Глава 1

Основные сведения о реестре

Данная глава посвящена основам работы с реестром операционной системы (ОС) Windows 7. Если вы уже встречались с реестром предыдущих версий операционной системы и знаете, что такое корневые разделы, файлы кустов, а также редактор реестра regedit.exe, то можете смело переходить к следующей главе. Дело в том, что все эти термины в Windows 7 практически не изменились. А если сравнивать с Windows Vista, то совсем не изменились.

Если же сравнивать с версиями Windows, вышедшими до Windows Vista, то следует обратить внимание на такие моменты:

- добавились новые файлы кустов;
- программа reg.exe поддерживает новые возможности;
- программа regini.exe теперь входит в стандартную поставку операционной системы.

1.1. Что такое реестр

Реестр любой операционной системы семейства Windows представляет собой большую базу данных, которая хранит настройки работы операционной системы и любых дополнительных программ.

Именно для хранения настроек и предназначен реестр. Ведь вы, наверное, замечали, что каждое приложение имеет различные окна, в которых можно настроить параметры его работы. Кроме того, почти каждая программа имеет внутренние настройки, которые нельзя изменить при помощи окон, но которые, тем не менее, влияют на ее работу. Как же приложению хранить такие настройки?

Конечно, для этого можно создавать различные текстовые файлы — раньше (да и сейчас иногда) делали именно так. Однако согласитесь, довольно сложно тонко настроить несколько программ или, тем более, операционную систему, когда настройки хранятся во множестве текстовых файлов, которые к тому же имеют ряд ограничений (например, раньше существовало ограничение на длину файла).

И вот, когда программисты Microsoft это поняли, они задумались над такой базой данных, которая предоставляла бы возможность хранения всех настроек не только операционной системы, но и любых других приложений, которые захотят воспользоваться этой возможностью.

Так появился реестр операционной системы Windows.

Файлы кустов

На уровне файловой системы реестр всех операционных систем семейства Windows реализован в виде набора файлов. Причем количество и названия файлов различаются для семейств Windows 9x и Windows NT. Поскольку семейство операционных систем Windows 9x морально и физически устарело, мы поговорим только о реестре семейства Windows NT — именно к этому семейству операционных систем относится Windows 7.

Файлы, из которых состоит реестр операционной системы Windows 7, называются файлами кустов, просто кустами или, реже, ульями. Каждый файл кустов содержит данные определенной ветви реестра. Часть этих данных, необходимая во время работы операционной системы или запрашиваемая программами, помещается в выгружаемый пул.

Размер файлов кустов кратен 4 Кбайт, так как файлы кустов состоят из блоков, размер которых равен 4 Кбайт.

Файл кустов не имеет никакого расширения. Большинство из этих файлов хранится в каталоге %systemroot%\System32\config.

ПРИМЕЧАНИЕ

%systemroot% — переменная среды (о них читайте далее в книге), которая указывает на папку Windows, в которой хранятся стандартные файлы и библиотеки операционной системы. Например, в вашей системе это может быть папка C:\Windows.

Как правило, помимо файла куста в каталоге можно найти файл с расширением LOG, имеющий точно такое же название, что и файл куста. Такие файлы содержат описание изменений, которые произошли в реестре операционной системы, но еще не были помещены в файлы куста. Файлы с расширением LOG называют регистрационными кустами.

Данные регистрационного куста сохраняются в файле куста с интервалом не менее пяти секунд.

Минимальный интервал сохранения данных регистрационного куста в файле куста можно изменить при помощи параметра REG_DWORD-типа RegistryLazyFlushInterval, расположенного в ветви реестра HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Configuration Manager.

Список всех ульев, которые были загружены в оперативную память при запуске операционной системы, можно найти, как это ни странно, непосредственно

в реестре. Для этого достаточно взглянуть на параметры строкового типа, расположенные в ветви HKLM\SYSTEM\CurrentControlSet\Control\hivelist (рис. 1.1).

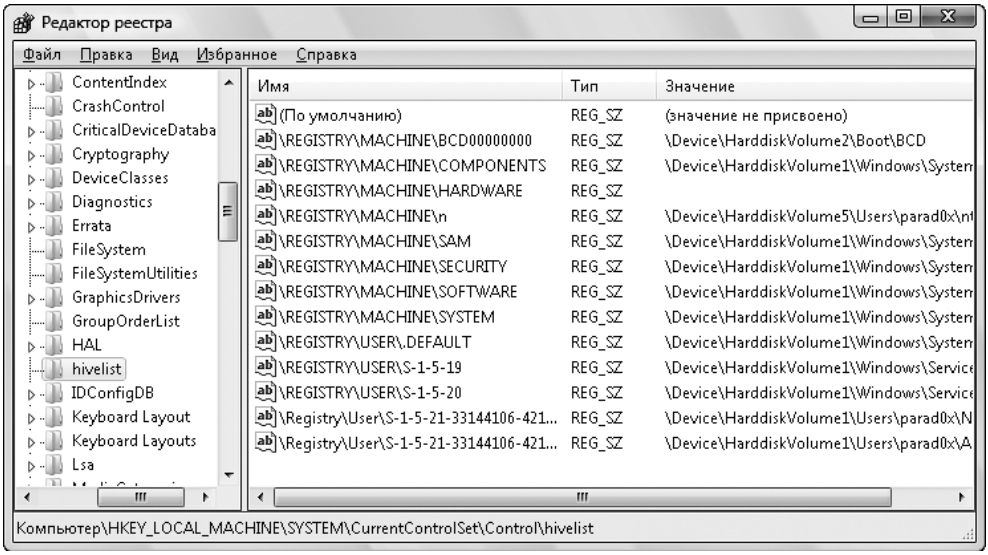

Рис. 1.1. Загруженные файлы кустов

Названия этих параметров определяют ветвь реестра, в которую был загружен соответствующий куст, а их значения задают путь к файлу кустов и его имя.

Рассмотрим подробнее все кусты, которые были загружены операционной системой.

BCD

Каталог: «буква активного диска»:\Boot[1].

Расположен в том разделе диска, на котором находятся файлы, используемые при загрузке операционной системы. Если вы устанавливали Windows 7 как вторую ОС, то, скорее всего, активным будет раздел, на котором установлена первая ОС.

Данный куст содержит ветвь реестра HKLM\BCD00000000. Эта ветвь хранит описание загрузочного меню, отображаемого при включении компьютера для выбора операционной системы, которая будет загружена.

Кроме того, в каталоге %systemroot%\System32\config существует куст с шаблоном данной ветви реестра. Он называется BCD-Template.

[1] По умолчанию для данного каталога установлен атрибут Скрытый.

COMPONENTS

Каталог: %systemroot%\System32\config.

Этот куст включает в себя ветвь реестра HKLM\COMPONENTS. Содержимое данной ветви реестра представляет собой список всех компонентов, из которых состоит операционная система Windows 7. Эти компоненты перечислены в диалоге Компоненты Windows (программа OptionalFeatures.exe).

В Windows 7 данный куст реестра не загружается автоматически.

HARDWARE

Каталог: не существует.

Этот куст определяет содержимое ветви HKLM\HARDWARE. Данная ветвь реестра содержит описание компьютерного оборудования, которое было обнаружено при загрузке компьютера.

Фактически данного куста не существует — ветвь создается на этапе загрузки компьютера и хранится в оперативной памяти на протяжении всего сеанса работы операционной системы. Однако ссылка на него до сих пор осталась в ветви реестра HKLM\SYSTEM\CurrentControlSet\Control\hivelist.

SAM

Каталог: %systemroot%\System32\config.

Куст хранит ветвь реестра HKLM\SAM. Ее содержимое представляет собой базу данных SAM (Security Access Manager), включающую в себя пароли учетных записей пользователей, групп, их права доступа и другую конфиденциальную информацию.

Поскольку содержимое данной ветви реестра представляет огромную ценность для ОС Windows, оно дублируется в ветви реестра HKLM\SECURITY\SAM.

SECURITY

Каталог: %systemroot%\System32\config.

Этот куст хранит ветвь реестра HKLM\SECURITY. Содержимое данной ветви реестра представляет собой еще одну часть базы менеджера безопасности SAM.

По умолчанию содержимое данной ветви реестра разрешено просматривать только учетной записи локальной системы (SYSTEM). Однако администратор может изменить права на просмотр этой ветви реестра.

SOFTWARE

Каталог: %systemroot%\System32\config.

Куст хранит ветвь реестра HKLM\SOFTWARE. В ней содержатся:

- настройки сторонних и стандартных программ ОС Windows;
- сведения о зарегистрированных в системе расширениях файлов и ActiveX-объектов;
- настройки компонентов ОС Windows;
- настройки интерфейса самой ОС Windows;
- содержимое корневого раздела реестра HKEY_CLASSES_ROOT.

SYSTEM

Каталог: %systemroot%\System32\config.

Данный куст хранит ветвь реестра HKLM\SYSTEM. Содержимое данной ветви определяет настройки аппаратных профилей компьютера, служб и драйверов, зарегистрированных в операционной системе, а также важные параметры работы самой операционной системы.

DEFAULT

Каталог: %systemroot%\System32\config.

Этот куст хранит ветвь реестра HKEY_USERS\.DEFAULT. Содержимое данной ветви реестра определяет настройки, используемые при создании нового профиля (при первом входе нового пользователя в систему). Эта ветвь также включает в себя информацию, которую использует Windows для построения интерфейса до входа какого-либо пользователя в систему (например, в диалоге приветствия).

NTUSER.DAT

Данный куст реестра хранится в профиле пользователей и определяет содержимое ветви реестра HKEY_USERS\«SID учетной записи пользователя». Он содержит всю информацию о настройках конкретного пользователя, параметрах установленного программного обеспечения, а также о настройках интерфейса пользователя.

Если внимательно посмотреть содержимое ветви системного реестра HKLM\SYSTEM\CurrentControlSet\Control\hivelist, то можно заметить, что в реестр загружается сразу несколько файлов NTUSER.DAT. Количество загружаемых в реестр файлов NTUSER.DAT определяется количеством профилей, которые были загружены опера-

ционной системой (с точки зрения реестра NTUSER.DAT как раз и является профилем пользователя).

Например, по умолчанию загружаются следующие профили.

- **Профиль пользователя** — для него загружается файл NTUSER.DAT каталога %userprofile%.
- **Профиль учетной записи локальной службы** — для него загружается файл NTUSER.DAT каталога %systemroot%\ServiceProfiles\LocalService. Данная учетная запись используется для запуска служб операционной системы, которым не нужна поддержка сети. В этом кусте хранится ветвь реестра HKEY_USERS\S-1-5-19.
- **Профиль учетной записи сетевой службы** — загружается файл NTUSER.DAT каталога %systemroot%\ServiceProfiles\NetworkService. Данная учетная запись применяется для запуска служб операционной системы, которым по каким-то причинам необходим доступ к сети. В этом кусте хранится ветвь реестра HKEY_USERS\S-1-5-20.

В реестр также могут загружаться профили других пользователей, если какие-либо службы работают от имени этих пользователей. Кроме того, в реестр может загружаться профиль определенного пользователя, если вы запускаете программу от его имени. Например, при помощи программы командной строки runas.exe.

UsrClass.dat

Куст хранится в каталоге %userprofile%\AppData\Local\Microsoft\Windows. Он включает в себя ветвь реестра HKEY_USERS\«SID учетной записи пользователя»_Classes. Данная ветвь реестра содержит перечень расширений файлов, которые были зарегистрированы конкретно для данного пользователя. Она дополняет корневой раздел HKEY_CLASSES_ROOT и содержит точно те же параметры, что и ветвь реестра HKCU\Software\Classes.

Корневые разделы и ветви реестра

Как было сказано выше, каждый файл куста содержит определенную ветвь реестра. Но что же представляет собой ветвь реестра?

Основные термины

Во избежание путаницы и для облегчения работы с реестром программисты Microsoft создали его в виде древовидной структуры, которая состоит из подразделов и параметров.