Федеральное государственное образовательное бюджетное

учреждение высшего образования

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

**(Финансовый университет)**

Колледж информатики и программирования

Специальность 10.02.05 Обеспечение информационной безопасности автоматизированных систем

**ОТЧЕТ**

**ПО УЧЕБНОЙ ПРАКТИКЕ**

Профессиональный модульПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих

Выполнил:

обучающийся учебной группы № 1022

Миненков Е.А.

*(И.О. Фамилия)*

Проверил:

руководитель практики от колледжа:

Сиберев И.В.

*(И.О. Фамилия)*

**Москва**

**20­­­­24**

Учебная практика (Сиберев)

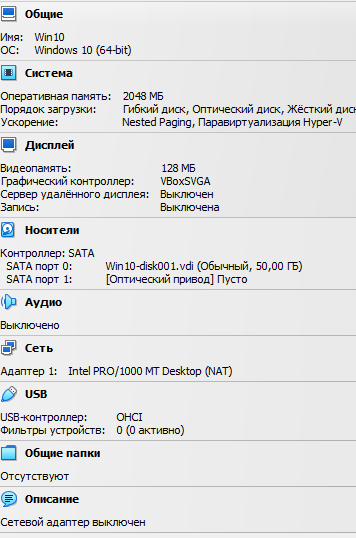
Лабораторная работа №1

Цель работы: Установить ОС.

Ход работы:

Я зашёл в проводник, написал в адресной строке

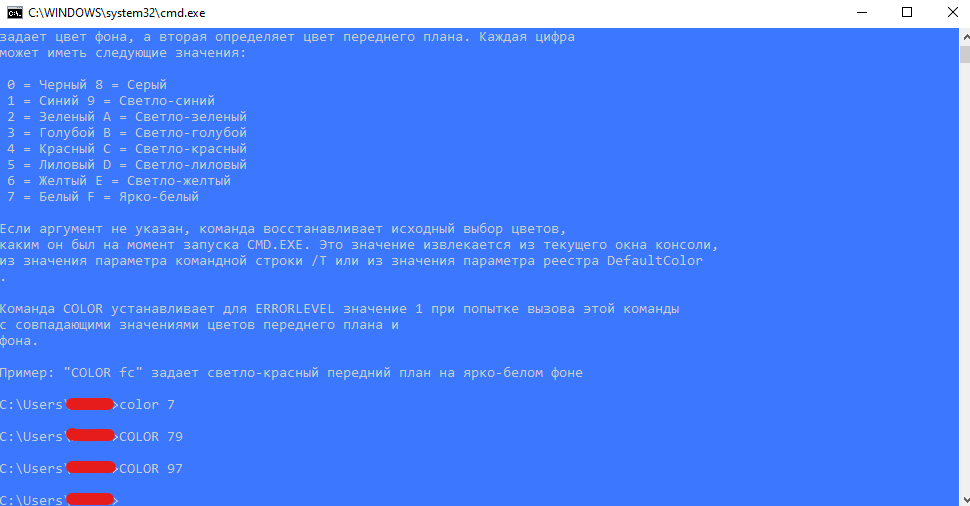
<ftp://fs-kip/Virtual%20Machine/VirtualBox/Win10/>

перекинул на рабочий стол запустил, далее автоматически установилась конфигурация и запустилась Windows 1

Лабораторная работа №2

Управление ОС MS Windows с помощью командной строки

Цель работы – знакомство с возможностями интерпретатора командной строки и командами MS Windows, приобретение навыков работы со справочной системой командного процессора, знакомство с командными файламиОС MS Windows, приобретение навыков разработки и отладки сценариев MS Windows

1. Запустить интерпретатор командной строки (сделано win + R)
2. Увеличить размер окна интерпретатора и задать цвет фона и цвет шрифта (рекомендуется синий фон и белый шрифт). 
3. Без использования текстового редактора создать список из 4-5 слов (например, фамилий), используя пример 1. Отсортировать список в алфавитном порядке и сохранить его в новом файле.



Лабораторная работа №3-4

@echo off

cd %~dp0

start notepad++ %0

::::::::::::::::::::::::::::::::::::::::::::::

Set /p input= вводиться число^>

echo "См= %input%"

set /a rez= 4\*%input%"

echo "Пириметр см=%rez%"

pause

**1)**

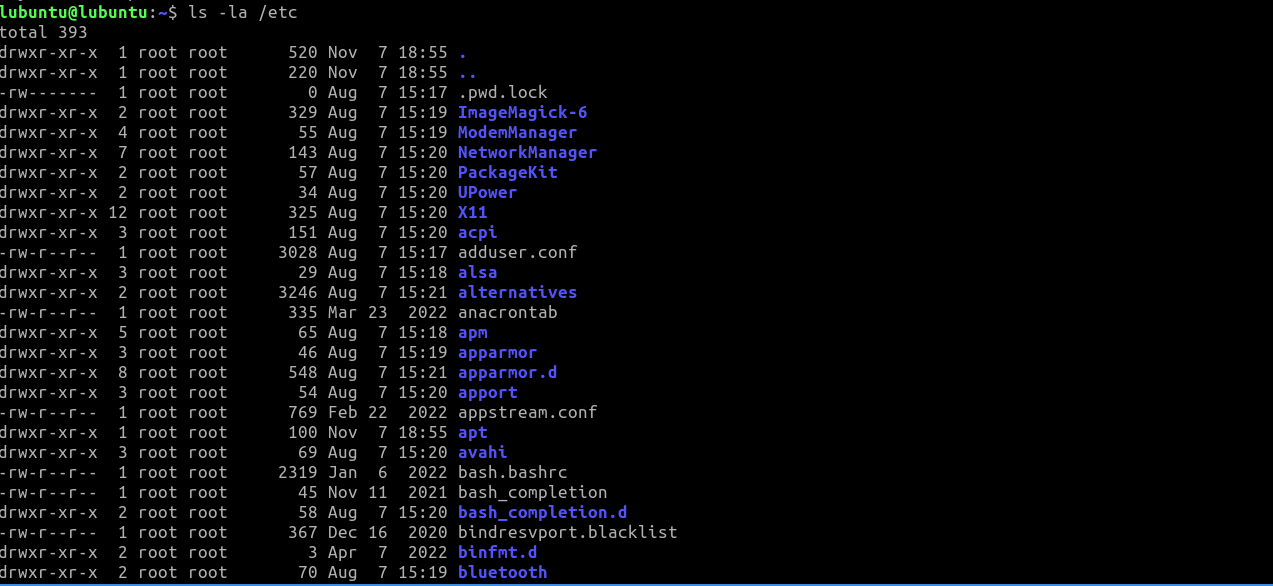
Чтобы просмотреть содержимое директорий /etc, /proc, /home, можно использовать команду ls с аргументом -l, которая позволяет просмотреть содержимое директорий в виде списка с дополнительной информацией о файлах.

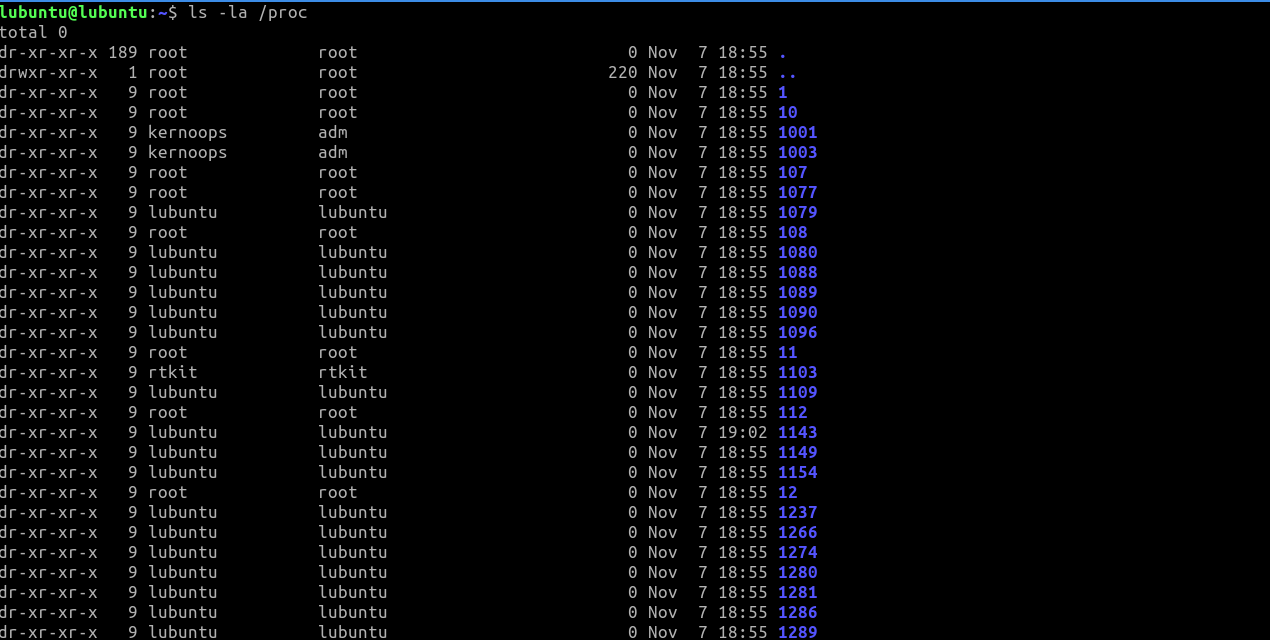
**Пример:**

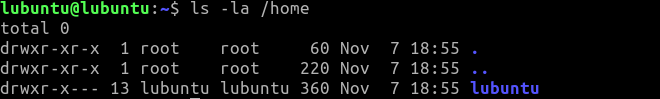
ls -l /etc

ls -l /proc

ls -l /home





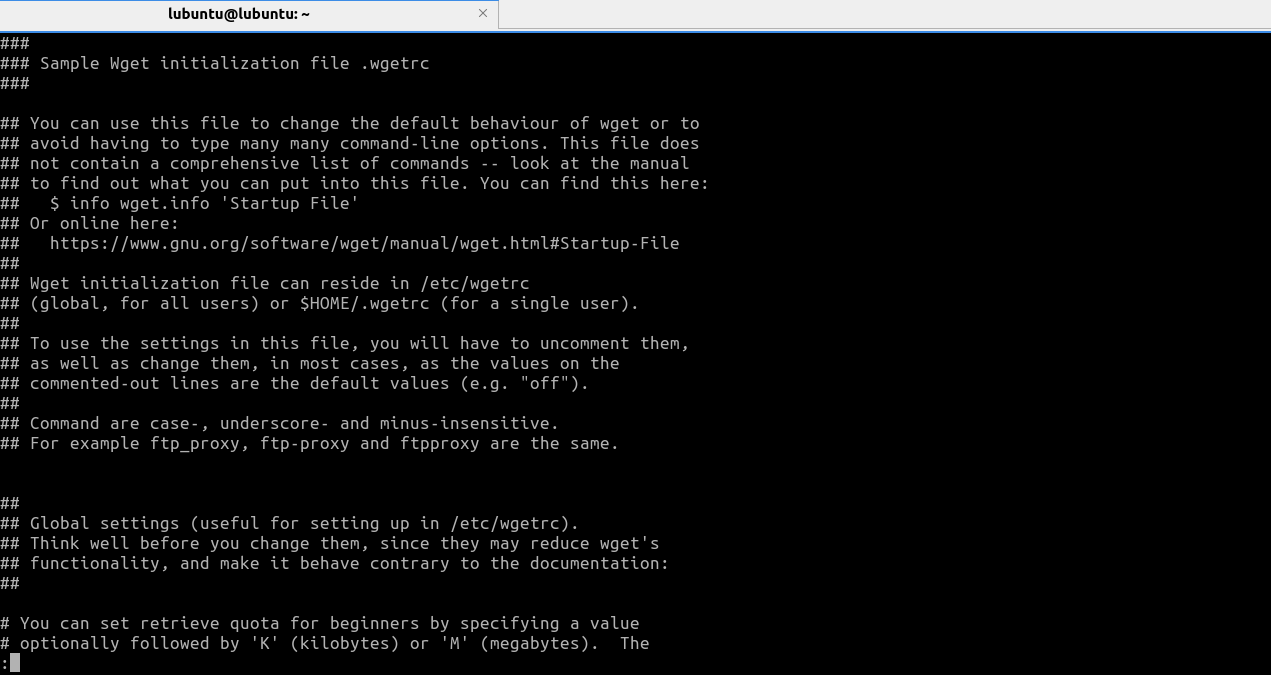


Для просмотра произвольных файлов в /etc можно использовать команду cat с указанием пути к файлу, который нужно просмотреть.

**Пример:**

cat /etc/hosts

cat /etc/resolv.conf



**2)**

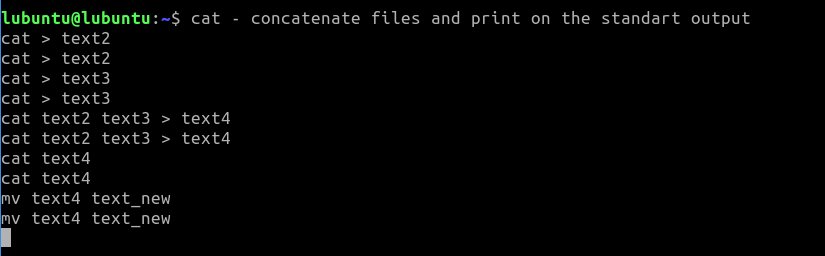
Команда cat (от англ. concatenate) предназначена для вывода содержимого файлов на экран или объединения файлов и вывода результатов на экран.

Примеры использования команды cat:

cat file.txt - выводит содержимое файла file.txt

cat file1.txt file2.txt - объединяет содержимое файлов file1.txt и file2.txt и выводит результат

cat file.txt > newfile.txt - создает файл newfile.txt и записывает в него содержимое файла file.txt



**3)**

Для создания файлов можно использовать команду touch, а для создания директории - команду mkdir. Для перемещения файлов и директорий можно использовать команду mv. Для удаления файлов и директорий можно использовать команду rm.

Примеры использования команд:

touch file1.txt file2.txt - создает файлы file1.txt и file2.txt

mkdir new\_dir - создает директорию new\_dir

mv file1.txt new\_dir - перемещает файл file1.txt в директорию new\_dir

rm file2.txt new\_dir - удаляет файл file2.txt и директорию new\_dir

**4)**

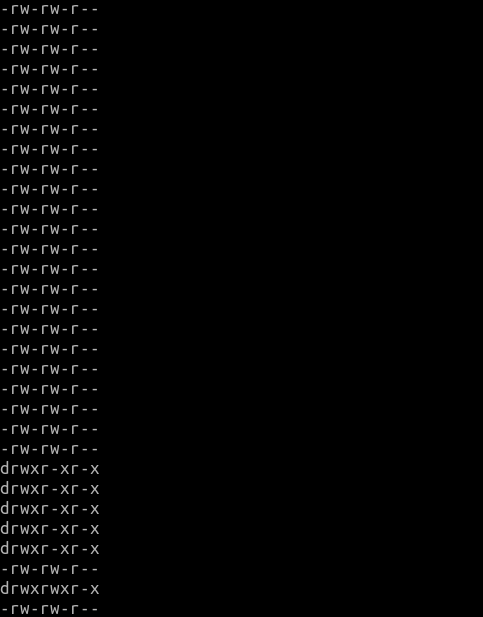
Чтобы подсчитать количество скрытых файлов в домашнем каталоге, можно использовать команду ls с аргументом -a, которая позволяет просмотреть все файлы, включая скрытые, и команду grep для поиска файлов, имена которых начинаются с точки. Затем можно использовать команду wc с аргументом -l, которая позволяет подсчитать количество строк

**5)**

Чтобы вывести содержимое всех файлов в директории /etc и направить ошибки в отдельный файл в домашней директории, можно использовать команду cat с аргументом \* для вывода содержимого всех файлов и команду 2> для перенаправления ошибок в файл.

**Пример:**

cat /etc/\* 2> ~/errors.txt



Затем для подсчета количества файлов, которые не удалось посмотреть, можно использовать команду wc с аргументом -l для подсчета строк в файле с ошибками.

**Пример:**

wc -l ~/errors.txt

**6)**

Для запуска программы в одном терминале и просмотра PID процесса можно использовать команду ps с аргументом aux. Для остановки процесса с помощью команды kill нужно указать PID процесса и тип сигнала, который нужно послать.

Пример:

В терминале 1:

./program\_name

В терминале 2:

ps aux | grep program\_name # получаем PID процесса

kill -SIGTERM PID # остановка процесса с помощью сигнала SIGTERM

kill -SIGKILL PID # остановка процесса с помощью сигнала SIGKILL

kill -SIGHUP PID # остановка процесса с помощью сигнала SIGHUP и перезапуск

Лабораторная работа №5

**Часть 1.**

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

Microsoft Edge

Microsoft Edge Update

 Oracle VM VirtualBox Guest Additions 7.0.8

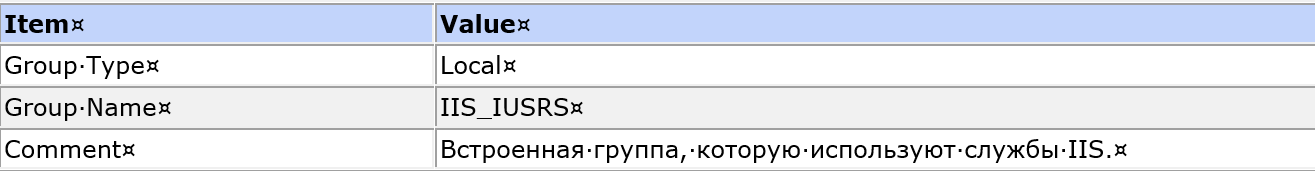
Dynamic HTML Data Binding

**2)** Обратите внимание на то какие .NET установлены

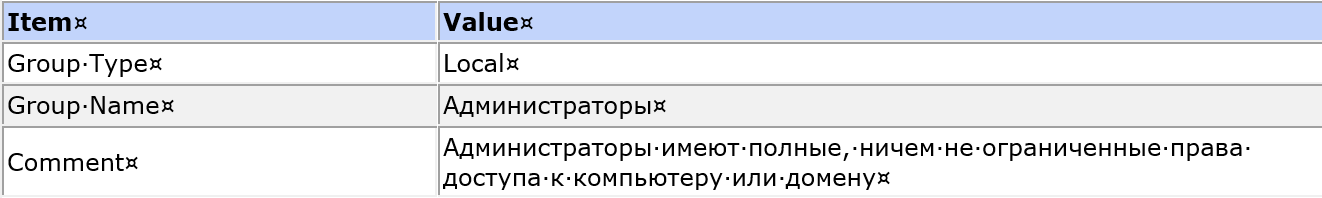


**3)** Получить таблицу групп пользователей(загуглить и разобраться что есть что)

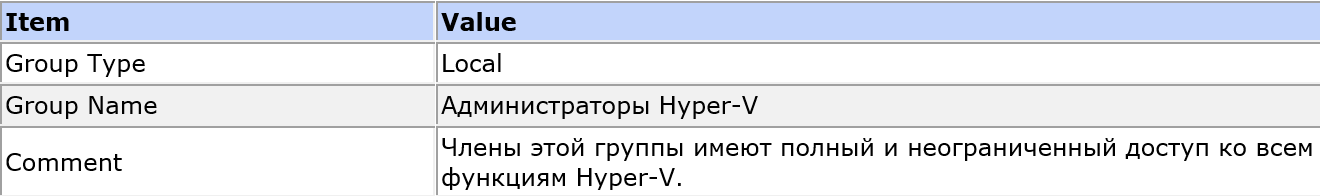
**63) IIS\_IUSRS**



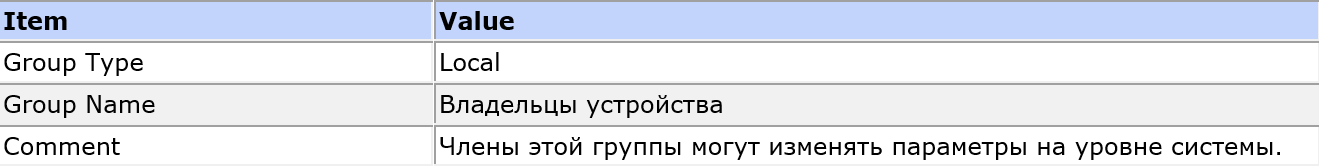
**64) Администраторы**



**65) Администраторы Hyper-V**



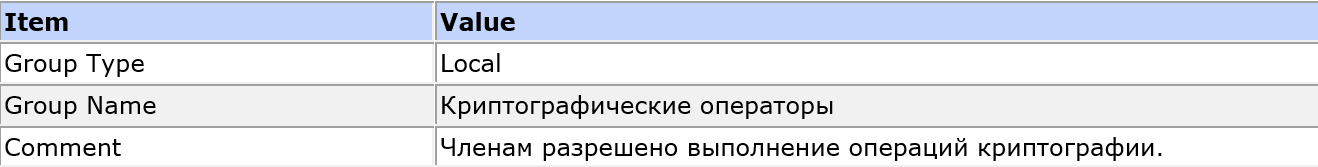
**66) Владельцы устройства**



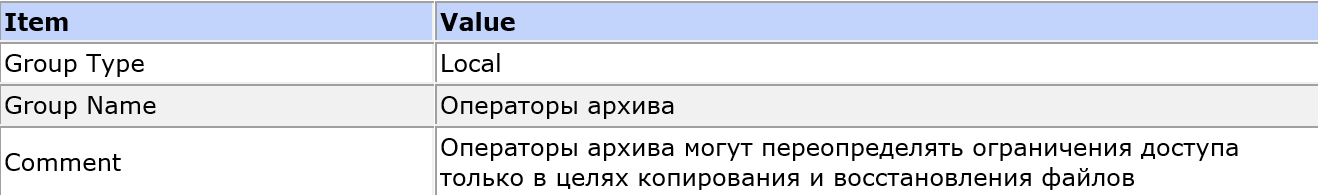
**67) Гости**



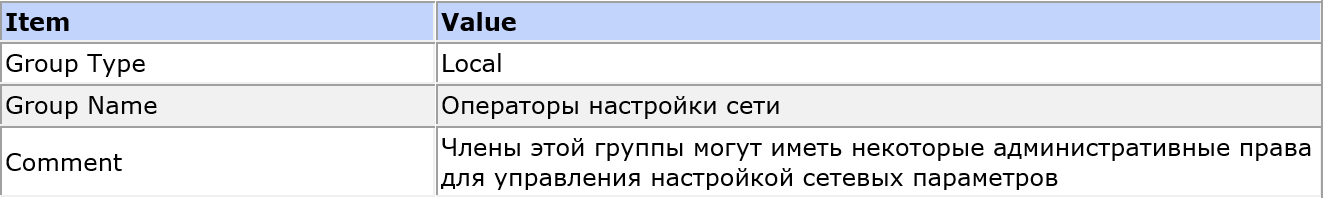
**68) Криптографические операторы**



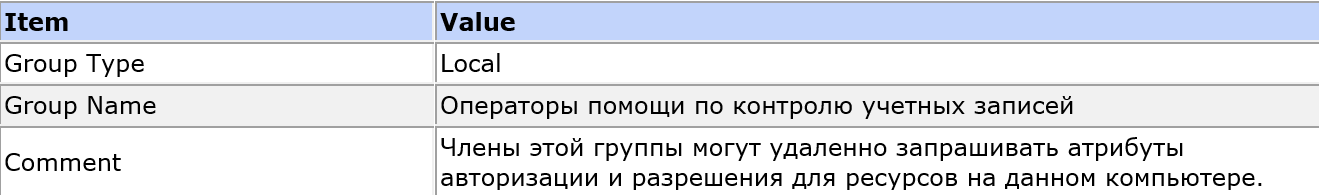
**69) Операторы архива**



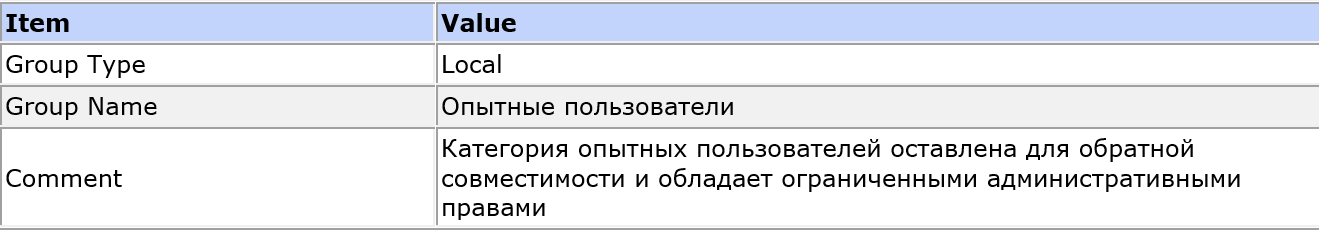
**70) Операторы настройки сети**



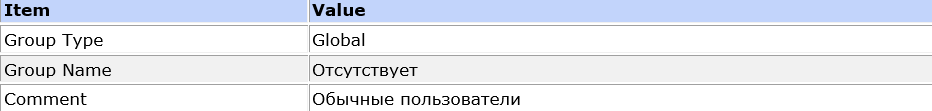
**71) Операторы помощи по контролю учетных записей**



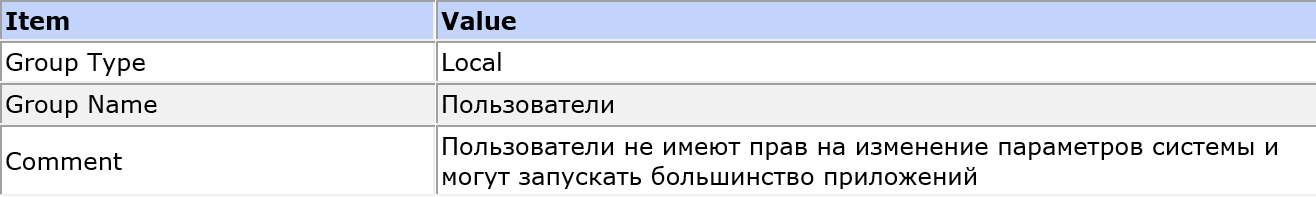
**72) Опытные пользователи**



**73) Отсутствует**



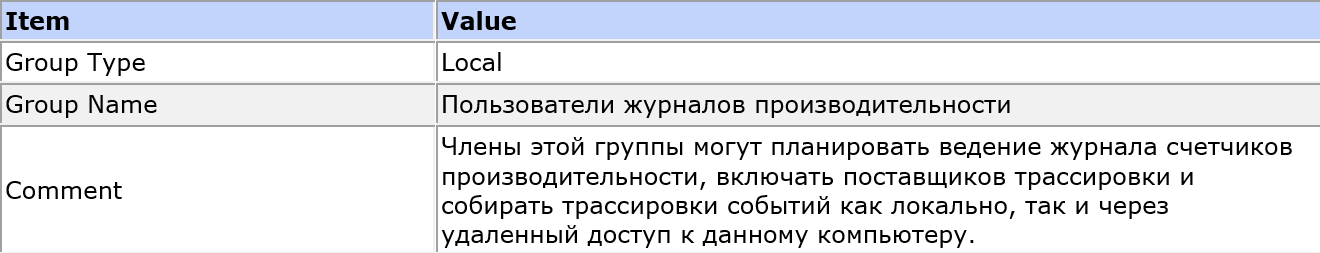
**74) Пользователи**



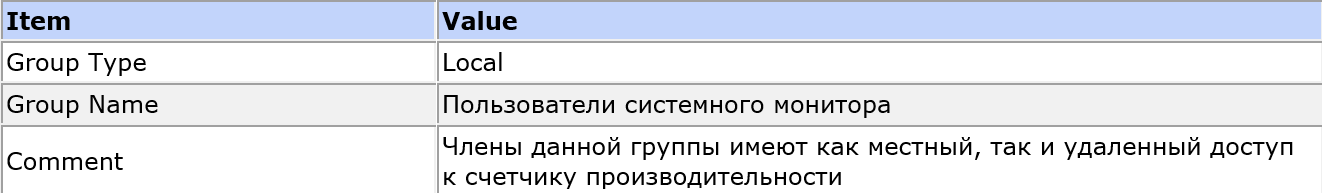
**75) Пользователи DCOM**



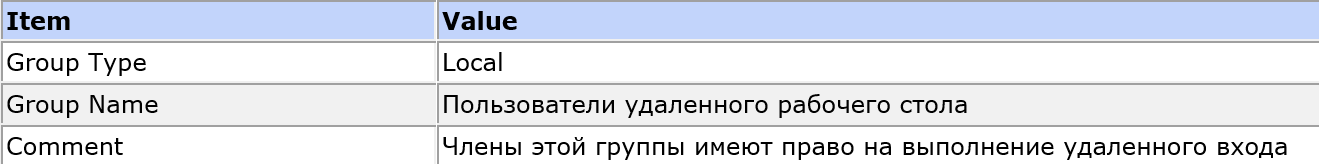
**76) Пользователи журналов производительности**



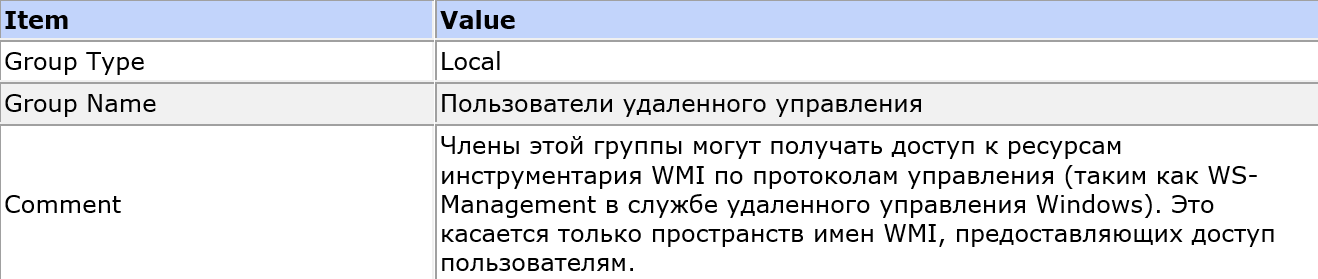
**77) Пользователи системного монитора**



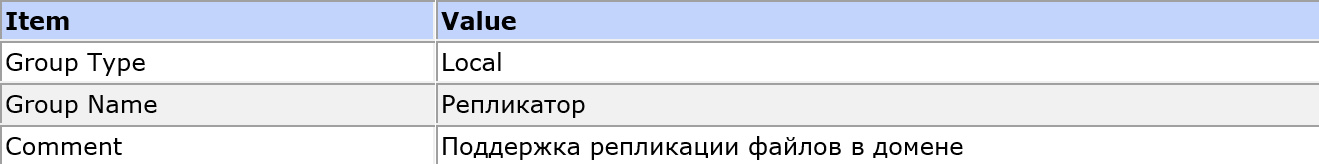
**78) Пользователи удаленного рабочего стола**



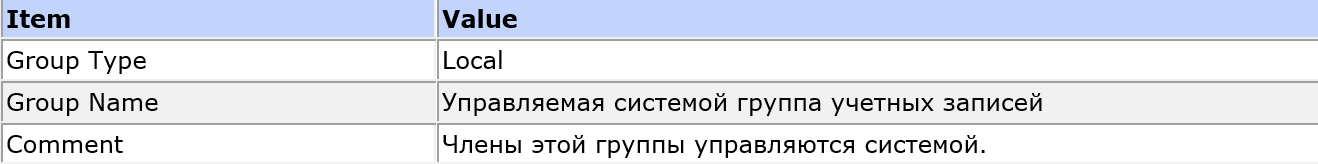
**79) Пользователи удаленного управления**



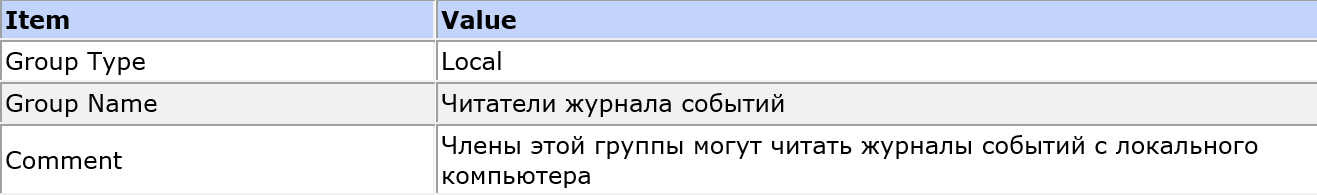
**80) Репликатор**



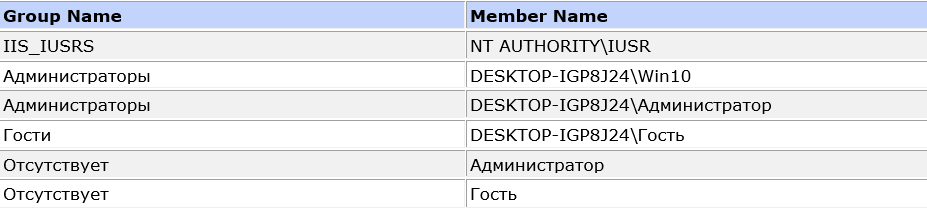
**81) Управляемая системой группа учетных записей**



**82) Читатели журнала событий**



**83) Group Members**

****

**4)**Переменные среды(Обратите внимание (программисты) это наше все)(https://lumpics.ru/environment-variables-in-windows-10/)

|  |  |
| --- | --- |
| **Name** | **Variable Value** |
| ALLUSERSPROFILE | C:\ProgramData |
| APPDATA | C:\Users\Win10\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-IGP8J24 |
| ComSpec | C:\Windows\system32\cmd.exe |
| DriverData | C:\Windows\System32\Drivers\DriverData |
| HOMEDRIVE | C: |
| HOMEPATH | \Users\Win10 |
| LOCALAPPDATA | C:\Users\Win10\AppData\Local |
| LOGONSERVER | \\DESKTOP-IGP8J24 |
| NUMBER\_OF\_PROCESSORS | 1 |
| OneDrive | C:\Users\Win10\OneDrive |
| OS | Windows\_NT |
| Path | C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Windows\System32\OpenSSH\;C:\Users\Win10\AppData\Local\Microsoft\WindowsApps; |
| PATHEXT | .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC |
| PROCESSOR\_ARCHITECTURE | x86 |
| PROCESSOR\_ARCHITEW6432 | AMD64 |
| PROCESSOR\_IDENTIFIER | Intel64 Family 6 Model 165 Stepping 3, GenuineIntel |
| PROCESSOR\_LEVEL | 6 |
| PROCESSOR\_REVISION | a503 |
| 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\Win10\AppData\Local\Temp |
| TMP | C:\Users\Win10\AppData\Local\Temp |
| USERDOMAIN | DESKTOP-IGP8J24 |
| USERDOMAIN\_ROAMINGPROFILE | DESKTOP-IGP8J24 |
| USERNAME | Win10 |
| USERPROFILE | C:\Users\Win10 |
| windir | C:\Window |

**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 |

**6)** Найти свой мак адрес, и ip

|  |  |
| --- | --- |
| MAC Address | 08:00:27:33:8A:55 |
| IP Address | 10.0.2.15 fe80::4ca7:3f40:ab73:f028 |

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

Что такое TCP и UDP

TCP (Transmission Control Protocol) — протокол сквозной связи, созданный в 1974 году и до сих пор востребованный в мире. Только вдумайтесь, почти 50 лет прошло, везде мобильный интернет и беспроводные сети, а TCP остаётся неизменным.

А всё потому, что TCP изначально был создан для надёжного соединения. Перед тем, как начинать передачу данных, протокол используется протокол рукопожатия для установления соединения, и лишь затем начинает передачу пакетов. Надёжность протокола объясняется тем, что он не теряет пакеты информации во время передачи, отправляя запрос на подтверждение получения. Если требуется, данные будут отправлены повторно. Тут надо уточнить, что очерёдность отправки пакетов сохраняется. Из недостатков протокола можно выделить низкую скорость работы протокола. Это объясняется сложностью обеспечения надёжной передачи данных с упорядочиванием пакетов.

UDP (User Datagram Protocol) создан в 1980 году. Это более простой протокол, который не требует установки соединения между хостами для передачи данных. Пакеты отправляются сразу, без проверки клиента на предмет готовности принимать данные. Из-за такого подхода протокол менее надёжен — пакеты легко могут потеряться. А ещё отсутствует порядок отправки пакетов с данными, из-за чего получатель принимает неупорядоченную информацию. Зато передача данных происходит намного быстрее, если сравнивать с TCP.

Основные отличия TCP и UDP

Итак, как вы уже поняли, UDP — быстрый протокол, но у TCP есть гарантия получения и упорядоченность данных. Давайте коротко сформулируем отличия этих двух протоколов:

Надёжность. TCP надёжнее, так как использует тайм-ауты, требует подтверждения получения данных и повторно отправляет данные при необходимости. У протокола UDP ничего такого нет, а данные нередко теряются на этапе доставки к хосту-получателю.

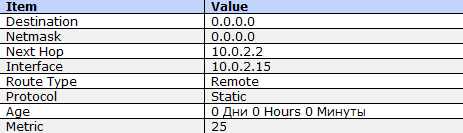
Упорядоченность. Здесь выигрывает TCP, который гарантированно передаёт пакеты данных именно в той последовательности, которая была задана изначально. В UDP такие возможности не реализованы.

Скорость. По этому критерию выигрывает UDP, который значительно быстрее тяжеловесного TCP, нуждающегося в установлении надёжного соединения и других необходимых для передачи данных условий.

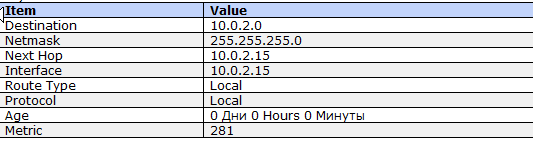
Метод передачи данных. TCP предполагает потоковую передачу данных, границы фрагментов данных не обозначены. UDP использует метод датаграмм, когда получатель проверяет целостность пакетов лишь при получении сообщения. Пакеты данных в данном случае имеют обозначения границ.

**8)** Разобраться с таблицей маршрутизации (Routing Table)

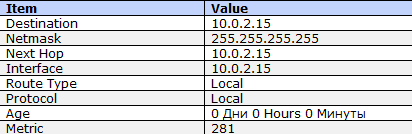
**120) 0.0.0.0**



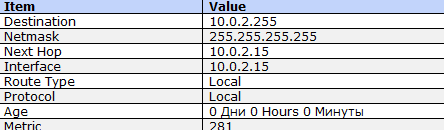
**121) 10.0.2.0**



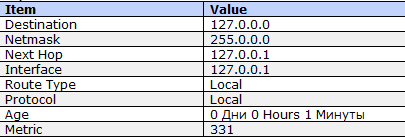
**122) 10.0.2.15**



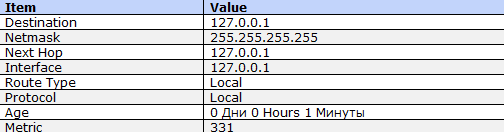
**123) 10.0.2.255**



**124) 127.0.0.0**

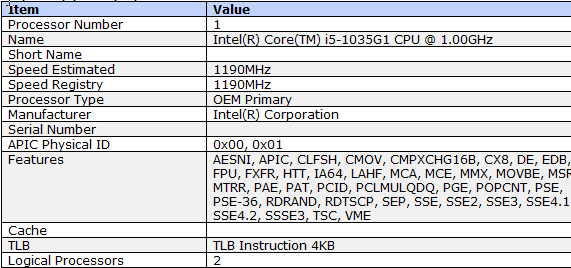


**125) 127.0.0.1**

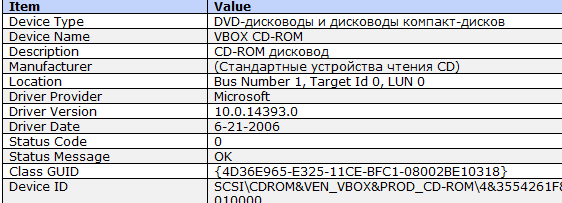


**9)** Диспетчер устройств(Найти процессор...)

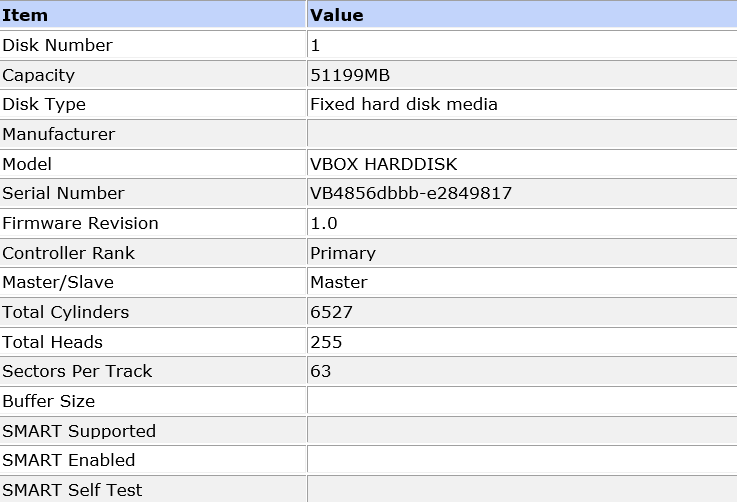
**151) Процессоры**



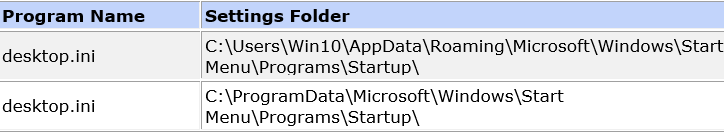
**10)** Узнать модель жесткого диска



**204) VBOX HARDDISK**

****

**11)** Посмотреть программы цв автозагрузке

****

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

Intel(R) Core(TM) i5-1035G1 @ 1.0GHz

2904MHz

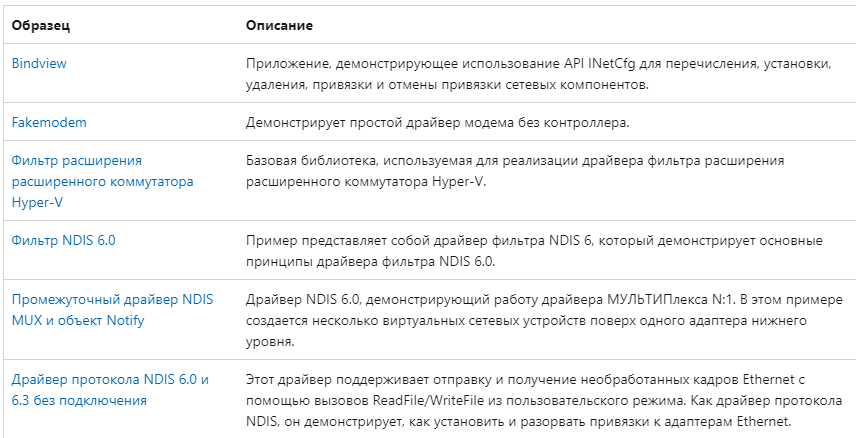
**13)** Проверить установлен ли Windows Bind Filter Driver и узнать что это такое

Есть

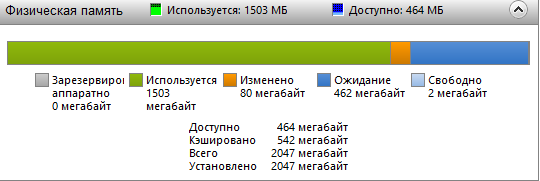
Драйвер фильтра файловой системы — это необязательный драйвер, который добавляет значение или изменяет поведение файловой системы. Это компонент в режиме ядра, который выполняется в рамках руководства Windows.

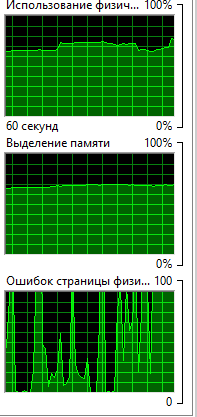
**14)**OLE DB Providers Прочитать в интернете что это такое...

Поставщик Microsoft OLE DB для публикации в Интернете позволяет ADO получать доступ к ресурсам, обслуживаемым Microsoft FrontPage или Microsoft Internet Information Server. Ресурсы включают исходные веб-файлы, например HTML-файлы или веб-папки Windows 2000.

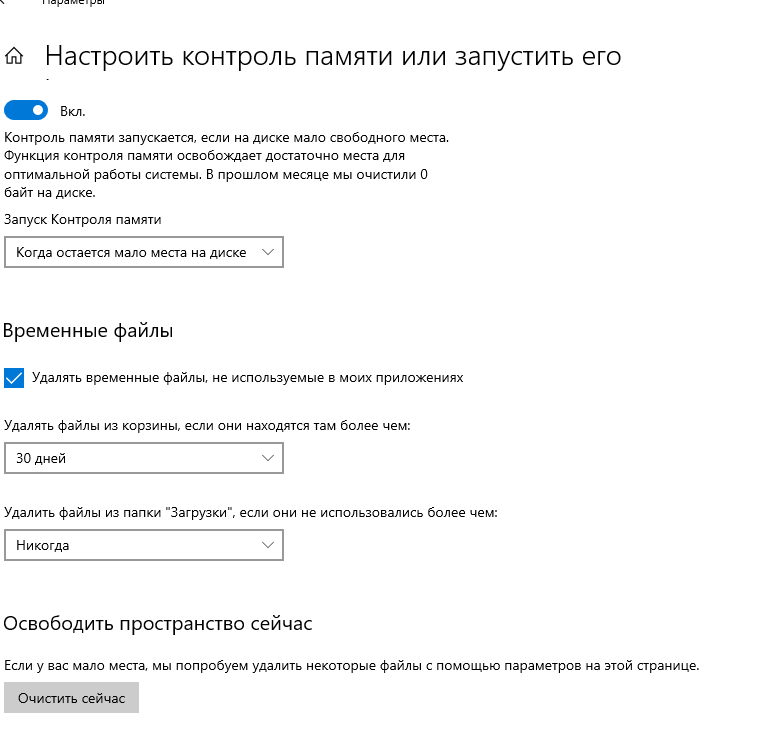
**15)** Выбрать ещё 4 службы или драйвера и узнать за что они отвечают (Найти в интернете) 

Часть 2.   
Запущенные программы: Paint,World Pad

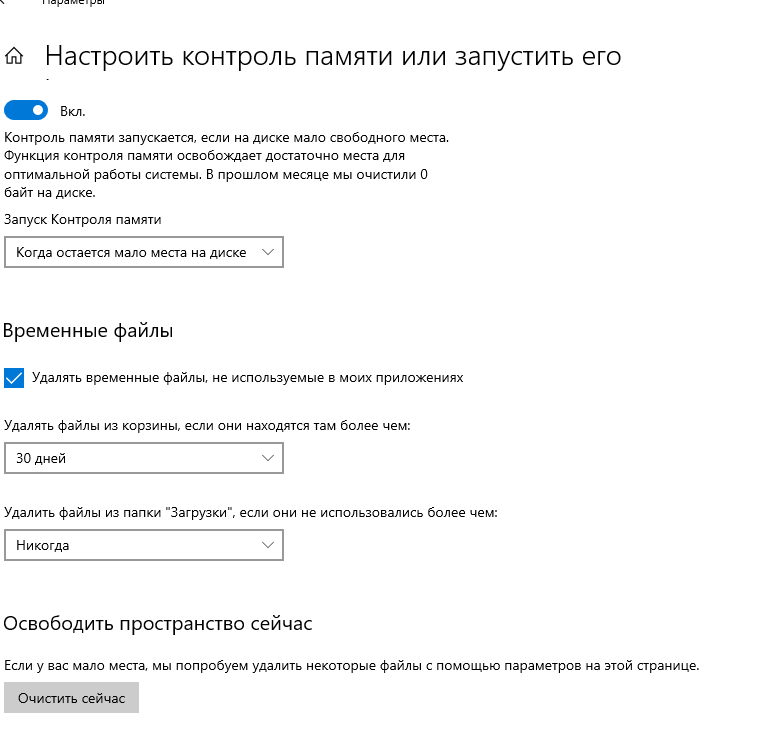




Лабораторная работа №6



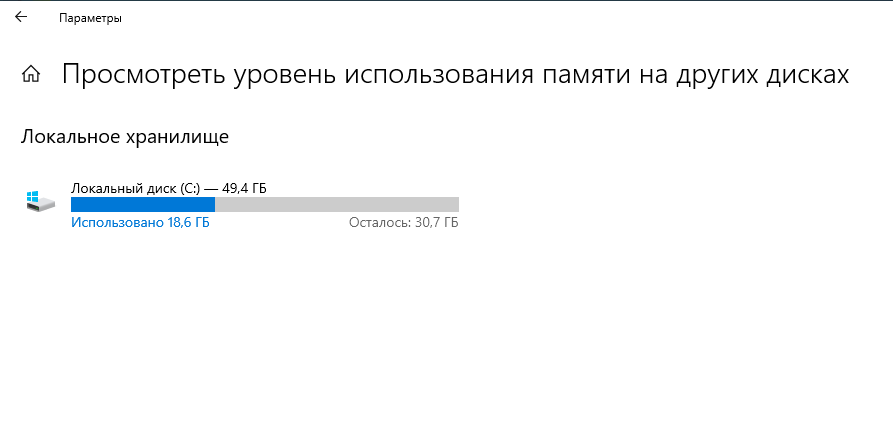
**1)**



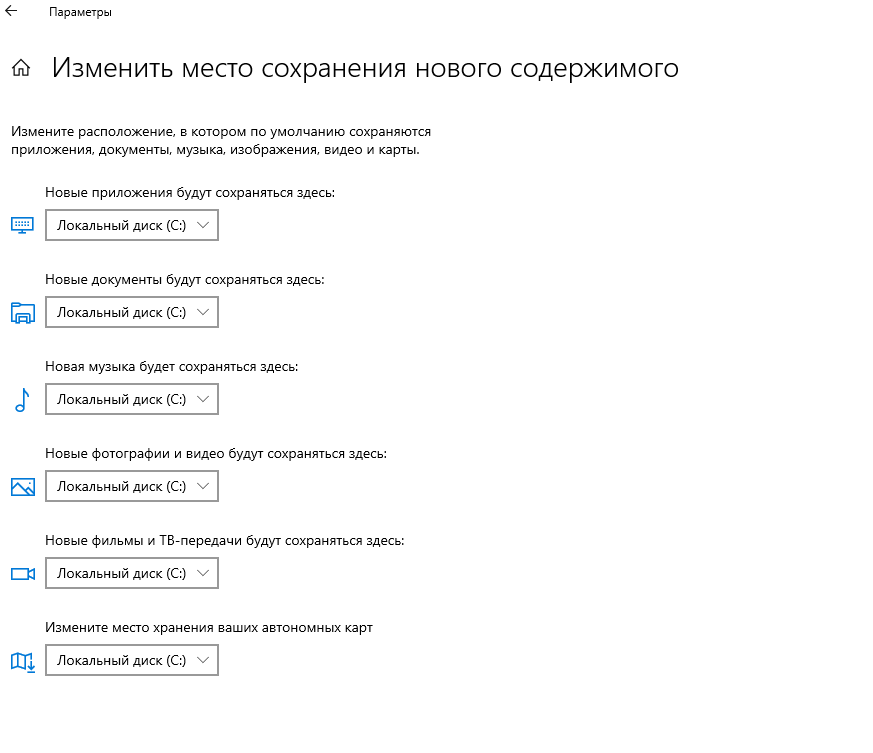
**2)**



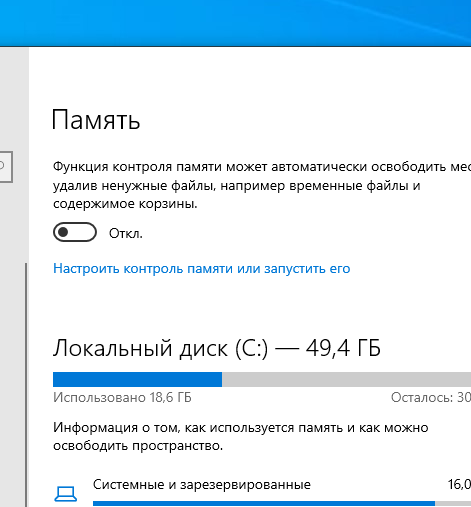
**3)**



**4)**



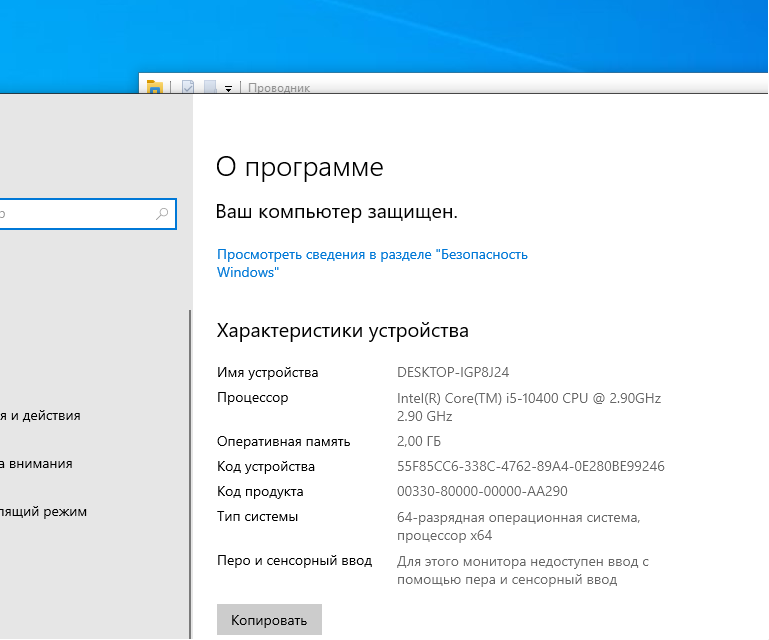
**5)**



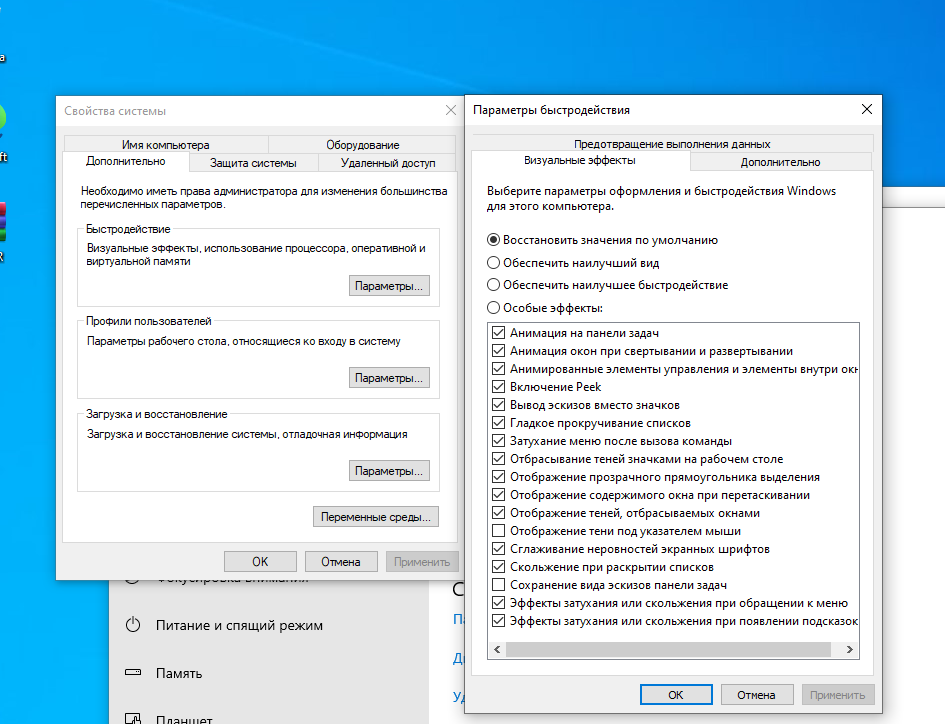
**6)**

**№7**

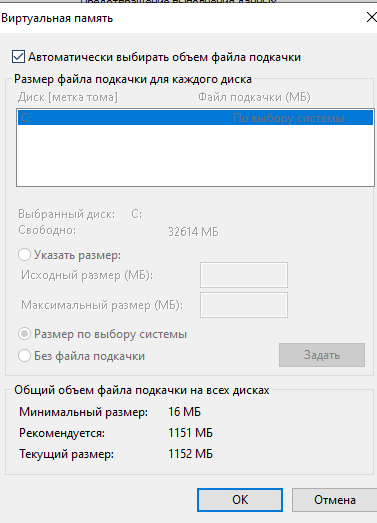
Т.к это виртуальная машина большую часть всего места занимают системные файлы , основа системы без которых она не будет работать , вторыми по размеру являются системные приложения без которых ОС потеряет возможность управления понятный пользователю. Третье место это временные файлы оставшиеся после установки WinRAR.



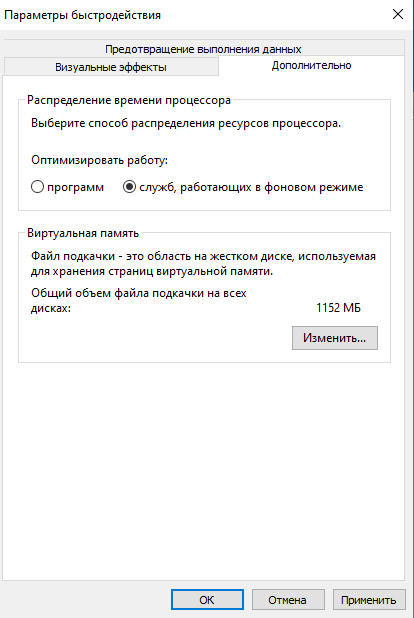
**7)**



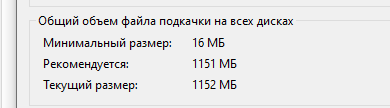
**8)**



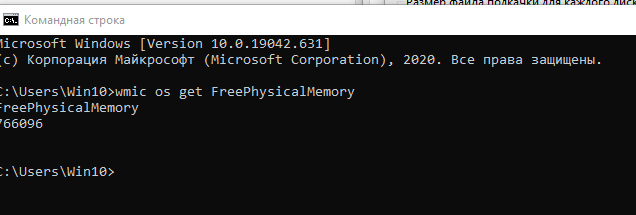
**9)**



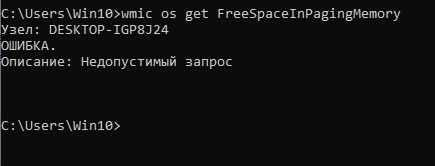
**10)**



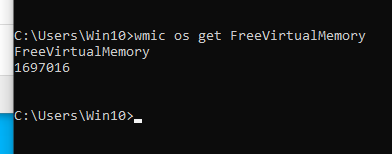
**11)**

****

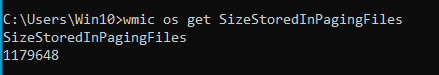
**12)**

****

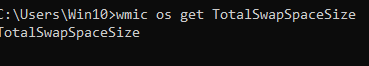
**13)**

****

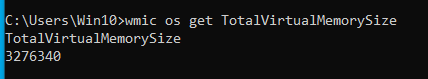
**14)**

****

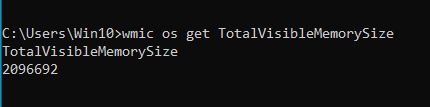
**15)**

****

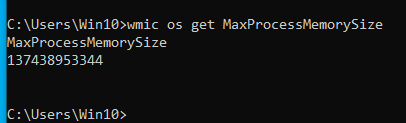
**16)**

****

**17)**

****

**18)**

****

**19)**

1) wmic os get FreePhysicalMemory; - Возвращает количество свободной физической памяти в байтах.

2) wmic os get FreeSpaceInPagingMemory; - Возвращает количество свободного пространства в файле подкачки (paging file) в байтах.

3) wmic os get FreeVirtualMemory; - Возвращает количество свободной виртуальной памяти в байтах.

4) wmic os get MaxProcessMemorySize; - Возвращает максимальный размер памяти, который может использовать один процесс.

5) wmic os get SizeStoredInPagingFiles; - Возвращает общий размер данных, хранящихся в файлах подкачки (paging files).

6) wmic os get TotalSwapSpaceSize; - Возвращает общий размер пространства подкачки (swap space).

7) wmic os get TotalVirtualMemorySize; - Возвращает общий размер виртуальной памяти.

8) wmic os get TotalVisibleMemorySize; - Возвращает общий размер видимой физической памяти.

Каждая из этих команд возвращает соответствующее значение в байтах, которое можно использовать для мониторинга и анализа использования ресурсов операционной системы Windows.

Лабораторная работа №7

**Цель**: сформировать навыки работы с Диспетчером задач, Командной

строкой, получение практических навыков управления процессами и самостоятельной работы с документацией команд.

**Перечень оснащения и оборудования, источников**: ПК, раздаточный

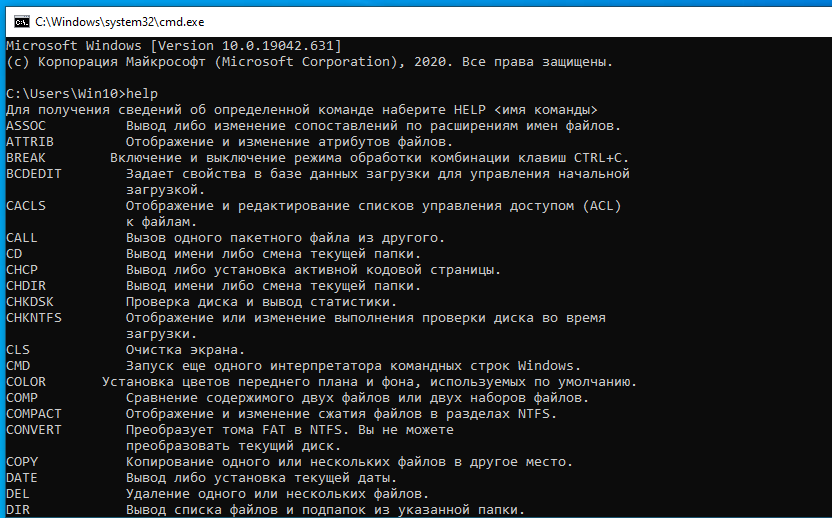
материал

**Задание:**

1.Просмотр списка запущенных процессов и завершение ра-

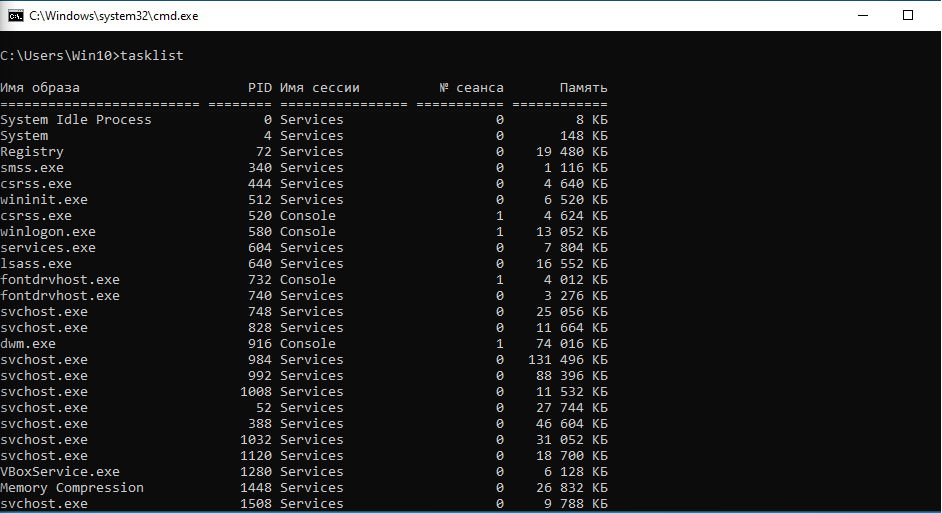
боты любого из них, в командной строке

1) Используя специальную команду отразить список команд Windows



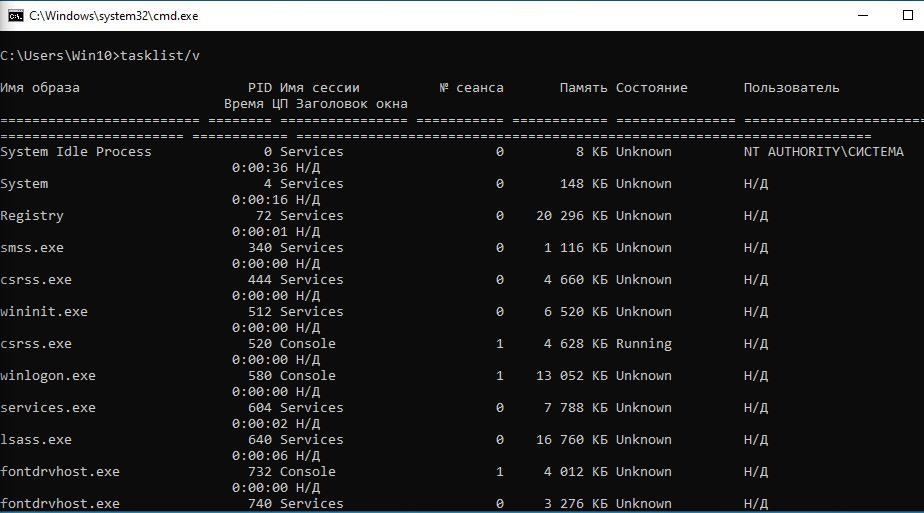
2) Используя специальную команду отразить список, выполняющихся

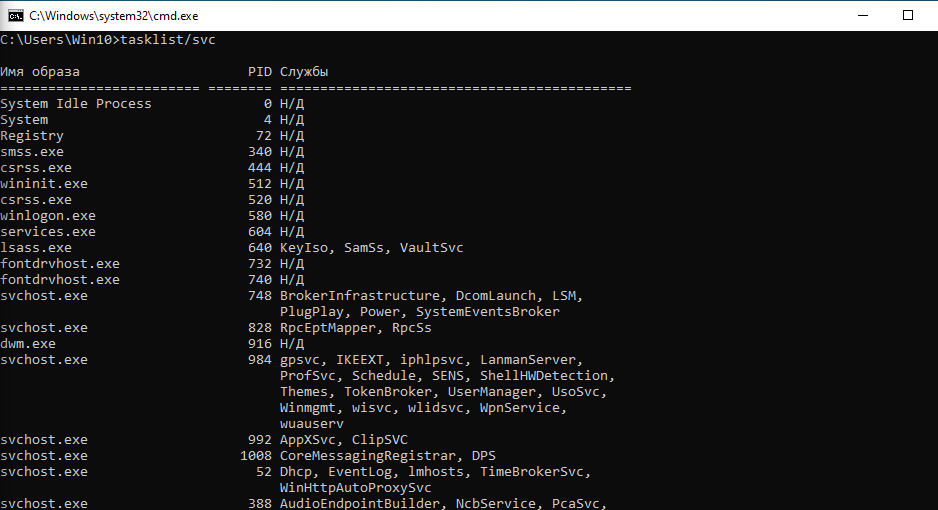
служб и приложений.

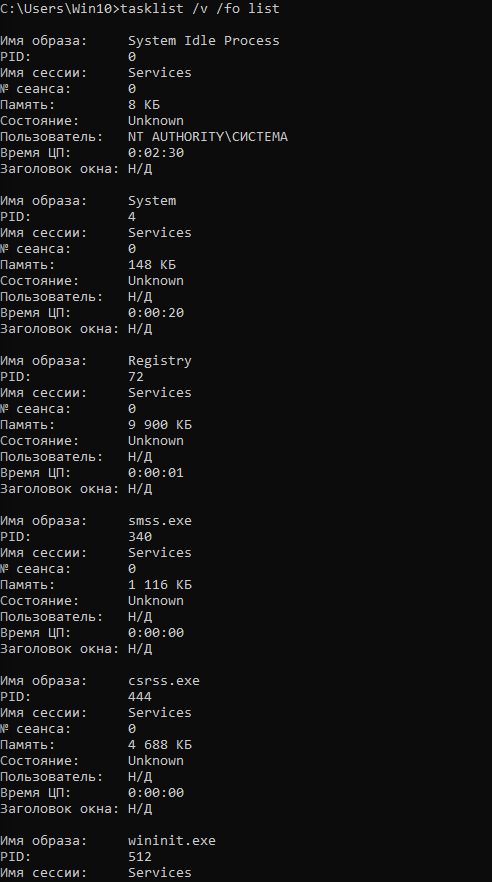


3) Задайте команду, отражающую список, выполняющихся служб и

приложений с расшифровкой

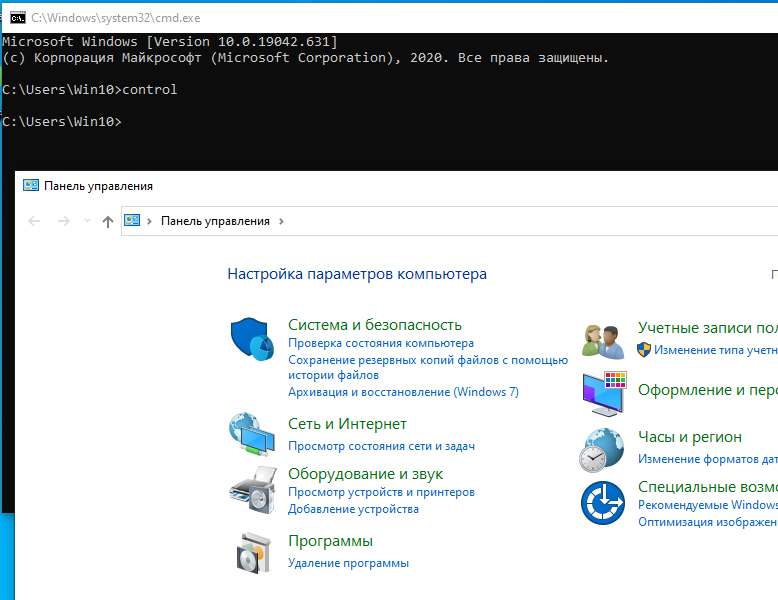


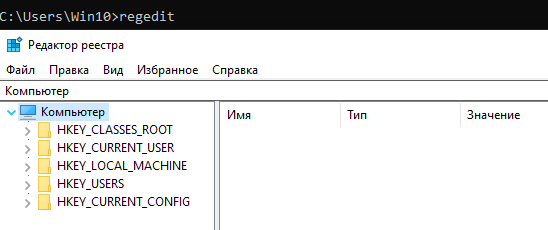


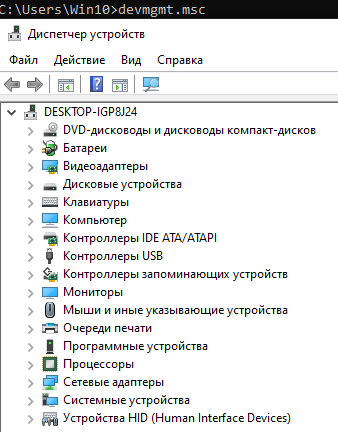


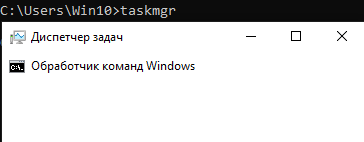
4) Запустить системные приложения и компоненты через Командную

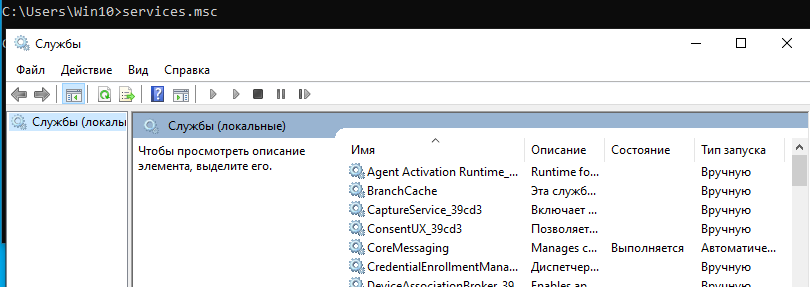
строку.

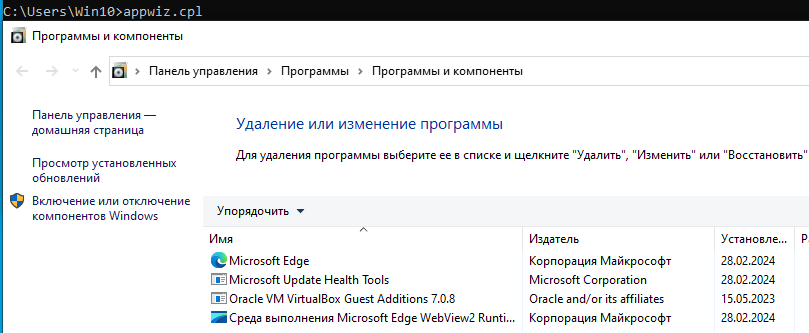


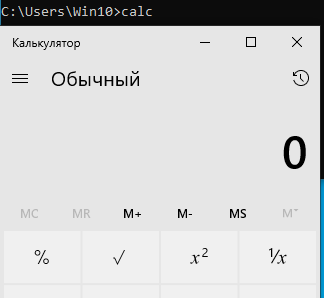


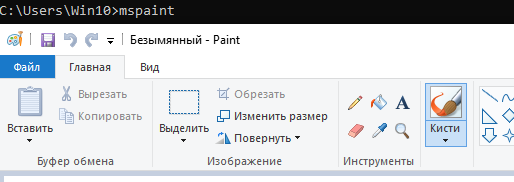


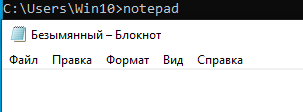








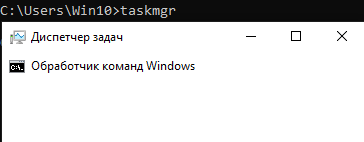




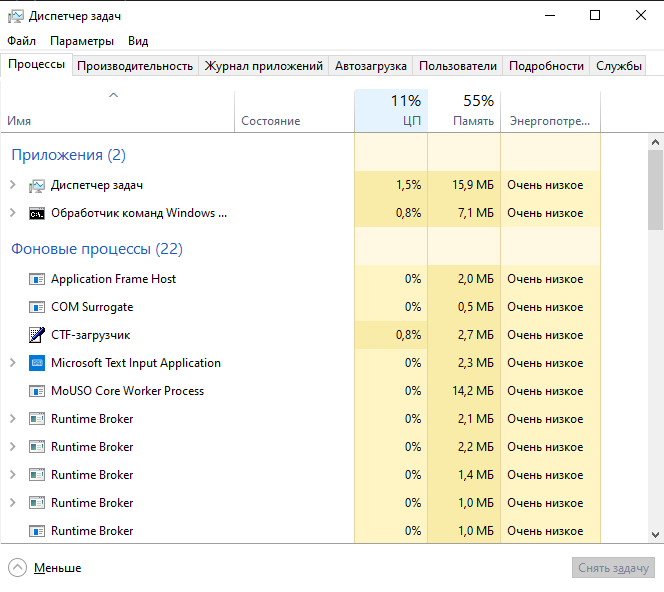
**1. Работа с процессами в Диспетчере задач Порядок работы.**

1) Запустить программу Диспетчер задач, используя Командную

строку.



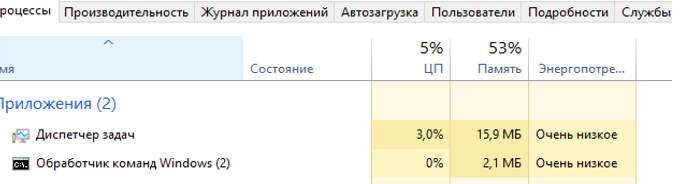
2) На вкладке Процессы Диспетчера задач изменить количество столбцов: Состояние, Память, ЦП, Энергопотребление.



Сначала надо кликнуть правой кнопкой мышки по названиям столбцов и выбрать галочками, какие столбы вам нужны. Потом во вкладке значения ресурсов нужно выбрать в каких единицах измерения нужно отобрадать потребление.

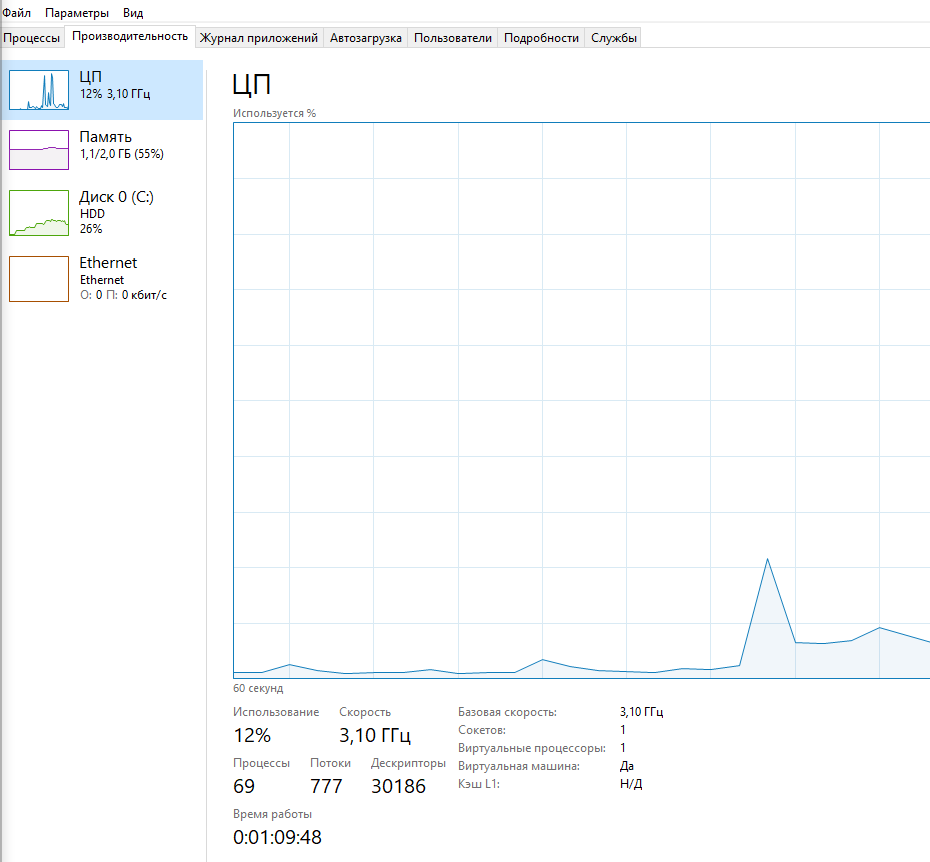
3)Диспетчер окон рабочего стола(Очень маленькое потребление)

4)



На момент работы запущено 2 приложения и 22 фоновых процесса. Процессор загружен на 5% памяти выделено 53%, а под открытые приложения выделено 18 Мб оперативной памяти.

5)



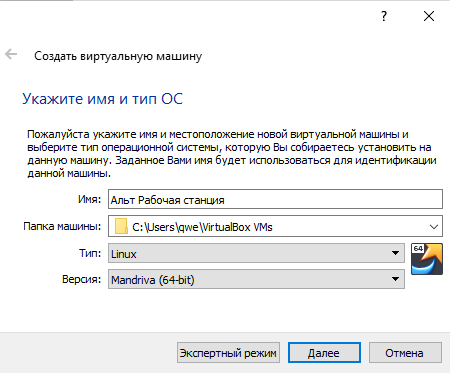
На момент работы 777 потоков.

**Контрольные вопросы:**

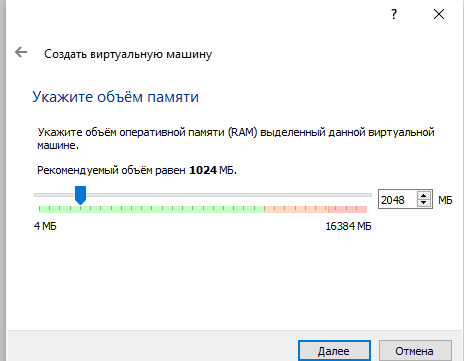
1. Командная строка – это консоль, которая напрямую работает с операционной системой.
2. Нужно написать в строку выполнить “cmd.exe”
3. Tasklist, Tasklist /v, Tasklist /v /fo, Tasklist /v /csv

Лабораторная работа №8

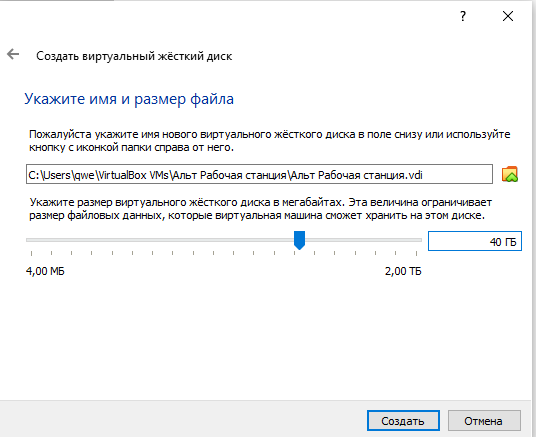
**Создаем виртуальную машину**



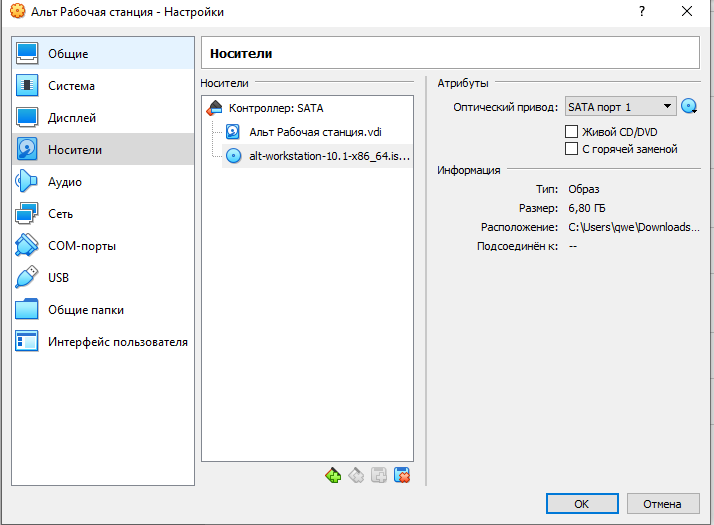
**Указываем кол-во оперативной памяти**

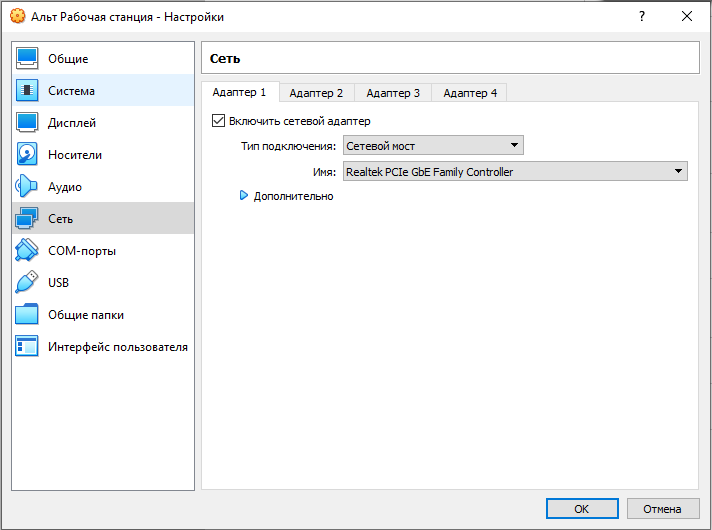


**Указываем кол-во памяти диска**

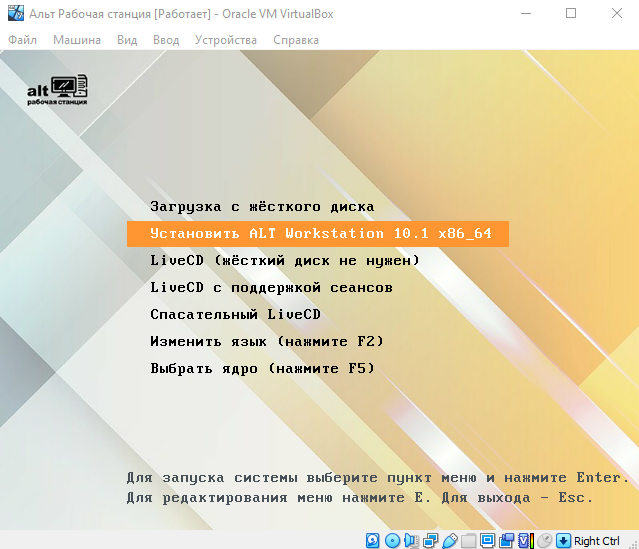


**Указываем путь к расположению iso-файлу**

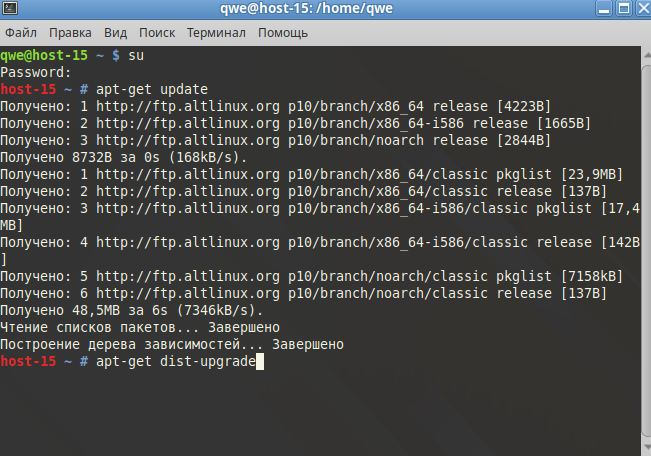


**Указываем тип подключения**

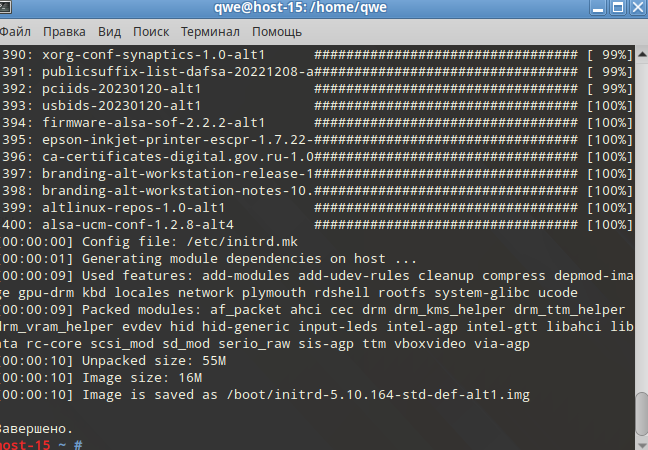
**Устанавливаем Альт Рабочую станцию**



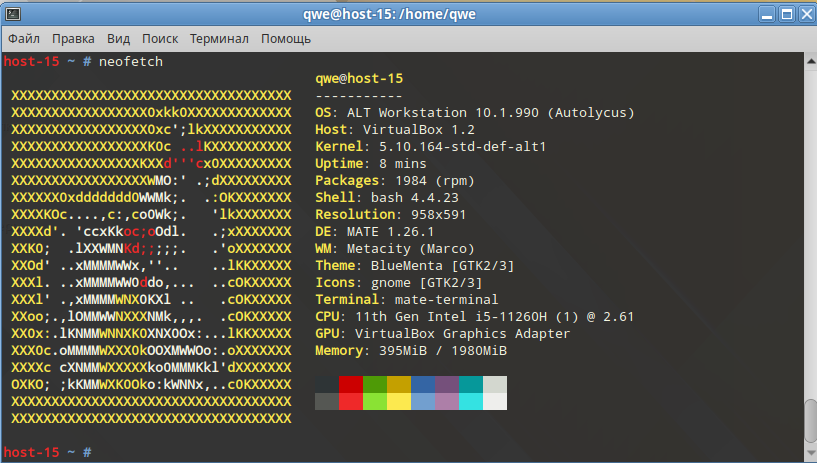
**Обновляем**

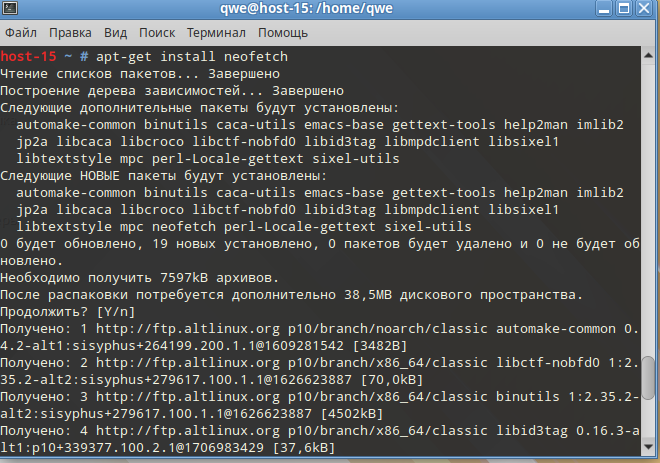


**Успешно установили**

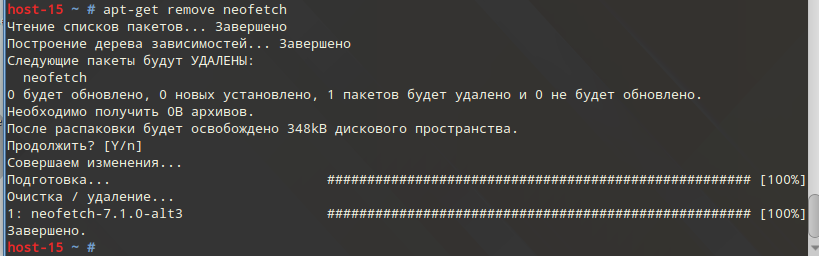


**Скачиваем Neofetch**

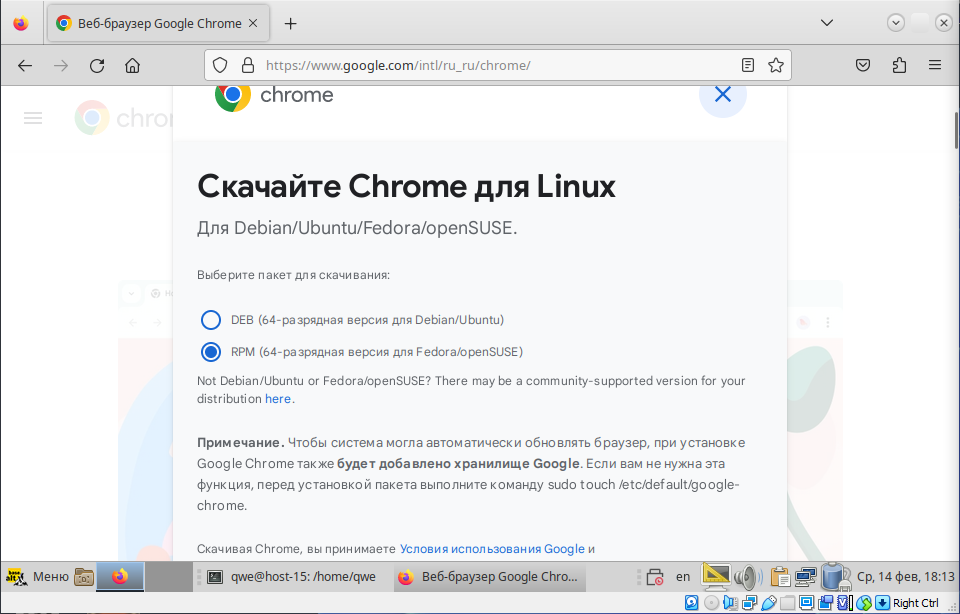


**Задача Neofetch**

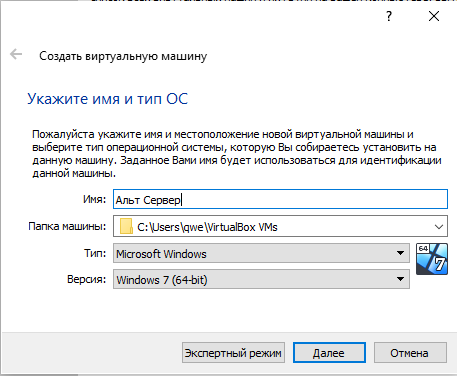
**Удаляем Neofetch**



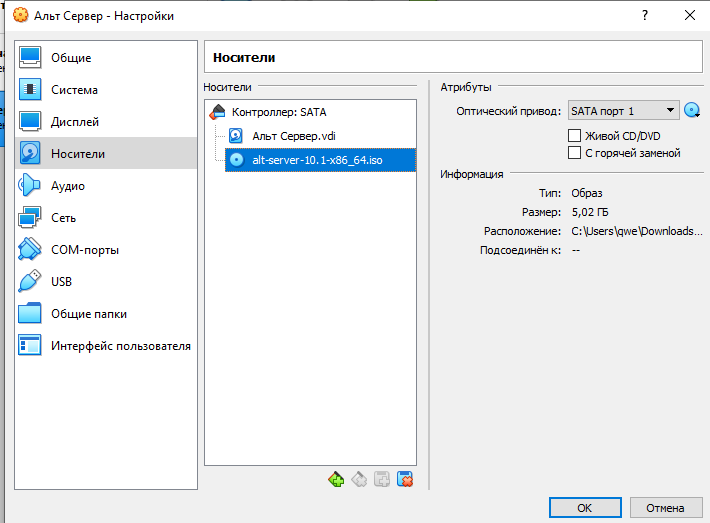
**Скачиваем GC**

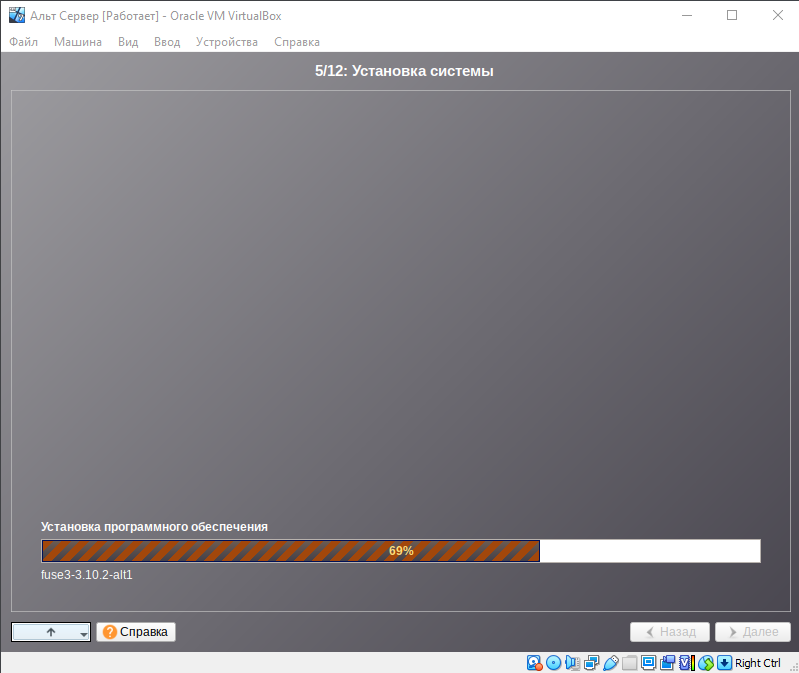


**Создаем Альт сервер**



**Указываем расположение Iso-файла**





Ошибка



Лабораторная работа №9

РАБОТА С СЕТЕВОЙ ФАЙЛОВОЙ СИСТЕМОЙ

**Цель**: сформировать навыки выполнять команды в командной строке,

создавать каталоги, файлы и манипулировать ими, навыки работы в Norton

Com-mander

**1)**

Исследование и оптимизация жесткого диска

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | Модель жёсткого диска | | Vbox cd-rom |
| 2 | Имена лог. Дисков | | с |
| 3 | Файловая система | | htfs |
| 4 | Емкость | | 53.8 |
| 5 | Объем занятого места | До очистки | 3.03 |
| После очистки | 3.03 |
| 6 | Процент свободного места | До очистки | 6 |
| После очистки | 6 |
| 7 | Размер кластера | | 36 |
| 8 | Всего файлов | | 24675 |
| 9 | Средний размер файла | | 100 мб |
| 11 | Количество фрагментированных файлов | До дефрагментации | 13678 |
| После дефрагментации | 4078 |
| 12 | Всего фрагментировано, % | До дефрагментации | 37 |
| После дефрагментации | 9 |
| 13 | Фрагментация Файлов, % | До дефрагментации | 37 |
| После дефрагментации | 9 |

**2)**

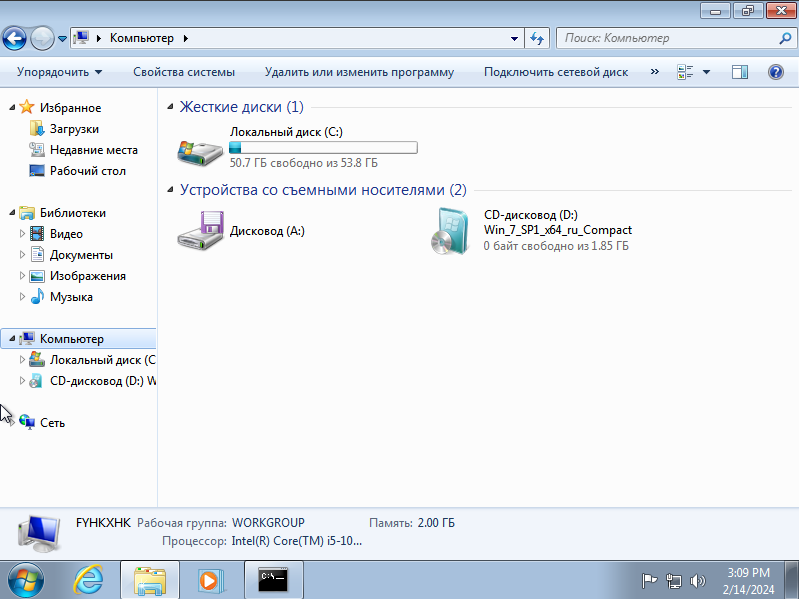


Рис 1. Определила имеющиеся дисков

**3)**

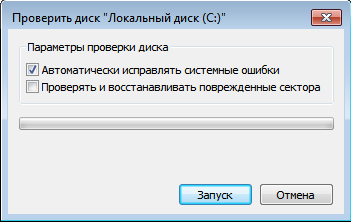


Рис 2. Проверка графики

**4)**

Проверка диска через консоль

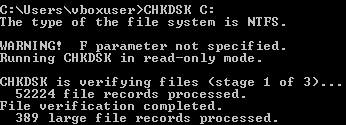


Рис 3. Команда CHKDSK C:



Рис 4. Команда CHKDSK C:\Windows\file.txt

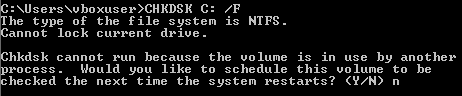


Рис 5. Команда CHKDSK C: /F

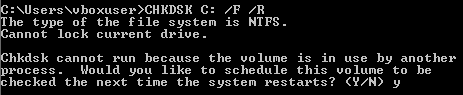


Рис 6. Команда CHKDSK C: /F /R

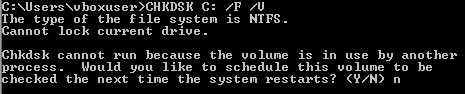


Рис 7. Команда CHKDSK C: /F /U



Рис 8. Команда CHKDSK C: /F /X



Рис 9. Команда CHKDSK C: /L  


Рис 10. Команда CHKDSK C: /F /L

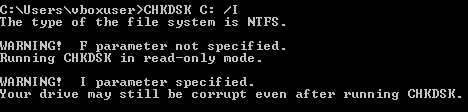


Рис 11. Команда CHKDSK C: /I

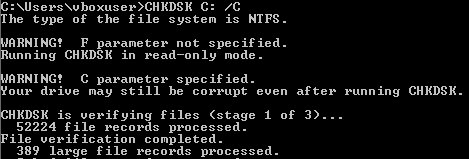


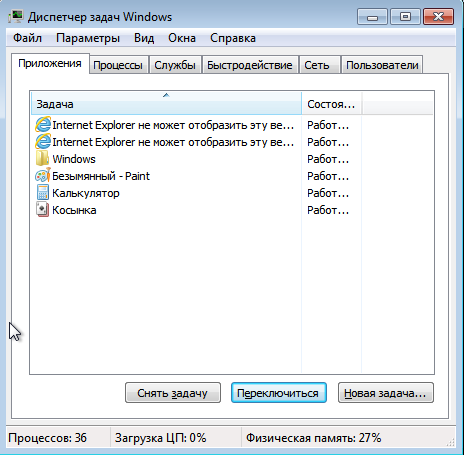
Рис 12. Команда CHKDSK C: /C

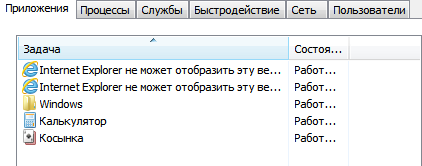


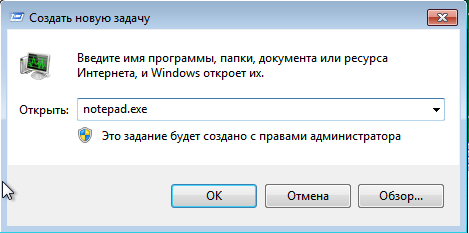
Рис 13. Команда CHKDSK C: /B

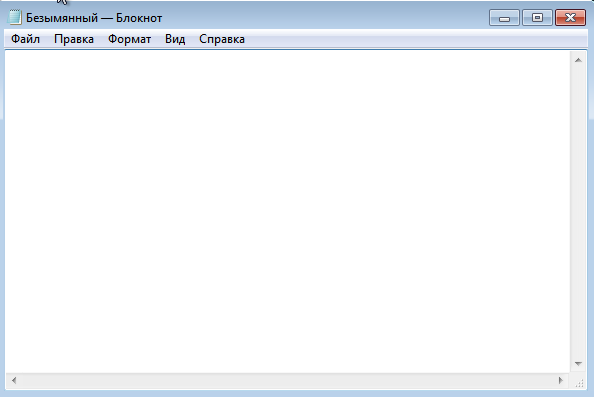
**5)**

Работа с диспетчером задач.

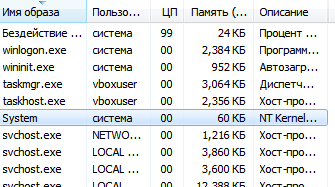


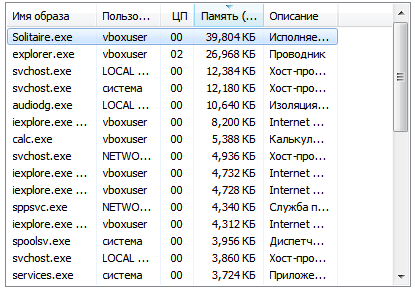


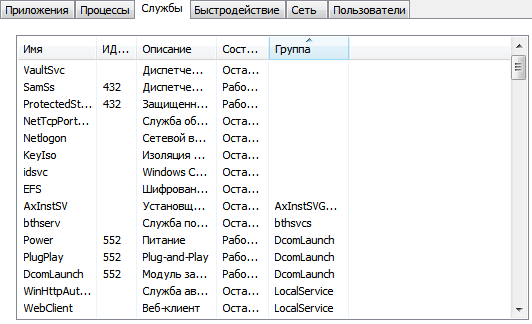


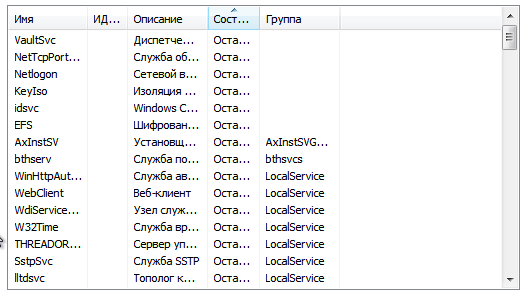
















Лабораторная работа №10

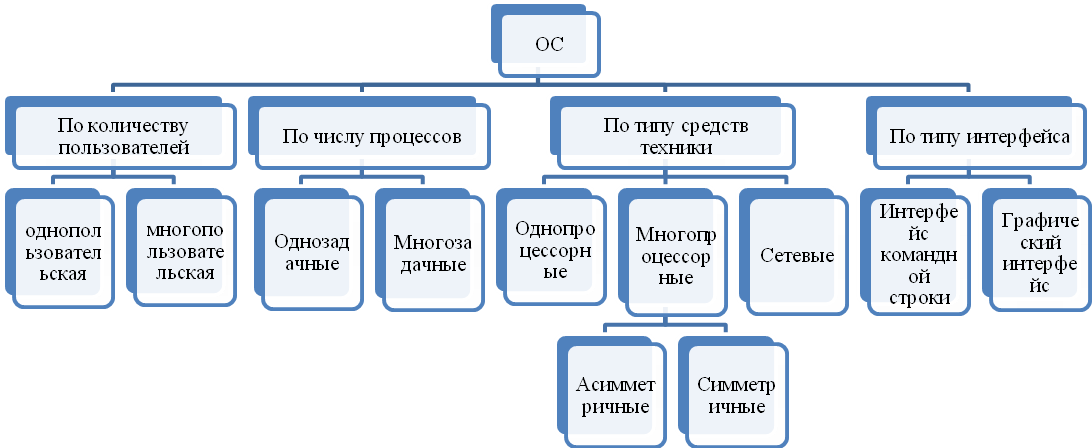
**Цель:** познакомить с сетевым программным обеспечением,

его функциями и структурой.

**Оборудование:** персональный компьютер с выходом в Интернет

**1)**

1. **NOS** (Network Operating System) это специализированная операционная система, предназначенная для управления сетевыми ресурсами и обеспечения взаимодействия компьютеров в сети. Основные функции NOS включают в себя управление файлами и папками, аутентификацию и авторизацию пользователей, управление доступом к ресурсам (серверам, принтерам и т. д.), обеспечение безопасности и мониторинг работы сети.

2. 

**2)**

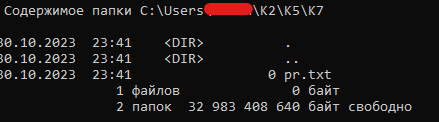
1. Важный вопрос сетевых ресурсов заключается в управлении доступом к данным и ресурсам в сети, обеспечении безопасности информации, а также оптимизации производительности сети.

2. Сервер выполняет дополнительные функции, такие как хранение данных, обработка запросов от клиентов, обеспечение доступа к общим ресурсам сети, а также обеспечение безопасности и мониторинга сетевой активности.

3. Преимущества комбинированной клиентско-серверной сетевой операционной системы включают более гибкую архитектуру, распределение ресурсов между клиентами и серверами, а также повышенную надежность и отказоустойчивость. Однако недостатки могут включать сложность настройки и управления системой, а также возможные проблемы совместимости между клиентами и серверами.

Индивидуальная работа №3

Создание заданной структуры файлов и каталогов на диске D с помощью команд MS DOS

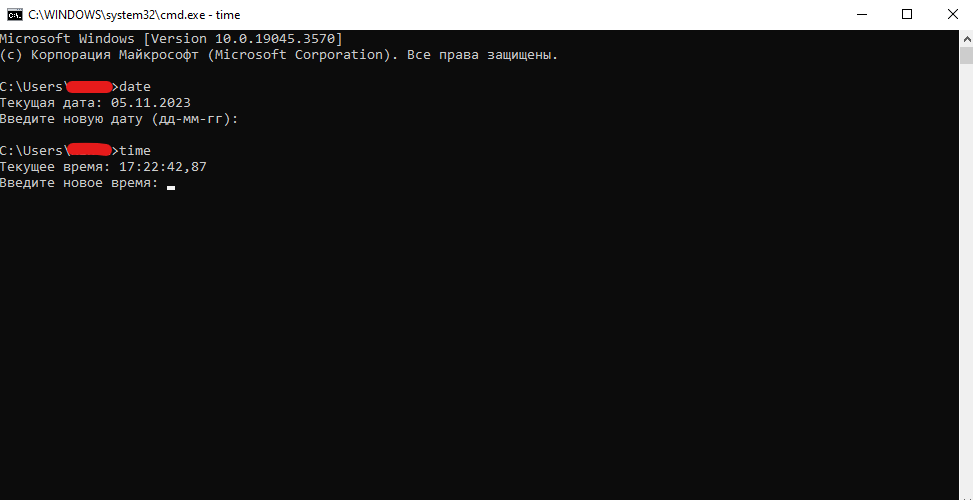


Индивидуальная работа №4

1. Создайте на рабочем столе папку Test.

2. Запустите командную строку cmd.exe (Пуск — ввод с клавиатуры «cmd» без кавычек

3. Проверьте системные дату и время с помощью команд date и time. Для этого в командной



4. С помощью утилиты cd измените текущий каталог на каталог Test, созданный Вами ранее

5. С помощью команды md создайте каталог с именем Cat.

6. Используя команду copy con, создайте файл с именем File.txt. (Команда copy con означает копирование с консоли, т. е. с клавиатуры). После данной команды введите следующий текст: Ваши Ф.И.О., группа и название лабораторной работы. Закройте файл сочетанием клавиш Ctrl+Z.

7. С помощью команды dir просмотрите список созданных объектов в папке Test. Команда в общей сложности фиксирует 3 каталога (папки), т. к. первая метка указывает на текущий

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

8. В каталоге Cat с помощью команды copy создайте две копии файла File.txt – File1.txt и File2.txt

Изображение выглядит как текст, снимок экрана, Шрифт, линия

Автоматически созданное описание

9. Объедините файлы File1.txt и File2.txt в файл oneFile.txt с помощью команды copy.

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

10. Просмотрите полученный файл oneFile с помощью утилиты copy.

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

11. C помощью команды move переместите файл oneFile.txt в папку Test.



12. С помощью команды rename переименуйте файл oneFile.txt в newFile.txt



13. С помощью той же команды смените расширения у всех файлов в каталоге Cat



14. Измените расширение файлов на исходное.



15. Создайте в папке Test две цепочки вложенных каталогов с помощью команды mkdir: а) Каталог Dog, содержащий каталоги Bulldog и Sheltie. б) Каталог Bird, содержащий каталоги Flying и Non-flying. Каталог Non-flying содержит два подкаталога: Ostrich и Penguin

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

16. Используя команду tree. постройте дерево каталогов папки Test

Изображение выглядит как текст, снимок экрана, Шрифт, диаграмма

Автоматически созданное описание

17. Удалите все файлы, содержащие в названии слово new, из каталога Test посредством утилиты del



18. Удалите все файлы из каталога Cat, можно использовать команду del \*.\*.



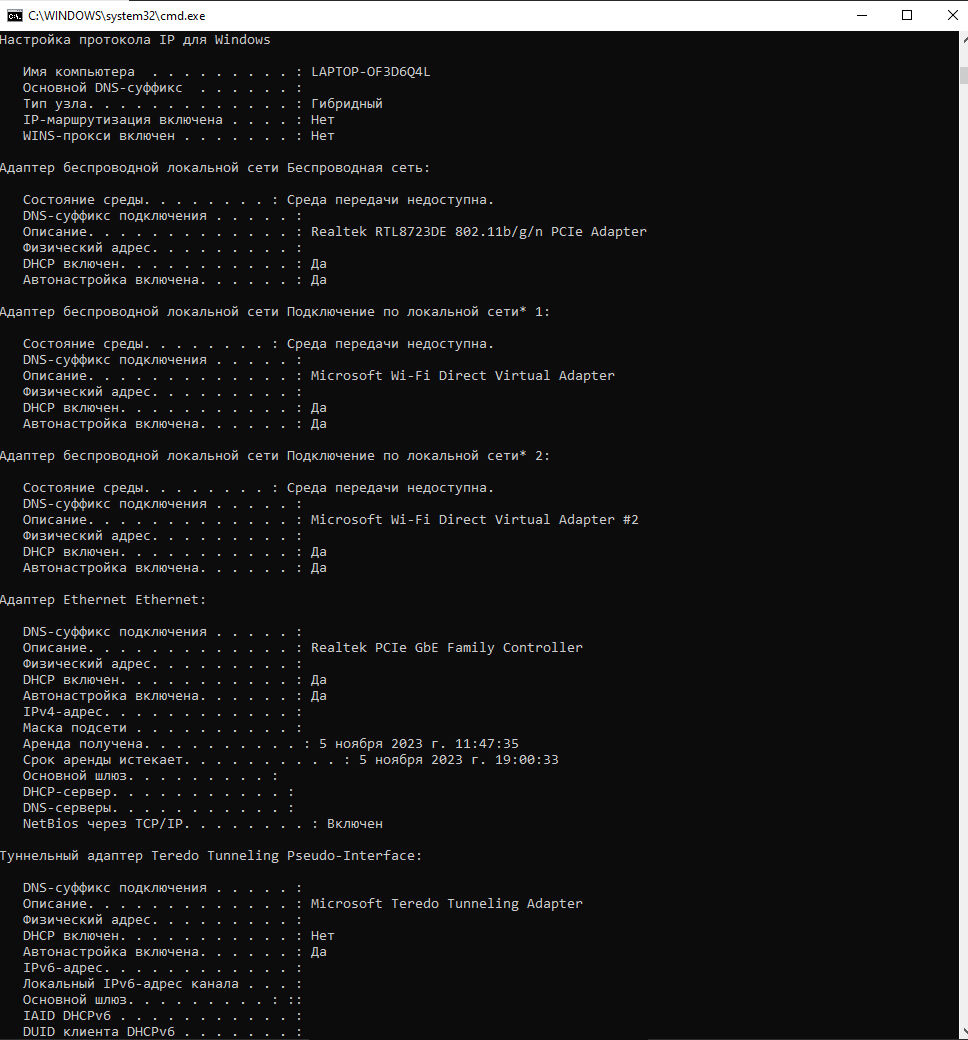
19. Удалите каталоги Bird и Dog с помощью команды rd /s, при необходимости укажите путь к удаляемому дереву каталогов

Изображение выглядит как текст, Шрифт, снимок экрана

Автоматически созданное описание

**2 ЧАСТЬ**

**1.**



**2.**

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

**3.**

Количество промежуточных устройств: 7

IP-адреса всех промежуточных устройств:

* 103.123.3.241
* 41.2.66.1
* 41.2.80.3
* 41.2.81.13
* 181.232.60.122
* 10.3.5.1
* 1.251.251.241

**4.**

1) Основной шлюз - 108.123.3.241

2) 3 любых компьютера

* 108.123.3.241
* 108.123.3.242
* 108.123.3.243

Индивидуальная работа №5

Описать что установлено:

|  |  |  |
| --- | --- | --- |
| **Name** | **Version** | **Installed** |
| .NET Framework | 4,0,30319,0 | Нет |
| .NET Framework | 2,0,50727,0 | Нет |
| .NET Framework | 2,0,50727,1 | Нет |
| Active Directory Service Interface | 5,0,00,0 | Да |
| Address Book 7 | 10,0,19041,2673 | Да |
| Browsing Enhancements | 11,1,19041,0 | Да |
| DirectDrawEx | 4,71,1113,0 | Да |
| Dynamic HTML Data Binding | 11,1,19041,0 | Да |
| HTML Help | 10,0,19041,1 | Да |
| Internet Explorer Core Fonts | 11,1,19041,0 | Да |
| Internet Explorer Help | 11,1,19041,0 | Да |
| Internet Explorer Setup Tools | 11,1,19041,0 | Да |
| Microsoft Windows Media Player | 12,0,10011,16384 | Да |
| Microsoft Windows Media Player | 12,0,10011,16384 | Нет |
| Microsoft Windows Media Player 12.0 | 12,0,10011,16384 | Да |
| Microsoft Windows Script 5.6 | 5,6,0,8833 | Да |
| MSN Site Access | 4,9,9,2 | Да |
| Offline Browsing Pack | 11,1,19041,0 | Да |

Таблицы групп пользователей:

|  |  |
| --- | --- |
| **Group Name** | **Member Name** |
| IIS\_IUSRS | NT AUTHORITY\IUSR |
| KLAdmins | NT SERVICE\ksnproxy |
| Администраторы | KB37-1-118-C14\localboss |
| Администраторы | FADOMAIN\Domain Admins |
| Администраторы | FADOMAIN\KB-Workstation\_Admins |
| Администраторы | KB37-1-118-C14\Администратор |
| Гости | KB37-1-118-C14\Гость |
| Отсутствует | Администратор |
| Отсутствует | Гость |
| Отсутствует | DefaultAccount |
| Отсутствует | WDAGUtilityAccount |
| Отсутствует | Admin |
| Отсутствует | localboss |
| Пользователи | NT AUTHORITY\Прошедшие проверку |
| Пользователи | KB37-1-118-C14\localboss |
| Пользователи | FADOMAIN\Domain Users |
| Пользователи | NT AUTHORITY\ИНТЕРАКТИВНЫЕ |
| Пользователи журналов производительности | NT AUTHORITY\ИНТЕРАКТИВНЫЕ |
| Управляемая системой группа учетных записей | KB37-1-118-C14\DefaultAccount |

Переменные среды:

|  |  |
| --- | --- |
| **Name** | **Variable Value** |
| \_\_COMPAT\_LAYER | DetectorsAppHealt |
| ALLUSERSPROFILE | C:\ProgramData |
| APPDATA | C:\Users\227363\AppData\Roaming |
| ChocolateyInstall | C:\ProgramData\chocolatey |
| CHROME\_CRASHPAD\_PIPE\_NAME | \\.\pipe\crashpad\_7884\_BOSZMFIAVSMBYFFU |
| CHROME\_RESTART | Microsoft Edge|Microsoft Edge перестал работать. Перезапустить его?|LEFT\_TO\_RIGHT |
| CommonProgramFiles | C:\Program Files (x86)\Common Files |
| CommonProgramFiles(x86) | C:\Program Files (x86)\Common Files |
| CommonProgramW6432 | C:\Program Files\Common Files |
| COMPONENT\_INSTALLER\_DIR | C:\Users\227363\AppData\Local\Microsoft\Edge\User Data |
| COMPUTERNAME | KB37-1-118-C14 |
| ComSpec | C:\Windows\system32\cmd.exe |
| DriverData | C:\Windows\System32\Drivers\DriverData |
| EDGE\_BROWSER\_PID | 7884 |
| EDGE\_METRICS\_CLIENT\_ID\_HASH | -3806260577389700653 |
| EDGE\_METRICS\_SESSION\_ID | 0 |
| EDGE\_RUNTIME\_VARIATIONS\_SEED\_ETAG |  |
| EDGE\_USER\_DATA\_DIR | C:\Users\227363\AppData\Local\Microsoft\Edge\User Data |
| EDGE\_UX\_CONFIG\_CORRELATION\_ID |  |
| EDGE\_VARIATIONS\_SEED\_ETAG |  |
| HOMEDRIVE | C: |
| HOMEPATH | \Users\227363 |
| LOCALAPPDATA | C:\Users\227363\AppData\Local |
| LOGONSERVER | \\KBDC |
| NUMBER\_OF\_PROCESSORS | 6 |
| OS | Windows\_NT |
| Path | C:\Python\Python311\Scripts\;C:\Python\Python311\;C:\Program Files\Common Files\Oracle\Java\javapath;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\Microsoft SQL Server\130\Tools\Binn\;C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\170\Tools\Binn\;C:\Program Files\Azure Data Studio\bin;C:\Program Files\Git\cmd;C:\Program Files (x86)\dotnet\;C:\Program Files\nodejs\;C:\ProgramData\chocolatey\bin;C:\Users\227363\AppData\Local\Microsoft\WindowsApps; |
| PATHEXT | .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC;.PY;.PYW |
| PROCESSOR\_ARCHITECTURE | x86 |
| PROCESSOR\_ARCHITEW6432 | AMD64 |
| PROCESSOR\_IDENTIFIER | Intel64 Family 6 Model 158 Stepping 13, GenuineIntel |
| PROCESSOR\_LEVEL | 6 |
| PROCESSOR\_REVISION | 9e0d |
| 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 |
| PT8HOME | C:\Program Files\Cisco Packet Tracer 8.2.1 |
| PUBLIC | C:\Users\Public |
| SESSIONNAME | Console |
| SystemDrive | C: |
| SystemRoot | C:\Windows |
| TEMP | C:\Users\227363\AppData\Local\Temp |
| TMP | C:\Users\227363\AppData\Local\Temp |
| USERDNSDOMAIN | FA.RU |
| USERDOMAIN | FADOMAIN |
| USERDOMAIN\_ROAMINGPROFILE | FADOMAIN |
| USERNAME | 227363 |
| USERPROFILE | C:\Users\227363 |
| VBOX\_MSI\_INSTALL\_PATH | C:\Program Files\Oracle\VirtualBox\ |
| windir | C:\Windows |
| ZES\_ENABLE\_SYSMAN | 1 |

IP и MAC адресс:

|  |  |
| --- | --- |
| **Item** | **Value** |
| IP Address | 10.37.12.15 |
| MAC Address | 1C:57:D8:13:BC:D3 |

Процессор:

|  |  |
| --- | --- |
| **Item** | **Value** |
| Device Type | Процессоры |
| Device Name | Intel(R) Core(TM) i9-9990K CPU @ 2.90GHz |
| Description | Intel процессор |
| Manufacturer | Intel |
| Location |  |
| Driver Provider | Microsoft |
| Driver Version | 10.0.19041.2728 |
| Driver Date | 4-21-2009 |
| Status Code | 0 |
| Status Message | OK |
| Class GUID | {50127DC3-0F36-415E-A6CC-4CB3BE910B65} |
| Device ID | ACPI\GENUINEINTEL\_-\_INTEL64\_FAMILY\_6\_MODEL\_158\_-\_INTEL(R)\_CORE(TM)\_I5-9400\_CPU\_@\_2.90GHZ\\_2 |

Программы на автозагрузке:

|  |  |  |
| --- | --- | --- |
| **Program Name** | **Settings Folder** | **Command** |
| Delete Cached Standalone Update Binary | HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce | C:\Windows\system32\cmd.exe /q /c del /q "C:\Users\227363\AppData\Local\Microsoft\OneDrive\StandaloneUpdater\OneDriveSetup.exe" |
| Delete Cached Update Binary | HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce | C:\Windows\system32\cmd.exe /q /c del /q "C:\Users\227363\AppData\Local\Microsoft\OneDrive\Update\OneDriveSetup.exe" |
| desktop.ini | C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\ |  |
| desktop.ini | C:\Users\227363\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ |  |
| MicrosoftEdgeAutoLaunch\_382B3F3BBBE8F9D8E55960B23F5C3D33 | 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\227363\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background |
| SunJavaUpdateSched | HKLM\Software\Microsoft\Windows\CurrentVersion\Run | "C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe" |

Модель жёсткого диска:

|  |  |
| --- | --- |
| Model | Kingston AS350 500GB |

Потребление памяти браузером:

|  |  |  |  |
| --- | --- | --- | --- |
| msedge.exe | 8080 | 259700KB |  |
| msedge.exe | 7904 | 7632KB |  |
| msedge.exe | 7884 | 231980KB |  |

Драйвер:

1084) 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 |  |

Ещё 4 драйвера:

|  |  |
| --- | --- |
| **Item** | **Value** |
| Name | Драйвер Intel процессора |
| Service Type | Kernel Driver |
| State | Stopped |
| Start Mode | Manual |
| Path Name | \SystemRoot\System32\drivers\intelppm.sys |
| Start Name |  |

1156) Драйвер Intel(R) Serial IO I2C Controller

|  |  |
| --- | --- |
| **Item** | **Value** |
| Name | Драйвер Intel(R) Serial IO I2C Controller |
| Service Type | Kernel Driver |
| State | Stopped |
| Start Mode | Manual |
| Path Name | \SystemRoot\System32\drivers\iaLPSSi\_I2C.sys |
| Start Name |  |

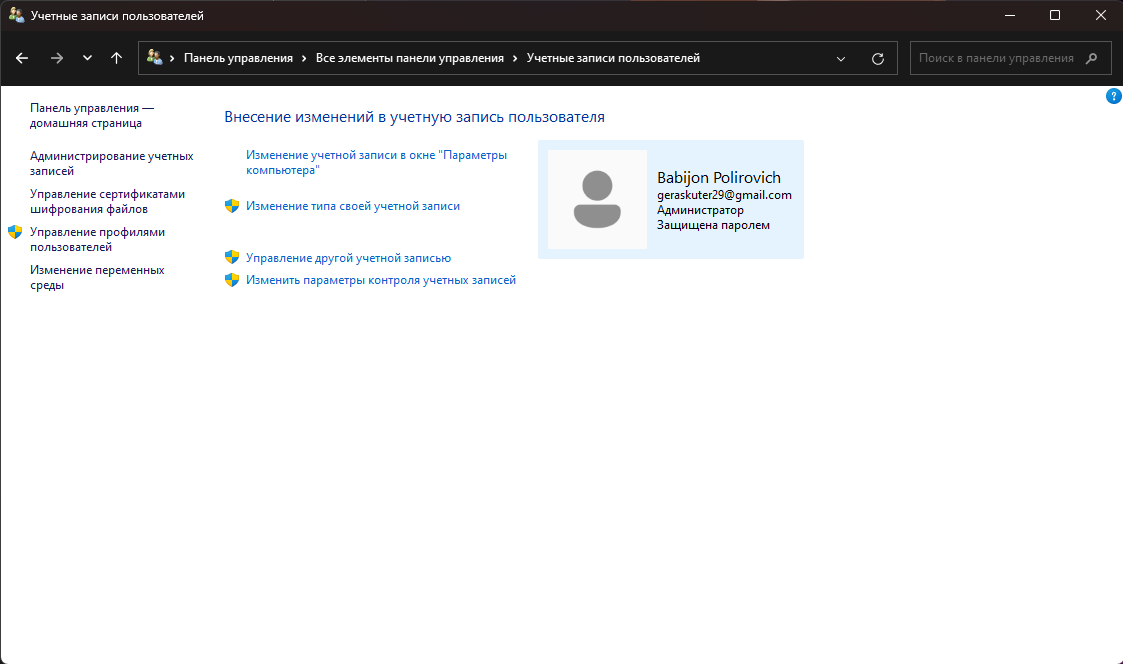
1157) Драйвер IP ARP для удаленного доступа

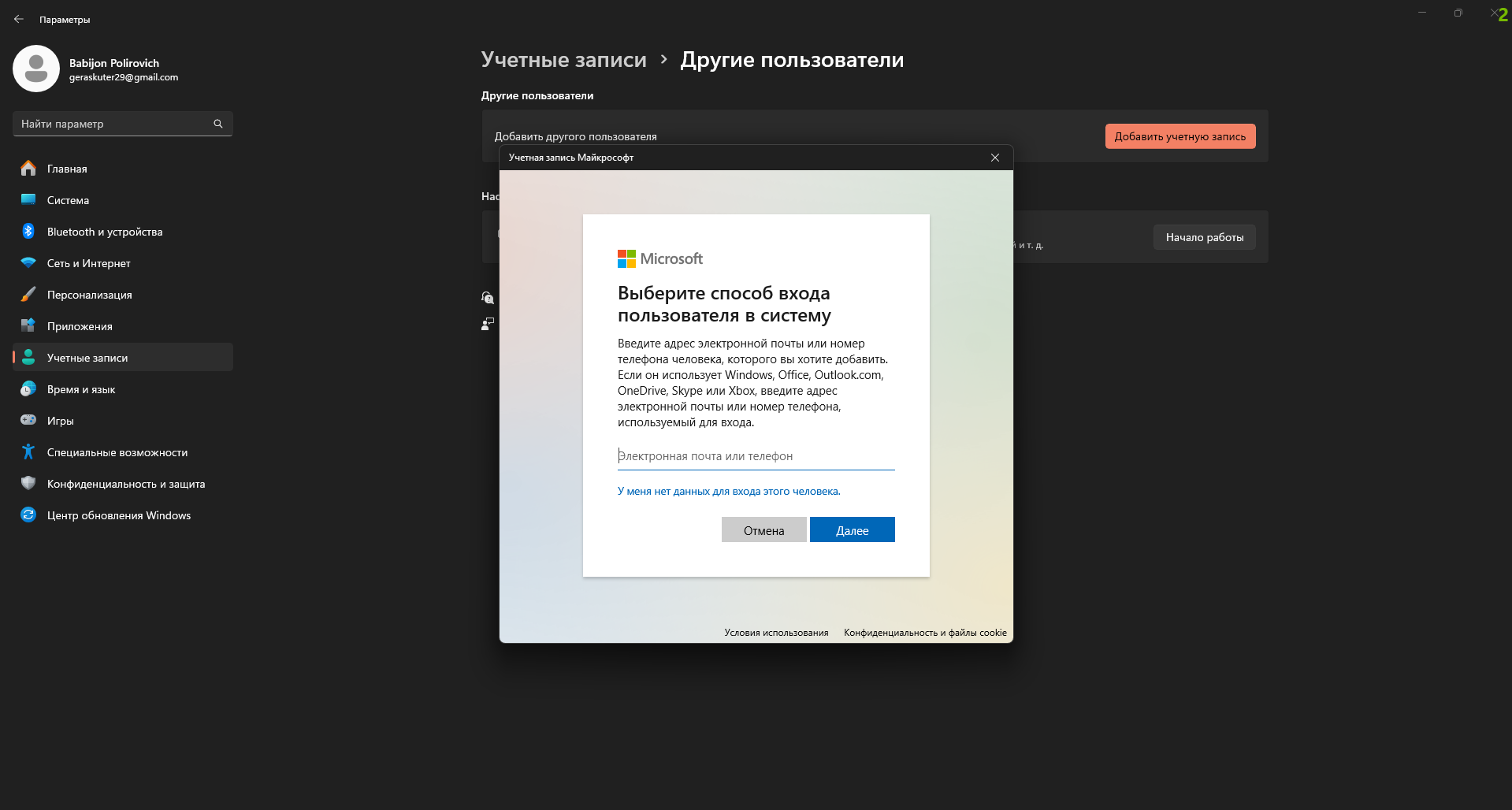
|  |  |
| --- | --- |
| **Item** | **Value** |
| Name | Драйвер IP ARP для удаленного доступа |
| Service Type | Kernel Driver |
| State | Running |
| Start Mode | Automatic |
| Path Name | System32\DRIVERS\wanarp.sys |
| Start Name |  |

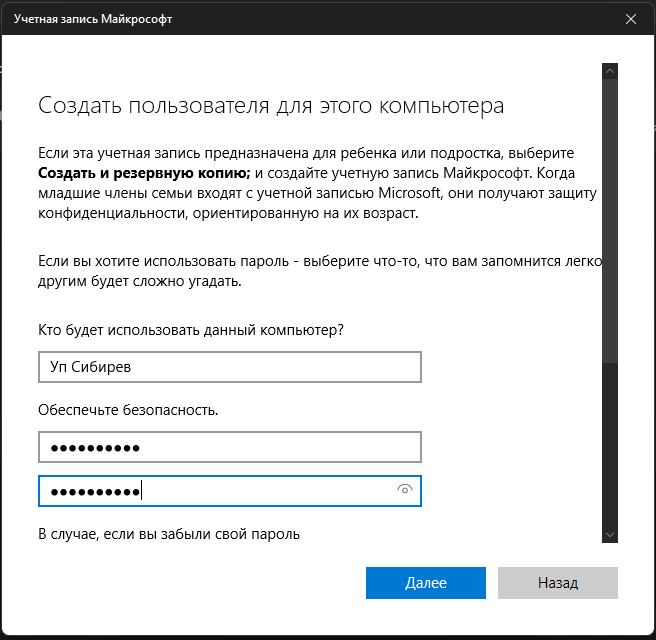
1152) Драйвер CD-ROM дисковода

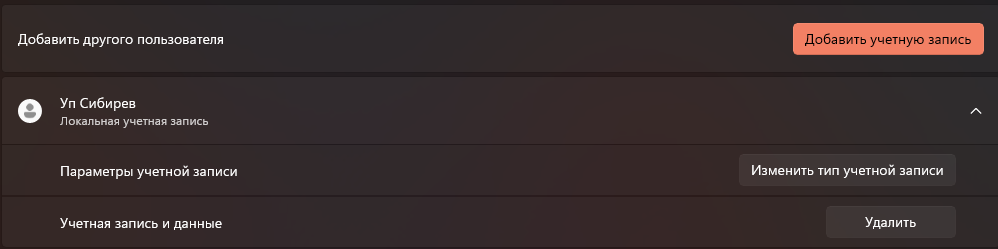
|  |  |
| --- | --- |
| **Item** | **Value** |
| Name | Драйвер CD-ROM дисковода |
| Service Type | Kernel Driver |
| State | Running |
| Start Mode | System |
| Path Name | \SystemRoot\System32\drivers\cdrom.sys |
| Start Name |  |

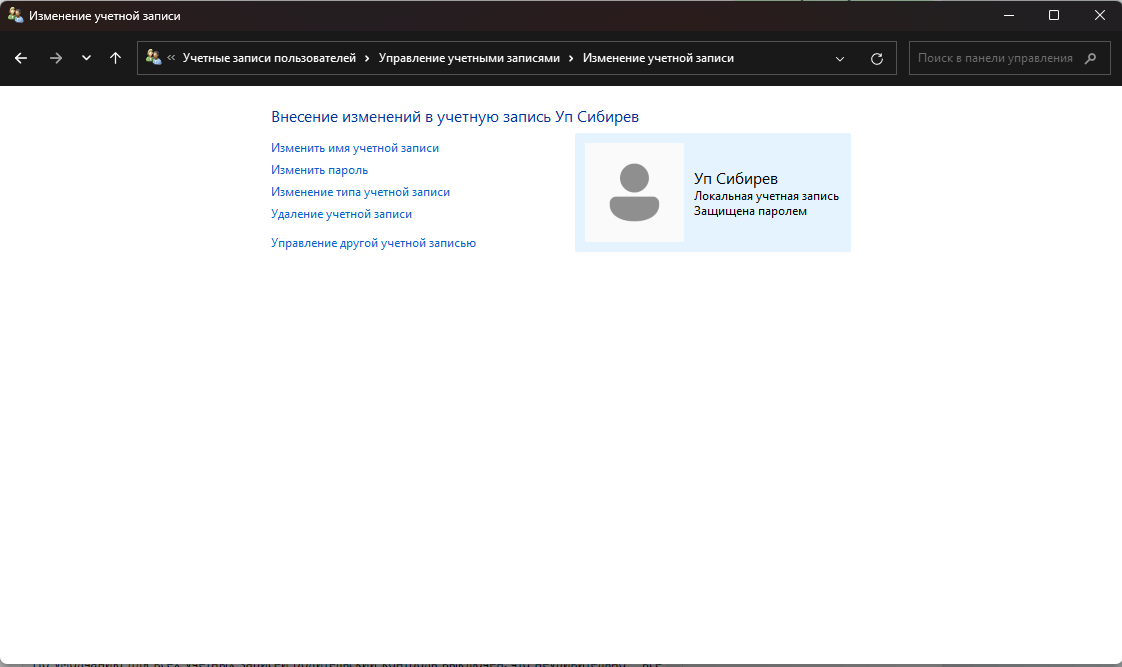
Учебная практика №1

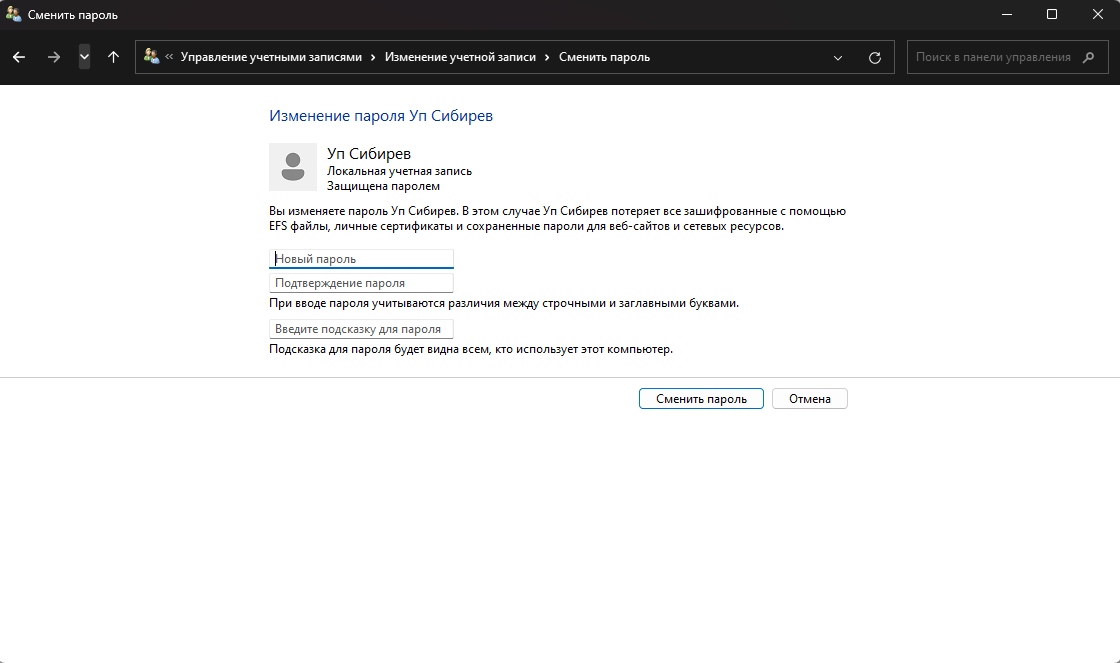


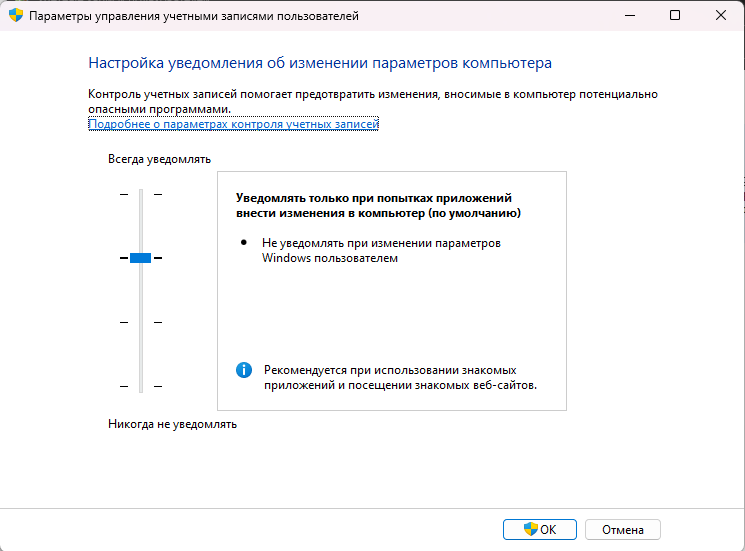












Учебная практика №3

**«Создание и настройка параметров мандатного управления доступом»**

**по дисциплине «Безопасность Astra Linux»**

**Цель работы:** изучить и освоить администрирование основных параметров мандатного управления доступом в ОССН Astra Linux Special Edition с применением графических утилит и консольных команд.

**Порядок выполнения работы**

1. Отключила блокировку экрана. Для этого нужно щелкнуть ПКМ на рабочем столе и выбрать «Свойства».
2. Создала учётную запись «user» c паролем «Student123». Добавила учетную запись «user» во вторичную группу astra-admin.

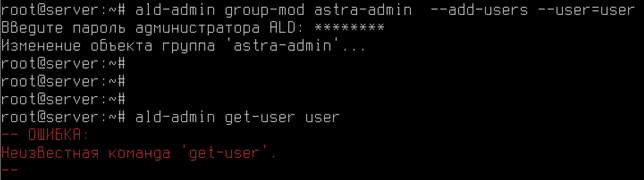


Рис. 1. Добавление учётной записи «user» во вторичную группу astra-admin

1. Начала работу со входа в ОССН в графическом режиме с учётной записью пользователя «user».

https://studfile.net/html/47320/250/html_48yoYFzjSP.jjR2/htmlconvd-PyvDzF_html_4836ed7d9bab7063.png

Рис. 2. Вход в учётную запись пользователя «user»

1. Запустила графическую утилиту редактирования учетных записей пользователей «Управление политикой безопасности» через команду sudo fly-admin-smc.

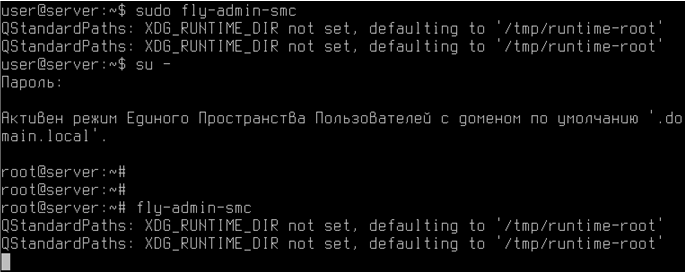


Рис. 3. Запуск графической утилиты

1. Модифицировать параметры мандатного управления доступом, для этого осуществить следующие действия:
   1. открыть раздел «Уровни» и выбрать «0: Уровень\_0» и переименовать данный уровень доступа: «Уровень0»;
   2. выполнить создание уровня доступа с именем «Уровень\_4», задав значение равное 4, после чего проверить наличие записи «Уровень\_4» в списке «Уровни»;
   3. выполнить обратное переименование: «Уровень0» в «Уровень\_0».



Рис.4. Создание уровней доступа

1. Создала учётную запись пользователя user1, установив максимальный уровень доступа (конфиденциальности): «Уровень\_4».

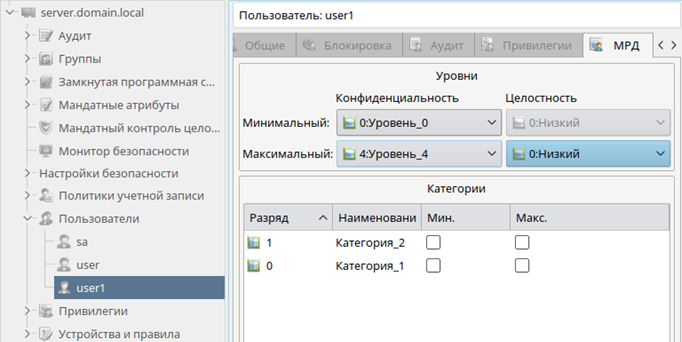


Рис. 5. Создание пользователя user1 с уровнем доступа 4

1. Выполнила удаление уровня доступа 4 из раздела «Уровни» путем выбора в контекстном меню пункта «Удалить».

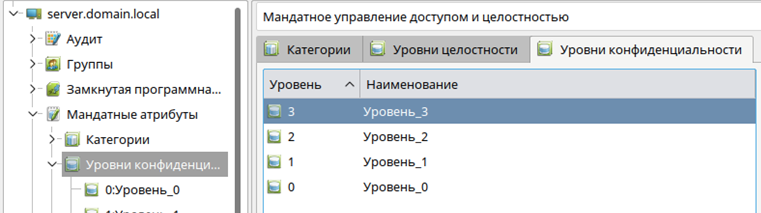


Рис. 6. Удаление уровня доступа

1. Открыла учётную запись пользователя user1 и в закладке «Дополнительные» в элементе «Максимальный уровень» проверить наличие записи «(4)», при этом, в списке выбора уровня «Уровень\_4» будет отсутствовать. Создать учетные записи user20, user30, user40. Задать в произвольном порядке значения для параметров «Конфиденциальность», «Целостность», «Категории».

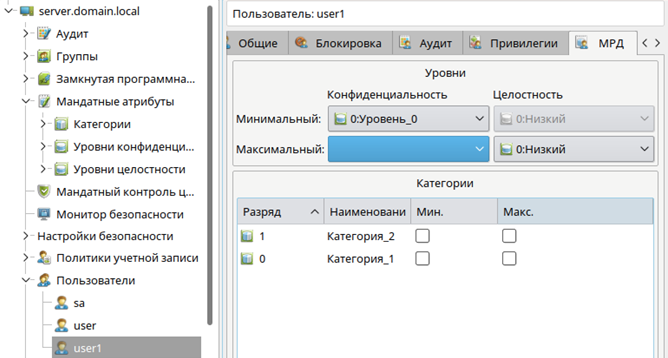


Рис. 7. Проверка отсутствия уровня 4

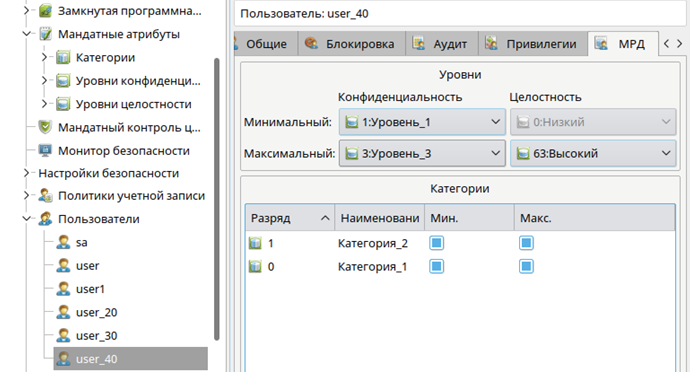


Рис. 8. Создание новых учётных записей

1. Ознакомилась с содержимым каталога etc/parsec/macdb. Вывести в терминал Fly параметры мандатного управления доступом для учётной записи пользователей user1, user20, user30, user40. Мандатные атрибуты, назначенные конкретным учётным записям пользователей, перечисляются в каталоге /etc/parsec/macdb. Для выполнения задания 7 осуществить следующие действия:
   1. запустить терминал Fly и перейти в каталог /etc/parsec/macdb (команда cd /etc/parsec/macdb )
   2. вывести на экран содержимое каталога /macdb ( ls )
   3. просмотреть содержимое файлов в каталоге /macdb ( sudo cat “имя файла” )
   4. прочитать параметры учётной записи user1 командой sudo grep “user1” \*
   5. определить максимальный уровень доступа учётной записи user1 командой sudo grep «user1» \* | cut -d : -f 5
   6. определить минимальный уровень доступа учётной записи user1 командой sudo grep «user1» \* | cut -d : -f 3 и проверить его соответствие данным, отображаемым в графической утилите «Управление политикой безопасности».

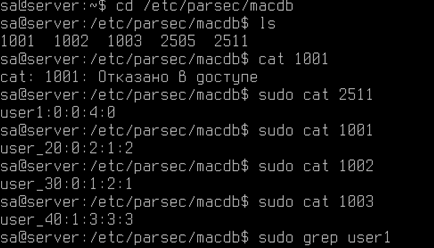


Рис. 9. Пункты a-c

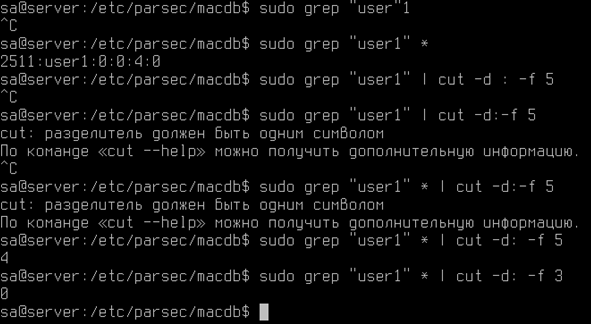


Рис. 10. Пункты d-f

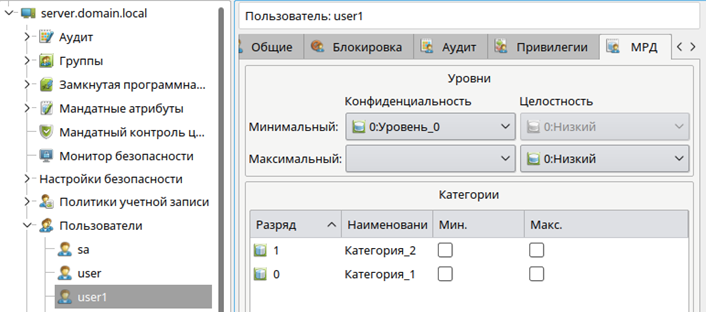


Рис. 11. Проверка вывода команд на соответствие выводу графической утилиты

1. Создала неиерархические категории с использованием графической утилиты «Управление политикой безопасности». Для этого выполнить следующие действия:
   1. в разделе «Категории» удалить все Категории.
   2. в разделе «Категории» создать новую неиерархическую категорию с именем «Otdel1», «Разряд» — 0;
   3. в разделе «Категории» создать новые неиерархические категории: «Otdel2» («Разряд» — 1), «Upravlenie» («Разряд» — 2).

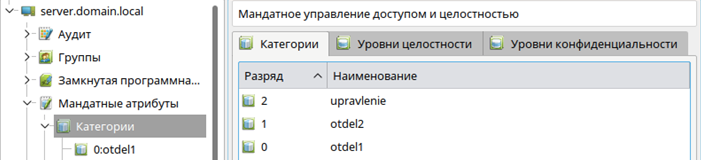


Рис. 12. Создание новой иерархической категории

1. Изменила набор неиерархических категорий с использованием графической утилиты «Управление политикой безопасности» (sudo fly-admin-smc), для этого выполнить следующие действия в разделе «Категории»:
   1. выбрать неиерархическую категорию «Otdel1» и ввести наименование «Отдел\_1»;
   2. аналогично переименовать неиерархические категории «Otdel2» и «Upravlenie» в «Отдел\_2» и «Управление» соответственно;
   3. проанализировать возможность одновременного изменения элемента «Разряд».

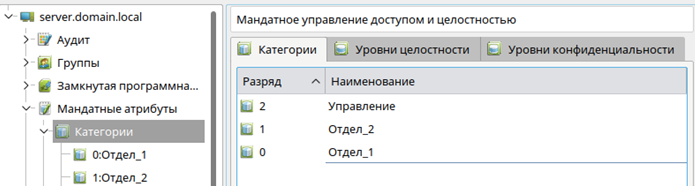


Рис. 13. Ввод наименований

1. Изменила мандатный уровень доступа с использованием графической утилиты «Управление политикой безопасности», для этого выполнить следующие действия:
   1. создать новую группу с именем «office1» и задать первичную группу учётной записи пользователя user1 — «office1»;
   2. создать новую учетную запись пользователя user2 и установить её первичную группу — «officel»;
   3. в закладке «МРД» осуществить попытку выбора минимального набора неиерархических категорий — «Отдел\_2» и проанализировать результат;
   4. в закладке «МРД» выбрать максимальный уровень доступа — «Уровень\_3», максимальный набор неиерархических категорий — «Отдел\_2», после чего задать минимальный набор неиерархических категорий — «Отдел\_2»;
   5. открыть параметры учётной записи пользователя user1 и выбрать максимальный уровень доступа — «Уровень\_3», максимальный набор неиерархических категорий — «Отдел\_1», минимальный набор неиерархических категорий — «Отдел\_1»;.
   6. создать учётную запись пользователя rukoffice1 и задать первичную группу: «office1» ;
   7. в закладке «МРД» выбрать максимальный уровень: «Уровень\_3», максимальный набор категорий: «Отдел\_1», «Отдел\_2», «Управление».

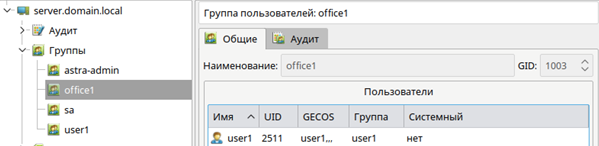


Рис. 14. Создание новой группы

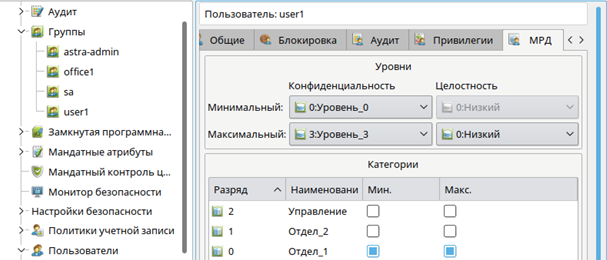


Рис. 15. Создание новой учётной записи

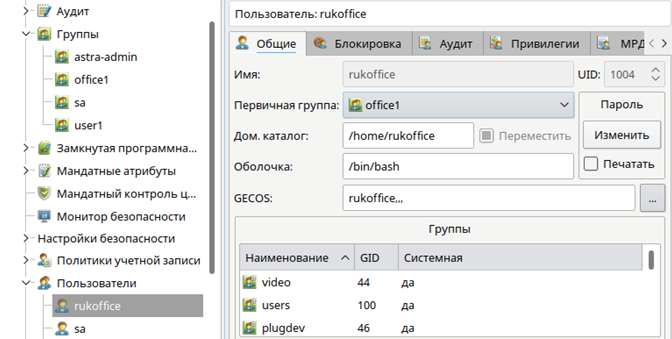


Рис. 16. Выполнение пункта c

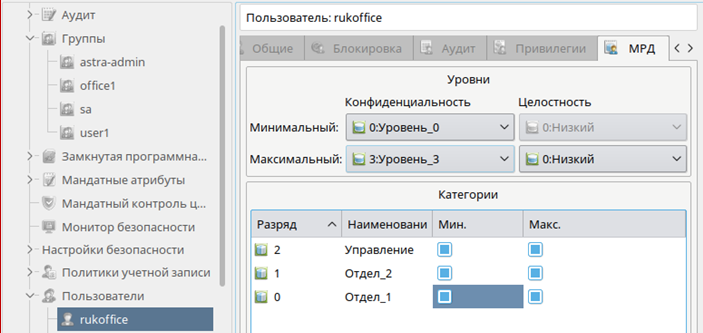


Рис. 17. Выполнение пункта d

1. Создала общий каталог для работы от имени учётных записей пользователей userl, user2, rukoffice1 в каталоге /home/work. Для работы от имени учётных записей пользователей с наборами неиерархическими категорий «Отдел\_1», «Отдел\_2» и «Управление» выделить отдельные каталоги «otdel1», «otdel2» и «upr» соответственно.

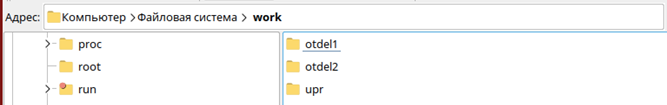


Рис. 18. Структура каталогов

1. При этом обеспечила хранение файлов с различными уровнями конфиденциальности в каталогах с использованием специального атрибута CCNR, для чего осуществить следующие действия:
   1. запустить терминал Fly в «привилегированном» режиме командой sudo fly-term;
   2. Прочесть информацию по командам mkdir, chown и chmode в приложении для практической работы.
   3. создать каталог work и задать параметры мандатного и дискреционного управления доступом командами:

*mkdir /home/work*

*chown user /home/work -v (назначение user владельцем каталога)*

*ls –lh (посмотрите изменения параметра “владелец” для каталога work)*

*chown :office1 /home/work –v (назначение группы)*

*ls –lh (посмотрите изменения параметра “группа” для каталога work)*

*chmod 750 /home/work*

*pdp-flbl 3:0:Отдел\_1,Отдел\_2,Управление:ccnr /home/work –v*

* 1. создать каталог для работы от имени учётных записей пользователей с набором неиерархических категорий «Отдел\_1» и задать параметры мандатного и дискреционного управления доступом командами:

*cd /home/work*

*mkdir otdel1*

*chown user1:office1 otdel1*

*chmod 770 otdel1*

*pdp-flbl 3:0:Отдел\_1:ccnr otdel1*

* 1. создать каталог для работы от имени учётных записей пользователей с набором неиерархических категорий «Отдел\_2» и задать параметры мандатного и дискреционного управления доступом командами:

*mkdir otdel2*

*chown user2:office1 otdel2*

*chmod 770 otdel2*

*pdp-flbl 3:0:Отдел\_2:ccnr otdel2*

* 1. создать каталог upr для работы от имени учётных записей пользователей с набором неиерархических категорий «Управление» командами:

*mkdir upr*

*chown rukoffice1:office1 upr*

*chmod 770 upr*

*pdp-flbl 3:0:Управление:ccnr upr*

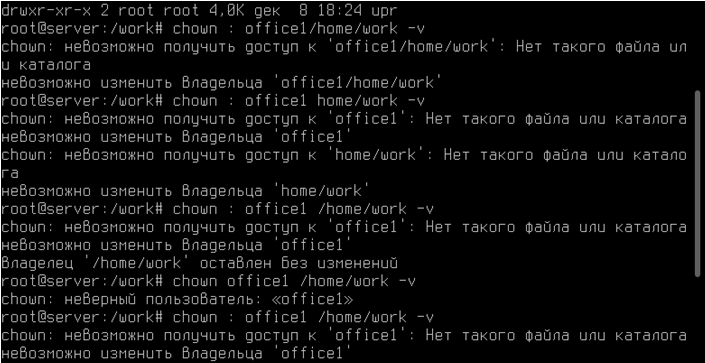


Рис. 19. Задание параметров мандатного и дискреционного управления доступом

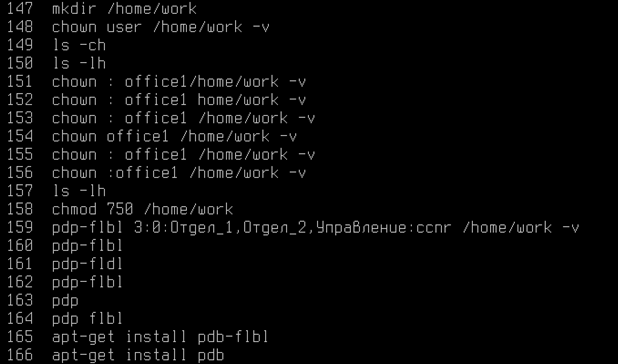


Рис. 20. Листинг команд 14 пункта

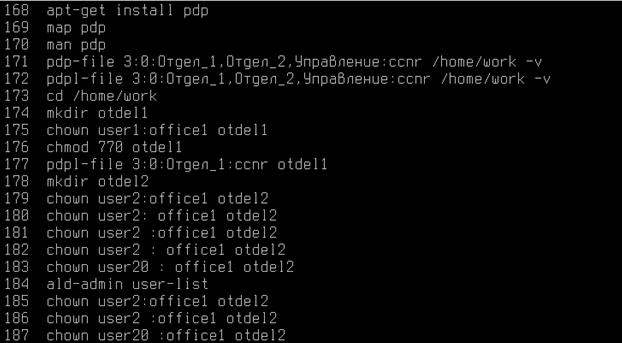


Рис. 21. Листинг команд 14 пункта (продолжение)



Рис. 22. Листинг команд 14 пункта (продолжение) (продолжения)

Учебная практика №4

**«Мандатный контроль целостности в Astra Linux 1.6 / Расщепление root / информационная безопасность»**

**Цель работы:** законспектировать видеофайл.

**Мандатный контроль целостности**

Мандатный контроль целостности - это процесс проверки целостности данных, который осуществляется на основе прав доступа и прав пользователей к информационной системе. Этот вид контроля обеспечивает защиту данных от несанкционированных изменений, разрушений или копирования.

В рамках мандатного контроля целостности устанавливаются и проверяются правила и ограничения доступа для пользователей и приложений. Система контроля целостности проверяет, что данные не были изменены или повреждены без разрешения, и что только уполномоченные пользователи имеют доступ к определенным данным.

Этот вид контроля является важной частью обеспечения безопасности данных и обеспечивает сохранность информации от угроз как внутри, так и за пределами организации. Важно поддерживать мандатный контроль целостности в актуальном состоянии и регулярно анализировать его эффективность для обеспечения безопасности информационной системы.

В Astra Linux 1.6 мандатный контроль целостности может быть реализован с помощью механизма SE Linux (Security Enhanced Linux), который позволяет определить правила доступа к ресурсам системы на основе меток безопасности.

**Дискреционное ограничение доступа**

В Astra Linux используется дискреционное ограничение доступа, которое регулирует доступ пользователей к файлам.

Недостатки этого механизма: не позволяет управлять информационными потоками и контролировать утечку данных.

Дискреционное ограничение доступа - это метод управления доступом к ресурсам информационной системы, основанный на предоставлении пользователю контроля над своими собственными данными и ресурсами. Сущность дискреционного ограничения доступа заключается в том, что владелец или создатель данных определяет, кому и какие права доступа предоставляются к собственной информации.

Основные принципы дискреционного ограничения доступа:

1. Владелец информации имеет право определять, кто и как может получить доступ к его данным.

2. Пользователь, который обладает правами доступа, может делиться своими данными или ресурсами с другими пользователями в соответствии с заданными правами.

3. Дискреционное ограничение доступа основывается на концепции "need-to-know" (необходимо знать), что означает, что пользователь получает доступ только к информации, необходимой для выполнения своих обязанностей или задач.

Примером дискреционного ограничения доступа являются системы управления правами доступа (Access Control Lists - ACL), где владелец информации может устанавливать список пользователей или групп пользователей с различными уровнями доступа к файлам или папкам.

Дискреционное ограничение доступа является одним из основных методов обеспечения безопасности данных в информационных системах и позволяет управлять доступом к информации на уровне индивидуальных пользователей.

**Мандатное управление доступом**

Мандатное управление доступом работает по уровням конфиденциальности и категориям.

Реализовано в Astra Linux с помощью подсистемы безопасности Parsec.

В Astra Linux 1.6 мандатное управление доступом реализуется с помощью механизма Security Enhanced Linux (SE Linux). SE Linux предоставляет возможность добавления дополнительного уровня обеспечения безопасности, который работает на основе меток безопасности.

SE Linux позволяет администраторам системы определить политики безопасности для контроля доступа к ресурсам системы, таким как файлы, каталоги, процессы и сетевые соединения. При этом SE Linux дополнительно к основным правам доступа (режим DAC - discretionary access control) использует мандатный контроль доступа (MAC - mandatory access control), который принуждает процессы к выполнению определенных правил безопасности.

Администратор Astra Linux может настроить уровень безопасности SE Linux в соответствии с требованиями безопасности своей системы, определяя разрешенные и запрещенные действия для различных сущностей в системе. SE Linux позволяет усилить защиту от атак, включая привилегированные угрозы, эксплойты и распространение вредоносного программного обеспечения.

Для работы с мандатным управлением доступом в Astra Linux 1.6 необходимо иметь соответствующие знания по настройке SE Linux и опыт в администрировании системы.

**Примеры работы мандатного контроля целостности**

В видео демонстрируется, как работает мандатный контроль целостности на примере процессов с разными уровнями целостности.

В Linux, если взламывают иксорга и получают привилегии рута, то в Windows это не получится, так как процессы с низким уровнем целостности не могут влиять на процессы с высоким уровнем.

**Мандатный контроль целостности**

В системе действует мандатный контроль целостности, но он не применяется к файлам.

Для включения мандатного контроля целостности необходимо зайти в панель управления и включить защиту файловой системы.

**Защита файловой системы**

После включения защиты файловой системы, все файлы получают максимальный уровень контроля целостности.

Если пользователь пытается изменить файл с высоким уровнем контроля целостности, ему будет отказано в доступе.

**Мониторинг и защита от эксплоитов**

Монитор Parsec отслеживает действия пользователей с низким уровнем мандатного контроля целостности и при обнаружении создания или запуска процесса с высоким уровнем, он его прибивает.

Это усложняет эксплуатацию уязвимостей и повышает уровень безопасности системы.