Работа с реестром Windows

Реестр Windows (системный реестр)

- это иерархическая (древовидная) база данных, содержащая записи, определяющие параметры и настройки операционных систем Microsoft Windows.

Реестр в том виде, как он выглядит при просмотре редактором реестра, формируется из данных, источниками которых являются файлы реестра и информация об оборудовании, собираемая в процессе загрузки. В описании файлов реестра на английском языке используется термин "Hive". В документации от Microsoft этот термин переводится как "Куст".

Файлы реестра создаются в процессе установки операционной системы и хранятся в папке

%SystemRoot%\system32\config

(обычно C:\windows\system32\config).

Для операционных систем Windows это файлы с именами:

default

sam

security

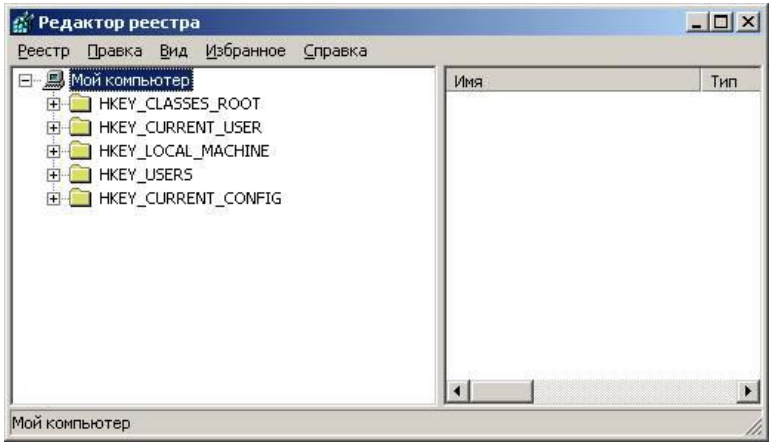
software

system

Место расположения файлов реестра в любой версии Windows можно просмотреть с помощью редактора реестра. В разделе ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\hivelist*** *хранится информация о всех кустах, включая пользовательские профили, со ссылками на их расположение в файловой системе Windows.*

В процессе загрузки система получает монопольный доступ к файлам реестра и, поэтому, их невозможно открыть для просмотра, скопировать, удалить или переименовать обычным образом. Для работы с содержимым системного реестра используется специальное программное обеспечение - редакторы реестра (REGEDIT.EXE, REGEDT32.EXE), являющиеся стандартными компонентами операционной системы. Для запуска редактора реестра можно использовать меню кнопки "Пуск"- "Выполнить" -

После старта редактора, в левой части основного окна вы видите список ***корневых разделов (root keys)*** реестра. Каждый корневой раздел может включать в себя ***вложенные разделы (subkeys)*** и ***параметры (value entries) или ключи реестра.***



Основное назначение корневых разделов:

1. **HKEY_CLASSES_ROOT (Общепринятое сокращенное обозначение HKCR)** - Ассоциации между приложениями и расширениями файлов и информацию о зарегистрированных объектах COM и ActiveX.

Основное назначение корневых разделов:

2. **HKEY_CURRENT_USER (HKCU)**- Настройки для текущего пользователя (рабочий стол, личные папки, настройки приложений). Этот раздел представляет собой ссылку на раздел HKEY_USERS\Идентификатор пользователя (SID).

SID - это уникальный номер, идентифицирующий учетную запись пользователя, группы или компьютера. Он присваивается учетной записи при создании каждого нового пользователя системы. Внутренние процессы Windows обращаются к учетным записям по их кодам SID, а не по именам пользователей или групп. Если удалить, а затем снова создать учетную запись с тем же самым именем пользователя, то предоставленные прежней учетной записи права и разрешения не сохранятся для новой учетной записи, так как их коды безопасности будут разными. Аббревиатура SID образована от Security ID.

Основное назначение корневых разделов:

3. **HKEY_LOCAL_MACHINE (HKLM)** - в данном разделе реестра хранятся глобальные аппаратные и программные настройки системы - записи для системных служб, драйверов, наборов управляющих параметров, общие настройки программного обеспечения, применимые ко **всем пользователям**. Это самая большая и самая важная часть реестра. Здесь сосредоточены основные параметры операционной системы, оборудования, программного обеспечения.

Основное назначение корневых разделов:

4. **HKEY_USERS(HKU)** - индивидуальные настройки среды для каждого пользователя системы (пользовательские профили) и профиль по умолчанию для вновь создаваемых пользователей.

Основное назначение корневых разделов:

5. **HKEY_CURRENT_CONFIG (HKCC)** - конфигурация для текущего аппаратного профиля. Обычно профиль один единственный, но имеется возможность создания нескольких с использованием "Панель управления" - "Система" - "Оборудование"- "Профили оборудования".

На самом деле HKCC не является полноценным разделом реестра, а всего лишь ссылкой на подраздел из HKLM HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\CurrentControlSet\Hardware Profiles\Current

Параметры или ключи реестра имеют **имена**, представленные в обычном текстовом виде и **значения**, которые хранятся в виде стандартизированных записей определенного типа.

Допустимые типы данных реестра:

REG_BINARY - двоичный параметр. Большинство сведений об аппаратных компонентах хранится в виде двоичных данных и выводится в редакторе реестра в шестнадцатеричном формате.

REG_DWORD - двойное слово. Данные представлены в виде значения, длина которого составляет 4 байта (32-разрядное целое). Этот тип данных используется для хранения параметров драйверов устройств и служб. Значение отображается в окне редактора реестра в двоичном, шестнадцатеричном или десятичном формате. Эквивалентами типа DWORD являются DWORD_LITTLE_ENDIAN (самый младший байт хранится в памяти в первом числе) и REG_DWORD_BIG_ENDIAN (самый младший байт хранится в памяти в последнем числе).

Допустимые типы данных реестра:

REG_QWORD - Данные, представленные в виде 64-разрядного целого. Начиная с Windows 2000, такие данные отображаются в окне редактора реестра в виде двоичного параметра.

REG_SZ - строковый параметр.

REG_EXPAND_SZ - Расширяемая строка данных. Многострочный параметр. Многострочный текст. Этот тип, как правило, имеют списки и другие записи в формате, удобном для чтения. Записи разделяются пробелами, запятыми или другими символами

Допустимые типы данных реестра:

REG_RESOURCE_LIST - Двоичный параметр. Последовательность вложенных массивов. Служит для хранения списка ресурсов, которые используются драйвером устройства или управляемым им физическим устройством. Обнаруженные данные система сохраняет в разделе \ResourceMap. В окне редактора реестра эти данные отображаются в виде двоичного параметра в шестнадцатеричном формате.

Допустимые типы данных реестра:

REG_RESOURCE_REQUIREMENTS_LIST - двоичный параметр. Последовательность вложенных массивов. Служит для хранения списка драйверов аппаратных ресурсов, которые могут быть использованы определенным драйвером устройства или управляемым им физическим устройством. Часть этого списка система записывает в раздел \ResourceMap. Данные определяются системой. В окне редактора реестра они отображаются в виде двоичного параметра в шестнадцатеричном формате.

Допустимые типы данных реестра:

REG_FULL_RESOURCE_DESCRIPTOR - двоичный параметр. Последовательность вложенных массивов. Служит для хранения списка ресурсов, которые используются физическим устройством. Обнаруженные данные система сохраняет в разделе \HardwareDescription. В окне редактора реестра эти данные отображаются в виде двоичного параметра в

Допустимые типы данных реестра:

REG_NONE - Данные, не имеющие определенного типа. Такие данные записываются в реестр системой или приложением. В окне редактора реестра отображаются в виде двоичного параметра в шестнадцатеричном формате.

REG_LINK - Символическая ссылка в формате Юникод.

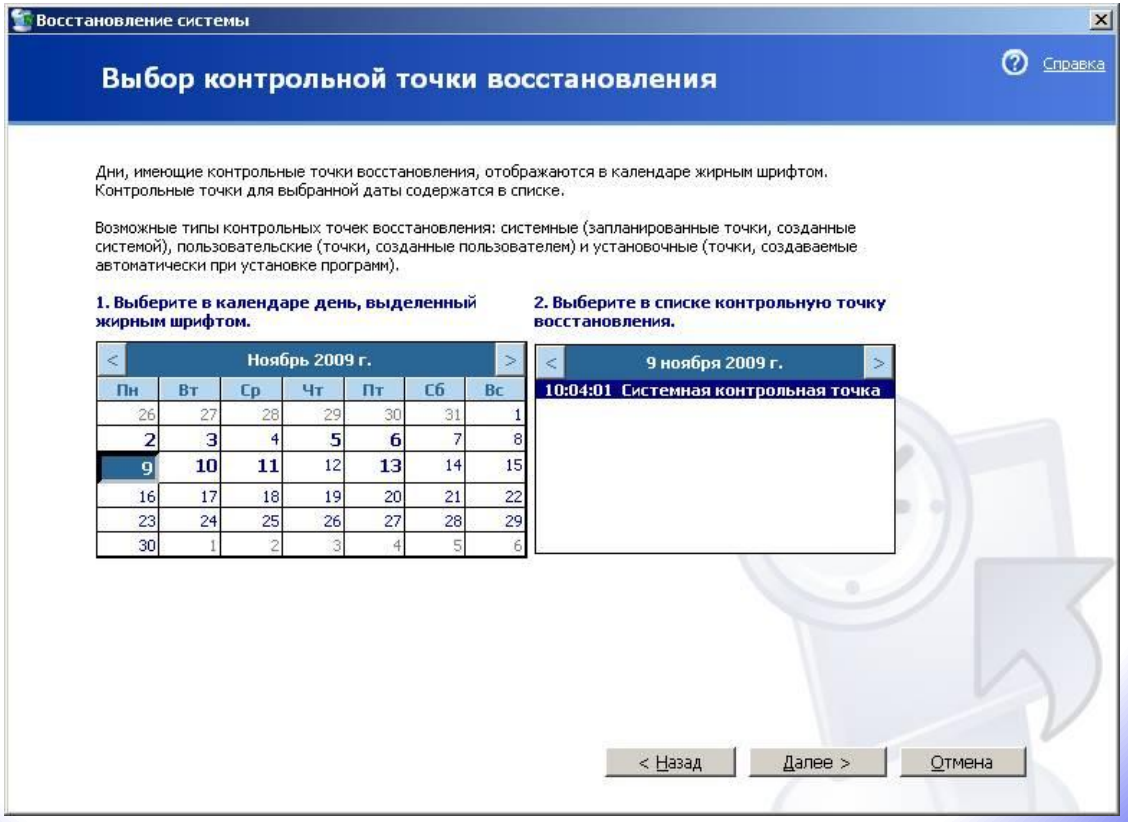
При добавлении новых параметров в реестр, необходимо задавать не только имя и значение, а также правильный тип данных.

Возможности конкретного пользователя при работе с данными реестра определяются правами его учетной записи.

При просмотре данных реестра в среде Windows XP, 2 подраздела с именами SAM и SECURITY, не отображаются, и доступ к ним разрешен только для локальной системной учетной записью (Local System Account), под которой обычно выполняются системные службы (system services). Обычно, учетные записи пользователей и даже администраторов, таких прав не имеют, и редактор реестра, запущенный от их имени, не отображает содержимое разделов SAM и SECURITY. Для доступа к ним нужно, чтобы regedit был запущен от имени учетной записи с правами Local System

Сохранение и восстановление реестра

1. Использование точек восстановления (Restore Points)



Сохранение и восстановление реестра

2. Использование утилиты для работы с реестром из командной строки REG.EXE

Запускается из командной строки.

Для резервного копирования реестра используется REG.EXE SAVE, для восстановления - REG.EXE RESTORE

Синтаксис REG SAVE и REG RESTORE одинаков и вполне понятен из справки

Сохранение и восстановление реестра

3. **Ручное копирование файлов реестра.**
   В случае повреждения файла system, можно воспользоваться, например, сохраненным с помощью команды **REG SAVE** файлом system.hiv, скопировав его в папку реестра и переименовав в system.
   Для Windows 7 – скопировать файл **system** из папки **\windows\system32\config\RegBack** в папку **\windows\system32\config**

Сохранение и восстановление реестра

4. **Использование режима экспорта-импорта реестра.**
   Данный способ не является в полном смысле слова способом полного восстановления реестра и более подходит для случаев, когда нужно сохранить и затем восстановить определенную его часть. Редактор реестра позволяет делать экспорт как всего реестра, так и отдельных разделов в файл с расширением ***reg*** Импорт полученного при экспорте reg-файла, позволяет восстановить реестр. Щелкаете на "Реестр"--> "Экспорт (Импорт) файла реестра". Импорт также можно выполнить двойным щелчком по ярлыку reg-файла.

Драйверы и службы

- Информация о драйверах и системных службах (сервисах) находится в разделе **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services**
  Каждому драйверу или сервису соответствует свой раздел. Например, "atapi" - для драйвера стандартного IDE контроллера жестких дисков, "DNScache" - для службы "DNS клиент"

Назначение основных ключей:

- **DisplayName** - выводимое имя - то что вы видите в качестве осмысленного названия при использовании, например, элементов панели управления.
- **Group** - название группы, к которой относится драйвер, например - "Видеоадаптеры"

Назначение основных ключей:

- **ErrorControl** - режим обработки ошибок.
  0 - игнорировать (Ignore) при ошибке загрузки или инициализации драйвера не выдается сообщение об ошибке и система продолжает работу.
  1 - нормальный (Normal) режим обработки ошибки. Работа системы продолжается после вывода сообщения об ошибке. Параметры ErrorControl для большинства драйверов устройств и системных служб равна 1.
  2 - особый (Severe) режим. Используется для обеспечения загрузки последней удачной конфигурации (LastKnownGood).
  3 - критическая (Critical) ошибка. Процесс загрузки останавливается, и выводится сообщение о сбое.

Назначение основных ключей:

- **ImagePath** путь и имя исполняемого драйвера. Файлы драйверов обычно имеют расширение .sys и располагаются в папке \Windows\System32\DRIVERS\. Файлы сервисов - обычно .exe и располагаются в \Windows\System32\.

Назначение основных ключей:

- **Start** управление загрузкой и инициализацией. Определяет, на каком этапе загрузки системы производится загрузка и инициализация данного драйвера или службы. Значения Start:
  0 - BOOT - драйвер загружается загрузчиком системы.
  1 - SYSTEM - драйвер загружается в процессе инициализации ядра.
  2 - AUTO - служба запускается автоматически при загрузке системы.
  3 - MANUAL - служба запускается вручную.
  4 - DISABLE - драйвер или сервис отключен.

Назначение основных ключей:

Загрузка драйверов и запуск служб с параметрами Start от 0 до 2 выполняются до регистрации пользователя в системе. Для отключения драйвера или службы достаточно установить значение параметра **Start** равным **4**. Отключение драйверов и служб через редактирование этого ключа реестра - довольно опасная операция. Если вы случайно или по незнанию отключите драйвер или сервис, без запуска которых невозможна загрузка или функционирование операционной системы, то получите ее аварийное завершение (чаще всего - синий экран смерти Blue Screen Of Death или сокращенно - BSOD).