

СЕКРЕТЫ, НАСТРОЙКА И ОПТИМИЗАЦИЯ РЕЕСТРА Windows 7



- Аудит и мониторинг
- Резервное копирование
- Восстановление системы
- Тонкая настройка системы и приложений
- Групповые политики
- Тениеры
- Программы для оптимизации реестра

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

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

© Колисниченко Д. Н., 2009
© Оформление, издательство "БХВ-Петербург", 2009

Оглавление

- Введение 1**
- Новые возможности Windows 7 1
 - Производительность 4
 - Новая панель задач 4
 - Расширенное управление окнами..... 5
 - Библиотеки 6
 - Слайд-шоу на рабочем столе 6
 - DirectX 11 8
 - Подключение к большому экрану 8
 - Запись ISO-образов 8
 - Федеративный поиск 8
- Совместимость реестра 9
- ЧАСТЬ I. ДЛЯ ПОЛЬЗОВАТЕЛЕЙ..... 11**
- Глава 1. Основы реестра..... 13**
- 1.1. Что такое реестр и для чего он используется?..... 13
- 1.2. Краткая история реестра 14
- 1.3. Что нужно знать для работы с реестром? 16
 - 1.3.1. Системы счисления 16
 - 1.3.2. Идентификаторы безопасности 18
 - 1.3.3. Глобальные идентификаторы 21
 - 1.3.4. Использование битовых масок 21
 - 1.3.5. Кодировки и реестр..... 23
- 1.4. Структура реестра..... 24
 - 1.4.1. Разделы 25
 - 1.4.2. Параметры 26

1.5. Корневые разделы реестра	29
1.5.1. <i>HKEY_CLASSES_ROOT</i> — корневые классы.....	30
1.5.2. <i>HKEY_CURRENT_USER</i> — параметры текущего пользователя	32
1.5.3. <i>HKEY_LOCAL_MACHINE</i> — глобальные параметры.....	33
1.5.4. <i>HKEY_USERS</i> — пользовательские параметры.....	34
1.5.5. <i>HKEY_CURRENT_CONFIG</i>	35
1.6. Кусты	35
1.6.1. Кусты <i>HKLM</i>	36
1.6.2. Кусты <i>HKU</i>	37

Глава 2. Редактор реестра Registry editor.....39

2.1. Знакомство с редактором реестра.....	39
2.2. Просмотр реестра	41
2.3. Поиск данных в реестре.....	43
2.4. Редактирование реестра и создание новых объектов в реестре.....	44
2.4.1. Создание нового раздела.....	44
2.4.2. Удаление разделов и параметров	45
2.4.3. Создание нового параметра	46
2.4.4. Редактирование параметров.....	46
2.4.5. Копирование имени раздела в буфер обмена.....	47
2.5. Импорт и экспорт разделов реестра	47
2.5.1. Экспорт параметров реестра в REG-файл	48
2.5.2. Экспорт параметров реестра в файл куста	49
2.5.3. Когда и какой способ выбрать?	50
2.6. Печать реестра	50
2.7. Работа с реестром удаленного компьютера	52
2.8. Установка прав доступа к разделам реестра.....	53

Глава 3. Секреты пользовательского интерфейса55

3.1. О чем эта глава?.....	55
3.2. Параметры рабочего стола	56
3.2.1. Отключение рабочего стола.....	56
3.2.2. Вывод версии Windows на рабочем столе	57
3.2.3. Запрет команды <i>Изменение значков рабочего стола</i>	58
3.2.4. Запрет изменения обоев рабочего стола.....	59
3.2.5. Запрет изменения параметров экранной заставки (Screensaver)	59
3.2.6. Добавление значка <i>Корзина</i> в окно <i>Компьютер</i>	60
3.2.7. Добавление новых команд в контекстное меню <i>Компьютер</i>	61
3.2.8. Удаление стрелок с ярлыков.....	62

3.3. Параметры панели задач	62
3.3.1. Скрытие часов на панели задач	62
3.3.2. Параметры области уведомления	62
3.3.2.1. Скрытие неиспользуемых пиктограмм в области уведомлений	62
3.3.2.2. Скрытие всех пиктограмм в области уведомлений	63
3.3.3. Некоторые параметры панели задач	63
3.3.3.1. Автоматическая группировка схожих кнопок	63
3.3.3.2. Изменение уровня группировки кнопок в Windows 7	64
3.3.4. Бесконечное мигание кнопок на панели задач	65
3.4. Меню <i>Пуск</i>	66
3.4.1. Как редактировать расширенное меню <i>Пуск</i> с помощью реестра	66
3.4.2. Другие параметры меню <i>Пуск</i>	68
3.4.2.1. Не отображать имя пользователя в меню <i>Пуск</i>	68
3.4.2.2. Не отображать список часто используемых программ	68
3.4.2.3. Список последних документов	68
3.4.3. Ускорение открытия меню	69
3.5. Включение технологии ClearType — сглаживание шрифтов	69

Глава 4. Параметры Проводника Windows

4.1. О параметрах Проводника	71
4.2. Запуск отдельных процессов Проводника	71
4.3. Отключение уведомления о недостатке свободного пространства	72
4.4. Автоматическая перезагрузка Проводника	73
4.5. Отключение записи состояния окна	73
4.6. Отключение кэширования изображений	74
4.7. Делаем ярлыки привлекательными	74
4.8. Отображение содержимого окна при его перемещении по экрану	75
4.9. Добавления команды удаления содержимого папки	75
4.10. Отключение поиска подходящей программы в Интернете	76
4.11. Изменение области предварительного просмотра в окне открытия файла (только для Vista)	77

Глава 5. Активация Aero в Windows Vista/Windows 7

5.1. Что такое Aero?	81
5.2. Принудительная активация Aero в Windows 7	84
5.3. Активация Aero Glass в Windows Vista	87

Глава 6. Повышение производительности локальной сети и интернет-соединения

6.1. Повышение производительности Интернета	89
---	----

6.2. Повышение производительности локальной сети	91
6.3. Установка способа доступа к общим ресурсам	91
6.4. Другие полезные сетевые настройки	91

Глава 7. Параметры носителей данных 93

7.1. Скрытие дисков	93
7.2. Запрет доступа к дискам	95
7.3. Создание виртуальных дисков средствами Windows	96
7.4. Отключение автозапуска	97
7.4.1. Стандартный способ	97
7.4.2. Новый способ: только для Vista и Windows 7	97
7.5. Windows 7 не распознает мой DVD-привод	97

Глава 8. Системные параметры. Повышение производительности 99

8.1. Повышение производительности.....	99
8.1.1. Ускорение работы с памятью	99
8.1.2. Выгрузка из памяти неиспользуемых DLL.....	100
8.1.3. Автоматическое очищение файла подкачки	100
8.1.4. Повышение производительности системы путем запрета выгрузки драйверов	101
8.1.5. Ускорение завершения работы системы.....	101
8.1.6. Отключение планировщика Windows.....	101
8.1.7. Увеличение производительности NTFS	102
8.1.8. Включить поддержку UDMA-66 на чипсетах Intel.....	103
8.1.9. Отключаем неиспользуемые сервисы.....	103
8.1.9.1. Зачем нужно отключать лишние сервисы?	103
8.1.9.2. Как отключить сервис?.....	104
8.2. Настройка автозапуска программ	106
8.3. Удаление программ из списка установленных (Uninstall своими руками)	108
8.4. Что делать с зависшими программами?.....	109
8.5. Служба SuperFetch.....	110
8.6. Уменьшение фрагментации больших файлов	111
8.7. Выключение автоматического обновления Windows.....	112
8.8. Установка пути к дистрибутиву Windows.....	112
8.9. Установка пути к каталогу <i>Program Files</i>	113
8.10. Настройка службы времени.....	113
8.11. Что делать в случае отказа системы	114
8.12. Исправление ошибки инсталлятора в Windows 7	114
8.13. Комплексная доработка Windows 7	114

Глава 9. Параметры Internet Explorer	117
9.1. Общие параметры IE	117
9.1.1. Автоматическое изменение размера рисунков	117
9.1.2. Отключение фоновых звуков.....	117
9.1.3. Отключение автоматического обновления Internet Explorer	118
9.1.4. Включение функции автозаполнения	118
9.1.5. Запрет автозаполнения форм	118
9.1.6. Запрет автозаполнения паролей	118
9.1.7. Удаление пароля на ограничение доступа к сайтам	118
9.1.8. Изменение стартовой страницы с помощью реестра	119
9.1.9. Скрытие редко используемых страниц в меню Избранное	119
9.1.10. Отключение автоматического дозвола	119
9.1.11. Изменение каталога для загрузки файлов.....	119
9.2. Параметры безопасности	119
9.2.1. Запрет изменения параметров IE.....	119
9.2.2. Отключение отображения вкладок окна настройки IE	120
9.3. Запрет доступа к Интернету. Установка IP-адреса прокси-сервера	120
9.4. Ускорение работы браузеров Internet Explorer 7 и 8	121
9.5. Удаление Internet Explorer из реестра Windows.....	122
 Глава 10. Параметры Windows Media Player	123
10.1. Автоматическая загрузка кодеков из Интернета.....	123
10.2. Отключение автоматического обновления	124
10.3. Удаление списка последних воспроизведенных файлов и URL.....	125
10.4. Изменение заголовка окна проигрывателя	125
10.5. Скрытие компонентов проигрывателя	125
10.6. Запрет изменения скина.....	125
10.7. Включение DVD-функций в Windows Media Player	126
10.8. Включение MP3-кодирования в Windows XP	126
10.9. Отключение вкладки <i>Сеть</i> в Windows XP	127
 Глава 11. Повышение привилегий процессов.....	129
11.1. Зачем это нужно?.....	129
11.2. Два способа повышения привилегий.....	129
11.2.1. Политики	130
11.2.2. Запуск программ от имени другого пользователя	131
11.3. Приоритет: фоновым или активным приложениям	133
 Глава 12. Твикеры	135
12.1. Что такое твикер?	135

12.2. Твикеры для Windows Vista/Windows 7	135
12.2.1. Thoosje Vista Tweaker.....	136
12.2.2. VistaTweaker	136
12.2.3. XdN Tweaker	137
12.2.4. Vista4Experts	138
12.2.5. Stardock TweakVista	138
12.2.6. Windows 7 Manager	140
12.2.7. Ultimate Windows Tweaker v2, a Tweak UI for Windows 7 & Vista	141
12.3. Твикер для Windows XP — XP Tweaker	142

Глава 13. Программы для чистки и оптимизации реестра 145

13.1. Уход за реестром	145
13.2. Программа <i>CleanMyPC Registry Cleaner</i>	145
13.3. Программа <i>CCleaner</i>	152
13.4. Программа <i>WinUtilities Registry Cleaner for Windows 7</i>	153

Глава 14. Программа редактирования реестра из командной строки 155

14.1. Утилита <i>Reg.exe</i>	155
14.2. Параметры программы.....	156
14.3. Резервное копирование реестра с помощью программы <i>reg</i>	159

Глава 15. Создание резервных копий реестра..... 161

15.1. Почему происходят сбои?.....	161
15.2. Защита реестра от неквалифицированного вмешательства пользователей	162
15.2.1. Создание резервных копий непосредственно в реестре	162
15.2.2. Экспорт параметров реестра в REG-файл	164
15.2.3. Экспорт параметров реестра в файл куста	165
15.2.4. Когда и какой способ выбрать?	167
15.3. Несколько советов.....	167

Глава 16. Точки восстановления системы..... 169

16.1. Что это такое?	169
16.2. Типы точек восстановления	172
16.3. Как создать точку восстановления.....	173
16.4. Как восстановить систему	174
16.5. Что делать, если Windows не загружается?	174

ЧАСТЬ II. ДЛЯ АДМИНИСТРАТОРОВ 179**Глава 17. Параметры системы восстановления Windows (Vista и Windows 7)..... 181**

17.1. Как работает система восстановления.....	181
17.2. Настройка системы восстановления с помощью реестра.....	182
17.3. Теневые копии в Windows 7	186
17.3.1. Управление теневыми копиями из командной строки	187
17.3.2. Отключение вкладки <i>Предыдущие версии</i> и задание других параметров теневых копий.....	187

Глава 18. Защита системы с помощью реестра 189

18.1. Общие параметры.....	189
18.1.1. Отключение редактора реестра.....	189
18.1.2. Запрет запуска диспетчера задач	189
18.1.3. Запрет запуска Панели управления	190
18.1.4. Запрет запуска программ.....	190
18.1.5. Запрет запуска командной строки	190
18.1.6. Запрещение изменения меню <i>Пуск</i>	191
18.2. Вход в систему и пароли.....	191
18.2.1. Запрет кэширования пароля для входа в сеть	191
18.2.2. Запрет кэширования интернет-паролей	192
18.2.3. Запрет запоминания пароля сетевого подключения	192
18.2.4. Установка минимальной длины пароля	192
18.2.5. Усложнение пароля.....	193
18.2.6. Вывод сообщения при входе в систему	193
18.2.7. Автоматический вход в систему	194
18.2.8. Требование пароля при выходе из спящего/ждущего режима	194
18.3. Сетевая безопасность	194
18.3.1. Запрет подключения сетевых дисков.....	194
18.3.2. Удаление значка <i>Вся сеть</i> в Windows 2000/XP	195
18.3.3. Запрет просмотра общих ресурсов анонимными пользователями.....	195
18.4. Отключение UAC в Windows Vista и Windows 7	195
18.4.1. Основной способ отключения UAC	195
18.4.2. Альтернативный способ настройки UAC	198
18.4.3. Решение проблемы с гаджетами и UAC в Windows 7	198
18.5. Удаление команды шифрования из контекстного меню в Windows Vista и Windows 7	199

Глава 19. Политики в Windows Vista/Windows 7	201
19.1. Что такое политики	201
19.2. Редактор политик	202
19.3. Расширения групповой политики	205
19.4. Административные шаблоны.....	205
19.5. Расширенные возможности политик в Windows Vista/Windows 7	207
19.5.1. Вычисление скорости сети	207
19.5.2. Несколько локальных GPO	208
19.5.3. ADMX-файлы: новый формат файлов	208
19.6. Практические примеры использования редактора политик.....	210
19.6.1. Отключение диспетчера задач	210
19.6.2. Запрет доступа к Панели управления.....	211
19.6.3. Запрет доступа к апплету <i>Установка и удаление программ</i>	212
19.6.4. Отключение правого щелчка мышью для меню и панелей	212
19.6.5. Запрет завершения работы системы и выхода из системы	213
19.6.6. Отключение окна запуска программ	214
19.6.7. Отключение редактора реестра.....	214
19.7. Применение политик без перезагрузки компьютера	214
Глава 20. Списки доступа (ACL).....	217
20.1. Что такое ACL?	217
20.2. Базовое редактирование ACL.....	218
20.3. Расширенное редактирование ACL	221
20.4. Права доступа по умолчанию.....	223
Глава 21. Аудит и мониторинг реестра.....	225
21.1. Аудит реестра.....	225
21.1.1. Сравнение реестра с помощью <i>WinDiff</i>	225
21.1.2. Аудит реестра с помощью стандартных средств Windows	227
21.2. Мониторинг реестра: программа <i>Regmon</i>	234
21.2.1. Отслеживание обращений к реестру определенного процесса	235
21.2.2. Отслеживание обращений к определенному разделу реестра.....	237
21.2.3. Установка фильтров.....	238
Глава 22. INF- и REG-файлы.....	241
22.1. Автоматизация внесения изменений в реестр	241
22.2. INF-файлы	242
22.2.1. Формат INF-файла.....	242
22.2.2. Добавление новых разделов и параметра реестра	244

22.2.3. Удаление разделов и параметров.....	246
22.2.4. Установка INF-файла	247
22.3. REG-файлы.....	248
Глава 23. Профили пользователей	251
23.1. Зачем используются перемещаемые профили?	251
23.2. Исследуем пользовательские профили	252
23.3. Служебные профили	257
23.4. Типы профилей.....	257
23.4.1. Локальные профили	258
23.4.2. Блуждающие профили	258
23.5. Удаление профиля пользователя в Windows 7	259
Глава 24. Управление Windows Installer	261
24.1. Что такое Windows Installer	261
24.2. Управление Windows Installer из командной строки	261
24.3. Управление Windows Installer с помощью политик	265
24.4. Максимальная безопасность.....	271
24.5. Создание пакетов Windows Installer	271
Глава 25. Клонирование системы с помощью утилиты sysprep	273
25.1. Преимущества и недостатки клонирования.....	273
25.2. Клонирование в общих чертах	274
25.3. Ограничения sysprep	275
25.4. Создание образа: выбор программы.....	276
25.5. Создание файла <i>sysprep.inf</i> (файла ответов)	276
25.6. Параметры программы <i>sysprep</i>	283
Глава 26. Удаленный рабочий стол.....	285
26.1. Зачем это нужно?.....	285
26.2. Активация удаленного рабочего стола.....	285
26.3. Клиентская часть	288
26.4. Параметры удаленного соединения	290
Заключение.....	293
Предметный указатель	295

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 Windows 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:

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

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

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

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).

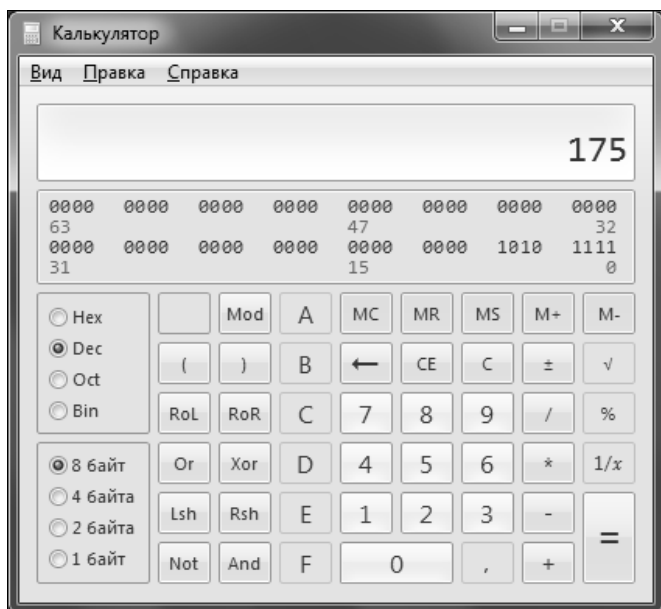


Рис. 1.1. Использование калькулятора для выполнения вычислений в шестнадцатеричной системе

Шестнадцатеричные числа часто записываются так: *0хчисло*. Например, запись *0х77* означает, что число 77 записано в шестнадцатеричной системе. Очевидно, что оно не равно числу 77 в десятичной системе: после преобразования *0х77* в десятичную систему мы получим число 119.

Иногда для указания того, что число записано в шестнадцатеричной системе вместо префикса *0х* 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 *0х00010203*. Если используется порядок "от старшего к младшему", то число будет сохранено в памяти таким образом:

0х00 0х01 0х02 0х03

Однако процессоры фирмы Intel, например, работают с обратным порядком следования байтов, в котором сначала сохраняются младшие байты, а потом — старшие. Следовательно, наше число *0х00010203* будет сохранено в памяти так:

0х03 0х02 0х01 0х00

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](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](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.