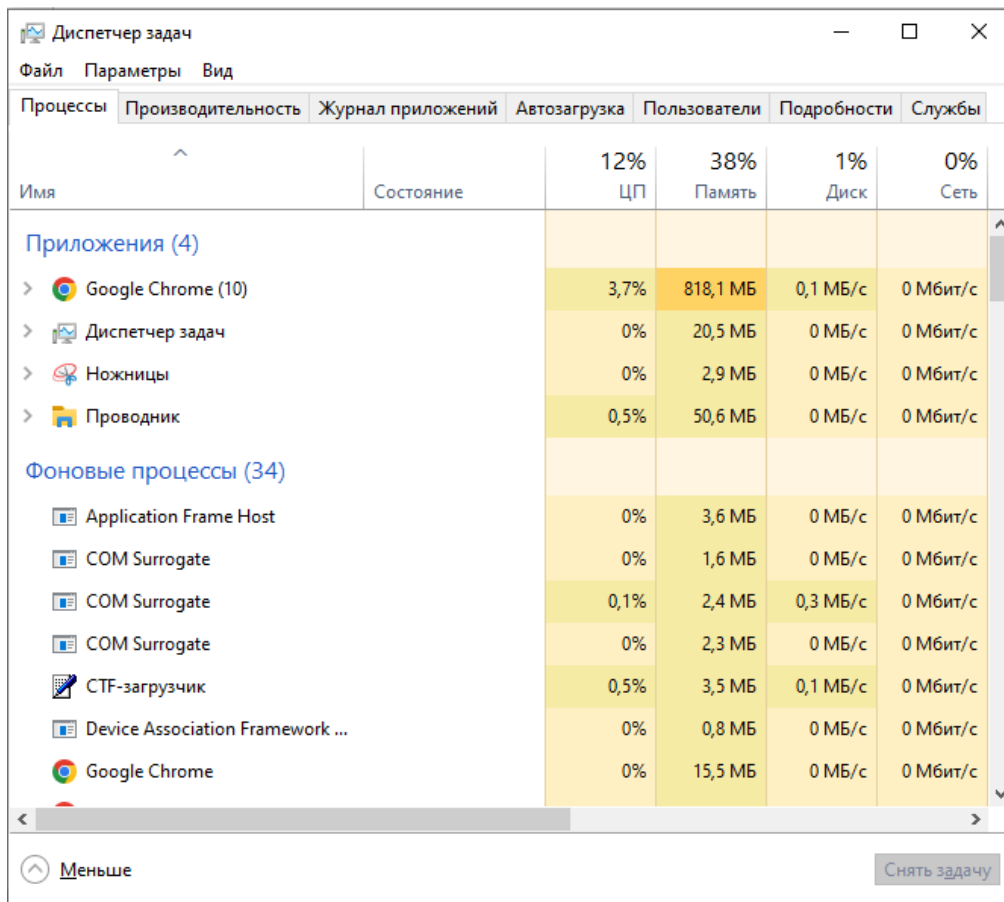


Практическая работа

По теме: “Исследование процессов и потребления ресурсов в Windows”

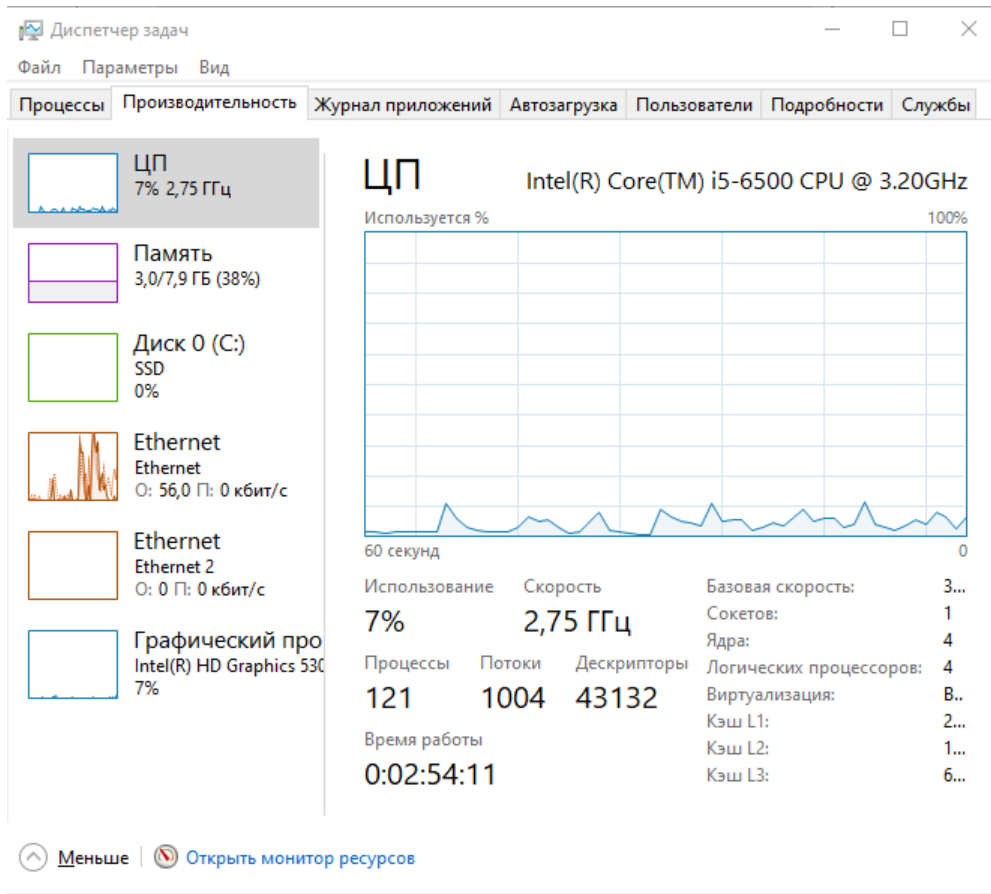
Задача 1: Базовый анализ с помощью графического интерфейса (Диспетчер задач).

1. Открыл диспетчер задач с помощью комбинации *Ctrl + Shift + Esc*.



Имя	Состояние	12% ЦП	38% Память	1% Диск	0% Сеть
Приложения (4)					
> Google Chrome (10)		3,7%	818,1 МБ	0,1 МБ/с	0 Мбит/с
> Диспетчер задач		0%	20,5 МБ	0 МБ/с	0 Мбит/с
> Ножницы		0%	2,9 МБ	0 МБ/с	0 Мбит/с
> Проводник		0,5%	50,6 МБ	0 МБ/с	0 Мбит/с
Фоновые процессы (34)					
Application Frame Host		0%	3,6 МБ	0 МБ/с	0 Мбит/с
COM Surrogate		0%	1,6 МБ	0 МБ/с	0 Мбит/с
COM Surrogate		0,1%	2,4 МБ	0,3 МБ/с	0 Мбит/с
COM Surrogate		0%	2,3 МБ	0 МБ/с	0 Мбит/с
CTF-загрузчик		0,5%	3,5 МБ	0,1 МБ/с	0 Мбит/с
Device Association Framework ...		0%	0,8 МБ	0 МБ/с	0 Мбит/с
Google Chrome		0%	15,5 МБ	0 МБ/с	0 Мбит/с

2. Открыл “Производительность” и изучил вкладки: “ЦП”, “Память”, “Диск”, “Сеть”.



3. После того как я оценил загрузку системы я пришел к выводу что компьютер работает стабильно без перегрузок.

Задача 2: Углубленный анализ с помощью PowerShell.

1. Запустил PowerShell через поисковую строку.
2. Выполнил команды для анализа *Get-Process | Sort-Object CPU -Descending | Select-Object -First 5 -Property Name, CPU, Id, WorkingSet*.

```
Администратор: Windows PowerShell
Windows PowerShell
(C) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

Попробуйте новую кроссплатформенную оболочку PowerShell (https://aka.ms/pscore6)

PS C:\Users\Администратор> Get-Process | Sort-Object CPU -Descending | Select-Object -First 5 -Property Name, CPU, Id, WorkingSet
>>

Name          CPU      Id WorkingSet
-----
dwm           509,375 1272 121782272
chrome       316,390625 3184 292409344
chrome        145,875 1948 403419136
chrome       109,78125 3952 225927168
svchost       94,921875 2744 16388096

PS C:\Users\Администратор>
```

Потом ввел команду *Get-Process | Sort-Object WorkingSet -Descending | Select-Object -First 5 -Property Name, CPU, Id, WorkingSet*.

```
PS C:\Users\Администратор> Get-Process | Sort-Object WorkingSet -Descending | Select-Object -First 5 -Property Name, CPU, Id, WorkingSet
>>

Name          CPU      Id WorkingSet
-----
chrome       170,03125 1948 414814208
chrome        337,75 3184 273866752
SearchApp     9,84375 5928 238456832
chrome       112,296875 3952 224432128
chrome        35,28125 6184 180944896

PS C:\Users\Администратор>
```

Потом ввел команду *Get-Counter '\Process(*)\% Processor Time' | Select-Object -ExpandProperty CounterSamples | Sort-Object CookedValue -Descending | Select-Object -First 5 InstanceName, CookedValue*.

```
PS C:\Users\Администратор> Get-WmiObject Win32_PerfFormattedData_PerfProc_Process |
>> Sort-Object -Property PercentProcessorTime -Descending |
>> Select-Object -First 5 Name, IDProcess, PercentProcessorTime
>>

Name          IDProcess PercentProcessorTime
-----
_Total         0             397
Idle           0             391
WmiPrvSE#2     6496           5
svchost#25     2552           0
svchost#26     2620           0

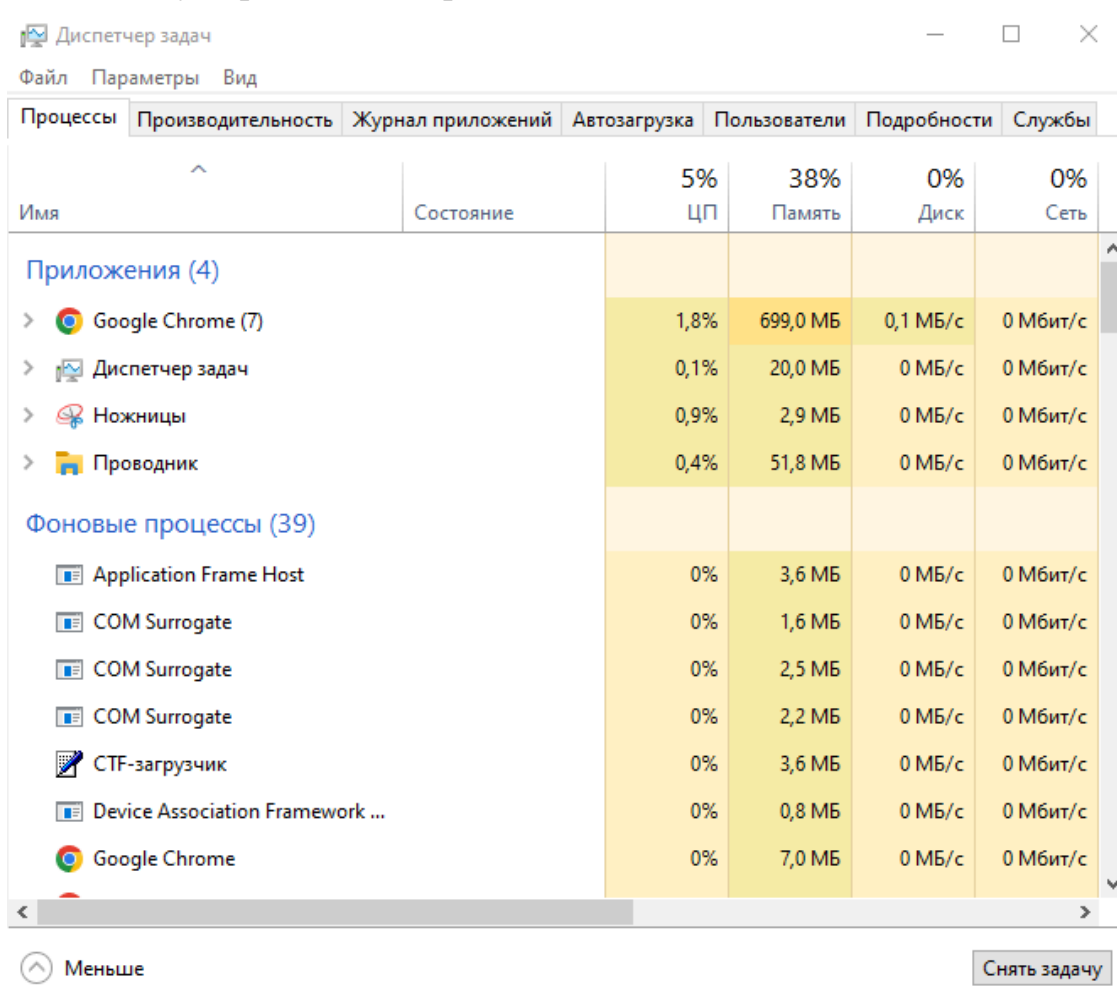
PS C:\Users\Администратор>
```

Задача 3: Управление процессами.

1. Запустил программу “Блокнот”



2. Снял задачу через диспетчер задач



Задача 4: Создание сценария базового мониторинга

1. Создал файл monitor.bat со следующими командами:

```
bat
```

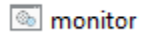
```
@echo off
```

```
echo %date% %time% >> log_processes.txt
```

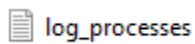
```
tasklist /fo table /v >> log_processes.txt
```

```
echo ===== >> log_processes.txt
```

```
pause
```



2. Запустил скрипт и появился файл под названием “log_processes.txt”



log_processes – Блокнот

Файл Правка Формат Вид Справка

24.09.2025 14:13:39,16

Имя	PID	Имя службы	Имя процесса	Состояние	Имя пользователя
System Idle Process	0	Services	System	Unknown	NT AUTHORITY\SYSTEM
System	4	Services	Registry	Unknown	NT AUTHORITY\SYSTEM
Registry	108	Services	smss.exe	Unknown	NT AUTHORITY\SYSTEM
smss.exe	412	Services	csrss.exe	Unknown	NT AUTHORITY\SYSTEM
csrss.exe	612	Services	wininit.exe	Unknown	NT AUTHORITY\SYSTEM
wininit.exe	700	Services	csrss.exe	Running	NT AUTHORITY\SYSTEM
csrss.exe	708	Console	winlogon.exe	Unknown	NT AUTHORITY\SYSTEM
winlogon.exe	804	Console	services.exe	Unknown	NT AUTHORITY\SYSTEM
services.exe	824	Services	lsass.exe	Unknown	NT AUTHORITY\SYSTEM
lsass.exe	856	Services	svchost.exe	Unknown	NT AUTHORITY\SYSTEM
svchost.exe	984	Services	fontdrvhost.exe	Unknown	Font Driver Host\UMFD-0
fontdrvhost.exe	1012	Services	fontdrvhost.exe	Unknown	Font Driver Host\UMFD-1
fontdrvhost.exe	1016	Console	svchost.exe	Unknown	NT AUTHORITY\NETWORK SERVICE
svchost.exe	944	Services	svchost.exe	Unknown	NT AUTHORITY\SYSTEM
svchost.exe	1036	Services	svchost.exe	Unknown	NT AUTHORITY\SYSTEM
svchost.exe	1156	Services	svchost.exe	Unknown	NT AUTHORITY\LOCAL SERVICE
svchost.exe	1164	Services	IntelCpHDCPSvc.exe	Unknown	NT AUTHORITY\SYSTEM
IntelCpHDCPSvc.exe	1252	Services			

Стр 1, столб 1 100% Windows (CRLF) ANSI