

Университет ИТМО
Факультет программной инженерии и компьютерной техники

Лабораторная работа №3
по дисциплине «Информационная безопасность»
Вариант 6

Выполнил: Ларочкин Г.И
Группа: Р3400
Преподаватель: Маркина Т.А.

Санкт-Петербург
2021 г.

Оглавление

Цель	3
Постановка задачи	3
Программные и аппаратные средства	3
Основная часть.....	4
1. Права веток и ключей	4
2. Резервного копирования реестра	4
3. Ключи реестра с различным параметром системы	5
4. Настройка аудита реестра.....	6
5. Аналоги Regedit	9
Вывод.....	10

Цель

Изучить объекты реестра, ознакомиться с основными принципами управления доступом к объектам реестра. Изучить основные способы настройки доступа к реестру.

Постановка задачи

1. Какие конкретно ветки и ключи доступны
 - a) Пользователю хотя бы на чтение
 - b) только Администратору
 - c) только System.
2. Опишите в отчете способ резервного копирования реестра
3. Укажите ключ, который отвечает за указанный параметр системы
 - a. Задание классического вида панели управления
 - b. Отображение пароля к сетевым ресурсам
 - c. Автоматическое завершение всех приложений при выключении компьютера.
4. Настройте на аудит какую-либо ветку реестра и проследите появление событий (минимум 5 подразделов)
5. Приведите примеры аналогов Regedit. Приведите плюсы и минусы по сравнению с Regedit (минимум 3)

Программные и аппаратные средства

- Oracle VM VirtualBox 6.1
- Microsoft Windows 10 Pro
- 3GB RAM, 64GB Постоянной памяти
- Intel Core i5-6200U, Nvidia GeForce 940MX

Основная часть

1. Права веток и ключей

Для пользователя доступно на чтение:

HKEY_CLASSES_ROOT**
HKEY_CURRENT_USER**
HKEY_USERS**

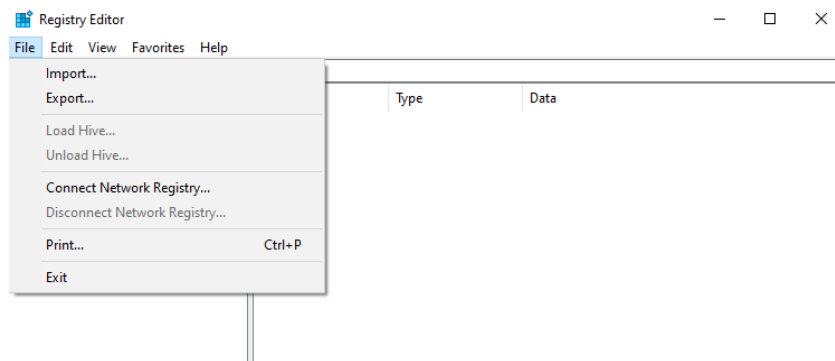
Только для администратора не доступно ничего

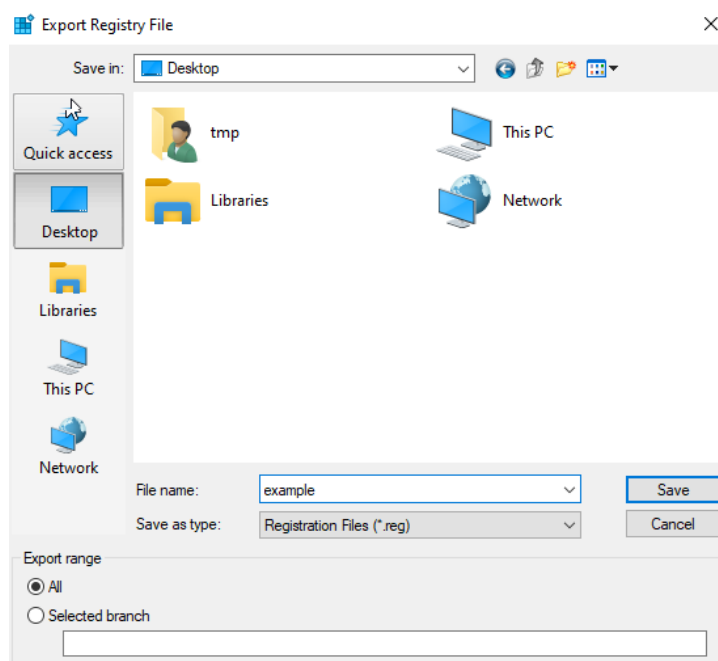
Только для System

HKEY_LOCAL_MACHINE\SAM
HKEY_LOCAL_MACHINE\SECURITY

2. Резервное копирование реестра

1. Открываем regedit.msc
2. File -> Export
3. Выбираем путь и имя файла .reg
4. Ожидаем завершения (regedit может показать Not response в это время)

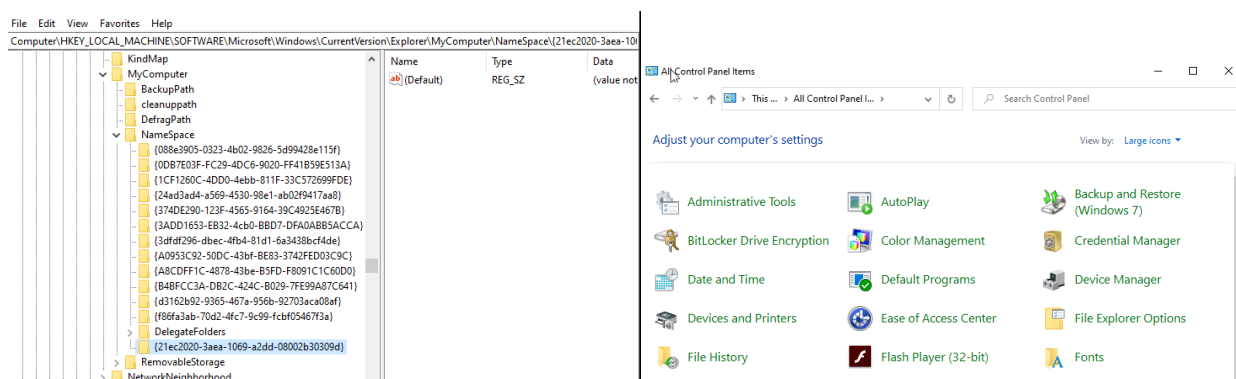




3. Ключи реестра с различным параметром системы

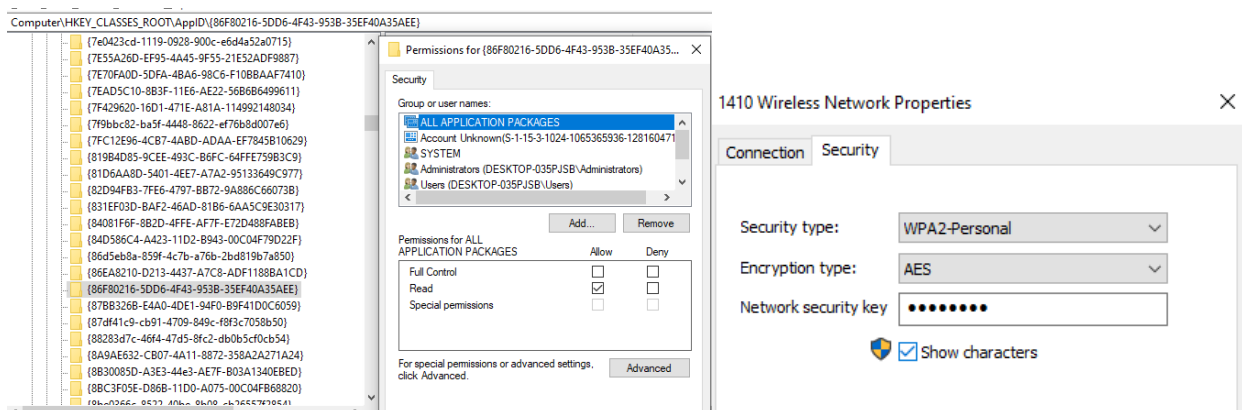
Классическая панель управления

1. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\MyComputer\NameSpace
2. Добавляем ключ *{21ec2020-3aea-1069-a2dd-08002b30309d}* для добавления классической панели с большими иконками



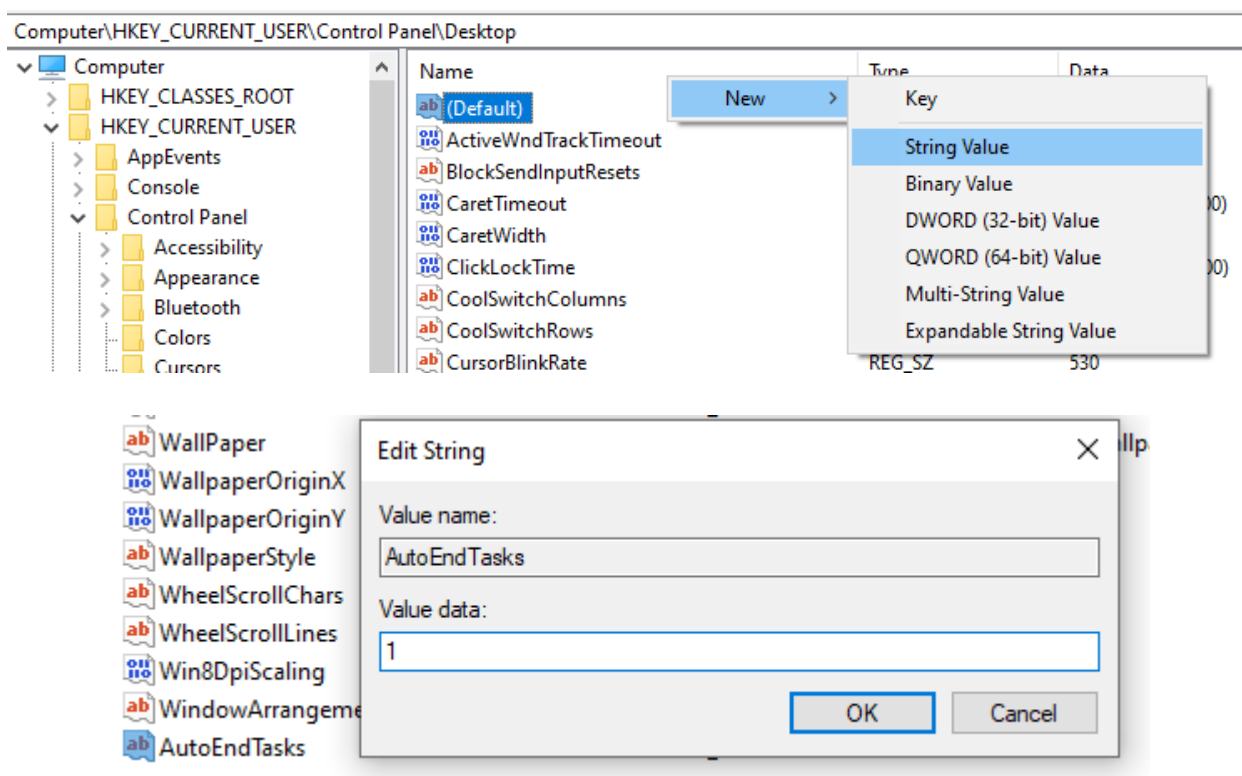
Отображение сетевого пароля

За это отвечает ключ HKEY_CLASSES_ROOT\AppID\{86f80216-5dd6-4f43-953b-35ef40a35aee}. Если его удалить, то не будет отображения сетевого пароля.



Автоматическое завершение задач

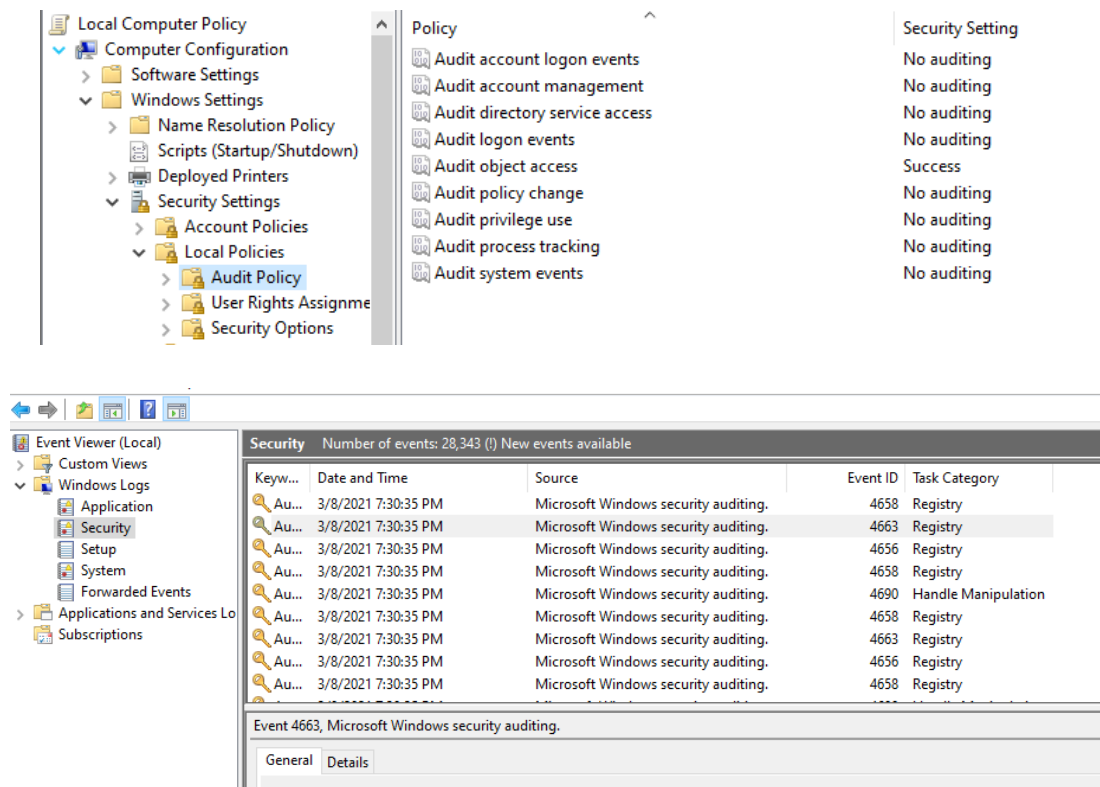
За это отвечает значение *AutoEndTasks* (0 или 1) у *HKEY_CURRENT_USER\Control Panel\Desktop*



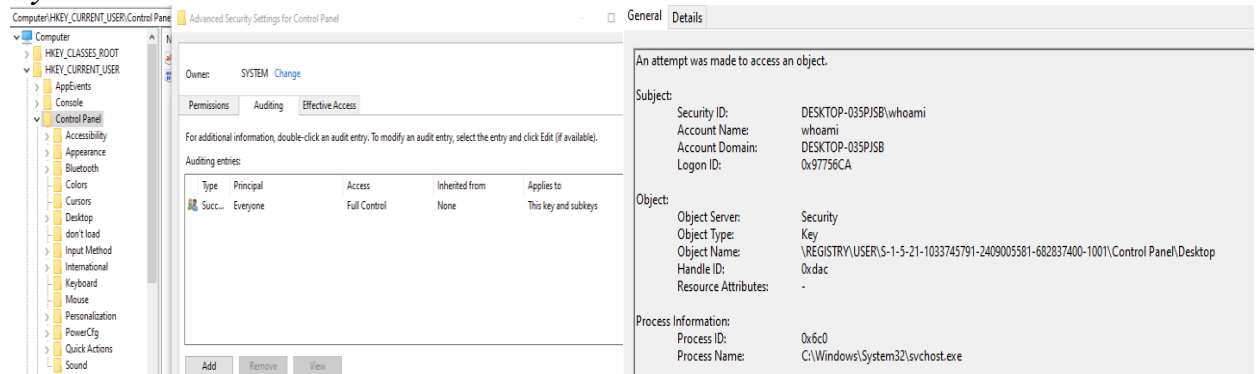
4. Настройка аудита реестра

1. Win+R -> gpedit.msc
2. Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Audit Policy
3. Меняем Audit object access на Success
4. Для просмотра аудита используется Event Viewer: Windows Logs -> Security

5. Для аудита ветки: regedit.msc -> ПКМ по ветке -> Permissions -> Advanced -> Auditing -> Добавляем субъектов для аудита



Aydam Control Panel



Аудит программы Bandicam

The screenshot shows the Windows Security Event Viewer with the 'Auditing' tab selected. The left pane shows the tree structure: Computer\HKEY_CURRENT_USER\SOFTWARE\BANDISOFT\BANDICAM. The right pane shows the 'Auditing entries' table with one entry: 'Success' for 'Everyone' with 'Full Control' access. The 'Details' pane on the right shows the event details for 'An attempt was made to access an object'. The subject is 'DESKTOP-035PJSB\whoami'. The object is 'Security' with 'Key' type and 'Object Name' '\REGISTRY\USER\S-1-5-21-1033745791-2409005581-682837400-1001\SOFTWARE\BANDISOFT\BANDICAM\OPTION'. The process information shows 'Process ID: 0x210c' and 'Process Name: C:\Program Files (x86)\Bandicam\bdcam.exe'.

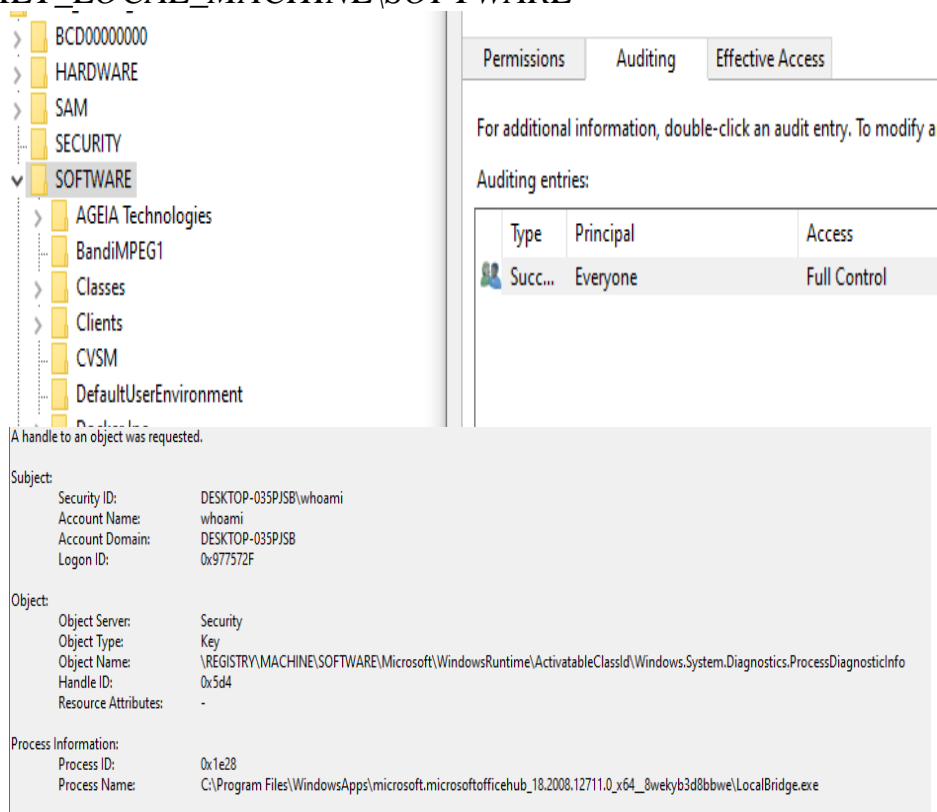
Аудит раскладки клавиатуры

The screenshot shows the Windows Security Event Viewer with the 'Auditing' tab selected. The left pane shows the tree structure: Computer\HKEY_USERS\DEFAULT\Keyboard Layout. The right pane shows the 'Auditing entries' table with one entry: 'Success' for 'Everyone' with 'Full Control' access. The 'Details' pane on the right shows the event details for 'An attempt was made to access an object'. The subject is 'DESKTOP-035PJSB\whoami'. The object is 'Security' with 'Key' type and 'Object Name' '\REGISTRY\USER\S-1-5-21-1033745791-2409005581-682837400-1001\Keyboard Layout\Substitutes'. The process information shows 'Process ID: 0x311c' and 'Process Name: C:\Windows\ImmersiveControlPanel\SystemSettings.exe'.

Аудит консоли Git Bash

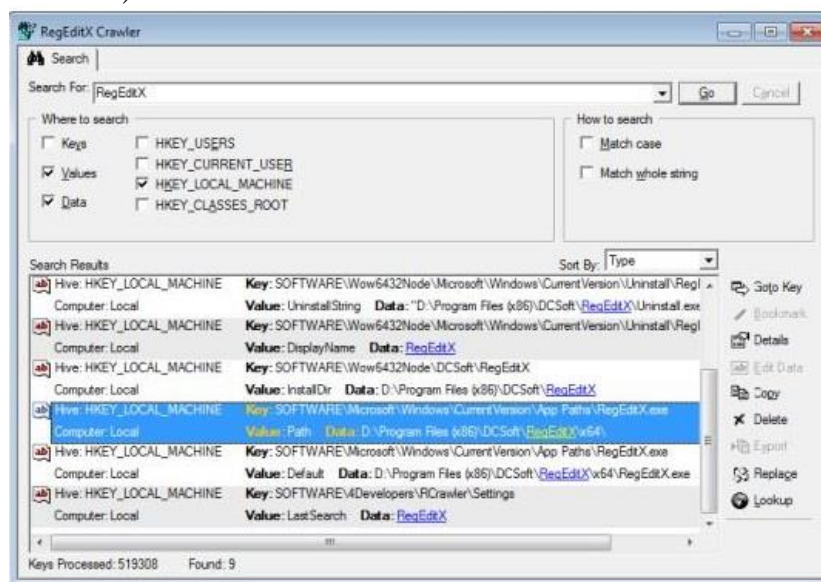
The screenshot shows the Windows Security Event Viewer with the 'Auditing' tab selected. The left pane shows the tree structure: Computer\HKEY_CURRENT_USER\Console. The right pane shows the 'Auditing entries' table with one entry: 'Success' for 'Everyone' with 'Full Control' access. The 'Details' pane on the right shows the event details for 'A handle to an object was requested'. The subject is 'DESKTOP-035PJSB\whoami'. The object is 'Security' with 'Key' type and 'Object Name' '\REGISTRY\USER\S-1-5-21-1033745791-2409005581-682837400-1001\Console'. The process information shows 'Process ID: 0x36bc' and 'Process Name: C:\Windows\System32\conhost.exe'.

Аудит HKEY_LOCAL_MACHINE\SOFTWARE



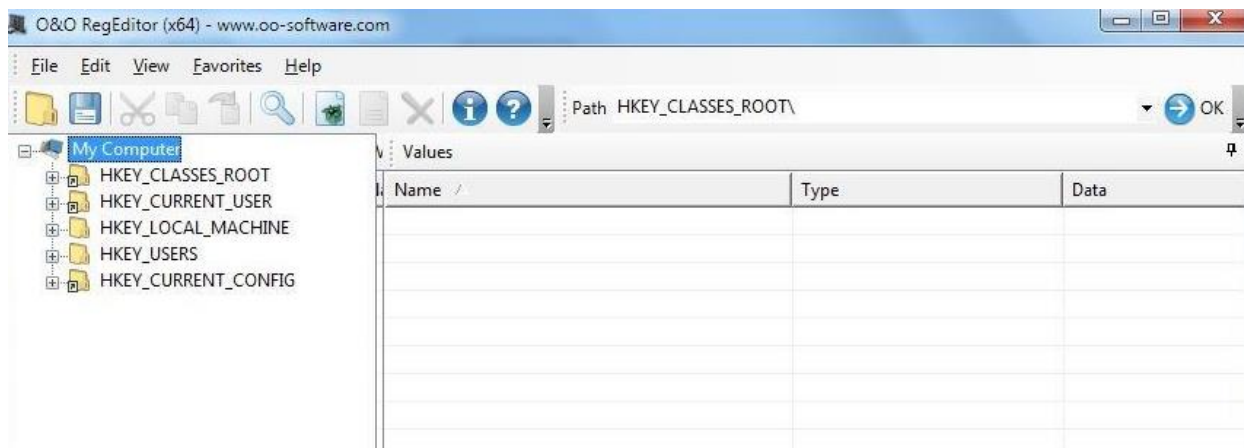
5. Аналоги Regedit

RegEditX (Платный)



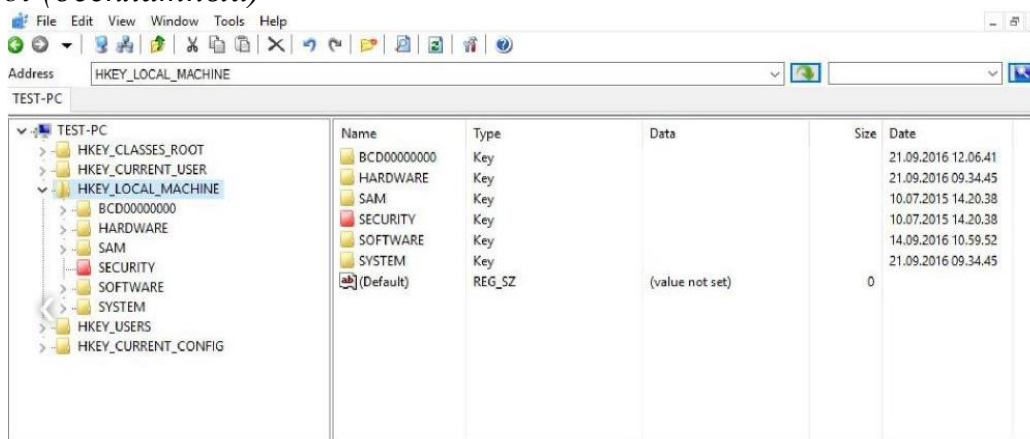
Данный аналог позволяет быстро в реестре. Поиск можно производить по ключам, по данным и по значениям. Для поиска может использоваться регулярное выражение. В поиске подсвечиваются искомые данные. Однако имеет довольно нагруженный.

O & O RegEditor (бесплатный)



Данный редактор имеет главное ключевое преимущество – он позволяет копировать/вставлять значения, а также отменять предыдущие действия. Однако этот редактор не поддерживает Windows Server 2012+

RegCool (бесплатный)



Данный редактор позволяет отменять, повторять действия. Поиск с заменой, сравнение реестров, копирование/вставка. Также позволяет производить оптимизацию реестра (дефрагментирование). Не поддерживает Windows Server.

Вывод

В ходе данной лабораторной работы я изучил работу с реестром windows. Изучил настройки доступа к реестру, а также настройки для аудита.