СТРУКТУРА РЕЕСТРА

Системный реестр – регистрационная база данных, хранящая различные настройки ОС и приложений. В более ранних версиях Windows все настройки (настройки конфигурации) сохранялись в информационных файлах (INI-файлах), точно так же как и в большинстве Windows-приложений. Однако Windows изменилась и теперь эти файлы не используются операционной системой, т.к. существует реестр, который представляет всю иерархию, необходимую для управления такой сложной операционной системой (рис.1).

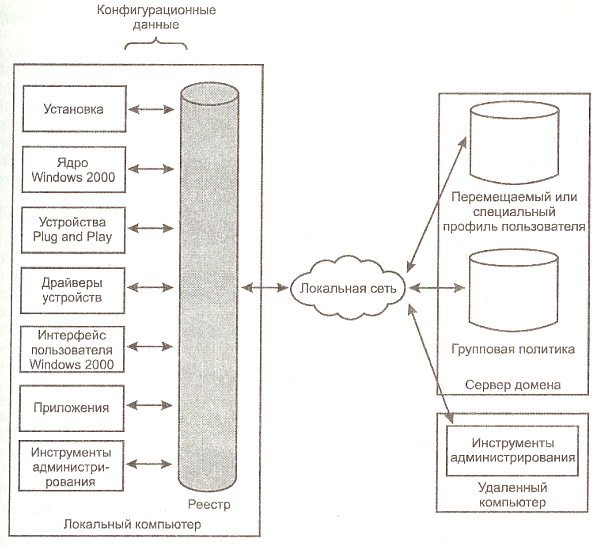


Рис.1. Реестр использует многие компоненты Windows

Изначально реестр был предназначен только для хранения сведений об объектах OLE (Object Linking and Embedding — связь и внедрение объектов) и сопоставлений приложений расширениям имен файлов, однако позже его структура и границы использования расширились.

Достоинства реестра.

1. Системный реестр обеспечивает также работу в сети и дает отдельным пользователям возможность сохранять выбранные ими глобальные параметры, благодаря чему в приложениях появляется возможность специальной настройки пользовательского интерфейса для конкретного пользователя. Данные системного реестра могут храниться централизовано и импортироваться в системный реестр рабочей станции во время регистрации пользователя в системе. Совершенно аналогично, системный администратор имеет удаленный доступ к системным реестрам рабочих станций для разрешения возникших конфликтов.

2. Используя системный реестр, можно связать определенные действия командного процессора (в частности, open и print) с соответствующими типами документов. А когда пользователь выполняет щелчок правой кнопкой мыши на пиктограмме документа в проводнике Windows Explorer, то в этом случае появляется контекстное меню, в котором перечислены определенные программные действия.

3. Возможность OLE-регистрации, поддержки локализованных версий приложений, применение сетевых протоколов и связывания, а также поддержка автоматической настройки приложений.

Формат отображения данных в системном реестре весьма похож на то, как папки и документы отображаются в проводнике Windows Explorer. Отчасти это связано с тем, что структура системного реестра подобна структуре каталогов (рис.2).

Реестр хранится в бинарном (двоичном) виде, поэтому для ручной работы с ним необходима специальная программа — редактор системного реестра (regedit). Один из способов исследования содержимого системного реестра связан с применением программы REGEDIT, утилиты компании Microsoft, которая обеспечивает возможность изменения содержимого системного реестра, а также соединения с системными реестрами других компьютеров.

|  |
| --- |
|  |
| Рис.2. Структура реестра |

Если прибегнуть к терминологии, используемой в системном реестре, то ЭКВИВАЛЕНТОМ ПАПКИ ИЛИ КАТАЛОГА здесь является КЛЮЧ или РАЗДЕЛ (KEY), а ДОКУМЕНТУ ИЛИ ФАЙЛУ соответствуют ПАРАМЕТР (VALUE). Разделы могут содержать как вложенные разделы (sub keys), так и параметры (рис.3). На верхнем уровне этой иерархии находятся корневые разделы (root keys).

|  |
| --- |
|  |
| Рис.3 Подразделы и параметры подобны папкам и файлам |

Каждый ключ может содержать как ключи более низкого уровня, так и конечные элементы данных. При необходимости приложение открывает ключ и использует данные, сохраненные в нем. Ключи, которые содержатся в других ключах, называются подключами данного ключа.

На рис.4 показана взаимосвязь между ключами и значениями в системном реестре.

В системных реестрах Windows используется обобщенная древовидная структура. Это означает, что в приложениях, написанных для разных версий Windows , может вполне допускаться тот факт, что данные хранятся в общих местах в зависимости от конкретного типа.

# Рис.4. Взаимосвязь между отдельными компонентами системного реестра

Ключ

Значение

Подключ1

Подключ2

Значение

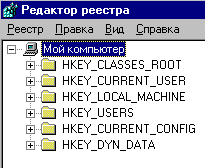
Значение

Значение

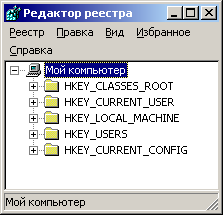
Значение

Подключ

На рис.5 показан верхний уровень системного реестра Windows, а в табл.1 перечислены корневые ветви системного реестра, а также приведено их назначение и взаимосвязь с другими ветвями.



**Windows 9x**



**Windows 2k\XP**

Рис. 5. Верхний уровень системного реестра

Таблица 1 Корневые разделы системного реестра

| № п/п | Раздел (аббревиатуры) | Описание |
| --- | --- | --- |
|  | HKEY\_CLASSES\_ROOT (HKCR) | Этот раздел содержит определения типов документов, связей с файлами и интерфейса командного процессора.  В Windows NT/9x этот ключ является составной частью ключа HKLM.  В Windows XP информация о регистрации класса хранится в обоих ключах HKEY\_LOCAL\_MACHINE и HKCU. При этом ключ HKCR объединяет содержимое указанных ключей в единой папке |
|  | HKEY\_CURRENT\_USER (HKCU) | С помощью этого ключа осуществляется доступ к пользовательским конфигурациям, программному обеспечению. Устанавливает связь с ключом HKEY\_USERS, который соответствует параметрам настройки текущего пользователя. Для стандартных пользователей, у которых отсутсвуют особые параметры настройки используются параметры настройки пользователя типа .Default. |
|  | HKEY\_LOCAL\_MACHINE (HKLM) | Хранит аппаратные конфигурации, сетевые протоколы и классы программного обеспечения |
|  | HKEY\_USERS (HKU) | Используется для хранения выбранных пользователями глобальных параметров, а также параметров настройки рабочего стола. При этом выбранные пользователями глобальные параметры должны хранится в подключе Software подключа каждого пользователя, содержащегося в ключе HKEY\_USERS. |
|  | HKEY\_CURRENT\_CONFIG (HKCC) | Этот ключ устанавливает связь с ключом отображения, входящим в состав подключа выбранной конфигурации config, содержащегося в ключе HKLM |
|  | HKEY\_DYN\_DATA (HKDD) | Используется только в Windows 9x. Здесь хранятся динамические данные о состоянии различных устройств, установленных на компьютере пользователя. |
|  | HKEY\_PERFORMANCE\_DATA (HKPD) | Используется только в Windows 2000. Аналогичен ключу HKEY\_DYN\_DATA, который используется в Windows 9x. |

Рассмотрим соответствующие разделы более детально.

1. HKEY\_CLASSES\_ROOT

Приложение Windows должно использовать системный реестр для хранения в разделе HKEY\_CLASSES\_ROOT данных следующих классов:

* Типы документов. Это различные типы документов, которыми манипулирует конкретное приложение.
* Идентификатор класс. OLE. Это класс OLE, который определяется конкретным приложением. В процессе установки данного приложения он должен быть зарегистрирован с помощью OLE.
* Имена команд OLE. Это протокол OLE. Каждое имя команды описывает действие, которое может выполнить объект. Например, MPLAYER позволяет воспроизводить звуковой файл формата .WAV.
* Протоколы командного процессора. Это действия, которые могут быть вызваны командным процессором. Возможные варианты выбора действий отображаются в контекстных меню, выводимых на экран при выполнении пользователем щелчка правой кнопкой мыши на пиктограмме документа.
* Пиктограмма, которая показывается для отображения документа. В этом случае должны быть предоставлены две пиктограммы — большая и малая. А использоваться будет та из них, которой пользователь отдаст наибольшее предпочтение.

При рассмотрении этой ветви следует особое внимание обратить на ключи командного процессора, содержащие три следующих подключа:

* + open – содержит команду, используемую для открытия (или запуска) документа;
  + print – содержит команду, которая отправляет документ на печать;
  + printto – содержит специальный интерфейс, который обеспечивает возможность передачи документа на принтер путем перетаскивания.

У каждого из этих подключей имеется подключ под названием command. В качестве ключа командного процессора может быть зарегистрировано любое число имен команд. Эти имена команд отображаются в контекстом меню, которое появляется всякий раз, когда пользователь выполняет щелчок правой кнопкой мыши на пиктограмме документа.

1. HKEY\_CURRENT\_USER

Раздел HKEY\_CURRENT\_USER содержит множество настроек программного обеспечения, в которых хранится информация о конфигурации рабочего стола и клавиатуры. Кроме того, в этом разделе есть информация о параметрах меню Пуск. Здесь - все настройки, специфичные для пользователя.

Раздел HKEY\_CURRENT\_USER полностью посвящен настройкам текущего пользователя, т.е. того пользователя, который в настоящий момент зарегистрирован в системе. Это отличается от пользовательской конфигурационной информации, которая хранится в других разделах реестра. Информация в этом разделе является динамической; информация в других разделах, которая относится к пользовательским настройкам - статическая. Реестр копирует содержимое одного из подразделов из HKEY\_USERS в данный раздел и по окончании работы обновляет раздел HKEY\_USERS.

Этот корневой раздел является ссылкой на подраздел HKU\SID, где SID – идентификатор безопасности пользователя, вошедшего в систему, воспользовавшись диалоговым окном Вход в Windows (Log On to Windows). Он никогда не связывается с любым подразделов раздела HKEY\_USERS, созданных Windows для поддержания вторичного доступа. Необходимо не путать подраздел HKU\SID с подразделом HKU\SID\_Classes, содержащий соответствия файлов и классы COM для определённого пользователя.

Ниже приведено краткое описание подразделов корневого раздела HKEY\_CURRENT\_USER (табл.2).

Таблица 2 Подразделы корневого раздела HKEY\_CURRENT\_USER

|  |  |
| --- | --- |
| AppEvents | Назначает звуковое сопровождение различным событиям, таким как вход в систему, раскрытие меню или закрытие окна. Звуковое сопровождение выбирается пользователями с помощью аплета Звук и мультимедиа (Sound) окна Панель управления. |
| Console | Содержит свойства окна консоли, например окна командной строки MS DOS. Пользователи настраивают эти свойства, выбирая команду Свойства (Properties) из контекстного меню окна. |
| Control  Panel | Содержит параметры, изменяемые пользователями в окне Панель управления (Control Panel). В качестве примера можно привести параметры электропитания, оформления рабочего стола и специальных возможностей. Не все параметры этого подраздела настраиваются в окне Панель управления (Control Panel) и не все параметры окна Панель управления (Control Panel) содержатся в этом подразделе. |
| Environment | Содержит переменные среды, настроенные пользователями с помощью аплета Система (System) окна Панель управления (Control Panel). |
| Identities | Содержит подразделы для всех удостоверений пользователей, созданных в Microsoft Outlook Express. Удостоверения упрощают совместное использование одного почтового клиента, так как каждому из них могут назначаться отдельные папки для хранения почты, адресная книга и другие настройки. Пользователи могут изменять эти настройки, выбирая команду Удостоверения (Identifies) из меню Файл (File) Microsoft Outlook Express. |
| Keyboard  Layout | Определяет текущую раскладку клавиатуры. Пользователи изменяют параметры раскладки клавиатуры с помощью аплета Клавиатура (Keyboard) окна Панель управления (Control Panel). |
| Network | Содержит подразделы для всех сетевых соединений. Таким образом, здесь присутствуют также и подключённые сетевые диски. Для создания сетевых соединений пользователи выбирают команду Подключить сетевой диск (Map Network Drive) из контекстного меню значка Мой компьютер (My Computer). |
| Printers | Здесь содержатся ведения о принтерах, с которыми может работать пользователь. Пользователи настраивают эти параметры с помощью аплета Принтеры (Printers) окна Панель управления (Control Panel). |
| RemoteAccess | Определяет параметры удалённого доступа к сети, которые настраиваются пользователями на вкладке Подключение (Connections) диалогового окна Свойства: Интернет (Internet Options), которое открывается в результате щелчка на значке Свойства обозревателя (Internet Options) в окне Панель управления (Control Panel). |
| Software | Содержит пользовательские настройки для каждого приложения, включая собственно и Windows. За исключением нескольких приложений от Microsoft, не следующих собственным правилам этой компании, многие приложения сохраняют свои настройки в подразделе Vendor/Application, где Vendor – имя компании-производителя приложения, а Application – имя этого приложения. Эти производители также следуют такому правилу, как добавление дополнительного подраздела Version, что позволяет каждой версии приложения отдельно сохранять собственные настройки. |
| UNICODE  Program  Groups | Здесь содержатся настройки для групп программ, унаследованные от ранних версий Windows NT, использующих программу Диспетчер программ (Program Manager). При чистой установке Windows XP этот подраздел всегда пустой. |
| Volatile  Environment | Здесь содержатся переменные среды, используемые в процессе входа в систему. |
| Windows 3.1  Migration  Status | Здесь представлены сведения о состоянии миграции программных групп и информационных файлов после обновления Windows 3.1. Этот ключ всегда присутствует, но не имеет важного значения, так как компания Microsoft не поддерживает обновление Windows 3.1 до Windows 2000. |

1. HKEY\_LOCAL\_MACHINE

В разделе HKEY\_LOCAL\_MACHINE содержатся основные сведения об аппаратных средствах компьютера, включая драйверы устройств и конфигурационную информацию. Если информации о каком-либо устройстве здесь нет, то Windows не сможет использовать его.

Раздел HKEY\_LOCAL\_MACHINE - для очень подробной информации об аппаратном обеспечении. Например, он содержит всю информацию, необходимую для Plug and Play, а также предоставляет полный список драйверов устройств и их уровни ревизии (revision level) и даже может содержать информацию о ревизии самого аппаратного обеспечения.

Кроме того в этом разделе имеется некоторая информация о программном обеспечении. Например, 32-разрядное приложение будет хранить таблицу установок и форматов (Setup and Format Table- STF) именно здесь. Эта информация используется приложением во время установки. Некоторые приложения используют ее во время изменений параметров их установки. Такие приложения, как Word, хранят всю информацию о своей установке в таблицах STF. В этом разделе содержится только информация глобального характера.

Ниже перечислены пять основных подразделов ключевого раздела HKEY\_LOCAL\_MACHINE (табл.3).

Таблица 3 Подразделы корневого раздела HKEY\_LOCAL\_MACHINE

|  |  |
| --- | --- |
| HARDWARE | Здесь содержатся сведения об оборудовании, обнаруженном Windows в компьютере. Помимо описаний процессора и памяти компьютера, этот раздел описывает ресурсы, используемые устройствами, а также связывает устройства с соответствующими драйверами, что объясняется добавлением поддержки Plug-and-Play в Windows. Необходимо обратить внимание на то, что этот подраздел создаётся Windows во время загрузки операционной системы. |
| SAM | Здесь содержится локальная база данных системы безопасности SAM (Security Account Manager – администратор учётных данных в системе безопасности). Windows содержит в этой базе данных сведения о локальных пользователях и группах, а Windows 2k Server здесь содержит ещё и сведения о пользователях и группах домена. Разрешения предотвращают просмотр этих данных пользователями, даже обладающими правами администратора. Для управления базой данных системы безопасности нужно воспользоваться аплетом Пользователи и пароли (Users and Passwords) окна Панель управления (Control Panel). Необходимо обратить внимание на то, что подраздел SAM – это ссылка на подраздел HKLM\SECURITY\SAM. |
| SECURITY | Содержит локальную базу данных, SAM, а также локальные политики и другие секреты. Windows предотвращает просмотр пользователями содержания этого подраздела. |
| SOFTWARE | Содержит настройки компьютера для каждого приложения, включая собственно и Windows. Как и в случае подраздела HKCU\Software, за исключением нескольких приложений от Microsoft, не следующих собственным правилам этой кампании, многие приложения сохраняют свои настройки в подразделе Vendor/Application, где Vendor – имя компании-производителя приложения, а Application – имя этого приложения. Эти производители также следуют такому правилу, как добавление дополнительного подраздела Version. Наиболее интересным, полезным и настраиваемым в подразделе HKLM\SOFTWARE является подраздел Classes. Этот подраздел определяет соответствие файлов и классы COM. Реестр упрощает доступ к этому подразделу, т.к. корневой раздел HKEY\_CLASSES\_ROOT определяется ссылкой именно на этот подраздел. |
| SYSTEM | Содержит наборы управления, описывающие драйверы устройств и службы, которые Windows загружает при запуске. Кроме того, наборы управления определяют все аспекты конфигурации компьютера на уровне операционной системы. Каждый из наборов управления представляет собой подраздел, который называется HKLM\SYSTEM\ControlSetnnn, где nnn – трёхзначное число, начиная с 000. Подраздел CurrentControlSet – это ссылка на текущий набор управления, используемый Windows. Подраздел HKLM\SYSTEM\Select содержит параметр Current, указывающий на то, какой из наборов управления используется Windows в данный момент. |

1. HKEY\_USERS

Раздел HKEY\_USERS содержит список всех пользователей данного файла реестра. Необходимости в изменении информации этого раздела никогда не возникает, но его можно использовать в справочных целях. Причина, по которой нужно следовать этим указаниям, проста: ни одно изменение не войдет в силу до тех пор, пока пользователь не зарегистрируется в системе следующий раз. Кроме того, изменение настроек для текущего пользователя является пустой тратой времени, потому что Windows заменяет все данные в соответствующем разделе данными, которые содержатся в разделе HKEY\_CURRENT\_USER, во время завершения сеанса или при завершении работы системы.

Существует еще одна проблема, связанная с использованием этого раздела в качестве единственного источника информации. На самом деле Windows поддерживает несколько копий реестра в многопользовательской среде, в некоторых случаях отдельную копию для каждого пользователя. По этой причине никогда нельзя быть уверенным, где именно можно найти информацию об определенном пользователе. Windows отслеживает эту информацию; необходимость поиска такой информации это головная боль для администратора. Сверх того, Microsoft поставляет утилиту, которая помогает администратору сети поддерживать различные реестры. Редактор системных правил (Policy Editor) позволяет упростить для администратора сети управление пользовательскими настройками, при этом является удобным средством доступа к нужным параметрам системы, которые распределены по различным разделам реестра.

Когда пользователь регистрируется в системе, Windows копирует информацию из его профиля в раздел реестра HKEY\_CURRENT\_USER. Когда пользователь выходит из системы или завершает работу, Windows заменяет информацию в разделе, соответствующему данному пользователю, информацией из раздела HKEY\_CURRENT\_USER.

1. HKEY\_CURRENT\_CONFIG

Раздел HKEY\_CURRENT\_CONFIG представляет собой самую простую часть реестра. Он содержит два главных раздела:

1. Display.

2. System..

По существу эти разделы используются программным интерфейсом GDI API для конфигурации монитора и принтера.

1. Раздел Display имеет два подраздела:

* Fonts.
* Setting.

Fonts определяет шрифты, которые Windows использует для вывода на экран. Имеются растровые шрифты (не True Type), которые представляют собой битовые изображения символов.

Setting содержит текущее разрешение экрана и количество битов на пиксел. Количество битов на пиксел определяет доступное количество цветов. Например, 4 бита на пиксел обеспечивают 16 цветов, 8 битов на пиксел обеспечивают 256 цветов. Три шрифта, перечисленных в этом разделе, являются шрифтами по умолчанию, которые система использует для отображения значков и меню приложений. Эти настройки можно изменить в диалоговом окне свойств экрана.

2. Раздел System производит впечатление чего-то запутанного. Однако только один подраздел этого раздела имеет смысл для пользователя - Printers. Раздел Printers содержит список принтеров, подсоединенных к системе. Этот список не включает принтеры, которые используются по сети.

1. HKEY\_DYN\_DATA (Win9x) или HKEY\_PERFORMANCE\_DATA (Win2000)

Раздел HKEY\_DYN\_DATA (HKEY\_PERFORMANCE\_DATA) содержит два подраздела:

* Config Manager
* PerfStats.

Просмотреть статус ключа Config Manager можно в окне "Свойства: "Система" на вкладке Устройства (Device Manager), вызываемого из Панели управления. Данные этого раздела изменяются самой операционной системой, так что редактировать что-либо вручную не рекомендуется. При этом в подключе Enum записываются данные о каждом аппаратном компоненте системы.

Значения ключей из раздела PerfStats отображаются в интерфейсе утилиты System Monitor и содержат данные измерения производительности системы.

### **Таким образом, системный реестр — это база данных для хранения сведений о конфигурации компьютера, настроек операционной системы и параметров программ. Реестр содержит данные, к которым Windows 7, Vista и установленные программы обращаются сотни раз в секунду во время загрузки и работы системы. Замусоренный и фрагментированный реестр может служить причиной серьезного замедления работы компьютера.**