

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
федеральное государственное автономное образовательное учреждение высшего образования  
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

---

КАФЕДРА № 24

КОНТРОЛЬНАЯ РАБОТА  
ЗАЩИЩЕН С ОЦЕНКОЙ  
ПРЕПОДАВАТЕЛЬ

канд. техн. наук, доцент		Саенко В.И
г, уч. степень, звание	дата	я, фамилия

ЛАБОРАТОРНАЯ РАБОТА № 5

**ТЕХНОЛОГИИ АВТОМАТИЗАЦИИ ДЛЯ  
ОПЕРАЦИОННЫХ СИСТЕМ И POWER SHELL**

по курсу: Информационные технологии

СТУДЕНТ ГР. №	2247	Ланин П.М
номер группы	подпись, дата	, фамилия

Промежуточный контроль (на усмотрение преподавателя)	Оценка	Дата	Подпись преподавателя
Отчет			
Навыки			
Теория			

Санкт-Петербург  
2024

**Цель работы –**

- как запустить и использовать CMD;
- как управлять файлами с помощью CMD;
- как пользоваться полезными утилитами с помощью CMD;
- как создавать сценарии для обеспечения процесса управления в компьютерной сети.

**Основные навыки:** CMD помогает нам: 1) управлять файлами, 2) использовать утилиты CLI и создавать простые программы-скрипты, 3) получать информацию о конфигурации и состоянии любого компьютера в сети, 4) устанавливать расширенную пользовательскую среду в ОС , 5) установить простую пользовательскую среду при входе в систему

## Упражнение 5.1.а. Полезные команды (тренировочные)

```
Командная строка
Microsoft Windows [Version 10.0.22621.3155]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\pavellanin>cd c:\

C:\>mkdir .\tmp

C:\>fir
"fir" не является внутренней или внешней
командой, исполняемой программой или пакетным файлом.

C:\>dir
Том в устройстве C не имеет метки.
Серийный номер тома: EE7F-9DC9

Содержимое папки c:\

07.11.2007 08:00             17 734 eula.1028.txt
07.11.2007 08:00             17 734 eula.1031.txt
07.11.2007 08:00             10 134 eula.1033.txt
07.11.2007 08:00             17 734 eula.1036.txt
07.11.2007 08:00             17 734 eula.1040.txt
07.11.2007 08:00              118 eula.1041.txt
07.11.2007 08:00             17 734 eula.1042.txt
07.11.2007 08:00             17 734 eula.2052.txt
07.11.2007 08:00             17 734 eula.3082.txt
27.12.2023 01:15    <DIR>          Games
07.11.2007 08:00              1 110 globdata.ini
07.11.2007 08:44          855 040 install.exe
07.11.2007 08:00              843 install.ini
07.11.2007 08:44          75 280 install.res.1028.dll
07.11.2007 08:44          95 248 install.res.1031.dll
07.11.2007 08:44          90 128 install.res.1033.dll
07.11.2007 08:44          96 272 install.res.1036.dll
07.11.2007 08:44          94 224 install.res.1040.dll
07.11.2007 08:44          80 400 install.res.1041.dll

07.11.2007 08:44          80 400 install.res.1041.dll
07.11.2007 08:44          78 864 install.res.1042.dll
07.11.2007 08:44          74 768 install.res.2052.dll
07.11.2007 08:44          95 248 install.res.3082.dll
07.05.2022 08:24    <DIR>          PerfLogs
27.03.2024 13:43    <DIR>          Program Files
27.03.2024 13:43    <DIR>          Program Files (x86)
07.04.2024 22:22    <DIR>          tmp
09.03.2023 21:36    <DIR>          Users
07.11.2007 08:00              5 686 vcredist.bmp
07.11.2007 08:50              1 927 956 VC_RED.cab
07.11.2007 08:53              242 176 VC_RED.MSI
27.03.2024 13:46    <DIR>          Windows
      24 файлов             3 947 633 байт
      7 папок   213 735 993 344 байт свободно

C:\>
C:\>cd .\tmp

C:\tmp>cd .\tmp

C:\tmp>echo my file txt
my file txt

C:\tmp>echo "my file txt"
"my file txt"

C:\tmp>echo my file txt > tr1.txt

C:\tmp>echo "my file txt" > tr2.txt

C:\tmp>type tr1.txt
my file txt

C:\tmp>type tr2.txt
"my file txt"

C:\tmp>type tr2.txt
"my file txt"

C:\tmp>echo my file cmd > tr1.cmd

C:\tmp>
C:\tmp>echo my file cmd > t1.cmd

C:\tmp>type t1.cmd
my file cmd

C:\tmp>copy con t2.txt
Testing
copy con
Скопировано файлов:      1.

C:\tmp>copy con t2.cmd
type tr2.txt
Скопировано файлов:      1.

C:\tmp>dir
Том в устройстве C не имеет метки.
Серийный номер тома: EE7F-9DC9

Содержимое папки c:\tmp

07.04.2024 22:27    <DIR>          .
07.04.2024 22:25             14 t1.cmd
07.04.2024 22:27             14 t2.cmd
07.04.2024 22:27             20 t2.txt
07.04.2024 22:25             14 tr1.cmd
07.04.2024 22:24             14 tr1.txt
07.04.2024 22:24             16 tr2.txt
      6 файлов             92 байт
      1 папок   213 735 981 056 байт свободно
```

```
Командная строка
c:\tmp>copy con t1.txt
test
Скопировано файлов:      1.

c:\tmp>
c:\tmp>dir
Том в устройстве C не имеет метки.
Серийный номер тома: EE7F-9DC9

Содержимое папки c:\tmp
07.04.2024  22:28    <DIR>          .
07.04.2024  22:25             14 t1.cmd
07.04.2024  22:28             6 t1.txt
07.04.2024  22:27             14 t2.cmd
07.04.2024  22:27            20 t2.txt
07.04.2024  22:25             14 tr1.cmd
07.04.2024  22:24             14 tr1.txt
07.04.2024  22:24             16 tr2.txt
              7 файлов             98 байт
              1 папок  213 735 915 520 байт свободно

c:\tmp>copy t2.cmd t3.cmd
Скопировано файлов:      1.

c:\tmp>ren t2.cmd t4.cmd

c:\tmp>dir
Том в устройстве C не имеет метки.
Серийный номер тома: EE7F-9DC9

Содержимое папки c:\tmp
07.04.2024  22:38    <DIR>          .
07.04.2024  22:25             14 t1.cmd

07.04.2024  22:25             14 tr1.cmd
07.04.2024  22:24             14 tr1.txt
07.04.2024  22:24             16 tr2.txt
              7 файлов             98 байт
              1 папок  213 735 915 520 байт свободно

c:\tmp>copy t2.cmd t3.cmd
Скопировано файлов:      1.

c:\tmp>ren t2.cmd t4.cmd

c:\tmp>dir
Том в устройстве C не имеет метки.
Серийный номер тома: EE7F-9DC9

Содержимое папки c:\tmp
07.04.2024  22:38    <DIR>          .
07.04.2024  22:25             14 t1.cmd
07.04.2024  22:28             6 t1.txt
07.04.2024  22:27            20 t2.txt
07.04.2024  22:27             14 t3.cmd
07.04.2024  22:27             14 t4.cmd
07.04.2024  22:25             14 tr1.cmd
07.04.2024  22:24             14 tr1.txt
07.04.2024  22:24             16 tr2.txt
              8 файлов            112 байт
              1 папок  213 735 698 432 байт свободно

c:\tmp>

1 папок  213 735 698 432 байт свободно

c:\tmp>echo my file txt > t1.txt

c:\tmp>type t1.txt
my file txt

c:\tmp>notepad t1.txt

c:\tmp>type t1.txt
my file txt
test editing

c:\tmp>copy t1.txt t11.txt
Скопировано файлов:      1.

c:\tmp>type t11.txt
my file txt
test editing

c:\tmp>del t11.txt

c:\tmp>dir
Том в устройстве C не имеет метки.
Серийный номер тома: EE7F-9DC9

Содержимое папки c:\tmp
07.04.2024  22:44    <DIR>          .
07.04.2024  22:25             14 t1.cmd
07.04.2024  22:43            28 t1.txt
07.04.2024  22:27            20 t2.txt
07.04.2024  22:27             14 t3.cmd
07.04.2024  22:27             14 t4.cmd
07.04.2024  22:25             14 tr1.cmd
07.04.2024  22:24             14 tr1.txt
```

```
my file txt

c:\tmp>notepad t1.txt

c:\tmp>type t1.txt
my file txt
test editing

c:\tmp>copy t1.txt t11.txt
Скопировано файлов:      1.

c:\tmp>type t11.txt
my file txt
test editing

c:\tmp>del t11.txt

c:\tmp>dir
Том в устройстве C не имеет метки.
Серийный номер тома: EE7F-9DC9

Содержимое папки c:\tmp

07.04.2024  22:44    <DIR>          .
07.04.2024  22:25                14 t1.cmd
07.04.2024  22:43                28 t1.txt
07.04.2024  22:27                20 t2.txt
07.04.2024  22:27                14 t3.cmd
07.04.2024  22:27                14 t4.cmd
07.04.2024  22:25                14 tr1.cmd
07.04.2024  22:24                14 tr1.txt
07.04.2024  22:24                16 tr2.txt
               8 файлов             134 байт
               1 папок    213 735 632 896 байт свободно

c:\tmp>

Командная строка  x  +  -  □  x

07.04.2024  22:43                28 t1.txt
07.04.2024  22:27                20 t2.txt
07.04.2024  22:27                14 t3.cmd
07.04.2024  22:27                14 t4.cmd
07.04.2024  22:25                14 tr1.cmd
07.04.2024  22:24                14 tr1.txt
07.04.2024  22:24                16 tr2.txt
               8 файлов             134 байт
               1 папок    213 735 632 896 байт свободно

c:\tmp>notepad t1.cmd

c:\tmp>t1.cmd

c:\tmp>echo Hello!
Hello!

c:\tmp>echo How are you?
How are you?

c:\tmp>echo What do you do?
What do you do?

c:\tmp>rd /S c:\tmp
c:\tmp, вы уверены [Y(да)/N(нет)]? y
Процесс не может получить доступ к файлу, так как этот файл занят другим процессом.

c:\tmp>y
"y" не является внутренней или внешней
командой, исполняемой программой или пакетным файлом.

c:\tmp>rd /S c:\tmp
c:\tmp, вы уверены [Y(да)/N(нет)]? y
Процесс не может получить доступ к файлу, так как этот файл занят другим процессом.

c:\tmp>
```

Комментарий: почему-то не удаляется, хотя все процессы закрыты — удалил вручную

Вывод:

Научились создавать и работать с директориями, также работать с файлами (создавать , удалять, редактировать, запускать)

## Упражнение 5.1.6. Рассмотрим простую задачу.

### Шаг 1. Переходим к \tmp

```
Командная строка

C:\Users\ravellanin>cd C:\


C:\>mkdir .\tmp

C:\>cd .\tmp

C:\tmp>|
```

### Шаг 2. Создаем несколько файлов в C: \tmp

```
C:\tmp>echo my file txt > t1.txt
C:\tmp>echo my file cmd > t1.cmd
C:\tmp>copy t1.txt t2.txt
Скопировано файлов:      1.
C:\tmp>copy t1.txt t3.txt
Скопировано файлов:      1.
C:\tmp>copy t1.txt t4.txt
Скопировано файлов:      1.
C:\tmp>dir > d1.txt
C:\tmp>|
```



### Шаг 3. Копируем файлы из C: \tmp в C: \tmp\tmp2

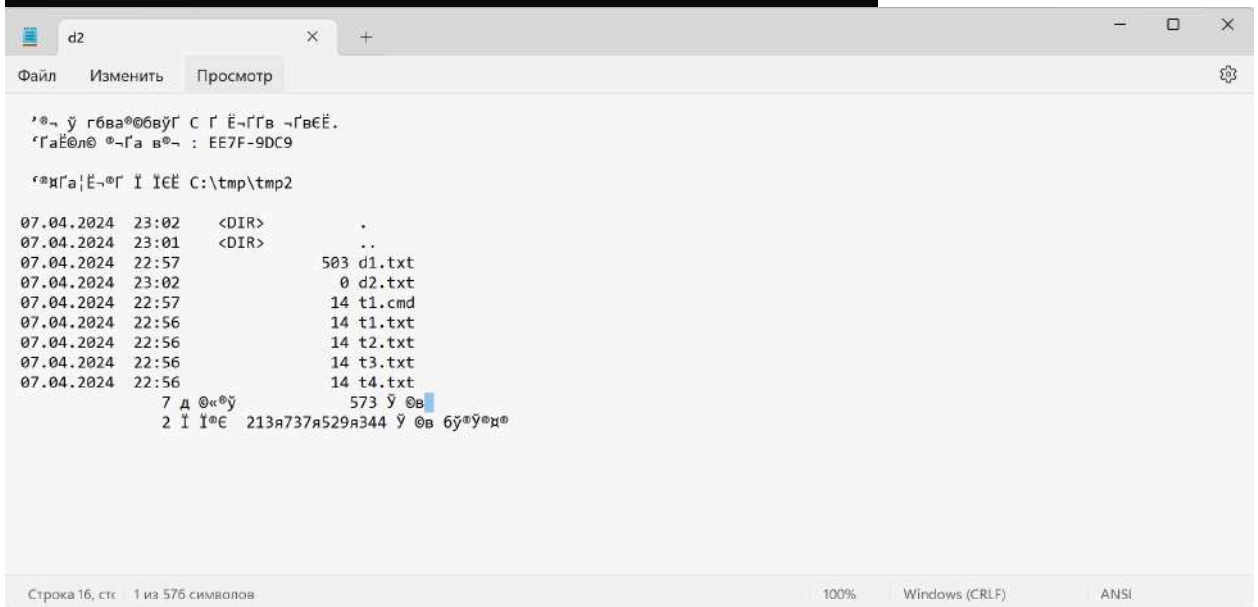
```
C:\tmp>mkdir .\tmp2

C:\tmp>copy c:\tmp\*. * c:\tmp\tmp2\*. *
c:\tmp\d1.txt
c:\tmp\t1.cmd
c:\tmp\t1.txt
c:\tmp\t2.txt
c:\tmp\t3.txt
c:\tmp\t4.txt
Скопировано файлов:           6.

C:\tmp>cd .\tmp2

C:\tmp\tmp2>dir > d2.txt

C:\tmp\tmp2>|
```



#### Шаг 4. Сохраняем все результаты в файле resd.txt

```
Командная строка
C:\tmp>cd .\tmp2
C:\tmp\tmp2>dir > d2.txt
C:\tmp\tmp2>copy c:\tmp\d1.txt + c:\tmp\tmp2\d2.txt c:\tmp\resd.txt
c:\tmp\d1.txt
c:\tmp\tmp2\d2.txt
Скопировано файлов:      1.
C:\tmp\tmp2>cd
C:\tmp\tmp2>cd tmp
Системе не удастся найти указанный путь.
C:\tmp\tmp2>cd tmp
Системе не удастся найти указанный путь.
C:\tmp\tmp2>cd..
C:\tmp>dir
Том в устройстве C не имеет метки.
Серийный номер тома: EE7F-9DC9

Содержимое папки C:\tmp
07.04.2024  23:04    <DIR>          .
07.04.2024  22:57             503 d1.txt
07.04.2024  23:04             1 096 resd.txt

Командная строка
C:\tmp\tmp2>cd tmp
Системе не удастся найти указанный путь.
C:\tmp\tmp2>cd tmp
Системе не удастся найти указанный путь.
C:\tmp\tmp2>cd..
C:\tmp>dir
Том в устройстве C не имеет метки.
Серийный номер тома: EE7F-9DC9

Содержимое папки C:\tmp
07.04.2024  23:04    <DIR>          .
07.04.2024  22:57             503 d1.txt
07.04.2024  23:04             1 096 resd.txt
07.04.2024  22:57             14 t1.cmd
07.04.2024  22:56             14 t1.txt
07.04.2024  22:56             14 t2.txt
07.04.2024  22:56             14 t3.txt
07.04.2024  22:56             14 t4.txt
07.04.2024  23:02    <DIR>          tmp2
7 файлов             1 669 байт
2 папок  213 738 045 440 байт свободно

C:\tmp>type resd.txt
Том в устройстве C не имеет метки.
Серийный номер тома: EE7F-9DC9

Содержимое папки C:\tmp
07.04.2024  22:57    <DIR>          .
07.04.2024  22:57             0 d1.txt
07.04.2024  22:57             14 t1.cmd
07.04.2024  22:56             14 t1.txt
07.04.2024  22:56             14 t2.txt
07.04.2024  22:56             14 t3.txt
07.04.2024  22:56             14 t4.txt
6 файлов             70 байт
1 папок  213 733 748 736 байт свободно
Том в устройстве C не имеет метки.
Серийный номер тома: EE7F-9DC9

Содержимое папки C:\tmp\tmp2
07.04.2024  23:02    <DIR>          .
07.04.2024  23:01    <DIR>          ..
07.04.2024  22:57             503 d1.txt
07.04.2024  23:02             0 d2.txt
07.04.2024  22:57             14 t1.cmd
07.04.2024  22:56             14 t1.txt
07.04.2024  22:56             14 t2.txt
07.04.2024  22:56             14 t3.txt
07.04.2024  22:56             14 t4.txt
7 файлов             573 байт
2 папок  213 737 529 344 байт свободно

C:\tmp>
```



```
resd
Файл  Изменить  Просмотр
| 'а- ь гбва@бвўГ С Г Ё-ГГв -ГвЁЁ.
'ГаЁ@л@ @-Га в@- : EE7F-9DC9

'аГга|Ё-@Г Ї ЇЁЁ C:\tmp

07.04.2024 22:57 <DIR> .
07.04.2024 22:57      0 d1.txt
07.04.2024 22:57     14 t1.cmd
07.04.2024 22:56     14 t1.txt
07.04.2024 22:56     14 t2.txt
07.04.2024 22:56     14 t3.txt
07.04.2024 22:56     14 t4.txt
      6 д @н@ў      70 ў @в
      1 Ї ЇЁЁ 213я733я748я736 ў @в бў@ў@н@
'а- ь гбва@бвўГ С Г Ё-ГГв -ГвЁЁ.
'ГаЁ@л@ @-Га в@- : EE7F-9DC9

'аГга|Ё-@Г Ї ЇЁЁ C:\tmp\tmp2

07.04.2024 23:02 <DIR> .
07.04.2024 23:01 <DIR> ..
07.04.2024 22:57    503 d1.txt
07.04.2024 23:02      0 d2.txt
07.04.2024 22:57     14 t1.cmd
07.04.2024 22:56     14 t1.txt
07.04.2024 22:56     14 t2.txt
07.04.2024 22:56     14 t3.txt
07.04.2024 22:56     14 t4.txt
      7 д @н@ў      573 ў @в
      2 Ї ЇЁЁ 213я737я529я344 ў @в бў@ў@н@

```

Вывод:

Научились глубже работать с копированием информации и ее перемещением  
Также сохранять информацию в отдельное место

## Упражнение 5.1.в. Используем утилиты для тестирования компьютера

```
Командная строка
Microsoft Windows [Version 10.0.22621.3155]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\pavellanin>NET HELP command|MORE
Синтаксис данной команды:

NET
[ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
  HELPMMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
  STATISTICS | STOP | TIME | USE | USER | VIEW ]

Ключевое слово NET указывает команды Windows.

NET HELP имя_команды | MORE – постраничный просмотр справки.

C:\Users\pavellanin>NET HELP command | MORE
Синтаксис данной команды:

NET
[ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
  HELPMMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
  STATISTICS | STOP | TIME | USE | USER | VIEW ]

Ключевое слово NET указывает команды Windows.

NET HELP имя_команды | MORE – постраничный просмотр справки.

C:\Users\pavellanin>net config workstation
Имя компьютера                \\188E
Полное имя компьютера         188E
Имя пользователя              pavellanin

NET HELP имя_команды | MORE – постраничный просмотр справки.

C:\Users\pavellanin>net config workstation
Имя компьютера                \\188E
Полное имя компьютера         188E
Имя пользователя              pavellanin

Активная рабочая станция на

Версия программы               Windows 10 Home

Домен рабочей станции         WORKGROUP
Домен входа                    188E

Интервал ожидания открытия COM-порта (с) 0
Отсчет передачи COM-порта (байт) 16
Таймаут передачи COM-порта (мс) 250
Команда выполнена успешно.

C:\Users\pavellanin>netstat -e
Статистика интерфейса

                Получено                Отправлено
Байт            0                        0
Одноадресные пакеты 0                    0
Многоадресные пакеты 0                    0
Отброшено       0                        0
Ошибки          0                        0
Неизвестный протокол 0
C:\Users\pavellanin>
```

## Упражнение 5.1.г.

```
Командная строка
5:
***** D1.TXT
3:
4:   Содержимое папки c:\tmp
5:
*****
***** d0.txt
6:  07.04.2024  23:45  <DIR>          .
7:  07.04.2024  23:45                0 d0.txt
8:  07.04.2024  22:57                503 d1.txt
9:  07.04.2024  23:04                1 096 resd.txt
10: 07.04.2024  22:57                14 t1.cmd
***** D1.TXT
6:  07.04.2024  23:45  <DIR>          .
7:  07.04.2024  23:45                635 d0.txt
8:  07.04.2024  23:45                0 d1.txt
9:  07.04.2024  22:57                14 t1.cmd
*****
***** d0.txt
15: 07.04.2024  23:02  <DIR>          tmp2
16:                8 файлов          1 669 байт
17:                2 папок   213 735 215 104 байт свободно
***** D1.TXT
14: 07.04.2024  23:02  <DIR>          tmp2
15:                7 файлов          705 байт
16:                2 папок   213 735 219 200 байт свободно
*****
C:\tmp>

Командная строка
C:\tmp>dir c:\tmp 1>c:\tmp\d1.txt
C:\tmp>dir c:\tmp\tmp2 1>c:\tmp\d2.txt
C:\tmp>net config workstation 1>c:\tmp\cws.txt
C:\tmp>copy c:\tmp\d1.txt + c:\tmp\d2.txt + c:\tmp\cws.r c:\tmp\resd.txt
c:\tmp\d1.txt
c:\tmp\d2.txt
Скопировано файлов:      1.
C:\tmp>Rem comparison of files
C:\tmp>fc d0.txt d1.txt /L /N
Сравнение файлов d0.txt и D1.TXT
***** d0.txt
3:
4:   Содержимое папки C:\tmp
5:
***** D1.TXT
3:
4:   Содержимое папки c:\tmp
5:
*****
***** d0.txt
6:  07.04.2024  23:45  <DIR>          .
7:  07.04.2024  23:45                0 d0.txt
8:  07.04.2024  22:57                503 d1.txt
9:  07.04.2024  23:04                1 096 resd.txt
10: 07.04.2024  22:57                14 t1.cmd
***** D1.TXT

Microsoft Windows [Version 10.0.22621.3155]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.
C:\Users\pavellanin>notepad test.cmd
C:\Users\pavellanin>test.cmd
C:\Users\pavellanin>Rem "нельзя использовать пробелы в имени файла"
C:\Users\pavellanin>Rem move to \tmp:
C:\Users\pavellanin>cd C:\
C:\>cd .\tmp
C:\tmp>dir 1>d0.txt
C:\tmp>Rmdir /s delete old reports and files. "Rmdir" не является внутренней или внешней командой, исполняемой программой или пакетным файлом.
C:\tmp>Rmdir /s "нельзя использовать пробелы в имени файла" "Rmdir" не является внутренней или внешней командой, исполняемой программой или пакетным файлом.
C:\tmp>del d1.txt d1.txt d2.txt cws.txt resd.txt
C:\tmp>Rmdir /s Get file structure in the C:\tmp and C:\tmp\tmp2 save result to files
"Rmdir" не является внутренней или внешней командой, исполняемой программой или пакетным файлом.
```

### 5.1.8. Задания 5.1

Задание 1 Изучите набор команд, приведите ответы на вопросы по CMD

Сколько всего команд,

Чтобы ответить на вопрос, воспользуемся командой help или help dir

Из интернета я прочитал, что их около 300 (в зависимости от версии ОС)м

```
[drive:][path][filename]
Диск, каталог или имена файлов для включения в список.

/A      Отображение файлов с указанными атрибутами.
атрибуты D Каталоги. R Файлы, доступные только для чтения
          H Скрытые файлы A Файлы, готовые для архивирования
          S Системные файлы I Файлы с неиндексированным содержимым
          L Точки повторной обработки O Автономные файлы
          - Префикс "-" имеет значение НЕ

/B      Вывод только имен файлов.
/C      Применение разделителя групп разрядов при выводе размеров файлов.
Используется по умолчанию. Чтобы отключить применение разделителя групп разрядов, задайте ключ /-C.
/D      Вывод списка в нескольких столбцах с сортировкой по столбцам.
/L      Использовать нижний регистр.
/N      Новый формат длинного списка, имена файлов выводятся в крайнем правом столбце.
/O      Сортировка списка отображаемых файлов.
sortorder N По имени (по алфавиту) S По размеру (начиная с минимального)
          E По расширению (по алфавиту) D По дате и времени (начиная с самого старого)
          G Начать список с каталогов - Префикс "-" обращает порядок

/P      Пауза после заполнения каждого экрана.
/Q      Вывод сведений о владельце файла.
/R      Отображение альтернативных потоков данных этого файла.
/S      Отображение файлов из указанного каталога и всех его подкаталогов.
/T      Выбор поля времени для сортировки.
timefield C Создание
          A Последнее использование
          W Последнее изменение

/W      Вывод списка в несколько столбцов.
/X      Отображение коротких имен для файлов, чьи имена не соответствуют стандарту 8.3.
Формат аналогичен выводу с ключом /N, но короткие
имена файлов выводятся слева от длинных. Если короткого имени у
файла нет, вместо него выводятся пробелы.

/4      Вывод номера года в четырехзначном формате

Стандартный набор ключей можно записать в переменную среды DIRCMD. Для отмены
```

Какие команды используются для работы с файлами,

- dir — выводит список файлов и папок в указанной директории.
- copy — копирует один или несколько файлов из одного места в другое.
- move — перемещает файлы из одной директории в другую.
- del или erase — удаляет один или несколько файлов.
- ren или rename — переименовывает файл.
- type — отображает содержимое текстового файла.
- xcopy — копирует файлы и каталоги, включая подкаталоги.
- robocopy — более мощная утилита для копирования файлов и директорий.

Какие команды используются для получения информации о конфигурации компьютера,

- systeminfo — выводит подробную информацию о системе и её конфигурации.
- msinfo32 — запускает утилиту системной информации, которая отображает более подробные данные о компьютере.

Какие команды используются для получения информации о сетевом окружении

- `ipconfig` — отображает конфигурацию IP-адресов на компьютере, включая маску подсети и шлюз по умолчанию.
- `ping` — проверяет доступность сетевого узла.
- `tracert` — отслеживает путь пакетов до конкретного узла сети.
- `netstat` — отображает статистику и текущее состояние всех сетевых соединений.
- `nslookup` — запрос информации у DNS-серверов о доменных именах и IP-адресах.
- `net` — серия команд для работы с сетевыми настройками, включая `net view`, `net user`, `net use` и другие.

Задание 2. Сформировать тестовые сценарии (варианты: настройки дисков, сбор конфигурационной информации) и привести пример выполнения сценария для одного варианта (любого).

### 1. Проверка состояние диска

Открыть CMD.

Ввести `diskpart`

Ввести `list disk`

Выбрать диск, введя `select disk <номер диска>`.

Ввести `detail disk`

Итог сценария: Отображается информация о выбранном диске, включая состояние, размер и количество разделов.

### 2. Сбор подробной информации о конфигурации компьютера, включая ОС, оборудование и сетевые настройки.

Открыть CMD.

Ввести `systeminfo` и нажать Enter.

Итог сценария:

Имя хоста, ОС, версию, производителя, конфигурацию ядра, физическую память, доступную виртуальную память.

Сведения о сетевых картах и IP-адресах.

Дату установки ОС, время работы системы и обновления.

## Тестирование 1 сценария

```
C:\Users\pavellanin>
C:\Users\pavellanin>
C:\Users\pavellanin>diskpart
```

Microsoft DiskPart, версия 10.0.22621.1

(C) Корпорация Майкрософт (Microsoft Corporation).  
На компьютере: 188E

DISKPART> list disk

Диск ###	Состояние	Размер	Свободно	Дин	GPT
Диск 0	В сети	256 Гбайт	0 байт		*

DISKPART> select disk 0

Выбран диск 0.

DISKPART> detail disk

Parallels Virtual NVMe Disk  
ИД диска : {A29679FF-19F1-4713-A59E-F0EB6E287854}  
Тип : NVMe  
Состояние : В сети  
Путь : 0  
Конечный объект : 0  
ИД LUN : 0  
Путь к расположению : PCIR00T(0)#PCI(1F07)#NVME(P00T00L00)  
Текущее состояние только для чтения : Нет  
Только для чтения: Нет  
Загрузочный диск: Да  
Диск файла подкачки: Да  
Диск файла спящего режима: Нет  
Диск аварийного дампа: Да  
Кластерный диск: Нет

Том	###	Имя	Метка	ФС	Тип	Размер	Состояние	Сведения
Том 1		C		NTFS	Раздел	255 Гб	Исправен	Загрузоч
Том 2				NTFS	Раздел	300 Мб	Исправен	Скрытый
Том 3				FAT32	Раздел	300 Мб	Исправен	Системны

DISKPART> \_

## 5.2. Скрипт WMIC

### Упражнение 5.2. Примеры команд.

wmic:root\cli>/? – справка

```
wmic:root\cli>/?
Программа WMIC устарела.

[глобальные параметры] <команда>

Имеются следующие глобальные параметры:
/namespace      Путь к пространству имен, с которым оперирует псевдоним.
/role            Путь к роли, содержащей определения псевдонимов.
/node            Серверы, с которыми будет работать псевдоним.
/implementlevel  Уровень олицетворения для клиента
/authlevel       Уровень проверки подлинности для клиента.
/locale          Код языка, который должен использовать клиент.
/privileges       Включает или выключает все привилегии.
/trace           Выводит отладочные данные в stderr.
/record          Записывает все вводимые команды и их выходные данные.
/interactive      Устанавливает или переустанавливает интерактивный режим.
/failfast        Устанавливает или переустанавливает режим FailFast.
/user            Имя пользователя для сеанса.
/password        Пароль для входа в сеанс.
/output          Задаёт режим перенаправления выходных данных.
/append          Задаёт режим перенаправления выходных данных.
/aggregate       Устанавливает или переустанавливает режим совместного вывода.
/authority       Задаёт <тип_полномочий> для подключения.
/?[<-BRIEF|FULL>] Сведения об использовании.

Для получения дополнительных сведений о конкретном глобальном параметре введите: имя_параметра /?

Для текущей роли доступны следующие псевдонимы:
ALIAS            - Доступ к псевдонимам, доступным на локальном компьютере
BASEBOARD        - Управление системной платой.
BIOS             - Управление BIOS.
BOOTCONFIG       - Управление конфигурацией загрузки.
Чтобы продолжить, нажмите любую клавишу; чтобы остановить работу, нажмите клавишу ESCAPE
```

### Информация об операционной системе

```
/? для вызова справки, QUIT для выхода.
wmic:root\cli>os
BootDevice      BuildNumber  BuildType      Caption      CodeSet Co
\Device\HarddiskVolume2  22621        Multiprocessor Free  Майкрософт Windows 11 Домашняя  1251    7
Win32_0

wmic:root\cli>os list Brief
BuildNumber  Organization  RegisteredUser  SerialNumber  SystemDirectory  Version
22621        Павел Ланин  00326-30000-00001-AA376  C:\Windows\system32  10.0.22621

wmic:root\cli>os list Status
Name                                     Status
Майкрософт Windows 11 Домашняя|C:\Windows\Device\Harddisk0\Partition4  OK

wmic:root\cli>os list Brief /format:list

BuildNumber=22621
Organization=
RegisteredUser=Павел Ланин
SerialNumber=00326-30000-00001-AA376
SystemDirectory=C:\Windows\system32
Version=10.0.22621

wmic:root\cli>os list Brief /format:table
BuildNumber  Organization  RegisteredUser  SerialNumber  SystemDirectory  Version
22621        Павел Ланин  00326-30000-00001-AA376  C:\Windows\system32  10.0.22621

wmic:root\cli>
```



## Информация об операционной системе

```
wmic:root\cli> cpu
AddressWidth  Architecture  AssetTag  Availability  Caption  Characteristics  ConfigManag
64              9              3              3              Intel64 Family 6 Model 142 Stepping 10  21280

wmic:root\cli>cpu list brief
Caption  DeviceID  Manufacturer  MaxClockSpeed  Name
Intel64 Family 6 Model 142 Stepping 10  CPU08  GenuineIntel  1392  Intel(R) Core(TM) i5-8257U CPU @ 1.40GHz

wmic:root\cli>cpu get Systemname, ame, escription, anufacturer, ddressWidth, eviceID
Узел: 188E
ОШИБКА.
Описание: Недопустимый запрос

wmic:root\cli>cpu get Systemname, ame, escription, anufacturer, dressWidth, eviceID
Узел: 188E
ОШИБКА.
Описание: Недопустимый запрос

wmic:root\cli>cpu get Systemname, ame, escription, anufacturer, dressWidth, eviceID /format:list
Узел: 188E
ОШИБКА.
Описание: Недопустимый запрос

wmic:root\cli>cpu get Systemname, ame, escription, anufacturer, dressWidth, eviceID, /format:list
Недопустимое выражение GET.
wmic:root\cli>cpu get Systemname, ame, escription, anufacturer, dressWidth, eviceID, /format:list
Недопустимое выражение GET.
wmic:root\cli>
```

## Информация о логических дисках

```
wmic:root\cli>logicaldisk
Access  Availability  BlockSize  Caption  Compressed  ConfigManagerErrorCode  ConfigManagerUserConfig  CreationClassName
0              0              0              C:  FALSE  0  0  Win32_LogicalDisk
0              0              0              D:  FALSE  0  0  Win32_LogicalDisk
0              0              0              X:  FALSE  0  0  Win32_LogicalDisk
0              0              0              Y:  FALSE  0  0  Win32_LogicalDisk
0              0              0              Z:  FALSE  0  0  Win32_LogicalDisk

wmic:root\cli>logicaldisk list brief /format:list

DeviceID=D:
DriveType=5
FreeSpace=
ProviderName=
Size=
VolumeName=

DeviceID=X:
DriveType=4
FreeSpace=9024212992
ProviderName=\\Mac\iCloud
Size=250685575168
VolumeName=Shared Folders

ProviderName=
Size=
VolumeName=

DeviceID=X:
DriveType=4
FreeSpace=9024212992
ProviderName=\\Mac\iCloud
Size=250685575168
VolumeName=Shared Folders

DeviceID=Y:
DriveType=4
FreeSpace=9024212992
ProviderName=\\Mac\Home
Size=250685575168
VolumeName=Shared Folders

DeviceID=Z:
DriveType=4
FreeSpace=9024212992
ProviderName=\\Mac\AllFiles
Size=250685575168
VolumeName=Shared Folders

wmic:root\cli>logicaldisk where name='Z:' get size,freespace,volumename
FreeSpace  Size  VolumeName
9023995904  250685575168  Shared Folders

wmic:root\cli>
```



## Информация об сетевой карте

```
wmic:root\cli>nic get * /format:list

AdapterType=
AdapterTypeId=
AutoSense=
Availability=3
Caption=[00000000] Microsoft Kernel Debug Network Adapter
ConfigManagerErrorCode=0
ConfigManagerUserConfig=FALSE
CreationClassName=Win32_NetworkAdapter
Description=Microsoft Kernel Debug Network Adapter
DeviceID=0
ErrorCleared=
ErrorDescription=
GUID=
Index=0
InstallDate=
Installed=TRUE
InterfaceIndex=14
LastErrorCode=
MACAddress=
Manufacturer=Microsoft
MaxNumberControlled=0
MaxSpeed=
Name=Microsoft Kernel Debug Network Adapter
NetConnectionID=
NetConnectionStatus=
NetEnabled=
NetworkAddresses=
PermanentAddress=
PhysicalAdapter=FALSE
PNPDeviceID=ROOT\KDNIC\0000

Name=WAN Miniport (Network Monitor)
NetConnectionID=
NetConnectionStatus=
NetEnabled=
NetworkAddresses=
PermanentAddress=
PhysicalAdapter=FALSE
PNPDeviceID=SWD\MSRRAS\MS_NDISWANBH
PowerManagementCapabilities=
PowerManagementSupported=FALSE
ProductName=WAN Miniport (Network Monitor)
ServiceName=NdisWan
Speed=
Status=
StatusInfo=
SystemCreationClassName=Win32_ComputerSystem
SystemName=188E
TimeOfLastReset=20240413070348.616185+180

wmic:root\cli>nic get macaddress, description
Description                                MACAddress
Microsoft Kernel Debug Network Adapter
Parallels VirtIO Ethernet Adapter         00:1C:42:9B:15:CF
WAN Miniport (SSTP)
WAN Miniport (IKEv2)
WAN Miniport (L2TP)
WAN Miniport (PPTP)
WAN Miniport (PPPOE)
WAN Miniport (IP)                         A0:75:20:52:41:53
WAN Miniport (IPv6)                       A2:D7:20:52:41:53
WAN Miniport (Network Monitor)            A6:31:20:52:41:53

wmic:root\cli>
```

Протестировал все команды, дабы не захламлять скринами отчет, сделал всего два, если необходимо добавлю

Информация об сервисах

```
wmic:root\cli>service
```

AcceptPause	AcceptStop	Caption	ErrorControl	ExitCode
FALSE	FALSE	Служба маршрутизатора AllJoyn		
\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p				
FALSE	FALSE	Служба шлюза уровня приложения	0	0
C:\Windows\System32\alg.exe				
ALG	FALSE	Удостоверение приложения		
FALSE	TRUE	C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p	0	0
Сведения о приложении				
process	TRUE	Manual	LocalSystem	Running
FALSE	FALSE	Готовность приложений	OK	Win32_ComputerSystem
C:\Windows\System32\svchost.exe -k AppReadiness -p				
adiness	FALSE	Служба развертывания AppX (AppXSVC)		
px -p	TRUE	Средство построения конечных точек Windows Audio	Share Process	FALSE
FALSE	TRUE	2228	0	Manual
FALSE	TRUE	Windows Audio	Share Process	TRUE
FALSE	TRUE	Auto	LocalSystem	Run
svchost.exe -k LocalServiceNetworkRestricted -p				
FALSE	FALSE	Время в сети мобильной связи	2652	0
Own Process				
C:\Windows\system32\svchost.exe -k autoTimeSvc				
autotimesvc	FALSE	Установщик ActiveX (AxInstSV)		
Share Process	FALSE	Manual	LocalSystem	Stopped
FALSE	FALSE	Manual	LocalSystem	OK
FALSE	FALSE	Manual	LocalSystem	Win32_ComputerSystem
FALSE	FALSE	Manual	LocalSystem	188E
FALSE	FALSE	Manual	LocalSystem	0

Протестировал все команды, дабы не захламлять скринами отчет, сделал всего один, если необходимо добавлю

Информация об процессах

```
"/?" для вызова справки, QUIT для выхода.
wmic:root\cli>process list brief
```

HandleCount	Name	Priority	ProcessId	ThreadCount	WorkingSetSize
0	System Idle Process	0	0	12	8192
2935	System	8	4	175	1347584
0	Registry	8	120	4	18493440
58	smss.exe	11	512	2	217088
472	csrss.exe	13	672	11	2691072
143	wininit.exe	13	752	2	1343488
417	csrss.exe	13	760	14	32645120
269	winlogon.exe	13	828	3	3530752
639	services.exe	9	904	6	7323648
1133	lsass.exe	9	928	6	11776000
1207	svchost.exe	8	552	10	20914176
263	WUDFHost.exe	8	644	8	1077248
40	fontdrvhost.exe	8	748	5	5754880
40	fontdrvhost.exe	8	744	5	364544
1154	svchost.exe	8	1084	8	11337728
269	svchost.exe	8	1152	3	3665920
998	dwm.exe	13	1208	16	117080064
307	svchost.exe	8	1352	4	7012352
185	svchost.exe	8	1360	2	2473984
235	svchost.exe	8	1404	1	3416064
205	svchost.exe	8	1412	1	2351104
134	svchost.exe	8	1484	1	2625536
810	svchost.exe	8	1556	9	6414336
169	svchost.exe	8	1572	3	2363392
267	svchost.exe	8	1788	6	4210688
206	svchost.exe	8	1840	1	7860224
421	svchost.exe	8	1864	5	12042240
124	svchost.exe	8	1888	1	1556480
239	svchost.exe	8	1960	3	5672960
196	svchost.exe	8	1972	2	4927488
193	svchost.exe	8	1980	2	1806336
183	svchost.exe	8	1988	5	4521984

#### 5.2.4. Задание 5.2

Написать cmd скрипт, используя wmic по аналогии с п. 5.1.7 с формированием отчета по вариантам (варианты: информация о процессах, информация об операционной системе и ЦПУ, информация о сервисах).

##### **Информация о процессах:**

@echo off

echo Формирование отчета о процессах

wmic process list brief /format:list > processes\_report.txt

echo Report saved to processes\_report.txt

##### **Информация об операционной системе и ЦПУ:**

@echo off

echo Формирование отчета о OS и CPU

wmic os get name,version /format:list > os\_report.txt

wmic cpu get name,maxclockspeed /format:list >> os\_report.txt

echo Report saved to os\_report.txt

##### **Информация о сервисах:**

@echo off

echo Формирование отчета о сервисах

wmic service where "state='Running'" get name,displayname,state /format:list > services\_report.txt

echo Report saved to services\_report.txt

Привести пример выполнения сценария для одного варианта (любого).

## Информация о сервисах:

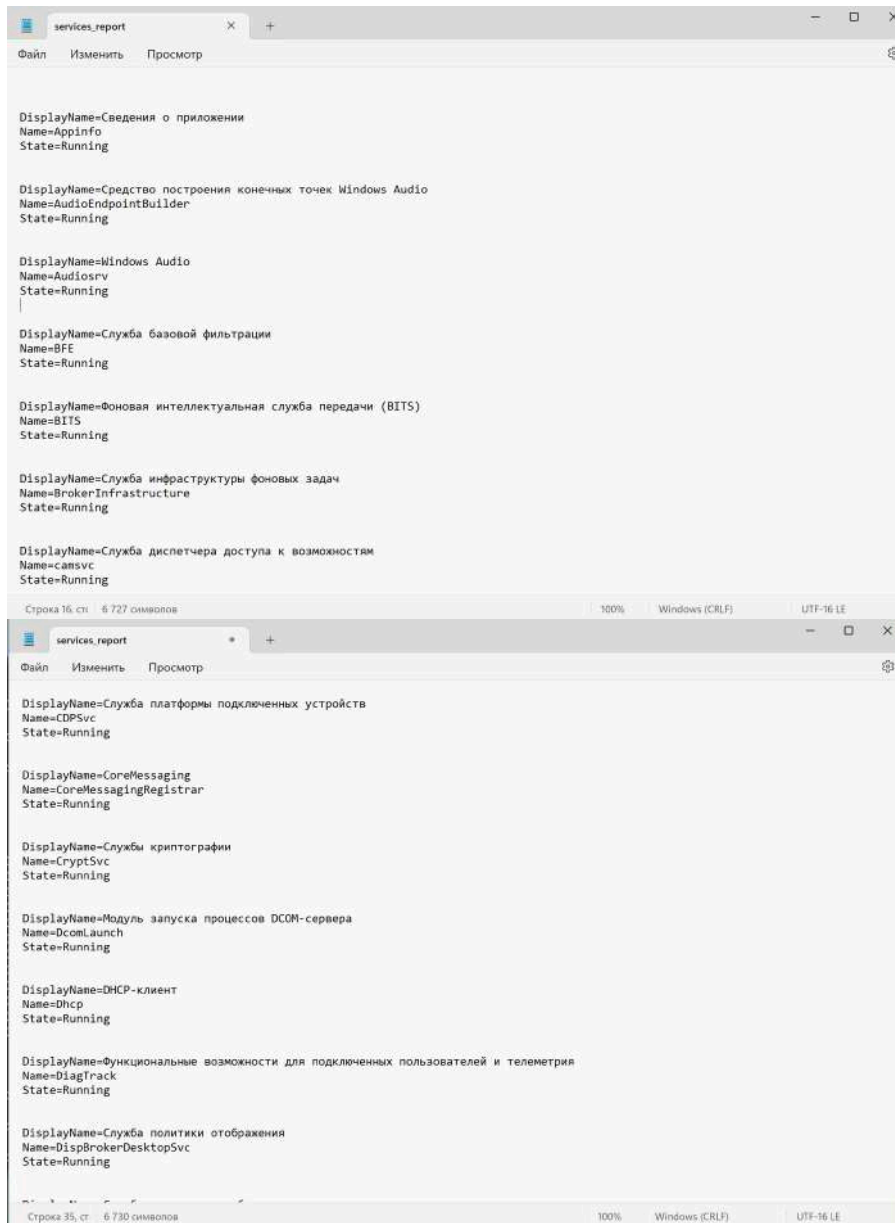
@echo off

echo Формирование отчета о сервисах

wmic service where "state='Running'" get name,displayname,state /format:list >

services\_report.txt

echo Report saved to services\_report.txt



```
services_report

DisplayName=Сведения о приложении
Name=Appinfo
State=Running

DisplayName=Средство построения конечных точек Windows Audio
Name=AudioEndpointBuilder
State=Running

DisplayName=Windows Audio
Name=Audiosrv
State=Running

DisplayName=Служба базовой фильтрации
Name=BFE
State=Running

DisplayName=Фоновая интеллектуальная служба передачи (BITS)
Name=BITS
State=Running

DisplayName=Служба инфраструктуры фоновых задач
Name=BrokerInfrastructure
State=Running

DisplayName=Служба диспетчера доступа к возможностям
Name=camsvc
State=Running

Строка 16, ст. 6 727 символов 100% Windows (CRLF) UTF-16 LE

services_report

DisplayName=Служба платформы подключенных устройств
Name=CDPSvc
State=Running

DisplayName=CoreMessaging
Name=CoreMessagingRegistrar
State=Running

DisplayName=Службы криптографии
Name=CryptSvc
State=Running

DisplayName=Модуль запуска процессов DCOM-сервера
Name=DcomLaunch
State=Running

DisplayName=DHCP-клиент
Name=Dhcp
State=Running

DisplayName=Функциональные возможности для подключенных пользователей и телеметрия
Name=DiagTrack
State=Running

DisplayName=Служба политики отображения
Name=DispBrokerDesktopSvc
State=Running

Строка 35, ст. 6 730 символов 100% Windows (CRLF) UTF-16 LE
```

```
services_report
Файл  Изменить  Просмотр
+

DisplayName=Служба улучшения отображения
Name=DisplayEnhancementService
State=Running

DisplayName=DNS-клиент
Name=Dnscache
State=Running

DisplayName=Служба политики диагностики
Name=DPS
State=Running

DisplayName=Диспетчер настройки устройств
Name=DsmSvc
State=Running

DisplayName=Служба совместного доступа к данным
Name=DsSvc
State=Running

DisplayName=Использование данных
Name=DsmSvc
State=Running

DisplayName=Журнал событий Windows
Name=EventLog
State=Running

Строка 56, ст 6 730 символов  100%  Windows (CRLF)  UTF-16 LE
```

```
services_report
Файл  Изменить  Просмотр
+

DisplayName=Система событий COM+
Name=EventSystem
State=Running

DisplayName=Служба кэша шрифтов Windows
Name=FontCache
State=Running

DisplayName=Клиент групповой политики
Name=gpsvc
State=Running

DisplayName=Служба установки Microsoft Store
Name=InstallService
State=Running

DisplayName=Вспомогательная служба IP
Name=iphlpsvc
State=Running

DisplayName=Изоляция ключей CNG
Name=KeyIso
State=Running

DisplayName=Сервер
Name=LanmanServer
State=Running

DisplayName=Рабочая станция
Name=LanmanServer
State=Running

Строка 124, с 6 730 символов  100%  Windows (CRLF)  UTF-16 LE
```

```
services_report
Файл  Изменить  Просмотр
+

Name=InstallService
State=Running

DisplayName=Темы
Name=Themes
State=Running

DisplayName=Брокер времени
Name=TimeBrokerSvc
State=Running

DisplayName=Диспетчер учетных веб-записей
Name=TokenBroker
State=Running

DisplayName=Клиент отслеживания изменившихся связей
Name=TrkWks
State=Running

DisplayName=Диспетчер пользователей
Name=UserManager
State=Running

DisplayName=Служба оркестратора обновлений
Name=Usosvc
State=Running

DisplayName=Диспетчер учетных данных
Name=VaultSvc
State=Running

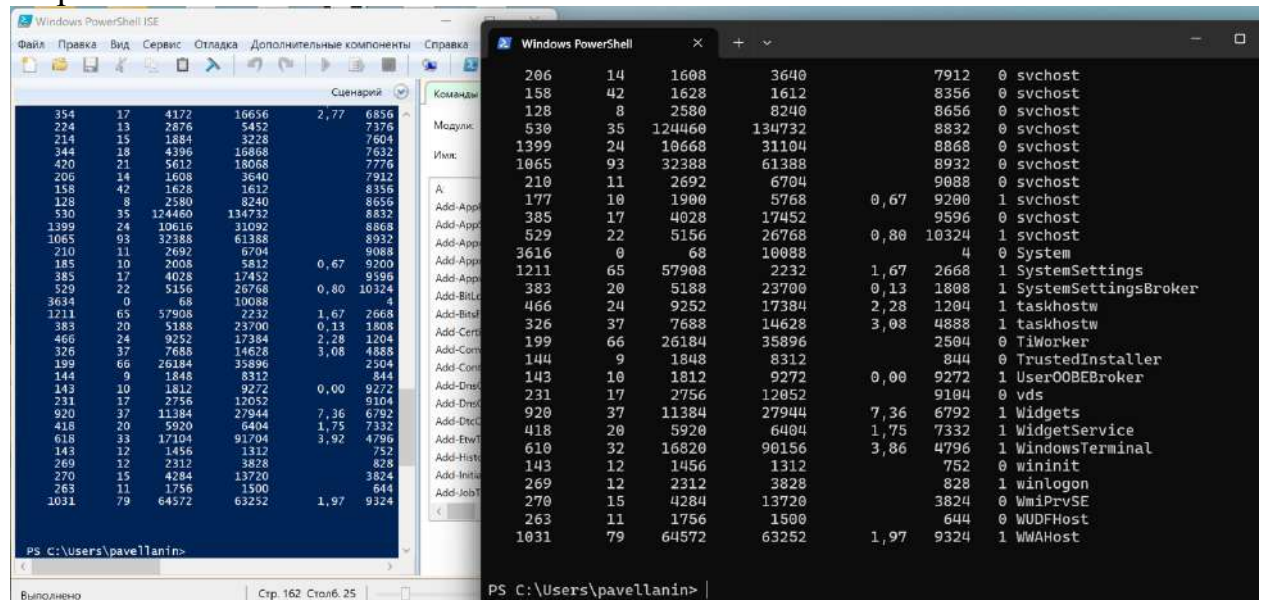
Строка 133, с 1 из 6 730 символов  100%  Windows (CRLF)  UTF-16 LE
```

## 5.3 Power Shell

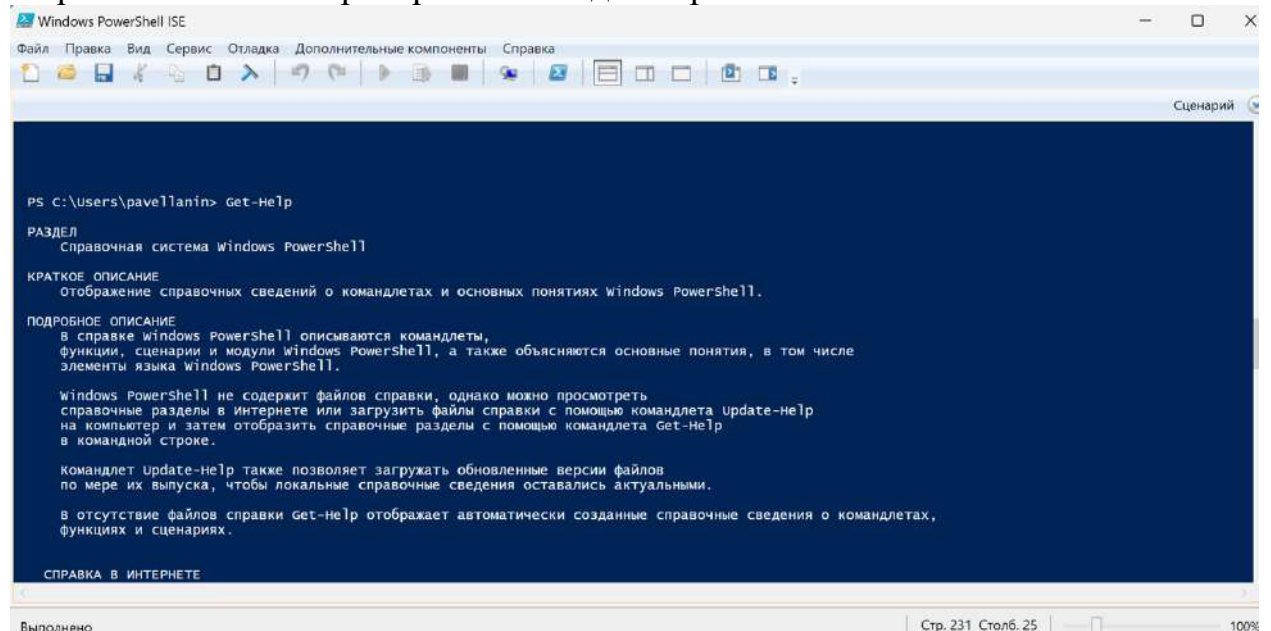
Цель работы – закрепить у студентов навыки проектирования программ-скриптов Power Shell и использования их для управления сетью

Упражнения 5.3.а - 5.3.з

Упражнения 5.3.а



Упражнение 5.3.б. Проверить команды help





```
PS C:\Users\pavellanin> get-process -?
```

ИМЯ  
Get-Process

СИНТАКСИС  
Get-Process [[-Name] <string[]>] [<CommonParameters>]  
Get-Process [[-Name] <string[]>] [<CommonParameters>]  
Get-Process [<CommonParameters>]  
Get-Process [<CommonParameters>]  
Get-Process [<CommonParameters>]  
Get-Process [<CommonParameters>]

ПСЕВДОНИМЫ  
gps  
ps

ЗАМЕЧАНИЯ  
Команде Get-Help не удалось найти файлы справки для этого командлета на этом компьютере. Она отображает только часть справки.  
- Чтобы скачать и установить файлы справки для модуля, включающего этот командлет, воспользуйтесь командой Update-Help.  
- Чтобы просмотреть раздел справки для этого командлета в Интернете, введите: "Get-Help Get-Process -Online" или перейдите к <https://go.microsoft.com/fwlink/?LinkID=113324>.

```
PS C:\Users\pavellanin> get-help get-process
```

ИМЯ  
Get-Process

СИНТАКСИС  
Get-Process [[-Name] <string[]>] [<CommonParameters>]  
Get-Process [[-Name] <string[]>] [<CommonParameters>]  
Get-Process [<CommonParameters>]  
Get-Process [<CommonParameters>]  
Get-Process [<CommonParameters>]  
Get-Process [<CommonParameters>]

ПСЕВДОНИМЫ  
gps  
ps

ЗАМЕЧАНИЯ  
Команде Get-Help не удалось найти файлы справки для этого командлета на этом компьютере. Она отображает только часть справки.  
- Чтобы скачать и установить файлы справки для модуля, включающего этот командлет, воспользуйтесь командой Update-Help.  
- Чтобы просмотреть раздел справки для этого командлета в Интернете, введите: "Get-Help Get-Process -Online" или перейдите к <https://go.microsoft.com/fwlink/?LinkID=113324>.

```
PS C:\Users\pavellanin> get-help get-process -Detailed
```

ИМЯ  
Get-Process

СИНТАКСИС  
Get-Process [[-Name] <string[]>] [<CommonParameters>]  
Get-Process [[-Name] <string[]>] [<CommonParameters>]  
Get-Process [<CommonParameters>]  
Get-Process [<CommonParameters>]  
Get-Process [<CommonParameters>]  
Get-Process [<CommonParameters>]

ПАРАМЕТРЫ  
-ComputerName <string[]>  
-FileVersionInfo  
-Id <int[]>  
-IncludeUserName  
-InputObject <Process[]>  
-Module

```
PS C:\Users\pavellanin> Get-Alias
```

CommandType	Name	Version	Source
Alias	----	-----	-----
Alias	% -> ForEach-Object		
Alias	? -> Where-Object		
Alias	ac -> Add-Content		
Alias	asnp -> Add-PSSnapin		
Alias	cat -> Get-Content		
Alias	cd -> Set-Location		
Alias	CFS -> ConvertFrom-String	3.1.0.0	Microsoft.PowerShell.Utility
Alias	chdir -> Set-Location		
Alias	clc -> Clear-Content		
Alias	clear -> Clear-Host		
Alias	clhy -> Clear-History		
Alias	cli -> Clear-Item		
Alias	clp -> Clear-ItemProperty		
Alias	cls -> Clear-Host		
Alias	clv -> Clear-Variable		
Alias	cnsn -> Connect-PSession		
Alias	compare -> Compare-Object		
Alias	copy -> Copy-Item		
Alias	cp -> Copy-Item		
Alias	cpi -> Copy-Item		
Alias	cpp -> Copy-ItemProperty		
Alias	curl -> Invoke-WebRequest		
Alias	cvpa -> Convert-Path		
Alias	dbp -> Disable-PSBreakpoint		
Alias	del -> Remove-Item		
Alias	diff -> Compare-Object		
Alias	dir -> Get-Childitem		

### Упражнение 5.3.в.

```
Mode                LastWriteTime         Length Name
----                -
d-----            07.04.2024    23:02             tmp2
-a-----            07.04.2024    23:45         572 cws.txt
-a-----            07.04.2024    23:45         635 d0.txt
-a-----            07.04.2024    23:45         589 d1.txt
-a-----            07.04.2024    23:45         592 d2.txt
-a-----            07.04.2024    23:45        1182 resd.txt
-a-----            14.04.2024    13:17       14370 services_report.txt
-a-----            14.04.2024    13:17         208 t1.cmd
-a-----            07.04.2024    22:56          14 t1.txt
-a-----            07.04.2024    22:56          14 t2.txt
-a-----            07.04.2024    22:56          14 t3.txt
-a-----            07.04.2024    22:56          14 t4.txt

PS C:\tmp> notepad helloworld.ps1

PS C:\tmp> dir

Каталог: C:\tmp

Mode                LastWriteTime         Length Name
----                -
d-----            07.04.2024    23:02             tmp2
-a-----            07.04.2024    23:45         572 cws.txt
-a-----            07.04.2024    23:45         635 d0.txt
-a-----            07.04.2024    23:45         589 d1.txt
-a-----            07.04.2024    23:45         592 d2.txt
-a-----            14.04.2024    13:52           0 helloworld.ps1
-a-----            07.04.2024    23:45        1182 resd.txt
-a-----            14.04.2024    13:52       14376 services_report.txt
-a-----            14.04.2024    13:17         208 t1.cmd
-a-----            07.04.2024    22:56          14 t1.txt
-a-----            07.04.2024    22:56          14 t2.txt
-a-----            07.04.2024    22:56          14 t3.txt
-a-----            07.04.2024    22:56          14 t4.txt

PS C:\tmp> |
```

Создали файл helloworld.ps1

```
PS C:\tmp> .\helloworld.ps1
hello world

PS C:\tmp>
```

Стр. 62 Стр. 6, 12 100%



## Упражнение 5.3.г.

```
PS C:\Users\pavellanin> Get-Childitem
```

Каталог: C:\Users\pavellanin

Mode	LastWriteTime	Length	Name
d-----	01.04.2023	12:54	.android
d-----	14.03.2024	18:35	Cisco Packet Tracer 7.3.0
d-r----	09.03.2023	21:04	Contacts
d-r----	07.05.2022	8:24	Desktop
d-r----	09.03.2023	21:04	Documents
d-r----	31.03.2023	2:14	Downloads
d-r----	09.03.2023	21:04	Favorites
d-r----	09.03.2023	21:04	Links
d-r----	31.03.2023	2:14	Music
d-----	01.04.2023	12:51	Nox_share
d-----	01.06.2023	11:18	OpenVPN
d-r----	31.03.2023	2:14	Pictures
d-r----	09.03.2023	21:04	Saved Games
d-r----	09.03.2023	21:36	Searches
d-r----	31.03.2023	2:14	Videos
d-----	01.04.2023	13:00	vmlogs
-a-----	02.04.2024	15:43	186 .packettracer
-a-----	01.04.2023	12:51	41 inst.ini
-a-----	20.02.2024	20:56	0 ipconfig
-a-----	01.04.2023	12:51	45 nuuid.ini
-a-----	14.04.2024	13:07	160454 Services_Info.txt
-a-----	07.04.2024	23:45	662 test.cmd
-a-----	07.04.2024	21:48	2493 th2.txt
-a-----	01.04.2023	12:51	53 useruid.ini
-a-----	20.02.2024	20:57	0 wmic

```
PS C:\Users\pavellanin> dir
```

Каталог: C:\Users\pavellanin

Mode	LastWriteTime	Length	Name
------	---------------	--------	------

```
PS C:\Users\pavellanin> dir
```

Каталог: C:\Users\pavellanin

Mode	LastWriteTime	Length	Name
d-----	01.04.2023	12:54	.android
d-----	14.03.2024	18:35	Cisco Packet Tracer 7.3.0
d-r----	09.03.2023	21:04	Contacts
d-r----	07.05.2022	8:24	Desktop
d-r----	09.03.2023	21:04	Documents
d-r----	31.03.2023	2:14	Downloads
d-r----	09.03.2023	21:04	Favorites
d-r----	09.03.2023	21:04	Links
d-r----	31.03.2023	2:14	Music
d-----	01.04.2023	12:51	Nox_share
d-----	01.06.2023	11:18	OpenVPN
d-r----	31.03.2023	2:14	Pictures
d-r----	09.03.2023	21:04	Saved Games
d-r----	09.03.2023	21:36	Searches
d-r----	31.03.2023	2:14	Videos
d-----	01.04.2023	13:00	vmlogs
-a-----	02.04.2024	15:43	186 .packettracer
-a-----	01.04.2023	12:51	41 inst.ini
-a-----	20.02.2024	20:56	0 ipconfig
-a-----	01.04.2023	12:51	45 nuuid.ini
-a-----	14.04.2024	13:07	160454 Services_Info.txt
-a-----	07.04.2024	23:45	662 test.cmd
-a-----	07.04.2024	21:48	2493 th2.txt
-a-----	01.04.2023	12:51	53 useruid.ini
-a-----	20.02.2024	20:57	0 wmic

```
PS C:\Users\pavellanin> ls
```

Каталог: C:\Users\pavellanin

PS C:\tmp> gps | convertto-html > C:\tmp\lproc.htm

PS C:\tmp> |

Выполнено

Стр. 163 Столб. 12

115%

tmp

← → ↑ ↻ 🖨 > Этот компьютер > Локальный диск (C:) > tmp >

Поиск в: tmp

📁 Создать ✂ 📄 📁 📄 📄 🗑

📄 Сортировать ▾

📄 Просмотреть ▾

⋮

📄 Сведения

Документы

Изображения

iCloud Drive

79209264909

79209263319

Музыка

Видео

Лабы

ЛР4

tmp

drive-download

Имя	Дата изменения	Тип	Размер
cws	07.04.2024 23:45	Текстовый документ	1 КБ
d0	07.04.2024 23:45	Текстовый документ	1 КБ
d1	07.04.2024 23:45	Текстовый документ	1 КБ
d2	07.04.2024 23:45	Текстовый документ	1 КБ
resd	07.04.2024 23:45	Текстовый документ	2 КБ
t1	14.04.2024 13:17	Сценарий Windows	1 КБ
t1	07.04.2024 22:56	Текстовый документ	1 КБ
t2	07.04.2024 22:56	Текстовый документ	1 КБ
t3	07.04.2024 22:56	Текстовый документ	1 КБ
t4	07.04.2024 22:56	Текстовый документ	1 КБ
services_report	14.04.2024 13:52	Текстовый документ	15 КБ
helloworld	14.04.2024 13:53	Сценарий Windows ...	1 КБ
lproc	14.04.2024 14:03	Microsoft Edge HTM...	291 КБ

Элементов: 14

Выбран 1 элемент: 290 КБ

Name	Просмотреть сведения о сайте	FileVersion	HandleCount	WorkingSet	PagedMemorySize	PrivateMemorySize	VirtualMemorySize	TotalProcessorTim
AccountsControlHost	3540 Normal	10.0.22621.2506 (WinBuild.160101.0800)	411	34873344	9007104	9007104	299249664	00:00:00.2812500
AggregatorHost	4112		171	7122944	2588672	2588672	73228288	
ApplicationFrameHost	8140 Normal	10.0.22621.2506 (WinBuild.160101.0800)	389	26193920	13660160	13660160	285028352	00:00:02.3281250
backgroundTaskHost	10968 Normal	10.0.22621.1 (WinBuild.160101.0800)	178	11128832	2678784	2678784	121950208	00:00:00.0156250
CNAB4RPD	948		101	389120	970752	970752	62787584	
coherence	3268		131	1826816	1445888	1445888	83722240	
coherence	4964		150	1855488	1867776	1867776	108191744	
csrss	672		492	2613248	1974272	1974272	94994432	
csrss	760		463	23601152	3207168	3207168	166805504	
ctfmon	8208		572	18644992	7954432	7954432	185683968	00:00:14.1718750
dllhost	2800 Normal	10.0.22621.1 (WinBuild.160101.0800)	133	8286208	1712128	1712128	94564352	00:00:00.6093750
dllhost	3520 Normal	10.0.22621.1 (WinBuild.160101.0800)	168	8699904	2457600	2457600	112582656	00:00:02.2656250

## Упражнение 5.3.д. Вывод списка сервисов и списка процессов, и полезные командлеты

### Список алиасов

```
PS C:\tmp> Get-Alias

CommandType      Name                                Version      Source
-----
Alias             % -> ForEach-Object
Alias             ? -> Where-Object
Alias             ac -> Add-Content
Alias             asnp -> Add-PSSnapin
Alias             cat -> Get-Content
Alias             cd -> Set-Location
Alias             cfs -> ConvertFrom-String          3.1.0.0     Microsoft.PowerShell.Utility
Alias             chdir -> Set-Location
Alias             clc -> Clear-Content
Alias             clear -> Clear-Host
Alias             clhy -> Clear-History
Alias             cli -> Clear-Item
Alias             clip -> Clear-ItemProperty
Alias             cls -> Clear-Host
Alias             clv -> Clear-Variable
Alias             cnsn -> Connect-PSsession
Alias             compare -> Compare-Object
Alias             copy -> Copy-Item
Alias             cp -> Copy-Item
Alias             cpi -> Copy-Item
Alias             cpp -> Copy-ItemProperty
Alias             curl -> Invoke-WebRequest
Alias             cvpa -> Convert-Path
Alias             dbp -> Disable-PSBreakpoint
Alias             del -> Remove-Item
Alias             diff -> Compare-Object
Alias             dir -> Get-ChildItem
Alias             dsn -> Disconnect-PSsession
Alias             ebp -> Enable-PSBreakpoint
Alias             echo -> Write-Output
Alias             epal -> Export-Alias
Alias             epsv -> Export-Csv
Alias             epsn -> Export-PSsession
Alias             erase -> Remove-Item
Alias             esep -> Export-PSsession
```

### История команд

```
PS C:\tmp> Get-History
```

Id	CommandLine
1	Get-ChildItem
2	dir
3	ls
4	pwd
5	cd c:\temp
6	cd C:\temp
7	cd
8	cd C:
9	cd C:\tmp
10	gps   convertto-html > c:\tmp\lproc.htm
11	gps   convertto-html > C:\tmp\lproc.htm
12	gps   convertto-html > c:\tmp\lproc.htm
13	gps   convertto-html > C:\tmp\lproc.htm
14	Get-Alias

## Список процессов

```
PS C:\tmp> ps
```

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
411	23	8796	2436	0,28	3540	1	AccountsControlHost
171	10	2552	3708		4112	0	AggregatorHost
439	26	17112	19808	3,19	8140	1	ApplicationFrameHost
101	10	948	92		948	0	CNAB4RPD
131	8	1412	412		3268	0	coherence
150	10	1824	276		4964	1	coherence
507	21	1940	2144		672	0	csrss
479	21	3384	52600		760	1	csrss
573	21	7884	12736	15,25	8208	1	ctfmon
133	9	1676	2408	0,78	2800	1	dllhost
157	10	2364	4064	2,67	3520	1	dllhost
519	25	6564	4080	1,45	6152	1	dllhost
1051	71	157128	46028		1208	1	dwm
7287	349	304404	216856	359,39	5196	1	explorer
40	6	1340	208		744	0	Fontdrvhost
40	12	8668	720		748	1	Fontdrvhost
758	34	15280	2800	0,94	10904	1	GameBar
288	14	3452	3696	0,42	3316	1	GameBarFTServer
0	0	60	8		0	0	Idle
1510	28	8260	11764		928	0	lsass
0	0	944	123756		2208	0	Memory compression
218	14	1972	3840		4452	0	MicrosoftEdgeUpdate
320	17	10732	16752	5,75	840	1	msedge
1489	51	61164	59916	26,63	3012	1	msedge
218	16	20588	2540	0,75	4272	1	msedge
168	10	2024	1332	0,27	6228	1	msedge
477	24	17064	34932	6,66	9500	1	msedge
177	11	6844	2640	0,70	11100	1	msedge
269	18	67036	13684	4,72	11120	1	msedge
249	15	7712	10864	1,05	11248	1	msedge
892	104	302128	96388		3232	0	MsMpEng
228	27	3788	3044		5784	0	NisSrv
1302	107	231844	97152	82,53	4868	1	PAD_Console.Host
896	65	156608	118660	24,42	7644	1	powershell_exe
813	43	14752	21416	55,45	5804	1	powershell_exe

## Список сервисов

```
PS C:\tmp> gsv
```

Status	Name	DisplayName
Stopped	AarSvc_4d6d9	Agent Activation Runtime_4d6d9
Stopped	AJRouter	Служба маршрутизатора AllJoyn
Stopped	ALG	Служба шлюза уровня приложения
Stopped	AppIDSvc	Удостоверение приложения
Running	AppInfo	Сведения о приложениях
Stopped	AppReadiness	Готовность приложений
Stopped	AppXSvc	Служба развертывания AppX (AppXSVC)
Running	AudioEndpointBu...	Средство построения конечных точек ...
Running	Audiosrv	Windows Audio
Stopped	autotimesvc	Время в сети мобильной связи
Stopped	AxInstSV	Установщик ActiveX (AxInstSV)
Running	BcastDVRUserSer...	Пользовательская служба DVR для игр...
Stopped	BDESVC	Служба шифрования дисков BitLocker
Running	BFE	Служба базовой фильтрации
Stopped	BITS	Фоновая интеллектуальная служба пер...
Stopped	BluetoothUserSe...	Служба поддержки пользователей Blue...
Running	BrokerInfrastru...	Служба инфраструктуры фоновых задач
Stopped	BTAGService	Служба звукового шлюза Bluetooth
Stopped	BthAvctpSvc	Служба AVCTP
Stopped	bthserv	Служба поддержки Bluetooth
Running	camsvc	Служба диспетчера доступа к возможн...
Stopped	CaptureService_...	CaptureService_4d6d9
Running	cbdhsvc_4d6d9	Пользовательская служба буфера обме...
Running	CDPSvc	Служба платформы подключенных устро...
Running	CDPUserSvc_4d6d9	Служба пользователя платформы подкл...
Stopped	CentPropSvc	Распространение сертификата
Running	clipsvc	Служба лицензий клиента (clipsvc)
Stopped	CloudBackupRest...	Облачная служба резервного копирова...
Stopped	COMSysApp	Системное приложение COM+
Stopped	ConsentUserSvc_...	Служба пользователя ConsentUX_4d6d9
Running	CoreMessagingRe...	CoreMessaging
Stopped	CredentialEnrol...	CredentialEnrollmentManagerUserSvc_...
Running	CryptSvc	Служба криптографии
Running	DCOMLaunch	Модуль запуска процессов DCOM-сервера



## Упражнение 5.3.е. Свойства для списков процессов и сервисов

```
PS C:\tmp> gsv | Get-Member

TypeName: System.ServiceProcess.ServiceController

Name MemberType Definition
-----
Name AliasProperty Name = ServiceName
RequiredServices AliasProperty RequiredServices = ServicesDependedon
Disposed Event System.EventHandler Disposed(System.Object, System.EventArgs)
Close Method void Close()
Continue Method void Continue()
CreateObjRef Method System.Runtime.Remoting.ObjRef CreateObjRef(type requestedType)
Dispose Method void Dispose(), void IDisposable.Dispose()
Equals Method bool Equals(System.Object obj)
ExecuteCommand Method void ExecuteCommand(int command)
GetHashCode Method int GetHashCode()
GetLifetimeService Method System.Object GetLifetimeService()
GetType Method type GetType()
InitializeLifetimeService Method System.Object InitializeLifetimeService()
Pause Method void Pause()
Refresh Method void Refresh()
Start Method void Start(), void Start(string[] args)
Stop Method void Stop()
WaitForStatus Method void WaitForStatus(System.ServiceProcess.ServiceControllerStatus desiredStatus), void WaitForStatus(System.ServiceP...
CanPauseAndContinue Property bool CanPauseAndContinue {get;}
CanShutdown Property bool CanShutdown {get;}
CanStop Property bool CanStop {get;}
Container Property System.ComponentModel.IContainer Container {get;}
DependentServices Property System.ServiceProcess.ServiceController[] DependentServices {get;}
DisplayName Property string DisplayName {get;set;}
MachineName Property string MachineName {get;set;}
ServiceHandle Property System.Runtime.InteropServices.SafeHandle ServiceHandle {get;}
ServiceName Property string ServiceName {get;set;}
ServicesDependedon Property System.ServiceProcess.ServiceController[] ServicesDependedon {get;}
ServiceType Property System.ServiceProcess.ServiceType ServiceType {get;}
Site Property System.ComponentModel.ISite Site {get;set;}
StartType Property System.ServiceProcess.ServiceStartMode StartType {get;}

PS C:\tmp> gps | Get-Member

TypeName: System.Diagnostics.Process

Name MemberType Definition
-----
Handles AliasProperty Handles = Handlecount
Name AliasProperty Name = ProcessName
NPM AliasProperty NPM = NonpagedSystemMemorySize64
PM AliasProperty PM = PagedMemorySize64
SI AliasProperty SI = SessionId
VM AliasProperty VM = VirtualMemorySize64
WS AliasProperty WS = WorkingSet64
Disposed Event System.EventHandler Disposed(System.Object, System.EventArgs)
ErrorDataReceived Event System.Diagnostics.DataReceivedEventHandler ErrorDataReceived(System.Object, System.Diagnostics.DataReceivedEvent...)
Exited Event System.EventHandler Exited(System.Object, System.EventArgs)
OutputDataReceived Event System.Diagnostics.DataReceivedEventHandler OutputDataReceived(System.Object, System.Diagnostics.DataReceivedEvent...)
BeginErrorReadLine Method void BeginErrorReadLine()
BeginOutputReadLine Method void BeginOutputReadLine()
CancelErrorRead Method void CancelErrorRead()
CancelOutputRead Method void CancelOutputRead()
Close Method void Close()
CloseMainWindow Method bool CloseMainWindow()
CreateObjRef Method System.Runtime.Remoting.ObjRef CreateObjRef(type requestedType)
Dispose Method void Dispose(), void IDisposable.Dispose()
Equals Method bool Equals(System.Object obj)
GetHashCode Method int GetHashCode()
GetLifetimeService Method System.Object GetLifetimeService()
GetType Method type GetType()
InitializeLifetimeService Method System.Object InitializeLifetimeService()
Kill Method void Kill()
Refresh Method void Refresh()
Start Method bool Start()
```

## Упражнения 5.3.ж. (А, Б, )

### Вывод только работающих сервисов

```
PS C:\tmp> get-service | where-object {$_.Status -eq "Running"}

Status Name Displayname
-----
Running Appinfo Сведения о приложениях
Running AppXSvc Служба развертывания AppX (AppXSvc)
Running AudioEndpointBu... Средство построения конечных точек ...
Running Audiosrv Windows Audio
Running BcastDVRUserSer... Пользовательская служба DVR для игр...
Running BFE Служба базовой фильтрации
Running BrokerInfrastru... Служба инфраструктуры фоновых задач
Running camsvc Служба диспетчера доступа к возможн...
Running cbdhsvc_4d6d9 Пользовательская служба буфера обме...
Running CDPSvc Служба платформы подключенных устро...
Running CDPUserSvc_4d6d9 Служба пользователя платформы подкл...
Running Clipsvc Служба лицензий клиента (Clipsvc)
Running CoreMessagingRe... CoreMessaging
Running CryptSvc Службы криптографии
Running DcomLaunch Модуль запуска процессов DCOM-сервера
Running Dhcp DHCP-клиент
Running DiagTrack Функциональные возможности для подк...
Running DisplayBroker Deskt... Служба политики отображения
Running DisplayEnhancem... Служба улучшения отображения
Running Dnscache DNS-клиент
Running DoSvc Оптимизация доставки
Running DPS Служба политики диагностики
Running DSSvc Служба совместного доступа к данным
Running DsmSvc Использование данных
Running Eventlog Журнал событий Windows
Running EventSystem Система событий COM
Running FontCache Служба кэша шрифтов Windows
Running InstallService Служба установки Microsoft Store
Running Iphlpsvc Вспомогательная служба IP
Running KeyIso Изоляция ключей CNG
Running LanmanServer Сервер
Running LanmanWorkstation Рабочая станция
Running lfrs Служба географического положения
Running LicenseManager Служба Windows License Manager
```

## Вывод процессов, у которых значение Handle больше 500

PS C:\tmp> gps   where-Object {\$_.Handles -gt 500}							
Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
503	21	1948	2288		672	0	csrss
578	21	7908	13148	15,84	8208	1	ctfmon
518	25	6564	4092	1,45	6152	1	dllhost
1102	73	143096	49700		1208	1	dwm
7345	367	302412	247000	369,84	5196	1	explorer
758	34	15280	2800	0,94	10904	1	GameBar
1462	27	8212	12436		928	0	lsass
1481	50	61096	58976	26,75	3012	1	msedge
879	104	301920	130144		3232	0	MsMpEng
625	34	17884	77808	0,58	2396	1	Notepad
1298	107	231840	97212	83,80	4868	1	PAD.Console.Host
776	65	162760	139036	29,06	7644	1	powershell_ise
825	44	13852	22532	55,78	5904	1	prl_cc
901	18	2588	3856		3392	1	prl_tools
648	32	13336	12596	8,09	6956	1	RuntimeBroker
590	25	8448	12224	3,05	8856	1	RuntimeBroker
1555	125	162848	3476	45,89	6424	1	SearchHost
683	21	17260	13864		5528	0	SearchIndexer
658	13	5064	6036		904	0	services
955	43	32212	2440	8,61	7900	1	ShellExperienceHost
680	22	6912	19300	35,17	4460	1	sihost
938	46	58452	26284	31,67	6448	1	StartMenuExperienceHost
1319	24	11644	19956		552	0	svchost
1197	19	8048	12008		1084	0	svchost
884	20	5868	11748		1556	0	svchost
552	30	12348	10372		3208	0	svchost
677	29	19552	18856		3256	0	svchost
502	23	8124	16724	10,52	4608	1	svchost
514	23	10640	12756		7776	0	svchost
520	20	4884	6232	3,39	10324	1	svchost
3507	0	68	10660		4	0	System
1211	65	57908	0	1,67	2668	1	SystemSettings
1031	79	64572	3132	1,97	9324	1	WAAHost

PS C:\tmp> gps   where-Object {\$_.Handles -lt 500}							
Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
411	23	8796	2436	0,28	3540	1	AccountsControlHost
169	10	2492	3672		4112	0	AggregatorHost
437	25	17052	18984	3,19	8140	1	ApplicationFrameHost
101	10	948	92		948	0	CNAB4RPP
131	8	1412	412		3268	0	coherence
150	10	1824	276		4964	1	coherence
133	9	1676	2408	0,78	2800	1	dllhost
161	11	2472	7488	2,67	3520	1	dllhost
40	6	1340	208		744	0	fontdrvhost
40	11	8756	1988		748	1	fontdrvhost
288	14	3452	3696	0,42	3316	1	GameBarFTServer
0	0	60	8		0	0	Idle
0	0	944	108332		2208	0	Memory Compression
218	14	1972	3840		4452	0	MicrosoftEdgeUpdate
320	17	10724	16752	5,75	840	1	msedge
218	16	20588	2496	0,75	4272	1	msedge
168	10	2024	1332	0,27	6228	1	msedge
477	23	17032	34820	6,73	9500	1	msedge
177	11	6844	2632	0,75	11100	1	msedge
269	18	67036	10804	4,72	11120	1	msedge
249	15	7712	10864	1,05	11248	1	msedge
228	19	3704	4376		5784	0	Nissrv
227	19	2596	2896		3224	0	prl_tools_service
0	12	5300	24988		120	0	Registry
262	15	7368	15504	1,17	3328	1	RuntimeBroker
276	16	5352	2888	0,41	5488	1	RuntimeBroker
339	21	8340	8800	13,67	6920	1	RuntimeBroker
161	11	2192	2532	0,08	9560	1	RuntimeBroker
349	17	3936	12120	2,59	11184	1	RuntimeBroker
496	21	7136	10476		8636	0	SecurityHealthService
187	10	1956	3708	0,73	8592	1	SecurityHealthSystray
175	11	2592	10392	0,06	5256	1	smartscreen
58	3	1124	124		512	0	smss
497	24	6540	4388		2972	0	spoolsv

Сохранение результатов в файл (с помощью `>`) + дописываем вторую часть (С помощью `>>`)

Handles NPM(K) PM(K) WS(K) CPU(s) Id SI ProcessName							
578	22	7952	13184	15,84	8208	1	ctfmon
518	25	6564	4092	1,45	6152	1	dllhost
1098	72	142940	49584		1208	1	dwm
7298	368	301772	246508	369,92	5196	1	explorer
758	34	15280	2800	0,94	10904	1	GameBar
1467	27	8128	12440		928	0	lsass
1479	50	61064	58976	26,77	3012	1	msedge
881	104	302128	128016		3232	0	MsMpEng
623	34	17880	78020	0,58	2396	1	Notepad
1349	108	231956	100100	84,05	4868	1	PAD.Console.Host
810	65	168204	144312	30,69	7644	1	powershell_ise
812	43	13728	22460	55,78	5904	1	prl_cc
898	18	2592	3860		3392	1	prl_tools
644	31	13200	12556	8,09	6956	1	RuntimeBroker
590	25	8380	12204	3,05	8856	1	RuntimeBroker
1555	125	162848	3476	45,89	6424	1	SearchHost
687	21	17416	13944		5528	0	SearchIndexer
651	13	5168	6076		904	0	services
955	43	32212	2440	8,61	7900	1	ShellExperienceHost
678	22	6920	19308	35,17	4460	1	sihost



Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
411	23	8796	2436	0,28	3540	1	AccountsControlHost
169	10	2492	3672		4112	0	AggregatorHost
437	25	17052	18984	3,19	8140	1	ApplicationFrameHost
178	11	2640	12064	0,06	5172	1	backgroundTaskHost
182	11	2584	11904	0,08	7700	1	backgroundTaskHost
182	11	2608	11812	0,02	8496	1	backgroundTaskHost
101	10	948	92		948	0	CNAB4RPD
131	8	1412	412		3268	0	coherence
150	10	1824	276		4964	1	coherence
133	9	1676	2408	0,78	2800	1	dllhost
161	11	2472	7488	2,67	3520	1	dllhost
40	6	1340	208		744	0	fontdrvhost
40	11	8756	1988		748	1	fontdrvhost
288	14	3452	3696	0,42	3316	1	GameBarFTServer
0	0	60	8		0	0	Idle
0	0	944	105708		2208	0	Memory Compression
218	14	1972	3840		4452	0	MicrosoftEdgeUpdate
320	17	10692	16736	5,75	840	1	msedge
218	16	20588	2496	0,75	4272	1	msedge

Строка 18, стр | 23 061 символ

100% Windows (CRLF) UTF-16 LE

## Упражнения 5.3.3.

PS C:\tmp> Get-Process   Where-Object {\$_.Handles -gt 500}   Sort-Object Handles -Descending							
Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
7288	373	301132	246536	370,52	5196	1	explorer
3404	0	68	10660		4	0	System
1555	125	162848	3312	45,89	6424	1	SearchHost
1488	27	8196	12480		928	0	lsass
1477	50	61032	61976	27,00	3012	1	msedge
1323	24	11752	20008		552	0	svchost
1309	107	231892	100064	84,42	4868	1	PAD.Console.Host
1211	65	57908	0	1,67	2668	1	SystemSettings
1204	18	7980	11972		1084	0	svchost
1054	71	142980	49768		1208	1	dwm
1031	79	64572	3132	1,97	9324	1	WAAHost
955	43	32212	2440	8,61	7900	1	ShellExperienceHost
936	46	58416	26360	31,67	6448	1	StartMenuExperienceHost
905	65	171940	148776	32,39	7644	1	powershell_ise
899	18	2592	3864		3392	1	prl_tools
883	20	5712	11688		1556	0	svchost
879	105	302236	129984		3232	0	MSMpEng
811	43	13756	22488	55,83	5904	1	prl_cc
758	34	15280	2800	0,94	10904	1	GameBar
681	21	17176	13980		5528	0	SearchIndexer
679	22	6952	19560	35,42	4460	1	sihost
663	28	19360	18604		3256	0	svchost
652	12	5012	6036		904	0	services
646	32	13268	12596	8,09	6956	1	RuntimeBroker
590	25	8380	12204	3,05	8856	1	RuntimeBroker
573	22	7964	13224	15,91	8208	1	ctfmon
548	30	12292	10556		3208	0	svchost
525	24	8484	17004	10,55	4608	1	svchost
520	20	4832	6220	3,39	10324	1	svchost
518	25	6564	4092	1,45	6152	1	dllhost
505	22	10556	12764		7776	0	svchost
505	21	1924	2264		672	0	csrss

PS C:\tmp> Get-Process   Where-Object {\$_.Handles -gt 500}   Sort-Object CPU -Descending							
Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
7288	373	301436	246620	370,52	5196	1	explorer
1319	107	231802	100064	84,53	4868	1	PAD.Console.Host
815	43	13784	22504	55,84	5904	1	prl_cc
1555	125	162848	3312	45,89	6424	1	SearchHost
677	22	6936	19544	35,42	4460	1	sihost
918	65	166312	144356	32,70	7644	1	powershell_ise
938	46	58444	26380	31,67	6448	1	StartMenuExperienceHost
1477	50	61032	61988	27,00	3012	1	msedge
573	22	7964	13224	15,91	8208	1	ctfmon
516	23	8288	16904	10,55	4608	1	svchost
955	43	32212	2440	8,61	7900	1	ShellExperienceHost
648	32	13336	12608	8,09	6956	1	RuntimeBroker
520	20	4832	6220	3,39	10324	1	svchost
590	25	8380	12204	3,05	8856	1	RuntimeBroker
1031	79	64572	3132	1,97	9324	1	WAAHost
1211	65	57908	0	1,67	2668	1	SystemSettings
518	25	6564	4092	1,45	6152	1	dllhost
758	34	15280	2800	0,94	10904	1	GameBar
3404	0	68	10660		4	0	System
505	22	10548	12756		7776	0	svchost
1054	71	142836	49628		1208	1	dwm
659	28	19252	18564		3256	0	svchost
548	30	12292	10556		3208	0	svchost
881	20	5684	11660		1556	0	svchost
1206	18	8080	11988		1084	0	svchost
1320	24	11968	20264		552	0	svchost
1485	27	8128	12444		928	0	lsass
875	104	301988	127020		3232	0	MSMpEng
652	12	4992	6040		904	0	services
681	21	17228	13996		5528	0	SearchIndexer
895	18	2528	3824		3392	1	prl_tools
504	21	1924	2264		672	0	csrss

```
PS C:\tmp> Get-Process | Where-Object {$_.Handles -gt 500} | Sort-Object PM -Descending
```

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
875	104	301904	127036		3232	0	MsMpEng
7292	376	301508	246500	370.53	5196	1	explorer
1330	107	231892	100064	84.55	4868	1	PAD.Console.Host
1555	125	162848	3312	45.89	6424	1	SearchHost
954	65	162680	140680	33.00	7644	1	powershell_ise
1052	71	142840	49540		1208	1	dwm
1031	79	64572	3132	1.97	9324	1	WAAHost
1477	50	61004	61976	27.00	3012	1	msedge
938	46	58444	26380	31.67	6448	1	StartMenuExperienceHost
1211	65	57908	0	1.67	2668	1	SystemSettings
955	43	32212	2440	8.61	7900	1	ShellExperienceHost
659	28	15252	18564		3256	0	svchost
681	21	17228	13996		5528	0	SearchIndexer
758	34	15280	2800	0.94	10904	1	GameBar
811	43	13728	22472	55.84	5904	1	prl_cc
648	32	13336	12608	8.09	6956	1	RuntimeBroker
548	30	12292	10556		3208	0	svchost
1322	24	11676	19976		552	0	svchost
504	22	10560	12768		7776	0	svchost
590	25	8380	12208	3.05	8856	1	RuntimeBroker
1484	27	8128	12444		928	0	lsass
1206	18	8120	12040		1084	0	svchost
502	23	8020	16800	10.55	4608	1	svchost
573	21	7936	13208	15.91	8208	1	ctfmon
676	22	6936	19544	35.42	4460	1	sihost
518	25	6564	4092	1.45	6152	1	dllhost
883	20	5684	11664		1556	0	svchost
654	12	4960	6024		904	0	services
520	20	4832	6220	3.39	10324	1	svchost
895	18	2528	3824		3392	1	prl_tools
503	21	1924	2264		672	0	csrss
3395	0	68	10660		4	0	System

## Упражнения 5.3.и. Вывод выборочных полей

```
PS C:\tmp> Get-Process | Where-Object {$_.Handles -gt 500} | Sort-Object CPU -Descending | select processname, id, cpu, handles
```

ProcessName	Id	CPU	Handles
explorer	5196	388.109375	7450
PAD.Console.Host	4868	93.578125	1345
prl_cc	5904	57.203125	813
SearchHost	6424	45.890625	1555
sihost	4460	36.375	684
powershell_ise	7644	34.6875	772
StartMenuExperienceHost	6448	31.734375	940
msedge	3012	28.05625	1483
ctfmon	8208	15.953125	573
svchost	4608	10.59375	502
ShellExperienceHost	7900	8.609375	955
RuntimeBroker	6956	8.140625	646
svchost	10324	3.4375	520
RuntimeBroker	8856	3.125	590
WAAHost	9324	1.96875	1031
SystemSettings	2668	1.671875	1211
dllhost	6152	1.515625	519
GameBar	10904	0.9375	758
System	4		3497
svchost	7776		502
dwm	1208		1054
svchost	3256		661
svchost	3208		546
svchost	1556		887
svchost	1084		1235
svchost	552		1337
lsass	928		1491
MsMpEng	3232		876
services	904		679
SearchIndexer	5528		687
prl_tools	3392		915
csrss	672		535

## Добавил поле PM

```
PS C:\tmp> Get-Process | Where-Object {$_.Handles -gt 500} | Sort-Object CPU -Descending | select processname, id, cpu, pm, handles
```

ProcessName	: explorer
Id	: 5196
CPU	: 388.15625
PM	: 311697408
Handles	: 7332
ProcessName	: PAD.Console.Host
Id	: 4868
CPU	: 93.65625
PM	: 237789184
Handles	: 1353
ProcessName	: prl_cc
Id	: 5904
CPU	: 57.203125
PM	: 14106624
Handles	: 809
ProcessName	: SearchHost
Id	: 6424
CPU	: 45.890625
PM	: 166756352
Handles	: 1555
ProcessName	: sihost
Id	: 4460
CPU	: 36.375
PM	: 7159808
Handles	: 677
ProcessName	: powershell_ise
Id	: 7644
CPU	: 35.25
PM	: 156896128



## Добавил форматирование Format-Table -Autosize

```
PS C:\tmp> Get-Process | Where-Object {$_.Handles -gt 500} | Sort-Object CPU -Descending | Select-Object Processname, Id, CPU, PM, Handles | Format-Table -Autosize
```

ProcessName	Id	CPU	PM	Handles
explorer	5196	388,21875	311230464	7301
PAD.Console.Host	4868	93,765625	237756416	1358
prl_cc	5904	57,203125	14106624	809
SearchHost	6424	45,890625	166756352	1555
sihost	4460	36,375	7139328	677
powershell_ise	7644	35,921875	156479488	863
StartMenuExperienceHost	6448	31,734375	59850752	938
msedge	3012	28,671875	62545920	1477
ctfmon	8208	15,96875	8089600	573
svchost	4608	10,59375	8204288	502
ShellExperienceHost	7900	8,609375	32985088	955
RuntimeBroker	6956	8,140625	13656064	648
svchost	10324	3,4375	4947968	520
RuntimeBroker	8856	3,125	8581120	590
WNAHost	9324	1,96875	66121728	1031
SystemSettings	2668	1,671875	59297792	1211
dllhost	6152	1,515625	6721536	519
GameBar	10904	0,9375	15646720	758
System	4		73728	3402
svchost	7776		10768384	501
dwm	1208		146894848	1052
svchost	3256		19824640	661
svchost	3208		12591104	548
svchost	1556		5709824	882
svchost	1084		8278016	1199
svchost	552		12161024	1315
lsass	928		8392704	1474
MsMpEng	3232		308834304	873
services	904		5308416	668
SearchIndexer	5528		17805312	687
prl_tools	3392		2625536	913
csrss	672		1986560	515

## Упрощенная запись

```
PS C:\tmp> gps | where {$_.handles -gt 500} | sort cpu -desc | select processname, id, cpu, pm, handles | ft -a
```

ProcessName	Id	CPU	PM	Handles
explorer	5196	388,34375	311320576	7301
PAD.Console.Host	4868	93,796875	237793280	1370
prl_cc	5904	57,21875	14106624	809
SearchHost	6424	45,890625	166756352	1555
sihost	4460	36,375	7139328	676
powershell_ise	7644	36,28125	162955264	898
StartMenuExperienceHost	6448	31,734375	59850752	938
msedge	3012	28,671875	62513152	1481
ctfmon	8208	15,96875	8085504	573
svchost	4608	10,59375	8204288	502
ShellExperienceHost	7900	8,609375	32985088	955
RuntimeBroker	6956	8,140625	13656064	648
svchost	10324	3,4375	4947968	520
RuntimeBroker	8856	3,125	8581120	590
WNAHost	9324	1,96875	66121728	1031
SystemSettings	2668	1,671875	59297792	1211
dllhost	6152	1,515625	6721536	519
GameBar	10904	0,9375	15646720	758
SearchIndexer	5528		17805312	687
services	904		5308416	667
MsMpEng	3232		308838400	872
lsass	928		8392704	1465
svchost	552		12144640	1314
svchost	1084		8294400	1199
svchost	1556		5709824	882
svchost	3208		12591104	548
svchost	3256		19824640	661
dwm	1208		147054592	1052
System	4		73728	3402
prl_tools	3392		2654208	912
csrss	672		1986560	515

## Сохранение отчета

ProcessName	Id	CPU	PM	Handles
explorer	5196	388,375	309096448	7301
PAD.Console.Host	4868	93,84375	237764608	1369
prl_cc	5904	57,21875	14135296	809
SearchHost	6424	45,890625	166756352	1555
powershell_ise	7644	36,484375	166076416	943
sihost	4460	36,375	7106560	676
StartMenuExperienceHost	6448	31,734375	59850752	938
msedge	3012	28,671875	62513152	1477
ctfmon	8208	15,96875	8089600	573
svchost	4608	10,59375	8204288	502
ShellExperienceHost	7900	8,609375	32985088	955
RuntimeBroker	6956	8,140625	13656064	648
svchost	10324	3,4375	4947968	520
RuntimeBroker	8856	3,125	8511488	590
WNAHost	9324	1,96875	66121728	1031
SystemSettings	2668	1,671875	59297792	1211
dllhost	6152	1,515625	6721536	519
GameBar	10904	0,9375	15646720	758
SearchIndexer	5528		17645568	683
services	904		5079040	657

# Проверим факт, что файл создан

```
PS C:\tmp> gps | where {$_.handles -gt 500} | sort cpu -desc | select processname, id, cpu, pm, handles | ft -a > proc_04.txt
PS C:\tmp> ls

Каталог: C:\tmp

Mode                LastWriteTime         Length Name
----                -
d-----          07.04.2024   23:02             tmp2
-a-----          07.04.2024   23:45             572 cms.txt
-a-----          07.04.2024   23:45             635 d0.txt
-a-----          07.04.2024   23:45             589 d1.txt
-a-----          07.04.2024   23:45             592 d2.txt
-a-----          14.04.2024   16:06             103 gsp.ps1
-a-----          14.04.2024   13:53             20 helloworld.ps1
-a-----          14.04.2024   14:03          297688 lproc.htm
-a-----          14.04.2024   16:14          46426 pc_1.txt
-a-----          14.04.2024   16:34          3908 proc_04.txt
-a-----          07.04.2024   23:45             1182 resd.txt
-a-----          14.04.2024   13:52          14376 services_report.txt
-a-----          14.04.2024   13:17             208 t1.cmd
-a-----          07.04.2024   22:56             14 t1.txt
-a-----          07.04.2024   22:56             14 t2.txt
-a-----          07.04.2024   22:56             14 t3.txt
-a-----          07.04.2024   22:56             14 t4.txt

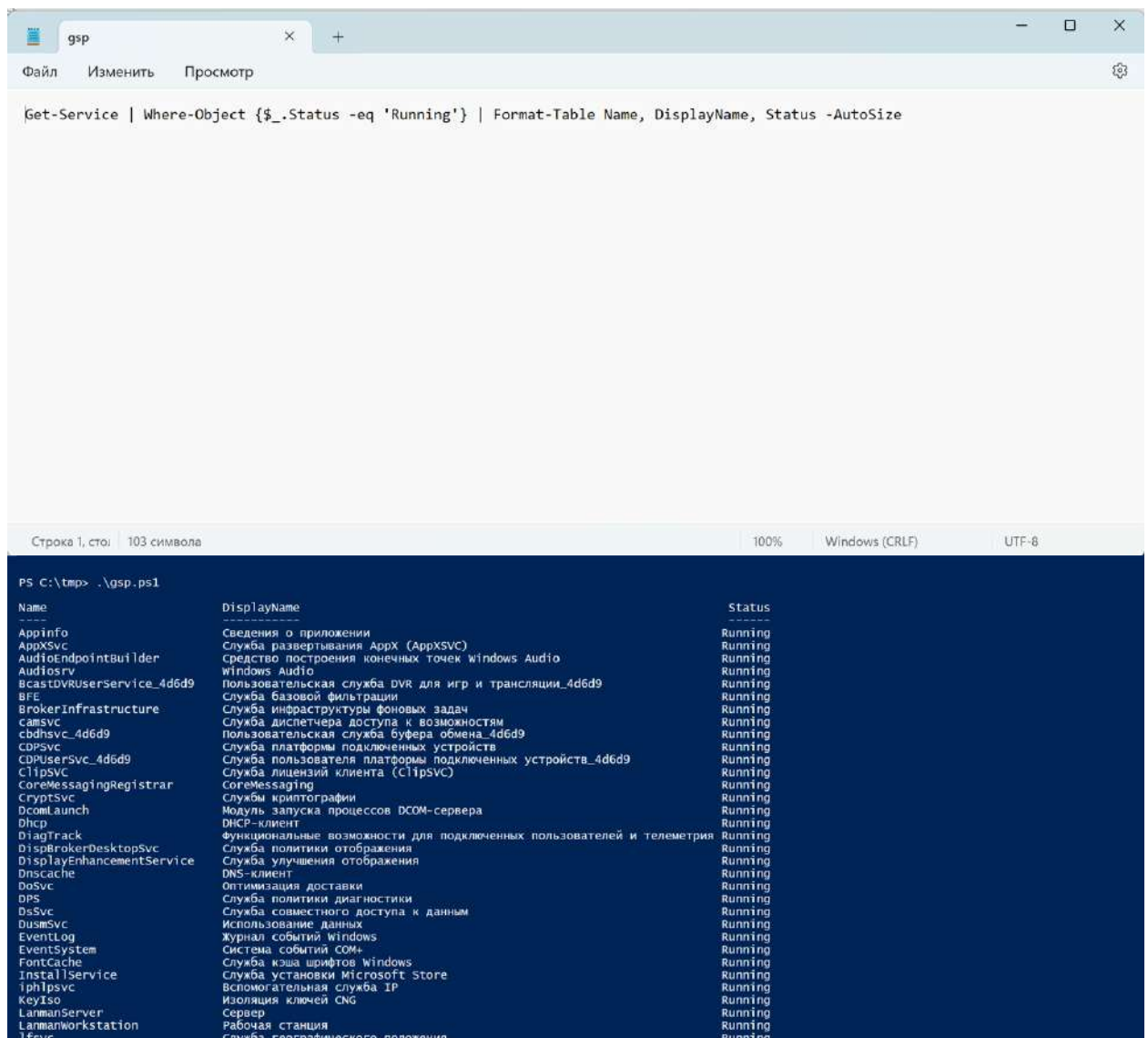
PS C:\tmp> cat proc_04.txt

ProcessName           Id      CPU      PM  Handles
-----
explorer               5196    388,375 309096448 7301
PAD.Console.Host      4868    93,84375 237764608 1369
prl_cc                 5904    57,21875 14135296 809
SearchHost            6424    45,890625 166756352 1555

PS C:\tmp> cat proc_04.txt

ProcessName           Id      CPU      PM  Handles
-----
explorer               5196    388,375 309096448 7301
PAD.Console.Host      4868    93,84375 237764608 1369
prl_cc                 5904    57,21875 14135296 809
SearchHost            6424    45,890625 166756352 1555
powershell_ise        7644    36,484375 166076416 943
sihost                4460    36,375 7106560 676
StartMenuExperienceHost 6448    31,734375 59850752 938
msedge                3012    28,671875 62513152 1477
cfmon                 8208    15,96875 8089600 573
svchost               4608    10,59375 8204288 502
ShellExperienceHost   7900    8,609375 32985088 955
RuntimeBroker         6956    8,140625 13656064 648
svchost               10324    3,4375 4947968 520
RuntimeBroker         8856    3,125 8511488 590
WUAHost               9324    1,96875 66121728 1031
SystemSettings        7668    1,671875 59297792 1211
dihost                6152    1,515625 6721536 519
GameBar               10904    0,9375 15646720 758
SearchIndexer         5528    17645568 683
services              904    5079040 657
MsMpEng               3232    308764672 872
lsass                 928    8392704 1464
svchost               552    11870208 1308
svchost               1084    8273920 1199
svchost               1556    5677056 879
svchost               3208    12591104 548
svchost               3256    19824640 661
dwm                  1208    146976768 1055
system                4    73728 3396
prl_tools              3392    2654208 912
csrss                 672    1986560 511
```

### Задание 5.3.1 (5.3.5.2.)



gsp

Файл Изменить Просмотр

```
Get-Service | Where-Object {$_.Status -eq 'Running'} | Format-Table Name, DisplayName, Status -AutoSize
```

Строка 1, столб 103 символа 100% Windows (CRLF) UTF-8

PS C:\tmp> .\gsp.ps1

Name	DisplayName	Status
Appinfo	Сведения о приложении	Running
AppXSvc	Служба развертывания AppX (AppXSVC)	Running
AudioEndpointBuilder	Средство построения конечных точек Windows Audio	Running
AudioSrv	Windows Audio	Running
BasicDVUserservice_4d6d9	Пользовательская служба DVR для игр и трансляции_4d6d9	Running
BFE	Служба базовой фильтрации	Running
BrokerInfrastructure	Служба инфраструктуры фоновых задач	Running
camsvc	Служба диспетчера доступа к возможностям	Running
cbdhsvc_4d6d9	Пользовательская служба буфера обмена_4d6d9	Running
CDPSvc	Служба платформы подключенных устройств	Running
CDPUserService_4d6d9	Служба пользователя платформы подключенных устройств_4d6d9	Running
CLIPsvc	Служба лицензий клиента (CLIPsvc)	Running
CoreMessagingRegistrar	CoreMessaging	Running
CryptSvc	Службы криптографии	Running
DcomLaunch	Модуль запуска процессов DCOM-сервера	Running
Dhcp	DHCP-клиент	Running
DiagTrack	Функциональные возможности для подключенных пользователей и телеметрия	Running
DispBrokerDesktopSvc	Служба политики отображения	Running
DisplayEnhancementService	Служба улучшения отображения	Running
Dnscache	DNS-клиент	Running
DoSvc	Оптимизация доставки	Running
DPS	Служба политики диагностики	Running
DsSvc	Служба совместного доступа к данным	Running
DusmSvc	Использование данных	Running
EventLog	Журнал событий Windows	Running
EventSystem	Система событий COM+	Running
FontCache	Служба кэша шрифтов Windows	Running
InstallService	Служба установки Microsoft Store	Running
Iphlpsvc	Вспомогательная служба IP	Running
KeyIso	Изоляция ключей CNG	Running
LanmanServer	Сервер	Running
LanmanWorkstation	Рабочая станция	Running
lfsvc	Служба географического положения	Running

Создал файл gsp.ps1

Ввел туда команду, которая показывает мне все запущенные службы

## Задание 5.3.2 (5.3.5.7.)

Задание выполняется вокруг службы gsv с учетом разных свойств вывода

# 1.Список запущенных служб, отсортированный по имени

## 1.1 Получаем список всех запущенных служб и сортируем их по имени

```
Get-Service | Where-Object {$_.Status -eq 'Running'} | Sort-Object Name | Select-Object Name, DisplayName, Status | Format-Table -AutoSize
```

## 1.2

```
PS C:\tmp> Get-Service | Where-Object {$_.Status -eq 'Running'} | Sort-Object Name | Select-Object Name, DisplayName, Status | Format-Table -AutoSize
```

Name	DisplayName	Status
AppInfo	Сведения о приложении	Running
AudioEndpointBuilder	средство построения конечных точек Windows Audio	Running
AudioSrv	Windows Audio	Running
BcastDVRUserService_4d6d9	Пользовательская служба DVR для игр и трансляции_4d6d9	Running
BFE	Служба базовой фильтрации	Running
BrokerInfrastructure	Служба инфраструктуры фоновых задач	Running
camsvc	Служба диспетчера доступа к возможностям	Running
cbdhsvc_4d6d9	Пользовательская служба буфера обмена_4d6d9	Running
CDPSvc	Служба платформы подключенных устройств	Running
CDUsersvc_4d6d9	Служба пользователя платформы подключенных устройств_4d6d9	Running
CoreMessagingRegistrar	CoreMessaging	Running
CryptSvc	Служба криптографии	Running
DcomLaunch	Модуль запуска процессов DCOM-сервера	Running
Dhcp	DHCP-клиент	Running
DiagTrack	Функциональные возможности для подключенных пользователей и телеметрия	Running
DispBrokerDesktopSvc	Служба политики отображения	Running
DisplayEnhancementService	Служба улучшения отображения	Running
Dnscache	DNS-клиент	Running
DsSvc	Оптимизация доставки	Running
DPS	Служба политики диагностики	Running
DsSvc	Служба совместного доступа к данным	Running
DusmSvc	Использование данных	Running
EventLog	Журнал событий Windows	Running
EventSystem	Система событий COM+	Running
FontCache	Служба кэша шрифтов Windows	Running
gpsvc	Клиент групповой политики	Running
InstallService	Служба установки Microsoft Store	Running
iphlpvc	Вспомогательная служба IP	Running
KeyIso	Изоляция ключей CNG	Running
LanmanServer	Сервер	Running
LanmanWorkstation	Рабочая станция	Running
Tfsvc	Служба географического положения	Running
LicenseManager	Служба Windows License Manager	Running
Tlshosts	Модуль поддержки NetBIOS через TCP/IP	Running

## 1.3

Комментарий:

- Get-Service извлекает список всех служб.
- Where-Object {\$\_.Status -eq 'Running'} фильтрует службы, оставляя только те, которые в данный момент запущены.
- Sort-Object Name сортирует отфильтрованные службы по имени.
- Select-Object Name, DisplayName, Status выбирает только поля имени, отображаемого имени и статуса для отображения.
- Format-Table -AutoSize выводит результаты в виде таблицы с автоматически подбираемой шириной столбцов.

## 2.Список запущенных служб с фильтрацией по специфическому статусу и имени

2.1 Получаем список запущенных служб, которые начинаются на букву 'A' и отображаем только их имя и статус

```
Get-Service | Where-Object {$_.Status -eq 'Running' -and $_.Name -like 'A*'} |  
Select-Object Name, Status | Format-Table -AutoSize
```

### 2.2

```
PS C:\tmp> Get-Service | Where-Object {$_.Status -eq 'Running' -and $_.Name -like 'A*'} | Select-Object Name, Status | Format-Table -AutoSize
```

Name	Status
Appinfo	Running
AudioEndpointBuilder	Running
AudioSrv	Running

```
PS C:\tmp>
```

### 2.3

Комментарий:

- Where-Object {\$\_.Status -eq 'Running' -and \$\_.Name -like 'A\*'} фильтрует службы по статусу "Running" и тем, чье имя начинается на 'A'.
- Select-Object Name, Status ограничивает вывод только именем службы и их статусом.
- Format-Table -AutoSize форматирует вывод в таблицу, подстраивая ширину колонок под содержимое.



## 3. Службы с определенным типом запуска

### 3.1

Фильтруем службы по типу запуска 'Automatic' и отображаем их имя и тип запуска

```
Get-Service | Where-Object {$_.Status -eq 'Running' -and $_.StartType -eq 'Automatic'} | Select-Object Name, StartType, Status | Format-Table -AutoSize
```

### 3.2

```
PS C:\tmp> Get-Service | Where-Object {$_.Status -eq 'Running' -and $_.StartType -eq 'Automatic'} | Select-Object Name, StartType, Status | Format-Table -AutoSize
```

Name	StartType	Status
AudioEndpointBuilder	Automatic	Running
AudioSrv	Automatic	Running
BFE	Automatic	Running
BrokerInfrastructure	Automatic	Running
cbdhsvc_4d6d9	Automatic	Running
CDPSvc	Automatic	Running
CDPUsersSvc_4d6d9	Automatic	Running
CoreMessagingRegistrar	Automatic	Running
CryptSvc	Automatic	Running
DcomLaunch	Automatic	Running
Dhcp	Automatic	Running
DiagTrack	Automatic	Running
DispBrokerDesktopSvc	Automatic	Running
Dnscache	Automatic	Running
Dosvc	Automatic	Running
DPS	Automatic	Running
DismSvc	Automatic	Running
EventLog	Automatic	Running
EventSystem	Automatic	Running
FontCache	Automatic	Running
gpsvc	Automatic	Running
IpHlpSvc	Automatic	Running
LanmanServer	Automatic	Running
LanmanWorkstation	Automatic	Running
LSM	Automatic	Running
mpssvc	Automatic	Running
nsi	Automatic	Running
OnesyncSvc_4d6d9	Automatic	Running
Parallels Coherence Service	Automatic	Running
Parallels Tools Service	Automatic	Running
Peasvc	Automatic	Running
Power	Automatic	Running
ProfSvc	Automatic	Running
RpcEptMapper	Automatic	Running
RpcSs	Automatic	Running

### 3.3

Комментарий:

- Where-Object {\$\_.Status -eq 'Running' -and \$\_.StartType -eq 'Automatic'} фильтрует службы, которые запущены и имеют автоматический тип запуска.
- Select-Object Name, StartType, Status выводит имя, тип запуска и статус каждой отфильтрованной службы.
- Этот запрос полезен для быстрой проверки автоматически запускаемых служб, чтобы убедиться в их надежной работе.

## 4. Службы, отсортированные по потреблению памяти

### 4.1

Получаем список всех запущенных служб и сортируем их по потреблению памяти в порядке убывания

# Получаем список всех запущенных служб

```
Get-Service | Where-Object {$_.Status -eq 'Running'} |
```

```
ForEach-Object {
```

```
    # Для каждой службы пытаемся найти процесс с таким же именем
```

```
    $process = Get-Process -Name $_.Name -ErrorAction SilentlyContinue
```

```
    if ($process) {
```

```
        # Если процесс найден, добавляем информацию о потреблении памяти
```

```
        $_ | Select-Object Name, DisplayName, Status, @{Name='MemoryUsage';
```

```
Expression={$process.WorkingSet}}
```

```
    }
```

```
} | Sort-Object MemoryUsage -Descending | Select-Object -First 15 Name,
```

```
DisplayName, MemoryUsage | Format-Table -AutoSize
```

### 4.2

```
PS C:\tmp> # Получаем список всех запущенных служб
Get-Service | Where-Object {$_.Status -eq 'Running'} |
ForEach-Object {
    # Для каждой службы пытаемся найти процесс с таким же именем
    $process = Get-Process -Name $_.Name -ErrorAction SilentlyContinue
    if ($process) {
        # Если процесс найден, добавляем информацию о потреблении памяти
        $_ | Select-Object Name, DisplayName, Status, @{Name='MemoryUsage'; Expression={$process.WorkingSet}}
    }
} | Sort-Object MemoryUsage -Descending | Select-Object -First 15 Name, DisplayName, MemoryUsage | Format-Table -AutoSize
```

Name	DisplayName	MemoryUsage
SecurityHealthService	Служба "Безопасность windows"	9175040
vds	Виртуальный диск	3239936

```
PS C:\tmp> |
```

### 4.3

Комментарий:

Решил немного расширить знания и сделать скрипт, который я буду использовать каждый день, для анализа потребления памяти

- `ForEach-Object {Get-Process -Id $_.Id}` для каждой запущенной службы получает соответствующий процесс, чтобы можно было увидеть потребление памяти.
- `Sort-Object WorkingSet -Descending` сортирует процессы по объему используемой памяти (`WorkingSet`) в порядке убывания.
- `Select-Object -First 15 Name, WorkingSet, Id` выбирает первые 15 записей после сортировки, отображая имя, объем используемой памяти и ID процесса.

Вывод по работе:

Мы изучили среду CMD: научились запускать и использовать в различных сценариях, управлять файлами, пользоваться полезными утилитами.

CMD помогает нам:

3. Управление файлами и папками, что включает создание, редактирование и удаление файлов и директорий.
4. Использование командной строки (CLI) для выполнения различных утилит и написание простых скриптов для автоматизации задач.
5. Получение информации о конфигурации и текущем состоянии компьютеров в сети, что позволяет облегчить их администрирование и мониторинг.
6. Настройка расширенной пользовательской среды в операционной системе, что включает настройку рабочего окружения, переменных среды и других параметров системы.
7. Создание настроек пользовательской среды, которые активируются при входе в систему, обеспечивая удобство и персонализацию работы пользователя.

Также изучили инструмент автоматизации Power Shell и Power Shell ISE

1. Мы узнали, как использовать основные команды PowerShell, такие как Get-Service для извлечения информации о службах и Get-Process для получения данных о процессах. Это знание помогает понять, как управлять и мониторить системные процессы через мощный интерфейс командной строки.
2. Мы изучили, как применять фильтры с помощью Where-Object для выборки данных по определенным критериям (например, по статусу службы или её свойствам). Также вы научились использовать Sort-Object для сортировки данных по нужным параметрам, что критически важно для организации больших объемов информации.
3. Мы поняли, как выбирать специфические свойства объектов с помощью Select-Object, что позволяет упростить вывод и сделать его более читаемым. Это включает в себя выборку только необходимых колонок данных из всего массива информации.
4. На примерах мы увидели, как можно комбинировать различные команды и фильтры для выполнения конкретных задач, таких как отображение топа служб по использованию памяти или фильтрация служб по типу запуска.

Эти знания позволяют мне глубже понять и эффективно использовать PowerShell для администрирования и автоматизации задач в Windows, делая мою работу более продуктивной и менее подверженной ошибкам.