Теоретические вопросы

1. Реестр Windows XP. Утилиты для работы с реестром

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 некоторых работах его переводят на русский язык как "Улей". 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.

В операционных системах Windows Vista/Windows 7/8/10, файлы реестра располагаются также в каталоге \Windows\system32\config и имеют такие же имена, однако в этих ОС добавился новый раздел реестра для хранения данных конфигурации загрузки (Boot Configuration Data) с именем BCD00000000. Файл с данными этого раздела имеет имя bcd и находится в скрытой папке Boot активного раздела (раздела, с которого выполняется загрузка системы). Обычно, при стандартной установке Windows 7, создается активный раздел небольшого размера (около 100 мегабайт), который скрыт от пользователя и содержит только служебные данные для загрузки системы – загрузочные записи, менеджер загрузки bootmgr, хранилище конфигурации загрузки BCD, файлы локализации и программы тестирования памяти . Расположение куста bcd зависит от того, как сконфигурирован загрузчик системы при ее установке, и может находиться на том же разделе, где и каталог Windows.

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" - regedit.exe.

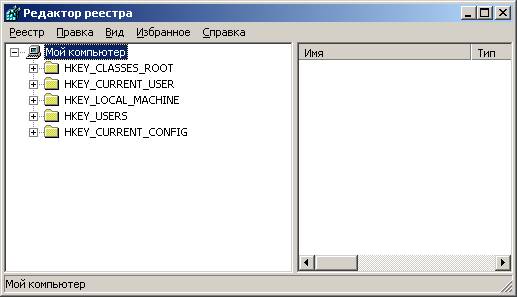


Рисунок 1 – Редактор реестра

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:

HKEY\_CLASSES\_ROOT (Общепринятое сокращенное обозначение HKCR) - Ассоциации между приложениями и расширениями файлов и информацию о зарегистрированных объектах COM и ActiveX.

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) в виде S-1-5-21-854245398-1035525444-...

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.

Идентификатор SID представляет собой числовое значение переменной длины, формируемое из номера версии структуры SID, 48-битного кода агента идентификатора и переменного количества 32-битных кодов субагентов и/или относительных идентификаторов (Relative IDentifiers, RID). Код агента идентификатора определяет агент, выдавший SID, и обычно таким агентом является локальная операционная система или домен под управлением Windows. Коды субагентов идентифицируют попечителей, уполномоченных агентом, который выдал SID, а RID - дополнительный код для создания уникальных SID на основе общего базового SID.

Для идентификатора S-1-5-21-854245398-1035525444: 1000, номер версии равен 1, код агента идентификатора - 5, а далее следуют коды четырех субагентов. В Windows NT и старше, при установке системы, создается один фиксированный (код 21) и три генерируемых случайным образом (числа после "S-1-5-21") кода субагентов. Также в процессе установки создаются некоторые (одинаковые для всех систем) учетные записи, как например, учетная запись администратора, которая всегда имеет RID равный 500

Для просмотра соответствия SID и имени пользователя можно воспользоваться утилитой PsGetSID.exe из пакета PSTools

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.

HKEY\_USERS(HKU) - индивидуальные настройки среды для каждого пользователя системы (пользовательские профили) и профиль по умолчанию для вновь создаваемых пользователей.

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).

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.

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.

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.

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 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\_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. Далее по тексту, предполагается, если это не оговорено особо, что пользователь имеет права администратора системы.

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, для чего можно воспользоваться утилитой PSExec

psexec.exe -i -s regedit.exe

Можно также воспользоваться стандартными средствами операционной системы, например, планировщиком заданий. С помощью команды at создаем задание на запуск regedit.exe в интерактивном режиме через 2-3 минуты от текущего времени (например- в 16час 14 мин.)

at 16:14 /interactive regedit.exe

Поскольку сам планировщик работает как системная служба, то порожденная им задача также будет выполняться с наследуемыми правами, а ключ /interactive позволит текущему пользователю взаимодействовать с запущенным заданием, т.е. с редактором реестра, выполняющимся с правами локальной системной учетной записи.

В Windows 7 разделы реестра SAM и SECURITY отображаются, однако не отображается их содержимое, для просмотра которого можно воспользоваться аналогичным приемом.

В процессе загрузки и функционирования операционной системы выполняется постоянное обращение к данным реестра, как для чтения, так и для записи. Файлы реестра постоянно изменяются, поскольку не только система, но и отдельные приложения могут использовать реестр для хранения собственных данных, параметров и настроек. Другими словами, обращение к реестру - это одна из наиболее распространенных операций. Даже если пользователь не работает за компьютером, обращения к реестру все равно выполняются системными службами, драйверами и приложениями.

Нарушение целостности файлов реестра (нарушение структуры данных) или неверное значение отдельных критических параметров может привести к краху системы. Поэтому, прежде чем экспериментировать с реестром, позаботьтесь о возможности его сохранения и восстановления.

1. ОС Linux. Организация файловой системы.

Файл – это понятие, привычное любому пользователю компьютера. Для пользователя каждый файл – это отдельный предмет, у которого есть начало и конец и который отличается от всех остальных файлов именем и расположением (“как называется” и “где лежит”). Как и любой предмет, файл можно создать, переместить и уничтожить, однако без внешнего вмешательства он будет сохраняться неизменным неопределенно долгое время. Файл предназначен для хранения данных любого типа – текстовых, графических, звуковых, исполняемых программ и многого другого. Аналогия файла с предметом позволяет пользователю быстро освоиться при работе с данными в операционной системе.

Для операционной системы Linux файл – не менее важное понятие, чем для ее пользователя: все данные, хранящиеся на любых носителях, обязательно находятся внутри какого-нибудь файла, в противном случае они просто недоступны ни для операционной системы, ни для пользователей. Более того, многие устройства, подключенные к компьютеру (начиная с клавиатуры и заканчивая любыми внешними устройствами, например, принтерами и сканерами), Linux представляет, как файлы (так называемые файлы-дырки). Конечно, файл, содержащий обычные данные, сильно отличается от файла, предназначенного для обращения к устройству, поэтому в Linux определено несколько различных типов файлов. В основном пользователь имеет дело с файлами трех типов: обычными файлами, предназначенными для хранения данных, каталогами и файлами-ссылками.

Отдельная область данных на одном из носителей информации, у которой есть собственное имя.

Система файлов: каталоги.

Файловая система с точки зрения пользователя – это “пространство”, в котором размещаются файлы. Наличие файловой системы позволяет определить не только “как называется файл”, но и “где он находится”. Различать файлы только по имени было бы нецелесообразно: приходилось бы помнить, как называется каждый файл и при этом заботиться о том, чтобы имена никогда не повторялись. Более того, необходим механизм, позволяющий работать с группами тематически связанных между собой файлов (например, компонентов одной и той же программы или разных глав диссертации). Иначе говоря, файлы нужно систематизировать.

Способ хранения и организации доступа к данным на информационном носителе или его разделе. Классическая файловая система имеет иерархическую структуру, в которой файл однозначно определяется полным путем к нему.

Linux может работать с различными типами файловых систем, которые различаются списком поддерживаемых возможностей, производительностью в разных ситуациях, надежностью и другими признаками. Подробнее о работе Linux с разными файловыми системами речь пойдет в лекции 11. В этой лекции будут описаны возможности файловой системы Ext2/Ext3, на сегодня de facto стандартной файловой системы для Linux.

Большинство современных файловых систем (но не все!) используют в качестве основного организационного принципа каталоги. Каталог – это список ссылок на файлы или другие каталоги. Принято говорить, что каталог содержит файлы или другие каталоги, хотя в действительности он только ссылается на них, физическое размещение данных на диске обычно никак не связано с размещением каталога. Каталог, на который есть ссылка в данном каталоге, называется подкаталогом или вложенным каталогом. Каталог в файловой системе более всего напоминает библиотечный каталог, содержащий ссылки на объединенные по каким-то признакам книги и другие разделы каталога (файлы и подкаталоги). Ссылка на один и тот же файл может содержаться в нескольких каталогах одновременно – это делает доступ к файлу более удобным. В файловой системе Ext2 каждый каталог – это отдельный файл особого типа (“d”, от англ. “directory”), отличающийся от обычного файла с данными: в нем могут содержаться только ссылки на другие файлы и каталоги.

В файловой системе Linux нет папок и документов. Есть каталоги и файлы, возможности которых куда шире.

В файловой системе, организованной при помощи каталогов, на любой файл должна быть ссылка как минимум из одного каталога, в противном случае файл просто не будет доступен внутри этой файловой системы, иначе говоря, не будет существовать.

1. Российские операционные системы.

Astra Linux

Astra Linux — российская сборка Linux (изначально создана на базе Debian), разработанная для силовиков и спецслужб. Она отличается высочайшим уровнем защиты и сертифицирована для работы со сведениями, содержащими государственную тайну. Для пущего патриотизма все релизы названы в честь городов-героев России.

Сейчас актуальны «Орел» — версия для повседневных офисных, простите, конторских задач и «Смоленск» для работы со сведениями категории «Совершенно секретно». Готовится к выходу «Новороссийск» — мобильная версия ОС для смартфонов и планшетов с ARM-процессорами.

С технической точки зрения «Астра» отличается от всех других Linux-систем собственной запатентованной системой разграничения доступа, а также имеет ряд других функций защиты данных — например, при удалении файла он удаляется полностью и место, которое занимал, заполняется случайными маскирующими последовательностями данных (в других ОС по умолчанию меняется лишь запись в FAT, и для того, чтобы удаленный файл нельзя было прочитать посекторным чтением накопителя, используют специальные утилиты).

ПО для спецслужб

«Заря» — еще одна сборка Linux специального назначения (на базе Red Hat), она используется исключительно в российской армии и существует в виде нескольких сборок — для рабочих станций, для ЦОД, для специализированных компьютеризированных комплексов и т.п.

Также существует МСВС — «Мобильная система Вооруженных Сил» и GosLinux — ОС для Федеральной службы судебных приставов (тоже на базе Red Hat). По последней есть статистика: она установлена на 660 серверов и 16 тыс. рабочих станций, при этом стоимость копии в пересчете на один компьютер оказалась равна 1500 рублей. По мере установки на большее число ПК к концу 2016 года (тогда она будет установлена на половине компьютеров ФССП) средняя стоимость снизится до 800 рублей. В любом случае это в несколько раз дешевле лицензий на Windows и MS Office.

«Эльбрус»

«Эльбрус» — операционная система для компьютеров с российскими процессорами с аналогичным названием. Поскольку процессоры эти, хоть и совместимы с x86, имеют собственную уникальную архитектуру, решили разработать специальную ОС — опять же, на ядре Linux — которая учитывает особенности ЦП и максимально эффективно использует их преимущества.

ПО с нуля

Все вышеперечисленные операционные системы, к сожалению, не являются полностью российскими разработками, поскольку это различные вариации на тему зарубежного Linux. Однако есть у нас и полностью своя ОС под названием «Фантом», разработанная с нуля.

Одна из ключевых особенностей «Фантома» — это персистентность, что означает, что приложения работают без остановки и даже «не знают» о том, что компьютер был выключен или перезагружен — работа продолжается ровно с того же момента. Это чем-то похоже на режим «гибернации» в других системах (когда содержимое памяти записывается на диск в виде файлов и затем загружается), но гарантированно работает без сбоев драйверов и программ, и все происходит автоматически. Даже если внезапно обесточить компьютер, данные не пропадут и после повторного включения все будет так же, как за несколько секунд до выключения.

Проблема «Фантома» только одна: под него нужно писать (или портировать из Unix-систем) прикладное ПО, а тут возникает проблема курицы и яйца: пока не будет хоть какого-то проникновения ОС, никто не захочет писать под нее программы, а пока нет программ — не будет проникновения.

Практические задания

Задание 1.

Задача №5. Пусть в вычислительную систему поступают пять процессов различной длительности. Вычислить среднее время ожидания и среднее время выполнения процесса при использовании алгоритма планирования RR (Round Robin) с квантом времени равным 3.

|  |  |
| --- | --- |
| Номер процесса | Время выполнения |
| 1 | 8 |
| 2 | 3 |
| 3 | 4 |
| 4 | 2 |
| 5 | 1 |

Среднее время ожидания: 7.0.

Среднее время выполнения: 10.6.

Задание 2.

4. Вы работаете на компьютере с 4-х байтовым машинным словом. С каким шагом меняются адреса машинных слов?

Адрес - это номер группы битов. В современных компьютерах адресуются байты (группы по 8 бит). Но возможна модификация адреса - в команде присутствует признак, что адреса заданы для другой длины группы бит - 32 или даже 64-х битовых слов. Если на компьютере, о котором идёт речь, существует ли байтовая адресация, то адрес каждого следующего слова будет отличаться от адреса предыдущего на 4. Если нет (минимальной адресуемой единицей является 32-х разрядное слово) - то на 1.

18. Программа написана на языке машинных команд и размещается в памяти, начиная с нулевого адреса. Каждая команда занимает в памяти компьютера четырехбайтовое машинное слово. Сколько команд содержит эта программа, если шестнадцатеричный адрес последней команды в программе равен: а) 28, б) 4С.

11 команд. Адрес последней команды 2816=4016 – это адрес байта, с которого начинается последняя команда (именно начинается, так как сказано, что адрес первой команды равен 0 – это адрес первого байта памяти). Значит, предыдущая команда закончилась байтом с адресом 39, и тогда последний байт команды будет иметь адрес 43. А так как адреса отсчитываются с 0, то всего в программе 44 байта, то есть 11 команд.

24. Известно, что для доступа к памяти через таблицу страниц необходимо 90 нс, а для доступа через ассоциативную память – 20 нс. Частота попаданий в ассоциативную память при обращении к данным составляет 80%. Чему равно среднее время обращения к памяти?

0.8\*20+0.2\*90=34 нс.

Задание 3.

1. Сформировать дерево заданной структуры (рис.10).

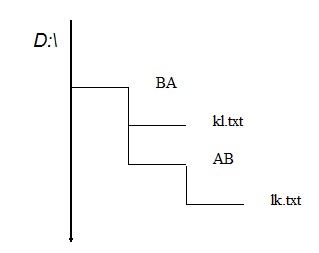


Рисунок 2 - Структура к варианту 10

2. Скопировать файл kl.txt в каталог AB с тем же именем.

3. Слить в каталоге AB файлы в один, результат записать в каталог BA с именем kllk.txt.

4. Просмотреть содержимое файла kllk.txt.

5. Скопировать файл kllk.txt в каталог AB с именем lkkl.txt.

6. Установить файлу lkkl.txt атрибут «скрытый».

7. Получить графическое представление полученной структуры.

Листинг

D:

Mkdir ba

Cd ba

Mkdir ab

Echo “Hello world” >> kl.txt

Cd ab

Echo “Hello all” >> lk.txt

Copy D:\ba\kl.txt D:\ba\ab\kl.txt

Copy kl.txt+lk.txt D:\ba\kllk.txt

Cd..

Type kllk.txt

Copy kllk.txt C:\ba\ab\lkkl.txt

Cd ab

Attrib +h lkkl.txt

Tree c:\ba /f