

Реестр Windows

Определение

Реестр Windows — иерархическая база данных, хранящая настройки для ОС Windows и для ее приложений.

Определение

Другими словами, реестр или реестр Windows содержит информацию, настройки, опции и другие значения для программ и оборудования, установленных во всех версиях операционных систем Microsoft Windows. Например, когда устанавливается программа, в реестр Windows добавляется новый подраздел, содержащий такие настройки, как местоположение программы, ее версия и способ запуска программы.

Данные:

Литература – Хонекайт (Honeycutt) «Реестр Windows XP».

https://en.wikipedia.org/wiki/Windows_Registry

<https://learn.microsoft.com/ru-ru/troubleshoot/windows-server/performance/windows-registry-advanced-users>

Реестр Windows

Ключи и значения

Реестр содержит два основных элемента: ключи и значения. Ключи реестра — это объекты-контейнеры, похожие на папки. Значения реестра — это неконтейнерные объекты, похожие на файлы. Ключи могут содержать значения и подразделы. Ключи ссылаются с помощью синтаксиса, похожего на имена путей Windows, с использованием обратных косых черт для указания уровней иерархии. Ключи должны иметь нечувствительное к регистру имя без обратных косых черт.

Основные ключи

- HKEY_LOCAL_MACHINE (HKLM);
- HKEY_CURRENT_CONFIG (HKCC);
- HKEY_CLASSES_ROOT (HKCR);
- HKEY_CURRENT_USER (HKCU);
- HKEY_USERS (HKU);
- HKEY_PERFORMANCE_DATA;
- HKEY_DYN_DATA.

Регистр Windows

Ключи реестра

Как и другие файлы и службы в Windows, все ключи реестра могут быть ограничены списками управления доступом (ACL) в зависимости от привилегий пользователя, токенов безопасности, полученных приложениями, или политик безопасности системы, применяемых системой (эти ограничения могут быть предопределены самой системой и настроены локальными системными администраторами или администраторами домена). Различные пользователи, программы, службы или удаленные системы могут видеть только некоторые части иерархии или отдельные иерархии из одних и тех же корневых ключей.

Реестр Windows

Ключи реестра

Значения реестра представляют собой пары имя/данные, хранящиеся в ключах. Значения реестра указываются отдельно от ключей реестра. Каждое значение реестра, хранящееся в ключе реестра, имеет уникальное имя, регистр букв которого не имеет значения. Функции API Windows, которые запрашивают и обрабатывают значения реестра, принимают имена значений отдельно от пути ключа или дескриптора, который идентифицирует родительский ключ. Значения реестра могут содержать обратные косые черты в своих именах, но это затрудняет их различение от их путей ключей при использовании некоторых устаревших функций API реестра Windows (использование которых устарело в Win32).

Регистр Windows

Значения регистра

Каждое значение может хранить произвольные данные с переменной длиной и кодировкой, но которые связаны с символическим типом (определяемым как числовая константа), определяющим, как анализировать эти данные.

Регистр Windows

Значения реестра

Стандартные типы:

- REG_NONE: без типа;
- REG_SZ: строковое значение;
- REG_EXPAND_SZ: Расширенное строковое значение, которое может содержать переменные окружения;
- REG_BINARY: бинарные данные;
- REG_DWORD: значение типа DWORD (32-битный integer);
- REG_LINK: символическая ссылка;
- REG_MULTI_SZ: многострочное значение;
- REG_RESOURCE_LIST: список ресурсов.

Определение

Куст реестра (hives) — группа ключей, подразделов и значений в реестре с набором вспомогательных файлов, содержащих резервные копии данных.

Вспомогательные файлы для всех кустов, кроме HKEY_CURRENT_USER, находятся в папке %SystemRoot%\System32\Config.

Вспомогательные файлы для HKEY_CURRENT_USER находятся в папке %SystemRoot%\Profiles\Username.

Расширения имен файлов в этих папках указывают тип содержащихся в них данных.

Регистр Windows

Подробнее про ключи реестра

HKEY_CURRENT_USER: Содержит корневой каталог сведений о конфигурации для пользователя, который в настоящее время выполнил вход. Здесь хранятся папки пользователя, образец экрана и параметры панели управления. Эти сведения связаны с профилем пользователя. Этот раздел иногда сокращается как HKCU.

Реестр Windows

Подробнее про ключи реестра

HKEY_USERS: Содержит все активно загруженные профили пользователей на компьютере. HKEY_CURRENT_USER является подразделом HKEY_USERS. HKEY_USERS иногда сокращается как HKU.

Реестр Windows

Подробнее про ключи реестра

HKKEY_LOCAL_MACHINE: Содержит сведения о конфигурации, относящиеся к компьютеру (для любого пользователя). Этот раздел иногда сокращается как HKLM.

Реестр Windows

Подробнее про ключи реестра

HKEY_CLASSES_ROOT: Является подразделом

HKEY_LOCAL_MACHINE\Software.X ранимая здесь информация гарантирует, что при открытии файла с помощью Windows Explorer откроется правильная программа. Этот раздел иногда сокращается как **HKCR**.

Начиная с Windows 2000, эти сведения хранятся в разделах

HKEY_LOCAL_MACHINE и **HKEY_CURRENT_USER**. Раздел

HKEY_LOCAL_MACHINE\Software\Classes содержит параметры по умолчанию, которые могут применяться ко всем пользователям на локальном компьютере.

Раздел **HKEY_CURRENT_USER\Software\Classes** содержит параметры, которые переопределяют параметры по умолчанию и применяются только к интерактивному пользователю.

Раздел **HKEY_CLASSES_ROOT** обеспечивает представление реестра, который объединяет сведения из этих двух источников. **HKEY_CLASSES_ROOT** также обеспечивает это объединенное представление для программ, предназначенных для более ранних версий Windows. Чтобы изменить параметры интерактивного пользователя, необходимо внести изменения в раздел

HKEY_CURRENT_USER\Software\Classes вместо **HKEY_CLASSES_ROOT**.

Чтобы изменить параметры по умолчанию, необходимо внести изменения в раздел **HKEY_LOCAL_MACHINE\Software\Classes**. Если вы записываете значения в ключ в **HKEY_CLASSES_ROOT**, система сохраняет сведения в разделе **HKEY_LOCAL_MACHINE\Software\Classes**. Если запись значений

осуществляется в раздел реестра в разделе **HKEY_CLASSES_ROOT**, при этом раздел реестра уже существует в разделе

HKEY_CURRENT_USER\Software\Classes, система будет хранить сведения там, а не в разделе **HKEY_LOCAL_MACHINE\Software\Classes**.

Регистр Windows

Подробнее про ключи реестра

HKEY_CURRENT_CONFIG: Содержит сведения о профиле оборудования, используемом локальным компьютером при запуске операционной системы.

Реестр Windows

Редактирование реестра

Редактор реестра: regedit.exe

Может быть использован для выполнения следующих действий:

- поиск поддерева, раздела, подраздела или значения;
- добавление подраздела или значения;
- изменение значения;
- удаление подраздела или значения;
- переименование подраздела или значения.

В области навигации редактора реестра отображаются папки. Каждая папка представляет predetermined раздел на локальном компьютере. При доступе к реестру удаленного компьютера отображаются только два predetermined раздела: HKEY_USERS и HKEY_LOCAL_MACHINE.

Реестр Windows

Использование средства реестра консоли для Windows

Для изменения реестра можно использовать средство реестра консоли (Reg.exe). Для получения справки по использованию средства Reg.exe введите `reg /?` в командной строке и нажмите кнопку ОК.

Реестр Windows

Восстановление реестра Восстановить реестр можно одним из следующих методов:

Восстановление подразделов реестра

Чтобы восстановить экспортированные подразделы реестра, можно дважды щелкнуть файл реестра (REG), сохраненный в разделе «Экспорт подразделов реестра». Кроме того, можно восстановить весь реестр из резервной копии.

Восстановление всего реестра

Чтобы восстановить весь реестр, можно восстановить состояние системы из резервной копии.

Реестр Windows

Задания

- 1 Найти в реестре настройку, отвечающую за раскладку клавиатуры для текущего пользователя. Экспортировать найденный раздел. Затем изменить основной язык на противоположный. Снова Экспортировать раздел реестра и сравнить полученные файлы с помощью утилиты *windiff*.
- 2 Разобраться, как Windows узнает, что файлы .txt надо открывать именно в блокноте.
- 3 Сделать так, чтобы при создании через контекстное меню нового CMD-файла он был не пустым. Пусть он содержит следующие строки:

```
@echo off
```

```
if "%1"=="?" echo help & goto:eof
```

Для этого аблон надо сохранить в каталог

```
C:\Users\<username>\AppData\Roaming\Microsoft\Templates\template.cmd
```

и добавить

```
[HKEY_CLASSES_ROOT\.cmd\ShellNew]
```

```
FileName="template.cmd"
```

Спасибо за внимание!