Лабораторная работа № 13 «Работа с системным реестром»

Цель работы: Получение основных сведений о структуре и функциях системного реестра операционной системы Windows 7

Оборудование: персональный компьютер (монитор, системный блок, клавиатура, мышь), ОС Windows, программа для виртуализации Oracle VM VirtualBox, образ виртуальной машины (Win7\_01).

Задание:

1. Изучить теоретическую часть;
2. Запустить редактор реестра.
3. Перейти в раздел реестра HKEY\_CURRENT\_USER;
4. Найти ключ, отвечающий за настройки Рабочего стола;
5. Ознакомиться со списком вложенных ключей;
6. Для произвольно выбранных из списка 5 ключей исследовать, аналогом каких настроек Панели управления они являются;
7. Перейти в раздел реестра HKEY\_CLASSES\_ROOT;
8. Выбрать из списка 5 ключей и описать, для файлов с какими расширениями они используются, и какие параметры для них установлены;
9. Результаты внести в отчет.

Теоретические сведения:

На смену ini-файлам, имеющим ряд концептуальных ограничений, еще в Windows 3.1 было введено понятие реестра – регистрационной базы данных, хранящей различные настройки ОС и приложений. 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. Реестры разных версий Windows имеют различия; это нужно помнить при импорте reg-файлов. В Windows 7 в

архитектуру реестра были введены важные новшества, улучшающие функциональность данного компонента ОС. Реестр хранится в бинарном (двоичном) виде, поэтому для ручной работы с ним необходима специальная программа — редактор реестра. В 7 это Regedit.exe, в других версиях NT ими являются Regedit.exe и Regedt32.exe, имеющий дополнительные возможности работы с реестром (Regedt32.exe есть и в 7, но на самом деле он всего лишь вызывает Regedit.exe). Есть и другие программы, в том числе и консольные (Reg.exe). Ручным модифицированием параметров реестра мы займемся чуть позже, а сейчас рассмотрим основные группы сведений, хранящихся в этой базе данных.

Программы установки. Любая грамотно написанная программа под Windows должна иметь свой инсталлятор-установщик. Это может быть встроенный в ОС Microsoft Installer либо любой другой. В любом случае инсталлятор использует реестр для хранения своих настроек, позволяя правильно устанавливать и удалять приложения, не трогая совместно используемые файлы.

Распознаватель. При каждом запуске компьютера программа NTDETECT.COM и ядро Windows распознает оборудование и сохраняет эту информацию в реестре.

Ядро ОС. Хранит много сведений в реестре о своей конфигурации, в том числе и данные о порядке загрузки драйверов устройств.

Диспетчер PnP (Plug and Play). Абсолютно необходимая вещь для большинства пользователей, которая избавляет их от мук по установке нового оборудования (не всегда, правда:)). Неудивительно, что он хранит свою информацию в реестре.

Драйверы устройств. Хранят здесь свои параметры.

Административные средства. Например, такие, как Панель управления, MMC (Micro-soft Management Console) и др.

Пользовательские профили. Это целая группа параметров, уникальная для каждого пользователя: настройки графической оболочки, сетевых соединений, программ и многое другое.

Аппаратные профили. Позволяют создавать несколько конфигураций с различным оборудованием.

Общие настройки программ. Почему общие? Потому, что у каждого пользователя есть профиль, где хранятся его настройки для соответствующей программы.

Таким образом, выше приведены данные о предназначении реестра. Теперь обратим внимание на логическую структуру реестра. Для лучшего понимания материала рекомендуется запустить Regedit.exe.

Структура реестра

Реестр Windows имеет древовидную структуру, схожую со структурой файловой системы. Папкам здесь соответствуют ключи (keys) или разделы (ветви), а файлам — параметры (values). Разделы могут содержать как вложенные разделы (sub keys), так и параметры. На верхнем уровне этой иерархии находятся корневые разделы (root keys).

HKEY\_LOCAL\_MACHINE

Содержит глобальную информацию о компьютерной системе, включая такие данные об аппаратных средствах и операционной системе, в том числе: тип шины, системная память, драйверы устройств и управляющие данные, используемые при запуске системы. Информация, содержащаяся в этом разделе, действует применительно ко вcем пользователям, регистрирующимся в системе Windows. На верхнем уровне иерархии реестра для этого раздела имеются три псевдонима:

HKEY CLASSES ROOT, HKEY CURRENT CONFIG и HKEY\_DYN\_DATA HKEY\_CLASSES\_ROOT

Содержит ассоциации между приложениями и типами файлов (по расширениям имени файла). Кроме того, этот раздел содержит информацию OLE (Object Linking and Embedding), ассоциированную с объектами COM, а также данные по ассоциациям файлов и классов (эквивалент реестра ранних версий. Windows, служивших настройкой над MS-DOS). Параметры этого раздела совпадают с параметрами, расположенными в разделе HKEY\_LOCAL\_MACHINE\Software\Classes. Подробную информацию о разделе HKEY\_CLASSES\_ ROOT можно найти в руководстве OLE Programmer's Reference, входящем в состав продукта Windows NT 4.0 Software Development Kit (SDK)

HKEY\_CURRENT\_CONFIG

Содержит конфигурационные данные для текущего аппаратного профиля. Аппаратные профили представляют собой наборы изменений, внесенных в стандартную конфигурацию сервисов и устройств, установленную данными разделов Software и System корневого раздела HKEY\_LOCAL\_MACHINE. В разделе HKEY\_CURRENT\_ CONFIG отражаются только изменения. Кроме того, параметры этого раздела появляются также в разделе HKEY\_LOCAL\_MACHINE\System \CurentControlSet\HardwareProfites\CuiTent

HKEY\_CURRENT\_USER

Содержит, профиль пользователя, на данный момент . зарегистрировавшегося в системе, включая переменные окружения, настройку рабочего стола, параметры настройки сети, принтеров и приложений. Этот раздел представляет собой ссылку на раздел HKEY USERS\username, где username — имя пользователя, зарегистрировавшегося в системе на текущий момент HKEY\_USERS Содержит все активно загруженные пользовательские профили, включая HKEY\_CURRENT\_USER, а также профиль по умолчанию. Пользователи, получающие удаленный доступ к серверу, не имеют профилей, содержащихся в этом разделе; их профили загружаются в реестры на их собственных компьютерах. Windows NT/2000 требует наличия учетных записей для каждого пользователя, регистрирующегося в системе.

Раздел HKEY\_USERS содержит вложенный раздел \Default, а также другие разделы, определяемые идентификатором безопасности (Security ID) каждого пользователя

Типы данных

Все параметры реестра имеют фиксированный тип. В таблице 2 приводится полный список используемых типов. Не все из них используются в разных версиях NT

— REG\_QWORD явно предназначен для 64-битной версии 7. Следует учесть, что ряд типов используется только системой в некоторых разделах, и создать свой параметр такого типа с помощью редактора реестра не получится.

REG\_BINARY

Двоичные данные. Большинство сведений об аппаратных компонентах хранится в виде двоичных данных и выводится в редакторе реестра в шестнадцатеричном формате

REG\_DWORD

Данные, представленные целым числом (4 байта). Многие параметры служб и драйверов устройств имеют этот тип и отображаются в двоичном, шестнадцатеричном или десятичном форматах

REG\_E7AND\_SZ

Строка Unicode переменной длины. Этот типданныхвключаетпеременные, обрабатываемые программой или службой

REG\_MULTI\_SZ

Многострочный текст Unicode. Этот тип, как правило, имеют списки и другие записи в формате, удобном для чтения. Записи разделяются пробелами, запятыми или другими символами

REG\_SZ

Текстовая Unicode строка фиксированной длины

REG\_DWORD\_LITTLE\_ENDIAN

32-разрядное число в формате “остроконечников” — младший байт хранится первым в памяти. Эквивалент REG\_DWORD

REG\_DWORD\_BIG\_ENDIAN

32-разрядное число в формате “тупоконечников” — старший байт хранится первым в памяти REG\_LINK Символическая ссылка Unicode. Только для внутреннего использования (некоторые корневые разделы являются такой ссылкой на другие подразделы)

REG\_NONE

Параметр не имеет определенного типа данных

REG\_QWORD

64-разрядное число

REG\_QWORD\_LITTLE\_ENDIAN

64-разрядное число в формате “остроконечников”. Эквивалент REG\_QWORD

REG\_RESOURCE\_LIST

Список аппаратных ресурсов. Используется только в разделе HKLM\HARDWARE

REG\_FULL\_RESOURCE\_DESCRIPTOR

Дескриптор (описатель) аппаратного ресурса. Применяется только в HKLM\HARDWARE.

REG\_RESOURCE\_REQUIREMENTS\_LIST

Список необходимых аппаратных ресурсов. Используется только в HKLM\HARDWARE.

Хранение реестра

Элементы реестра хранятся в виде атомарной структуры. Реестр разделяется на составные части, называемые ульями (hives), или кустами. Ульи хранятся на диске в виде файлов. Некоторые ульи, такие, как HKLM\HARDWARE, не сохраняются в файлах, а создаются при каждой загрузке, то есть являются изменяемыми (vola-tile). При запуске системы реестр собирается из ульев в единую древовидную структуру с корневыми разделами. Перечислим ульи реестра и их местоположение на диске (для NT старше версии 4.0)

HKLM\SYSTEM %SystemRoot%\system32\config\system

HKLM\SAM %SystemRoot%\system32\config\SAM

HKLM\SECURITY %SystemRoot%\system32\config\SECURITY

HKLM\SOFTWARE %SystemRoot%\system32\config\software

HKLM\HARDWARE Изменяемый улей

HKLM\SYSTEM\Clone Изменяемый улей

HKU\<SID\_пользователя> %USERPROFILE%\ntuser.dat

HKU\<SID\_пользователя>\_Classes %USERPROFILE%\Local Settings\Application

Data\Microsoft\Windows\UsrClass.dat

HKU\.DEFAULT %SystemRoot%\system32\config\default

Кроме этих файлов, есть ряд вспомогательных, со следующими расширениями:

ALT – резервная копия улья HKLM\SYSTEM (отсутствует в 7).

LOG – журнал транзакций, в котором регистрируются все изменения реестра. SAV – копии ульев в том виде, в котором они были после завершения текстовой фазы установки.

Дополнительные сведения

Реестр является настоящей базой данных, поэтому в нем используется технология восстановления, похожая на оную в NTFS. Уже упомянутые LOG-файлы содержат журнал транзакций, который хранит все изменения. Благодаря этому реализуется атомарность реестра – то есть в данный момент времени в реестре могут быть либо старые значения, либо новые, даже после сбоя. Как видим, в отличие от NTFS, здесь обеспечивается сохранность не только структуры реестра, но и данных. К тому же, реестр поддерживает такие фишки NTFS, как управление избирательным доступом и аудит событий – система безопасности пронизывает всю NT снизу доверху. Да, эти функции доступны только из Regedt32.exe или Regedit.exe для 7. А еще весь реестр или его отдельные части можно экспортировать в текстовые reg-файлы (Unicode для Windows 2000 и старше), редактировать их в блокноте, а затем экспортировать обратно. Во многих редакторах реестра можно подключать любые доступные ульи реестра, в том числе и на удаленных машинах (при соответствующих полномочиях). Есть возможность делать резервные копии с помощью программы NTBackup.

Ход работы:

Для запуска системного реестра Windows 7 необходимо нажать кнопку <Пуск>, <Выполнить>, ввести команду <Regedit> и нажать <ОК>. Запуститься программа Редактор реестра .

Для перехода по разделам реестра необходимо выбрать соответствующий раздел

нажать кнопку раскрывающегося списка, находящуюся слева он названия раздела. Ключ, отвечающий за настройки рабочего стола находится по адресу

<HKEY\_CURRENT\_USER\Control Panel\Desktop>

Размеры элементов экрана в Windows (иконки, шрифты, рамки, меню, полосы

прокрутки) хранятся в разделе HKEY\_CURRENT\_USER\Control Panel\desktop\WindowMetrics реестра

Ниже приведены некоторые параметры, содержащиеся в этом разделе.

BorderWidth Ширина рамки окна

CaptionFont Шрифт заголовка

CaptionHeight Высота шрифта заголовка

CaptionWidth Ширина заголовка

IconFont Шрифт названия иконки

IconSpacing Горизонтальный интервал между иконками

IconSpacingFactor Фактор, используемый для вычисления положения иконок

IconVerticalSpacing Вертикальный интервал между значками

MenuFont Параметры шрифта (гарнитура, имя шрифта, и т.д.), используемого в строках меню

MenuHeight Высота ячейки символа, используемого в строке меню

MenuWidth Ширина ячейки символа, используемого в строке меню

MessageFont Шрифт, используемый в сообщениях

ScrollHeight Высота горизонтальной полосы прокрутки

ScrollWidth

Ширина вертикальной полосы прокрутки

ShellIconBPP Число цветов (битов на точку), используемых для иконок

ShellIconSize Размер иконок на Рабочем столе (и в проводнике в режиме "Крупные значки")

SmCaptionFont Шрифт в маленьких заголовках

SmCaptionHeight Высота ячейки символа в маленьком заголовке

SmCaptionWidth Ширина ячейки символа в маленьком заголовке

Каждый ключ, содержащий данные для шрифта, состоит из последовательности байтов, соответствующих имени шрифта и нескольким флагам, определяющим тип шрифта, типы начертания (полужирный, курсив) и т.д. Эти параметры можно изменять на вкладке «Оформление» диалога «Свойства: Экран».

Некоторые параметры настройки элементов экрана:

HKEY\_CURRENT\_USER\Control Panel\Desktop\WindowMetrics\ShellIconSize – управляет размером отображения значков рабочего стола. Значение 48 указывает, что значки рабочего стола будут отображаться размером 48х48 точек. Аналог <Свойства: Экран> / <Оформление> / <Эффекты> / <Применять крупные значки>.

HKEY\_CURRENT\_USER\Control Panel\Desktop\FontSmoothing – управляет сглаживанием неровностей экранных шрифтов. Аналог <Свойства: Экран> / <Оформление> / <Эффекты> / <Применять следующий метод сглаживания экранных шрифтов>.

HKEY\_CURRENT\_USER\Control Panel\Desktop\DragFullWindows – управляет отображением содержимого окна при его перетаскивании. Аналог <Свойства: Экран> / <Оформление>/<Эффекты>/<Отображать содержимое окна при его перетаскивании>.

HKEY\_CURRENT\_USER\Control Panel\Desktop\Wallpaper – содержит путь к файлу рисунка обоев, , аналог <Свойства: Экран> / <Рабочий стол>.

HKEY\_CURRENT\_USER\Control Panel\Desktop\SCRNSAVE.EXE – содержит путь к файлу с заставкой, аналог <Свойства: Экран> / <Заставка>.

Далее рассмотрим ключ реестра HKEY\_CLASSES\_ROOT

Корневой ключ реестра HKEY\_CLASSES\_ROOT содержит информацию обо всех ассоциациях (связях) расширений имен файлов, с приложениями, поддерживающими эти типы файлов, и о данных, ассоциированных с объектами СОМ. Эти данные совпадают с информацией, которая содержится в ключе classes, расположенной в иерархии ниже ключа HKEY\_LOCAL\_MACHINE\SOFTWARE.

Некоторые ключи раздела HKEY\_CLASSES\_ROOT:

HKEY\_CLASSES\_ROOT\.ico – определяет параметры файлов с расширением ico (значков, иконок);

HKEY\_CLASSES\_ROOT\.xls\Excel.Sheet.8\ShellNew – определяет параметры открытия файлов с расширением XLS (параметр Filename=excel9.xls);

HKEY\_CLASSES\_ROOT\.zip\ShellNew – определяет параметры открытия файлов

расширением ZIP(параметр Filename= C:\Program Files\WinRAR\zipnew.dat);

HKEY\_CLASSES\_ROOT\Excel.Template\shell\Print\command – определяет команды печати для шаблонов электронных таблиц Excel

HKEY\_CLASSES\_ROOT\jpg – определяет программу с которой ассоциированы файлы с расширением JPG