# Лабораторная работа № 12

**РЕЕСТР**

**(4 часа) ЦЕЛЬ РАБОТЫ:** изучение работы в реестре

# ЗАДАЧИ РАБОТЫ

1. Познакомиться с месторасположением файлов, составляющих реестр Windows.
2. Изучить стандартные средства просмотра и редактирования реестра Windows.

# ПЕРЕЧЕНЬ ОБЕСПЕЧИВАЮЩИХ СРЕДСТВ

1. ПК.
2. Программное обеспечение: Oracle VirtualBox, ОС Windows Server 2003.
3. Учебно-методическая литература.

# ОБЩИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

В операционной системе Windows сведения о параметрах и настройках устройств и приложений хранятся в глобальной базе данных, которая носит на- звание реестр. В реестре находятся профили всех пользователей компьютера, сведения о конфигурации конкретного компьютера, параметры установленных программ и прочая важная информация. Windows использует эти сведения в процессе своей работы. Реестр расположен в нескольких файлах, которые из- меняются в процессе работы ОС Windows. Доступ к реестру защищен и кон- тролируется редактором реестра.

Реестр является основой ОС, представляя собой большую базу функций и параметров системы и программного обеспечения, хранящуюся по адресу

%SystemRoot%\System32\Config и в папке профилей пользователей компьютера (Ntuser.dat). Следует отметить, что без реестра работа операционной системы невозможна.

Реестр связывает и координирует действия всех элементов операционной системы и отвечает за ее стабильную работу. Именно поэтому надо быть мак- симально осторожным при работе с ним.

Реестр Windows является:

* динамическим;
* иерархическим;
* защищенным.

*Динамичность реестра* проявляется в том, что Windows и программы во время работы постоянно изменяют его содержимое. Все изменения, которые были внесены в реестр, сразу же становятся доступными для всех остальных работающих приложений и утилит. В реестре сохраняются все настройки про-

граммного обеспечения и операционной системы, что позволяет не проводить повторного процесса конфигурации после перезагрузки системы.

Структура реестра является *иерархической*. Реестр делится на несколько основных разделов, которые носят название поддеревьев (Subtrees). Поддерево содержит множество различных ключей (Keys), каждый из которых способен содержать в себе несколько подключей (Subkeys). Каждый ключ или подключ может иметь несколько различных значений (Values).

Реестр содержит данные о приоритетах задач, процессов или устройств системы. Кроме того, в реестре находится информация о зависимости различ- ных составляющих операционной системы друг от друга. Определенные разде- лы реестра содержат информацию о порядке загрузки системы — порядок ини- циализации, запуска и конфигурирования драйверов, запуска сервисов и опре- деления устройств, окончания загрузки и входа пользователя в систему.

*Защищенность реестра* означает, что у него присутствует собственная система безопасности, которая необходима для защиты от несанкционирован- ного доступа и изменения, а также регулярной проверки целостности реестра. То, что приложения помещают информацию о собственной конфигурации в ре- естр, имеет два аспекта: позитивный и негативный. Позитив состоит в том, что реестр позволяет эффективно хранить и использовать информацию. Негатив- ный эффект проявляется в увеличении размеров реестра. По мере установки и удаления приложений в реестре накапливается множество ненужных ключей, что может значительно снизить производительность системы.

Научиться работать с реестром достаточно сложно, тем более что Microsoft не предоставляет официальной документации по его использованию. Однако если вы хотите подробно изучить возможности Windows и получить доступ к более гибкой настройке системы, то придется немного поработать.

Реестр Windows ХР состоит из пяти основных поддеревьев, которые носят имена корневых разделов реестра. Вся информация, находящаяся в реестре, де- лится с помощью поддеревьев на несколько логических разделов.

Поддеревья реестра содержат огромное количество разделов (ключей).

«HKEY\_CLASSES\_ROOT» - данный раздел содержит сведения о файло- вых расширениях и программы, которые этим расширениям соответствуют. Здесь также содержится информация, необходимая для работы технологий СОМ и OLE. Некоторые данные, связанные с названным выше, содержатся в ключе HKEY\_LOCAL\_MACHINE\Software\Classes.

«HKEY\_CURRENT\_USER» - данный раздел является корневым для дан- ных конфигурации пользователя, вошедшего в систему в настоящий момент. Здесь хранятся папки пользователя, цвета экрана и параметры панели управле- ния. Эти сведения сопоставлены с профилем пользователя. Вместо полного имени раздела иногда используется аббревиатура HKCU.

«HKEY\_LOCAL\_MACHINE» - раздел содержит информацию о конфигу- рации компьютера и о том, как будут обрабатываться запуск и остановка уста- новленных в системе служб и оборудования. Здесь также содержится информа-

ция, которая относится к Security Accounts Manager (SAM) и политикам безо- пасности. Данная ветвь наиболее интенсивно используется приложениями.

«HKEY\_USERS» - раздел содержит данные о пользователях компьютера. Каждому пользователю назначается определенная запись, название которой со- ответствует идентификатору SID данного пользователя.

«HKEY\_CURRENT\_CONFIG» - эта ветвь связана с подключами в HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\HardwareProfiles\Current.

Данный раздел содержит информацию, которая относится к аппаратному обес- печению и используется в процессе предварительной загрузки, чтобы разре- шить взаимосвязи определенного аппаратного обеспечения.

Как уже было упомянуто, ключи реестра имеют одно или несколько значе- ний разных типов. В зависимости от того, какой тип будет использован, значе- ние ключа может быть двоичным, десятичным или шестнадцатеричным чис- лом, текстом ASCII или же комбинацией из чисел и текста.

«REG\_BINARY» - двоичный параметр. Необработанные двоичные данные. Большинство сведений об аппаратных компонентах хранится в виде двоичных данных и выводится в редакторе реестра в шестнадцатеричном формате.

«REG\_DWORD» - параметр DWORD. Данные представлены в виде значе- ния, 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).

«REG\_EXPAND\_SZ» - расширяемая строка данных. Строка данных пере- менной длины. Этот тип данных включает переменные, обрабатываемые при использовании данных программой или службой. Такая строка содержит имена переменных, которые могут замещаться приложением на фактические значения этих переменных. Значения такого типа используются, в частности, для под- держки переменных окружения.

«REG\_MULTI\_SZ» - 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.

«REG\_SZ» - строковый параметр. Текстовая строка, удобная для воспри- ятия. Значениям, представляющим собой описания компонентов, обычно при- сваивается именно этот тип данных.

«REG\_DWORD\_BIGENDIAN» - данные этого типа являются 32-битными значениями, при этом старший байт располагается в первой позиции.

«REG\_LINK» - ссылка в формате Unicode.

«REG\_FULL\_RESOURCE\_DESCRIPTOR» - двоичный параметр. Последо- вательность вложенных массивов. Служит для хранения списка ресурсов, кото- рые используются физическим устройством. Обнаруженные данные система

сохраняет в разделе \HardwareDescription. В окне редактора реестра эти данные отображаются в виде двоичного параметра в шестнадцатеричном формате.

«REG\_RESOURCE\_LIST» - двоичный параметр. Последовательность вло- женных массивов. Служит для хранения списка ресурсов, которые используют- ся драйвером устройства или управляемым им физическим устройством. Обна- руженные данные система сохраняет в разделе \ResourceMap. В окне редактора реестра эти данные отображаются в виде двоичного параметра в шестнадцате- ричном формате.

«REG\_RESOURCE\_REQUIREMENTS\_LIST» - двоичный параметр. По- следовательность вложенных массивов. Служит для хранения списка драйверов аппаратных ресурсов, которые могут быть использованы определенным драй- вером устройства или управляемым им физическим устройством. Часть этого списка система записывает в раздел \ResourceMap. Данные определяются сис- темой. В окне редактора реестра они отображаются в виде двоичного параметра в шестнадцатеричном формате.

«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\_QWORD» - параметр QWORD. Данные, представленные в виде 64- разрядного целого. Начиная с Windows 2000, такие данные отображаются в ок- не редактора реестра в виде двоичного параметра.

# ЗАДАНИЕ

1. Изучить теоретический материал по данной теме.
2. Изучить возможности редактора по созданию, удалению и изменению элементов реестра, а также возможности поиска информации в реестре и копи- рования части реестра в файл.

# ТРЕБОВАНИЯ К ЗАЧЕТУ

1. К зачету необходимо предоставить результаты выполненной работы.
2. Отчет с подробным описанием выполненных работ.
3. Подготовить ответы на вопросы.

# ТЕХНОЛОГИЯ ВЫПОЛНЕНИЯ РАБОТЫ

Исследование структуры редактора реестра:

1. Выполнить команду «Пуск» - «Выполнить».
2. В появившемся окне ввести команду редактирования реестра «regedit».
3. При помощи редактора исследовать структуру реестра.
4. Открыть ветвь реестра «HKEY\_CURRENT\_USER\Software\» и создать в ней новый раздел (рис. 12.1).

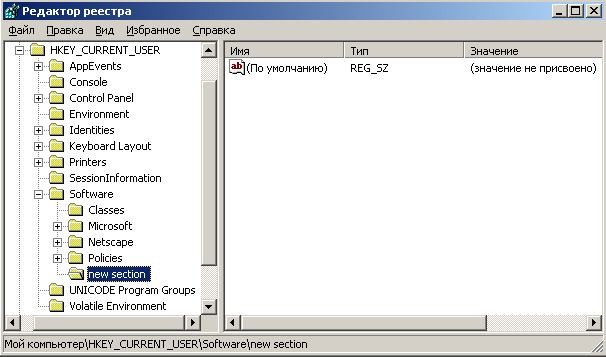


Рис. 12.1. Редактор реестра

1. Нажать правой кнопкой мыши на новый раздел и из контекстного меню выбрать команду «Создать» и последовательно создать пять параметров раз- личных типов: «Строковый параметр», «Двоичный параметр», «Параметр DWORD», «Мультистроковый параметр», «Расширяемый строковый пара- метр».
2. Нажать правой кнопкой мыши на новый раздел и из контекстного меню выбрать команду «Разрешения» (рис.12.2).

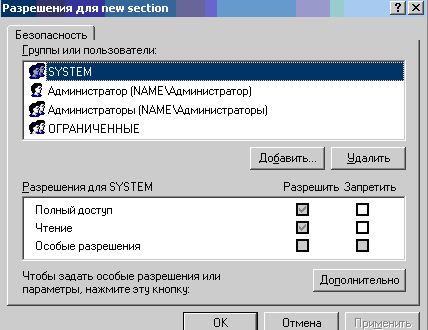


Рис. 12.2 Диалоговое окно «Разрешения»

1. Установить права доступа к новому разделу:
   * пользователю «User1» – чтение;
   * пользователю «Администратор» - полный доступ.
2. В меню выбрать команду «Файл» - «Экспорт» и создать копию нового раздела в текстовом файле.
3. При помощи команды «Правка» - «Найти» найти в реестре все парамет- ры, значение которых равно действующему IP- адресу сервера. Внести полу- ченные данные в отчет.
4. Самостоятельно создать ещё один запрос, результаты которого также занести в отчет.

# КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что представляет собой реестр?
2. Возможна ли работа операционной системы без реестра?
3. В чем проявляется динамичность реестра?
4. Какую структуру имеет реестр?
5. Что означает защищенность реестра?
6. Из чего состоит Реестр Windows ХР?
7. Какие разделы (ключи) содержат поддеревья реестра?
8. Какие возможности предоставляет редактор реестра?