***Лабораторная работа 8.***

**Тема: Работа с реестром**

***Цель работы:*** *научиться выявлять* *вредоносные программы с помощью реестра* *Windows.*

**Внимание! Данная лабораторная работа предназначена для опытных пользователей, имеющих навыки работы в реестре. В случае ошибочной правки ключей реестра можно серьезно повредить систему. Рекомендуется выполнять данную лабораторную работу на виртуальной машине под управлением Windows XP.**

**Реестр операционной системы Windows** - это иерархически построенная база данных, где хранится информация о конфигурации системы. Этой информацией пользуются как операционная система Windows, так и другие программы. В некоторых случаях восстановить работоспособность системы после сбоя можно, загрузив работоспособную версию реестра, но для этого, естественно, необходимо иметь копию реестра.

Реестр формируется из различных данных. Чтобы получилось то, что видит пользователь, редактируя реестр, происходит следующее.

Вначале, в процессе установки и настройки Windows, на диске формируются файлы, в которых хранится часть данных относительно конфигурации системы.

Затем, в процессе каждой загрузки системы, а также в процессе каждого входа и выхода каждого из пользователей, формируется некая виртуальная сущность, называемая "реестром" — объект REGISTRY\. Данные для формирования "реестра" частично берутся из тех самых файлов (Software, System …), частично из информации, собранной ntdetect при загрузке (HKLM\Hardware\Description).

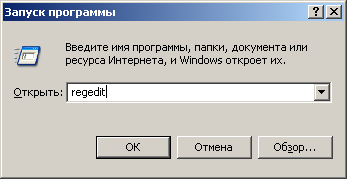
То есть часть данных реестра хранится в файлах, а часть данных формируется в процессе загрузки Windows.

Характеристики основных разделов реестра представлены в таблице 1.

|  |  |
| --- | --- |
| Таблица 1. | |
| **HKEY\_LOCAL\_MACHINE\SAM** | Содержит информацию SAM (Security Access Manager), хранящуюся в файлах SAM, SAM.LOG, SAM.SAV в папке \%System-root%\System32\Confiq |
| **HKEY\_LOCAL\_MACHINE\SECURITY** | Содержит информацию безопасности в файлах SECURITY.SECURITY.LOG, SECURITY.SAV в папке \%Systemroot%\System32\Confiq |
| **HKEY\_LOCAL\_MACHINE\SYSTEM** | Содержит информацию об аппаратных профилях этого подраздела. Информация хранится в файлахSYSTEM.SYSTEM.LOG, SYSTEM.SAV в папке \%Systemroot%\System32\Config |
| **HKEY\_CURRENT\_CONFIG** | Содержит информацию о подразделе System этого улья, которая хранится в файлах SYSTEM.SAV и SYSTEM.ALT в папке \%Systemroot%\System32\Config |
| **HKEY\_USERS\DEFAULT** | Содержит информацию, которая будет использоваться для создания профиля нового пользователя, впервые регистрирующегося в системе. Информация хранится в файлах DEFAULT, DEFAULT.LOG, DEFAULT.SAV в папке \%Systemroot%\System32\Confiq |
| **HKEY\_CURRENT\_USER** | Содержит информацию о пользователе, зарегистрированном в системе на текущий момент. Эта информация хранится в файлах NTUSER.DAT и - NTUSER.DAT.LOG, расположенных в каталоге \%Systemroot%\Profiles\User name, где User name — имя пользователя, зарегистрированного в системе на данный момент |

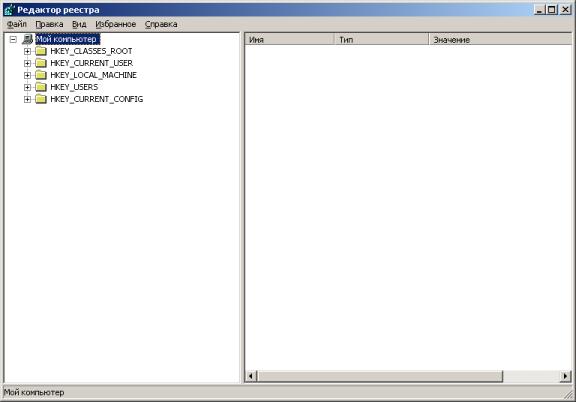
Основным средством для просмотра и редактирования записей реестра служит специализированная утилита **"Редактор реестра"**.

Для того чтобы открыть редактор реестра откройте Пуск->Выполнить. В окне введите **regedit**.



**Рис. 1.**

Откроется окно редактора реестра.

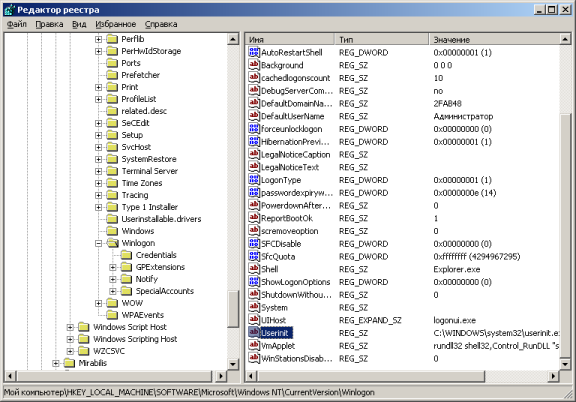


**Рис. 2.**

В левой части окна находится дерево ключей реестра, ключи изображены в виде папок. В правой части окна отображаются записи, относящиеся к выбранному ключу. В ключе могут находиться и записи — параметры настройки, и другие ключи — группы параметров настройки.

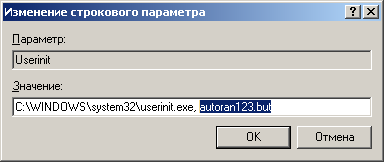
Вредоносные программы, как и любые программы, для работы нуждаются в запуске. Поэтом они часто используют реестр, в частности, его разделы, отвечающие за автоматический запуск программ при загрузке операционной системы.

1. Откройте Редактор реестра.
2. В ветви **HKEY\_LOCAL\_MACHINE** выберите **Software\ Microsoft\WindowsNT\CurrentVersion\Winlogon.**
3. В правой половине окна появится список ключей для данной ветви. Найдите ключ **Userinit** и проверьте его содержимое.



**Рис. 3.**

Нормальным значением данного ключа является запись **C:\WINDOWS\system32\userinit.exe** . Наличие в ключе других записей может свидетельствовать о наличии на компьютере вредоносных программ. Для удаления из ключа подозрительной записи щелкните на нем два раза левой кнопкой мыши. После редактирования нажмите ОК.



**Рис. 4.**

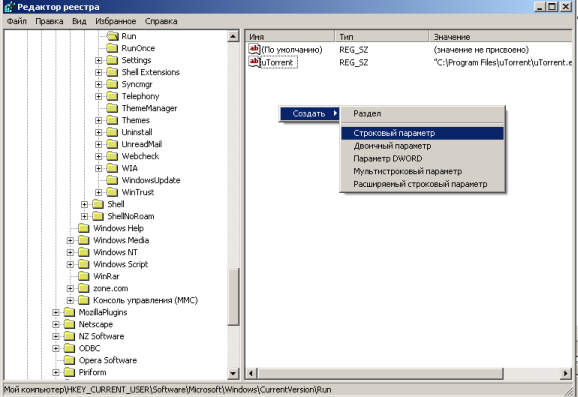
Далее перейдите в папку, где находится подозрительный файл и удалите его вручную. После этого перезагрузите систему. Если после перезагрузки в ключе удаленное значение не появилось снова – система вылечена.

Как уже говорилось выше, любимым местом вредоносных программ являются разделы реестра, отвечающие за автозапуск.

В реестре автозагрузка представлена в нескольких местах:

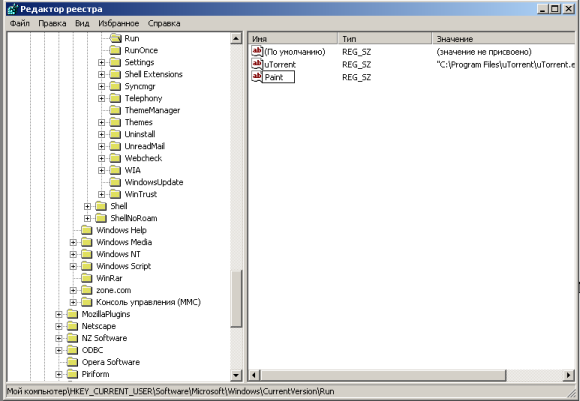
* + **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run** - программы, которые запускаются при входе в систему. Данный раздел отвечает за запуск программ для всех пользователей системы.
  + **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce** - программы, которые запускаются только один раз при входе пользователя в систему. После этого ключи программ автоматически удаляются из данного раздела реестра. Данный раздел отвечает за запуск программ для всех пользователей системы.
  + **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx** - программы, которые запускаются только один раз, когда загружается система. Этот раздел используется при инсталляции программ, например для запуска настроечных модулей. После этого ключи программ автоматически удаляются из данного раздела реестра. Данный раздел отвечает за запуск программ для всех пользователей системы.
  + **HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run** - программы, которые запускаются при входе текущего пользователя в систему
  + **HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce** - программы, которые запускаются только один раз при входе текущего пользователя в систему. После этого ключи программ автоматически удаляются из данного раздела реестра.
  + **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices** - программы, которые загружаются при старте системы до входа пользователя в Windows.
  + **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServicesOnce** - программы отсюда загружаются только один раз, когда загружается система.

1. Откройте Редактор реестра
2. Откройте следующий раздел HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run
3. В правой части окна вызовите правой кнопкой мыши контекстное меню и выберите Создать->Строковый параметр



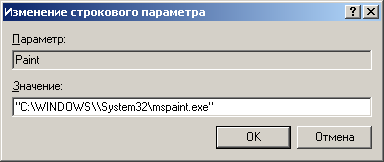
**Рис. 5.**

1. Задайте имя для создаваемого параметра.



**Рис. 6.**

1. Откройте вновь созданный параметр и задайте ему значение в виде пути к исполняемому файлу Paint - **C:\WINDOWS\\System32\mspaint.exe**

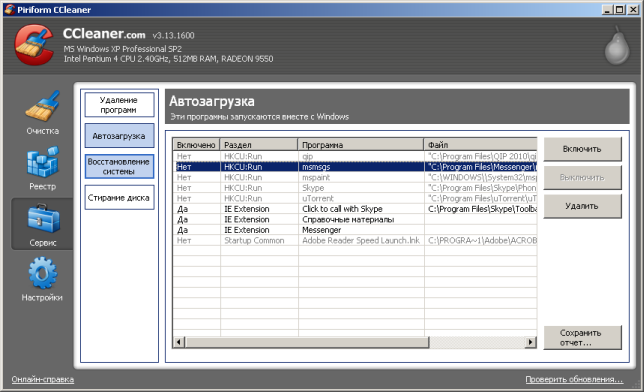


**Рис. 7.**

1. Нажмите ОК и перезагрузите компьютер. Paint загрузится автоматически после загрузки операционной системы.

Помимо **regedit** реестр можно править с помощью специальных программ сторонних производителей. Одна из наиболее распространенных программ называется **CCleaner**. Она бесплатная и имеет достаточно простой интерфейс. Скачать ее можно здесь : [http://www.piriform.com/ccleaner](http://www.intuit.ru/studies/courses/2291/591/lecture/23.http:/www.piriform.com/ccleaner) или здесь [http://www.ccleaner.org.ua/download](http://www.intuit.ru/studies/courses/2291/591/lecture/23.http:/www.ccleaner.org.ua/download).Скачайте и установите программу на виртуальной машине.

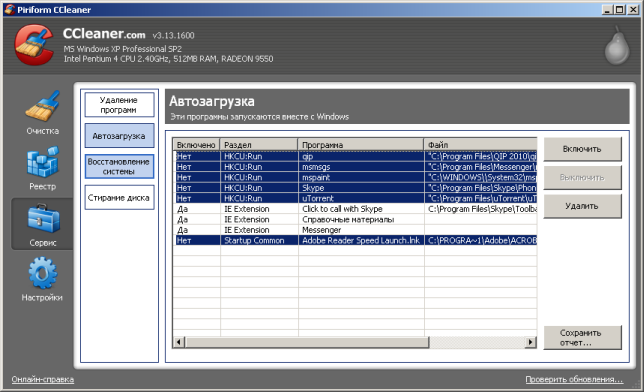
Откройте программу CCleaner. В левом меню выберите **Сервис** и откройте вкладку **Автозагрузка**.



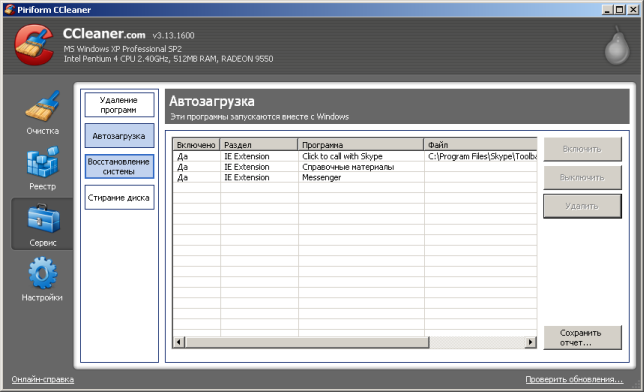
**Рис. 8.**

Здесь показаны программы, которые запускаются или запускались вместе с Windows. В столбце "Включено" отображен статус программы на данный момент. Если Вы хотите удалить программу из автозагрузки, выберите ее и нажмите на кнопку Удалить.

Можно выбрать несколько программ сразу, как показано на рис. 9.



**Рис. 9.**



**Рис. 10.**

Здесь также можно включить и выключить программы с помощью соответствующих кнопок на правой панели. Попробуйте самостоятельно добавить программу "Блокнот" в автозагрузку (поместив ярлык в папку Автозагрузки) и удалить ее с помощью CCLeaner.