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

Выполнил студент

Группы: 2ОИБАС-1222

Протасов Д.К.

Преподаватель

Сибирев И.В.

Оценка за работу :\_\_\_\_\_\_\_

**Москва – 2023г.**

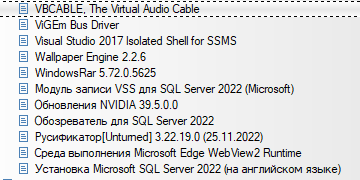
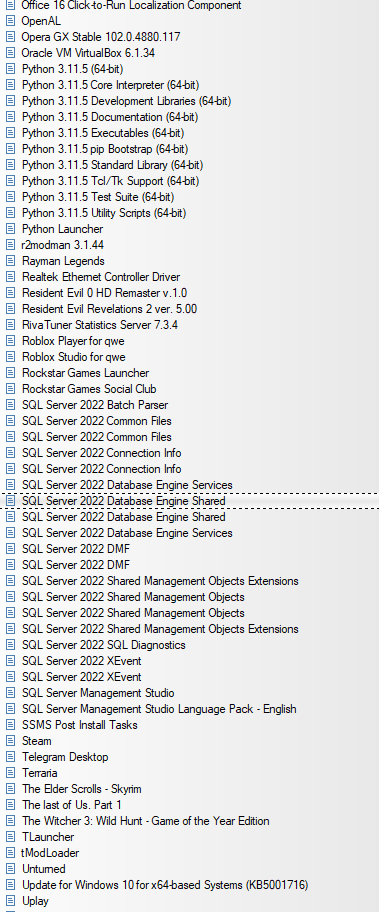
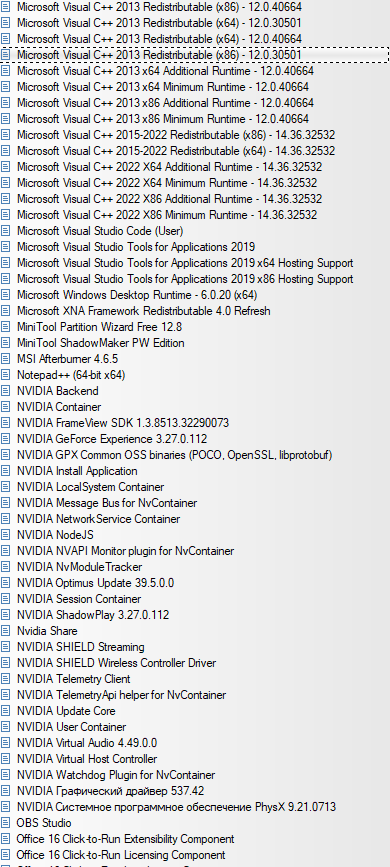
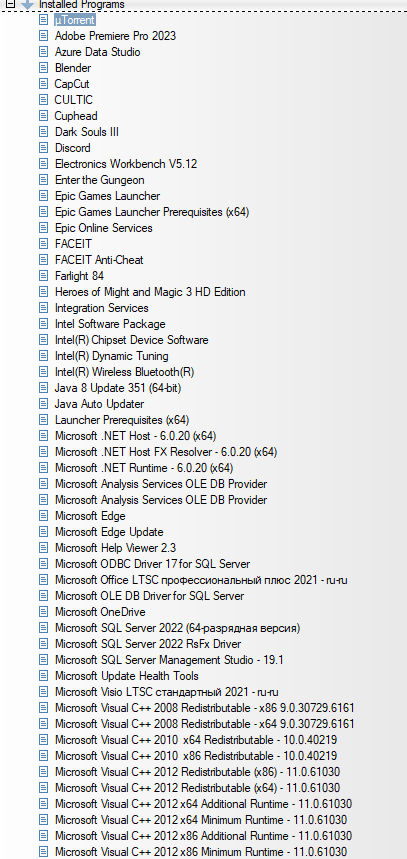
**Лабораторная работа**

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

**Задание:**

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

Программы:



2.Обратите внимание на то какие .NET установлены

|  |  |  |
| --- | --- | --- |
| .NET Framework | 4,0,30319,0 | Нет |

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

248) IIS\_IUSRS

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

|  |
| --- |
|  |

249) SQLServer2005SQLBrowserUser$DESKTOP-JKV8MO3

|  |  |
| --- | --- |
| **Item** | **Value** |
| Group Type | Local |
| Group Name | SQLServer2005SQLBrowserUser$DESKTOP-JKV8MO3 |
| Comment | Члены группы обладают необходимыми правами доступа для использования в качестве учетной записи для доступа к связанному экземпляру обозревателя SQL Server. |

|  |
| --- |
|  |

250) Администраторы

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

|  |
| --- |
|  |

251) 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. |

|  |
| --- |
|  |

252) Владельцы устройства

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

|  |
| --- |
|  |

253) 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. |

|  |
| --- |
|  |

254) Отсутствует

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

|  |
| --- |
|  |

255) Пользователи

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

|  |
| --- |
|  |

256) 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. |

|  |
| --- |
|  |

257) 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. |

|  |
| --- |
|  |

258) 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 |

|  |
| --- |
|  |

259) 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. |

|  |
| --- |
|  |

260) Управляемая системой группа учетных записей

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

|  |
| --- |
|  |

261) 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(Обратите внимание (программисты) это наше все)(<https://lumpics.ru/environment-variables-in-windows-10/>)

|  |  |
| --- | --- |
| **Name** | **Variable Value** |
| \_\_COMPAT\_LAYER | DetectorsAppHealt |
| ALLUSERSPROFILE | C:\ProgramData |
| APPDATA | C:\Users\qwe\AppData\Roaming |
| CommonProgramFiles | C:\Program Files (x86)\Common Files |
| CommonProgramFiles(x86) | C:\Program Files (x86)\Common Files |
| CommonProgramW6432 | C:\Program Files\Common Files |
| COMPUTERNAME | DESKTOP-JKV8MO3 |
| 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\qwe |
| LOCALAPPDATA | C:\Users\qwe\AppData\Local |
| LOGONSERVER | \\DESKTOP-JKV8MO3 |
| NUMBER\_OF\_PROCESSORS | 12 |
| OneDrive | C:\Users\qwe\OneDrive |
| OS | Windows\_NT |
| Path | C:\Program Files (x86)\Common Files\Oracle\Java\javapath;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Windows\System32\OpenSSH\;C:\Program Files (x86)\NVIDIA Corporation\PhysX\Common;C:\Program Files\NVIDIA Corporation\NVIDIA NvDLISR;C:\Program Files\dotnet\;C:\Program Files (x86)\Microsoft SQL Server\160\Tools\Binn\;C:\Program Files\Microsoft SQL Server\160\Tools\Binn\;C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\170\Tools\Binn\;C:\Program Files\Microsoft SQL Server\160\DTS\Binn\;C:\Program Files (x86)\Microsoft SQL Server\160\DTS\Binn\;C:\Program Files\Azure Data Studio\bin;C:\Users\qwe\AppData\Local\Microsoft\WindowsApps;;C:\Users\qwe\Desktop\Visual Studio\Microsoft VS Code\bin;C:\Program Files\Azure Data Studio\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 141 Stepping 1, GenuineIntel |
| PROCESSOR\_LEVEL | 6 |
| PROCESSOR\_REVISION | 8d01 |
| 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;C:\Program Files (x86)\Microsoft SQL Server\160\Tools\PowerShell\Modules\ |
| PUBLIC | C:\Users\Public |
| SESSIONNAME | Console |
| SystemDrive | C: |
| SystemRoot | C:\Windows |
| TEMP | C:\Users\qwe\AppData\Local\Temp |
| TMP | C:\Users\qwe\AppData\Local\Temp |
| USERDOMAIN | DESKTOP-JKV8MO3 |
| USERDOMAIN\_ROAMINGPROFILE | DESKTOP-JKV8MO3 |
| USERNAME | qwe |
| USERPROFILE | C:\Users\qwe |
| VBOX\_MSI\_INSTALL\_PATH | C:\Program Files\Oracle\VirtualBox\ |
| windir | C:\Windows |
| ZES\_ENABLE\_SYSMAN | 1 |

5.Найти Региональные стандарты и рассказать что в них входит

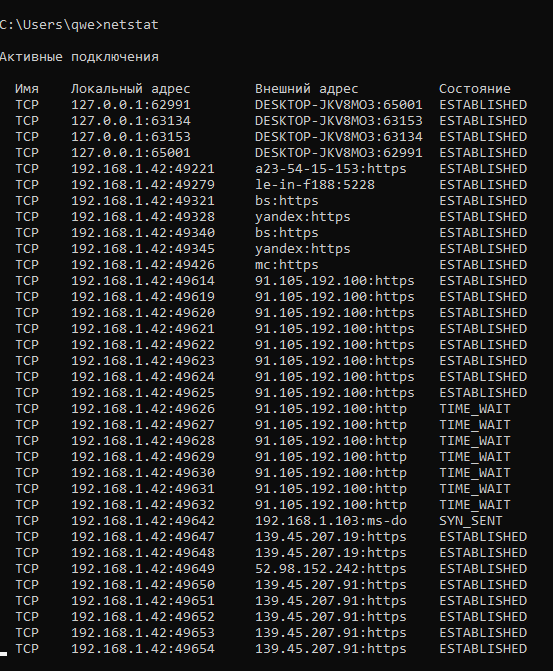
|  |  |  |
| --- | --- | --- |
| **Item** | **Name** | **Setting** |
| Locale | Country | Россия |
| Locale | Language | Русский (Россия) |
| Number | Digits | 0123456789 |
| Number | Digit Separator |  |
| Number | Decimal Separator | , |
| Number | Decimal Places | 2 |
| Number | Measurement System | Metric |
| Currency | Name | рубль |
| Currency | Symbol | ₽ |
| Currency | ISO Code | RUB |
| Currency | Money Separator |  |
| Currency | Decimal Separator | , |
| Currency | Decimal Places | 2 |
| Date | Short Date | dd.MM.yyyy |
| 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 Address | 192.168.1.42 fe80::5c28:8ef2:2993:f1b3 |
| MAC Address | 9A:7F:43:C6:AC:20 |

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



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)

337) 0.0.0.0

|  |  |
| --- | --- |
| **Item** | **Value** |
| Destination | 0.0.0.0 |
| Netmask | 0.0.0.0 |
| Next Hop | 192.168.1.1 |
| Interface | 192.168.1.42 |
| Route Type | Remote |
| Protocol | Static |
| Age | 0 Дни 0 Hours 2 Минуты |
| Metric | 60 |

|  |
| --- |
|  |

338) 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 | 1 Day 23 Hours 2 Минуты |
| Metric | 331 |

|  |
| --- |
|  |

339) 127.0.0.1

|  |  |
| --- | --- |
| **Item** | **Value** |
| Destination | 127.0.0.1 |
| Netmask | 255.255.255.255 |
| Next Hop | 127.0.0.1 |
| Interface | 127.0.0.1 |
| Route Type | Local |
| Protocol | Local |
| Age | 1 Day 23 Hours 2 Минуты |
| Metric | 331 |

|  |
| --- |
|  |

340) 127.255.255.255

|  |  |
| --- | --- |
| **Item** | **Value** |
| Destination | 127.255.255.255 |
| Netmask | 255.255.255.255 |
| Next Hop | 127.0.0.1 |
| Interface | 127.0.0.1 |
| Route Type | Local |
| Protocol | Local |
| Age | 1 Day 23 Hours 2 Минуты |
| Metric | 331 |

|  |
| --- |
|  |

341) 192.168.1.0

|  |  |
| --- | --- |
| **Item** | **Value** |
| Destination | 192.168.1.0 |
| Netmask | 255.255.255.0 |
| Next Hop | 192.168.1.42 |
| Interface | 192.168.1.42 |
| Route Type | Local |
| Protocol | Local |
| Age | 0 Дни 0 Hours 2 Минуты |
| Metric | 316 |

|  |
| --- |
|  |

342) 192.168.1.42

|  |  |
| --- | --- |
| **Item** | **Value** |
| Destination | 192.168.1.42 |
| Netmask | 255.255.255.255 |
| Next Hop | 192.168.1.42 |
| Interface | 192.168.1.42 |
| Route Type | Local |
| Protocol | Local |
| Age | 0 Дни 0 Hours 2 Минуты |
| Metric | 316 |

|  |
| --- |
|  |

343) 192.168.1.255

|  |  |
| --- | --- |
| **Item** | **Value** |
| Destination | 192.168.1.255 |
| Netmask | 255.255.255.255 |
| Next Hop | 192.168.1.42 |
| Interface | 192.168.1.42 |
| Route Type | Local |
| Protocol | Local |
| Age | 0 Дни 0 Hours 2 Минуты |
| Metric | 316 |

|  |
| --- |
|  |

344) 192.168.56.0

|  |  |
| --- | --- |
| **Item** | **Value** |
| Destination | 192.168.56.0 |
| Netmask | 255.255.255.0 |
| Next Hop | 192.168.56.1 |
| Interface | 192.168.56.1 |
| Route Type | Local |
| Protocol | Local |
| Age | 1 Day 23 Hours 2 Минуты |
| Metric | 281 |

|  |
| --- |
|  |

345) 192.168.56.1

|  |  |
| --- | --- |
| **Item** | **Value** |
| Destination | 192.168.56.1 |
| Netmask | 255.255.255.255 |
| Next Hop | 192.168.56.1 |
| Interface | 192.168.56.1 |
| Route Type | Local |
| Protocol | Local |
| Age | 1 Day 23 Hours 2 Минуты |
| Metric | 281 |

|  |
| --- |
|  |

346) 192.168.56.255

|  |  |
| --- | --- |
| **Item** | **Value** |
| Destination | 192.168.56.255 |
| Netmask | 255.255.255.255 |
| Next Hop | 192.168.56.1 |
| Interface | 192.168.56.1 |
| Route Type | Local |
| Protocol | Local |
| Age | 1 Day 23 Hours 2 Минуты |
| Metric | 281 |

|  |
| --- |
|  |

347) 224.0.0.0

|  |  |
| --- | --- |
| **Item** | **Value** |
| Destination | 224.0.0.0 |
| Netmask | 240.0.0.0 |
| Next Hop | 127.0.0.1 |
| Interface | 127.0.0.1 |
| Route Type | Local |
| Protocol | Local |
| Age | 1 Day 23 Hours 2 Минуты |
| Metric | 331 |

|  |
| --- |
|  |

348) 224.0.0.0

|  |  |
| --- | --- |
| **Item** | **Value** |
| Destination | 224.0.0.0 |
| Netmask | 240.0.0.0 |
| Next Hop | 192.168.56.1 |
| Interface | 192.168.56.1 |
| Route Type | Local |
| Protocol | Local |
| Age | 1 Day 23 Hours 2 Минуты |
| Metric | 281 |

|  |
| --- |
|  |

349) 224.0.0.0

|  |  |
| --- | --- |
| **Item** | **Value** |
| Destination | 224.0.0.0 |
| Netmask | 240.0.0.0 |
| Next Hop | 192.168.1.42 |
| Interface | 192.168.1.42 |
| Route Type | Local |
| Protocol | Local |
| Age | 0 Дни 0 Hours 2 Минуты |
| Metric | 316 |

|  |
| --- |
|  |

350) 255.255.255.255

|  |  |
| --- | --- |
| **Item** | **Value** |
| Destination | 255.255.255.255 |
| Netmask | 255.255.255.255 |
| Next Hop | 127.0.0.1 |
| Interface | 127.0.0.1 |
| Route Type | Local |
| Protocol | Local |
| Age | 1 Day 23 Hours 2 Минуты |
| Metric | 331 |

|  |
| --- |
|  |

351) 255.255.255.255

|  |  |
| --- | --- |
| **Item** | **Value** |
| Destination | 255.255.255.255 |
| Netmask | 255.255.255.255 |
| Next Hop | 192.168.56.1 |
| Interface | 192.168.56.1 |
| Route Type | Local |
| Protocol | Local |
| Age | 1 Day 23 Hours 2 Минуты |
| Metric | 281 |

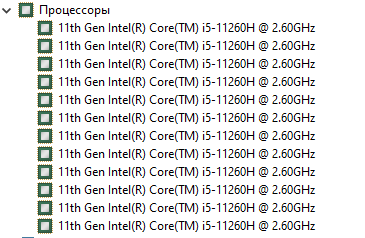
|  |
| --- |
|  |

352) 255.255.255.255

|  |  |
| --- | --- |
| **Item** | **Value** |
| Destination | 255.255.255.255 |
| Netmask | 255.255.255.255 |
| Next Hop | 192.168.1.42 |
| Interface | 192.168.1.42 |
| Route Type | Local |
| Protocol | Local |
| Age | 0 Дни 0 Hours 2 Минуты |
| Metric | 316 |

9.Диспетчер устройств(Найти процессор...)

|  |  |
| --- | --- |
| **Item** | **Value** |
| Processor Number | 1 |
| Name | 11th Gen Intel(R) Core(TM) i5-11260H @ 2.60GHz |
| Short Name |  |
| Speed Estimated | 2611MHz |
| Speed Registry | 2611MHz |
| Processor Type | OEM Primary |
| Manufacturer | Intel(R) Corporation |
| Serial Number |  |
| APIC Physical ID | 0x00, 0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08, 0x09, 0x0A, 0x0B |
| Features | 1-GByte, ACPI, AESNI, APIC, AVX, CLFSH, CMOV, CMPXCHG16B, CX8, DE, DS, DS-CPL, DTES64, EDB, EIST, F16C, FMA, FPU, FXFR, HTT, IA64, LAHF, MCA, MCE, MMX, MONITOR, MOVBE, MSR, MTRR, OSXSAVE, PAE, PAT, PBE, PCID, PCLMULQDQ, PDCM, PGE, POPCNT, PSE, PSE-36, RDRAND, RDTSCP, SEP, SS, SSE, SSE2, SSE3, SSE4.1, SSE4.2, SSSE3, TM, TM2, TSC, TSC-Deadline, VME, VMX, x2APIC, XSAVE, xTPR |
| Cache |  |
| TLB | TLB Instruction 4KB |
| Logical Processors | 12 |



10.Узнать модель жесткого диска



11.Посмотреть программы на автозагрузке

|  |  |  |
| --- | --- | --- |
| **Program Name** | **Settings Folder** | **Command** |
| Adobe CCXProcess | HKLM\Software\Microsoft\Windows\CurrentVersion\Run | C:\Program Files (x86)\Adobe\Adobe Creative Cloud Experience\CCXProcess.exe |
| desktop.ini | C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\ |  |
| desktop.ini | C:\Users\qwe\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ |  |
| Discord | HKCU\Software\Microsoft\Windows\CurrentVersion\Run | "C:\Users\qwe\AppData\Local\Discord\Update.exe" --processStart Discord.exe --process-start-args --start-minimized |
| EpicGamesLauncher | HKCU\Software\Microsoft\Windows\CurrentVersion\Run | "C:\Program Files (x86)\Epic Games\Launcher\Portal\Binaries\Win64\EpicGamesLauncher.exe" -silent -launchcontext=boot |
| FACEIT | HKCU\Software\Microsoft\Windows\CurrentVersion\Run | "C:\Users\qwe\AppData\Local\FACEIT\update.exe" --processStart "FACEIT.exe" |
| MicrosoftEdgeAutoLaunch\_F77213E3CCE205988F4C5F7CC17C9A9F | HKCU\Software\Microsoft\Windows\CurrentVersion\Run | "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --no-startup-window --win-session-start /prefetch:5 |
| OneDrive | HKCU\Software\Microsoft\Windows\CurrentVersion\Run | "C:\Users\qwe\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background |
| Opera GX Browser Assistant | HKCU\Software\Microsoft\Windows\CurrentVersion\Run | C:\Users\qwe\AppData\Local\Programs\Opera GX\assistant\browser\_assistant.exe |
| Opera GX Stable | HKCU\Software\Microsoft\Windows\CurrentVersion\Run | C:\Users\qwe\AppData\Local\Programs\Opera GX\launcher.exe |
| Steam | HKCU\Software\Microsoft\Windows\CurrentVersion\Run | "C:\Program Files (x86)\Steam\steam.exe" -silent |
| SunJavaUpdateSched | HKLM\Software\Microsoft\Windows\CurrentVersion\Run | "C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe" |

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



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

893) Windows Bind Filter Driver

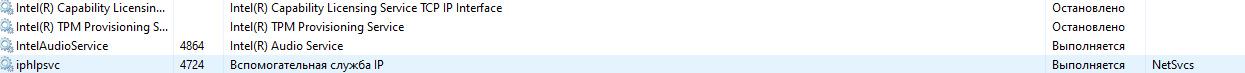
|  |  |
| --- | --- |
| **Item** | **Value** |
| Name | Windows Bind Filter Driver |
| Service Type | System Driver |
| State | Running |
| Start Mode | Automatic |
| Path Name | \SystemRoot\system32\drivers\bindflt.sys |
| Start Name |  |

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)



IntelAudioService – 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.

TPMProvisioningService.exe — это процесс Intel, который обычно находится в папке C:\Program Files\Intel\. Доверенный платформенный модуль (TPM) — это микросхема. Его основная функция — генерировать безопасные криптографические ключи. Проблема с TPMProvisioningservice.exe, которая перестала работать в Windows, может вызвать проблемы с безопасностью..

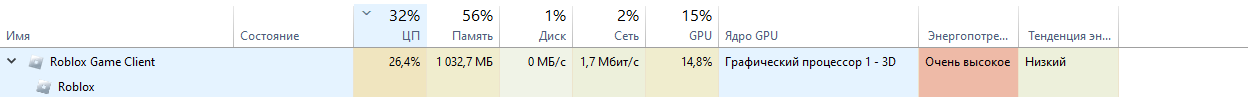
iphlpsvc - Вспомогательная служба IP: Обеспечивает возможность туннельного подключения с помощью технологий туннелирования для IP версии 6 (6to4, ISATAP, порты прокси и Teredo), а также IP-HTTPS. Если остановить эту службу, компьютер не сможет использовать дополнительные возможности подключения, предоставляемые этими технологиями.

**Вывод:** изучили программу WinAudit и выполнили с её помощью задания.

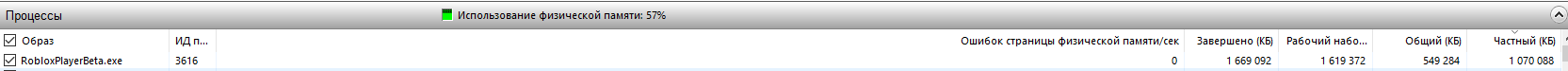
**2часть**

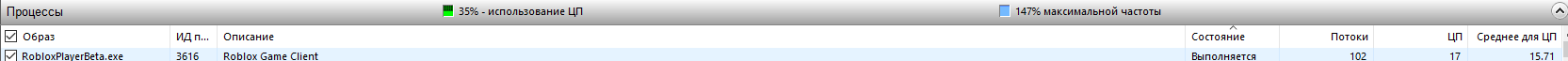
**Roblox**

Диспетчер задач



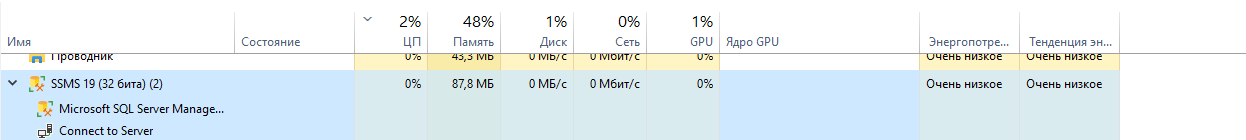
Монитор ресурсов





**SQL**

Диспетчер Задач



Монитор ресурсов

