

Лабораторная работа №3

Защита реестра ОС Windows. Ограниченное использование программ

1. Реестр Windows

Реестр – централизованная база данных, которая хранит все параметры настройки системы и работающих в ней приложений. В этом смысле реестр аналогичен ini-файлам, а также файлам autoexec.bat и config.sys, которые использовались в ранних версиях Windows. Помимо этого в реестре хранится информация о всех имеющихся аппаратных средствах, системная информация OLE, информация о конфигурации сетевых параметров, а также о связях расширений имен файлов.

Реестр содержит разделы (ключи) и параметры. Разделы реестра представляют собой контейнеры, в состав которых могут входить как вложенные разделы, так и параметры. Разделы, находящиеся на верхнем уровне этой иерархической структуры, называются корневыми разделами.

Реестр Windows NT/2000/XP состоит из пяти корневых разделов:

- 1. HKEY_CLASSES_ROOT** – содержит ассоциации между приложениями и типами файлов, информацию OLE, параметры совпадают с параметрами, расположенными в HKEY_LOCAL_MACHINE\Software\Classes;
- 2. HKEY_CURRENT_USER** – содержит пользовательский профиль пользователя, на данный момент зарегистрированного в системе, включая переменные окружения, настройку рабочего стола, параметры настройки сети, принтеров и приложений;
- 3. HKEY_LOCAL_MACHINE** – содержит глобальную информацию 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 составе этого ключа, действует применительно ко всем пользователям, зарегистрированным в системе Windows;
- 4. HKEY_USERS** – содержит все активно загруженные пользовательские профили, включая HKEY_CURRENT_USER, а также профиль по умолчанию. Ключ HKEY_USERS содержит вложенный ключ .\Default, а также другие ключи, определяемые идентификатором безопасности (SID) каждого пользователя;
- 5. HKEY_CURRENT_CONFIG** – содержит конфигурационные данные для текущего аппаратного профиля.

Все данные реестра хранятся в файлах, которые располагаются в каталогах %SystemRoot%\System32\Config и %SystemDrive%\Documents and Settings\UserName.

Для просмотра и редактирования реестра в Windows XP предусмотрен стандартный компонент: regedit.exe. Появившееся окно разделено на две области. Левая панель отображает иерархию реестра, организованную в виде ветвей (разделов) и вложенных ветвей. В правой панели отображаются текущие параметры выбранного ключа реестра. Каждый параметр характеризуется именем, отображаемым в столбце **Name(Имя)**, типом данных, отображаемых в панели **Type(Тип)**, и значением, отображаемом в столбце **Data(Значение)**. Для создания раздела необходимо в левой панели редактора реестра выбрать ключ, в котором вы хотите создать новый ключ, и затем выбрать пункт меню «Правка -> Создать -> Раздел» или пункт контекстного меню «Создать -> Раздел» и ввести название раздела.

2. Обеспечение безопасности реестра

Редактирование реестра осуществляется с помощью системной утилиты regedit.

Программа regedit позволяет:

- 1) Устанавливать владельца и права доступа на ключи реестра.
- 2) Установить аудит на доступ к отдельным ключам реестра.

Для того, чтобы установить владельца или права доступа на ключ реестра выберите в левой панели интересующий вас ключ и выполните пункт меню **«Разрешения...»**. Нажав на кнопку **«Дополнительно»** мы попадаем в следующее окно с дополнительными настройками безопасности. Для добавления нового разрешения необходимо на вкладке **«Разрешения»** нажать на кнопку **«Добавить»**. В поле имени следует ввести имя пользователя, для которого необходимо настроить разрешения и нажать **«ОК»**. Установив соответствующие галочки на разрешении или запрете каких-либо действий, вы можете настроить доступ к выбранному ключу.

Для смены владельца выберите в левой панели интересующий вас ключ и выполните пункт меню **«Разрешения...»**. Нажав на кнопку **«Дополнительно...»** мы попадаем в окно с дополнительными настройками безопасности. Далее, перейдя на вкладку **«Владелец»**, мы попадаем в окно редактирования прав владельца на ключ. В этом окне указан текущий владелец, а также пользователи, которые могут стать владельцами. Для изменения владельца выберете желаемого владельца и нажмите **«Применить»**.

3. Аудит ключей реестра

Для установки аудита на ключи реестра, необходимо активизировать аудит. Для этого в меню Пуск выбрать **«Панель Управления -> Администрирование -> Локальная политика безопасности»**. В появившейся оснастке ММС в левой части экрана выбрать **«Политика аудита»**. В правой части экрана выполнить двойной щелчок мыши на одном из элементов и в появившемся окне установить аудит как минимум на пункте **«Аудит доступа объектов»(Audit Object Access)**. Далее можно установить аудит на необходимые действия с ключами реестра. Для этого в редакторе реестра в левой панели выберите необходимый ключ и выберите пункт меню **«Разрешения...»**. Нажав на кнопку **«Дополнительно...»** мы попадаем в окно с дополнительными настройками безопасности. Далее, перейдя на вкладку **«Аудит»**, мы попадаем в окно редактирования событий аудита на ключ. Для добавления события нажимаем кнопку **«Добавить»** и в появившемся окне вводим необходимое имя пользователя и нажимаем **«ОК»**. Далее нажимаем **«ОК»** и для применения изменений на главном окне аудита нажимаем кнопку **«Применить»**.

Для того, чтобы просмотреть результаты аудита нажмите правой кнопки мыши на пиктограмме **«Мой компьютер»** и выберите в появившемся меню **«Управление»**. Выбираем пункт **«Просмотр событий -> Безопасность»**. В результате появится журнал событий, в котором с помощью фильтра можно выбрать соответствующие записи.

4. Редактирование реестра из командной строки

Редактирование реестра из командной строки можно осуществлять с помощью системной утилиты reg.exe:

REG <Операция> [Список параметров]

<Операция> == [QUERY | ADD | DELETE | COPY | SAVE | LOAD | UNLOAD | RESTORE |
COMPARE | EXPORT | IMPORT]

Код возврата: (за исключением REG COMPARE): 0 – Успешно, 1 - С ошибкой.

1. REG QUERY Раздел [/v Параметр | /ve] [/s]

Раздел - Имя раздела в формате: [\\Компьютер]Путь Компьютер Имя удаленного компьютера, если оно опущено, то по умолчанию считается равным имени локального компьютера. Для удаленных компьютеров доступны только HKLM и HKU.

Путь - Полный путь к разделу реестра в виде: КОРЕНЬ\Подраздел

КОРЕНЬ - Корневой раздел. Значения: [HKLM | HKCU | HKCR | HKU | HKCC]

Подраздел - Полный путь к разделу реестра в выбранном корневом разделе

/v - Запрос указанного раздела реестра

Параметр - Имя запрашиваемого параметра в указанном разделе. Если опущено, будут запрошены значения всех параметров.

/ve - Запрос стандартного параметра с пустым именем.

/s - Запрос всех подразделов и их параметров.

Примеры:

1) REG QUERY HKLM\Software\Microsoft\ResKit /v Version

Отображает значение параметра Version в реестре

2) REG QUERY HKLM\Software\Microsoft\ResKit\Nt\Setup /s

Отображает все подразделы и параметры в разделе Setup реестра.

2. REG ADD <раздел> [/v <параметр> | /ve] [/t <тип>] [/s <разделитель>] [/d <данные>] [/f] <раздел> [\\<компьютер>]\<путь>

<компьютер> - Имя удаленного компьютера, если оно опущено, то по умолчанию считается равным имени локального компьютера. На удаленных компьютерах доступны только разделы HKLM и HKU.

<путь> - Полный путь к разделу реестра в виде КОРЕНЬ\Подраздел.

<КОРЕНЬ> - Корневой раздел. Значения [HKLM | HKCU | HKCR | HKU | HKCC].

<подраздел> - Полный путь к разделу реестра в выбранном корневом разделе.

/v - Имя добавляемого параметра в указанном разделе.

/ve - Добавить пустой параметр (По умолчанию) в указанный раздел.

/t - Типы данных.

[REG_SZ | REG_MULTI_SZ | REG_DWORD_BIG_ENDIAN |
REG_DWORD | REG_BINARY | REG_DWORD_LITTLE_ENDIAN |
REG_NONE | REG_EXPAND_SZ]

По умолчанию, считается равным REG_SZ.

/s - Определяет разделитель, который используется для разделения данных в многострочных параметрах типа REG_MULTI_SZ. По умолчанию, считается равным "\".

/d - Значение, присваиваемое добавляемому параметру реестра.

/f - Принудительно перезаписывать существующие записи реестра без предупреждения.

Примеры:

1) REG ADD \\ABC\HKLM\Software\MyCo

Добавляет раздел HKLM\Software\MyCo на удаленный компьютер ABC

2) REG ADD HKLM\Software\MyCo /v Data /t REG_BINARY /d fe340ead

Добавляет параметр с именем: Data, типом: REG_BINARY, и значением: fe340ead

3) REG ADD HKLM\Software\MyCo /v MRU /t REG_MULTI_SZ /d fax\0mail

Добавляет параметр с именем: MRU, типом: REG_MULTI_SZ, и значением: fax\0mail\0\0

4) REG ADD HKLM\Software\MyCo /v Path /t REG_EXPAND_SZ /d %%systemroot%%

Добавляет параметр с именем: Path, типом: REG_EXPAND_SZ, и значением:

%systemroot%

Примечание: Используйте в строке двойные символы процента (%%)

3. REG DELETE <раздел> [/v <параметр> | /ve | /va] [/f]

<раздел> - Имя раздела в формате: [\\Компьютер]Путь

<компьютер> - Имя удаленного компьютера, если оно опущено, то по умолчанию считается равным имени локального компьютера. Для удаленных компьютеров доступны только HKLM и HKU.

<путь> - Полный путь к разделу реестра в виде: КОРЕНЬ\Подраздел
<КОРЕНЬ> - Корневой раздел. Значения: [HKLM | HKCU | HKCR | HKU | HKCC]
<подраздел> - Полный путь к разделу реестра в выбранном корневом разделе.
<параметр> - Имя удаляемого параметра в указанном разделе. Если опущено, из указанного раздела будут удалены все подразделы и параметры.
/ve - Удалять безымянные параметры.
/va - Запрашивать все параметры данного раздела.
/f - Удалять принудительно, без дополнительного предупреждения.

Примеры:

- 1) REG DELETE HKLM\Software\MyCo\MyApp\Timeout
Удаляет раздел реестра Timeout и все его подразделы и параметры.
- 2) REG DELETE \\ZODIAC\HKLM\Software\MyCo /v MTU
Удаляет параметр MTU из раздела MyCo реестра на компьютере ZODIAC.

4. REG COPY <раздел1> <раздел2> [/s] [/f]

/s - Копировать все подразделы и параметры.

/f - Принудительное копирование без дополнительного предупреждения.

Примеры:

- 1) REG COPY HKLM\Software\MyCo\MyApp HKLM\Software\MyCo\SaveMyApp /s
Копирует все подразделы и параметры раздела MyApp в раздел SaveMyApp
- 2) REG COPY \\ZODIAC\HKLM\Software\MyCo HKLM\Software\MyCo1
Копирует все параметры раздела MyCo с компьютера ZODIAC в раздел MyCo1 на локальном компьютере

5. REG SAVE <раздел> <имя Файла>

<имя Файла> - Имя сохраняемого файла на диске. Если путь не указан, файл создается вызывающим процессом в текущей папке.

Пример:

REG SAVE HKLM\Software\MyCo\MyApp AppBkUp.hiv

Сохраняет раздел MyApp в файле AppBkUp.hiv в текущей папке.

6. REG RESTORE <раздел> <имя файла>

<имя файла> - Имя файла сохраненного раздела для его восстановления.

Для создания таких файлов используйте команду REG SAVE.

Пример:

REG RESTORE HKLM\Software\Microsoft\ResKit NTRKBkUp.hiv

Восстанавливает подраздел ResKit из файла NTRKBkUp.hiv перезаписывая текущие подразделы и параметры

7. REG LOAD <раздел> <имя файла>

<раздел> - Полный путь к разделу реестра в виде: КОРЕНЬ\Подраздел (только для локального компьютера).

<КОРЕНЬ> Возможные значения для корневого раздела: [HKLM | HKU].

<подраздел> Имя нового раздела в который будет загружен сохраненный ранее файл куста реестра.

<имя файла> Имя загружаемого файла куста реестра. Для создания этого файла используйте команду REG SAVE.

Пример:

REG LOAD HKLM\TempHive TempHive.hiv

Загружает файл TempHive.hiv в раздел HKLM\TempHive

8. REG COMPARE <раздел1> <раздел2> [/v <параметр> | /ve] [<вывод>] [/s]

<параметр> - Имя параметра в указанном разделе, для сравнения. Если опущен, будут сравниваться все параметры раздела.

/ve - Сравнивать безымянные параметры.

/s - Сравнивать все подразделы и параметры.

<вывод> - Одно из значений: [/oa | /od | /os | /on].

Если не указано, используется значение /od.

/oa - Выводить и совпадения, и отличия.

/od - Выводить только отличия.

/os - Выводить только совпадения.

/on - Не выводить результаты сравнения.

Код возврата:

0 - Успешно, сравниваемые данные идентичны

1 - При обработке произошла ошибка

2 - Успешно, сравниваемые данные отличаются

Примеры:

1) REG COMPARE HKLM\Software\MyCo\MyApp HKLM\Software\MyCo\SaveMyApp

Сравнивает все параметры раздела MyApp с параметрами раздела SaveMyApp

2) REG COMPARE HKLM\Software\MyCo HKLM\Software\MyCo1 /v Version

Сравнивает значение параметра Version в разделах MyCo и MyCo1

3) REG COMPARE \\ZODIAC\HKLM\Software\MyCo \\. /s

Сравнивает все подразделы и значения параметров в разделе HKLM\Software\MyCo реестра на компьютере ZODIAC с аналогичным разделом на локальном компьютере

9. REG EXPORT <раздел> <имя файла>

<имя файла> - Имя файла на диске для экспорта.

Пример:

REG EXPORT HKLM\Software\MyCo\MyApp AppBkUp.reg

Экспортирует все подразделы и значения параметров раздела MyApp в файл AppBkUp.reg

10. REG IMPORT <имя файла>

<имя файла> Имя файла для импорта (только на локальном компьютере).

Пример:

REG IMPORT AppBkUp.reg

Импортирует записи реестра из файла AppBkUp.reg

5. Политика ограниченного использования программ (SAFER)

Политика ограниченного использования программ позволяет администратору вводит ограничения на запуск приложений для пользователей. Запуск консоли политики ограниченного использования программ можно осуществить из командной строки, с помощью оснастки Secpol.msc. Первоначально политики ограниченного использования программ находятся в неопределенном состоянии. Первым действием необходимо нажать правую кнопку мыши и в меню выбрать создание новой политики. Политика содержит следующие параметры.

1. Контейнер «Уровни безопасности».

В данном контейнере необходимо выбрать один из объектов, который будет применяться, как правило по умолчанию:

А) «Не разрешено» - программное обеспечение запускаться не будет, вне зависимости от прав доступа пользователя. Для разрешения запуска приложений необходимо создавать дополнительные правила. Политика безопасности по «белому списку».

Б) «Ограниченный» - доступ программ к ресурсам определяется правами пользователя. Для запрета запуска необходимо создавать дополнительные правила. Политика безопасности по «черному списку».

2. Контейнер «Дополнительные правила».

Существует четыре типа дополнительных правил для контроля над запускаемыми процессами. Для выбора правила надо нажать правую кнопку мыши на контейнере «Дополнительные правила».

А) Правила для хеша – идентификация программы по хеш-значению исполняемого кода.

Б) Правило сертификата – контроль над программами по наличию сертификата.

В) Правило для зоны Интернета – контроль над программами .msi по зоне Интернета, из которой они взяты

Г) Правило для пути - контроль над программами по строки пути к исполняемому файлу. Правила задания путей:

1) можно использовать символы * и ?,

2) %USERPROFILE% - означает домашний каталог пользователя.

3. Параметр «Принудительный».

Данный параметр определяет, на какие программы распространяются правила ограниченного использования программ и на каких пользователей.

4. Параметр «Назначенные типы файлов».

Данный параметр определяет, какие файлы (по расширению) считаются исполняемыми.

5. Параметр «Доверенные издатели»

Параметр определяет, кто выбирает доверенных издателей для активных объектов.

Задания к лабораторной работе:

Задание 1. Используя утилиту regedit, выполните следующие действия:

1. В ключе реестра HKEY_CURRENT_CONFIG создайте раздел TMP
2. В разделе TMP создайте строковый параметр username и присвойте ему значение user1.
3. Создайте пользователей user1 и user2. Пользователю user1 предоставьте полный доступ к ключу реестра TMP, а user2 полный запрет на доступ к реестру.
4. Настройте аудит обращений user2 к ключу TMP, а пользователя user1 к параметру username.
5. В сеансе пользователя user1 обратитесь к параметру username, а в сеансе пользователя user2 обратитесь к ключу TMP. Затем в сеансе администратора найдите соответствующие записи в журнале событий.

Задание 2. Реализуйте файл пакетной обработки, выполняющий следующие действия:

1. Записывает в файл reg.txt значение параметра user1 раздела TMP ключа HKEY_CURRENT_CONFIG.
2. Добавляет пустой параметр user2 в раздел TMP ключа HKEY_CURRENT_CONFIG.
3. Удаляет параметр user1 в раздел TMP ключа HKEY_CURRENT_CONFIG.
4. Сохраняет раздел HKEY_CURRENT_CONFIG в файл hcc.hiv

Задание 3. Настройте политику ограниченного использования программ следующим образом:

1. Задайте политику безопасности по «белому списку».
2. Добавьте к исполняемым файлам, файлы с расширением «.isp».
3. Разрешите всем пользователям проверять сертификаты.
4. Запретите по хеш-значению запуск программы «Калькулятор».
5. Запретите установку программ, загруженных из Интернета.
6. Запретите запуск приложений, начинающихся на символ «D», из домашних каталогов пользователей.