Федеральное государственное образовательное бюджетное

учреждение высшего образования

**«Финансовый университет при Правительстве Российской Федерации»**

**(Финансовый университет)**

Колледж информатики и программирования

**ОТЧЁТ**

**По лабораторной работе**

**№5**

Дисциплина: Операционные системы

Выполнили студенты

Группы: 2ОИБАС-1322

Студент: Аин Даниил

Преподаватель: Сибирев И.В.

**Москва – 2024г.**

**Цель работы:** изучить программу WinAudit и выполнить с её помощью задания.

**Задание:**

1.Описать что установлено (Все непонятное посмотреть в интернете)

Программы:

* 7-Zip
* Adobe Acrobat
* AIDA64
* S.T.A.L.K.E.R Call Of Chernobyl [by stason174] 6.05
* CCleaner v6.11.10435

2.Обратите внимание на то какие .NET установлены

|  |  |  |
| --- | --- | --- |
| .NET Framework | 4,0,30319,0 | Нет |
| .NET Framework | 2,0,50727,0 | Нет |
| .NET Framework | 2,0,50727,1 | Нет |
| .NET Framework | 4,0,30319,0 | Нет |

3.Получить таблицу групп пользователей(загуглить и разобраться что есть что)

3) Device Owners

|  |  |
| --- | --- |
| **Item** | **Value** |
| Group Type | Local |
| Group Name | Device Owners |
| Comment | Члены этой группы могут изменять параметры на уровне системы. |

4) IIS\_IUSRS

|  |  |
| --- | --- |
| **Item** | **Value** |
| Group Type | Local |
| Group Name | IIS\_IUSRS |
| Comment | Встроенная группа, которую используют службы IIS. |

5) Администраторы

|  |  |
| --- | --- |
| **Item** | **Value** |
| Group Type | Local |
| Group Name | Администраторы |
| Comment | Администраторы имеют полные, ничем не ограниченные права доступа к компьютеру или домену |

6) Администраторы Hyper-V

|  |  |
| --- | --- |
| **Item** | **Value** |
| Group Type | Local |
| Group Name | Администраторы Hyper-V |
| Comment | Члены этой группы имеют полный и неограниченный доступ ко всем функциям Hyper-V. |

7) Гости

|  |  |
| --- | --- |
| **Item** | **Value** |
| Group Type | Local |
| Group Name | Гости |
| Comment | Гости по умолчанию имеют те же права, что и пользователи, за исключением учетной записи "Гость", еще более ограниченной в правах. |

8) Криптографические операторы

|  |  |
| --- | --- |
| **Item** | **Value** |
| Group Type | Local |
| Group Name | Криптографические операторы |
| Comment | Членам разрешено выполнение операций криптографии. |

9) Операторы архива

|  |  |
| --- | --- |
| **Item** | **Value** |
| Group Type | Local |
| Group Name | Операторы архива |
| Comment | Операторы архива могут переопределять ограничения доступа только в целях копирования и восстановления файлов |

10) Операторы настройки сети

|  |  |
| --- | --- |
| **Item** | **Value** |
| Group Type | Local |
| Group Name | Операторы настройки сети |
| Comment | Члены этой группы могут иметь некоторые административные права для управления настройкой сетевых параметров |

11) Операторы помощи по контролю учетных записей

|  |  |
| --- | --- |
| **Item** | **Value** |
| Group Type | Local |
| Group Name | Операторы помощи по контролю учетных записей |
| Comment | Члены этой группы могут удаленно запрашивать атрибуты авторизации и разрешения для ресурсов на данном компьютере. |

12) Опытные пользователи

|  |  |
| --- | --- |
| **Item** | **Value** |
| Group Type | Local |
| Group Name | Опытные пользователи |
| Comment | Категория опытных пользователей оставлена для обратной совместимости и обладает ограниченными административными правами |

13) Отсутствует

|  |  |
| --- | --- |
| **Item** | **Value** |
| Group Type | Global |
| Group Name | Отсутствует |
| Comment | Обычные пользователи |

14) Пользователи

|  |  |
| --- | --- |
| **Item** | **Value** |
| Group Type | Local |
| Group Name | Пользователи |
| Comment | Пользователи не имеют прав на изменение параметров системы и могут запускать большинство приложений |

15) Пользователи DCOM

|  |  |
| --- | --- |
| **Item** | **Value** |
| Group Type | Local |
| Group Name | Пользователи DCOM |
| Comment | Члены этой группы могут запускать, активизировать и использовать объекты DCOM на этом компьютере. |

16) Пользователи журналов производительности

|  |  |
| --- | --- |
| **Item** | **Value** |
| Group Type | Local |
| Group Name | Пользователи журналов производительности |
| Comment | Члены этой группы могут планировать ведение журнала счетчиков производительности, включать поставщиков трассировки и собирать трассировки событий как локально, так и через удаленный доступ к данному компьютеру. |

17) Пользователи системного монитора

|  |  |
| --- | --- |
| **Item** | **Value** |
| Group Type | Local |
| Group Name | Пользователи системного монитора |
| Comment | Члены данной группы имеют как местный, так и удаленный доступ к счетчику производительности |

18) Пользователи удаленного рабочего стола

|  |  |
| --- | --- |
| **Item** | **Value** |
| Group Type | Local |
| Group Name | Пользователи удаленного рабочего стола |
| Comment | Члены этой группы имеют право на выполнение удаленного входа |

19) Пользователи удаленного управления

|  |  |
| --- | --- |
| **Item** | **Value** |
| Group Type | Local |
| Group Name | Пользователи удаленного управления |
| Comment | Члены этой группы могут получать доступ к ресурсам инструментария WMI по протоколам управления (таким как WS-Management в службе удаленного управления Windows). Это касается только пространств имен WMI, предоставляющих доступ пользователям. |

20) Репликатор

|  |  |
| --- | --- |
| **Item** | **Value** |
| Group Type | Local |
| Group Name | Репликатор |
| Comment | Поддержка репликации файлов в домене |

21) Управляемая системой группа учетных записей

|  |  |
| --- | --- |
| **Item** | **Value** |
| Group Type | Local |
| Group Name | Управляемая системой группа учетных записей |
| Comment | Члены этой группы управляются системой. |

22) Читатели журнала событий

|  |  |
| --- | --- |
| **Item** | **Value** |
| Group Type | Local |
| Group Name | Читатели журнала событий |
| Comment | Члены этой группы могут читать журналы событий с локального компьютера |

4.Переменные среды

|  |  |
| --- | --- |
| ALLUSERSPROFILE | C:\ProgramData |
| APPDATA | C:\Users\User\AppData\Roaming |
| CommonProgramFiles | C:\Program Files (x86)\Common Files |
| CommonProgramFiles(x86) | C:\Program Files (x86)\Common Files |
| CommonProgramW6432 | C:\Program Files\Common Files |
| COMPUTERNAME | WIN-LVC1BUC8UGT |
| ComSpec | C:\WINDOWS\system32\cmd.exe |
| DriverData | C:\Windows\System32\Drivers\DriverData |
| FPS\_BROWSER\_APP\_PROFILE\_STRING | Internet Explorer |
| FPS\_BROWSER\_USER\_PROFILE\_STRING | Default |
| HOMEDRIVE | C: |
| HOMEPATH | \Users\User |
| LOCALAPPDATA | C:\Users\User\AppData\Local |
| LOGONSERVER | \\WIN-LVC1BUC8UGT |
| NUMBER\_OF\_PROCESSORS | 4 |
| OneDrive | C:\Users\User\OneDrive |
| OS | Windows\_NT |
| Path | C:\Program Files\Microsoft\jdk-11.0.16.101-hotspot\bin;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem;C:\WINDOWS\System32\WindowsPowerShell\v1.0\;C:\WINDOWS\System32\OpenSSH\;C:\Program Files (x86)\Windows Kits\10\Windows Performance Toolkit\;C:\Users\User\AppData\Local\Microsoft\WindowsApps;;C:\Users\User\AppData\Local\Programs\Microsoft VS Code\bin |
| PATHEXT | .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC |
| PROCESSOR\_ARCHITECTURE | x86 |
| PROCESSOR\_ARCHITEW6432 | AMD64 |
| PROCESSOR\_IDENTIFIER | Intel64 Family 6 Model 78 Stepping 3, GenuineIntel |
| PROCESSOR\_LEVEL | 6 |
| PROCESSOR\_REVISION | 4e03 |
| ProgramData | C:\ProgramData |
| ProgramFiles | C:\Program Files (x86) |
| ProgramFiles(x86) | C:\Program Files (x86) |
| ProgramW6432 | C:\Program Files |
| PSModulePath | C:\Program Files\WindowsPowerShell\Modules;C:\WINDOWS\system32\WindowsPowerShell\v1.0\Modules |
| PUBLIC | C:\Users\Public |
| SESSIONNAME | Console |
| SystemDrive | C: |
| SystemRoot | C:\WINDOWS |
| TEMP | C:\Users\User\AppData\Local\Temp |
| TMP | C:\Users\User\AppData\Local\Temp |
| USERDOMAIN | WIN-LVC1BUC8UGT |
| USERDOMAIN\_ROAMINGPROFILE | WIN-LVC1BUC8UGT |
| USERNAME | User |
| USERPROFILE | C:\Users\User |
| windir | C:\WINDOWS |
| ZES\_ENABLE\_SYSMAN |  |

5.Найти Региональные стандарты и рассказать что в них входит

|  |  |  |
| --- | --- | --- |
| **Item** | **Name** | **Setting** |
| Locale | Country | Россия |
| Locale | Language | Русский (Россия) |
| Number | Digits | 0123456789 |
| Number | Digit Separator |  |
| Number | Decimal Separator | , |
| Number | Decimal Places | 2 |
| Number | Measurement System | Metric |
| Currency | Name | рубль |
| Currency | Symbol | ₽ |
| Currency | ISO Code | RUB |
| Currency | Money Separator |  |
| Currency | Decimal Separator | , |
| Currency | Decimal Places | 2 |
| Date | Short Date | ddd dd.MM.yy |
| Date | Long Date | d MMMM yyyy 'г.' |
| Date | Calendar | Gregorian |
| Time | Time Format | H:mm:ss |
| Time | Ante Meridiem |  |
| Time | Post Meridiem |  |
| Time | Time Zone | RTZ 2 (зима) |
| Time | GMT Difference (mins.) | -180 |

В них входит: Страна нахождения, валюта и ее обозначения, часовой пояс, формат даты, информация о календаре, система измерения-метрическая

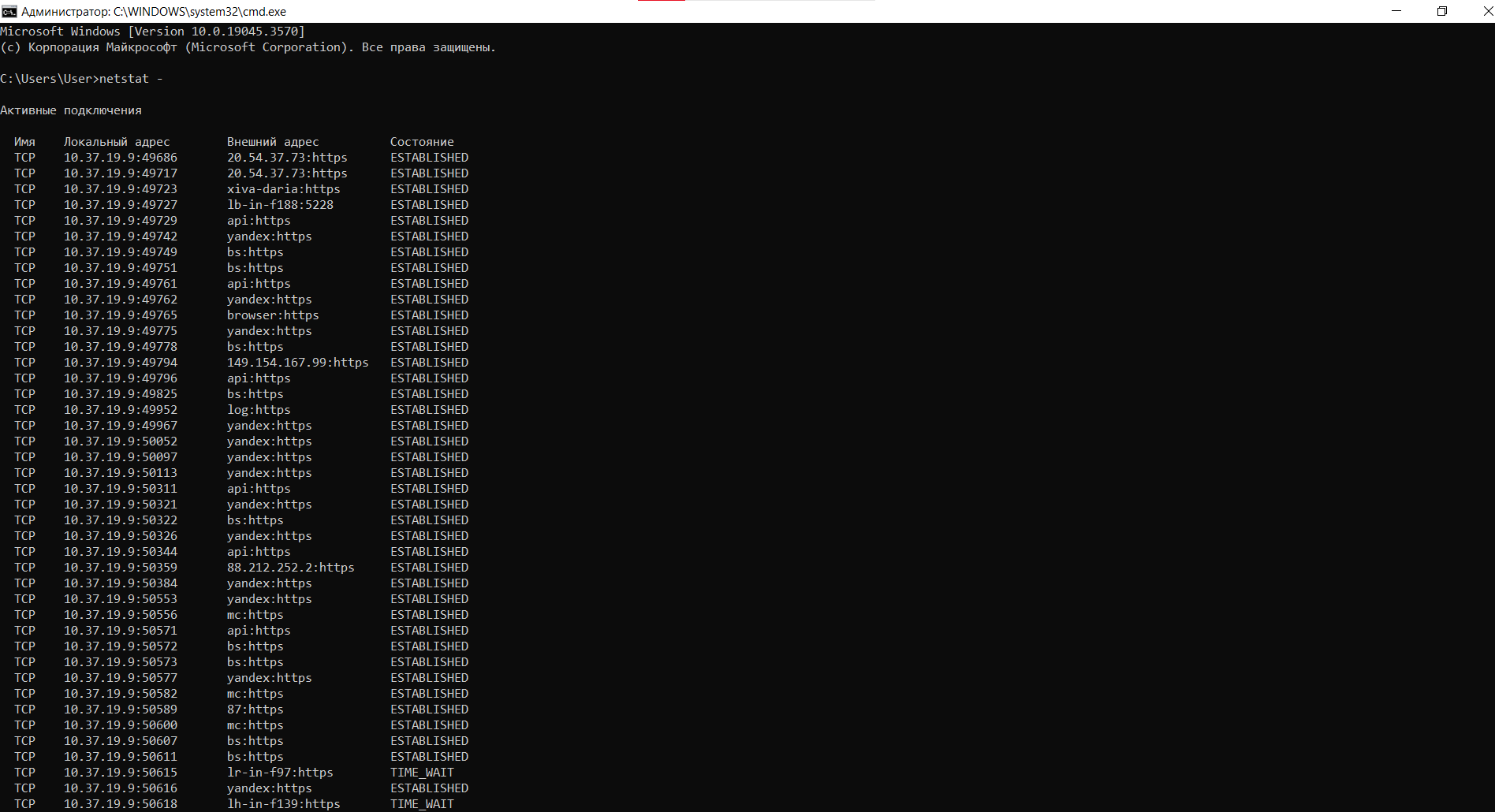
6.Найти свой мак адрес, и ip

IP: 109.232.111.178

|  |  |
| --- | --- |
| MAC Address | DC:8B:28:41:2D:F4 |

7.Прочитать в интернете что такое порт и узнать какие из них открыты (TCP и UDP и чем они отличаются) (рис.1)

|  |  |
| --- | --- |
| Local Port | 49567 |



Рисунок

TCP (**Протокол Управления Передачей**) - важный протокол сети интернет, который позволяет двум хостам создать соединение и обмениваться потоками данных.

UPD – сокращение от английского Update ( «**обновление**», «корректировка информации»). Пометка делается в основном для тех, кто уже прочитал новость до того, как она была обновлена.

Разница: Ключевым различием между TCP и UDP является скорость, поскольку TCP сравнительно медленнее UDP. В целом, UDP является быстрым, простым и эффективным протоколом, однако повторная передача потерянных пакетов данных возможна только в TCP.

Еще одно заметное различие между TCP и UDP заключается в том, что первый обеспечивает упорядоченную доставку данных от пользователя к серверу (и наоборот).

8.Разобраться с таблицей маршрутизации (Routing Table)

464) 0.0.0.0

|  |  |
| --- | --- |
| **Item** | **Value** |
| Destination | 0.0.0.0 |
| Netmask | 0.0.0.0 |
| Next Hop | 10.37.19.1 |
| Interface | 10.37.19.9 |
| Route Type | Remote |
| Protocol | Static |
| Age | 0 Дни 0 Hours 43 Минуты |
| Metric | 25 |

465) 10.37.19.0

|  |  |
| --- | --- |
| **Item** | **Value** |
| Destination | 10.37.19.0 |
| Netmask | 255.255.255.0 |
| Next Hop | 10.37.19.9 |
| Interface | 10.37.19.9 |
| Route Type | Local |
| Protocol | Local |
| Age | 0 Дни 0 Hours 43 Минуты |
| Metric | 281 |

466) 10.37.19.9

|  |  |
| --- | --- |
| **Item** | **Value** |
| Destination | 10.37.19.9 |
| Netmask | 255.255.255.255 |
| Next Hop | 10.37.19.9 |
| Interface | 10.37.19.9 |
| Route Type | Local |
| Protocol | Local |
| Age | 0 Дни 0 Hours 43 Минуты |
| Metric | 281 |

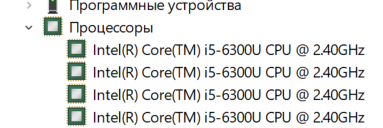
467) 10.37.19.255

|  |  |
| --- | --- |
| **Item** | **Value** |
| Destination | 10.37.19.255 |
| Netmask | 255.255.255.255 |
| Next Hop | 10.37.19.9 |
| Interface | 10.37.19.9 |
| Route Type | Local |
| Protocol | Local |
| Age | 0 Дни 0 Hours 43 Минуты |
| Metric | 281 |

468) 127.0.0.0

|  |  |
| --- | --- |
| **Item** | **Value** |
| Destination | 127.0.0.0 |
| Netmask | 255.0.0.0 |
| Next Hop | 127.0.0.1 |
| Interface | 127.0.0.1 |
| Route Type | Local |
| Protocol | Local |
| Age | 0 Дни 0 Hours 43 Минуты |
| Metric | 331 |

9.Диспетчер устройств (процессор.рис.2)



Рисунок

10.Узнать модель жесткого диска (рис.3)

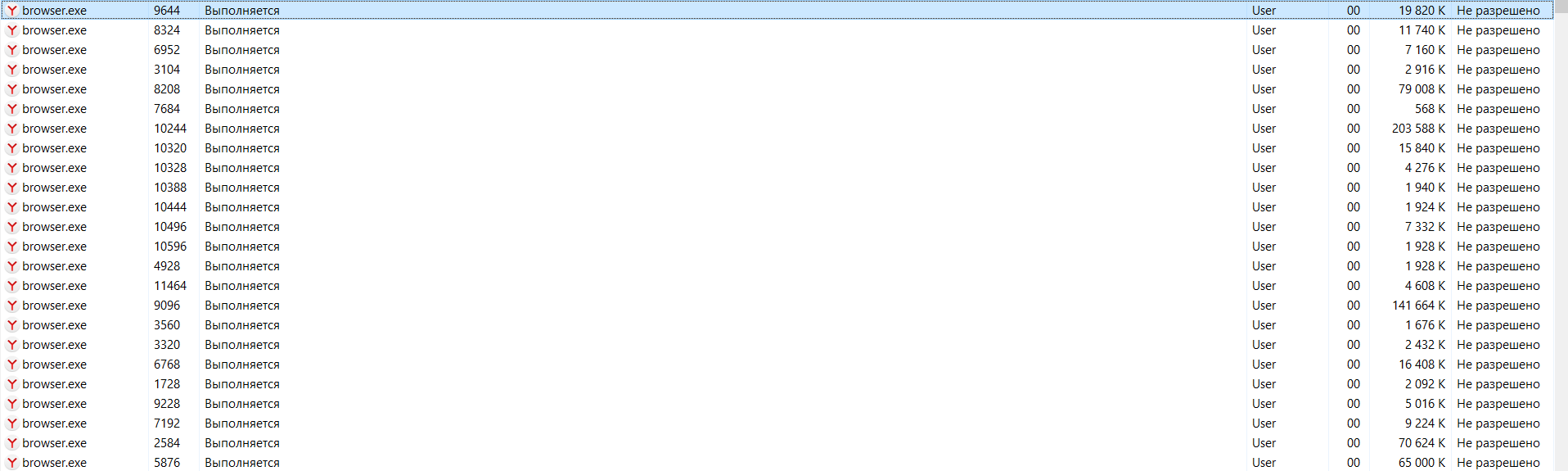


Рисунок

11.Посмотреть программы на автозагрузке

|  |  |  |
| --- | --- | --- |
| **Program Name** | **Settings Folder** | **Command** |
| Adobe Acrobat Synchronizer | HKCU\Software\Microsoft\Windows\CurrentVersion\Run | "C:\Program Files\Adobe\Acrobat DC\Acrobat\AdobeCollabSync.exe" |
| CCleaner Smart Cleaning | HKCU\Software\Microsoft\Windows\CurrentVersion\Run | "C:\Program Files\CCleaner\CCleaner64.exe" /MONITOR |
| desktop.ini | C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\ |  |
| desktop.ini | C:\Users\User\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ |  |
| MicrosoftEdgeAutoLaunch\_C46CFC0629905CC775E70B50EA8A519C | HKCU\Software\Microsoft\Windows\CurrentVersion\Run | "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --no-startup-window --win-session-start /prefetch:5 |
| NoxMultiPlayer | HKCU\Software\Microsoft\Windows\CurrentVersion\Run | "C:\Program Files (x86)\Nox\bin\MultiPlayerManager.exe" -startSource:auto\_start |
| OneDrive | HKCU\Software\Microsoft\Windows\CurrentVersion\Run | "C:\Users\User\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background |
| Steam | HKCU\Software\Microsoft\Windows\CurrentVersion\Run | "C:\Program Files (x86)\Steam\steam.exe" -silent |
| Xvid | HKCU\Software\Microsoft\Windows\CurrentVersion\Run | C:\Program Files (x86)\Xvid\CheckUpdate.exe |
| YandexBrowserAutoLaunch\_B64B7D5D07784CD66F00CA43360BB68B | HKCU\Software\Microsoft\Windows\CurrentVersion\Run | "C:\Users\User\AppData\Local\Yandex\YandexBrowser\Application\browser.exe" --no-startup-window --atlogin-bgr-mark /prefetch:5 |
| Zona | HKCU\Software\Microsoft\Windows\CurrentVersion\Run | C:\PROGRA~1\Zona\Zona.exe /MINIMIZED |

12. Узнать номер процесса и размер в памяти запущенного браузера с 2-3 открытыми сайтами (рис.4)



Рисунок

13.Проверить установлен ли Windows Bind Filter Driver и узнать что это такое

956) Windows Bind Filter Driver

|  |  |
| --- | --- |
| **Item** | **Value** |
| Name | Windows Bind Filter Driver |
| Service Type | System Driver |
| State | Running |
| Start Mode | Automatic |
| Path Name | \SystemRoot\system32\drivers\bindflt.sys |
| Start Name |  |

Драйвер Windows Bind Filter, который связывает пространства имен файловой системы с разными местоположениями и скрывает переназначение от пользователей.

14.OLE DB Providers Прочитать в интернете что это такое...

OLE DB провайдер представляет собой драйвер для доступа к БД через стандартные OLE DB интерфейсы. OLE DB провайдеры можно использовать совместно со многими клиентскими библиотеками: ADO, dbGo (ADO Express), ADO .Net, и др.

15.Выбрать ещё 4 службы или драйвера и узнать за что они отвечают (Найти в интернете) (рис.5)



Рисунок

Intel(R) audio – это драйвер аудиоустройства, разработанный компанией Intel для использования в компьютерах с процессорами Intel. Данный драйвер предоставляет возможность передачи аудио сигнала через выходы видеокарты.

Intel (R) Capability Licensing Service TCP IP Interface: Эта служба отвечает за проверку лицензий Intel. Если вы не используете продукты, требующие лицензирования, ее можно отключить.

Intel (R) Content Protection HECI Service: Данная служба отвечает за защиту цифрового контента на вашем компьютере. Однако, если вы не смотрите защищенное цифровое видео или не используете контент, который требует защиты, то можете безопасно отключить данную службу.

High-bandwidth Digital Content Protection (HDCP) - это форма защиты от цифрового копирования, разработанная корпорацией Intel для предотвращения копирования цифрового аудио-и видеоконтента при его перемещении по соединениям.

**Вывод:** изучили программу WinAudit и помощью нее различные задания.