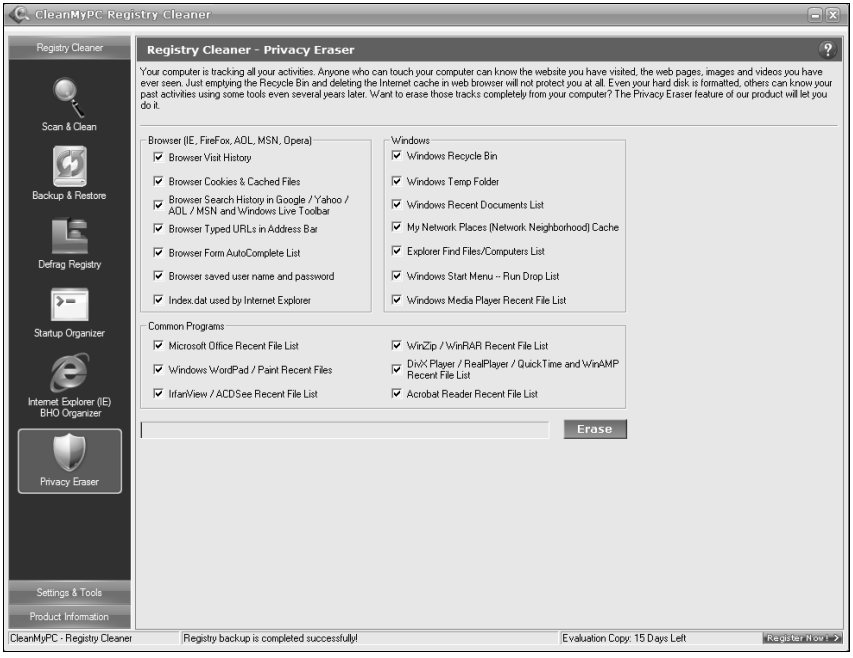


Рис. 13.3. Удаление приватной информации

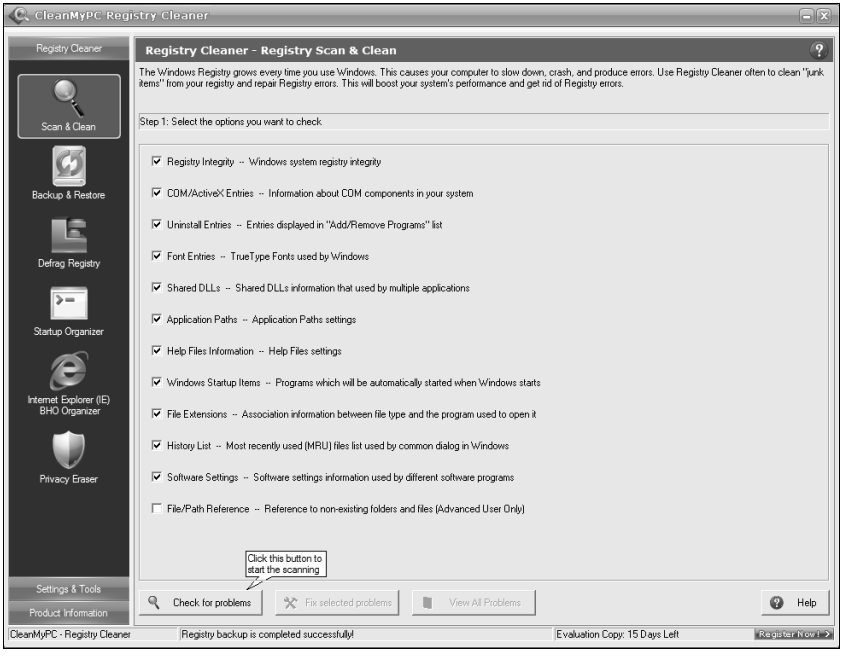


Рис. 13.4. Запуск сканирования реестра

ку **Check for problems**. Программа нашла 72 проблемы (рис. 13.5). Правда, я ее запустил уже после установки дополнительных программ в свою Windows 7. Но, согласитесь, это не 1340 ошибок в свежей установке Windows. Для исправления ошибок нужно нажать кнопку **Fix selected problems**.

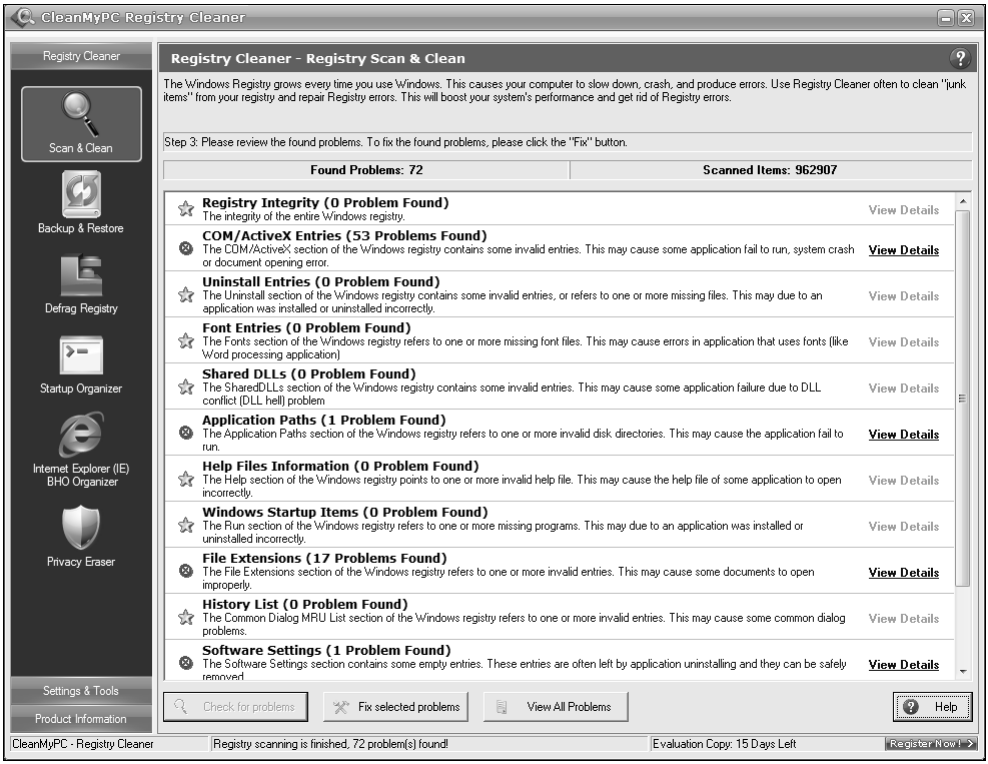


Рис. 13.5. Найденные проблемы

После исправления ошибок я перезапустил систему, чтобы убедиться в ее работоспособности. Все нормально — система запустилась, следовательно, программу CleanMyPC не только можно, но и нужно использовать.

Кроме чистки реестра и приватной информации программа позволяет запускать ряд системных утилит. Для их запуска перейдите в раздел **Settings & Tools** и нажмите кнопку **Advanced Tools**. В появившемся окне (рис. 13.6) можно запустить различные утилиты: информацию о системе (рис. 13.7), чистку диска, дефрагментатор диска, диспетчер устройств, программу восстановления Windows, редактор реестра, программу msconfig и средство диагностики DirectX (программа dxdiag).

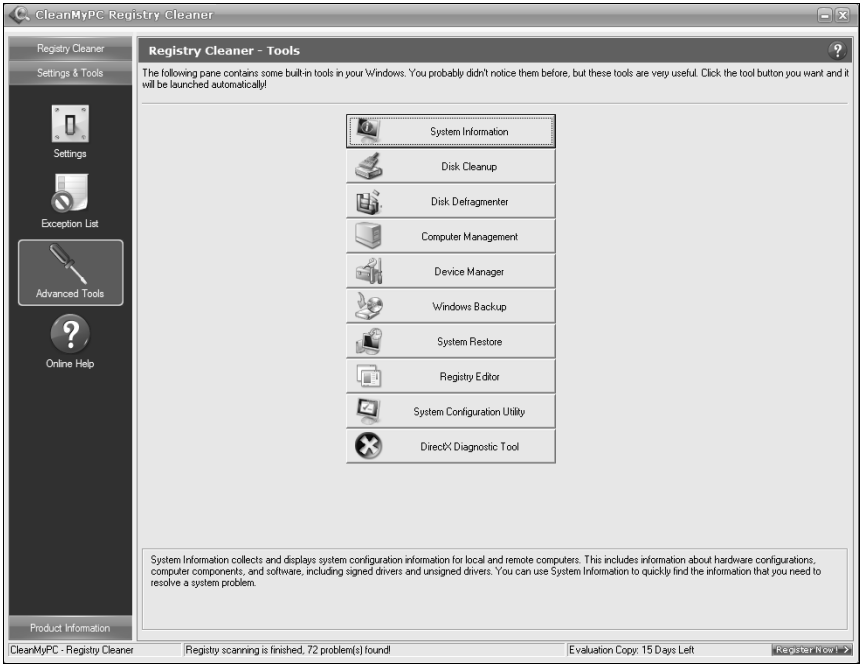


Рис. 13.6. Меню запуска системных утилит

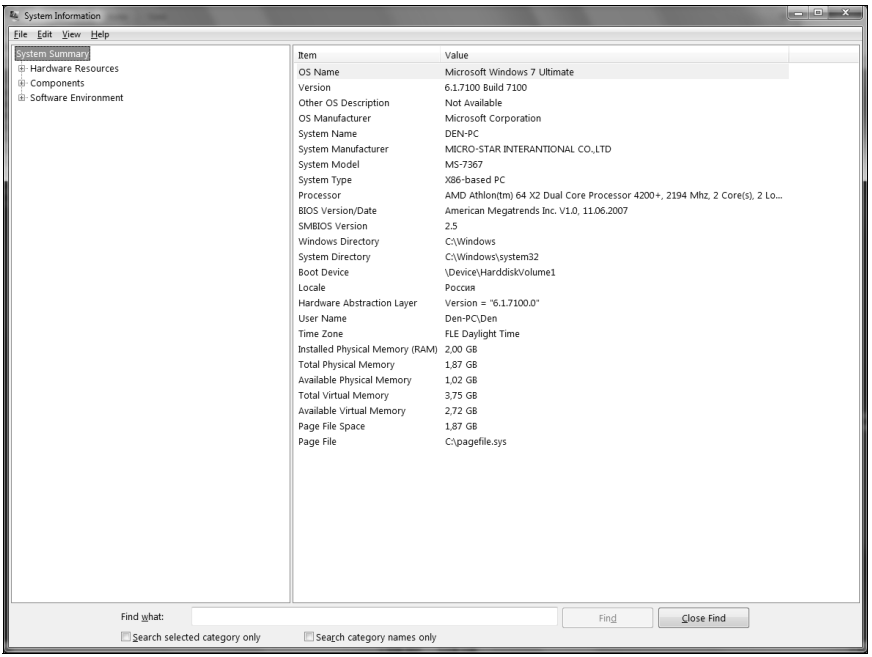


Рис. 13.7. Информация о системе

13.3. Программа *CCleaner*

Программа CCleaner — бесплатная программа для оптимизации и чистки Windows 7. Кроме оптимизации реестра программа умеет удалять временные файлы Интернета, файлы Cookies, историю Internet Explorer. Кроме IE программа умеет "чистить" следующие браузеры: Opera, Firefox, Safari, Google Chrome (если они, конечно, установлены).

Лично мне понравилось то, что программа изначально была разработана с учетом Windows 7 и обладает русским интерфейсом. А более 310 миллионов загрузок программы говорит о ее популярности и надежности. Скачать программу можно по адресу **http://www.ccleaner.com**.

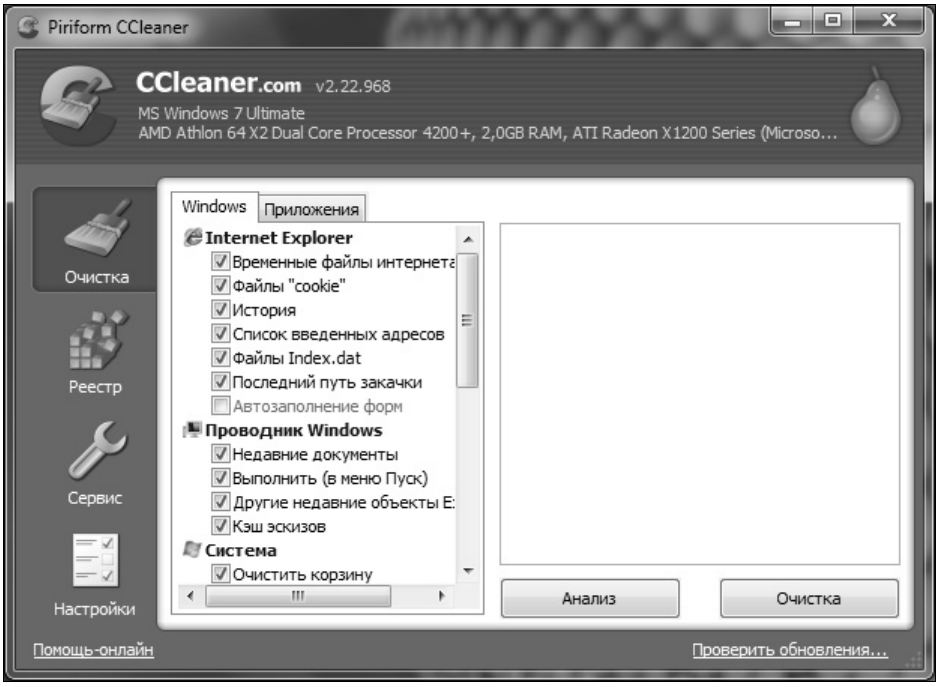


Рис. 13.8. Программа CCleaner

Также понравилось, что программа перед изменением реестра сохраняет резервную копию в обычном REG-файле, что позволяет проанализировать сделанные программой изменения и легко восстановить предыдущее состояние реестра.

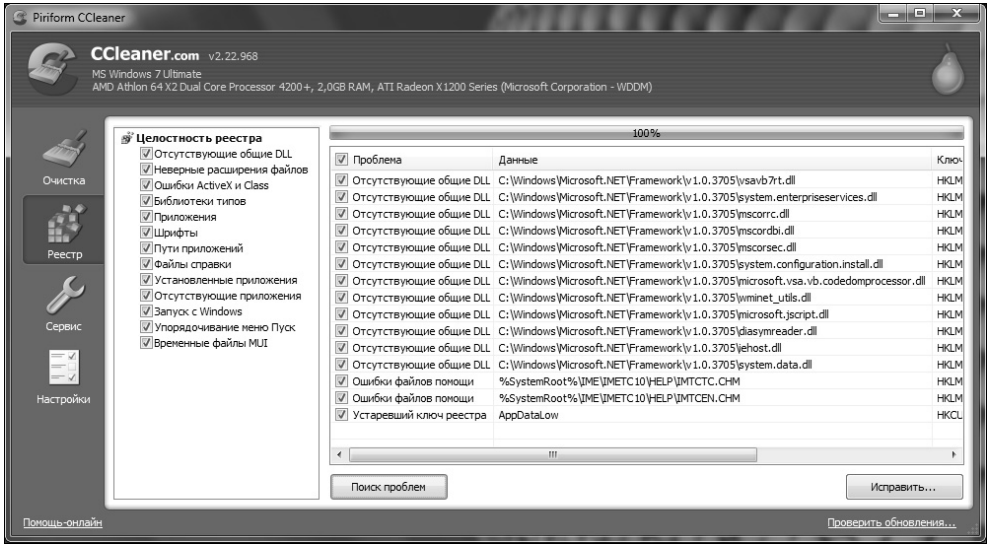


Рис. 13.9. Найдены некоторые проблемы

13.4. Программа *WinUtilities Registry Cleaner for Windows 7*

WinUtilities Registry Cleaner for Windows 7 — условно-бесплатная (с испытательным периодом в 1 месяц) программа для очистки и оптимизации Windows 7 (рис. 14.10). По сути, еще один "чистильщик" для Windows.

Меню программы содержит следующие пункты:

- **System Cleaners** — позволяет вызвать один из трех "чистильщиков". Вы можете очистить место на диске, реестр и историю браузера;
- **System Optimizers** — вызывает оптимизаторы системы (дефрагментатор диска, оптимизатор памяти и др.);
- **System Control** — содержит команды вызова различных системных утилит, позволяющих управлять автозапуском программы, автоматическим завершением работы Windows и т. д.;
- **System Tools** — позволяет запустить менеджер-процессор, менеджер удаления программ, программу, выводящую системную информацию;
- **Registry Tools** — вызывает утилиты для работы с реестром (создание резервной копии и восстановление реестра из резервной копии, а также программу расширенного поиска в реестре);

- **File Tools** — содержит утилиты восстановления файлов, разделения больших файлов на части (полезно, когда файл не помещается на CD/DVD), а также программу, позволяющую защитить EXE-файл (другую программу) паролем.

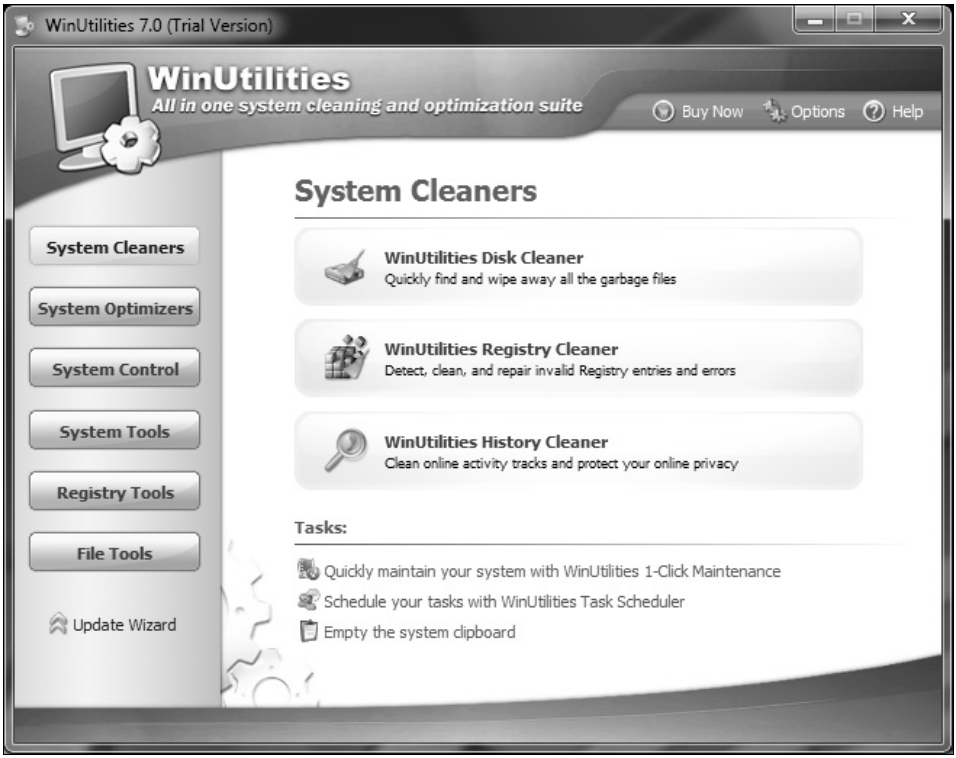
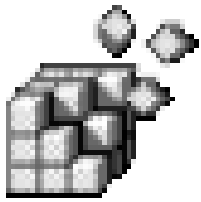


Рис. 13.10. Программа WinUtilities Registry Cleaner for Windows 7

Из недостатков могу отметить только отсутствие русского интерфейса программы, а так программу очень даже можно использовать. Была бы она еще бесплатной!

ГЛАВА 14



Программа редактирования реестра из командной строки

14.1. Утилита *Reg.exe*

Ранее в этой книге мы познакомились с графическим редактором системного реестра — программой Regedit.exe. Но в Windows есть и еще один официальный редактор реестра, предназначенный для запуска из командной строки. Это — утилита reg.exe, которая ранее поставлялась в составе программных продуктов из серии Windows Resource Kit и которая, начиная с Windows XP, входит в состав самой операционной системы.

Зачем нужен такой редактор? В основном он используется для редактирования реестра из командных файлов (файлы с расширением .cmd или .bat, содержащие список команд, которые должен выполнить командный интерпретатор).

Кроме того, в версиях Windows, более ранних, чем Windows Vista, программа reg.exe была нужна, если Windows отказывалась запускаться в графическом режиме, а запускалась только в режиме командной строки. Хотя такое происходило чрезвычайно редко, но, тем не менее, грамотный администратор обязан был знать о существовании "консольной" версии редактора реестра. Впрочем, уже начиная с Windows Vista, новая среда восстановления Windows (Windows Recovery Environment) позволяет запускать из командной строки и графические утилиты, в том числе редактор реестра.

Тем не менее, автоматизация рутинных операций по редактированию реестра на множестве машин (что весьма актуально для администраторов) — это уже достаточный повод для того, чтобы подробно ознакомиться с данной утилитой. Да и, кроме того, утилита Reg.exe позволяет выполнять некоторые операции, недоступные через стандартный Редактор реестра Regedit.exe.

14.2. Параметры программы

В этом разделе мы рассмотрим опции программы reg.exe (рис. 14.1); они представлены в табл. 14.1.

Таблица 14.1. *Параметры программы reg.exe*

Параметр	Описание
SAVE *ключ файл*	Сохраняет ветвь реестра (указанный ключ и все его подключи) в указанный файл куста. Обратите внимание: не в REG-файл, а в файл куста. Имя ключа может называться с аббревиатуры HKLM, HKCU, HKCR, HKU или HKCC
RESTORE *ключ файл*	Восстанавливает файл куста в указанный раздел реестра; при этом происходит полное замещение указанного раздела реестра
EXPORT *ключ reg-файл*	Экспортирует выбранный ключ реестра в указанный REG-файл
IMPORT *reg-файл*	Импортирует указанный REG-файл
LOAD *ключ файл*	Загружает указанный файл куста во временную ветвь, которая начинается с указанного ключа
UNLOAD *ключ*	Выгружает загруженный с помощью LOAD файл куста
COPY *ключ1 ключ2* [/s]	Копирует параметры из *ключ1* в *ключ2*. Если второй ключ не существует, то он будет создан. Если указана опция /s, то будут скопированы также и все подключи, а не только параметры
QUERY *ключ* [/v *Параметр* | /ve] [/s]	Используется для отображения раздела или параметра. Допустимы следующие параметры: /v — используется для отображения параметра с указанным именем; /ve — используется для отображения значения по умолчанию для указанного раздела реестра; /s — используется для вывода всех подразделов и параметров
ADD *ключ* [/v *Параметр* | /ve] [/t *тип*] [/s *разделитель*] [/d *данные*] [/f]	Добавляет раздел или параметр реестра. Если не задана опция /v или /ve, то добавляется раздел реестра. При добавлении допустимы следующие параметры: /v — определяет имя создаваемого параметра; /ve — создает параметр по умолчанию; /t — задает тип создаваемого параметра реестра (REG_SZ, REG_DWORD и т. д.). По умолчанию используется REG_SZ;

Таблица 14.1 *(окончание)*

Параметр	Описание
	/s — задает разделитель строк для параметра типа REG_MULTI_SZ; /d — содержит значение, которое будет присвоено создаваемому параметру. Используется только вместе с опциями /v или /ve; /f — дает указание переписать значение параметра, даже если он уже существует
DELETE *ключ* [/v *Параметр* | /ve | /va] [/f]	Удаляет раздел или параметр. Для удаления допустимы следующие параметры: /v — удалить параметр; /ve — удалить параметр по умолчанию; /va — удалить все параметры из указанного ключа; /f — удалить без запроса
COMPARE *ключ1 ключ2* [*вывод*] [/s]	Сравнивает один раздел реестра с другим. При сравнении допустимы следующие параметры: /od — выводить только отличия (по умолчанию); /oa — выводить совпадения и отличия; /os — только совпадения; /on — не выводить результаты сравнения (используется в командных файлах); /s — сравнивать все подразделы и параметры
flags	Новая команда, появившаяся в Windows Vista в связи с введением функции виртуализации реестра[1]. Эта команда устанавливает или сбрасывает флаги виртуализации для указанного подключа. В программе Regedit.exe аналогичная возможность отсутствует

[1] Что такое виртуализация реестра? Это новшество, впервые введенное в Windows Vista, тесно связано с функцией UAC. 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 получать доступ к этим областям при работе от имени учетной записи обычного пользователя, Windows Vista/7 и реализуют 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 опе-

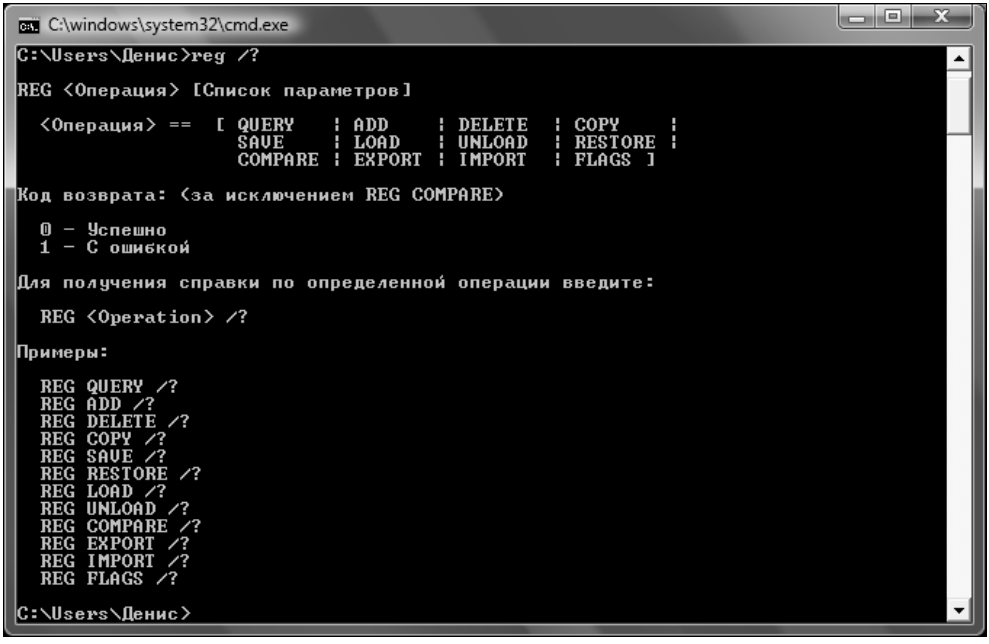


Рис. 14.1. Параметры программы reg

Рассмотрим несколько примеров:

```
reg add hklm\key
reg add hklm\key /v Value /t REG_DWORD /d 10
reg add hklm\key /ve /d data
reg query hklm\key /v Value
reg query hklm\key /ve
reg query hklm\key /s
```

Первая команда создает раздел `HKLM\key`, вторая — создает в этом разделе параметр `Value` типа `REG_DWORD` и присваивает ему значение 10. Третья команда присваивает значение по умолчанию (`Data`) разделу `HKLM\key`.

Четвертая команда выводит значение параметра `HKLM\key\Value`, пятая — отображает значение по умолчанию для раздела `HKLM\key`, а последняя команда — выводит значения всех параметров и подразделов раздела `HKLM\key`.

рация 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. — *Прим. ред.*

14.3. Резервное копирование реестра с помощью программы *reg*

Для резервного копирования реестра можно создать командный файл reg-backup.bat, текст которого приведен в листинге 14.1.

Листинг 14.1. Командный файл reg-backup.bat

```
CD\
MD C:\REG
CD C:\REG
REG EXPORT HKLM C:\REG\HKLM_BACK.REG
REG EXPORT HKCU C:\REG\HKCU_BACK.REG
REG EXPORT HKCR C:\REG\HKCR_BACK.REG
REG EXPORT HKCC C:\REG\HKCC_BACK.REG
REG EXPORT HKU C:\REG\HKU_BACK.REG
```

Данный командный файл сначала создает каталог C:\REG, а затем экспортирует в него ветви реестра. Для восстановления реестра можно использовать командный файл reg-restore.bat (листинг 14.2).

Листинг 14.2. Командный файл reg-restore.bat

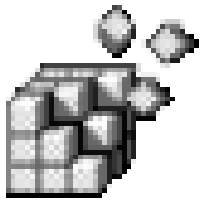
```
CD\
CD C:\REG
REG IMPORT HKLM_BACK.REG
REG IMPORT HKCU_BACK.REG
REG IMPORT HKCR_BACK.REG
REG IMPORT HKCC_BACK.REG
REG IMPORT HKU_BACK.REG
```

Данный файл сначала осуществляет переход в каталог C:\REG, а после — импортирует ранее экспортированные REG-файлы.

Примечание

Кроме программы reg.exe есть еще утилита regini.exe, которая используется для установки прав доступа к ключам реестра. О том, как использовать данную утилиту, вы можете прочитать по адресу **http://support.microsoft.com/kb/237607**.

ГЛАВА 15



Создание резервных копий реестра

15.1. Почему происходят сбои?

Первые версии Windows не отличались особой надежностью. Если вы ни разу не работали с Windows 3.11, то вы даже не можете себе представить, сколько раз в день она зависала. Временами просто не хватало терпения работать с ней. В этом случае разъяренный пользователь ее выгружал и запускал старый добрый Norton Commander. Windows 95 была, конечно, стабильнее, но не настолько, насколько хотелось бы. В 1996 году появилась операционная система Windows NT 4.0. Несмотря на то, что ее появление наделало гораздо меньше шума, чем появление Windows 95, данная операционная система считалась эталоном надежности.

В 1998 году появилась Windows 98. Она была однозначно надежнее, чем Windows 95, но до NT ей было далеко. Потом вышла следующая версия Windows — Windows ME. Не знаю, может это мне с ней так не повезло, или же просто Microsoft решила вспомнить прошлое, а именно Windows 3.11, — но по надежности и стабильности работы Windows ME недалеко ушла от Windows 3.11. Поэтому нет ничего удивительного в том, что некоторые пользователи о ней даже не слышали: ее очень быстро забыли.

Все последующие версии Windows — 2000, XP, Vista были построены по образу и подобию NT. Например, Windows Vista идентифицируется как NT 6.0, а Windows 7 — как NT 6.1.

Современные версии Windows довольно надежны — тут нужно отдать должно Microsoft. Windows XP проработала на моем компьютере два года без переустановки, в то время как предыдущие версии приходилось переустанавливать по несколько раз в год.

Но все же время от времени происходят сбои и в этих версиях. В 99% случаев они случаются из-за внесения неправильной информации в реестр: удаление

или некорректное редактирование параметра/раздела пользователем или какой-либо программой (случайно или намеренно).

Защитить реестр от некорректного вмешательства со стороны пользователей довольно просто — регулярно выполняйте его резервное копирование. Для этого существует три основных способа. Мы рассмотрим их все, и вы выберете тот, который понравится вам больше всего. Что же касается защиты от неправильного изменения реестра программами, то для этой цели лучше всего использовать точки восстановления системы, которые мы рассмотрим в следующей главе.

15.2. Защита реестра от неквалифицированного вмешательства пользователей

Вот три способа защиты системы от некорректных действий пользователя, о которых мы говорили в первом разделе этой главы:

- создание резервных копий непосредственно в реестре;
- экспорт параметров (или целых разделов) реестра в REG-файл;
- экспорт параметров (или целых разделов) реестра в файл куста.

15.2.1. Создание резервных копий непосредственно в реестре

Данный способ подходит, если вам нужно произвести небольшие изменения в реестре, например, модифицировать пару-тройку параметров. Способ даже не прост, а очень прост. Перейдите в раздел реестра, содержащий параметр, который вы хотите изменить. Создайте новый параметр такого же типа, как и изменяемый параметр. Имя нового параметра задайте так: `ВК_<имя параметра>`. Например, если имя исходного параметра `2`, то новый параметр будет называться `ВК_2` — это наша резервная копия. Дважды щелкните на исходном параметре. В окне изменения значения параметра скопируйте значение параметра в буфер обмена (рис. 15.1).

Затем дважды щелкните на резервной копии и вставьте значение исходного параметра в поле **Значение** (Value) резервной копии. Обратите внимание на рис. 15.2. У нас есть два параметра: `2` и `ВК_2` с одинаковыми значениями. Второй параметр — это резервная копия, которую можно использовать для восстановления значения исходного параметра, если что-то пойдет не так.

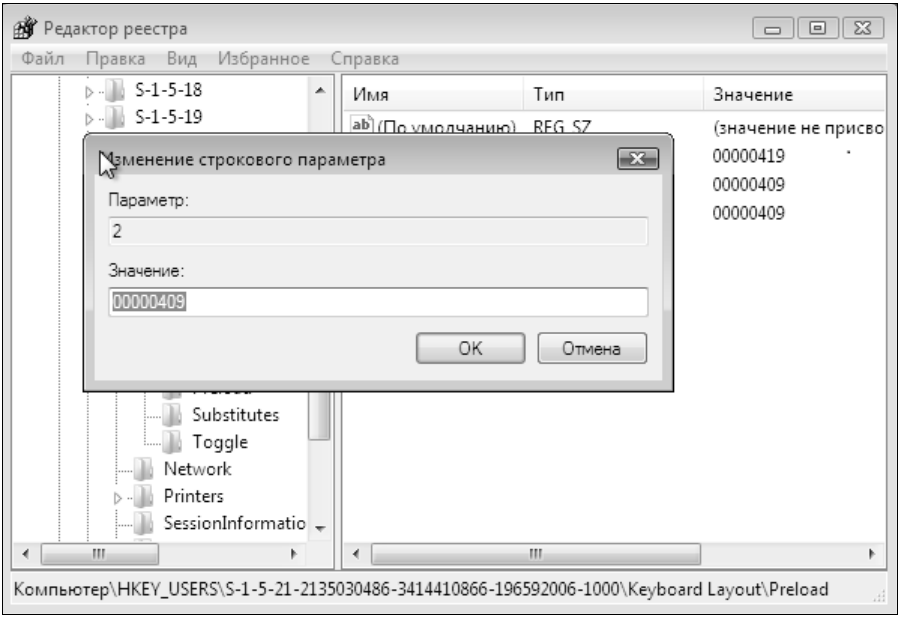


Рис. 15.1. Изменение параметра

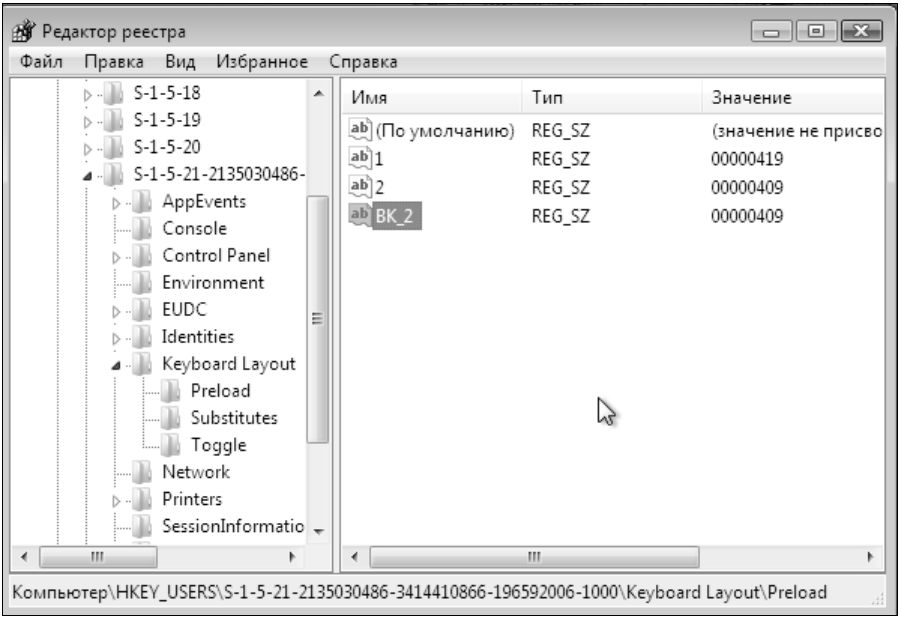


Рис. 15.2. Параметр и его резервная копия

После того как резервная копия создана, вы можете изменять исходный параметр. Если все в порядке, можете удалить резервную копию. Если же что-то пошло не так, удалите исходный параметр, а резервную копию переименуйте, удалив из ее имени строку `BK_`.

Преимущество этого способа заключается в том, что резервные копии параметров находятся рядом с исходными значениями. Но если вы затеяли "капитальную перестройку" реестра, затрагивающую не несколько параметров реестра, а целые ветви реестра, то вам нужно использовать или REG-файлы, или файлы кустов для хранения резервной копии реестра.

15.2.2. Экспорт параметров реестра в REG-файл

Суть этого способа заключается в следующем. Вы выбираете раздел или подраздел реестра, в котором собираетесь произвести изменения. Заметьте, что если выбрать корневой раздел целиком, то REG-файл получится очень большим. После этого выполните команду **Файл** (File) | **Экспорт** (Export). Выберите тип файла **Файлы реестра (*.reg)** (Registry Files (*.reg)), введите имя файла и нажмите кнопку **Сохранить** (Save), как показано на рис. 15.3. Обратите внимание: с помощью переключателей из группы **Диапазон экспорта** (Export Range) вы можете сохранить сразу весь реестр, однако сохранять реестр целиком удобнее с помощью точек восстановления системы, о которых мы поговорим в следующей главе. С другой стороны, учитывая, что ни файлы кустов, ни файлы точки восстановления вы не можете перенести на другой компьютер, можно экспортировать в REG-файл весь реестр и записать его на сменный носитель (например, CD-ROM): так вы будете совершенно уверены, что резервная копия находится в целости и сохранности.

Преимущество этого способа заключается в том, что с его помощью создается читаемый текстовый файл, который можно изменить с помощью любого текстового редактора.

Чтобы восстановить реестр из REG-файла, достаточно дважды щелкнуть по его имени в окне Проводника и утвердительно ответить на вопрос системы о добавлении его данных в реестр. При использовании REG-файлов для восстановления удаленных и неправильно измененных параметров реестра действуют следующие правила:

- если в реестре нет параметра, который есть в REG-файле, то редактор реестра создаст такой же параметр в реестре;
- если в реестре есть параметр с таким же именем, как в REG-файле, то редактор реестра восстановит значение параметра из REG-файла.

Более подробно о REG-файлах мы поговорим в *главе 22*, а пока перейдем к следующему разделу.

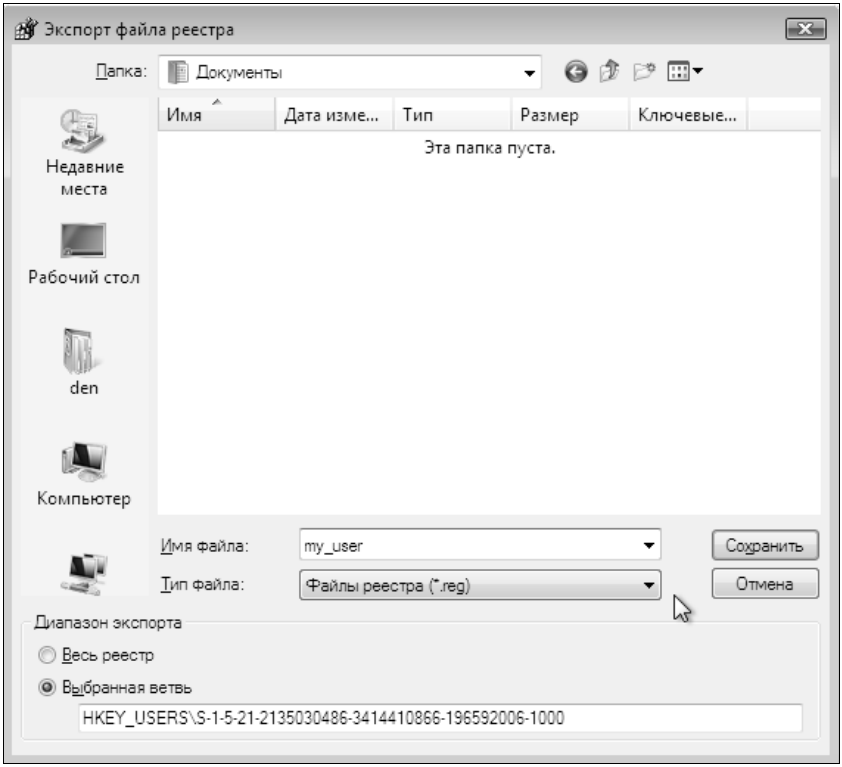


Рис. 15.3. Экспорт раздела реестра в REG-файл

15.2.3. Экспорт параметров реестра в файл куста

REG-файлы довольно удобны, но у них есть один большой недостаток, из-за которого их лучше не использовать для резервного копирования всего реестра. Предположим, что вы экспортировали весь реестр в REG-файл. После этого "вражеская" программа добавила в реестр какой-то параметр, из-за которого нарушилась работа всей системы. Если данного параметра нет в REG-файле, но он есть в реестре, при обработке REG-файла этот параметр сохранится, и система будет по-прежнему "глючить".

Выход из этой ситуации есть: экспорт реестра в файл куста, который имеет двоичный формат. Преимущество очевидно. Например, вы экспортировали весь `HKLM` в файл куста. При импорте файла куста раздел `HKLM` будет полностью удален, включая и параметры, созданные "вражеской" программой, а на его место будет установлен `HKLM` из выбранного вами файла куста. Улавливаете разницу?

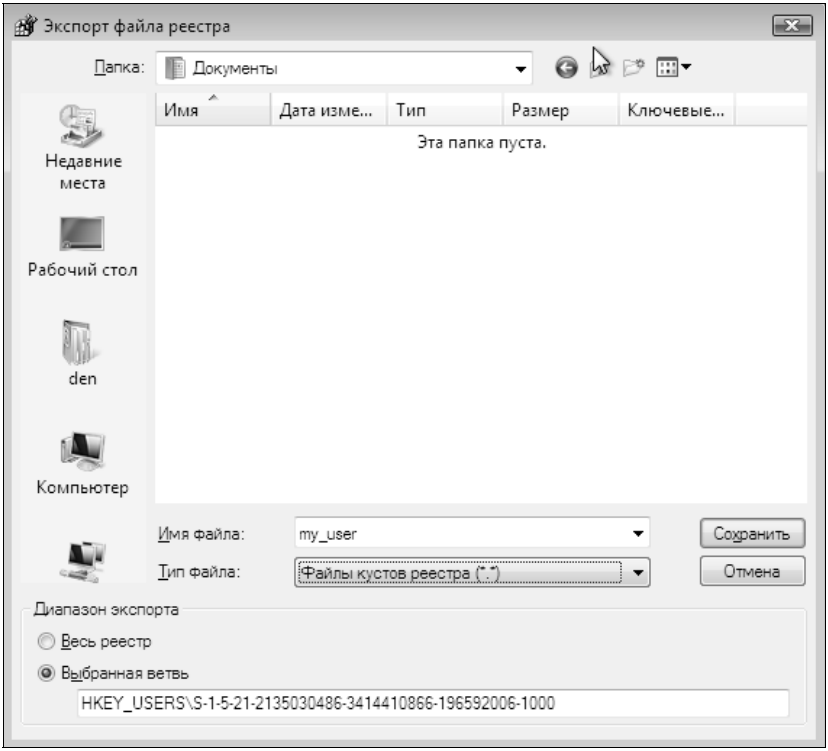


Рис. 15.4. Экспорт раздела реестра в файл куста

Для экспорта реестра в файл куста выберите команду **Файл** (File) | **Экспорт** (Export), в качестве типа файла выберите **Файлы кустов реестра** (Registry hive files), после чего затем нажмите кнопку **Сохранить** (Save) (рис. 15.4).

Для восстановления файла куста выполните команды **Файл** (File), **Импорт** (Import), в качестве типа файла укажите **Файлы кустов реестра** (Registry hive files), выберите файл куста и нажмите кнопку **Открыть** (Open).

Обратите внимание: в меню **Файл** (File) есть команды **Загрузить куст** (Load Hive) и **Выгрузить куст** (Unload Hive). Не нужно путать их с командами импорта/экспорта реестра.

При импорте файла куста происходит изменение рабочей части реестра. При загрузке файла куста в реестре создается новая ветка, которую можно просматривать и редактировать, но которая не влияет на работу системы. Это равносильно открытию еще одного документа в окне Word: оно никак не отображается на уже открытых документах.

Выгрузка куста удаляет ссылку на него из реестра. Вы можете выгружать только те файлы кустов, которые загрузили сами. Вы не можете выгрузить файл куста, который загрузила сама Windows.

15.2.4. Когда и какой способ выбрать?

Первый способ, как уже было отмечено, удобен, если нужно изменить один-два (в крайнем случае, три) параметра. Если параметров больше, то вы просто устанете создавать аналогичные и присваивать им значения. В этом случае вам намного удобнее будет использовать REG-файлы.

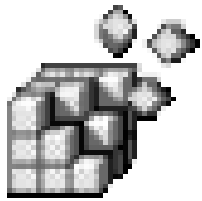
Можно экспортировать весь реестр в REG-файл, однако делать этого не стоит, поскольку восстановление реестра из REG-файла не всегда дает ожидаемые результаты (см. выше). Если нужно сохранить корневые разделы реестра (или весь реестр), намного удобнее и правильнее будет использовать экспорт в файлы кустов. У экспорта в REG-файлы есть еще одно огромное преимущество: невозможно скопировать файлы кустов, которые находятся в каталоге *%Systemroot%*\system32\config и *%Userprofile%*, если запущена Windows. При обращении к файлу вы получите сообщение о том, что файл не существует, несмотря на то, что он виден в оглавлении каталога. Чтобы скопировать эти файлы, нужно загрузить другую версию Windows, если она установлена на компьютере параллельно, или с загрузочного CD: вот тогда Windows не будет мешать копированию этих файлов. Но, согласитесь, не у каждого установлены две версии Windows, да и загрузочный диск не всегда есть под рукой. Поэтому намного удобнее экспортировать весь реестр в файлы кустов, а затем восстановить, когда это будет нужно. Созданные вами файлы кустов (например, путем экспорта реестра) вы можете свободно копировать, записывать на сменные носители и т. д.

15.3. Несколько советов

В заключение главы дадим несколько важных советов, связанных с реестром:

- если какая-то программа стала неправильно работать или вообще перестала запускаться (не важно, по какой причине), попробуйте удалить раздел реестра `HKCU\Software\<Производитель>\<Программа>`. Качественные программы умеют восстанавливать в реестре свои параметры по умолчанию и, вероятно, после этого все будет работать. Если же совет не помог, переустановите программу;
- если после изменения реестра перестало работать какое-либо устройство, откройте диалоговое окно **Свойства системы** (System Properties) при помощи сочетания клавиш <Win>+<Break>, перейдите на вкладку **Оборудование** и нажмите кнопку **Диспетчер устройств** (Device Manager). В окне диспетчера устройств выделите неправильно работающее устройство и нажмите клавишу <Del> для его удаления из системы. После этого перезагрузите компьютер.

ГЛАВА 16



Точки восстановления системы

16.1. Что это такое?

Точки восстановления системы (system restore points) — это "моментальные снимки" (snapshots) текущего состояния Windows, позволяющие вернуть систему к более раннему состоянию. Конечно, при таком откате будет потеряна часть настроек, включая список последних документов, списки истории, избранное, настройки прикладных программ, произведенные с момента создания последней точки восстановления. Но все это не имеет особого значения, когда речь идет о восстановлении всей системы — на восстановление пользовательских настроек уйдет меньше времени и сил, чем на переустановку системы и всех программ.

Для работы системы восстановления (System Restore) нужно, чтобы на диске имелось минимум 200 Мбайт (или не менее 300 Мбайт для Windows Vista/7) свободного пространства.

> ***Примечание***
>
> Если объем доступного дискового пространства на этом разделе падает ниже критического уровня, то функция восстановления системы автоматически блокируется.

Вообще же Windows резервирует под нужды системы восстановления 12% от общего объема жесткого диска (на жестких дисках объемом более 4 Гбайт, или 400 Мбайт — на дисках меньшего объема). В Windows Vista, System Restore 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 зарезервировать за собой до 5 процентов свободного диско-

вого пространства или не более 10 Гбайт (в зависимости от того, какое значение меньше). На жестких дисках объемом менее 64 Гбайт System Restore по умолчанию резервирует за собой не более 3 процентов дискового пространства.

Вы можете определить, для каких дисков нужно создавать точки восстановления, а для каких — нет. Также вы можете задать, сколько места может быть отведено под восстановление системы.

Для этого выполните следующие действия:

- Откройте окно **Система** (System). Проще всего для этого нажать клавиатурную комбинацию <Win>+<Break>.
- Щелкните по ссылке **Защита системы** (System Protection), расположенной в левой части окна.
- В открывшемся окне **Свойства системы** (System Properties) на вкладке **Защита системы** (System Protection) можно задать, для каких дисков нужно создавать точки восстановления, а для каких — нет (рис. 16.1).

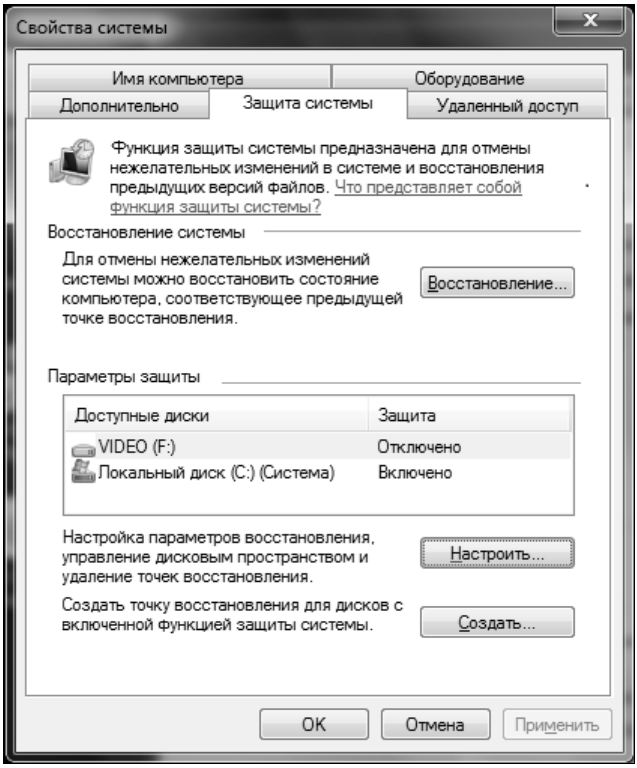


Рис. 16.1. Свойства системы: защита системы

- Выделите диск, параметры системы восстановления которого вы хотите изменить, и нажмите кнопку **Настроить** (Configure). На экране появится окно, показанное на рис. 16.2.

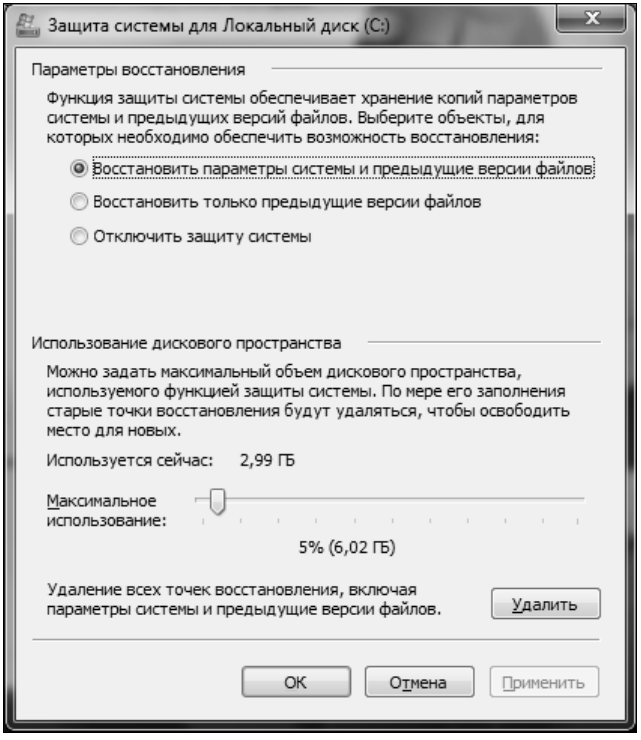


Рис. 16.2. Параметры системы восстановления для диска C:

- Вы можете выбрать один из вариантов защиты:
  - **Восстановить параметры системы и предыдущие версии файлов** (Restore system settings and previous versions of files) — для этого диска будут создаваться точки восстановления и храниться предыдущие версии файлов;
  - **Восстановить только предыдущие версии файлов** (Only restore previous versions of files) — для диска будут только храниться предыдущие версии файлов;
  - **Отключить защиту системы** (Turn off system protection) — система восстановления будет отключена для этого диска.
- После этого можно задать максимальный размер дискового пространства, который будет использоваться для хранения точек восстановления систе-

мы и предыдущих версий файлов — для этого используется ползунок **Максимальное использование** (Max. usage).

- Нажав кнопку **Удалить** (Delete), вы сможете удалить все точки восстановления и предыдущие версии файлов, если вам это нужно.
- Нажмите кнопку **ОК** для сохранения параметров.

> ***Примечание***
>
> Чтобы быстро вызвать окно, изображенное на рис. 16.1, можно нажать кнопку **Пуск** (Start), ввести команду `systempropertiesprotection` и нажать клавишу <Enter>.

Нужно помнить следующее:

- если размер диска менее 1 Гбайт, для него нельзя включить автоматическое создание точек восстановления системы;
- если на компьютере параллельно установлена Windows XP, то при запуске последней будут уничтожены все точки восстановления, которые создала Windows 7. Тут ничего не поделаешь: Windows XP просто еще не "знала" о том, что в планах Microsoft будет создание новой версии ОС. Единственное, что можно сделать — это отключить систему восстановления в XP[1].

> ***Примечание***
>
> Вам интересно, где физически хранятся точки восстановления? Они хранятся в каталоге System Volume Information. Такой каталог есть в корневом каталоге каждого диска (кроме сменных).

16.2. Типы точек восстановления

Существуют следующие типы точек восстановления:

- начальные точки — такие точки создаются при первом запуске Windows. С их помощью можно вернуть все настройки в исходное состояние и получить "чистую" Windows — в том виде, который она имела сразу после установки;
- контрольные точки системы — создаются каждые 24 часа вне зависимости от того, вносились ли в систему какие-либо изменения. Если компьютер был выключен более 24 часов, то Windows создаст точку восстановления сразу после запуска;
- контрольные точки установки — создаются при установке программ, чтобы можно было вернуть систему в состояние до установки программы;

[1] Лучше скрыть от Windows XP тот раздел, на котором установлена Windows Vista или Windows 7. О том, как это делается, уже рассказывалось в данной книге. — *Прим. ред.*

- контрольные точки пользователя — создаются вручную пользователем;
- контрольные точки службы автоматического обновления — перед каждым обновлением системы создается контрольная точка;
- контрольные точки восстановления — создаются перед восстановлением системы из более ранней контрольной точки (чтобы в случае, если стало еще хуже, можно было вернуться назад);
- контрольные точки драйверов — создаются перед установкой неподписанных драйверов устройств;
- резервные контрольные точки — создаются перед восстановлением системы утилитой Backup (тоже на случай, если после восстановления компьютер будет работать еще хуже).

16.3. Как создать точку восстановления

Иногда Windows почему-то "забывает" создать точку восстановления, поэтому желательно перестраховаться и создать ее вручную в следующих случаях:

- у вас есть несколько минут свободного времени, а ваш компьютер работает просто замечательно. Можно создать контрольную точку восстановления, чтобы в случае сбоя (а он может произойти и через 5 минут, и через неделю или вообще не произойти) можно было быстро вернуть систему в нормальное состояние. Если создавать такие точки восстановления хотя бы раз в неделю, то восстановить систему после сбоя будет гораздо проще;
- перед установкой/обновлением драйвера какого-либо устройства, даже если драйвер подписан производителем. Лишняя точка восстановления никогда не помешает;
- перед серьезной реорганизацией реестра. Хотя можно сделать резервную копию только реестра — это будет несколько экономнее по отношению к вашему дисковому пространству;
- перед установкой программы, которая может затронуть работу всей системы (например, брандмауэра, антивируса и т. д.).

Для создания точки восстановления нажмите кнопку **Пуск** (Start), щелкните правой кнопкой мыши по пункту **Компьютер** (Computer), из раскрывшегося контекстного меню выберите команду **Свойства** (Properties), затем нажмите ссылку **Защита системы** (System Protection). Вы увидите окно, изображенное на рис. 16.1. Нажмите кнопку **Создать** (Create). После этого нужно ввести имя контрольной точки (рис. 16.3) и подождать, пока система создаст точку восстановления.

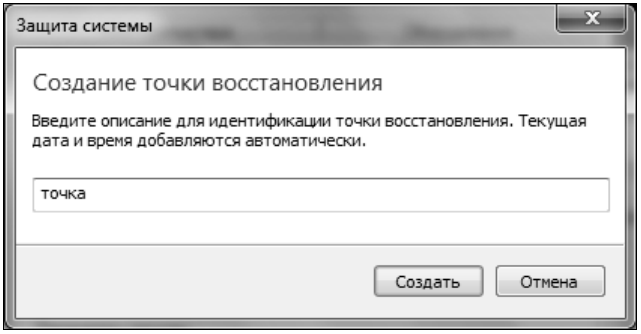


Рис. 16.3. Имя новой точки восстановления

Windows 7, в отличие от Vista, создает точку восстановления практически мгновенно, поэтому долго ждать не придется.

16.4. Как восстановить систему

Выполните команды меню **Пуск** (Start) | **Все программы** (All Programs) | **Стандартные** (Standard) | **Служебные** (System Tools) | **Восстановление системы** (System Restore). После чего появится окно **Восстановление системы** (System Restore), показанное на рис. 16.4. В этом окне можно выбрать или рекомендуемую системой точку восстановления или выбрать другую точку восстановления, отметив соответствующий режим программы восстановления (рис. 16.5).

В заключение вам нужно подтвердить выбор точки восстановления, нажав кнопку **Готово** (Finish). Если вы не уверены, то нажмите кнопку **Назад** (Back), чтобы вернуться к списку контрольных точек, или кнопку **Отмена** (Cancel) для выхода из окна восстановления системы (рис. 16.6).

16.5. Что делать, если Windows не загружается?

В некоторых особо сложных случаях восстановление системы может оказаться невозможным, потому что... Windows откажется загружаться. Что делать? Нужно попытаться загрузиться в безопасном режиме. Для этого до загрузки Windows нужно нажать клавишу <F8>. Современные компьютеры загружаются настолько быстро, что вы можете просто "прозевать" нужный момент. Поэтому клавишу <F8> можно нажимать сразу после окончания проверки памяти.

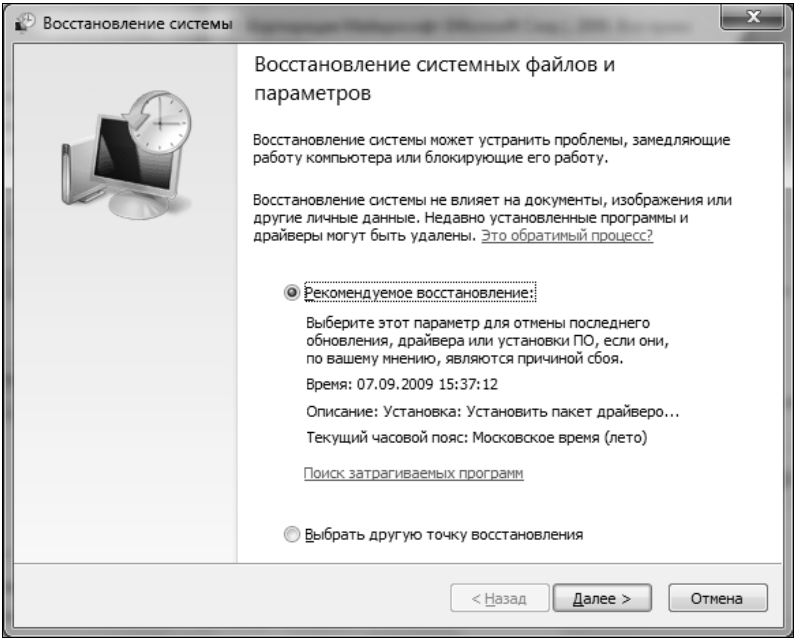


Рис. 16.4. Восстановление системы

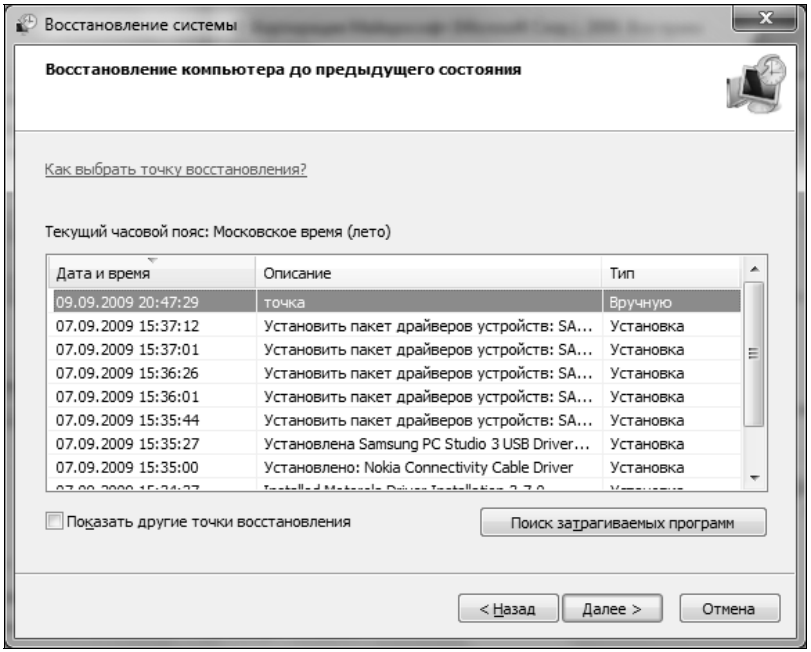


Рис. 16.5. Выбор другой точки восстановления

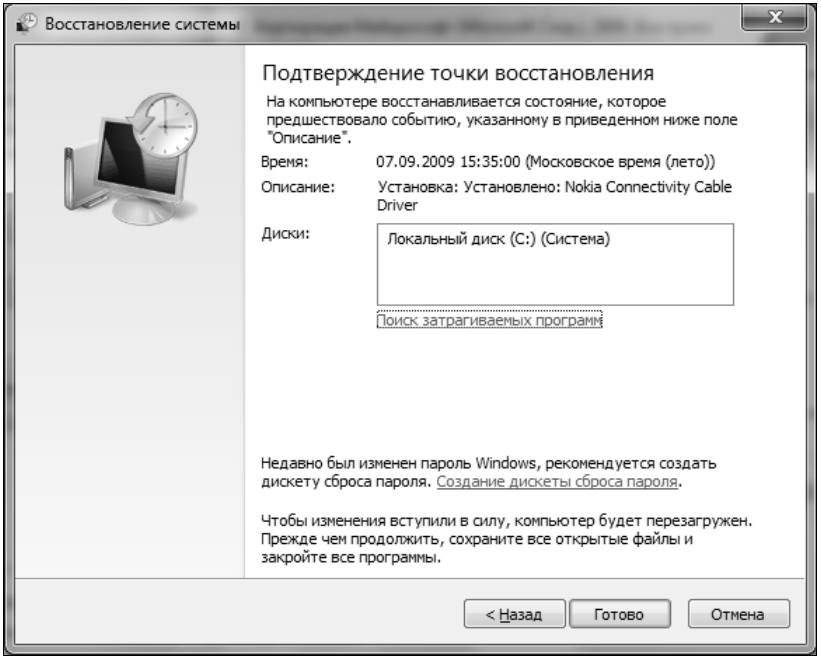


Рис. 16.6. Подтверждение выбора контрольной точки

Вы увидите меню возможных вариантов загрузки Windows (рис. 16.7):

- **Устранение неполадок компьютера** (Computer Troubleshooting) — данная команда отображает дополнительное меню, позволяющее выбрать средство восстановления системы.
- **Безопасный режим** (Safe Mode) — безопасный режим без поддержки сети. В этом режиме будут загружены только самые необходимые драйверы и службы.
- **Безопасный режим с загрузкой сетевых драйверов** (Safe Mode with Network support) — безопасный режим с поддержкой сети.
- **Безопасный режим с поддержкой командной строки** (Safe Mode with Command Prompt) — безопасный режим, но вместо Проводника будет использоваться командная строка (в качестве оболочки системы).
- **Ведение журнала загрузки** (Enable Boot Logging) — журнал сохраняется в файле C:\BOOTLOG.TXT.
- **Включение видеорежима с низким разрешением** (Enable low resolution video (640×480)) — помогает устранить проблемы с драйверами видеокарты — после загрузки в таком режиме можно обновить драйвер видеокарты.

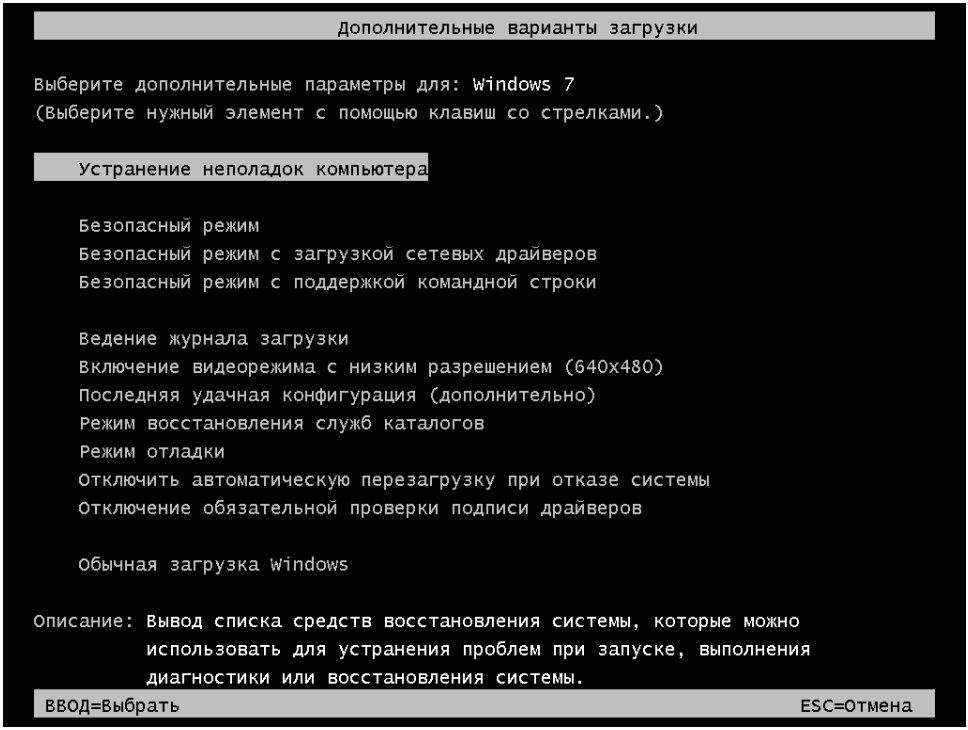


Рис. 16.7. Меню дополнительных вариантов загрузки Windows

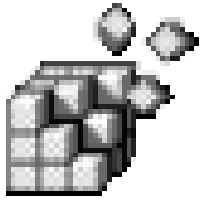
- **Последняя удачная конфигурация** (Last Known Good Configuration (Advanced)) — позволяет восстановить последнюю конфигурацию, при которой компьютер нормально загружался. Именно этот пункт меню позволяет в большинстве случаев привести Windows "в чувство"[1].
- **Режим восстановления служб каталогов** (Directory Services Restore Mode) — позволяет восстановить ActiveDirectory.
- **Режим отладки** (Debugging Mode) — запускает Windows в отладочном режиме.
- **Отключить автоматическую перезагрузку при отказе системы** (Disable automatic restart on system failure) — при критической ошибке компьютер сразу перезагружается и вы не успеваете прочитать сообщение об ошибке.

[1] Использование этого пункта меню имеет смысл, только если вы после сбоя ни разу не регистрировались в системе. Дело в том, что сразу же после успешной регистрации происходит перезапись последней успешно загруженной конфигурации, после чего использование данной опции вам уже не поможет. — *Прим. ред.*

Отключив автоматическую перезагрузку, вы сможете полюбоваться "синим экраном смерти" (кстати, в Windows 7 он тоже синий).

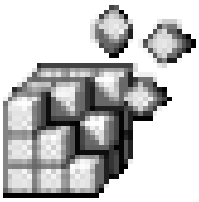
- **Отключение обязательной проверки подписей драйверов** (Disable Driver Signature Enforcement) — эту команду меню нужно выбрать, если есть проблемы с цифровой подписью драйвера, но лучше обновить драйвер, иначе придется выбирать эту команду при каждом запуске системы.
- **Обычная загрузка Windows** (Start Windows Normally) — обычный запуск Windows.

ЧАСТЬ II



Для администраторов

ГЛАВА 17



Параметры системы восстановления Windows (Vista и Windows 7)

17.1. Как работает система восстановления

В *главе 16* мы научились пользоваться системой восстановления Windows. В этой главе мы изучим данную систему "изнутри".

Как было сказано в *главе 16*, система восстановления хранит точки восстановления в каталоге System Volume Information, который есть на каждом логическом диске Windows. Данный каталог скрыт, поэтому, чтобы увидеть его, вы должны включить отображение скрытых и системных файлов и папок. А чтобы получить доступ к этой папке (войти в нее), вы должны быть зарегистрированы от имени учетной записи `Администратор` (`Administrator`). В Windows Vista и Windows 7 по умолчанию эта учетная запись отключена. Для ее включения нужно выполнить команду (в русской версии Windows):

```
net user Администратор /active:yes
```

В английской версии используется команда:

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

Команду нужно вводить в командной строке с повышенными правами пользователя. Для этого щелкните правой кнопкой мыши на ярлыке командной строки и выберите команду **Запуск от имени администратора** (Run as Administrator).

Вообще говоря, в этой папке все равно нет ничего интересного, поскольку все имена файлов закодированы. Это сделано специально, чтобы для восстановления системы вы использовали программу восстановления.

Сама же программа восстановления системы называется rstrui.exe и находится в каталоге *%Systemroot%*\system32. В каталоге *%Systemroot%*\system32\Restore находится файл MachineGuid.txt, содержащий уникальный идентификатор компьютера (он используется для идентификации точек восстановления).

17.2. Настройка системы восстановления с помощью реестра

В *главе 16* мы научились настраивать параметры системы восстановления с помощью графического интерфейса Windows. В этой главе мы поговорим о том, как настроить эту систему с помощью реестра. Но сначала обсудим, как немного сэкономить дисковое пространство без изменения реестра.

Если ваш компьютер работает стабильно и никаких "ЧП" замечено не было, вы можете удалить все точки восстановления, кроме последней. Для этого выполните команды **Пуск** (Start) | **Компьютер** (Computer), щелкните правой кнопкой на диске C:, выберите из контекстного меню команду **Свойства** (Properties). В появившемся окне нажмите кнопку **Очистка диска** (Disk clean-up). Выберите опцию **Файлы всех пользователей на этом компьютере** (All user files on this computer), как показано на рис. 17.1. В окне UAC нажмите **Продолжить** (Continue) и немного подождите. В окне **Очистка диска** (Disk clean-up) (рис. 17.2) перейдите на вкладку **Дополнительно** (Advanced). В группе **Восстановление системы и теневое копирование** (System Restore and Volume Shadow Copy) нажмите кнопку **Очистить** (Clear). Появится окно, изображенное на рис. 17.3 — нажмите кнопку **Удалить** (Delete). После этого будут удалены все точки восстановления, кроме самой последней.

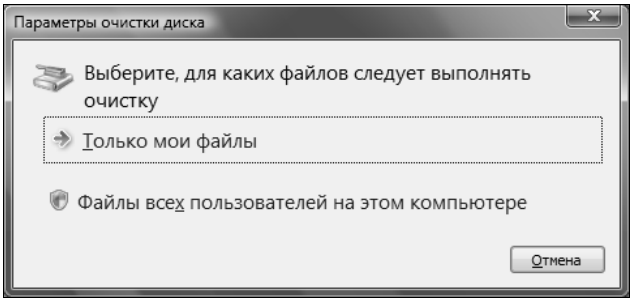


Рис. 17.1. Выберите
Файлы всех пользователей на этом компьютере

Примечание

Чтобы проделать то же самое в Windows XP, откройте окно **Мой компьютер** (My Computer), выберите диск C:, щелкните правой кнопкой мыши и выберите

из контекстного меню пункт **Свойства** (Properties), затем нажмите кнопку **Очистка диска** (Disk clean-up). Перейдите на вкладку **Дополнительно** (Advanced) и нажмите кнопку **Очистить** (Clear) в группе **Восстановление системы** (System Restore).

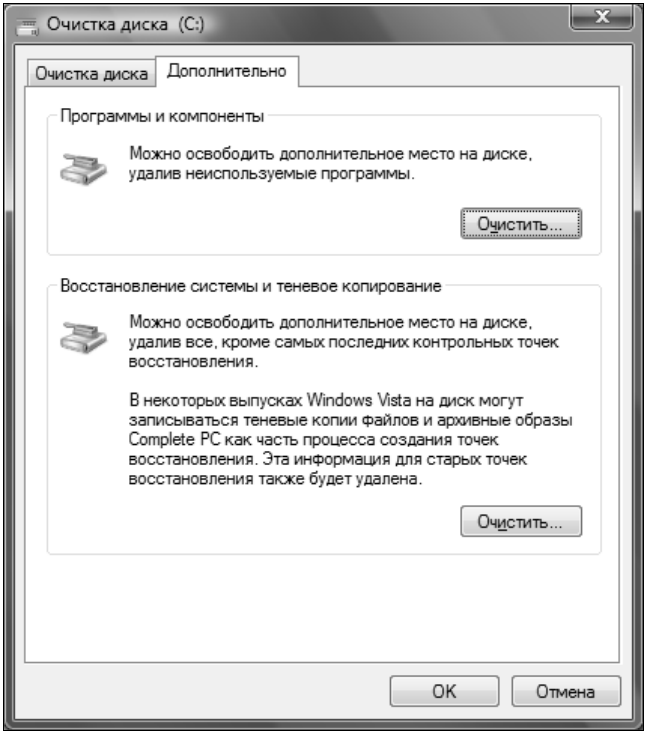


Рис. 17.2. Окно **Очистка диска**

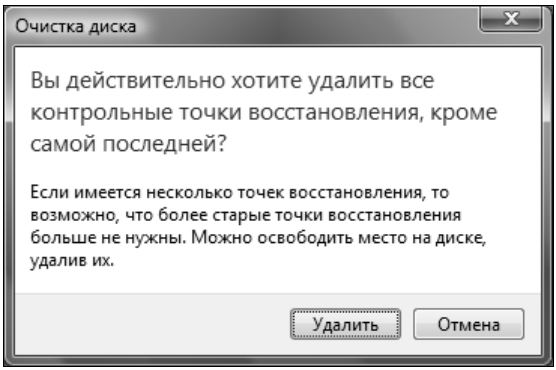


Рис. 17.3. Нажмите кнопку **Удалить**

В результате выполненных действий будут удалены все точки восстановления, кроме последней. Можно сказать, что пару сотен мегабайт дискового пространства вы уже сэкономите.

Если у вас слабый компьютер или жесткий диск небольшого размера, скажем 20 Гбайт или меньше, вы можете вообще отключить систему восстановления. О том, как это сделать, было сказано в *главе 16*.

Теперь можно приступить к рассмотрению параметров системы восстановления. Параметры системы восстановления хранятся в двух разделах реестра: в `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore` (см. табл. 17.1) и `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SPP\Clients`.

Таблица 17.1. *Параметры раздела* `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore`

Параметр	Описание
`CompressionBurst`	Время сжатия при простое системы, на протяжении которого будут запаковываться файлы, помещаемые в точку восстановления. Система восстановления будет упаковывать файлы указанное количество секунд, а затем прекратит операцию до следующего простоя
`DiskPercent`	Объем дискового пространства в % от размера диска, которое может использоваться для хранения точек восстановления (по умолчанию составляет 12%). Система восстановления выбирает большее из значений данного параметра и `DSMax`
`DSMax`	Максимальный объем дискового пространства, которое может отводиться для хранения точек восстановления, задается в мегабайтах (по умолчанию равно 400 Мбайт). Система восстановления выбирает наибольшее из значений данного параметра и `DiskPercent`
`DSMin`	Минимальный объем дискового пространства, доступного системе восстановления. Указывается в мегабайтах
`RestoreStatus`	Статус последней операции системы восстановления: `0×00` — последняя операция завершена с ошибкой; `0×01` — последняя операция завершена успешно; `0×02` — последняя операция прервана
`RPGlobalInterval`	Интервал между созданием контрольных точек (указывается в секундах). Обычно равен 24 ч или `0x15180` в шестнадцатеричной системе
`RPLifeInterval`	Время жизни контрольной точки в секундах. По умолчанию 90 суток или `0x76A700` в шестнадцатеричной системе

Таблица 17.1 *(окончание)*

Параметр	Описание
`RPSessionInterval`	Время ожидания в секундах перед созданием новой контрольной точки при включенном компьютере. По умолчанию используется значение `0`, что означает, что данная возможность отключена
`ThawInterval`	Время ожидания в секундах для продолжения работы после освобождения достаточного объема свободного места для создания контрольной точки
`DisableSR`	Отключение системы восстановления при значении, равном 1, при этом все ее параметры будут сохранены. Если вы отключите систему восстановления через GUI (графический интерфейс пользователя), то все ее параметры при включении вернутся к значениям по умолчанию. В связи с этим лучше отключить систему восстановления через реестр

Примечание

Все параметры, описанные в табл. 17.1, имеют тип `REG_DWORD`, а все значения приведены в десятичной системе, кроме тех, которые явно указаны в шестнадцатеричной (`0x`).

Остальные параметры, которые вы встретите в `HKLM\ SOFTWARE\ Microsoft\ Windows NT\CurrentVersion\SystemRestore`, лучше не изменять.

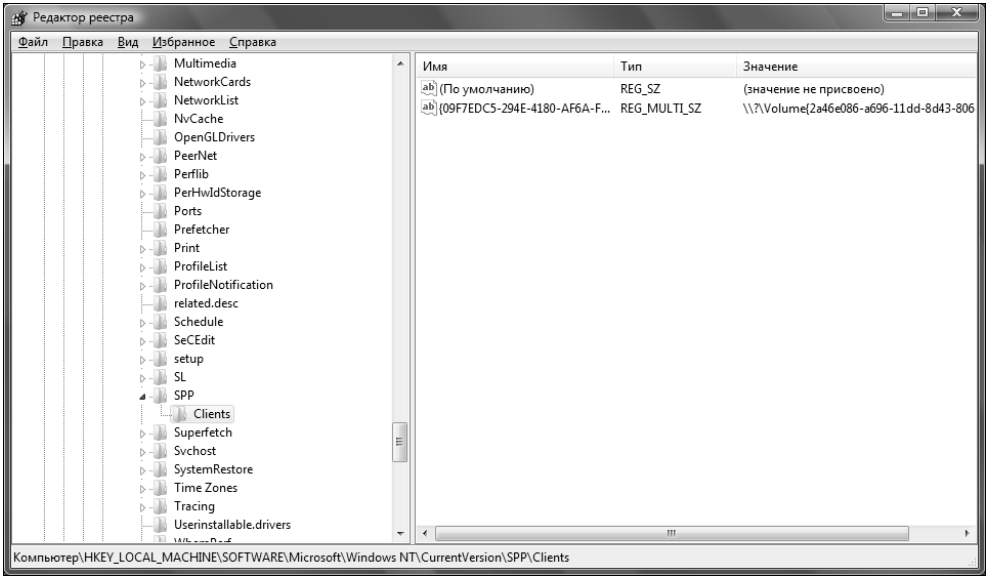


Рис. 17.4. Раздел реестра
`HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SPP\Clients`

Во втором разделе реестра (HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SPP\Clients) хранятся параметры создания точек восстановления. Например, список всех разделов диска, для которых разрешено создание точки восстановления, содержится в параметре {09F7EDC5-294E-4180-AF6A-FB0E6A0E9513} с типом данных REG_MULTI_SZ (рис. 17.4). Вы также можете создать два параметра типа REG_DWORD:

- CreateTimeout — определяет тайм-аут создания теневой копии (в миллисекундах) при создании новой точки восстановления. Если тайм-аут вышел, а теневая копия создана не будет, создание точки восстановления будет завершено ошибкой;
- DisableOptimizedRPCreation — позволяет отключить оптимизацию при создании точки восстановления.

17.3. Теневые копии в Windows 7

Служба восстановления тесно связана со службой теневого копирования. В ОС Windows Vista и Windows 7 окно свойств любого файла или каталога

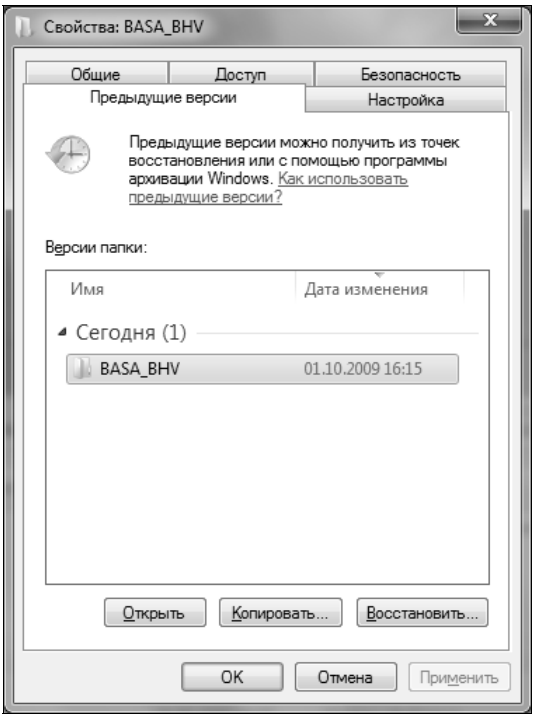


Рис. 17.5. Предыдущие версии

содержит новую вкладку — **Предыдущие версии** (Previous Versions). На этой вкладке вы можете просмотреть список копий файла или каталога, созданных ранее с помощью службы теневого копирования. Вы также можете открыть любую копию файла или каталога (кнопка **Открыть** (Open)), создать новую теневую копию (кнопка **Копировать** (Copy)), а также восстановить содержимое файла на основании одной из теневых копий (кнопка **Восстановить** (Restore)).

17.3.1. Управление теневыми копиями из командной строки

Для управления теневыми копиями из командной строки используется утилита vssadmin.exe, находящаяся в каталоге %systemroot%\system32\. Примеры использования этой утилиты приведены в табл. 17.2.

Таблица 17.2. *Примеры использования утилиты vssadmin.exe*

Команда	Описание
`vssadmin.exe list shadows`	Отображает список существующих теневых копий файлов и предоставляет подробную информацию о каждой копии — ее идентификатор, раздел диска, имя компьютера, атрибуты файла и т. д.
`vssadmin.exe list writers`	Отображает компоненты системы, которые могут создавать теневые копии
`vssadmin.exe list shadowstorage`	Показывает список хранилищ теневых копий на вашем компьютере
`vssadmin.exe list volumes`	Показывает список всех разделов вашего компьютера

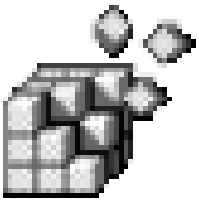
17.3.2. Отключение вкладки *Предыдущие версии* и задание других параметров теневых копий

Параметры теневого копирования хранятся в разделе реестра `HKCU\Software\Policies\Microsoft\PreviousVersions`. Все параметры имеют тип `REG_DWORD`. Вот список параметров:

- `DisableBackupRestore` — установите значение `1`, если хотите отключить теневое копирование;
- `DisableLocalPage` — отключает вкладку **Предыдущие версии** в окне свойств локальных файлов/каталогов (при значении `1`);

- `DisableLocalRestore` — при значении `1` запрещает восстановление копий, расположенных на локальном диске компьютера;
- `DisableRemotePage` — отключает вкладку **Предыдущие версии** в окне свойств удаленных файлов/каталогов, расположенных в общих папках (при значении `1`);
- `DisableRemoteRestore` — при значении `1` запрещает восстановление копий, расположенных в общих папках;
- `HideBackupEntries` — запрещает (при значении `1`) восстановление файла из копий, которые хранятся на архивных носителях.

ГЛАВА 18



Защита системы с помощью реестра

18.1. Общие параметры

В одной из глав я обещал вам, что расскажу, как запретить вызов редактора реестра. В этой главе мы поговорим не только об этом, но и обо всем, что сделает вашу систему более защищенной.

18.1.1. Отключение редактора реестра

Неопытным пользователям не нужно разрешать запускать редактор реестра regedit.exe и другие средства редактирования реестра. Для запрета запуска редактора реестра выполните следующие действия:

1. Добавьте параметр с типом данных `REG_DWORD` и именем `DisableRegistryTools` со значением `0` в раздел `HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System`.
2. Экспортируйте вышеуказанный раздел реестра в REG-файл.
3. Измените значение параметра `DisableRegistryTools` на `1`.

Когда вам самим понадобится редактор реестра, вы сможете запустить созданный вами REG-файл для установки параметра `DisableRegistryTools` в `0`, иначе запустить редактор реестра у вас не получится.

18.1.2. Запрет запуска диспетчера задач

Существуют программы, устанавливающие ограничения на время работы конкретных пользователей за компьютером. Например, вы можете установить такую программу, чтобы она контролировала время, проведенное за компьютером вашим ребенком. Но дети развиваются очень быстро, и если

еще вчера ваш ребенок только осваивал азы работы с компьютером, то сегодня он вполне может запустить диспетчер задач и завершить ненавистную ему программу — после этого он сможет играть в любимую игрушку без всяких ограничений. Чтобы такого не произошло, нужно запретить запуск диспетчера задач. Для этого в разделе `HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System` создайте параметр с типом данных `REG_DWORD`, назовите его `DisableTaskMgr` и присвойте ему значение `1`.

После этого запуск диспетчера задач будет невозможен. Впрочем, данный метод действительно рассчитан на совсем "зеленых" новичков, так что вы можете даже не надеяться на то, что ваше чадо не узнает о существовании Total Commander, плагин TaskManager которого позволяет "убивать" процессы одним нажатием клавиши <F8>. Так что наилучший метод воспитания ребенка — это побольше проводить с ним времени, и заинтересовать его еще хоть чем-то, кроме игрушек.

18.1.3. Запрет запуска Панели управления

Запрещать отдельные вкладки того или иного апплета **Панель управления** (Control Panel) — это рутинная работа. Гораздо проще запретить запуск всей Панели управления. Для этого перейдите в раздел `HKCU\Software\Microsoft\Windows\CurrentVersion\ Policies\Explorer`, добавьте параметр с типом данных `REG_DWORD` `NoControlPanel` и присвойте ему значение `1`.

18.1.4. Запрет запуска программ

Вы можете составить "черный" список приложений: приложения из этого списка не могут быть запущены пользователем. Для этого создайте раздел `HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowRun`. Параметры в этом разделе создаются так:

имя параметра: *N*

тип: `REG_SZ`

значение: `имя exe-файла программы`

где *N* — это порядковый номер параметра. На рис. 18.1 приведен небольшой "черный" список программ.

18.1.5. Запрет запуска командной строки

Для запрета запуска командной строки перейдите в раздел реестра `HKCU\Software\Policies\Microsoft\Windows\System` и добавьте параметр `DisableCMD` (тип данных — `REG_DWORD`).

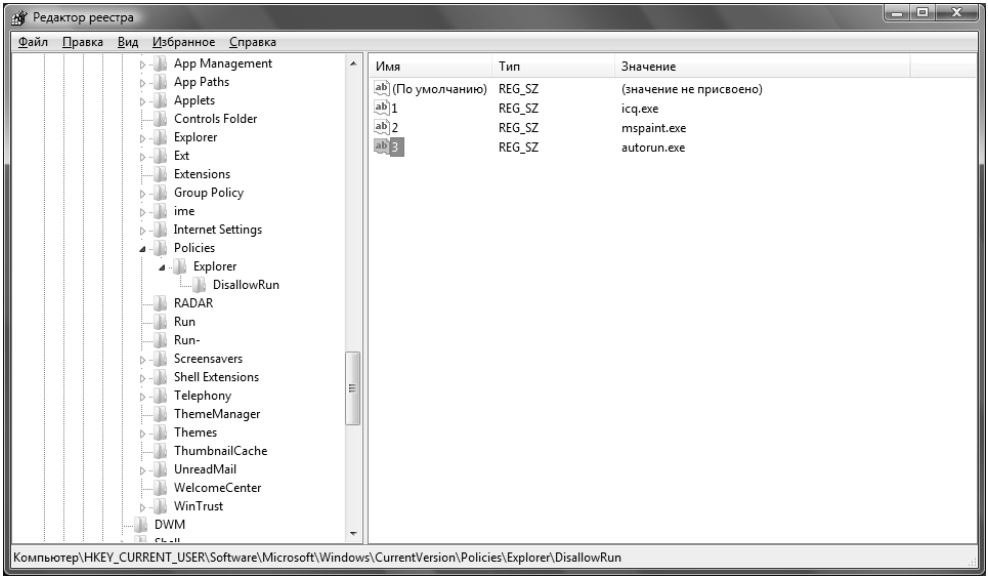


Рис. 18.1. "Черный" список программ

Вот допустимые значения этого параметра:

- `0` — разрешить использование командной строки;
- `1` — запретить использование командной строки;
- `2` — разрешить запуск командных файлов.

18.1.6. Запрещение изменения меню *Пуск*

Если вы не хотите, чтобы пользователь имел возможность редактировать меню **Пуск** (Start), например, добавлять, удалять или изменять пункты меню, добавьте в раздел `HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer` параметр `NoChangeStartMenu` (тип данных — `REG_DWORD`) со значением `1`.

18.2. Вход в систему и пароли

18.2.1. Запрет кэширования пароля для входа в сеть

Windows кэширует пароль для входа в сеть на локальном компьютере, чтобы при повторном входе в сеть пользователь мог его не вводить. Из соображений безопасности рекомендуется отключить эту функцию. Конечно, при каж-

дом входе в сеть пользователю придется вводить пароль заново, но это даже к лучшему. Во-первых, никто другой не сможет войти под именем пользователя, во-вторых, пользователь никогда не забудет свой пароль.

Запретить кэширование пароля можно с помощью параметра с типом данных `REG_DWORD` и именем `DisablePwdCaching` в разделе `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\`. По умолчанию данного параметра нет, поэтому его придется создать и присвоить ему значение `1`.

Также нужно запретить кэширование пароля домена: для этого необходимо присвоить значение, равное `1`, параметру с типом данных `REG_DWORD` и именем `NoDomainPwdCaching` из раздела `HKEY_LOCAL_MACHINE\Network\Logon`.

18.2.2. Запрет кэширования интернет-паролей

Windows также запоминает пароли, которые пользователь вводит при входе на сайты, защищенные паролями, если активна опция сохранения пароля. Многие пользователи ленятся вводить пароль при каждом входе на сайт, поэтому разрешают Windows запомнить пароль. Из соображений безопасности лучше отключить функцию запоминания пароля. Для этого выполните следующие действия:

- перейдите в раздел `HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings`;
- создайте параметр с типом данных `REG_DWORD` и именем `DisablePasswordCaching` и присвойте ему значение `1`.

Включение данного параметра отключает возможность запоминания пароля при входе на сайт.

18.2.3. Запрет запоминания пароля сетевого подключения

Windows может запоминать пароли сетевых подключений (для удаленного доступа к сети). Для отключения этой возможности создайте параметр `REG_DWORD DisableSavePassword` в разделе `HKLM\SYSTEM\CurrentControlSet\Services\RasMan\Parameters`. Значение параметра, равное `1`, отключает запоминание пароля сетевых подключений.

18.2.4. Установка минимальной длины пароля

С помощью параметра `MinPwdLen` (тип данных — `REG_DWORD`) можно установить минимальную длину пароля пользователя. Данный параметр находит-

ся в разделе HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Network. Значение этого параметра — минимальная длина пароля (в символах).

Данный параметр бесполезен для домашних пользователей, но очень пригодится администраторам. Пользователи слишком часто устанавливают очень короткие пароли, например, 1 или 123, а с помощью этого параметра можно заставить пользователя придумать более длинный пароль.

> ***Примечание***
>
> В этом и в следующем совете имеются в виду пароли для входа в систему, а не пароли для доступа к сайту или пароли сетевых подключений.

18.2.5. Усложнение пароля

Вы можете установить минимальную длину пароля хоть 8, хоть 10 символов, а пользователь все равно установит пароль наподобие этого: 12345678. Нужно заставить его придумать более оригинальный пароль. Для этого создайте параметр AlphanumPwds (тип данных — REG_DWORD) в разделе HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Network. После присвоения этому параметру значения 1 Windows будет требовать от пользователя алфавитно-цифровой пароль, т. е. пароль, содержащий как цифры, так и буквы.

18.2.6. Вывод сообщения при входе в систему

Вы хотите, чтобы все пользователи видели установленное вами сообщение при входе в систему? Тогда перейдите в раздел HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon и найдите два параметра с типом данных REG_SZ — legalnoticecaption и legalnoticetext. Первый из них задает заголовок индивидуального сообщения, а второй — собственно сам текст[1].

[1] Обратите внимание на то, что это — очень старый совет, который работал не только в Windows Vista, но и в Windows XP. Следует также иметь в виду, что аналогичные параметры с теми же именами лучше создавать не под ключом HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon, а под ключом HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system. Дело в том, что параметры, расположенные под этим ключом, имеют приоритет. Если аналогичные параметры существуют и под ключом HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system, и под ключом Winlogon, то значения под ключом Winlogon действовать не будут. — *Прим. ред.*

18.2.7. Автоматический вход в систему

Если вы — единственный пользователь домашнего компьютера, можете настроить автоматический вход в систему. Тогда вам не придется каждый раз при запуске системы выбирать пользователя и вводить пароль[1].

Перейдите в раздел `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon` и найдите параметр `AutoAdminLogon` (тип данных — `REG_SZ`). Присвойте ему значение `1`. Затем присвойте значения следующим параметрам (все они тоже имеют тип данных `REG_SZ`):

- `DefaultUserName` — имя пользователя для входа в систему;
- `DefaultPassword` — пароль для входа в систему;
- `DefaultDomainName` — домен по умолчанию (если вы работаете в сети);
- `ForceAutoLogon` — значение параметра, равное `1`, обеспечивает принудительный вход в систему.

18.2.8. Требование пароля при выходе из спящего/ждущего режима

При выходе из спящего режима Windows обычно не требует пароль. А это нежелательно, поскольку на момент выхода компьютера из спящего режима за компьютером может оказаться посторонний. Чтобы Windows запрашивала пароль, нужно создать параметр `PromptPasswordOnResume` (тип данных — `REG_DWORD`) со значением `1` в разделе `HKLM\SOFTWARE\Policies\Microsoft\Windows\System\Power`.

18.3. Сетевая безопасность

18.3.1. Запрет подключения сетевых дисков

Отключить появление кнопок **Подключить сетевой диск** (Connect Network Drive) и **Отключить сетевой диск** (Disconnect Network Drive) на панели инструментов Проводника можно с помощью параметра `NoNetConnectDisconnect` в разделе `HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`

[1] 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 к информации, хранящейся в нем, а также потенциально и ко всем сетям, к которым он подключен. — *Прим. ред.*

(тип данных — REG_DWORD). Если параметру NoNetConnectDisconnect присвоено значение 1, пользователь не увидит данных кнопок.

18.3.2. Удаление значка *Вся сеть* в Windows 2000/XP

Параметр NoEntireNetwork (тип данных — REG_DWORD) раздела HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Network при значении 1 удаляет значок **Вся сеть** (Entire Network) в окне **Сетевое окружение** (Network Environment).

18.3.3. Запрет просмотра общих ресурсов анонимными пользователями

Параметр с типом данных REG_DWORD и именем RestrictAnonymous (значение 1) в разделе HKLM\System\CurrentControlSet\Control\Lsa позволяет запретить анонимным пользователям просматривать общие ресурсы и учетные записи пользователей.

18.4. Отключение UAC в Windows Vista и Windows 7

18.4.1. Основной способ отключения UAC

UAC (User Account Control) — контроль учетных записей пользователей Windows. Впервые UAC появился в Windows Vista. Компонент UAC запрашивает подтверждение действий, требующих прав администратора, из соображений безопасности. Вирус или другая вредоносная программа, которой необходимы права администратора, не сможет их получить, поскольку UAC приостановит выполнение программы до вашего разрешения. Если вы знаете, что это за программа, вы можете продолжить ее выполнение или завершить ее.

Недостатков у UAC — два. Первый заключается в том, что UAC раздражает своей назойливостью, особенно если производится много административных действий. Второй заключается в том, что окно UAC не выводит достаточного объема информации о том, что собирается сделать программа.

UAC отключается элементарно — через Панель управления (Control Panel), для этого даже не нужно редактировать реестр.

Для отключения UAC выполните следующие действия:

1. Откройте окно **Панель управления** (Control Panel) и зайдите в раздел **Учетные записи пользователей и семейная безопасность** (User accounts and Parental Controls). Откроется окно, показанное на рис. 18.2.

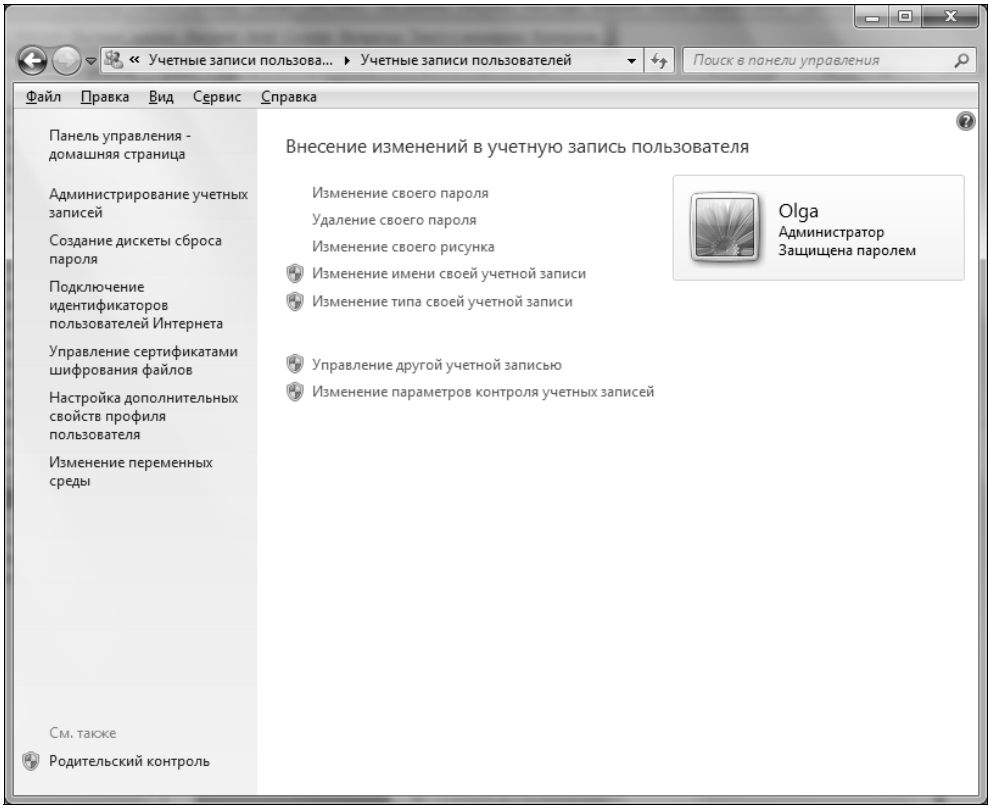


Рис. 18.2. Внесение изменений в учетную запись пользователя

2. Выберите команду **Включение или отключение контроля учетных записей (UAC)** (Change User Account Control (UAC) Parameters). Откроется окно, показанное на рис. 18.3.
3. Обратите внимание, что, в отличие от Windows Vista, где имелось только две возможности (включение и выключение UAC), в Windows 7 появились две промежуточных 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 (см. рис. 18.3).

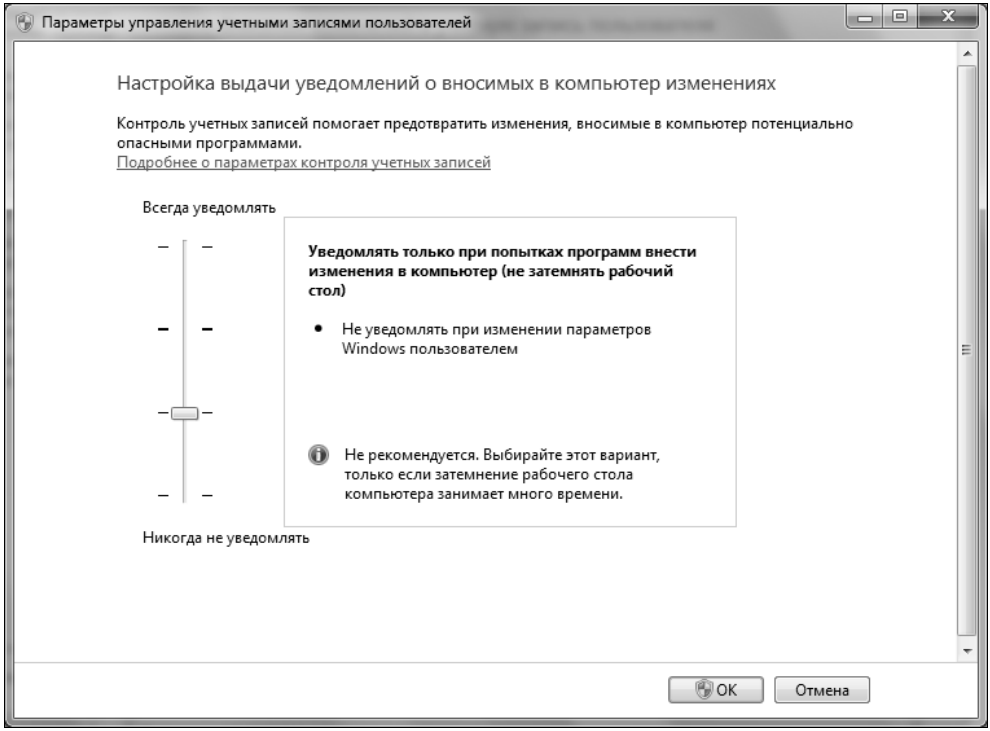


Рис. 18.3. Настройка уровней выдачи уведомлений UAC — новая возможность Windows 7

4. Выбрав нужный вариант настройки, нажмите кнопку **OK** и согласитесь с уведомлением, выведенным UAC.
5. Перезагрузите компьютер

Примечание

Из соображений безопасности лучше не отключать UAC. Делать это рекомендуется только в том случае, если вы установили сверхнадежный брандмауэр. Но вот сделать работу с UAC немного более удобной — можно и нужно. Для этого просто выберите вариант настройки, отключающий затемнение экрана (рис. 18.3). Разумеется, сделать это можно и через реестр. Для этого перейдите в следующий раздел реестра:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
```

Найдите параметр `PromptOnSecureDesktop` и присвойте ему значение `0`. Закройте редактор реестра и перезагрузите компьютер.

18.4.2. Альтернативный способ настройки UAC

Существует еще, как минимум, два способа выполнить настройку UAC. Первый из них заключается в запуске утилиты Msconfig.exe. Нажмите клавиатурную комбинацию <Win>+<R>, введите команду `msconfig` и нажмите клавишу <Enter>. В появившемся окне перейдите на вкладку **Сервис** (Tools), выберите команду **Изменение параметров контроля учетных записей** (Modify User Account Control Parameters) и нажмите кнопку **Запуск** (Start), как показано на рис. 18.4. После этого вы увидите окно настройки уровней UAC (см. рис. 18.3)[1].

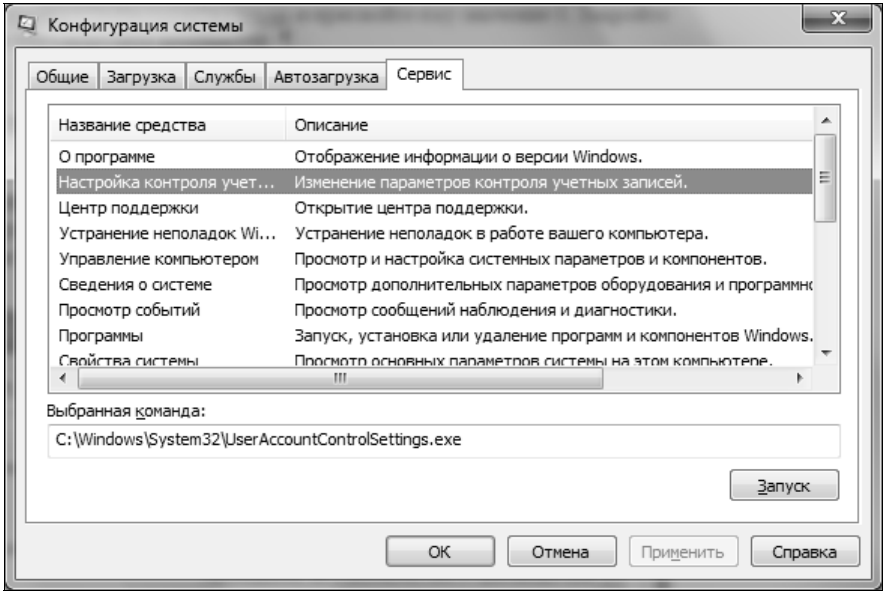


Рис. 18.4. Запуск настройки UAC через утилиту Msconfig.exe

18.4.3. Решение проблемы с гаджетами и UAC в Windows 7

В Windows 7 есть одна особенность. Если вы отключили UAC, некоторые гаджеты могут работать некорректно. Чтобы все было в порядке и гаджеты

[1] А самый простой способ — ввести не команду `msconfig`, а команду `UserAccountControlSettings`. Тогда апплет, позволяющий выполнить настройку UAC, запустится сразу же, минуя все промежуточные шаги. — *Прим. ред.*

работали, как и раньше, вам нужно изменить всего один параметр реестра. Перейдите в следующий раздел реестра:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Sidebar\Settings
```

Измените значение параметра `AllowElevatedProcess` в `1`. Чтобы изменения вступили в силу, нужно перезагрузить компьютер.

18.5. Удаление команды шифрования из контекстного меню в Windows Vista и Windows 7

Если за компьютером работает несколько пользователей, вы можете зашифровать свои файлы, чтобы другие пользователи не смогли их открыть. Возможности шифрования уже встроены в Windows, нужно их только активировать. Для этого перейдите в раздел реестра:

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
```

Создайте новый параметр `EncryptionContextMenu` (тип данных — `REG_DWORD`) и установите для него значение `1` (рис. 18.5).

После этого при щелчке на файле правой кнопкой мыши в контекстном меню появится команда **Зашифровать** (Encrypt) (рис. 18.6).

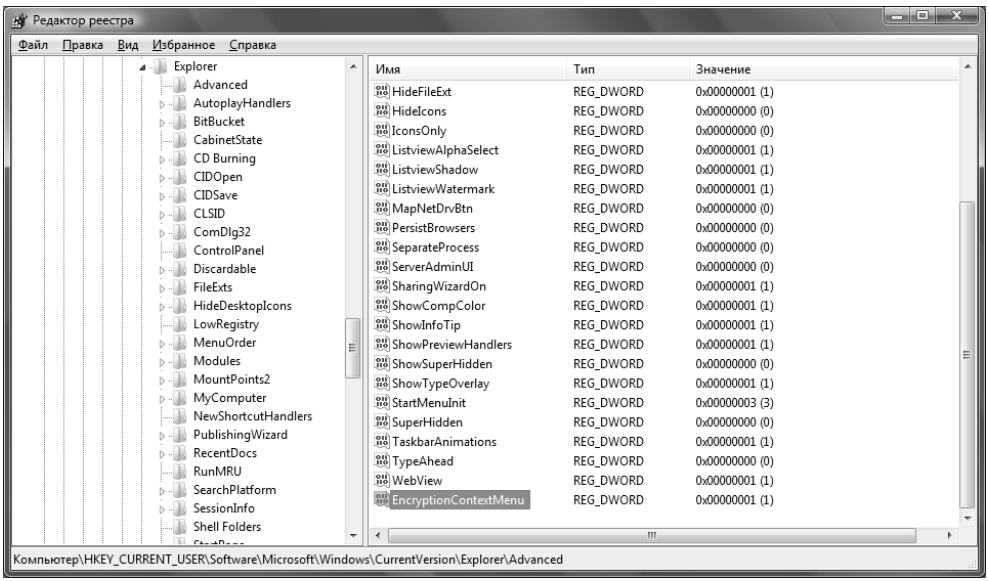


Рис. 18.5. Включение шифрования файлов

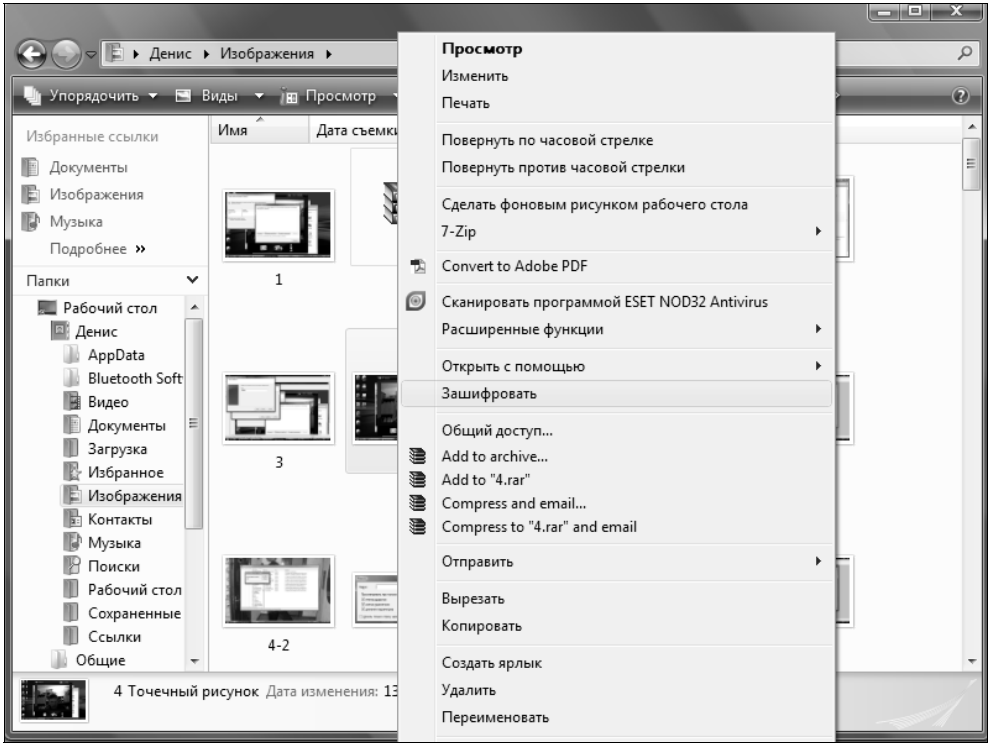
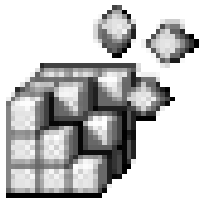


Рис. 18.6. Команда **Зашифровать**

ГЛАВА 19



Политики в Windows Vista/Windows 7

19.1. Что такое политики

Впервые политики (policies) появились еще в Windows 2000[1]. Групповая политика (Group Policy) используется для управления рабочими столами пользователей. Благодаря тому, что политика может управлять окружением всех пользователей, это существенно облегчает развертывание и сопровождение системы — администратору не нужно управлять окружением каждого пользователя. К тому же политики связаны с пользователем и "преследуют" его по всей сети — вне зависимости от того, с какой машины пользователь зайдет в сеть, к его рабочему столу будут применены установленные администратором политики.

В этой главе мы поговорим о локальных политиках, основанных на реестре. Поскольку локальные политики тесно связаны с Active Directory (AD), то вам нужно знать основы AD. Я сделаю все возможное, чтобы вы поняли, о чем идет речь, даже если вы не знакомы с AD, хотя не следует расценивать эту главу как краткое руководство по Active Directory.

Давайте разберемся, что такое политика. Я решил воздержаться от сухого определения и попытался просто объяснить ее суть. Предположим, вы устанавливаете какое-либо свойство рабочего стола, например, экранную заставку, обои или тип отображения обоев. Как пользователь, вы можете изменить свойства в любое время, когда вам этого захочется. Политики устанавливаются администраторами и имеют более высокий приоритет, чем аналогичные пользовательские свойства. В реестре политики хранятся отдельно от свойств.

---

[1] Не совсем так — впервые они появились еще в Windows NT 4.0. — *Прим. ред.*

Операционная система работает со свойствами и политиками так:

- если политика и свойство не установлены, то используются параметры по умолчанию;
- если политика не установлена, но установлено пользовательское свойство, то операционная система использует свойство;
- если же, наоборот, не установлено свойство, а установлена политика, то будет использоваться политика;
- наконец, самое интересное: если установлены и политика, и свойство, то будет использована политика, а свойство будет проигнорировано.

Это означает, что если администратор установил политику рабочего стола, например, обои или параметры заставки, то что бы ни делал пользователь, он не сможет их изменить.

Все политики определяются в GPO (Group Policy Object, объект групповой политики). В AD есть несколько GPO: один применяется к пользователям, а другой — к компьютерам. На локальном компьютере всего один GPO, который применяется только к локальному компьютеру и всем пользователям, которые входят в сеть с этого компьютера. Настройки локального GPO могут быть переопределены сетевыми GPO из AD. Первым обрабатывается локальный GPO, затем — сетевые GPO.

19.2. Редактор политик

В GPO содержатся настройки, касающиеся как пользователя, так и всего компьютера — это мы уже знаем. Локальные политики можно редактировать с помощью редактора политик `gpedit.msc`. Для его запуска нажмите клавиатурную комбинацию <Win>+<R>, введите команду `gpedit.msc` и нажмите клавишу <Enter>.

> ***Примечание***
>
> Редактор политик доступен только в Windows 7 Ultimate, Business и Enterprise.

Как видно из рис. 19.1, групповая политика состоит из двух разделов: **Конфигурация компьютера** (Computer Configuration) и **Конфигурация пользователя** (User Configuration). Первый содержит параметры настройки, общие для компьютера в целом, а второй — пользовательские настройки.

Использовать редактор политик довольно просто. Давайте попробуем ограничить резервируемую пропускную способность диспетчера QoS. QoS (Quality of Service) резервирует 20% пропускной способности сети, другими словами, ограничивает пропускную способность каждого компьютера сети, на котором включена QoS.

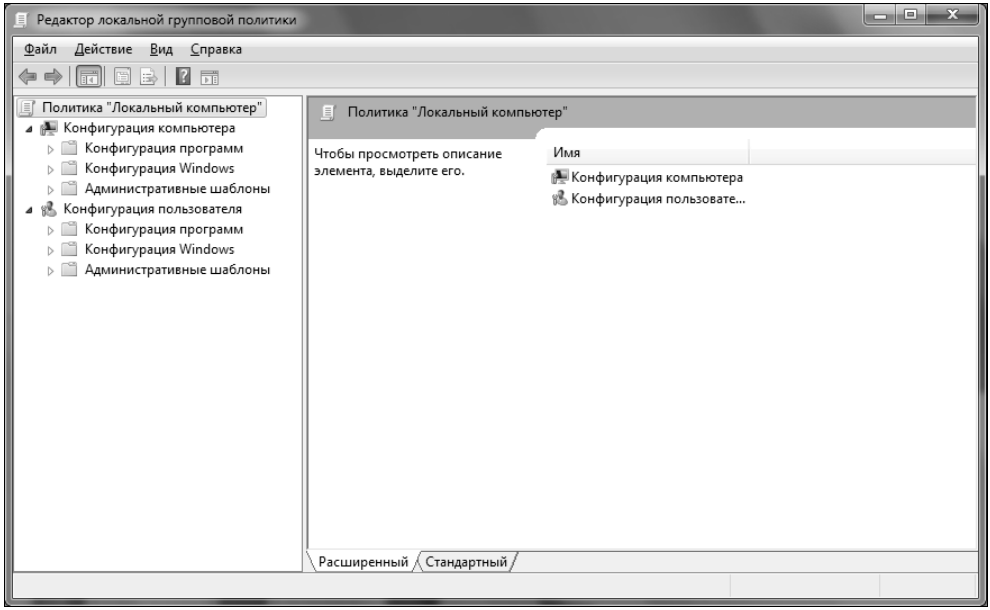


Рис. 19.1. Редактор политик

Перейдите в раздел **Конфигурация компьютера** (Computer Configuration)**|** **Административные** шаблоны (Administrative Templates)**|** **Сеть** (Network)**|** **Планировщик пакетов QoS** (QoS Sheduler), как показано на рис. 19.2.

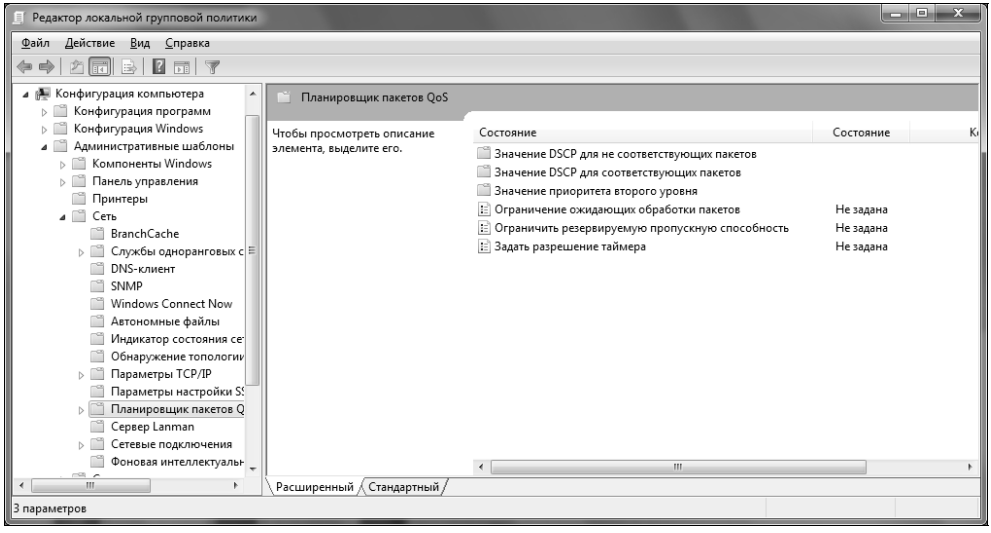


Рис. 19.2. Редактирование политик QoS

Дважды щелкните по элементу **Ограничить резервируемую пропускную способность** (Limit the reserved bandwidth). Даже если ограничение не задано, то QoS все равно резервирует 20% пропускной способности, поэтому нужно включить ограничение и установить 0% в качестве значения параметра (рис. 19.3). После этого нажмите кнопку **Применить** (Apply). После перезагрузки ваша сеть должна заработать быстрее, особенно это будет заметно при передаче по ней больших файлов.

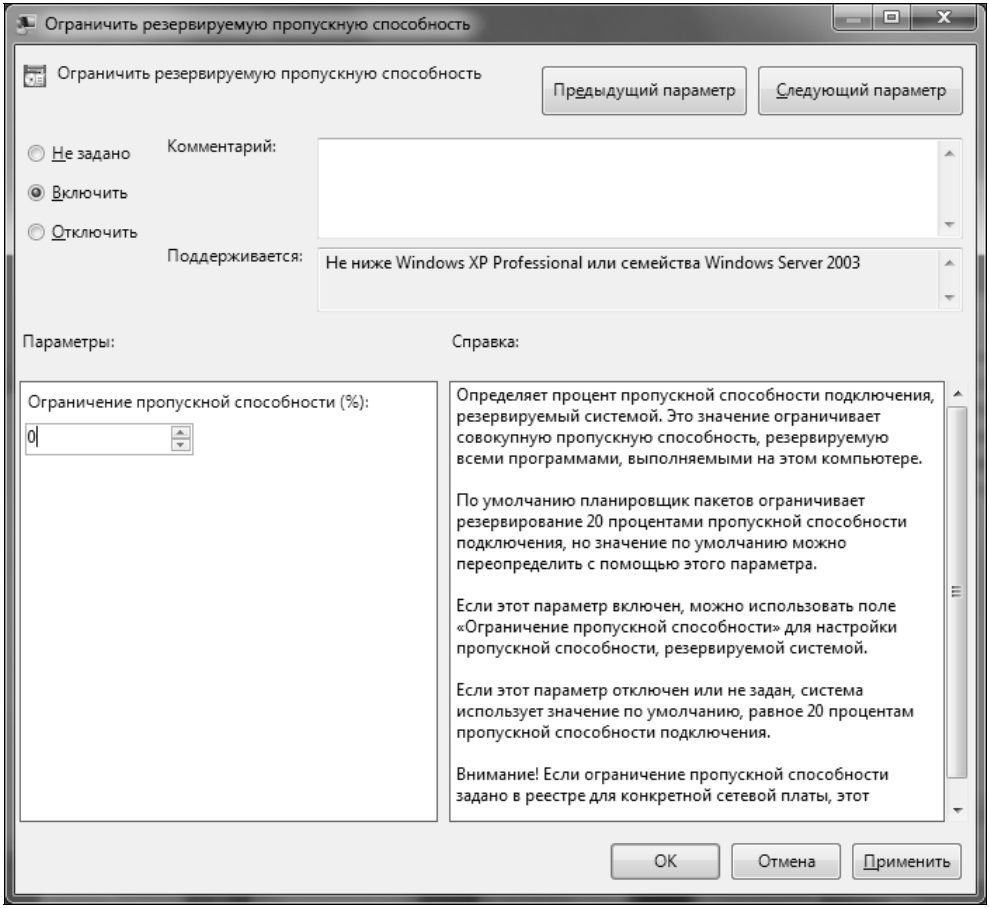


Рис. 19.3. Ограничение пропускной способности сети

В больших сетях выключать QoS подобным образом не рекомендуется — ведь ограничивая пропускную способность каждого отдельного компьютера, она обеспечивает работоспособность сети во время максимальной нагрузки (в часы пик). Однако в небольших сетях (5–15 компьютеров) QoS можно отключить.

19.3. Расширения групповой политики

Для настройки GPO вы можете использовать так называемые расширения групповой политики. Если быть предельно точным, то ее расширением является каждый подраздел, который вы видите в редакторе политик. При запуске редактор политик загружает все доступные расширения.

Вот некоторые расширения, предоставляемые групповой политикой в GPO:

- административные шаблоны — групповая политика для создания специального файла, в котором содержатся настройки реестра, записываемые как в `HKCU`, так и в `HKLM`. Операционная система читает настройки из этого файла при запуске системы и входе пользователя;
- сценарии — вы можете создать сценарии, которые будут выполняться при входе или выходе пользователей. Данные сценарии вы найдете в разделе **Конфигурация Windows** (Windows Configuration) редактора политик;
- параметры безопасности — администратор может управлять параметрами безопасности, в том числе политикой паролей, правами пользователей, ограничением запуска приложений. Параметры безопасности вы найдете в разделе **Конфигурация Windows** (Windows Configuration) редактора политик.

19.4. Административные шаблоны

Данная глава посвящена политикам, основанным на реестре. Другое их название — административные шаблоны или административные политики. Это настройки, переопределяющие свойства пользователей; они хранятся в реестре, и пользователи не могут их изменить.

Разберемся, как политики, вернее, административные шаблоны попадают в реестр. Политики определяются административными шаблонами, файлами с расширением `.admx` (в XP — `.adm`). Шаблоны (ADMX-файлы) описывают интерфейс пользователя для изменения определенных настроек реестра. Редактор политик загружает ADM-файлы, и администратор с помощью редактора политик редактирует настройки реестра. После этого они передаются в локальный GPO, а оттуда попадают в реестр.

Запомните один важный момент. Можно изменить параметры реестра с помощью редактора реестра, но при этом нужно помнить названия ключей и их допустимые значения. Можно сделать процесс редактирования реестра намного удобнее. Для этого нужно создать административный шаблон, ADMX-файл, в котором будут записаны элементы пользовательского интерфейса для изменения того или иного параметра реестра, например, окно с названием

параметра и его допустимыми значениями. ADMX-файл — это не самостоятельная программа. Хотя она и определяет элементы графического интерфейса пользователя, созданные ADMX-файлом окна вы сможете увидеть только с помощью редактора политик. Итак, в редакторе политик вы выбираете нужный ADMX-файл, появляется окно, подобное изображенному на рис. 20.3, в котором подробно описан изменяемый параметр. Вы устанавливаете новое значение параметра и нажимаете кнопку **ОК**. Все, изменения переданы в реестр.

Преимущество административных шаблонов заключается в том, что вам не нужно помнить ни имя ключа, ни имя параметра реестра, ни список допустимых значений — достаточно запустить редактор политик и изменить значение нужного вам параметра. Это намного удобнее, чем использовать редактор реестра.

Далее в этой главе мы заглянем за занавес административных шаблонов и даже научимся создавать собственные.

Чуть ранее было сказано, что при нажатии кнопки **ОК** изменения попадают в реестр, однако это происходит не мгновенно. Сначала настройки передаются в файл Registry.pol. Windows обрабатывает данный файл при запуске системы, при входе пользователя в систему и через некоторые промежутки времени.

Политика может находиться в одном из трех состояний: не задана, включена, выключена (рис. 20.3). Разница между этими состояниями следующая:

- если политика не задана, то соответствующий ей параметр реестра удаляется, что приводит к использованию свойства пользователя;
- если политика включена, то соответствующему ей параметру реестра присваивается значение `1` или другое (любое больше `0`), соответствующее активному состоянию;
- если политика выключена, то соответствующему ей параметру реестра присваивается значение `0`.

Политики хранятся в разделе реестра `Software\Policies`. Такой раздел имеется как в `HKLM`, так и в `HKCU`. Понятно, что в `HKLM\Software\Policies` хранятся общесистемные политики, а в `HKCU\Software\Policies` — пользовательские.

Кроме этих разделов политики могут содержаться еще в разделе `Software\Microsoft\Windows\CurrentVersion\Policies`. Политики из этого раздела вносят в реестр постоянные, необратимые изменения. Чтобы пользователь не мог изменить эти разделы реестра и, соответственно, политику, устанавливаются списки контроля доступа (Access Control Lists, ACL). Согласно ACL, по умолчанию эти разделы имеет право редактировать только администратор.

Теперь поговорим о размещении политик на диске. Определения политик, т. е. ADMX-файлы, хранятся в каталоге *%SystemRoot%*\PolicyDefinitions, а файл Regisrty.pol находится в каталоге *%SystemRoot%*\System32\GroupPolicy\Machine.

19.5. Расширенные возможности политик в Windows Vista/Windows 7

В новых версиях Windows групповые политики были значительно обновлены и расширены. Хорошо это или плохо — будет видно со временем, поскольку сейчас даже Windows Vista еще не используется повсеместно. Пока можно сказать лишь одно: групповые политики похожи на политики в Windows XP, но имеют расширенные по сравнению с ней возможности и некоторые отличия в работе. Например, если в Windows XP для обработки групповых политик был предназначен процесс `winlogon`, то теперь этим занимается целая служба Windows, имеющая высокий уровень защиты (это означает, что даже администратор не имеет права ее остановить). В целом такая организация повышает общую надежность механизма групповых политик.

Далее в этой главе мы поговорим о новых возможностях групповых политик, а также об отличиях от Windows XP.

19.5.1. Вычисление скорости сети

Механизм групповых политик всегда вычисляет скорость подключения к сети, используя эту информацию для определения набора политик, которые следует применять для того или иного компьютера сети. Если компьютер подключен к сети по низкоскоростному соединению, например по модему, то на этот компьютер отправлялись не все параметры политик, поскольку такая загрузка заняла бы очень много времени.

В Vista механизм групповых политик также вычисляет скорость подключения к сети, но делает это иначе. Если в предыдущих версиях Windows для этого использовались ICMP-пакеты `ping`, то Vista использует обработчик NLA 2.0. О нем — чуть позже, а пока поговорим о том, почему в новой версии Windows отказались от `ping`-пакетов.

Многие администраторы отключают протокол ICMP на маршрутизаторах. В этом случае механизм групповых политик считает, что компьютер недоступен, и ничего на него не отправляет. С другой стороны, даже если ICMP не отключен, он все равно не позволяет точно вычислить скорость соединения с сетью. Например, если компьютер подключается через спутниковый канал или другой канал с высоким уровнем задержки, скорость соединения невоз-

можно определить однозначно: она высока, но механизм групповых политик может посчитать, что компьютер подключен по низкоскоростному соединению.

В предыдущих версиях Windows механизм групповых политик не мог определить, что компьютер долгое время работал автономно, не подключаясь к сети или же подключаясь на короткое время. В результате обновление групповых политик не производилось.

В Vista механизм групповых политик работает иначе. Он использует службу NLA, которая оповещает механизм групповых политик о доступности DC (Domain Controller, контроллер домена). Если DC доступен, то по мере необходимости выполняется обновление групповых политик.

19.5.2. Несколько локальных GPO

До Windows Vista было возможно использование только одного локального GPO (объект групповой политики). В Windows Vista/7 допускается использование нескольких локальных GPO. Рассмотрим небольшой пример, демонстрирующий преимущество такого решения.

Предположим, что вам нужно изменить параметры команды **Настройка** (или **Выполнить**) из меню **Пуск** так, чтобы пользователи не видели эту команду, а администраторы могли ею пользоваться в обычном режиме. При наличии одного локального GPO справиться с поставленной задачей было невозможно.

В Windows Vista/7 используется многоуровневая система GPO, изображенная на рис. 19.4.

Как видно из рисунка, используются три GPO: GPO компьютера, GPO администратора и GPO пользователя. Первый GPO определяет параметры компьютера и пользователя, второй может переопределить параметры пользователей из группы Администраторы (Administrators), а третий относится к отдельным пользователям, не входящим в группу Администраторы (Administrators).

19.5.3. ADMX-файлы: новый формат файлов

Для описания политик в предыдущих версиях Windows использовались ADM-файлы. В Windows Vista/Windows 7 вместо ADM-файлов используются ADMX-файлы (файлы с расширением .admx), которые можно найти в каталоге \Windows\PolicyDefinitions.

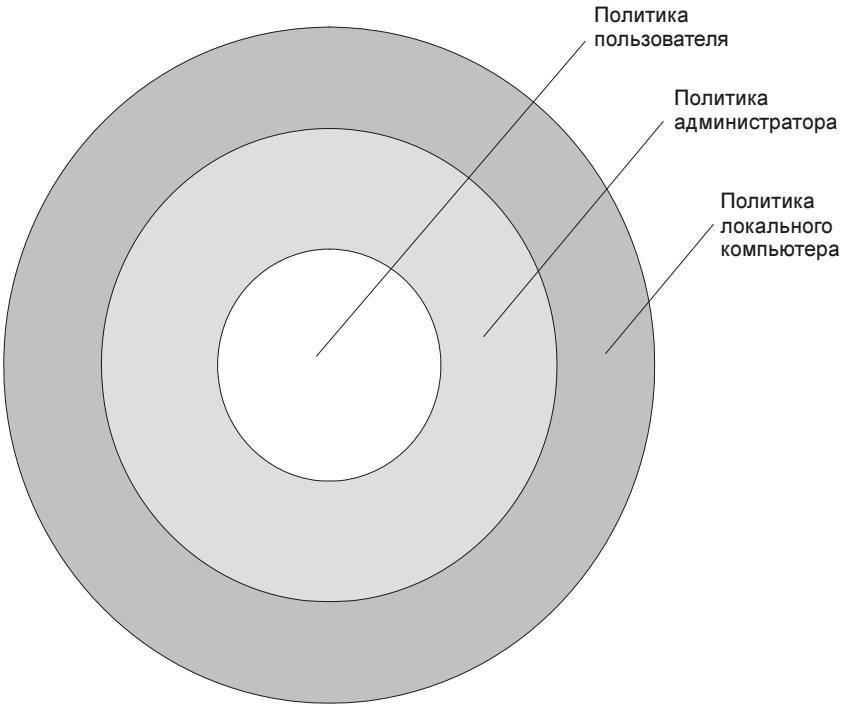


Рис. 19.4. Новая многоуровневая система GPO

Зачем нужно было менять формат файлов политик? ADM-файлы далеки от совершенства. Начнем с того, что, как правило, ADM-файлы используют один из языков (русский, английский и т. д.), т. е. все сообщения в этом файле, которые видит пользователь при редактировании политики, написаны на одном языке. ADMX-файлы не привязаны к языку, однако каждый ADMX-файл должен сопровождать ADML-файл, в котором содержатся сообщения на одном из языков. Загляните в каталог PolicyDefinitions: вы найдете в нем ADMX-файлы и два каталога: en-US и ru-RU. В первом находятся ADML-файлы, написанные на английском языке, а во втором — на русском. Добавить нужный язык очень просто — достаточно создать ADML-файл, написанный на нужном языке.

Кроме того, ADMX-файлы поддерживают централизованное хранилище, что значительно упрощает обновление файлов политик. Например, вам достаточно поместить ADMX-файл в хранилище, и все рабочие станции, работающие под управлением Vista, получат этот файл. В случае с ADM-файлом вам нужно самостоятельно скопировать его обновленную версию на каждый компьютер.

Формат ADMX-файлов также изменен. С одной стороны, это к лучшему, поскольку теперь используется стандартный язык разметки — XML (ознако-

миться с этим языком вы можете по адресу **http://www.citforum.ru /internet/xml/index.shtml**). С другой стороны, это не очень хорошо, потому что нет никаких программ для преобразования файлов формата ADM в формат ADMX, а также графических редакторов для ADMX-файлов, упрощающих процесс создания таких файлов.

19.6. Практические примеры использования редактора политик

Чтобы данная глава не была сугубо теоретической, рассмотрим некоторые примеры использования редактора политик. Работоспособность примеров проверялась в ОС Windows Vista и Windows 7, но некоторые примеры будут также работать в Windows XP — экспериментируйте.

19.6.1. Отключение диспетчера задач

Когда пользователь нажимает клавиатурную комбинацию <Ctrl>+<Alt>+<Del>, система отображает экран, позволяющий запустить диспетчер задач[1]. Пользователь может выбрать любой процесс из списка на вкладке **Процессы** (Processes) и завершить его. Не всегда такое действие хорошо сказывается на работоспособности системы, особенно когда пользователь не знает, что делает. Администратору может пригодиться функция отключения вызова диспетчера задач, что не позволит пользователям завершать произвольные процессы.

Запустите редактор политик. В левой панели перейдите в раздел **Конфигурация пользователя** (User Configuration) | **Административные шаблоны** (Administrative Templates) | **Система** (System) | **Варианты действий после нажатия CTRL + ALT + DEL** (Possible reactions to CTRL + ALT + DEL).

В правой панели вы увидите список возможностей <Ctrl>+<Alt>+<Del>. Включите параметр **Удалить диспетчер задач** (Remove Task Manager). Для этого дважды щелкните по нему и выберите значение **Включен** (Enabled).

Отключить диспетчер задач можно и через реестр. Для этого перейдите в один из разделов реестра:

- `HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\system` — если нужно отключить диспетчер задач только для текущего пользователя;

[1] Более быстрый доступ к диспетчеру задач в Windows Vista/7 дает клавиатурная комбинация <Ctrl>+<Shift>+<Esc>. — *Прим. ред.*

- `HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\system` — если нужно отключить диспетчер задач для всех пользователей.

Создайте новое `DWORD`-значение `DisableTaskMgr` и установите значение `1`. Если нужно будет снова включить диспетчер задач, установите значение `0`.

> ***Примечание***
>
> Для остальных административных задач не будут приводиться соответствующие им изменения реестра. Чтобы узнать, какие значения реестра изменяются, исследуйте соответствующие действиям ADMX-файлы в каталоге PolicyDefinitions.

19.6.2. Запрет доступа к Панели управления

Не всегда можно допускать пользователя к Панели управления, особенно если этот пользователь неопытный. С помощью редактора политик можно запретить доступ к Панели управления.

Откройте редактор политик и перейдите в раздел **Конфигурация пользователя** (User Configuration) | **Административные шаблоны** (Administrative Templates) | **Панель управления** (Control Panel). Включите параметр **Запретить доступ к Панели управления** (Disallow access to Control Panel).

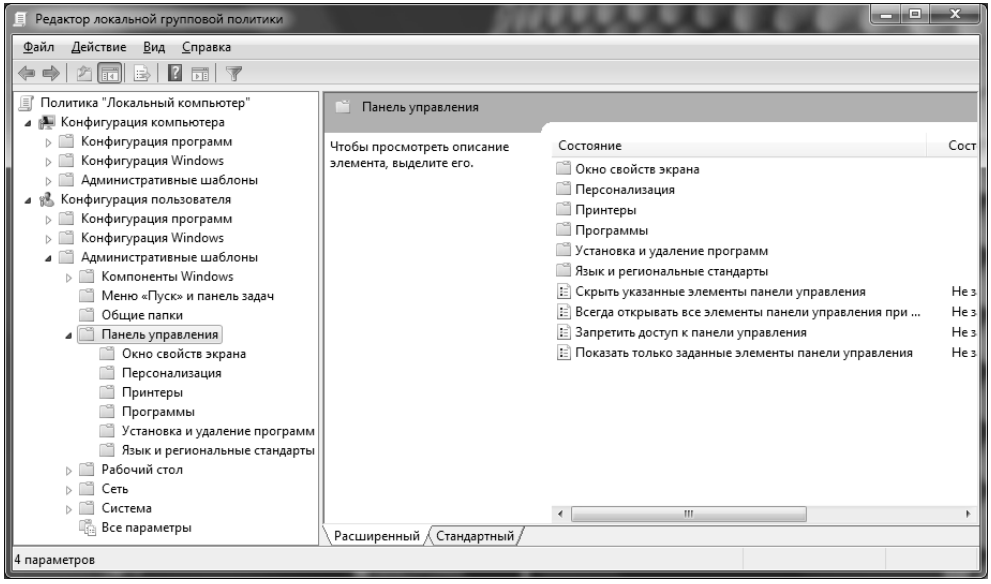


Рис. 19.5. Запрет доступа к Панели управления в Windows 7

19.6.3. Запрет доступа к апплету *Установка и удаление программ*

Иногда нужно запретить пользователю доступ только к апплету **Установка и удаление программ** (Add/Remove Programs), но не нужно запрещать доступ ко всей Панели управления. Для этого перейдите в раздел редактора политик **Конфигурация пользователя** | (User Configuration) | **Административные шаблоны** (Administrative Templates) | **Панель управления** (Control Panel) | **Установка и удаление программ** (Add/Remove Programs). Включите параметр **Удаление окна "Установка и удалеине программ"** (Remove Add/Remove Programs Window).

В этом же разделе вы можете выбрать и другие возможности, например, скрыть страницу удаления программ, что позволит устанавливать новые программы, но не позволит удалять уже установленные, или запретить установку программ по локальной сети.

> ***Примечание***
>
> Если вы исследуете файл AddRemovePrograms.admx, то придете к заключению, что для запрета отображения окна установки и удаления программ нужно перейти в раздел реестра `HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Uninstall` (или `HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Uninstall`) и добавить `DWORD`-параметр `NoAddRemovePrograms`. Значение `1` этого параметра запрещает отображения окна установки и удаления программ.

19.6.4. Отключение правого щелчка мышью для меню и панелей

Если вы не хотите разрешать пользователям редактировать меню **Пуск** (Start) и панели задач, то нужно отключить правый щелчок мышью для меню и панелей.

Перейдите в раздел редактора политик **Конфигурация пользователя** (User Configuration) | **Административные шаблоны** (Administrative Templates) | **Меню "Пуск" и панель задач** (Taskbar and Start Menu). Включите параметр **Запретить доступ к контекстному меню для панели задач** (Disallow access to Taskbar Context Menu).

В этом же разделе можно полностью настроить меню **Пуск** (Start), например, отключить некоторые его элементы, запретить слежение за пользователем (т. е. запись последних открытых документов и запущенных программ) и т. д.

Если вы хотите запретить контекстное меню Проводника Windows (сразу скажу, что это доставит некоторые неудобства пользователям)[1], тогда перейдите в раздел редактора **Конфигурация пользователя, Административные шаблоны, Компоненты Windows, Проводник Windows**.

Включите параметр **Запретить вывод контекстного меню по умолчанию для Проводника Windows** (Disallow Context Menu for Windows Explorer).

19.6.5. Запрет завершения работы системы и выхода из системы

Запретить отображения команд завершения работы можно в разделе **Конфигурация пользователя** (User Configuration) | **Административные шаблоны** (Administrative Templates) | **Меню "Пуск" и панель задач** (Taskbar and Start Menu).

Включите параметр **Удалить и запретить доступ к команде "Завершение работы", "Перезагрузка", "Сон", "Гибернация" и запрет доступа к ним** (Remove and prevent access to the Shutdown, Restart, Sleep, and Hibernate commands).

Данная политика удаляет пункты завершения работы (собственно, само завершение работы и команду перезагрузки), что не позволяет пользователю завершать работу компьютера и перезагружать Windows.

Однако пользователь все еще может завершить работу системы путем ввода команды `shutdown /s` (завершение работы) или `shutdown /r` (перезагрузка). Чтобы запретить ему и это, нужно отключить запуск программ (см. *следующий раздел*).

Для запрета выхода из системы включите параметр **Удалить "Завершение сеанса" из меню "Пуск"** (Remove "Logoff" from the Start Menu). Но выйти из системы все еще можно через диспетчер задач. Поэтому нужно отключить диспетчер задач полностью или отключить только возможность выхода из системы. Для этого нужно включить параметр **Запретить завершение сеанса** (Remove Logoff) в разделе **Конфигурация пользователя** (User Configuration), **Административные шаблоны** (Administrative Templates), **Система** (System), **Варианты действия после нажатия CTRL + ALT + DEL** (Ctrl + Alt + Del Options).

---

[1] Правильно, "спасибо" они за это не скажут. — *Прим. ред.*

19.6.6. Отключение окна запуска программ

Перейдите в раздел **Конфигурация пользователя** (User Configuration), **Административные шаблоны** (Administrative Templates), **Меню "Пуск" и панель задач** (Taskbar and Start Menu).

Включите параметр **Удалить команду "Выполнить" из меню "Пуск"**.

Данная политика:

- отключает команду **Выполнить** (Run) в Windows XP;
- отключает диалог ввода команды в Windows Vista/Windows 7;
- отключает команду **Новая задача** (New task) в меню **Файл диспетчера задач**;
- запрещает использование UNC-пути (\\) в строке адреса браузера Internet Explorer;
- запрещает доступ к локальным дискам и папкам;
- отключает окно запуска программы, появляющееся при нажатии клавиатурной комбинации <Win>+<R>.

19.6.7. Отключение редактора реестра

С помощью редактора политик можно отключить даже редактор реестра (regedit.exe), чтобы пользователь не мог изменять системный реестр. В этой книге вы найдете способ отключения редактора реестра путем редактирования самого реестра, а сейчас мы пока рассмотрим, как использовать редактор политик для отключения regedit.exe.

Перейдите в раздел **Конфигурация пользователя** (User Configuration), **Административные шаблоны** (Administrative Templates), **Система** (System).

Включите параметр **Запретить доступ к средствам редактирования реестра** (Prevent access to registry editing tools).

19.7. Применение политик без перезагрузки компьютера

Многие политики требуют для своего применения перезагрузки компьютера. Перезагружать компьютер не всегда удобно. Оказывается, есть способ применения политик без перезагрузки. Нажмите кнопку **Пуск** (Start), введите `cmd`, щелкните на поле для запуска программы правой кнопкой мыши и выберите **Запустить как администратор** (Run as Administrator).

В окне командной строки введите команду:

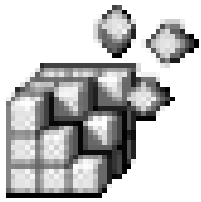
```
gpupdate/force
```

Вы увидите следующее сообщение:

```
Updating Policy...

User Policy update has completed successfully.
Computer Policy update has completed successfully.
```

Это означает, что политики применены успешно. Перезагружать компьютер не нужно.



ГЛАВА 20

Списки доступа (ACL)

20.1. Что такое ACL?

ACL (Access Control List) — список управления доступом, используемый для ограничения доступа к любому объекту, который существует в операционной системе. В реестре есть ключи, которые совсем не обязательно редактировать как обычным пользователям, так и программам, запущенным от их имени. В большинстве случаев обычным пользователям предоставляется только право чтения этих ключей, а администратор может производить над ключами любые действия[1].

Вообще редактировать ACL реестра вам придется очень редко, а то и вообще не придется. Это достаточно опасное занятие: установив неправильные права доступа, можно нарушить нормальную работу Windows.

Спрашивается, зачем тогда мы вообще рассматриваем списки контроля доступа? Некоторые приложения могут работать, только если их запустил пользователь, состоящий в группе `Администраторы` (`Administrators`). Не будете же вы добавлять в группу `Администраторы` всех пользователей, которым нужна эта программа? Да, на домашнем компьютере можно это сделать, но на предприятии, в корпоративной среде такое решение не приемлемо. Выйти из ситуации можно, если предоставить доступ к запрашиваемым ключам реестра только определенным пользователям — тем, которым нужна программа. Это

[1] Так было в версиях Windows, более ранних, чем Windows Vista. Теперь же даже и администратор — не всегда и не любые! Причем, это относится не только к пользователям с привилегиями администратора, но даже и к встроенной (и по умолчанию заблокированной учетной записи `Администратор` (`Administrator`). Есть в реестре и такие ключи, к которым имеет право доступа только учетная запись `SYSTEM` (сама операционная система) или сервис `TrustedInstaller` — да и то, не в полном объеме. — *Прим. ред.*

достаточно кропотливая работа, особенно при отсутствии четкого руководства по программе: с помощью средства мониторинга реестра вам придется самостоятельно вычислить необходимые ей ключи. Но результат того стоит.

20.2. Базовое редактирование ACL

Изменить ACL конкретного ключа реестра очень просто. Для этого выполните следующие действия:

1. Запустите редактор реестра.
2. Перейдите к разделу, ACL которого вы хотите изменить.
3. Выберите из меню команды **Правка** (Edit) | **Разрешения** (Permissions).
4. В открывшемся окне (рис. 20.1) выберите пользователя или группу пользователей, права доступа которого (которой) вы хотите изменить.
5. В нижней части окна установите права доступа к ключу:
   - **Полный доступ** (Full Access) — разрешает производить любые операции с ключом: чтение, редактирование параметров, удаление как параметров, так и всего ключа, получение статуса владельца ключа;

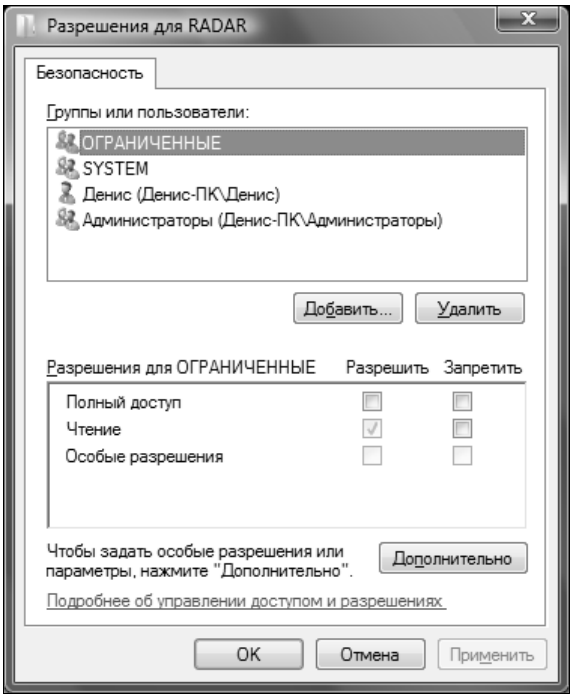


Рис. 20.1. Редактирование ACL для группы ОГРАНИЧЕННЫЕ

- **Чтение** (Read) — разрешает только читать значения параметров ключа реестра;
- **Особые разрешения** (Special Permissions) — о них мы поговорим чуть позже.

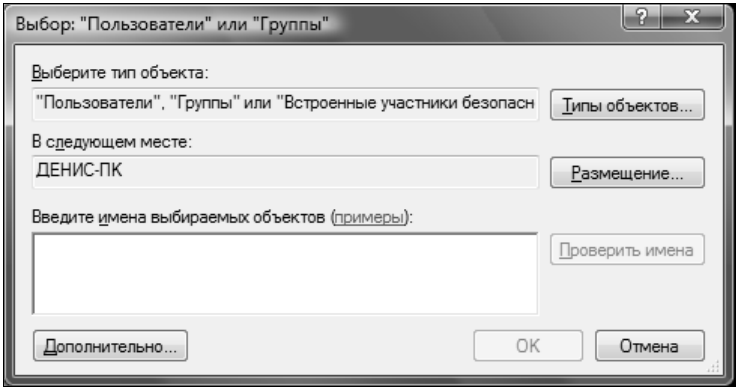


Рис. 20.2. Добавление пользователя/группы

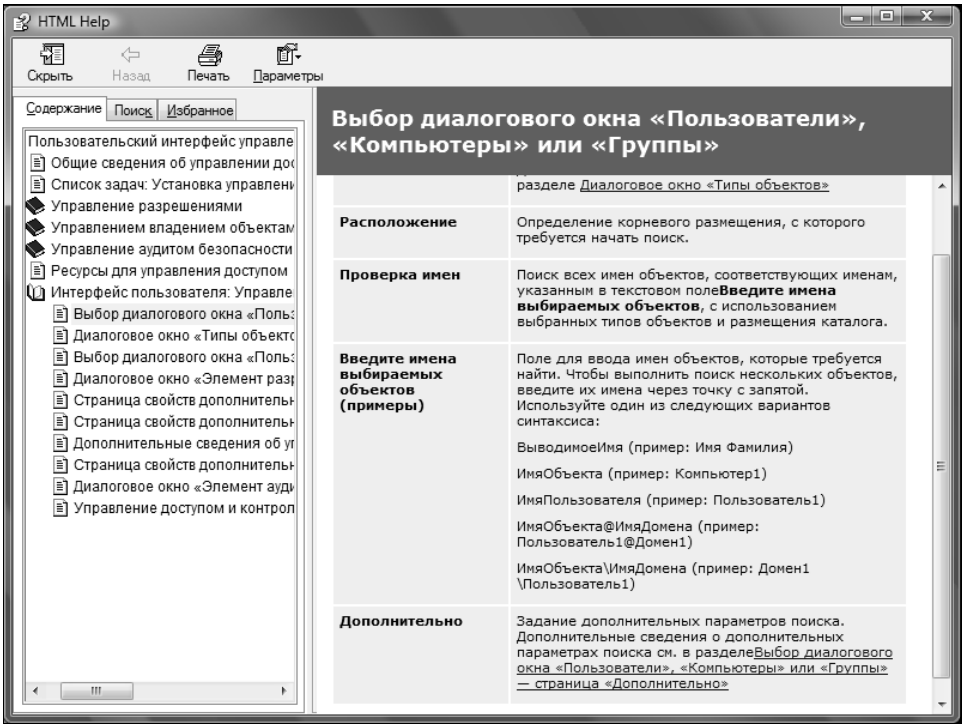


Рис. 22.3. Синтаксис описания пользователя/группы

6. Установив права доступа, нажмите кнопку **Применить** (Apply), затем — кнопку **ОК**.

Если в списке **Группы или пользователи** (Groups or user names) нет нужного вам пользователя или группы пользователей, нажмите кнопку **Добавить** (Add). В появившемся окне (рис. 20.2) введите имя пользователя или группы, которую вы хотите добавить в список. Если вы забыли формат ввода имени пользователя/группы, нажмите ссылку **Примеры** (Examples), и на экране появится окно с необходимой справочной информацией (рис. 20.3).

Если вы не помните точное имя пользователя или группы, нажмите кнопку **Дополнительно** (Advanced), а в появившемся окне нажмите кнопку **Поиск** (Find now). Результаты поиска отображены на рис. 20.4.

Для добавления пользователя в список выберите его и нажмите кнопку **ОК**.

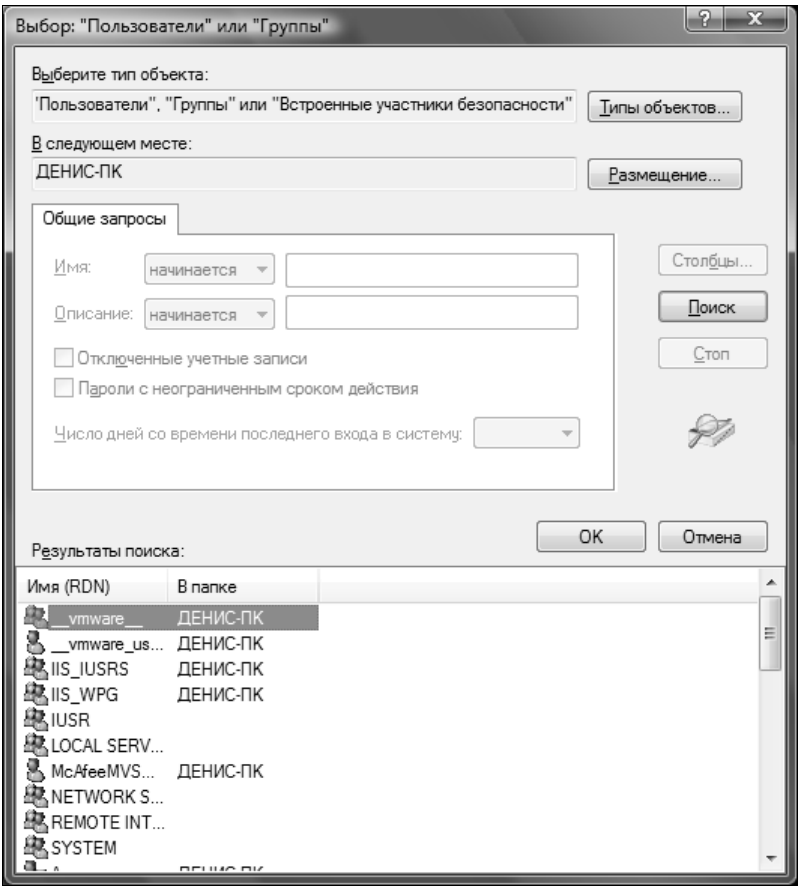


Рис. 20.4. Поиск пользователя группы

20.3. Расширенное редактирование ACL

Для установки специальных разрешений выберите ключ реестра и откройте окно редактирования ACL (**Правка** (Edit) | **Разрешения** (Permissions)). После этого выберите пользователя/группу и нажмите кнопку **Дополнительно** (Advanced) в окне редактирования ACL (см. рис. 20.1).

В открывшемся окне (рис. 20.5) дважды щелкните по записи пользователя/группы.

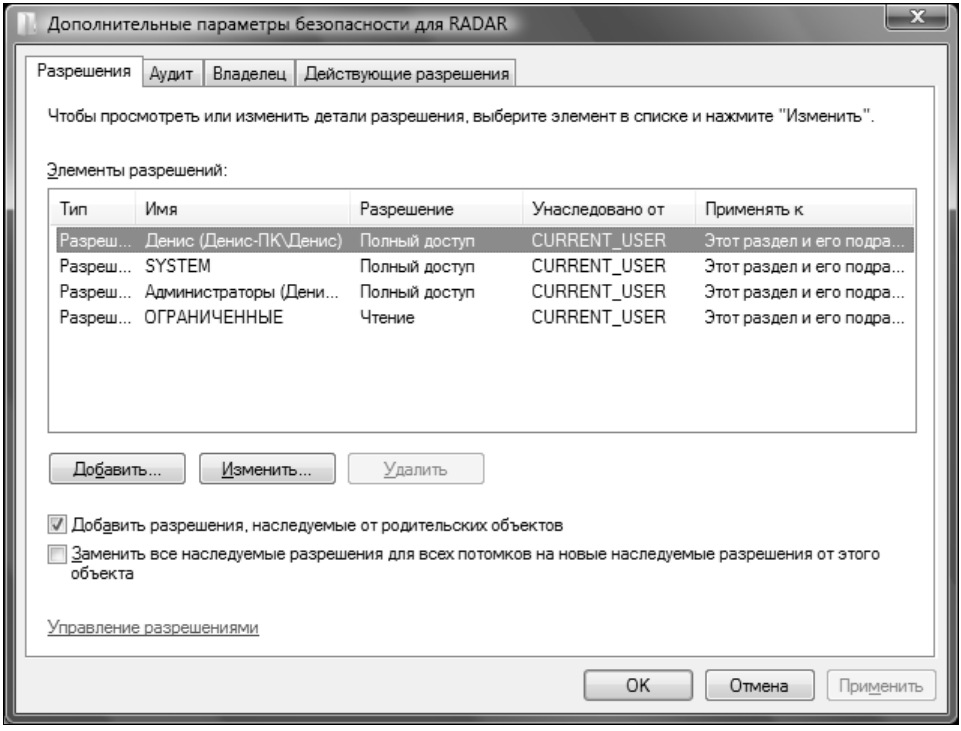


Рис. 20.5. Дополнительные параметры безопасности

Откроется окно **Элемент разрешения** (Permission Entry), в котором вы сможете установить специальные разрешения для выбранного ключа реестра (рис. 22.6).

Обратите внимание на список **Применять** (Apply to). В нем нужно выбрать одно из следующих значений:

- **Только этот раздел** (This key only) — параметры безопасности будут применены только к этому разделу (ключу);

- **Этот раздел и его подразделы** (This key and its subkeys) — параметры безопасности будут применены к этому разделу и всем его подразделам;
- **Только подразделы** (Subkeys only) — разрешения будут применены только к подразделам выбранного раздела.

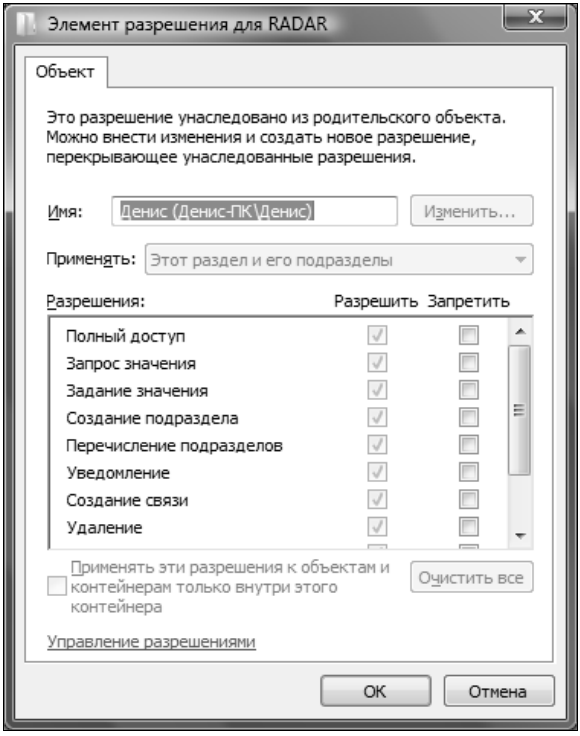


Рис. 22.6. Элемент разрешения

В списке **Разрешения** (Permissions) выберите необходимые разрешения с помощью флажков **Разрешить** или **Запретить**:

- **Полный доступ** (Full access) — разрешает/запрещает полный доступ к ключу реестра, который представляет собой совокупность приведенных ниже разрешений;
- **Запрос значения** (Query value) — право чтения параметров выбранного раздела реестра;
- **Задание значения** (Set value) — право изменения значений параметров выбранного раздела реестра;
- **Создание подраздела** (Create subkey) — создание подраздела в выбранном разделе;

- **Перечисление подразделов** (Enumerate subkeys) — определение подразделов выбранного раздела;
- **Создание связи** (Create Link) — создание ссылок в выбранном разделе;
- **Удаление** (Delete) — удаление раздела или его параметров;
- **Запись DAC** (Write DAC) — запись списка выборочного контроля доступа (Discretionary Access Control — DAC);
- **Смена владельца** (Write Owner) — изменение владельца раздела;
- **Чтение разрешений** (Read Control) — чтение списка DAC.

Для сохранения разрешений сначала нажмите кнопку **Применить** (Apply), затем — кнопку **OK**.

20.4. Права доступа по умолчанию

Сначала я предполагал привести в этом разделе табличку, в которой бы были описаны права доступа к основным разделам реестра. Но потом воздержался, поскольку есть прекрасная утилита AccessChk, написанная авторитетнейшим специалистом в области Windows — Марком Руссиновичем (Mark Russinovich).

Скачать AccessChk можно по адресу:

http://www.microsoft.com/rus/technet/sysinternals/utilities/accesschk.mspx

Вот примеры использования этой утилиты:

- вывод прав доступа к разделу `hkcu\software`

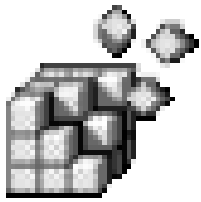
```
accesschk -k hkcu\software
```

- вывод прав доступа группы Пользователи к файлам и каталогам каталога C:\Windows

```
accesschk "Пользователи" C:\Windows
```

Подробнее об использовании AcessChk вы можете прочитать на указанной чуть ранее Web-странице.

ГЛАВА 21



Аудит и мониторинг реестра

21.1. Аудит реестра

Суть аудита реестра заключается в том, чтобы выяснить, какие изменения произошли в реестре за определенный период времени, кем, когда и при каких обстоятельствах они были внесены. Например, представьте себе, что вы хотите выяснить, какие изменения произошли в интересующем вас разделе реестра за последнюю истекшую неделю.

Существует несколько способов аудита реестра, а именно:

- сравнение разделов реестра с помощью программы reg.exe — этот метод был рассмотрен в *главе 14* данной книги;
- сравнение реестра с помощью утилиты WinDiff.exe — несмотря на то, что программа WinDiff.exe используется для сравнения файлов, ее можно применять для сравнения разделов реестра;
- аудит реестра с помощью встроенных средств аудита — этот способ наименее удобный, его следует использовать только тогда, когда первые два способа по тем или иным причинам неприемлемы.

21.1.1. Сравнение реестра с помощью *WinDiff*

Программа WinDiff предназначена для сравнения двух версий текстовых файлов или каталогов. Обычно она используется программистами для сравнения различных версий исходных кодов программы. Программа WinDiff входит в состав программного продукта Windows Software Development Kit. Чтобы не загружать весь пакет разработчика, вы можете скачать только

программу WinDiff. Она доступна по адресу **http://www.grigsoft.com/download-windiff.htm**

Там же вы сможете скачать исходный код этой программы, а также условно-бесплатную (Shareware) версию программы CompareIt, позволяющую сравнивать файлы MS Word и Excel. Впрочем, для наших текущих целей эта программа не нужна, нам вполне достаточно возможностей WinDiff.

Методика сравнения разделов реестра следующая:

1. Вы экспортируете интересующий вас раздел реестра в REG-файл.
2. Через некоторое время (например, после установки какой-то программы, выполнения в ней какого-то действия или же просто через день, два или через неделю) вы снова экспортируете этот же раздел в REG-файл, но под другим именем.
3. Запускаете WinDiff и сравниваете два REG-файла.

Как видите, все очень просто. Перед тем как мы будем использовать WinDiff, хочу отметить, что для наблюдения за реестром в реальном времени (например, при установке программы или выполнении в ней какого-либо действия) лучше использовать программы для мониторинга реестра. Одну из таких программ мы рассмотрим в *разделе 21.2*.

Запустите WinDiff и выберите из меню **File** команду **Compare Files**. Выберите первый файл (пусть это будет файл с именем reg1.reg), а затем программа предоставит возможность выбрать второй файл (например, reg2.reg).

Вы увидите сообщение о том, что второй файл более новый (создан позже первого файла). Щелкните по строчке с этим сообщением, и вы увидите окно сравнения файлов (рис. 21.1).

Как видно из рис. 21.1, во втором файле отсутствуют строки:

```
"My1"=dword:00000001
"My2"=dword:00000001
```

Другими словами, из раздела `HKCU\Software\Policies` были удалены параметры `My1` и `My2`.

Чуть выше видно, что подобная строка есть во втором файле, но она немного отличается от аналогичной строки в первом файле. Видно, что в первом файле параметру `My` было присвоено значение `1`, а во втором файле этому же параметру присвоено значение `0`.

Вывод: между экспортом первого и второго REG-файлов в разделе реестра `HKCU\Software\Policies` был изменен параметр `My` и удалены параметры `My1` и `My2`.

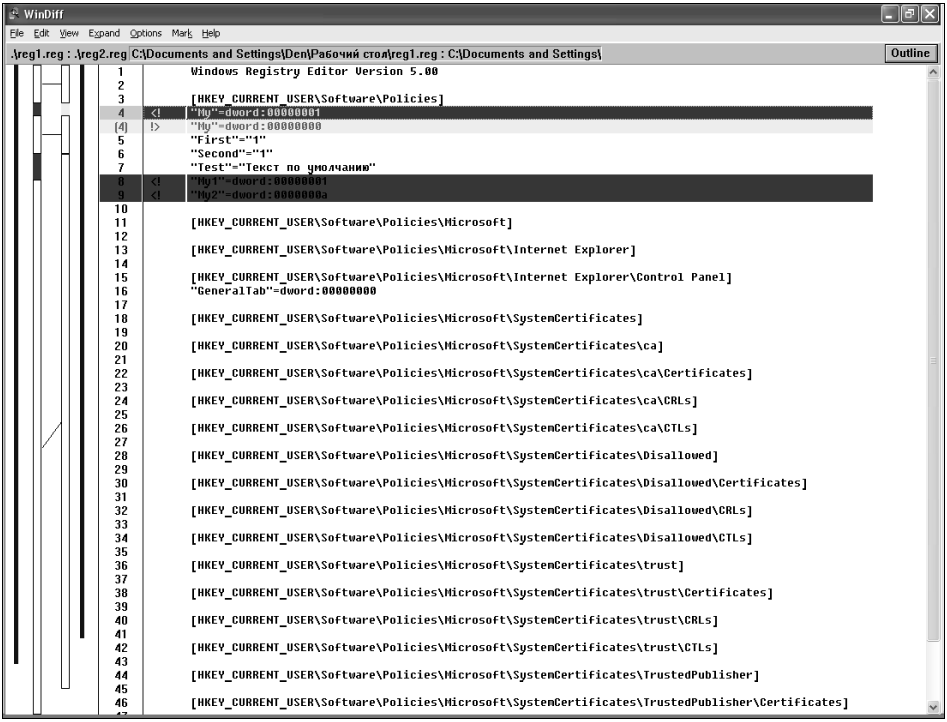


Рис. 21.1. Сравнение двух файлов

21.1.2. Аудит реестра с помощью стандартных средств Windows

Как уже было отмечено, этот способ наименее удобен: намного проще создать два REG-файла, а потом сравнить их. Основной недостаток данного метода заключается в том, что анализ результатов сравнения производится путем просмотра системного журнала безопасности. Почему это недостаток? Интерфейс программы **Просмотр событий** (Event Viewer), как и формат вывода самих сравнений, нельзя назвать удачным. К тому же, события аудита придется искать среди остальных событий безопасности, что не очень удобно[1] (рис. 21.2).

[1] Довольно спорное утверждение. Конечно, в более ранних версиях Windows анализ системного журнала был сложным делом, но в Windows Vista/7 программа просмотра событий была существенно дополнена и усовершенствована. Впрочем, согласиться можно только в одном — данная задача сложна, и сама по себе заслуживает написания отдельной книги. Но, все же, и так безапелляционно говорить не стоит. Кроме того, если вы попробуете с помощью WinDiff сравнить более масштабные файлы, в которых и изменений будет намного больше, то увидите, что это — тоже дело трудоемкое. — *Прим. ред.*

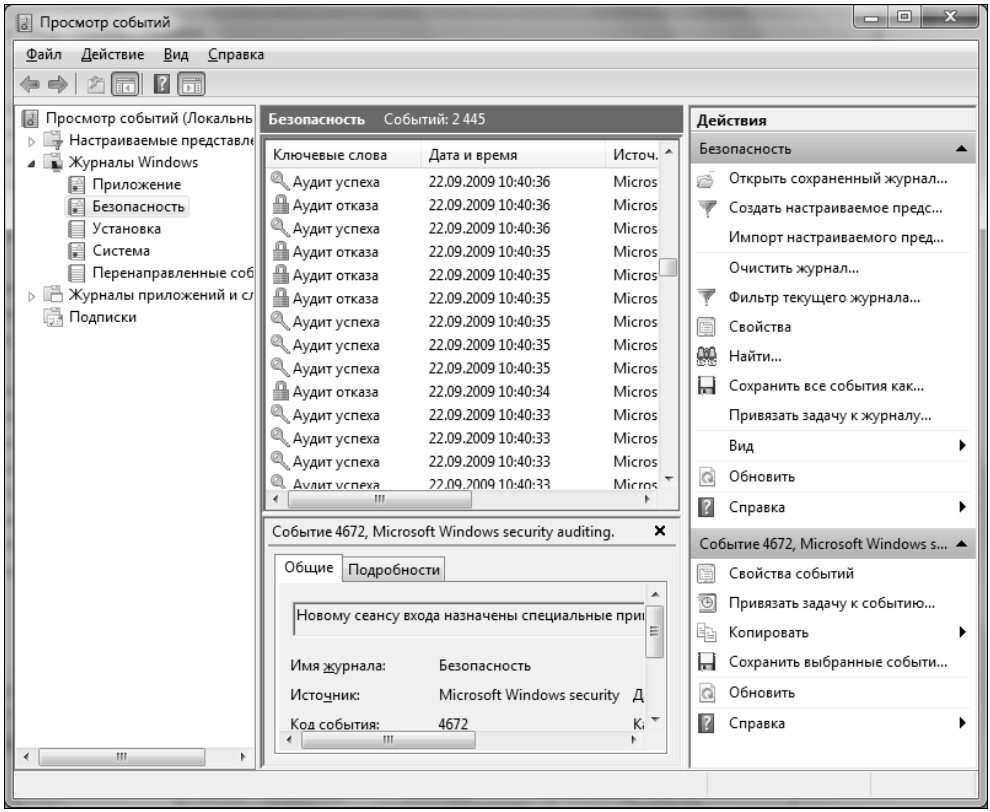


Рис. 21.2. Мониторинг реестра путем просмотра журнала безопасности в Windows 7

Но, как администратор, вы должны знать этот способ, а использовать его или нет — решать вам.

В Windows NT/2000/XP для этой цели требовалось в первую очередь включить политику аудита. В Windows Vista и Windows 7, даже если политика аудита не активизирована, аудит ведется все равно, в чем нетрудно убедиться, просмотрев сначала политики аудита, а затем — системный журнал безопасности. Тем не менее, установка политики аудита позволит вам более точно указать, какие именно события и из каких источников вас интересуют, и потому должны регистрироваться с журнале безопасности. Чтобы настроить политику аудита, выполните команду меню **Пуск** (Start) | **Панель управления** (Control Panel) | **Система и безопасность** (System and Security) | **Администрирование** (Administrative Tools). Запустите утилиту **Локальная политика безопасности** (Local Security Policy), см. рис. 21.3.

Выберите в левой панели раздел **Локальные политики** (Local Policy) | **Политика аудита** (Audit), как показано на рис. 21.4, а затем на правой панели

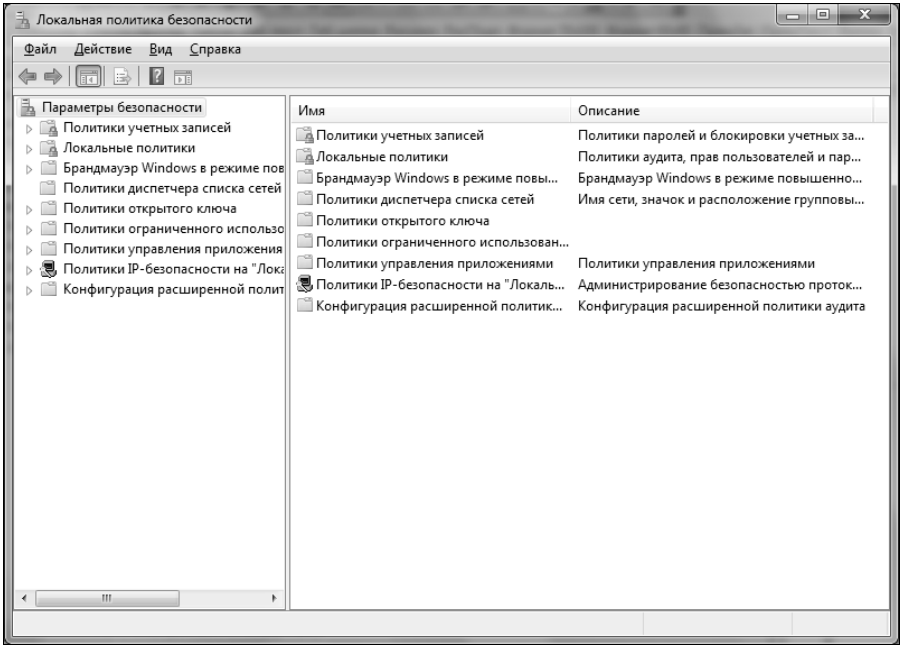


Рис. 21.3. Локальная политика безопасности

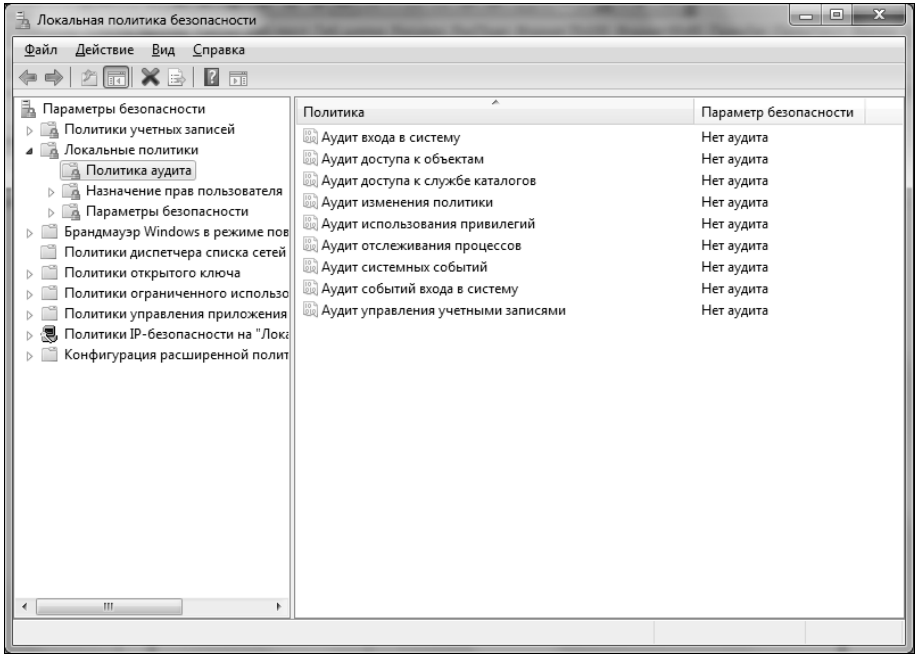


Рис. 21.4. Политики аудита

дважды щелкните по строке политики **Аудит доступа к объектам** (Audit object access). В появившемся окне (рис. 21.4) установите оба переключателя: **Успех** (Success) и **Отказ** (Failure), см. рис. 23.4.

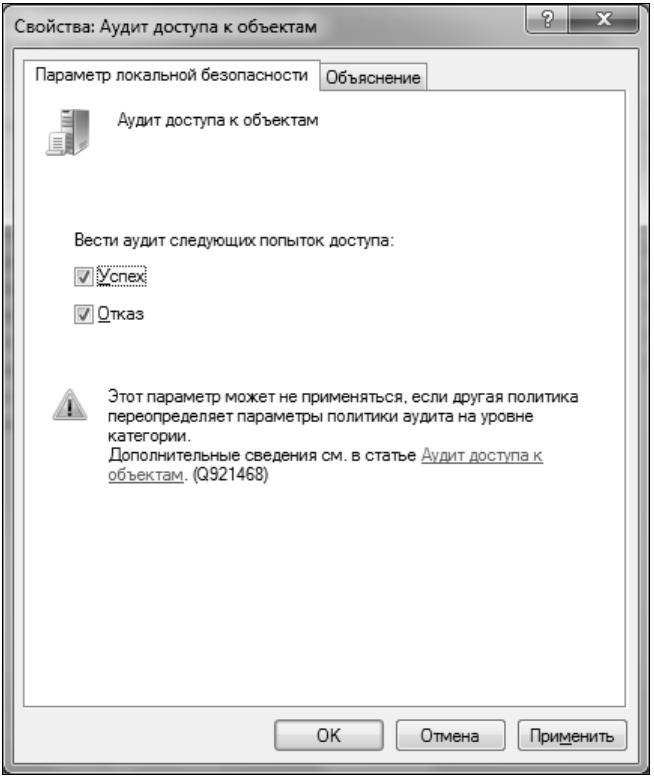


Рис. 21.5. Включение политики аудита доступа к объектам

Теперь запустите редактор реестра и перейдите в тот раздел, за которым вы хотите присмотреть. Пусть это будет `HKCU\Software\Policies\Explorer`. Выберите из меню **Правка** (Edit) команду **Разрешения** (Permissions) и в появившемся окне нажмите кнопку **Дополнительно** (Advanced). В результате выполненных действий на экране появится окно **Дополнительные параметры безопасности** (Advanced Security Settings for Policies), в котором нужно перейти на вкладку **Аудит** (Auditing), как показано на рис. 21.6.

Нажмите кнопку **Добавить** (Add) и с помощью окна **Выбор: "Пользователь" или "Группа"** (Select User or Group) выберите учетные записи, за которыми вы собираетесь осуществлять контроль (рис. 21.7). Для эксперимента можете выбрать свое имя пользователя — просто чтобы научиться использовать аудит реестра.

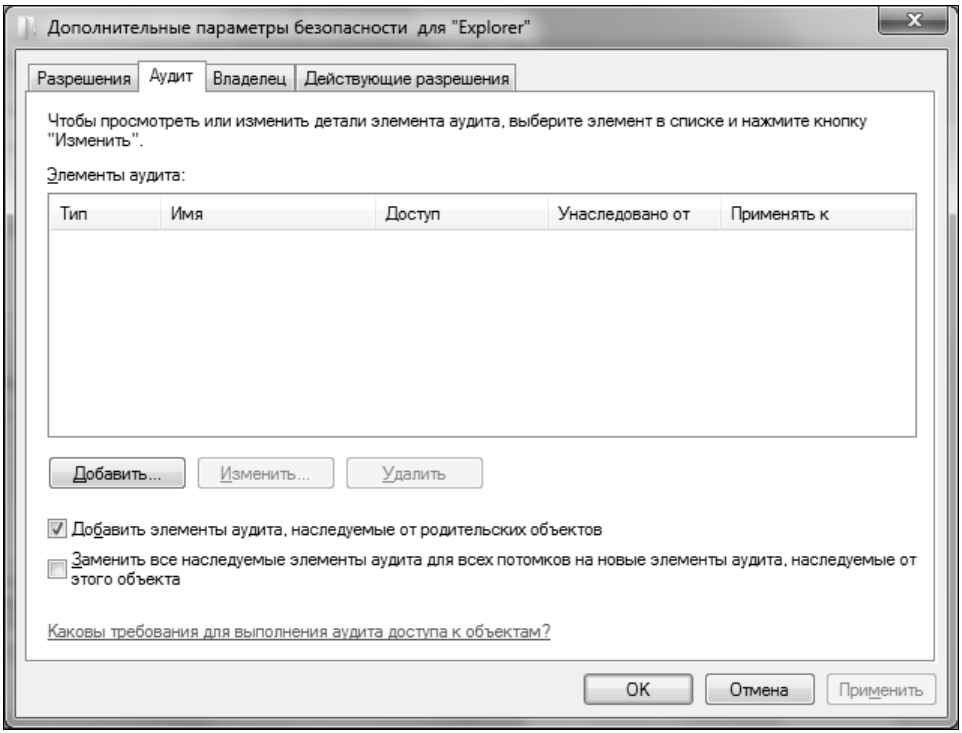


Рис. 21.6. Дополнительные параметры безопасности

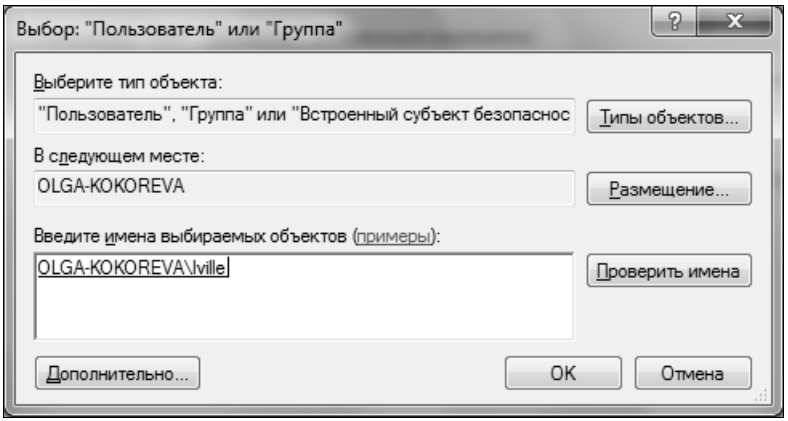


Рис. 21.7. Выбор пользователя или группы

Далее в окне **Элемент аудита** (Auditing Entry for Policies) (рис. 21.8) нужно установить флажок **Успех** (Success) или **Отказ** (Failure) рядом с действиями, которые вы хотите отслеживать.

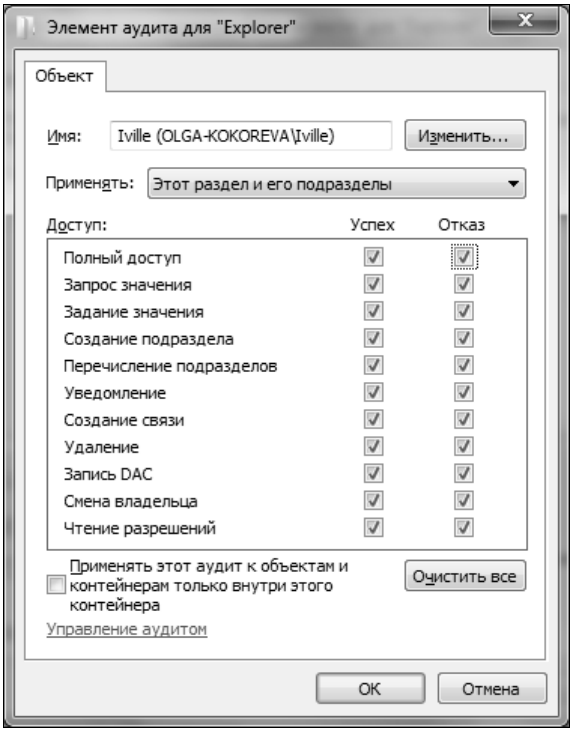


Рис. 21.8. Элементы аудита

Нажмите кнопку **Применить** (Apply), затем — кнопку **OK**. Все необходимое мы настроили.

Попробуйте теперь изменить параметры реестра. Не нужно модифицировать много параметров, например, измените какой-нибудь один — из того раздела, который вы контролируете. Сейчас вы поймете, почему не нужно было изменять много параметров. Откройте программу **Просмотр событий** (**Панель управления, Система и безопасность, Администрирование, Просмотр событий**). Выберите журнал **Безопасность** (Security). В нем шесть событий, хотя я изменил всего один параметр (рис. 21.9).

Давайте просмотрим события. Выделите самое раннее из событий (оно расположено в нижней строке) и дважды щелкните по нему. Появится окно **Свойства событий** (Event Properties), см. рис. 21.10, в котором приводится

подробное описание выбранного вами события. С помощью кнопок вверх/вниз вы можете переходить к просмотру деталей других событий.

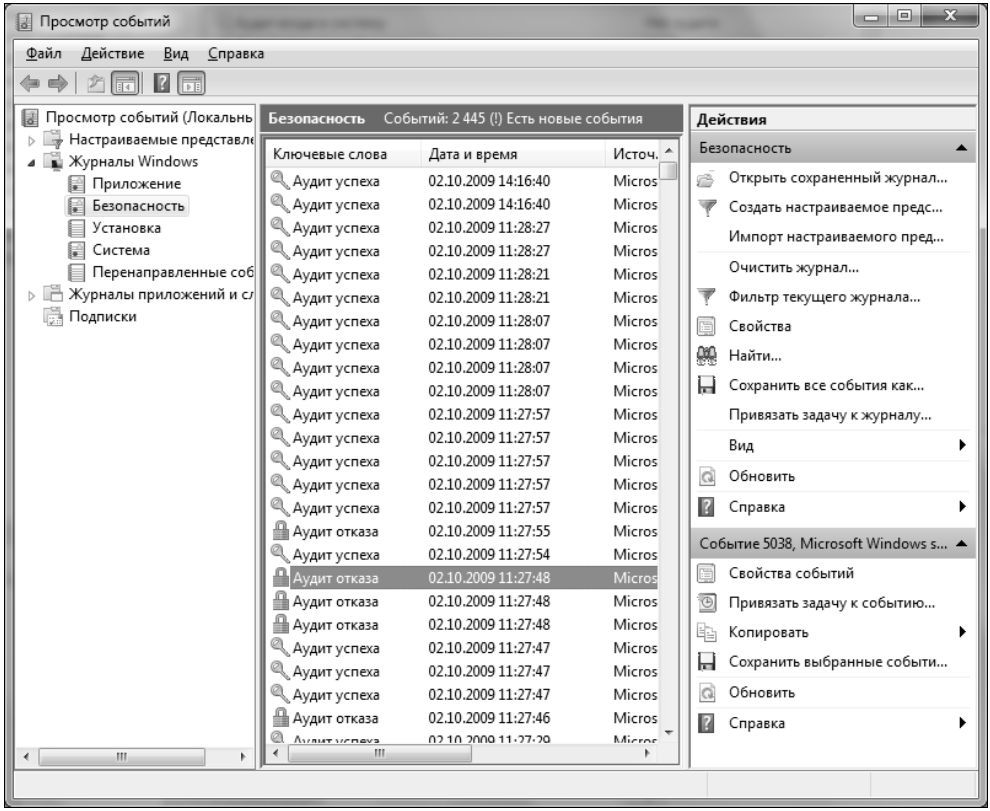


Рис. 21.9. Окно **Просмотр событий** (Event Viewer)

Теперь посмотрим, какие события произошли при изменении параметра:

1. Открытие объекта `\REGISTRY\USER\S-1-5-21-2052111302-436374069-1343024091-1003\Software\Policies`. Код дескриптора 623.
2. Закрытие дескриптора. Код дескриптора 623.
3. Открытие объекта `\REGISTRY\USER\S-1-5-21-2052111302-436374069-1343024091-1003\Software\Policies`. Код дескриптора 136.
4. Попытка доступа к объекту: Запрос значения раздела.
5. Попытка доступа к объекту: Задание значения раздела.
6. Закрытие дескриптора. Код дескриптора 136.

Не знаю, как вам, но мне удобнее использовать WinDiff.

Рис. 21.10. Просмотр свойств события

21.2. Мониторинг реестра: программа *Regmon*

Мониторинг реестра похож на аудит, но выполняется в реальном времени. Вы запускаете программу для мониторинга реестра и с ее помощью отслеживаете производимые в нем изменения. Программа-монитор может выводить изменения как во всем реестре, так и в определенном его разделе, кроме того, можно отслеживать обращение к реестру определенных программ.

Одной из самых лучших программ для мониторинга реестра является RegMon (Registry Monitor), разработанная Марком Руссиновичем (Mark Russinovich). Программа доступна по следующим адресам[1]:

http://download.sysinternals.com/Files/Regmon.zip

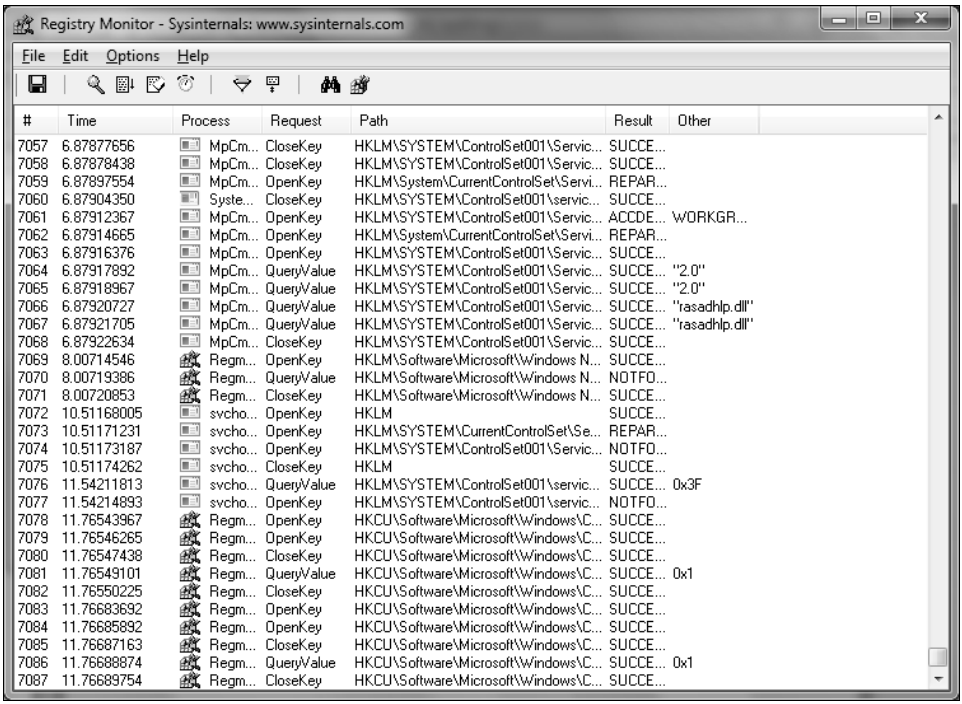
http://www.microsoft.com/technet/sysinternals/utilities/regmon.mspx

[1] На момент редактирования книги эта программа уже была убрана с указанных адресов разработчиков, но скачать ее пока еще можно, например, отсюда: **http://www.snapfiles.com/get/regmon.html**. Дело в том, что разработчик программы уже выпустил ей на смену новую утилиту, Process Monitor, сочетающую в себе функциональные возможности RegMon и FileMon. — *Прим. ред.*

Примечание

Кроме программы Regmon есть программа FileMon, отслеживающая обращения различных процессов к файловой системе, но мы ее рассматривать не будем, поскольку она не имеет отношения к реестру.

Скачайте и запустите программу RegMon (рис. 21.11). Вы увидите, что к реестру то и дело обращаются различные программы, добавляя новые записи в журнал монитора реестра.



#	Time	Process	Request	Path	Result	Other
7057	6.87877656	MpCm...	CloseKey	HKLM\SYSTEM\ControlSet001\Servic...	SUCCE...	
7058	6.87878438	MpCm...	CloseKey	HKLM\SYSTEM\ControlSet001\Servic...	SUCCE...	
7059	6.87897554	MpCm...	OpenKey	HKLM\System\CurrentControlSet\Servi...	REPAR...	
7060	6.87904350	Syste...	CloseKey	HKLM\SYSTEM\ControlSet001\servic...	SUCCE...	
7061	6.87912367	MpCm...	OpenKey	HKLM\SYSTEM\ControlSet001\Servic...	ACCDE...	WORKGR...
7062	6.87914665	MpCm...	OpenKey	HKLM\System\CurrentControlSet\Servi...	REPAR...	
7063	6.87916376	MpCm...	OpenKey	HKLM\SYSTEM\ControlSet001\Servic...	SUCCE...	
7064	6.87917892	MpCm...	QueryValue	HKLM\SYSTEM\ControlSet001\Servic...	SUCCE...	"2.0"
7065	6.87918967	MpCm...	QueryValue	HKLM\SYSTEM\ControlSet001\Servic...	SUCCE...	"2.0"
7066	6.87920727	MpCm...	QueryValue	HKLM\SYSTEM\ControlSet001\Servic...	SUCCE...	"rasadhlp.dll"
7067	6.87921705	MpCm...	QueryValue	HKLM\SYSTEM\ControlSet001\Servic...	SUCCE...	"rasadhlp.dll"
7068	6.87922634	MpCm...	CloseKey	HKLM\SYSTEM\ControlSet001\Servic...	SUCCE...	
7069	8.00714546	Regm...	OpenKey	HKLM\Software\Microsoft\Windows N...	SUCCE...	
7070	8.00719386	Regm...	QueryValue	HKLM\Software\Microsoft\Windows N...	NOTFO...	
7071	8.00720853	Regm...	CloseKey	HKLM\Software\Microsoft\Windows N...	SUCCE...	
7072	10.51168005	svcho...	OpenKey	HKLM	SUCCE...	
7073	10.51171231	svcho...	OpenKey	HKLM\SYSTEM\CurrentControlSet\Se...	REPAR...	
7074	10.51173187	svcho...	OpenKey	HKLM\SYSTEM\ControlSet001\Servic...	NOTFO...	
7075	10.51174262	svcho...	CloseKey	HKLM	SUCCE...	
7076	11.54211813	svcho...	QueryValue	HKLM\SYSTEM\ControlSet001\servic...	SUCCE...	0x3F
7077	11.54214893	svcho...	OpenKey	HKLM\SYSTEM\ControlSet001\servic...	NOTFO...	
7078	11.76543967	Regm...	OpenKey	HKCU\Software\Microsoft\Windows\C...	SUCCE...	
7079	11.76546265	Regm...	OpenKey	HKCU\Software\Microsoft\Windows\C...	SUCCE...	
7080	11.76547438	Regm...	CloseKey	HKCU\Software\Microsoft\Windows\C...	SUCCE...	
7081	11.76549101	Regm...	QueryValue	HKCU\Software\Microsoft\Windows\C...	SUCCE...	0x1
7082	11.76550225	Regm...	CloseKey	HKCU\Software\Microsoft\Windows\C...	SUCCE...	
7083	11.76683692	Regm...	OpenKey	HKCU\Software\Microsoft\Windows\C...	SUCCE...	
7084	11.76685892	Regm...	OpenKey	HKCU\Software\Microsoft\Windows\C...	SUCCE...	
7085	11.76687163	Regm...	CloseKey	HKCU\Software\Microsoft\Windows\C...	SUCCE...	
7086	11.76688874	Regm...	QueryValue	HKCU\Software\Microsoft\Windows\C...	SUCCE...	0x1
7087	11.76689754	Regm...	CloseKey	HKCU\Software\Microsoft\Windows\C...	SUCCE...	

Рис. 21.11. Монитор реестра (Registry Monitor)

Использовать программу в таком режиме неудобно — очень сложно отыскать обращения к нужному разделу реестра или обращения нужной программы к реестру.

21.2.1. Отслеживание обращений к реестру определенного процесса

Для отслеживания обращений определенной программы к реестру выполните следующие действия:

1. Нажмите клавиатурную комбинацию <Ctrl>+<E> для прекращения мониторинга реестра или кнопку **Capture** на панели инструментов.

2. Выберите в списке процессов интересующий вас процесс, щелкнув по нему правой кнопкой мыши, и выберите команду **Include Process**. Будет установлен фильтр по выбранному вами процессу.
3. Нажмите клавиатурную комбинацию <Ctrl>+<E> для продолжения мониторинга реестра.

На рис. 21.12 отображена информация об обращении к реестру процесса `regedit`. Информация представлена в следующем виде:

- **Time** — время обращения к реестру. Изменить формат времени можно, нажав клавиатурную комбинацию <Ctrl>+<T>. Очень рекомендую пользоваться клавиатурной комбинацией <Ctrl>+<T> — так будет удобнее (рис. 21.13);

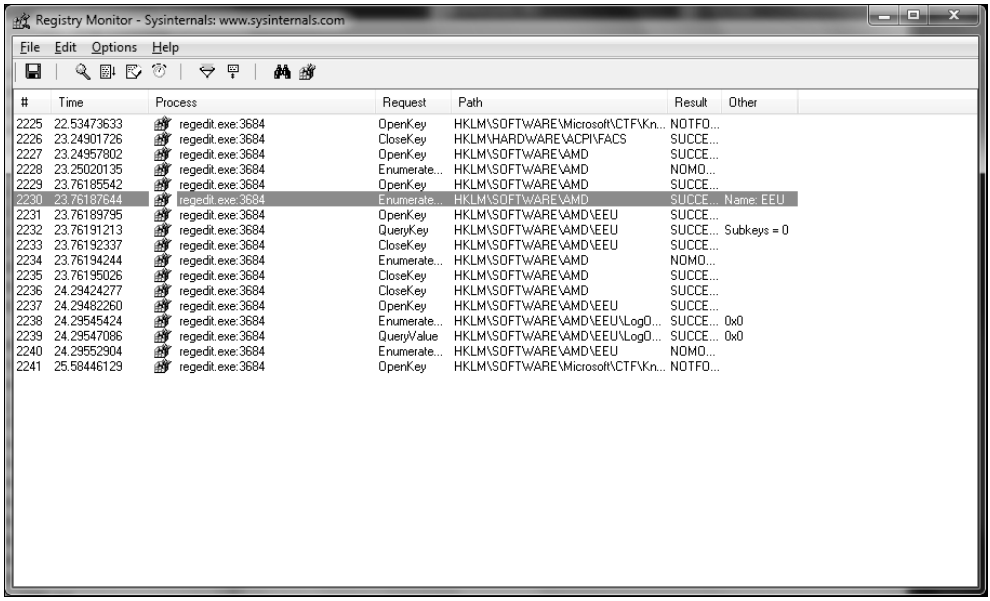


Рис. 21.12. Обращение к реестру программы regedit

- **Process** — процесс, который обращается к реестру;
- **Request** — тип запроса к реестру, например:
  - **OpenKey** — открыть раздел реестра;
  - **QueryValue** — запросить значение параметра;
  - **SetValue** — установить значение параметра;
- **Result** — результат операции (`SUCCESS` — операция завершена успешно, `NOT FOUND` — параметр или ключ не найден и т. д.);

- **Other** — значение прочитанного параметра или устанавливаемое значение параметра.

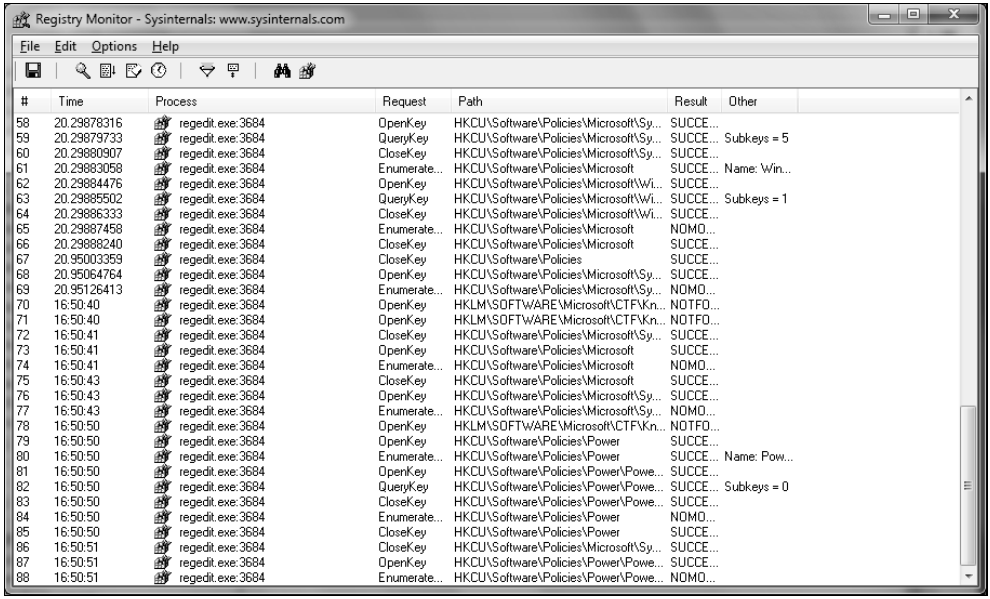


Рис. 21.13. Изменен формат времени

21.2.2. Отслеживание обращений к определенному разделу реестра

Для отслеживания обращений к определенному разделу реестра выполните следующие действия:

1. Нажмите клавиатурную комбинацию <Ctrl>+<E> для прекращения мониторинга. Это необходимо для того, чтобы вы могли легко найти нужный вам путь (раздел реестра).
2. Если в предыдущем примере вы установили фильтр по процессу, то для его сброса нажмите комбинацию клавиш <Ctrl>+<L>, а в появившемся окне — кнопку **Defaults**.
3. Выберите нужный вам раздел реестра, щелкните по нему правой кнопкой мыши и выполните команду **Include Path**.
4. Нажмите клавиши <Ctrl>+<E> для продолжения мониторинга реестра.

Второй шаг не является обязательным. Вы можете добавить в фильтр одновременно несколько процессор и/или разделов реестра. Если сначала доба-

вить процесс, а потом раздел реестра (или наоборот), то будут отслеживаться действия, выполняемые указанным процессом в выбранном разделе реестра.

21.2.3. Установка фильтров

Иногда бывает так, что в журнале монитора реестра нет нужного вам процесса или раздела реестра — просто этот процесс еще не запущен или к нужному ключу пока еще не обращалась ни одна программа. Нажмите комбинацию клавиш <Ctrl>+<L> для вызова окна редактирования фильтров (рис. 23.14).

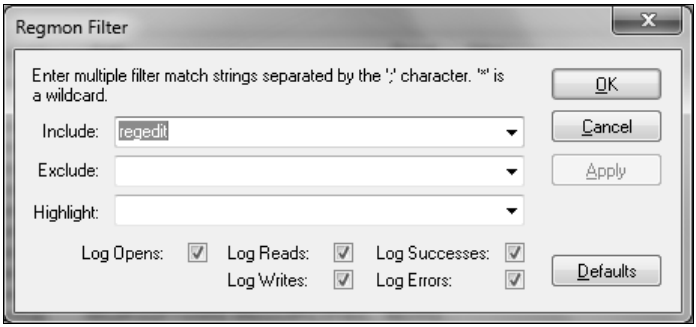


Рис. 21.14. Окно редактирования фильтров

В список **Include** можно включить все, что вы хотите увидеть — имена процессов, разделов. Различные элементы списка разделяются точкой с запятой, например:

```
regedit.exe;HKCU\Software\Policies\My
thebat.exe;regedit.exe;"HKCU\Software\RIT\The Bat!"
```

В список **Exclude**, наоборот, помещаются те элементы, которые вы не хотите видеть в результате мониторинга. В список **Highlight** нужно добавить те значения списка мониторинга, которые нужно выделить.

Некоторые примеры установки фильтра приведены в табл. 21.1.

Таблица 21.1. *Установка фильтра мониторинга*

Желаемый результат	Include	Exclude	Highlight
Вывести все обращения к реестру программы regedit	regedit.exe		
Вывести все обращения к ключу `HKLM\Software`	`HKLM\Software`		
Вывести все обращения к ключу `HKLM\Software`, исключая обращения программы regedit	`HKLM\Software`	regedit.exe	

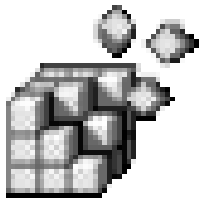
Таблица 21.1 *(окончание)*

Желаемый результат	Include	Exclude	Highlight
Вывести все обращения к реестру, выделить обращения программы thebat.exe	*		thebat.exe
Вывести все обращения к `HKLM\Software` программы regedit.exe	regedit; `HKLM\Software`		

Группа параметров **Log Opens** (см. рис. 21.14) позволяет указать обращения к реестру, которые следует протоколировать:

- **Log Reads** — чтение разделов/параметров реестра;
- **Log Writes** — операции записи;
- **Log Successes** — успешные операции обращения к реестру;
- **Log Errors** — неудачные операции обращения к реестру.

ГЛАВА 22



INF- и REG-файлы

22.1. Автоматизация внесения изменений в реестр

Предположим, что у вас есть любимые параметры реестра, которые вы изменяете каждый раз после установки Windows. Нет, я не намекаю на то, что Windows очень ненадежная система. Возможно, вы настраиваете новые компьютеры в компьютерном магазине или работаете системным администратором довольно большого парка компьютеров и вам приходится несколько раз в месяц переустанавливать Windows на том или ином компьютере. А может, вы просто хотите установить аналогичные параметры на другом компьютере (компьютера друга или на втором вашем компьютере). Не будете же вы носить с собой эту книжку?

Гораздо проще использовать для внесения изменений в реестр скрипты. В Windows вы можете использовать следующие скрипты:

- INF- и REG-файлы — с этими файлами мы подробно познакомимся в данной главе;
- командные (пакетные) файлы — эти скрипты подразумевают использование программы reg.exe, которую мы рассмотрели в *главе 14*;
- WSH-скрипты — скрипты на языках VBScript или JavaScript;
- пакеты Windows Installer — об установщике программ мы поговорим в *главе 24*.

Наиболее простыми в использовании являются REG-файлы. INF-файлы более сложны, но позволяют выполнять операции с реестром более гибко, чем REG-файлы.

Пакетные файлы — это файлы с расширением .cmd. Пакетный файл содержит список команд, которые должен выполнить командный интерпретатор. В нашем случае это список команд, вызывающий консольный редактор реестра — программу reg.exe, которая была описана в *главе 14* этой книги.

WHS-скрипты использовать сложнее всего, поскольку вы должны знать один из скриптовых языков — VBScript или JavaScript. Здесь не будем рассматривать WSH (Windows Script Host), поскольку это выходит за рамки книги.

В *главе 24* мы познакомимся с пакетами Windows Installer, имеющими расширение .msi, с помощью которых также можно вносить изменения в реестр. Пакеты MSI удобны тогда, когда вам не нужно, чтобы вносимые в реестр изменения были видны невооруженным взглядом, ведь поскольку INF- и REG-файлы — текстовые, их можно открыть и просмотреть в любом текстовом редакторе. С MSI-файлами такого сделать нельзя. Можно, конечно, проследить изменения, вносимые MSI-пакетами в реестр с помощью программы RegMon.exe, но большинство пользователей не подозревает о ее существовании.

22.2. INF-файлы

INF-файлы (Setup Information Files) предназначены для создания сценариев инсталляций. Обычно INF-файлы используются для установки драйверов — устанавливать с их помощью приложения также допустимо, но неудобно.

Мы можем использовать INF-файлы для изменения параметров реестра. Преимущество INF-файлов перед REG-файлами заключается в том, что изменения, внесенные в реестр посредством INF-файлов, можно отменить с помощью апплета **Установка и удаление программ** (Add/Remove Programs), который можно запустить с Панели управления (Control Panel), тогда как для возвращения параметров, модифицированных REG-файлом, вам придется искать их вручную. При этом если вы не знаете значений параметров по умолчанию, то вам поможет только точка восстановления системы, что тоже нежелательно, поскольку вместе с настройками, внесенными в реестр REG-файлом, могут быть удалены настройки программ, внесенные после применения REG-файла. В случае с INF-файлами таких неудобств нет.

22.2.1. Формат INF-файла

Формат INF-файла похож на формат INI-файла. В INF-файле, как и в INI-файле, есть разделы (*или секции*), а каждый раздел содержит элементы, обычно имеющие вид `Имя=Значение`.

Создать INF-файл можно в любом текстовом редакторе — в частности, для этих целей идеально подходит Блокнот (Notepad). Чтобы не создавать INF-

файл каждый раз с чистого листа, вы можете создать шаблон, содержащий обязательные секции INF-файла. В листинге 22.1 приведен простейший шаблон INF-файла для внесения изменений в реестр.

Примечание

В листинге 22.1 приведен шаблон файла именно для внесения изменений в реестр. Как уже отмечалось, INF-файл может использоваться для установки драйверов и программ, поэтому в нем может быть секция копирования нужных файлов. В нашем случае такой секции не будет, поэтому приведенный шаблон INF-файла нельзя назвать полным.

Листинг 22.1. Простейший шаблон INF-файла

```
[Version]
Signature=$Windows NT$

[DefaultInstall]
; Действия при установке файла
AddReg=Add

[DefaultUninstall]
; действия при удалении
DelReg=Del

[Add]
; добавляем данные в реестр

[Del]
; удаляем данные из реестра
```

Секция `[Version]` является обязательной. Изменять ее нельзя. Вторая секция обычно называется `[DefaultInstall]`. Можно изменить имя этой секции, но лучше этого не делать. Директивы `AddReg` и `DelReg` задают имена секций, в которых находятся разделы и параметры, которые нужно добавить или удалить из реестра соответственно.

Директивы `AddReg` и `DelReg` могут располагаться как в секции `[DefaultInstall]`, так и в `[DefaultUninstall]`, причем в одной и той же секции может быть указано несколько директив `AddReg` и `DelReg`:

```
[DefaultInstall]
; Действия при установке файла
AddReg=Add1
AddReg=Add2
AddReg=Add3
```

```
DelReg=Del
[DefaultUninstall]
; действия при удалении
DelReg=Del1
DelReg=Del2
DelReg=Del3
AddReg=Del
```

Для сокращения длины INF-файла можно в одной из директив `AddReg` или `DelReg` указать несколько секций (через запятую):

```
[DefaultInstall]
; Действия при установке файла
AddReg=Add1,Add2,Add3
DelReg=Del
[DefaultUninstall]
; действия при удалении
DelReg=Del1,Del2,Del3
AddReg=Del
```

> ***Примечание***
>
> Названия секций (в приведенном выше примере — `[Add1]`, `[Add2]` и т. д.) должны быть уникальными в пределах INF-файла.

22.2.2. Добавление новых разделов и параметра реестра

Теперь поговорим о том, как задаются разделы и параметры реестра в секциях INF-файла. Общий формат такой:

`корневой раздел, [`*`подраздел`*`], [`*`параметр`*`], [`*`флаги`*`], [`*`данные`*`]`

Корневой раздел нужно указывать в любом случае. Допускается использование сокращенных имен: `HKCU`, `HKLM`, `HKCR`, `HKU`, `HKCC`. Подраздел можно не указывать — в этом случае все действия будут относиться к корневому разделу. Если вы не указываете подраздел, не забудьте поставить запятую, относящуюся к подразделу:

`корневой раздел, , [`*`параметр`*`], [`*`флаги`*`], [`*`данные`*`]`

`[`*`Параметр`*`]` представляет собой имя добавляемого или изменяемого параметра реестра, который уже существует. Имя параметра указывать необязательно. Если значение не указано, но указаны флаги и данные, то при выполнении операции будет использовано значение по умолчанию. Если не указаны параметр, флаги и данные, то это — операция добавления раздела реестра.

С помощью флагов вы можете задать тип создаваемого параметра и определить дополнительные атрибуты операции добавления или изменения параметра. Наиболее часто используемые флаги приведены в табл. 22.1.

***Таблица 22.1.** Некоторые флаги операций (при добавлении/изменении параметров)*

Флаг	Операция
0x00000000	Задает тип REG_SZ. Этот тип используется по умолчанию, поэтому можно не указывать данный флаг
0x00000001	Задает тип REG_BINARY
0x00010000	Задает тип REG_MULTI_SZ
0x00020000	Задает тип REG_EXPAND_SZ
0x00010001	Задает тип REG_DWORD
0x00020001	Задает тип REG_NONE
0x00000002	Если значения уже существуют, то они не должны перезаписываться
0x00000004	Используется для удаления подраздела или параметра реестра
0x00000008	Используется для присвоения значения параметру типа REG_MULTI_SZ. Значение не присваивается, если оно уже существует
0x00000010	Создает подраздел, но при этом игнорирует параметр и данные, если они указаны
0x00000020	Установить значение, если параметр уже существует
0x00001000	Изменения должны быть произведены в 64-разрядном реестре. Если флаг не задан, то изменения производятся в "родном" реестре — 64-разрядном для 64-разрядной системы и 32-разрядном для 32-разрядной системы
0x00004000	Изменение должны быть произведены в 32-разрядном реестре

Флаги, выделенные курсивом, можно объединять с другими флагами с помощью битового OR (или). Эту операцию можно произвести в калькуляторе, переведенном в инженерный режим.

После флагов должно быть указано значение параметра. Если параметр не существует, то он будет создан, а если существует — перезаписан. Если параметра имеет тип REG_MULTI_SZ и установлен флаг 0x00010008 (REG_MULTI_SZ + 0x00000008), то список строк будет добавлен к уже существующему.

Если значение параметра не указано, то параметр будет создан без указания значения.

Рассмотрим несколько примеров:

```
[Add]
; Создаем параметр Active типа REG_DWORD и присваиваем значение 1
HKCU,Software\Company\Program,Active, 0x10001,1

; Создаем параметр Str типа REG_SZ и присваиваем значение "Test String"
HKCU,Software\Company\Program,Str, ,"Test String"

; Устанавливаем значение по умолчанию
HKCU,Software\Company\Program,,,"По умолчанию"
```

22.2.3. Удаление разделов и параметров

Синтаксис описания разделов реестра такой же, как и в предыдущем случае:

Корневой раздел, [*подраздел*], [*параметр*], [*флаги*], [***значение***]

Корневой раздел — это основной раздел, содержащий раздел реестра или параметр, который нужно удалить. *Подраздел* — это дочерний раздел, который нужно удалить, или же подраздел, содержащий параметр, который вы хотите удалить. *Параметр* — это имя параметра, который нужно удалить.

Как и в случае с добавлением/изменением значений, можно указать дополнительные флаги, представленные в табл. 22.2.

Таблица 22.2. *Флаги для удаления разделов/параметров*

Флаг	Операция
0x00002000	Удалить весь подраздел
0x00018002	Если параметр имеет тип REG_MULTI_SZ, то удаляются все строки, соответствующие строке, указанной в качестве значения

Значение (см. выше) используется, только если установлен флаг 0x00018002 и тип параметра равен REG_MULTI_SZ. В этом случае указанное значение будет удалено.

В листинге 22.2 приведен код INF-файла, удаляющего отмеченные параметры и разделы реестра при его установке.

Листинг 22.2. Пример удаления

```
[Version]
Signature=$Windows NT$
[DefaultInstall]
```

```
DelReg=Del
[Del]
; удаляем параметр Str из Software\Company\Program
HKCU,Software\Company\Program,Str
; удаляем строку "Text" из списка строк
HKCU, Software\Company\Program,StringList,0x00018002,"Text"
;удаляем весь раздел Software\Company\Program
HKCU, Software\Company\Program
```

22.2.4. Установка INF-файла

Для установки INF-файла нужно щелкнуть по нему правой кнопкой мыши и выбрать из контекстного меню команду **Установить** (Install), как показано на рис. 22.1.

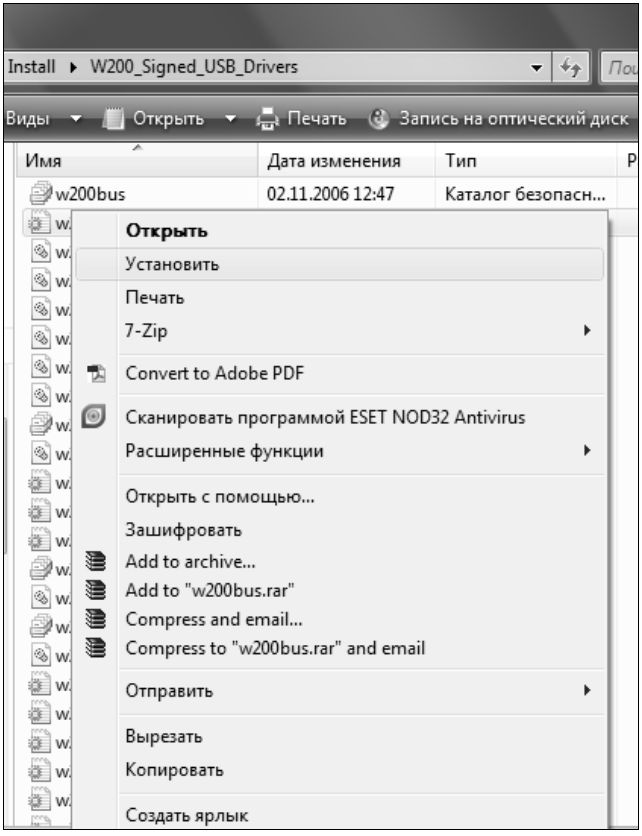


Рис. 22.1. Установка INF-файла

22.3. REG-файлы

Использовать REG-файлы просто и удобно: вы можете создать все необходимые параметры в реестре, а затем экспортировать их в REG-файл. Преимущество заключается в том, что в REG-файлах исключены синтаксические ошибки — они создаются редактором реестра автоматически, без вашего вмешательства.

На рис. 22.2 изображен примерный вид раздела реестра, который я попытаюсь экспортировать в REG-файл с помощью команд **Файл** (File) | **Экспорт** (Export).

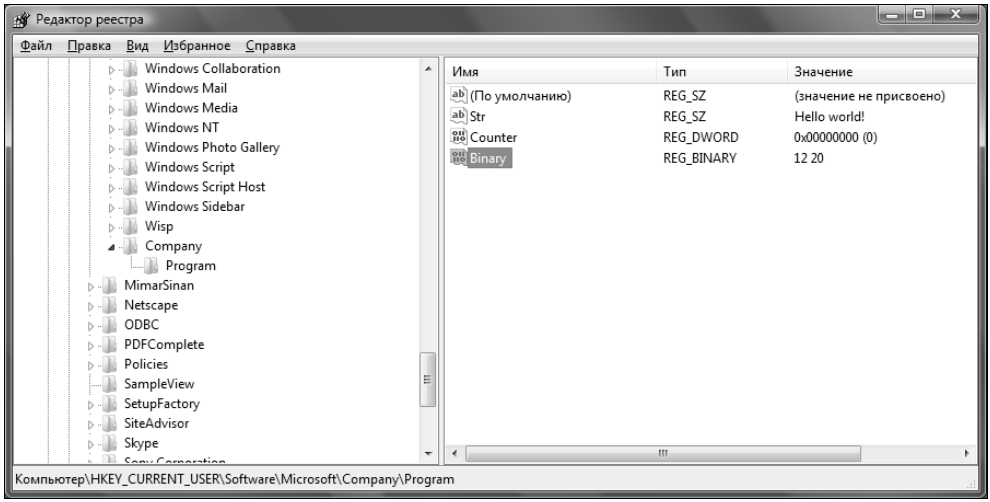


Рис. 22.2. Примерный раздел реестра

В результате экспорта получился REG-файл, приведенный в листинге 22.3.

Листинг 22.3. REG-файл

```
Windows Registry Editor Version 5.00
[HKEY_CURRENT_USER\Software\Company\Program]
"Str"="Hello world!"
"Counter"=dword:00000000
"Binary"=hex:12,20
```

Название разделов реестра в REG-файле, так же как и секции в INF-файлах, записываются в квадратных скобках.

Строковые значения (`REG_SZ`) заключаются в кавычки; перед значениями типа `REG_DWORD` указывается ключевое слово `dword:`, а перед шестнадцатеричными значениями — `hex`.

Некоторые специальные символы, например обратный слэш, цитируются с помощью обратной косой черты (\) так:

```
C:\\Windows\\system32
```

У REG-файлов есть один недостаток: REG-файл, сгенерированный для вашего реестра, может использоваться только для экспортированных в него ключей и параметров. А как с его помощью удалить разделы и параметры? Для этого вам придется писать REG-файл вручную.

Для удаления целого раздела реестра нужно перед именем раздела поставить знак "-", например:

```
[-HKEY_CURRENT_USER\Software\Company\Program]
```

Если вы хотите удалить параметр, то минус нужно поставить перед его значением:

```
"имя"=-"значение"
```

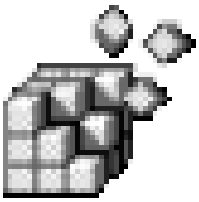
Вот пример REG-файла для удаления раздела `HKEY_CURRENT_USER\Software\Company\Program`:

```
Windows Registry Editor Version 5.00
[-HKEY_CURRENT_USER\Software\Company\Program]
```

Напомню, что создать REG-файл можно в любом текстовом редакторе, например в Блокноте (Notepad). При создании REG-файла в Блокноте убедитесь, что файл сохранен с расширением .reg, а не .reg.txt, иначе система будет считать его обычным текстовым файлом.

Для применения REG-файла нужно дважды щелкнуть по его имени в окне Проводника, при этом система спросит вас, хотите ли вы применить REG-файл. Вам нужно согласиться.

ГЛАВА 23



Профили пользователей

23.1. Зачем используются перемещаемые профили?

Как известно, Windows хранит индивидуальные параметры настройки системы и приложений, заданные для каждого пользователя, в отдельном профиле. У каждого пользователя могут быть свои параметры рабочего стола, свои документы, своя папка Избранное (Favorites). Разработчики из Microsoft задумывали Windows как операционную систему, ведущую себя максимально дружелюбно по отношению к пользователю, поэтому удобство работы и комфорт пользователя имели для них первоочередной приоритет. Но одним лишь комфортом сыт не будешь. Профили пользователей содержат еще и настройки реестра, действующие индивидуально для конкретного пользователя. Такие настройки необходимо отделить от других настроек, действующих применительно ко всей системе в целом, поэтому второе назначение пользовательских профилей — это обеспечение стабильности работы операционной системы. Принцип "Разделяй и властвуй!" в Windows, как и в любой другой современной операционной системе, используется почти в полном объеме.

Администраторам часто приходится сталкиваться с перемещаемыми профилями: это позволяет сэкономить огромное количество времени, а значит, и денег. Когда я работал администратором довольно большого предприятия, постоянно возникала проблема печати. Компьютеров в сети было не очень много — около 50, но за каждым из них в разное время могло работать 2–3 человека. Так вот, когда пользователь в первый раз заходил в сеть предприятия и пытался что-нибудь распечатать, ему приходилось настраивать принтер. А поскольку он не знал, как это сделать, он дергал администратора, т. е. меня или моего коллегу. Спасли именно перемещаемые профили: по

умолчанию были добавлены сведения о сетевых принтерах, и после этого администраторам уже не приходилось настраивать принтеры для каждого пользователя отдельно.

Управление профилями полезно не только для администраторов. Опытные пользователи могут переносить свои профили на другие компьютеры, чтобы всегда работать с привычными настройками.

23.2. Исследуем пользовательские профили

Профиль пользователя загружается, когда пользователь входит в систему, и выгружается при выходе пользователя из нее. Профиль содержит настройки реестра (куст реестра), которые к нему добавляются при загрузке профиля. Но профиль пользователя — это не только куст реестра, но и совокупность различных папок, хранящих большой объем разнообразной информации — от служебных файлов системы до личных файлов пользователя. В этом разделе мы подробно рассмотрим структуру пользовательских профилей.

Обычно профили пользователей находятся в каталоге *%Systemdrive%*\Documents and Settings (например, C:\Documents and Settings) для Windows XP или *%Systemdrive%*\Users для Windows Vista и Windows 7.

> ***Примечание***
>
> Если система Windows XP устанавливалась как обновление с Windows NT 4.0 до Windows XP, то профили пользователей находились в каталоге *%Systemroot%*\Profiles. А вот встретить систему, обновленную с Windows XP до Windows 7 — сложно. Как свидетельствуют сообщения на форумах, головной боли при переходе с Windows XP на Windows 7 достаточно, поэтому многие пользователи после неудачной попытки обновления выполняют обычную установку (не обновление) Windows 7.

Список профилей пользователей хранится в реестре в разделе `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList`. Каждый подраздел этого раздела описывает отдельный профиль пользователя. Имя раздела соответствует идентификатору безопасности пользователя (SID). В каждом разделе, описывающем профиль, находится параметр `ProfileImagePath` типа `REG_SZ`, содержащий название домашнего каталога пользователя.

В каждом профиле (папке *%Systemdrive%*\Users*Username*, где *Username* — это имя пользователя, под которым он регистрируется в системе) есть файл Ntuser.dat. Этот файл, как мы уже знаем, является файлом куста профиля пользователя. При загрузке профиля Windows загружает данный файл в подключ `HKU\<SID>`,

где SID — это идентификатор безопасности пользователя. После этого Windows связывает ключ HKCU с HKU\<*SID*>.

В Windows 7 профиль пользователя, кроме файла куста, включает в себя названия служебных папок и их содержимое:

- AppData — содержит настройки приложений. Аналога этому каталогу в Windows XP нет. Внутри этой папки вы найдете три папки:
  - Local и LocalLow — содержат неперемещаемые данные, например, общесистемные параметры или же очень большие файлы;
  - Roaming — данные, которые будут перемещаться вместе с профилем пользователя по сети;
- Application Data* — данные, относящиеся к определенному приложению. Что будет содержаться в этом каталоге, зависит от использующихся программ. По сути, это ссылка на папку AppData\Roaming. Аналог в Windows XP — каталог Documents and Settings\%*username*%\Application Data;
- Contacts — информация о контактах пользователя. Графический интерфейс отображает название этой папки как "Контакты". Аналога в Windows XP нет.
- Cookies* — пользовательские файлы cookie для Internet Explorer. В Windows XP файлы cookie хранились в каталоге Documents and Settings\%*username*% \Cookies;
- Desktop — ярлыки, файлы и папки рабочего стола. Практически все, что находится на рабочем столе, хранится в этой папке. В Windows XP элементы рабочего стола хранились в Documents and Settings\%*username*%\Desktop;
- Documents — используется для хранения документов пользователя. Кроме этого, некоторые приложения сохраняют файлы, созданные пользователем, в подкаталогах этого каталога, например, ICQ хранит историю переписки и другие параметры учетной записи пользователя, а все игры от Electronics Arts — сохраненные игры. Аналог в Windows XP — Documents and Settings\%*username*%\My Documents. В Windows XP в каталоге Мои документы были также каталоги Мои рисунки, Моя музыка и некоторые другие, предназначенные для хранения графических и музыкальных файлов пользователя, а также файлов с другим содержимым. В Windows 7 есть подобные каталоги (понятно, что их названия отличаются), но они находятся не в каталоге Documents, а в каталоге профиля пользователя. Что же касается каталога Documents, то в нем есть ссылки на эти каталоги;
- Downloads — здесь хранится загружаемая из Интернета информация, например, файлы, которые вы загружаете с помощью браузера или Torrent-клиента. В Windows XP аналогичной папки не было;

- Favorites — каталог содержит избранные ссылки Internet Explorer. Содержимое этого каталога отображается в меню **Избранное** (Favorites) браузера Internet Explorer. Аналог в Windows XP — папка Documents and Settings\%*username*%\Favorites;
- Links — используется для хранения ссылок на избранное содержимое. В Windows XP подобной папки нет;
- Local Settings* — файлы приложений, которые не перемещаются вместе с профилем пользователя по сети. Обычно здесь находятся или общекомпьютерные файлы (одинаковые для всех пользователей), или файлы, которые слишком велики для копирования по сети. Это ссылка на каталог AppData\Local. Аналог в XP — Documents and Settings\%*username*%\Local Settings;
- Music — используется для хранения музыкальных файлов пользователя. Аналог в Windows XP — Documents and Settings\%*username*%\My Music;
- NetHood* — содержит ярлыки объектов, расположенных в сети. Подобная папка в XP — Documents and Settings\%*username*%\NetHood;
- Pictures — содержит графические файлы пользователя. Аналогом этой папки в Windows XP является папка Documents and Settings\%*username*%\My Pictures;
- PrintHood* — содержит ярлыки принтеров. Аналог в Windows XP — папка Documents and Settings\%*username*%\PrintHood;
- Recent* — в этом каталоге находятся ярлыки на недавние документы. Подобная папка в Windows XP — Documents and Settings\%*username*%\My Recent Documents;
- Saved Games — сохраненные игры. В Windows XP такой папки не было;
- Searches — здесь хранятся результаты поиска. В Windows XP такой папки не было;
- SendTo* — содержит ярлыки дисков, папок и приложений, которые способны принять целевой файл. Эти ярлыки пользователь видит в контекстном меню **Отправить** (Send To). Аналог в Windows XP — Documents and Settings\%*username*%\SendTo;
- Videos — видеофайлы пользователя. В Windows XP видеофайлы пользователя хранились в папке Documents and Settings\%*username*%\My Videos;
- Main Menu* (Главное меню) — содержит папки и ярлыки главного меню (меню **Пуск**) пользователя. Аналог в Windows XP — папка Documents and Settings\%*username*%\Main Menu;
- Templates* (Шаблоны) — ярлыки, указывающие на шаблоны. Аналог в Windows XP — Documents and Settings\%*username*%\Templates.

Примечание

Символом "звездочки" (*) отмечены папки, являющиеся точками разветвления NTFS (junction points), ссылающиеся на соответствующие вложенные папки пользовательских профилей.

Некоторые из этих каталогов скрыты, поэтому для их отображения нужно включить отображение скрытых файлов и каталогов (рис. 23.1). На этой иллюстрации изображены две панели Total Commander: слева — содержимое каталога профиля Windows 7, а справа — Windows XP.

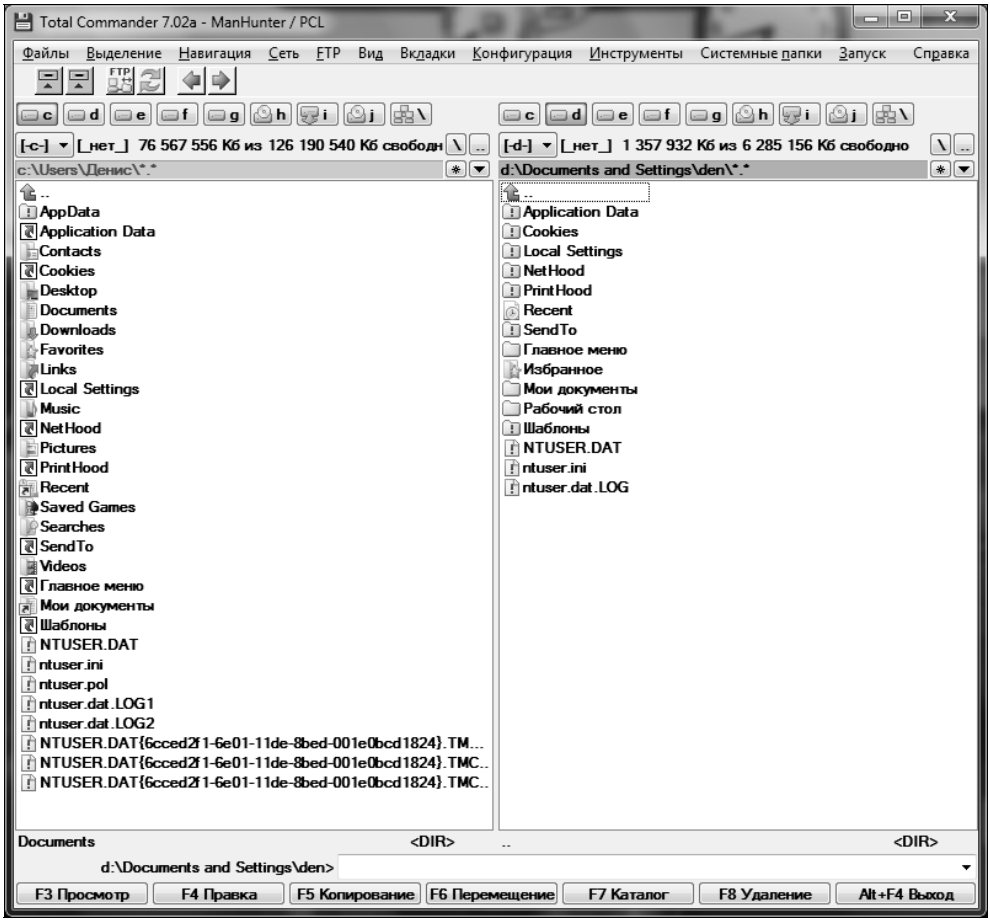


Рис. 23.1. Каталоги профиля пользователя Windows 7 и Windows XP

Графическая оболочка Windows отображает имена служебных каталогов в локализованном виде (см. рис. 23.2). Например, каталог C:\Users превратится в C:\Пользователи, а каталог C:\Users\<*имя пользователя*>\Searches — в C:\Пользователи

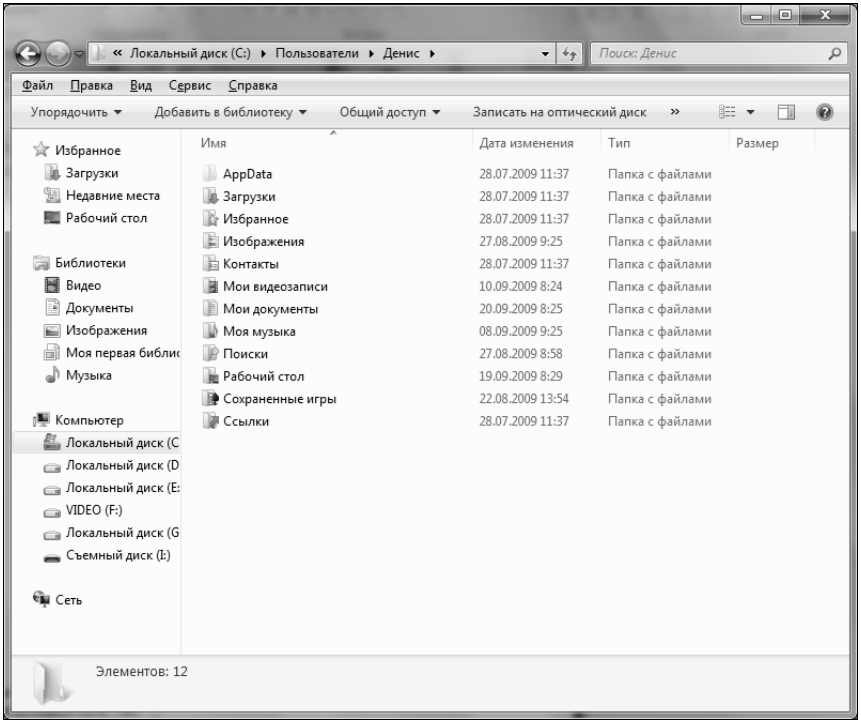


Рис. 23.2. Графическая оболочка выполняет локализацию имен служебных каталогов

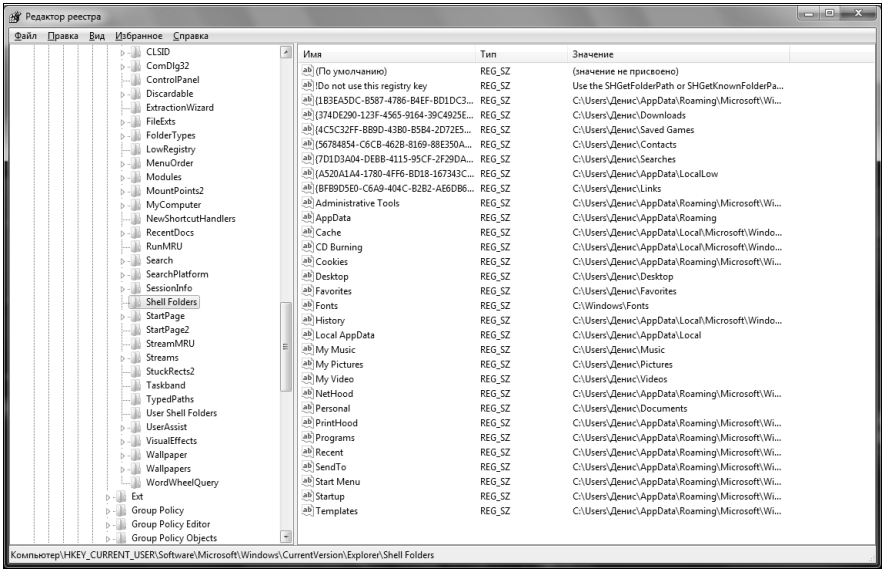


Рис. 25.3. Раздел
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders

\<*имя пользователя*>\Поиски и т. д. Но если просмотреть содержимое пользовательского профиля не через Проводник, а через командную строку или такое приложение, как Total Commander, то вы обнаружите, что все имена служебных каталогов — англоязычные.

Кроме только что упомянутых, в реестре есть еще один очень интересный раздел — `HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders`. Если в него заглянуть, то вы найдете в нем размещение каждой из папок, которая является частью профиля пользователя (рис. 23.3).

23.3. Служебные профили

Давайте рассмотрим каталог C:\Users. В нем вы обнаружите каталог Default — стандартный профиль пользователя (используемый по умолчанию). Содержимое этого каталога копируется в профиль пользователя при создании нового пользователя. Ссылка Default User ссылается как раз на каталог Default.

В Windows XP в каталоге Documents and Settings был каталог All Users, содержащий настройки, которые относятся ко всем пользователям компьютера. В Windows 7 такой каталог тоже есть в каталоге C:\Users, но он оставлен исключительно из соображений совместимости. Вместо этого используется папка Public (Общие). Однако в этой папке вы не найдете улья Ntuser.dat (он был в каталоге All Users), поскольку Windows не загружает этот файл.

23.4. Типы профилей

В Windows существует три типа профилей:

- *Локальный* (local) — создается при создании новой учетной записи, точнее, когда пользователь в первый раз входит в систему. Локальные профили хранятся на жестком диске локального компьютера и не следуют за пользователем от одного компьютера к другому, если пользователь перемещается в пределах сети.
- *Блуждающий* (roaming) — такой профиль следует за пользователем при его перемещении по сети. С какого бы компьютера сети пользователь бы ни зашел, его настройки всегда будут загружены. Такой профиль обычно хранится на контроллере домена. Изменения в профиле сохраняются при выходе пользователя из сети.
- *Неизменяемый* (mandatory) — похож на блуждающий профиль, он загружается с контроллера домена, когда пользователь входит в сеть с любого компьютера, даже не входящего в сеть; однако изменения, произведенные

в профиле, сбрасываются при выходе из сети. Неизменяемые профили уже теряют свое значение и используются только для обратной совместимости.

В следующих разделах мы поговорим об отличиях этих типов профилей более подробно.

25.4.1. Локальные профили

Рассмотрим, как Windows работает с локальными профилями. При входе пользователя в систему Windows первым делом проверяет, есть ли в разделе реестра `ProfileList` локальный профиль пользователя. Если профиль уже создан, Windows использует его. Если же профиль не существует, действия компьютера зависят от того, является ли он членом домена или нет. В первом случае (компьютер — член домена) операционная система выполняет поиск *профиля по умолчанию* в сетевом ресурсе `NETLOGON` контроллера домена. Если профиль найден, то операционная система использует его, выполняя копирование NETLOGON\Default User в %*Systemdrive*%\Documents and Settings\<*имя пользователя*> (Windows XP) или %*Systemdrive*%\Users\<*имя пользователя*> (Windows Vista и Windows 7).

В противном случае (если компьютер не является членом домена или если профиль по умолчанию в NETLOGON не найден) Windows использует локальный профиль по умолчанию. При этом содержимое каталога %*Systemdrive*%\Documents and Settings\Default User копируется в %*Systemdrive*%\Documents and Settings\<*имя пользователя*> (Windows XP) или %*Systemdrive*%\Users\<*имя пользователя*> (Windows Vista и Windows 7). После этого производится загрузка куста профиля Ntuser.dat в HKU\<*SID*> и связывание HKU\<*SID*> с ключом `HKCU`.

При выходе пользователя из системы все изменения, выполненные в локальном профиле, сохраняются на жестком диске локального компьютера и не копируются в сеть. Таким же образом производится выгрузка куста реестра.

23.4.2. Блуждающие профили

С блуждающими профилями Windows работает немного иначе. При входе пользователя в систему обычно проверяется существование его локального профиля (в разделе `ProfileList`). Если локальный профиль существует, то он объединяется со своей сетевой версией (которая хранится на контроллере домена).

Если же локальная версия профиля не существует, Windows производит поиск на ресурсе NETLOGON, расположенном на контроллере домена, в папке Default User. Если она существует, то операционная система копирует ее в каталог %*Systemdrive*%\Documents and Settings\<*имя пользователя*> (Windows XP) или %*Systemdrive*%\Users\<*Username*> (Windows Vista/7). Если профиль по умолчанию не найден, содержимое каталога %*Systemdrive*%\Documents and Settings\Default User

(Windows XP) или %*Systemdrive*%\Users\Default (Windows Vista/7) копируется в каталог %*Systemdrive*%\Documents and Settings\<*имя пользователя*> (Windows XP) или %*Systemdrive*%\Users\<*username*> (Windows Vista/7).

В обоих случаях Windows загружает файл куста в `HKU\<SID>`, а затем связывает `HKU\<SID>` с ключом `HKCU`.

При выходе пользователя из системы производится сохранение профиля пользователя с последующим копированием его в сеть (в то место, которое указано администратором при конфигурировании контроллера домена).

Создание блуждающих профилей выполняется на контроллере домена, который обычно работает под управлением Microsoft Windows 2003 (или 2000) Server. Настройку таких профилей мы рассматривать не будем, поскольку это выходит за рамки данной книги. Если вам это интересно, следует прочитать одну из книг, посвященную Active Directory или Windows 2003 Server — в ней вы найдете всю интересующую информацию по данной теме.

23.5. Удаление профиля пользователя в Windows 7

Для удаления профиля пользователя перейдите в раздел реестра `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList`. Перейдите в подраздел с длинным именем, например, `S-1-5-21-1482476501-448539723-839522115-1003`.

В этом разделе параметр `ProfileImagePath` (рис. 23.4) содержит название каталога пользователя. Если вы хотите полностью удалить профиль пользователя, то вам нужно удалить как его личный подраздел реестра (`S-1-5-21-1482476501-448539723-839522115-1003`), так и домашний каталог.

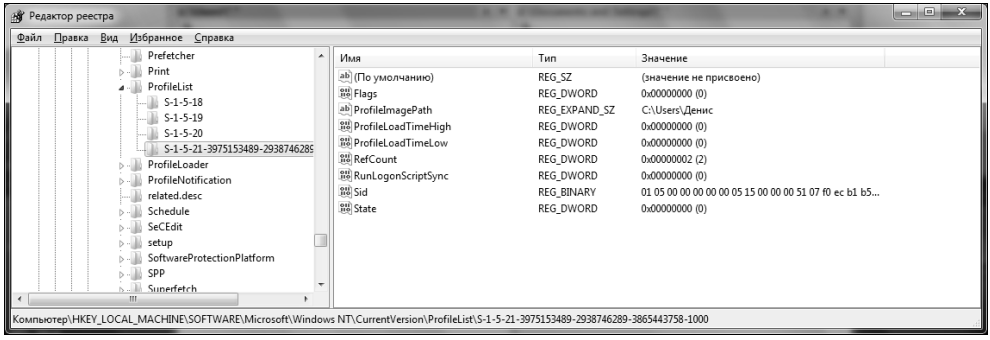
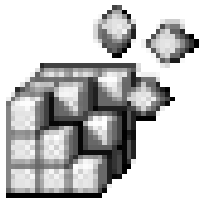


Рис. 23.4. Информация о профиле пользователя

ГЛАВА 24



Управление Windows Installer

24.1. Что такое Windows Installer

Windows Installer, как можно догадаться и по названию, управляет установкой и удалением приложений. Как вы знаете, почти все приложения инсталлируются при помощи отдельной программы, которая обычно имеет название setup.exe (или install.exe), а некоторые, более современные, используют Windows Installer. В последнем случае все файлы приложения (кроме разделяемых библиотек, которые, возможно, уже имеются на вашем компьютере) вместе с инструкциями (правилами) по установке помещаются в один пакет Windows Installer — файл с расширением .msi. Windows Installer устанавливает приложение в соответствии с инструкциями, находящимися в MSI-пакете.

Нужно отметить, что Windows Installer — это не просто компонент Windows, это служба, которой можно управлять через консоль управления services.msc.

Кроме установки программ, Windows Installer выполняет другие функции, но в этой книге все возможности Windows Installer мы рассматривать не будем, а сосредоточимся лишь на взаимодействии Windows Installer с реестром. Если вам нужна дополнительная информация, вы ее можете получить по адресу:

http://msdn.microsoft.com/en-us/library/cc185688%28VS.85%29.aspx

24.2. Управление Windows Installer из командной строки

Наверное, вы заметили, что в окне **Установка и удаление программ** (Add/Remove Programs) возле некоторых программ есть кнопка **Изменить** (Change). При ее нажатии появляется окно, подобное приведенному на

рис. 24.1, позволяющее изменить (Modify) или восстановить (Repair) программу. Изменение необходимо, если вы хотите установить обновление или, наоборот, удалить некоторые компоненты программы, а восстановление нужно, если некоторые файлы повреждены и их нужно восстановить из MSI-пакета.

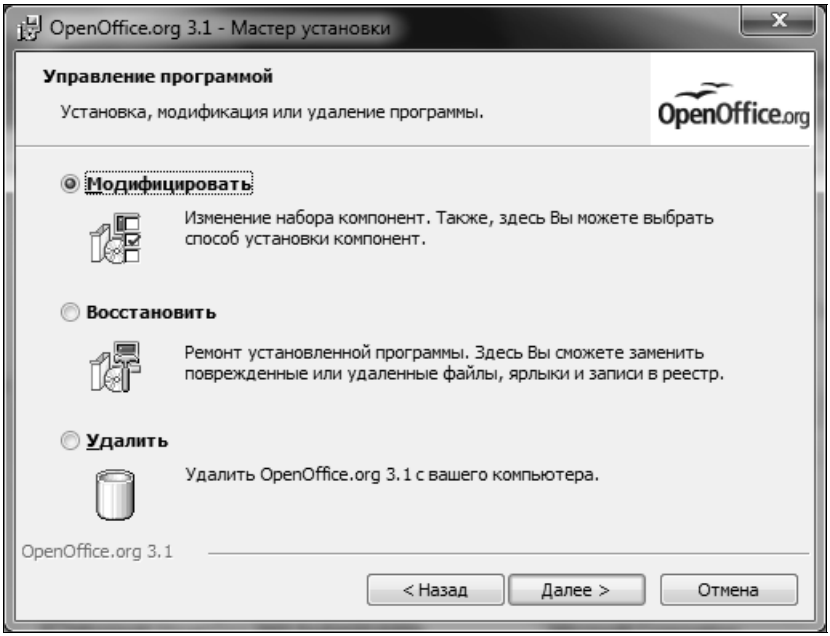


Рис. 24.1. Изменение или восстановление программы

Некоторые программы открыто не предоставляют возможности изменения компонентов или восстановления, но, тем не менее, такая возможность существует. Для этого нужно использовать программу msiexec. Вот несколько полезных команд, которые следует, как и обычно в таких случаях, запускать из командной строки с правами администратора:

```
msiexec /fu пакет
msiexec /fm пакет
msiexec /fmu пакет
```

Первая команда используется для восстановления настроек пользователя (`u` — сокращение от `user`); вторая — настроек компьютера (`m` — `machine`), а третья восстанавливает настройки и компьютера, и пользователя. *Пакет* — это MSI-пакет, из которого была установлена программа. Учтите, что, давая команду, необходимо указывать полный путь к пакету.

Примечание

Хотите попробовать приведенные выше команды в действии? Установите любую программу, найдите в реестре ее настройки и удалите их. Затем выполните одну из только что описанных команд — настройки будут восстановлены.

Другие параметры msiexec приведены в табл. 24.1. Общий синтаксис вызова msiexec следующий:

```
msiexec /Option <обязательный параметр> [необязательный параметр]
```

Параметры можно комбинировать, например, следующим образом: `msiexec /fmu`.

Таблица 24.1. *Параметры утилиты командной строки msiexec*

Параметр	Описание
`</package	/i> <Product.msi>`	Установка или настройка продукта (пакета)
`/a <Product.msi>`	Установка продукта в сеть
`/j<u|m> <Product.msi> [/t <список преобразований>] [/g <код языка>]`	Объявление о продукте: `m` — всем пользователям; `u` — текущему пользователю
`</uninstall	/x> <Product.msi	Код_продукта>`	Удаление продукта
`/quiet`	Неинтерактивный режим, нет взаимодействия с пользователем
`/passive`	Автоматический режим — только указатель хода выполнения
`/q[n|b|r|f]`	Выбор уровня интерфейса пользователя: `n` — без интерфейса `b` — основной интерфейс `r` — сокращенный интерфейс `f` — полный интерфейс (по умолчанию)
`/norestart`	Не перезапускать после завершения установки
`/promptrestart`	Запрашивать перезапуск при необходимости
`/forcerestart`	Всегда перезапускать компьютер после завершения установки
`/l[i|w|e|a|r|u|c|m|o|p|v|x|+|!|*] <файл_журнала>`	Параметры ведения журнала: `i` — сообщения о состоянии `w` — сообщения об устранимых ошибках `e` — все сообщения об ошибках `a` — запуски действий

Таблица 24.1 *(продолжение)*

Параметр	Описание
	r — записи, специфические для действий u — запросы пользователя c — начальные параметры интерфейса пользователя m — сведения о выходе из-за недостатка памяти или неустранимой ошибки o — сообщения о недостатке места на диске p — свойства терминала v — подробный вывод x — дополнительные отладочные сведения + — добавление в существующий файл журнала ! — сбрасывание каждой строки в журнал * — заносить в журнал все сведения, кроме параметров v и x
/update <Update1.msp>[;Update2.msp]	Применение обновлений
/uninstall <*Код_Guid_обновления*>[;Update2.msp] /package <*Product*.msi | *код_продукта*>	Удаление обновлений продукта
/f[p|e|c|m|s|o|d|a|u|v] <*Product*.msi | *код_продукта*>	Параметры восстановления: P — устанавливает отсутствующие файлы (используется для восстановления удаленных файлов программы) o — похож на p, но устанавливает не только отсутствующие файлы, но и файлы более ранней версии e — похож на p, но переустанавливает еще и те файлы, которые имеют текущую версию d — переустанавливает отсутствующие файлы или те, у которых версия отличается от текущей c — используется для переустановки отсутствующих или поврежденных файлов. Поврежденным считается файл, контрольная сумма которого не совпадает с контрольной суммой исходного файла в пакете

Таблица 24.1 *(окончание)*

Параметр	Описание
	a — переустанавливает все файлы (при этом Windows Installer "не смотрит" ни на версию файла, ни на контрольную сумму) u — перезаписывает пользовательские параметры в разделах HKCU и HKU m — перезаписывает параметры в разделах HKLM и HKCR s — используется для переустановки ярлыков v — восстанавливает локальный кэш пакета

Спрашивается, зачем восстанавливать параметры приложения с помощью Windows Installer, если можно воспользоваться системой восстановления, что более удобно? Дело в том, что с помощью Windows Installer вы можете восстановить параметры и изменившиеся/поврежденные файлы только нужной вам программы, а служба восстановления влияет на все программы. Допустим, два дня назад вы установили две программы, выполнили их настройку и работали с ними. В результате сбоя первая программа была повреждена. Если вы сделаете откат на два дня, то восстановите первую программу, но при этом потеряете настройки второй. В этом случае лучше использовать Windows Installer для восстановления только первой программы.

24.3. Управление Windows Installer с помощью политик

Политики Windows Installer находятся в разделе **Административные шаблоны** (Administrative Templates) | **Компоненты Windows** (Windows Components) | **Установщик Windows** (Windows Installer). Такие подразделы есть как в разделе **Конфигурация компьютера** (Computer Configuration), так и в разделе **Конфигурация пользователя** (User Configuration).

Политики Windows Installer хранятся в разделе реестра `Software\Policies\Microsoft\Windows\Installer`. Напомню, что общесистемные политики хранятся в разделе `HLKM`, а пользовательские — в `HKCU`.

В табл. 24.2 описаны пользовательские политики, хранящиеся в `HKCU\Software\Policies\Microsoft\Windows\Installer`, а в табл. 24.3 — общесистемные.

Таблица 24.2. *Пользовательские политики Windows Installer*

Политика	Описание
Всегда устанавливать с повышенными привилегиями (Always install with elevated privileges)	Указывает, что Windows Installer всегда должен использовать системные права для установки любой программы. При включении данной политики "продвинутые" пользователи могут использовать ее для повышения своих полномочий и доступа к файлам и каталогам с ограниченным доступом. Если политика выключена или не задана, при установке программ система будет следовать разрешениям (полномочиям) текущего пользователя. Данная политика вступает в силу только после включения аналогичной политики в разделе **Конфигурация компьютера**. Соответствующий ей параметр реестра — `AlwaysInstallElevated`
Запретить установки со съемных носителей (Prevent removable media source for any install)	Запрещает пользователям устанавливать приложения со съемных носителей. Идея заключается в том, чтобы пользователи могли устанавливать только те программы, которые находятся в пределах корпоративной сети и доступны на общих ресурсах, предотвращая, таким образом, установку не проверенных и потенциально опасных программ. Что же касается реализации, то она оставляет желать лучшего: пользователю достаточно скопировать MSI-пакет на жесткий диск, и эта политика прекратит свое действие. К тому же данная политика распространяется только на программы, которые устанавливаются с помощью Windows Installer. Соответствующий параметр реестра — `DisableMedia`
Запретить откат (Prohibit rollback)	Запрещает установщику создавать файлы, необходимые для восстановления исходного состояния после прерванной или неудачной установки. Используйте эту политику с осторожностью. Если ее включить, то установщик не сможет сделать откат в случае неудачной установки. С другой стороны, эта политика позволяет сэкономить место на диске. Соответствующий политике параметр реестра — `DisableRollback`
Порядок поиска (Search order)	Задает порядок поиска установочных файлов. Доступные значения: `m` — съемные носители; `n` — локальная сеть; `u` — Интернет. Значения можно комбинировать, например, `mnu`. Соответствующий политике параметр реестра — `SearchOrder`

Таблица 24.3. *Общесистемные политики Windows Installer*

Политика	Описание
Разрешить обзор источника при повышенных правах (Enable user to browse for source while elevated)	По умолчанию установщик запрещает пользователям производить поиск установочных файлов, если устанавливается программа с повышенными привилегиями (по умолчанию кнопку **Обзор** видят только администраторы). Применение данной политики, напротив, позволяет пользователю это сделать. Параметр `AllowLockdownBrowse`
Разрешить использование носителей при повышенных правах (Enable user to use media source while elevated)	По умолчанию устанавливать пакеты со сменных носителей могут лишь администраторы (см. табл. 24.2), но эта политика разрешает пользователям устанавливать программы со сменных носителей, даже если программы устанавливаются с повышенными привилегиями. Параметр `AllowLockdownMedia`
Разрешить применение пакетов исправлений при установке с повышенными правами (Enable user to patch elevated products)	Разрешает пользователям использовать патчи во время привилегированных установок. По умолчанию такую возможность имеют лишь администраторы. Пакеты исправлений часто являются носителями вирусов, поэтому использовать эту политику следует с осторожностью. Параметр `AllowLockdownPatch`
Всегда устанавливать с повышенными правами (Always install with elevated privileges)	Данная политика была описана в табл. 26.2. Чтобы она вступила в силу, необходимо включить ее как в разделе **Конфигурация компьютера**, так и в разделе **Конфигурация пользователя**. Параметр `AlwaysInstallElevated`
Запретить диспетчер перезапуска (Prohibit use of Restart Manager)	API диспетчера перезапуска позволяет уменьшить или вообще свести до нуля количество перезагрузок системы, необходимых для завершения установки или обновления. Этот параметр управляет взаимодействием инсталлятора Windows с диспетчером перезапуска. Если этот параметр включен, то вы можете использовать параметры в окне "Запретить диспетчер перезапуска" для управления методами определения занятости файла. При включенном диспетчере перезапуска заставляет инсталлятор Windows использовать диспетчер перезапуска для обнаружения занятых файлов и избегать перезагрузки системы, если это возможно. Если параметр выключен или не задан, установщик Windows не будет использовать диспетчер перезапуска. Параметр `DisableAutomaticApplicationShutdown`

Таблица 24.3 *(продолжение)*

Политика	Описание
Удалить диалоговое окно обзора нового источника (Remove browse dialog for new source)	Запрещает пользователям производить поиск установочных файлов при добавлении компонентов к уже установленной программе. Делается это для того, чтобы все программы были установлены из одного источника, санкционированного администратором. В корпоративной среде позволяет повысить надежность системы, поскольку запрещает использование посторонних пакетов, которые могут содержать вирусы. Параметр `DisableBrowse`
Запретить оптимизацию применения пакетов исправлений (Prohibit Flyweight Patching)	Параметр контролирует отключение всех параметров оптимизации пакетов управлений. Если этот параметр включен, установка будет выполняться при отключенных всех параметрах оптимизации пакетов исправлений. Отключение этого параметра ускорит применение пакетов за счет исключения необязательных операций. Параметр `DisableFlyweightPatching`
Отключить ведение журнала с помощью параметров пакета (Disable logging via package settings)	Свойство `MsiLogging` в пакете установки используется для включения автоматического ведения журнала всех операций установки для этого пакета. Данный параметр управляет обработкой этого свойства инсталлятором Windows. Параметр `DisableLoggingFromPackage`
Запретить установщик Windows (Disable Windows Installer)	В зависимости от параметра запрещает или ограничивает возможности установщика Windows: Никогда — использование установщика разрешено; Всегда — использование установщика запрещено, но можно установить старые программы, которые работают в обход установщика Windows; Только для не обслуживаемых программ — разрешает устанавливать только программы, которые были предложены на рабочем столе или опубликованы в разделе **Установка и удаление программ**. Соответствующий параметр — `DisableMSI`
Запретить пакеты исправлений (Prohibit Patching)	Запрещает использовать патчи. Позволяет оградить пользователей от вирусов, которые нередко распространяются в виде патчей. Параметр `DisablePatch`

Таблица 24.3 *(продолжение)*

Политика	Описание
Запретить откат (Prohibit rollback)	См. табл. 24.2. Данная политика, если она установлена, распространяется на всех пользователей, поскольку находится в Конфигурации компьютера. Параметр `DisableRollback` в `HKLM`
Разрешить администраторам установку в сеансе службы удаленных рабочих столов (Allow Admin to install from Remote services session)	Разрешает администраторам терминальных служб удаленно устанавливать программы. Функция довольно привлекательная, особенно на больших предприятиях, где нужно полчаса только для того, чтобы добраться до нужного компьютера. Параметр `EnableAdminTSRemote`
Разрешить пользователям изменять параметры установки (Enable User Control over installs)	Разрешает пользователям изменять параметры установки приложений, которые обычно доступны только администраторам. Параметр `EnableUserControl`
Ведение журнала событий (Logging)	Включает журналирование событий установщика. Файл журнала называется Msi.Log и записывается в каталог %Systemroot%\Temp. Параметр `Logging`
Запретить пользователям, не являющимися администраторами, устанавливать обновления, подписанные изготовителем программы (Prohibit non-Administrators from applying vendor-signed updates)	Параметр определяет, имеют ли право не являющиеся администраторами пользователи устанавливать обновления программ с цифровой подписью изготовителя. Если параметр политики включен, только администраторы или пользователи с административными правами могут устанавливать обновления приложений, использующих установщик Windows. Если параметр политики отключен, то пользователи, не имеющие административных прав, не могут устанавливать неадминистративные обновления. Параметр `DisableLUAPatching`
Запретить удаление обновлений (Prohibit removal of updates)	Параметр определяет, имеют ли право обычные пользователи или администраторы удалять обновления, установленные установщиком Windows. Параметр `DisablePatchUninstall`
Отключить создание контрольных точек восстановления системы (Turn off creation of system Restore checkpoints)	По умолчанию установщик создает контрольные точки перед каждой установкой программы, поэтому, если программа нарушила работоспособность системы, всегда есть возможность вернуть систему в исходное состояние. Эта политика позволяет отключить создание контрольных точек, что сделает невозможным откат назад. Параметр `LimitSystemRestoreCheckpointing`

Таблица 24.3 *(окончание)*

Политика	Описание
Запретить установки пользователям (Prohibit user Installs)	Запрещает пользователям установку программ. Данная политика позволяет настроить желаемое поведение установщика, а именно: • Разрешить установки пользователям — при этом отдается предпочтение пользовательским установкам перед общесистемными; • Скрыть установки для пользователей — предпочтение будет отдано общесистемным установкам. Параметр `DisableUserInstalls`
Задать обязательные правила обновления компонентов (Enforce upgrade component rules)	Параметр заставляет установщик Windows применять обязательные правила обновления компонентов. Это может привести к тому, что некоторые обновления откажутся устанавливать. Параметр `EnforceUpgradeComponentRules`
Максимальный размер кэша базисных файлов (Baseline file cache maximum size)	Задает процент свободного места на дисак, доступного для кэширования базисных файлов установщика Windows. Параметр `MaxPatchCacheSize`
Отключить запрос безопасности IE для сценариев установщика Windows (Disable IE security prompt for Windows Installer scripts)	Позволяет Web-программам устанавливать программы на компьютер без уведомления пользователя. Лучше никогда не включать эту политику! Параметр `SafeForScripting`
Кэшировать файлы преобразования в безопасном месте на рабочей станции (Cache transforms in secure location on workstation)	Сохраняет копии преобразуемых файлов в безопасном месте локального компьютера. Обычно преобразования хранятся в папках профилей пользователей, поэтому преобразования (трансформации) будут следовать за пользователем от одного компьютера к другому. Но пользователи могут модифицировать эти файлы, что нежелательно. Данная политика позволяет изменить это поведение: преобразования будут сохранены в безопасном месте, куда пользователи не имеют доступа (обычно это %*Systemroot*%), и не будут следовать за пользователем по сети. Параметр `TransformSecure`

Нужно отметить, что политики позволяют более удобно управлять установщиком Windows, чем непосредственное изменение реестра программой regedit.

24.4. Максимальная безопасность

Для максимальной безопасности вам нужно установить общесистемные политики следующим образом:

- **Всегда устанавливать с повышенными правами** (Always install with elevated privileges) — не задана;
- **Удалить диалоговое окно обзора нового источника** (Remove browse dialog box for new source) — включена;
- **Разрешить обзор источника при повышенных правах** (Enable user to browse source while elevated) — не задана;
- **Разрешить использование носителей при повышенных правах** (Enable user to use media source while elevated) — не задана;
- **Разрешить применение пакетов исправлений при установке с повышенными правами** (Enable user to patch elevated products) — не задана;
- **Запретить пакеты исправлений** (Prohibit patching) — включена;
- **Разрешить пользователю изменять параметры установки** (Enable user control over installs) — не задана;
- **Отключить запрос безопасности IE для сценариев установщика Windows** (Disable IE secutiry prompt for Windows Installer scripts) — не задана;
- **Кэшировать файлы преобразования в безопасном месте на рабочей станции** (Cache transforms in secure location on workstation) — включена.

Политики пользователя нужно установить так:

- **Всегда производить установку с повышенными правами** (Always install with elevated privileges) — не задана;
- **Запретить установки со съемных носителей** (Prevent removable source media for any install) — включена.

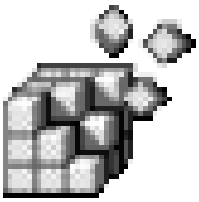
24.5. Создание пакетов Windows Installer

MSI-пакеты обычно создаются для установки приложения. Создание пакетов установщика Windows только для изменения реестра рациональной не назовешь. Для развертывания реестра гораздо удобнее использовать REG- и INF-файлы.

Если вам просто интересно, как же создаются MSI-пакеты, тогда посетите следующую страницу:

http://www.windowsnetworking.com/articles_tutorials/MSI-Packaging-Tools.html

ГЛАВА 25



Клонирование системы с помощью утилиты *sysprep*

25.1. Преимущества и недостатки клонирования

Представьте себе, что у вас есть целый парк компьютеров одинаковой конфигурации. Как правило, организации закупают большую часть компьютерного оборудования одновременно, поэтому высока вероятность того, что конфигурация компьютеров будет одинаковой (одинаковые процессоры, материнские платы и другие аппаратные компоненты).

Установка Windows занимает около 45 минут (операционной системы и драйверов устройств), еще минимум 30 минут нужно для установки необходимых программ (зачастую на установку программ уходит больше времени, чем на установку операционной системы). Возможно, еще полчаса понадобится на настройку системы и установку политик. В итоге получается, что настройка одного компьютера занимает 1 час 45 минут (105 минут). Даже если компьютерный парк небольшой, скажем, 10 компьютеров, на настройку всех компьютеров придется потратить два дня (или один день, если выполнять настройку всего парка "параллельно", что не всегда возможно).

Для ускорения процесса настройки можно использовать клонирование. Вы настраиваете один компьютер (устанавливаете ОС, драйверы и необходимые компьютеры), затем создаете образ системного диска и развертываете его на остальных компьютерах. Развертывание отнимет у вас около 10 минут. Теперь считаем. Пусть мы потратим 1 час 45 минут на настройку первого компьютера, и еще час уйдет на создание образа, зато потом для настройки остальных 9 компьютеров понадобится всего 90 минут, таким образом, настройка всего компьютерного парка отнимет 4 часа и 15 минут. Эффективно?

К тому же, как несложно подсчитать, эффективность клонирования возрастает прямо пропорционально количеству компьютеров в вашей сети.

Клонирование удобно не только в сети предприятия, но и дома. Однажды я попал в ситуацию, когда мне пришлось довольно долго работать в очень нестабильной операционной системе, поскольку в тот момент я не имел возможности потратить 4 часа на переустановку Windows и всех необходимых мне программ. А ведь можно создать образ системного диска сразу же после завершения конфигурирования системы, после чего, потратив на переустановку всего 10–20 минут, вы можете получить "чистую" операционную систему и все нужные вам программы. Конечно, перед развертыванием системы с системного диска будут стерты все имеющиеся на нем данные, поэтому заранее нужно скопировать с него важные для вас файлы и каталоги — Документы (Documents), Рисунки (Images), Избранное (Favorites) и т. д.

25.2. Клонирование в общих чертах

Рассмотрим основные этапы процесса клонирования:

1. Сначала установите Windows.
2. Далее установите все необходимые драйверы. Этот этап следует пропустить, если предназначенные для клонирования компьютеры имеют разную конфигурацию. Также пока не нужно подключать компьютер к домену и настраивать сеть.
3. Затем нужно установить все программы, которые вы хотите включить в образ, например, Microsoft Office, программы для просмотра изображений, видеокодеки и т. д.
4. Следующий шаг — подготовка каталога %*Systemdrive*%\Sysprep. В него нужно скопировать файлы sysprep.exe и setupcl.exe. Кроме того, вам нужно создать файл sysprep.inf и тоже скопировать его в данный каталог (о создании этого файла мы поговорим позже).
5. Запустите sysprep.exe, включите параметр **Mini-Setup**, затем нажмите кнопку **Reseal** (Запечатать компьютер). Sysprep автоматически завершит работу вашего компьютера.
6. Последний этап — создание образа системного диска.

> ***Примечание***
>
> Утилита sysprep входит в состав пакета Deployment Tools, который вы можете найти на компакт-диске Windows XP. В Windows 7 и Windows Vista программа sysprep уже включена в состав операционной системы, и вы найдете ее в каталоге %*windir*%\system32\sysprep\sysprep.exe. Если вы все еще используете Windows XP, загрузить sysprep можно по следующим адресам:

http://www.microsoft.com/downloads/details.aspx?FamilyId=3BD8561F-77AC-4400-A0C1-FE871C461A89&displaylang=en (для Windows 7, Vista и XP SP2 и SP3);

http://www.microsoft.com/downloads/details.aspx?displaylang=en&familyid=7A83123D-507B-4095-9D9D-0A195F7B5F69 (для XP Service Pack 1);

http://www.microsoft.com/downloads/details.aspx?displaylang=ru&FamilyID=7a83123d-507b-4095-9d9d-0a195f7b5f69 (для XP Service Pack 1, русская версия);

http://www.microsoft.com/downloads/details.aspx?FamilyId=3E90DC91-AC56-4665-949B-BEDA3080E0F6&displaylang=en (для XP Service Pack 2);

http://www.microsoft.com/downloads/details.aspx?displaylang=ru&FamilyID=3e90dc91-ac56-4665-949b-beda3080e0f6 (для XP Service Pack 2, русская версия).

После создания образа его нужно перенести на другие компьютеры. При включении компьютера будет запущен мастер мини-установки, который проверит конфигурацию компьютера, выведет лицензионное соглашение и запросит информацию о пользователе, настройках сети, региональных настройках и т. д. С помощью sysprep.inf вы можете определить, какие настройки мастер должен пропустить, а какие — отобразить. После завершения работы мастер перезагрузит компьютер. Работа мастера занимает 5–10 минут.

Подробности использования программы мы рассмотрим в следующих разделах.

25.3. Ограничения *sysprep*

Sysprep — очень удобная утилита, но она имеет ряд существенных ограничений:

- конфигурация компьютеров, на которые планируется развертывание системы, должна быть примерно одинаковой. Например, если вы создали образ однопроцессорной системы, то вы не сможете использовать его для развертывания на двухпроцессорной машине;
- у целевых компьютеров должны быть одинаковые типы BIOS. Например, образ исходного компьютера, имеющего ACPI BIOS, не подойдет для компьютера с APM BIOS;
- очевидно, что размер системного диска целевого компьютера должен быть таким же или больше, чем у исходного компьютера;
- и, наконец, самое главное: sysprep не создает образ диска, а только подготавливает систему к клонированию. Для самого клонирования придется воспользоваться продуктами сторонних производителей, а какими именно — мы поговорим в следующих разделах.

25.4. Создание образа: выбор программы

То, что sysprep не умеет создавать образ диска, — главный недостаток этой утилиты. Я готов мириться со всеми остальными, но не с этим. Однако другого выхода нет, поэтому порядок клонирования остается следующим — sysprep подготавливает систему к клонированию, а потом вы с помощью сторонней программы создаете образ диска. Могу порекомендовать следующие программы:

- PowerQuest DeployCenter (**http://www.powerquest.com**);
- Phoenix ImageCast (**http://www.it-infusion.com**);
- Symantec Ghost (**http://www.symantec.com**).

Возможности всех программ по созданию образов примерно одинаковы, но последняя (Ghost) умеет больше, чем просто создавать образы, например, она умеет развертывать образы на удаленных компьютерах, что очень удобно, поскольку не нужно подходить к другому компьютеру для запуска процесса.

25.5. Создание файла *sysprep.inf* (файла ответов)

Файл sysprep.inf используется для автоматизации мастера мини-установки (Mini-Setup Wizard). В этом файле вы можете определить параметры по умолчанию: мастер установки не будет просить пользователя установить параметры, указанные в этом файле (вот поэтому данный файл и называется файлом ответов).

Рассмотрим пример простейшего файла sysprep.inf (листинг 25.1).

Листинг 25.1. Пример простейшего файла sysprep.inf

```
[GuiUnattended]
AdminPassword = пароль_администратора
OemSkipWelcome = 1
TimeZone = 145
[Identification]
DomainAdmin = "DOMAIN\AcctAddID"
DomainAdminPassword = пароль домена
JoinDomain = "DOMAIN"
[Unattended]
OemSkipEula = Yes
[UserData]
FullName = "Название подразделения компании"
OrgName = "Название компании"
```

Как видите, sysprep.inf — самый обычный INF-файл, самые полезные разделы которого описаны в табл. 25.1. В каждом разделе могут быть параметры, которые для большего удобства также представлены в табл. 25.1.

Таблица 25.1. *Некоторые разделы и параметры разделов файла sysprep.inf*

Раздел	Параметр	Описание раздела/параметра

`Display`		Содержит настройки монитора. Пример раздела:
		`[Display]`
		`BitsPerPel = 16`
		`Vrefresh = 85`
		`Xresolution = 1024`
		`Yresolution = 768`

	`BitsPerPel`	Задает глубину цвета (bits per pixel). Заметьте, что указывается не количество цветов, а степень, в которую нужно возвести 2, чтобы получить искомое количество цветов, например, если вы укажете в качестве значения этого параметра значение 8, то это будет соответствовать 256 цветам (2^8), значение 16 соответствует 65 536 цветам
	`Vrefresh`	Частота обновления экрана в герцах. Оптимальное для зрения значение — 85
	`Xresolution`	Количество точек по горизонтали. Оптимальное разрешение (его поддерживают все современные мониторы) — 1024×768
	`Yresolution`	Количество точек по вертикали

`GuiRunOnce`		Используется для формирования раздела реестра `RunOnce` целевого компьютера. Параметры указываются следующим образом:
		`Название_программы = путь`
		Пример раздела:
		`Program = c:\my\prog.exe`

`GuiUnattended`		Настраивает графический интерфейс пользователя. Пример раздела:
		`[GuiUnattended]`
		`AdminPassword = sNN53htY`
		`AutoLogon = Yes`
		`AutoLogonCount = 3`
		`EncryptedAdminPassword = Yes`
		`OEMDuplicatorString = "Моя утилита"`
		`OEMSkipRegional = 1`
		`OEMSkipWelcome = 1`
		`TimeZone = 145`

Таблица 25.1 *(продолжение)*

Раздел	Параметр	Описание раздела/параметра
	AdminPassword	Задает пароль администратора. Максимальная длина пароля — 127 символов
	AutoLogon	Если для этого параметра указано значение Yes, то при *первой* перезагрузке будет обеспечен автоматический вход администратора (что очень удобно). При входе в систему будет использован пароль, указанный с помощью параметра AdminPassword
	AutoLogonCount	Количество попыток автоматического входа с использованием пароля, указанного в AdminPassword
	EncryptedAdmin Password	Определяет, будет ли зашифрован пароль администратора. Предпочтительнее использовать значение Yes
	OEMDuplicatorString	Задает название программы-дубликатора. Обычно этот параметр не используется
	OEMSkipRegional	Если установлено значение 1, то мастер установки пропустит установку региональных параметров и языка
	OEMSkipWelcome	Если установлено значение 1, то мастер установки пропустит страницу приветствия (она на самом деле не нужна)
	TimeZone	Часовой пояс: 145 — Москва (GMT +03:00); 125 — Киев (GMT +02:00). С остальными часовыми поясами вы можете ознакомиться в файле ref.chm
Homenet		Задает параметры домашней сети
Identification		Содержит параметры идентификации компьютера
	DomainAdmin	Администратор домена (см. листинг 25.1)
	DomainAdminPassword	Пароль администратора домена
	JoinDomain	Имя домена
	JoinWorkgroup	Имя рабочей группы
InternetServer		Содержит параметры Web-сервера. Обычно не задаются (представляю себе парк компьютеров, на каждом из которых запущено по Web-серверу)

Таблица 25.1 *(продолжение)*

Раздел	Параметр	Описание раздела/параметра
Networking		В этом разделе нет параметров, но вы можете использовать подразделы этого раздела для настройки различных сетевых служб. Дополнительные подразделы подробно описаны в файле ref.chm
OEMBootFiles		Содержит различные драйверы устройств, необходимые на этапе установки Windows, например, драйверы SCSI. Если у вас есть необходимость в использовании этого раздела, внимательно прочитайте соответствующий раздел файла ref.chm

Proxy		Задает параметры прокси-сервера. Пример раздела:
		`[Proxy]`
		`FTP_Proxy_Server = http://proxy:80`
		`HTTP_Proxy_Server = http://proxy:80`
		`Proxy_Enable = 1`
		`Proxy_Override = <local>`
		`Secure_Proxy_Server = http://proxy:80`
		`Use_Same_Proxy = 1`

	FTP_Proxy_Server	Имя прокси-сервера для FTP
	HTTP_Proxy_Server	Имя прокси-сервера для HTTP
	Proxy_Enable	Если значение параметра равно 1, то подключение к Интернету будет производиться через указанный прокси-сервер
	Proxy_Override	Задает список адресов, разделенных точкой с запятой, для подключения к которым не должен использоваться прокси-сервер
	Use_Same_Proxy	Если значение параметра равно 1, то один и тот же прокси-сервер будет использоваться для всех протоколов
	Secure_Proxy_Server	Прокси-сервер для HTTPS-соединений
Regional Settings		Содержит региональные параметры. Вы можете указать параметры клавиатуры, языка. Для создания комбинаций региональных настроек используется специальная программа, которую можно скачать по адресу: **www.microsoft.com/globaldev/tools/msklc.mspx**
TapiLocation		Задает параметры TAPI (телефонии)
	AreaCode	Код города

Таблица 25.1 *(окончание)*

Раздел	Параметр	Описание раздела/параметра
	CountryCode	Код страны
	Dialing	Тип набора: тоновый (Tone) или пульсовый (Pulse)
Unattended		Позволяет задать различные опции программы установки
	OemSkipEula	Если установить значение Yes, то мастер установки пропустит вывод лицензии
	InstallFilesPath	Задает путь к дистрибутивным файлам в следующем формате: InstallFilesPath = C:\Sysprep\i386
	EnableBigLBA	Включает 48-битный LBA для ATAPI-дисков
UserData		Задает пользовательские параметры
	ComputerName	Имя компьютера
	FullName	Полное имя компьютера
	OrgName	Название организации
	ProductKey	Ключ Windows (должен быть уникален для каждой копии Windows, поэтому его лучше не задавать в sysprep.inf)

Если вам не хочется создавать файл ответов вручную, вы можете создать его с помощью программы setupmgr.exe. Однако данная программа не входит в состав Windows 7. Она включена в состав пакета Windows Automated Installation Kit (WAIK), скачать который можно с сайта Microsoft. Правда, здесь есть одно "но". Скачать этот пакет для Vista могут только пользователи, у которых установлена подлинная версия Windows. Если у вас "пиратка", о WAIK можете забыть (или скачать его с пиратского сайта, но с какого именно я вам не подскажу, поскольку мне это совершенно не интересно). Итак, счастливые обладатели подлинной версии Windows без проблем найдут WAIK на сайте Microsoft (рис. 25.1). Для проверки подлинности Windows нажмите кнопку **Продолжить** (Continue) на странице загрузки WAIK. Сам адрес страницы приводить не стану — уж очень он замысловатый, проще найти его через поисковик. После нажатия кнопки **Продолжить** (Continue) будет загружена утилита GenuineCheck.exe. Запустите ее. Она сообщит вам код, который нужно ввести в поле проверки кода и нажать кнопку **Проверить** (Check). Если ваша копия Windows подлинная, вы увидите страницу загрузки WAIK (рис. 25.2), но вместо кнопки **Продолжить** (Continue) здесь будет присутствовать кнопка

Загрузить (Download), позволяющая загрузить образ WAIK, который потом нужно будет записать на диск, используя встроенные средства записи образов Windows 7 или стороннюю программу, например, Nero.

Я ничего не перепутал — чуть ранее я правильно упомянул о версии WAIK для Vista. Для Windows 7 пока доступна Beta-версия WAIK, которую могут скачать все желающие (правда, интерфейс будет только английский). Скоро появится релиз WAIK, но, сами понимаете, он будет доступен только подлинным пользователям, как и Vista-версия.

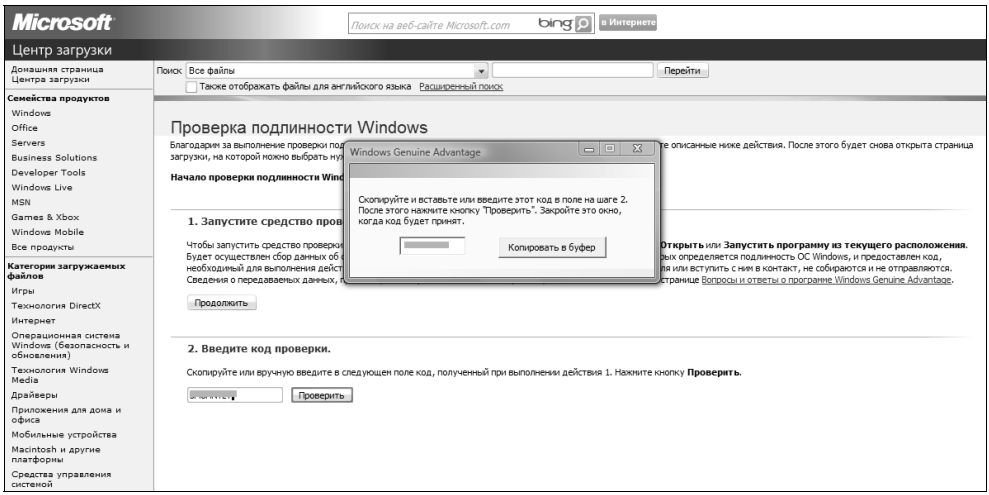


Рис. 25.1. Проверка подлинности Windows

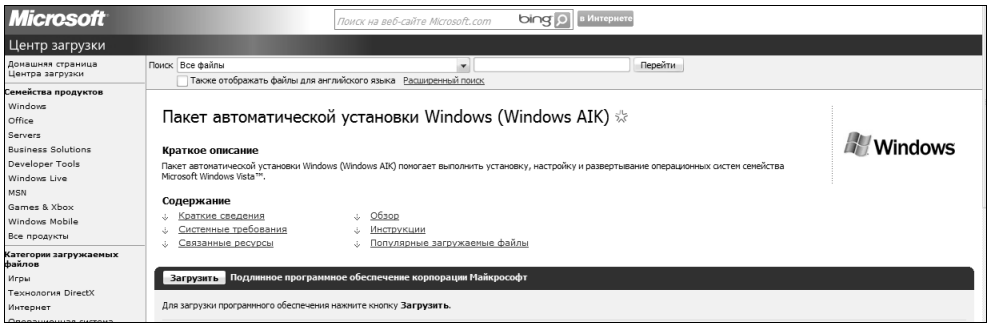


Рис. 25.2. Страница загрузки WAIK

Примечание

Свой код проверки (см. рис. 25.1) по понятным причинам на иллюстрации я затер.

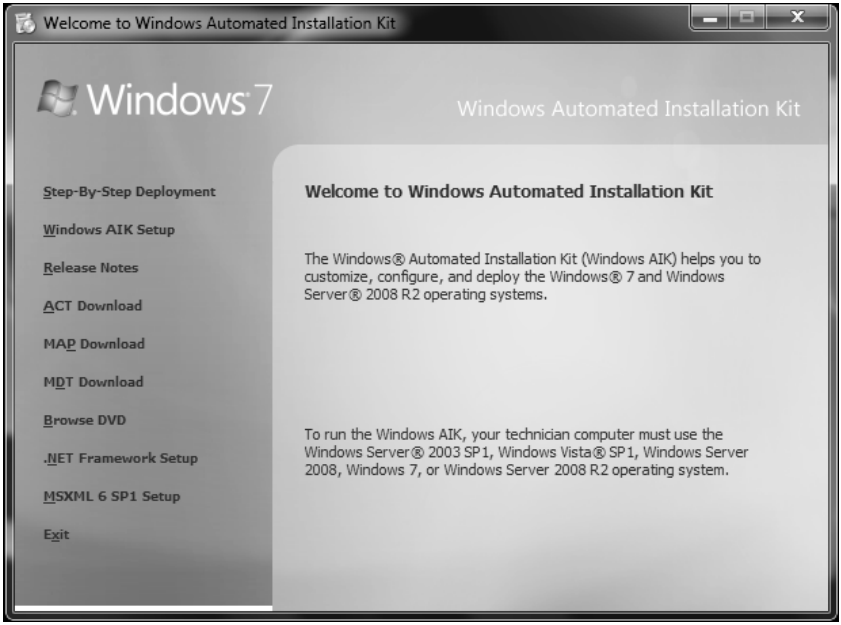


Рис. 25.3. Установка AIK

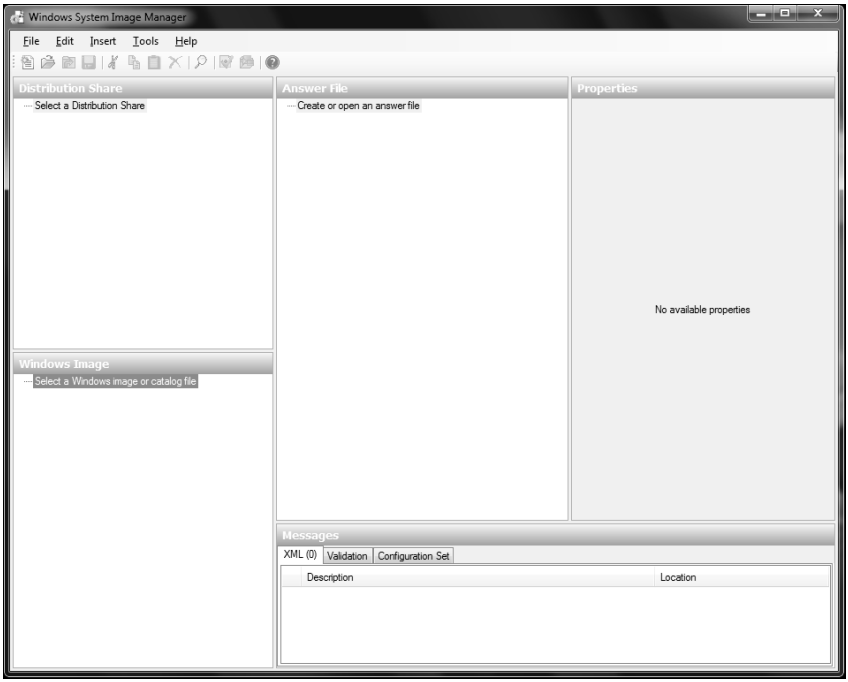


Рис. 25.4. Диспетчер образов

После того как вы скачаете ISO-образ, запишите его на DVD и вставьте записанный диск в привод (рис. 25.3). Выберите команду **Windows AIK Setup**. Установка проходит без проблем, и уже через минуту-две вы сможете запустить Диспетчер образов системы Windows, выбрав из меню **Пуск** (Start) следующие команды: **Все программы** (All Programs) | **Microsoft Windows AIK** | **Windows System Image Manager** (рис. 25.4).

Для создания нового файла ответов выполните команду меню **File** | **New answer file**.

25.6. Параметры программы *sysprep*

При запуске sysprep вы можете использовать параметры, указанные в табл. 25.2.

Таблица 25.2. *Параметры sysprep*

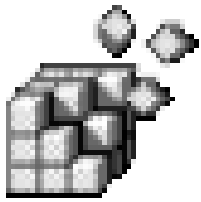
Параметр	Описание
`/audit (-activated)`	Позволяет не сбрасывать информацию об активации вашей копии Windows. Данную опцию нужно использовать, если ваша версия Windows активирована в режиме **Factory**. Перезагружает систему в режиме включенных сетевых подключений. Мастер мини-установки не запускается. Режим **Factory** полезен, когда нужно обновить какой-нибудь драйвер. Когда завершите работу в режиме **Factory**, запустите sysprep в режиме **Reseal** для подготовки компьютера к созданию образа (см. ниже)
`/audit (-audit)`	Перезагружает систему в режим **Factory**, при этом не генерируются новые SID и не обрабатываются элементы в разделе `[OEMRunOnce]` файла winbom.ini. Об этом файле можно прочитать в файле ref.chm
`/clean (-clean)`	Очищает базу данных критически важных устройств. Рекомендуется указывать при вызове sysprep
`/oobe (-mini)`	Настраивает систему на запуск мастера мини-установки
`/noreboot (-noreboot)`	Используется в основном для тестирования, не используйте эту опцию в обычном режиме
`/generalize (-nosidgen)`	В Windows 7 опции `-nosidgen` как таковой нет, вместо нее используется опция `generalize`.
`/reboot (-reboot)`	Обычно используется при тестировании, когда нужно убедиться, что все работает корректно

Таблица 25.2 *(окончание)*

Параметр	Описание
`/generalize (-reseal)`	"Запечатывает" компьютер. Запечатывать компьютер нужно в тот момент, когда уже все готово, и вы собираетесь приступить к созданию образа диска

Примечание

В Windows 7 параметры sysprep отличаются от параметров sysprep в Windows XP, поэтому в табл. 27.2 старые параметры, использующиеся в Windows XP-версии, указаны в скобках.



ГЛАВА 26

Удаленный рабочий стол

26.1. Зачем это нужно?

Наверное, каждому администратору знакома программа Remote Administrator, которая была очень популярна во времена Windows 98 и позволяла управлять клиентскими компьютерами с компьютера администратора сети. Это было очень удобно: например, к вам пришел пользователь и жалуется, что у него что-то работает не так, как ему хотелось бы. Вместо того чтобы идти к нему в кабинет, вы можете "зайти" на его компьютер с помощью программы Remote Administrator, при условии, конечно, что она установлена на компьютере пользователя. Таким образом, можно решить проблему за 5 минут, сэкономив 20 минут только на дороге туда и обратно!

Начиная с Windows 2000, в составе операционной системы появилась встроенная возможность, обеспечивающая аналогичную функциональность. Теперь вы избавлены от необходимости устанавливать программы сторонних разработчиков. В этой главе мы поговорим о том, как использовать удаленный рабочий стол в Windows Vista/7. Кстати, сервер удаленного рабочего стола есть только в версиях Business и Ultimate.

26.2. Активация удаленного рабочего стола

Перед использованием удаленного рабочего стола нужно убедиться, что эта функция включена. В Windows 7 для этого выполните следующую команды: **Пуск** (Start) | **Панель управления** (Control Panel) | **Система и безопасность** (System and Security), как показано на рис. 26.1. Затем щелкните мышью по

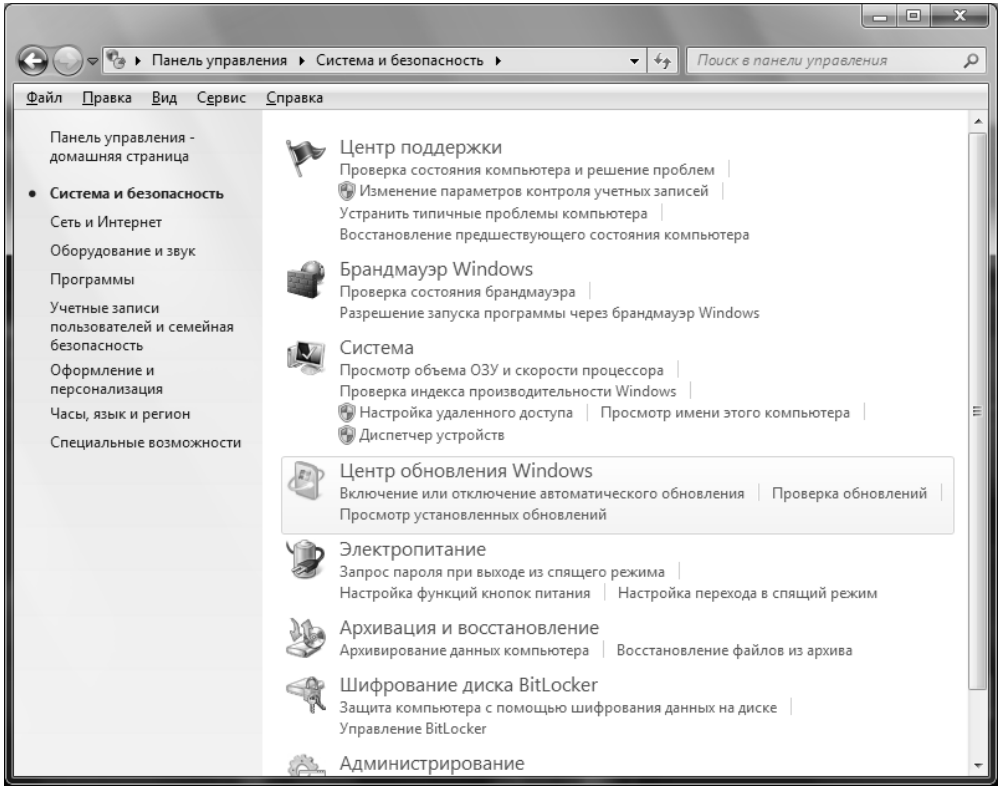


Рис. 26.1. Панель управления, раздел **Система и безопасность**

значку **Система** (System), на экране появится окно, показанное на рис. 26.2. Пройдите по ссылке **Дополнительные параметры системы** (Advanced system settings). В появившемся окне перейдите на вкладку **Удаленный доступ** (Remote), как показано на рис. 26.3. Отключите удаленный помощник — он вам не нужен. Для этой цели выключите параметр **Разрешить подключения удаленного помощника к этому компьютеру** (Allow Remote Assistance connections to this computer). Затем настройте доступ к удаленному рабочему столу, задав опции из группы **Удаленный рабочий стол** (Remote Desktop) в соответствии с вашими потребностями:

- **Не разрешать подключения к этому компьютеру** (Don't allow connections to this computer) — удаленный доступ к рабочему столу запрещен;
- **Разрешать подключения от компьютеров с любой версией удаленного рабочего стола** (Allow connections from computers running any version of Remote Desktop) — разрешить подключения с использованием любых вер-

сий удаленного рабочего стола, менее безопасная опция, но позволяет использовать устаревшие клиенты (Windows 2000, XP);

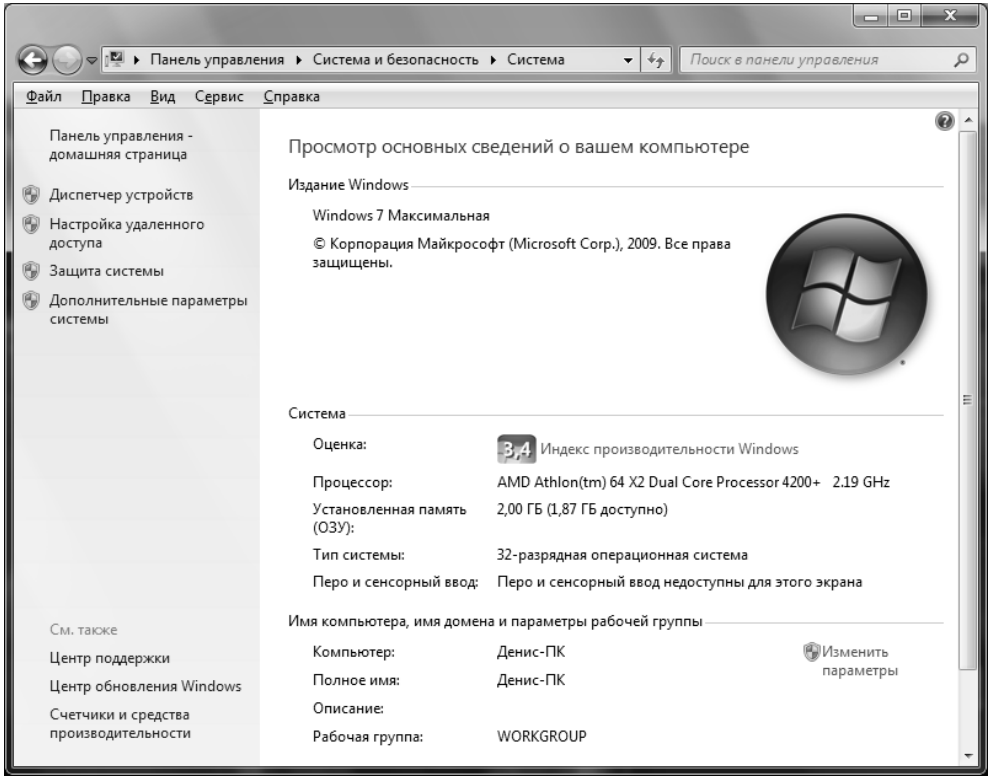


Рис. 26.2. Панель управления, раздел **Система и безопасность** (System and Security), **Система** (System)

- **Разрешить подключаться только с компьютеров, на которых работает удаленный рабочий стол с проверкой подлинности на уровне сети** (Allow connections from computers running Remote Desktop with Network Level Authentication) — будет использовать аутентификацию сетевого уровня для проверки подлинности пользователей. Нажав кнопку **Выбрать пользователей** (Select Users), вы можете выбрать пользователей, которым разрешено подключаться к вашему рабочему столу.

В Windows Vista активировать параметр можно, выбрав на Панели управления следующие опции: **Система** (System) | **Настройка удаленного доступа** (Configure Remote Access).

Удаленный рабочий стол нужно активировать на каждом компьютере, к которому вы хотите подключаться удаленно.

Примечание

Если вы не собираетесь использовать удаленный рабочий стол, то из соображений безопасности рекомендуется выбрать опцию **Не разрешать подключения к этому компьютеру** (Don't allow connections to this computer).

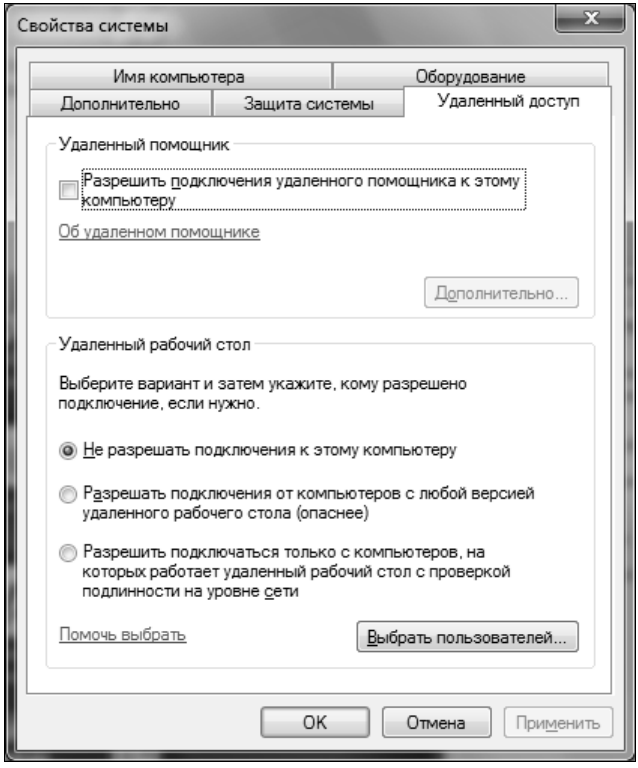


Рис. 26.3. Настройка удаленного доступа к компьютеру

26.3. Клиентская часть

В предыдущем разделе мы рассмотрели, как активировать серверную часть удаленного рабочего стола. В этом поговорим о его клиентской части. Если у вас установлена система Windows 2000/XP/Vista/7, все необходимое программное обеспечение у вас также имеется. Необходимое программное обеспечение для более ранних версий Windows можно загрузить с диска Windows XP Professional.

Для запуска клиентской части выберите из главного меню команды **Пуск** (Start) | **Все программы** (All Programs) | **Стандартные** (Accessories) | **Под-**

ключение к удаленному рабочему столу (Remote Desktop connection). В появившемся окне (рис. 26.4) введите имя компьютера и нажмите кнопку **Подключить** (Connect).

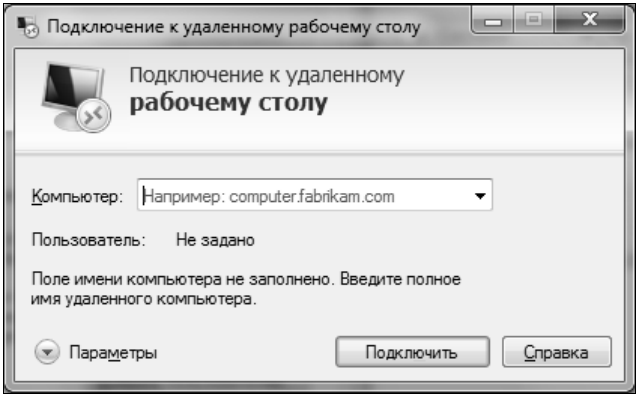


Рис. 26.4. Подключение к удаленному рабочему столу

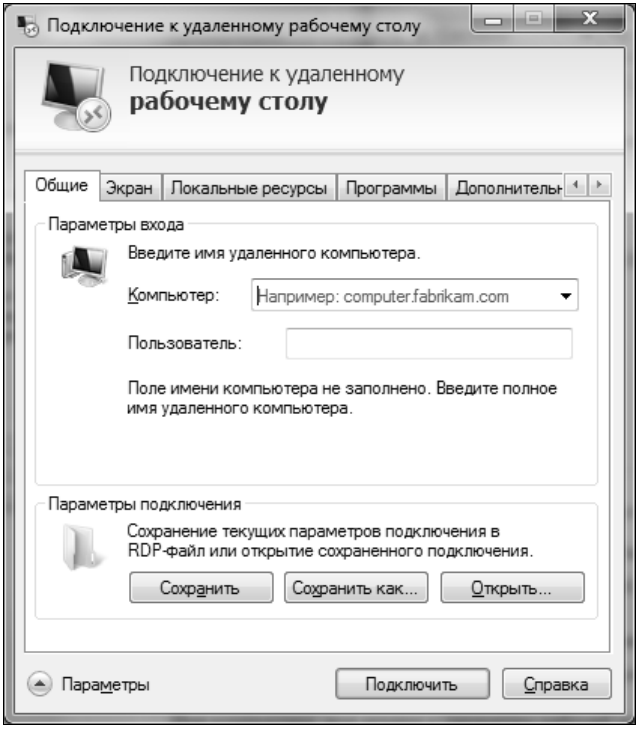


Рис. 26.5. Параметры удаленного доступа к рабочему столу

Для настройки параметров соединения нажмите кнопку **Параметры** (Options) (рис. 26.5). Все параметры удаленного доступа очень просты, поэтому вы разберетесь с ними без моих комментариев.

26.4. Параметры удаленного соединения

Запустите gpedit.msc и перейдите в раздел **Конфигурация компьютера** (Computer Configuration) | **Административные шаблоны** (Administrative Templates) | **Компоненты Windows** (Windows Components) | **Служба удаленных рабочих столов** (Remote Desktop Services) | **Узел сеансов удаленных рабочих столов** (Remote Desktop Session Host), как показано на рис. 26.6. Далее вы можете отредактировать политики удаленного рабочего стола по своему усмотрению. Здесь тоже можно обойтись без дополнительных пояснений, поскольку все они хорошо прокомментированы. Например, в подразделе **Подключения** (Connections) находятся политики соединений. Вы можете включить автоматическое переподключение (Automatic reconnection), установить лимит соединений (Limit number of connections) и т. д.

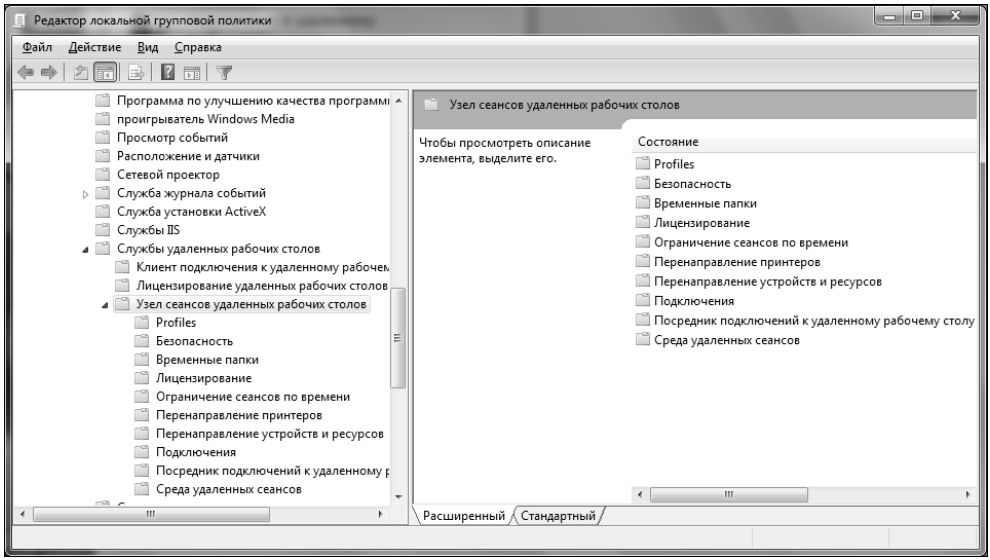


Рис. 26.6. Политики удаленного рабочего стола

Параметры службы удаленных рабочих столов хранятся в разделе реестра `HKLM\System\CurrentControlSet\Control\Terminal Server`. Так, параметр `fDenyTSConnections` определяет, могут ли другие пользователи подключаться к нашему компьютеру:

- `1` — не могут (аналогично значению **Не разрешать подключения к этому компьютеру** (Don't allow remote connections to this computer));
- `0` — к нашему компьютеру могут подключаться удаленные пользователи.

Если вам интересно, какие параметры реестра изменяет та или иная политика, запустите программу мониторинга реестра (тот же regmon), начните мониторинг, измените значение политики и проанализируйте, какие параметры реестра были изменены. Результаты нужно отфильтровать по ветке реестра `HKLM\System\CurrentControlSet\Control\Terminal Server`.

Заключение

Прочитав эту книгу, вы познакомились с одной из самых главных частей операционной системы Windows — ее реестром. По возможности, я старался максимально подробно раскрыть каждый вопрос, связанный с реестром, будь то описание какого-нибудь параметра или политики.

Если у вас есть какие-нибудь вопросы, комментарии или пожелания, свяжитесь со мной, я с радостью вам отвечу.

Предметный указатель

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W

X

А

Б

В

Г

Д

Ж

З

И

К

Л

М

О

П

Р

С

Т

У

Ф

Ч

Ш

Э