Практическое занятие 16. Работа с реестром. Основы работы с reg-файлами.

Цель работы: отработать навыки практической работы с реестром.

Краткие теоретические сведения:

В независимости от того, в каких файлах хранятся данные реестра его логическая структура одинакова для всех ОС Windows. Реестр состоит из пяти разделов:

HKEY_USERS – содержит все активные загруженные профили пользователей компьютера(HKU).

HKEY_CURRENT_USER – корневой раздел конфигурации пользователя, работающего в данный момент. Здесь хранятся установки для папок этого пользователя, цвета экрана и параметры панели управления. Эти сведения сопоставлены с профилем пользователя. Вместо полного имени раздела иногда используется аббревиатура HKCU; раздел HKEY_CURRENT_USER является подразделом раздела HKEY_USERS;

HKEY_LOCAL_MACHINE – содержит параметры конфигурации, относящиеся к данному компьютеру (для всех пользователей). Вместо полного имени раздела иногда используется аббревиатура HKLM;

HKEY_CLASSES_ROOT – подраздел HKEY_LOCAL_MACHINE\Software. Хранящиеся здесь сведения отвечают за запуск необходимой программы при открытии файла с помощью проводника. Вместо полного имени раздела иногда используется аббревиатура HKCR;

HKEY_CURRENT_CONFIG – раздел содержит сведения о профиле оборудования, используемом локальным компьютером при запуске системы.

Порядок выполнения работы:

1. Запустить виртуальную машину с ОС Windows 10 и активировать справочное меню (Пуск | Справка и поддержка).
2. Ознакомиться с описанием Реестра и возможностями его применения в ОС Windows.
3. Ознакомиться с описанием и возможностями служебного программного средства «Редактор Реестра» (Regedit), изучив справочный материал по данному приложению, находящийся в системном каталоге C:\Windows\Help\ в одноименном файле с расширением .chm.

4. В появившемся окне «Редактора Реестра», обратите внимание на то, что с левой стороны окна расположена панель ключей, а с правой стороны – панель значений.

5. Самостоятельно выберите в Реестре ОС какой-либо ключ (с соответствующими подключами), содержащий одновременно значения с основными системными типами **REG_BINARY**, **REG_DWORD** и **REG_SZ**. Обратите внимание на имеющуюся в редакторе возможность представления данных выбранного значения в двоичном виде (команда «Вывод двоичных данных» в меню «Вид»). Полученные данные перенесите в отчет.

6. Выберите пункт «Найти…» в меню «Правка». В поле «Найти:» введите строку hivelist («список файлов кустов») в качестве примера текста, который необходимо найти.

7. В диалоговом окне «Изменение параметра DWORD» ключа **HKLM\SYSTEM\CurrentControlSet\Services\Cdrom** при необходимости измените значение параметра **AutoRun** (тип значения REG_DWORD) на 0, тем самым, отключив автозапуск оптического привода.

8. Удалите из Реестра параметры **Optional** и связанный с ним **Posix** в ключе **HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\SubSystems**, щелкнув на них правой кнопкой манипулятора мышь и выбрав команду «Удалить» из появившегося списка команд.

9. Для экспорта ветвей реестра выполните следующие инструкции:

- щелкните мышью на ключе, находящемся в вершине ветви, выбранной самостоятельно, которую необходимо экспортировать;
- в меню «Файл» выберите пункт «Экспорт», чтобы вывести на экран диалоговое окно «Экспорт файла Реестра»;
- в поле «Имя файла» введите имя файла для экспорта;
- выберите диапазон экспорта: чтобы создать копию всего реестра, щелкните на «Весь реестр», чтобы создать копию выделенной ветви, щелкните на «Выбранная ветвь»;
- в выпадающем списке «Тип файла» выберите тип файла для экспорта: «Файлы Реестра *.reg», «Файлы кустов Реестра *.*», «Текстовые файлы *.txt» или «Файлы Реестра Win9x/NT4 *.reg»;

- экспортируйте ветвь, мышью щелкнув на кнопке «Сохранить».

10. Проверить содержимое параметра **HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon** По умолчанию этот параметр имеет значение C:\Windows\system32\userinit.exe Если в значении содержатся дополнительные записи, то это могут быть «**троянские программы**». В этом случае проанализируйте место расположения программы, обратите внимание на время создания файла.

11. Проверить раздел автозапуска **HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\Run.** Проанализируйте записи раздела. Какие программы автоматически запускаются при загрузке Windows.

12. Выделите записи, вызывающие подозрения. Зафиксируйте этапы работы, используя скриншоты (Alt + PrintScreen). Составьте отчет о результатах проверки.

13. Создайте 2 reg-файла: Первый – изменяет 10 любых параметров(ключей) реестра (можно на удаление). Второй – возвращает параметры реестра в исходное состояние.

Форма представления результата:

Отчет по работе (цель, ход работы и вывод) оформите в электронном виде в формате MS Word и прикрепите к заданию (структура - как в тетради). Не забудьте про СКРИНЫ!!!

Формат документа - А4 вертикальной ориентации, поля - 1 см, выравнивание текста - по ширине, абзацный отступ - 1,25 см, шрифт - Times New Roman 12 пт, межстрочный интервал - полуторный. Изображения выравниваются по центру, обтекание текста отсутствует.