

21.01.2024

Курс:

Практическая работа к уроку № Lesson_2

--

Основные инструменты администрирования Windows

Задание:

1. Создайте нового пользователя, с необходимостью смены пароля при первом входе в систему и добавьте его в группу Пользователи удаленного рабочего стола
2. Остановите и запустите службу Sstp (SstpSvc) из графической оболочки и из командной строки
3. Сожмите том, создайте раздел, потом верните в исходное состояние
4. Подключите второй диск, преобразуйте его в GPT
5. Добавьте третий диск, создайте из 2 и 3 диска зеркальный том
6. Найдите ИД оборудования (`pci\ven` , например, контроллер жесткого диска или видеокарта) и сайт в интернете, откуда можно скачать драйвера для этого устройства
7. В диспетчере задач отфильтруйте приложения которые больше всего потребляют ресурсов процессора и оперативную память
8. Отфильтруйте системные события с кодом 6013 или 7036
9. Создайте задание, которое будет в 14.00 в рабочие дни запускать команду `ping 8.8.8.8`
10. Промониторьте через Системный монитор загрузку процессора и пришлите лог
11. Через Монитор ресурсов просмотрите в разделе Диск-Процессы с дисковой активностью-System какие используются файлы

Команды

```
Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled False  
(отключение Firewall через Powershell)
```

```
winrm quickconfig
```

```
Set-Item WSMan:\localhost\Client\TrustedHosts -Value 'w2019gui01'
```

```
Enter-PSSession -ComputerName w2019core01
```

Задание_1:

Создайте нового пользователя, с необходимостью смены пароля при первом входе в систему и добавьте его в группу Пользователи удаленного рабочего стола

```
C:\Users\Администратор>whoami  
w2019gui01\администратор
```

Управление компьютером

Диспетчер серверов

Панель мониторинга

Вас приветствует диспетчер серверов

- 1 Настроить этот локальный сервер
- 2 Добавить роли и компоненты
- 3 Добавить другие серверы для управлен
- 4 Создать группу серверов
- 5 Подключить этот сервер к облачным слу

Быстрый запуск

Что нового

Подробнее

РОЛИ И ГРУППЫ СЕРВЕРОВ

Роли: 1 | Группы серверов: 1 | Всего серверов: 1

1

Выполнить

Введите имя программы, папки, документа или ресурса Интернета, которые требуется открыть.

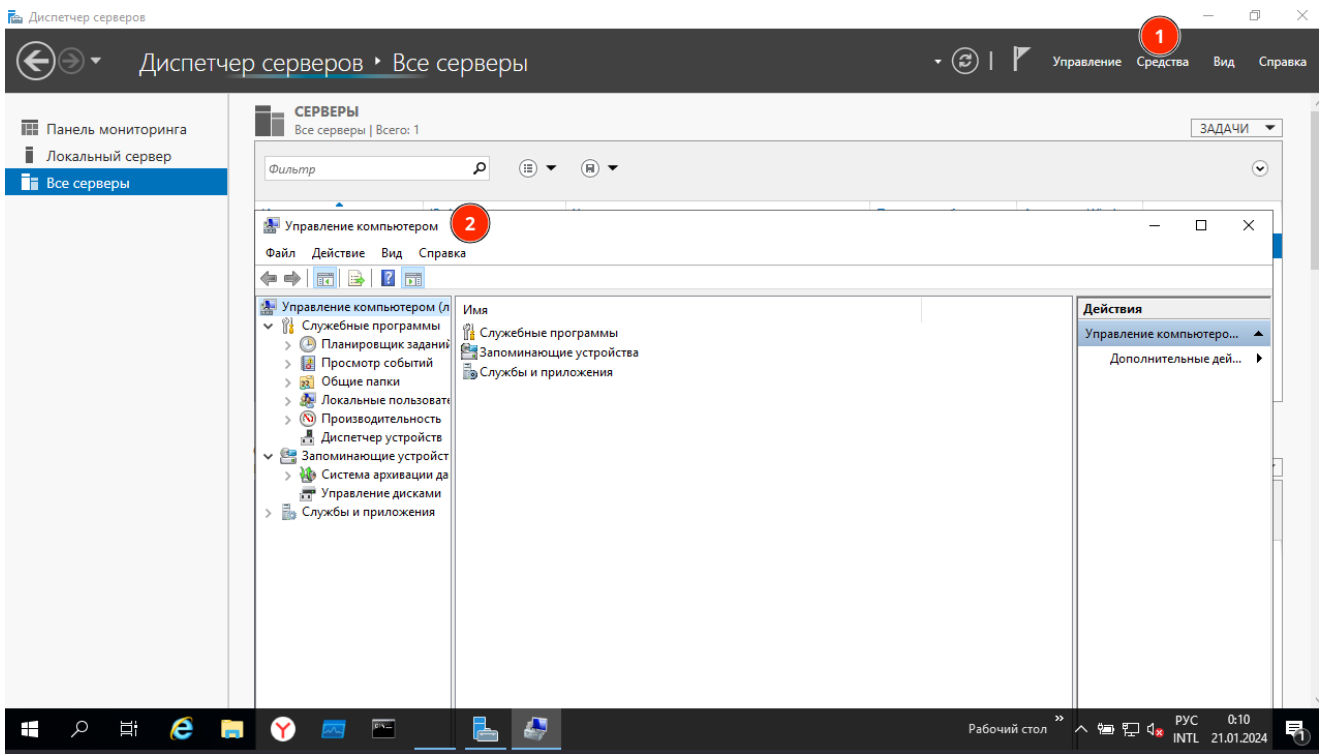
Открыть:

Это задание будет создано с правами администратора

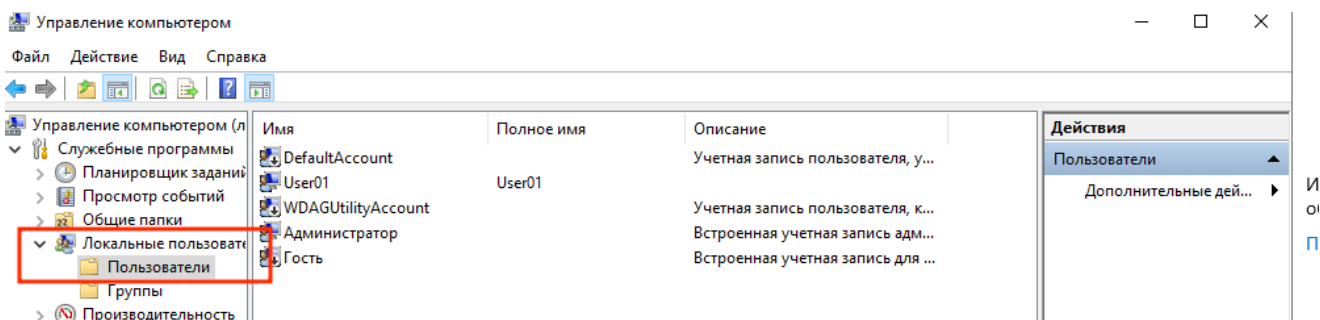
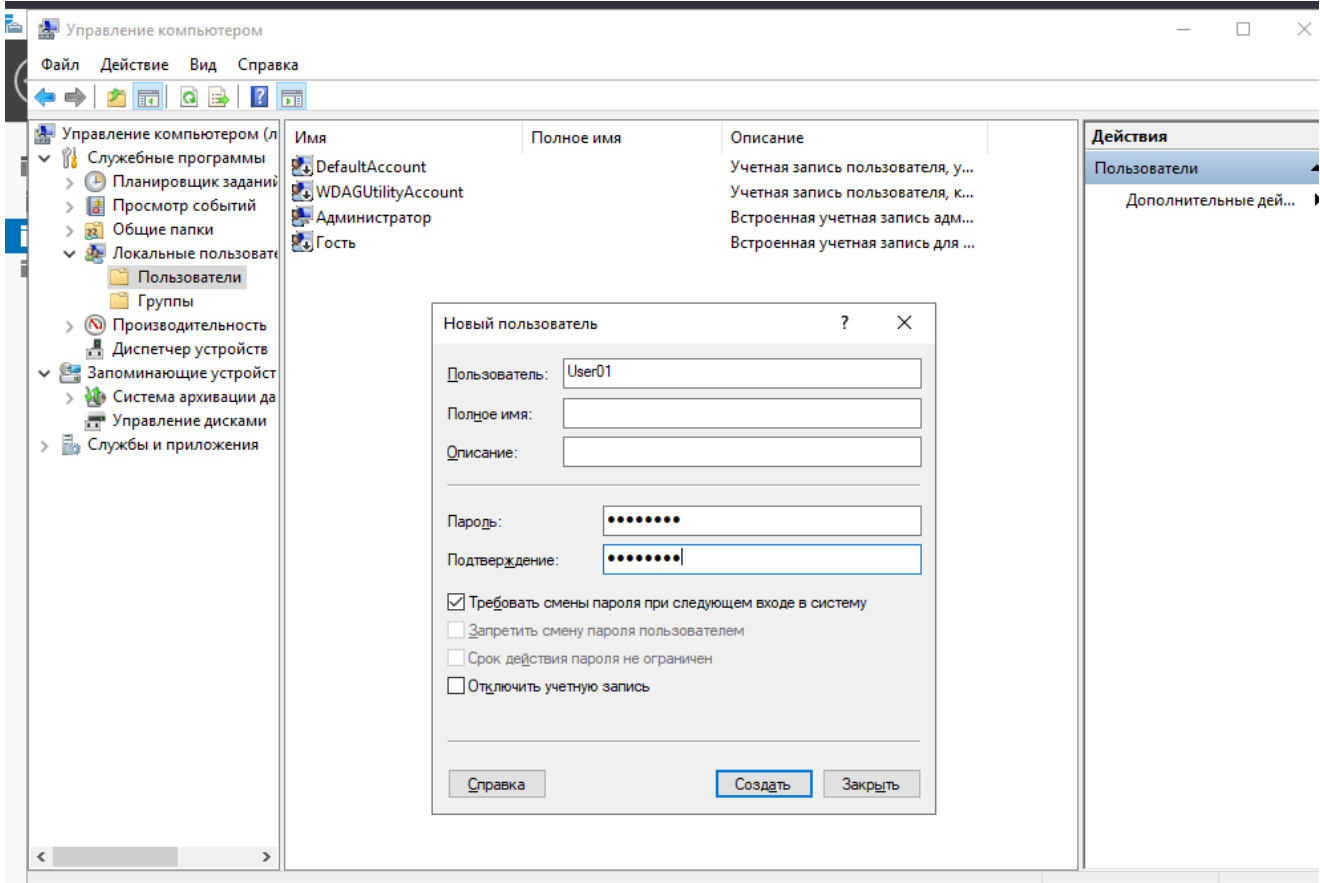
ОК Отмена Обзор...

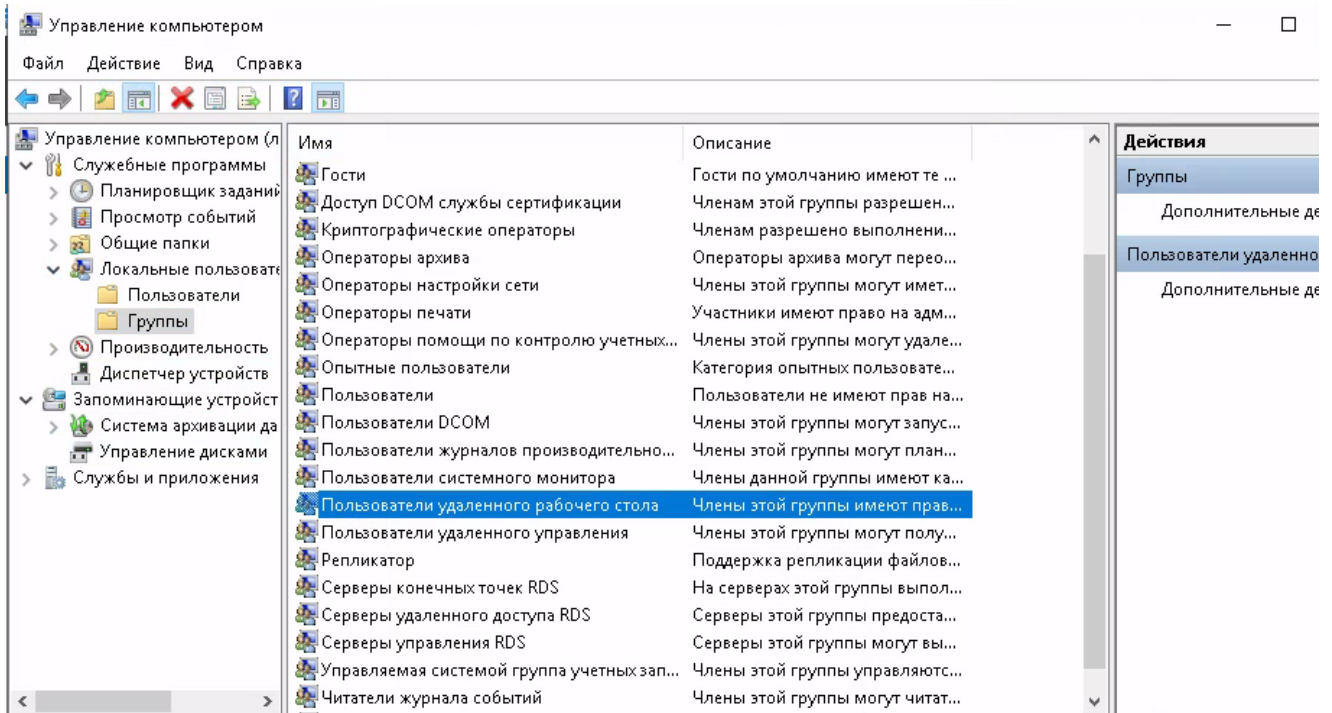
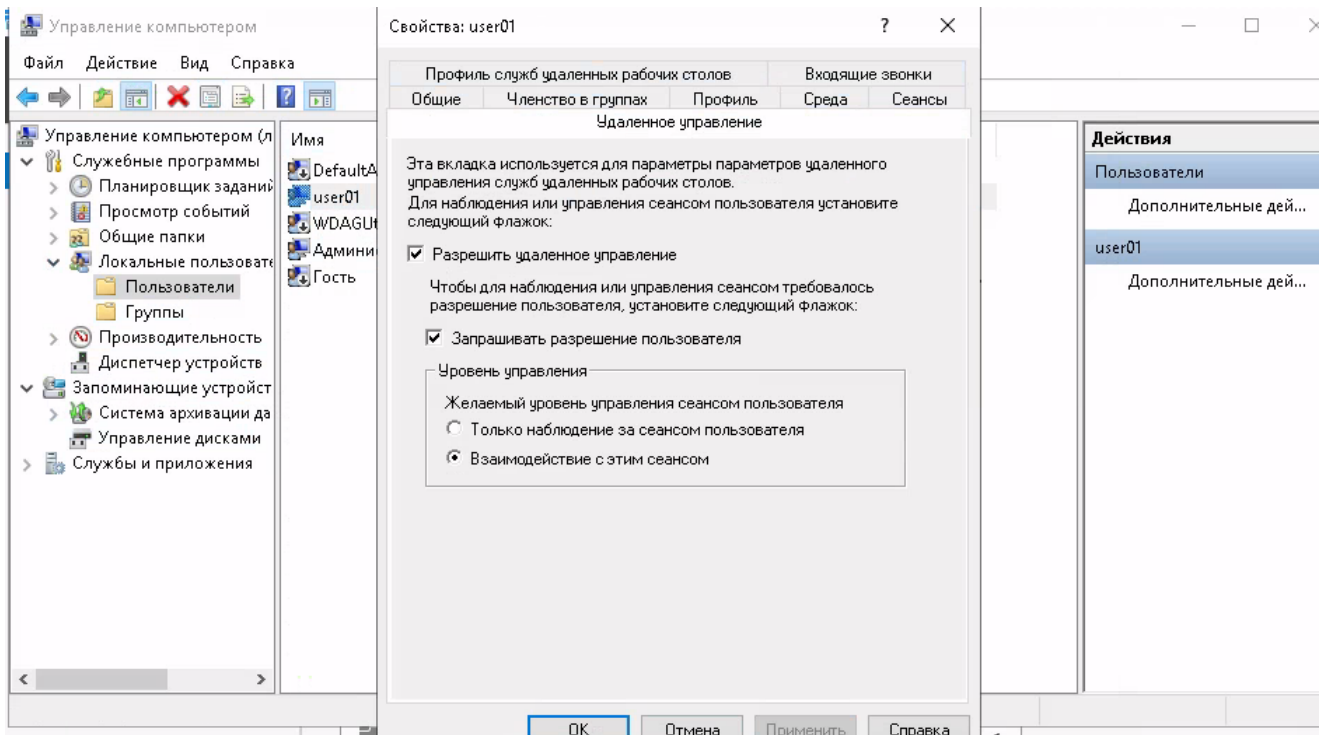
Локальный сервер 1

- Управляемость
- 1 События
- Службы
- Производительность
- Результаты ВРА



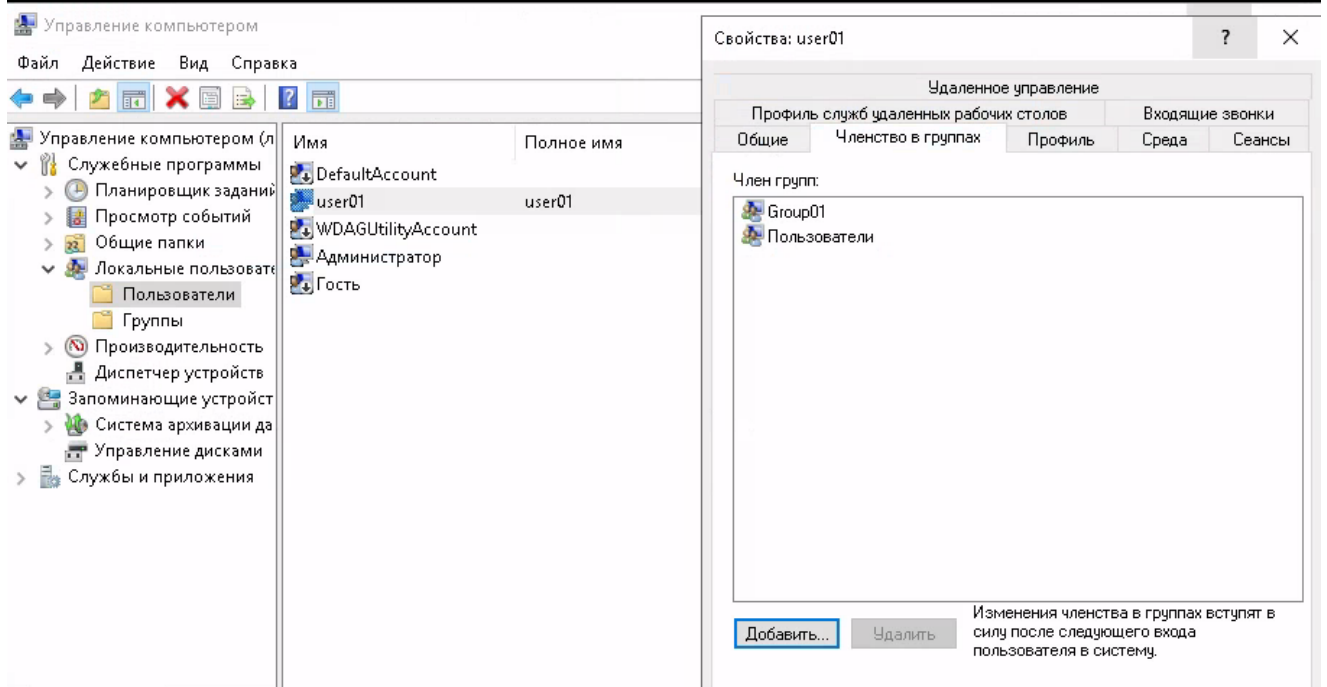
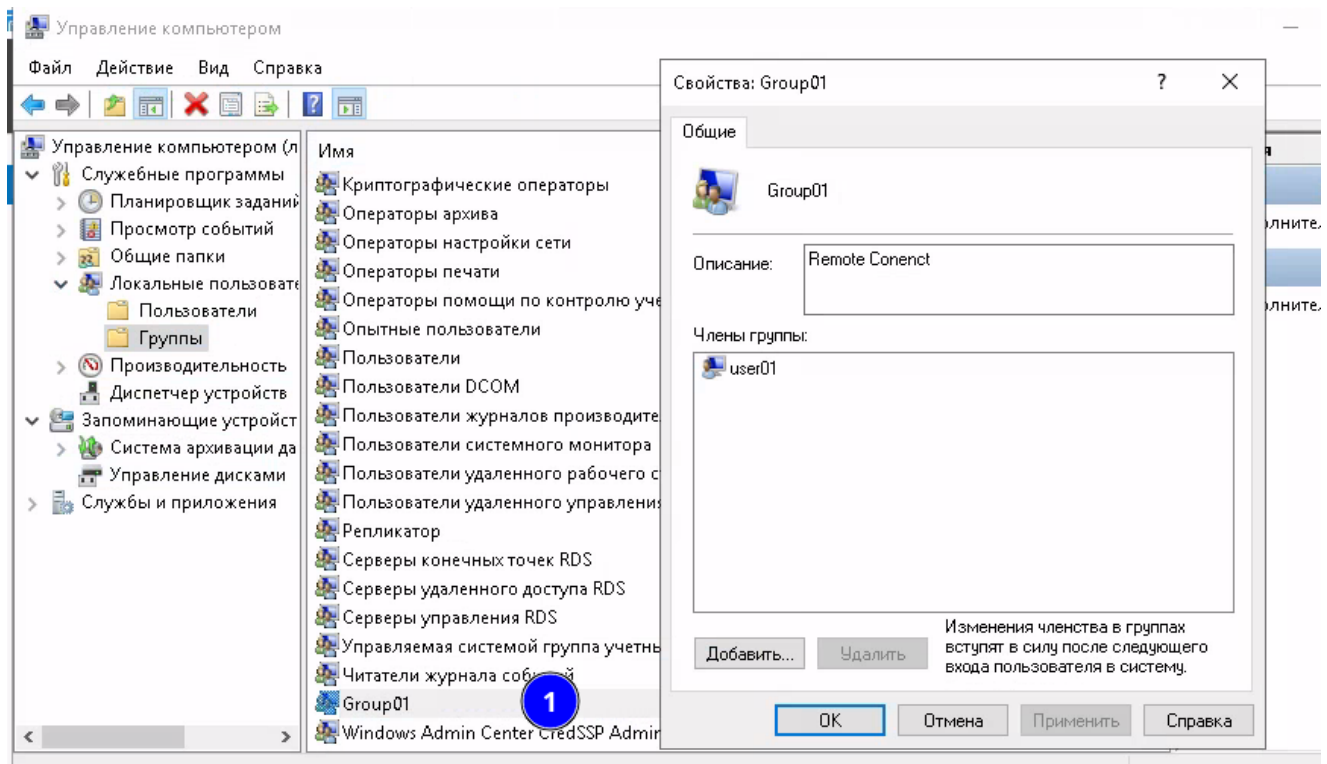
Добавим пользователя через Управление компьютером user01 с паролем Pa\$\$word

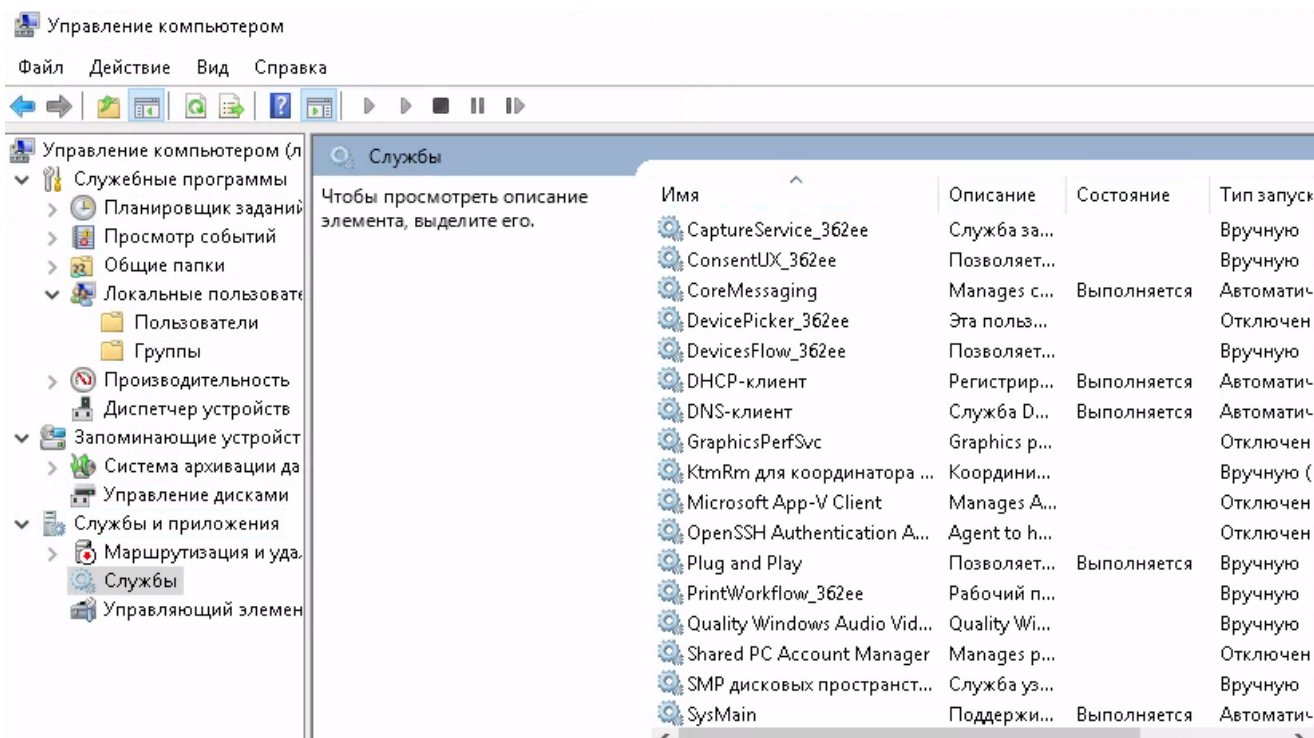




Создадим новую группу



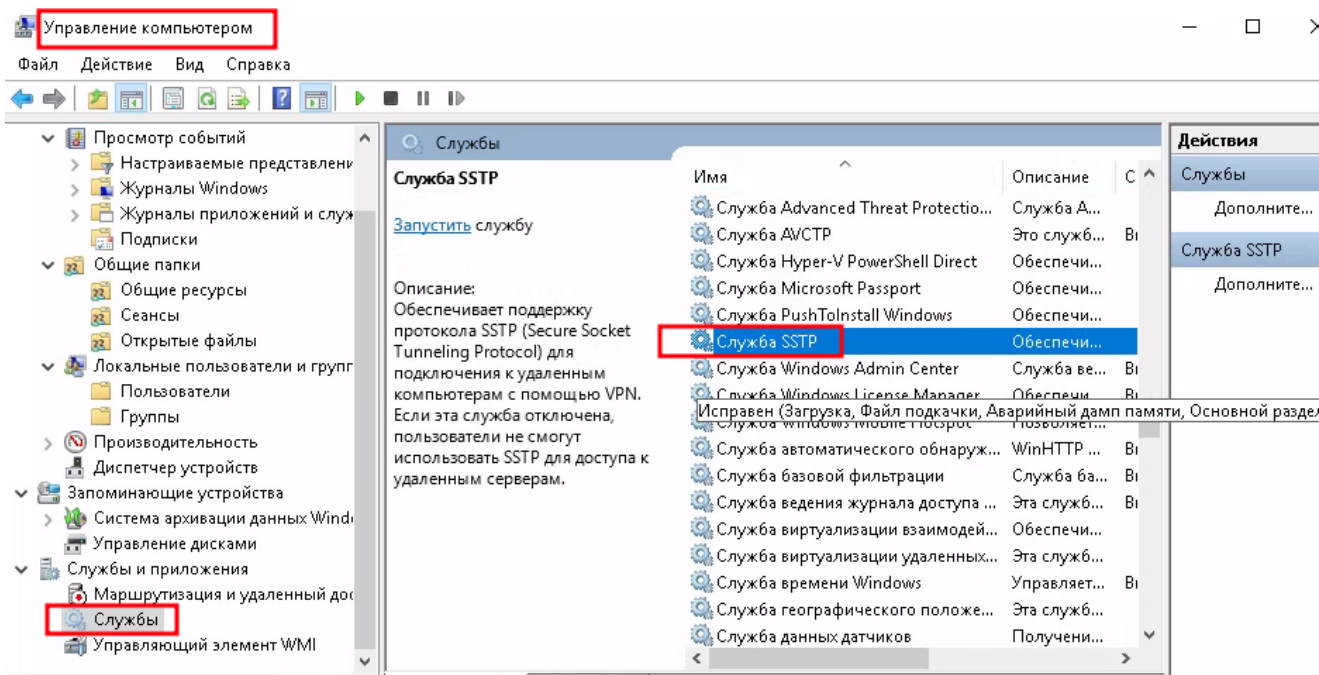


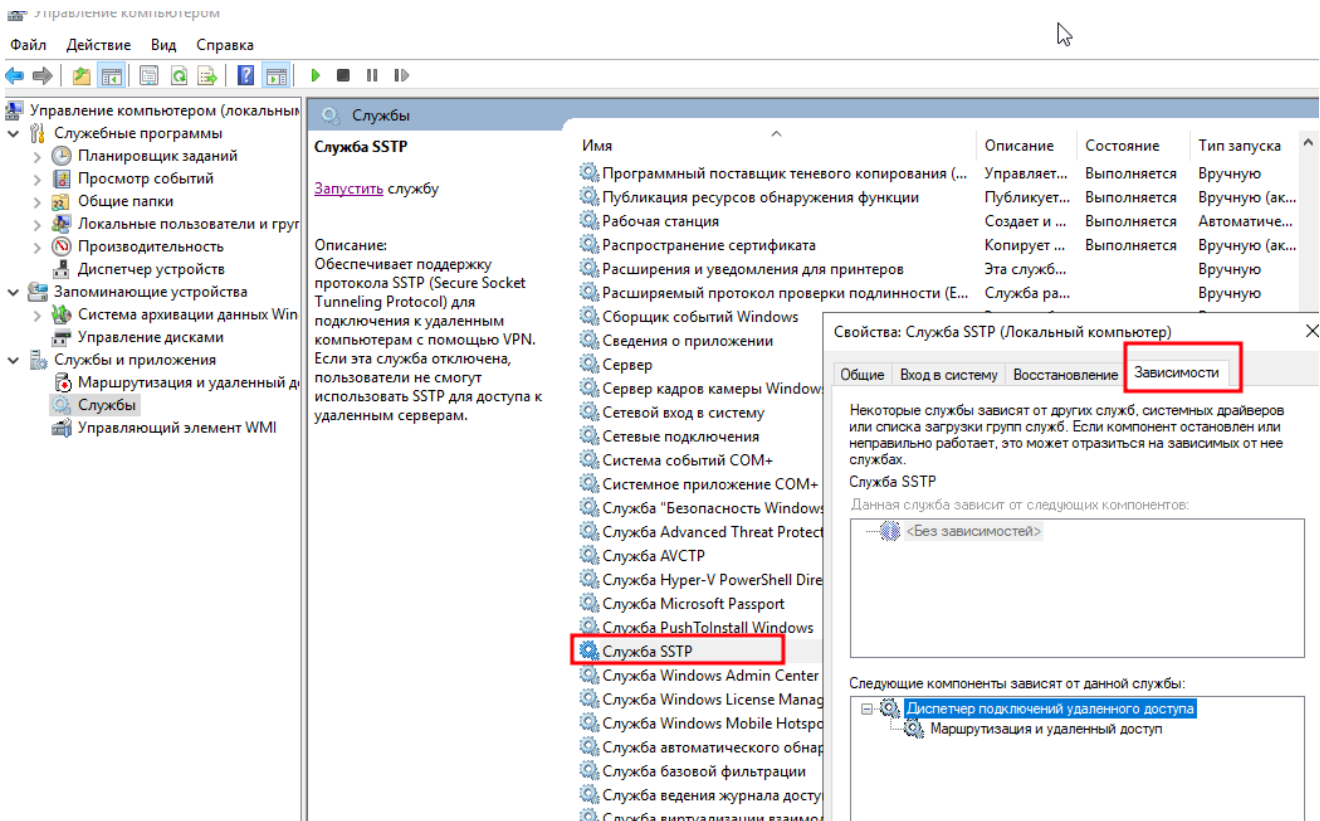
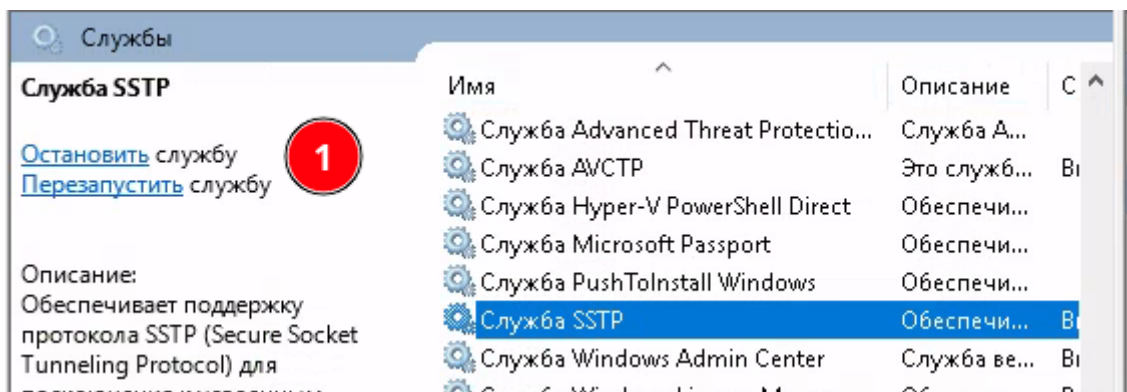


```
net localgroup "Remote Desktop Users" /add user01
```

Задание_2:

Остановите и запустите службу SSTP (SstpSvc) из графической оболочки и из командной строки





```
PS C:\Users\Администратор> Get-Service sstpsvc
```

Status	Name	DisplayName
Running	sstpsvc	Служба SSTP

Get-Command -noun Service

```
PS C:\Users\Администратор> Get-Command -noun Service
```

CommandType	Name	Version	Source
Cmdlet	Get-Service	3.1.0.0	Microsoft.PowerShell...
Cmdlet	New-Service	3.1.0.0	Microsoft.PowerShell...
Cmdlet	Restart-Service	3.1.0.0	Microsoft.PowerShell...
Cmdlet	Resume-Service	3.1.0.0	Microsoft.PowerShell...
Cmdlet	Set-Service	3.1.0.0	Microsoft.PowerShell...
Cmdlet	Start-Service	3.1.0.0	Microsoft.PowerShell...
Cmdlet	Stop-Service	3.1.0.0	Microsoft.PowerShell...
Cmdlet	Suspend-Service	3.1.0.0	Microsoft.PowerShell...

```

PS C:\Users\Администратор> Stop-Service sstpvc
PS C:\Users\Администратор> Get-Service sstpvc

Status      Name                DisplayName
-----
Stopped     sstpvc              Служба SSTP

PS C:\Users\Администратор> Start-Service sstpvc
PS C:\Users\Администратор> Get-Service sstpvc

Status      Name                DisplayName
-----
Running     sstpvc              Служба SSTP

```

- net start / stop

Управление компьютером

Файл Действие Вид Справка

Управление компьютером (локальный)

Службы
 Планировщик заданий
 Просмотр событий
 Общие папки
 Локальные пользователи и груп
 Производительность
 Диспетчер устройств
 Запоминающие устройства
 Система архивации данных Win
 Управление дисками
 Службы и приложения
 Маршрутизация и удаленный д
 Службы
 Управляющий элемент WMI

Служба SSTP	Имя	Описание	Состояние	Тип з	Дей
Остановить службу	Служба Advanced Threat Protection в Защитнике Windows	Служба A...	Выполняется	Вруч	Слу
Перезапустить службу	Служба AV/CTP	Это служб...	Выполняется	Вруч	Слу
	Служба Hyper-V PowerShell Direct	Обеспечи...	Выполняется	Вруч	
	Служба Microsoft Passport	Обеспечи...	Выполняется	Вруч	
	Служба PushToInstall Windows	Обеспечи...	Откл	Вруч	
	Служба SSTP	Обеспечи...	Выполняется	Вруч	
	Служба Windows Admin Center	Служба ве...	Выполняется	Авто	

Описание: Обеспечивает поддержку протокола SSTP (Secure Socket Tunneling Protocol) для

Администратор: Командная строка

```

C:\Users\Администратор>net
Синтаксис данной команды:
NET
[ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
HELPMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
STATISTICS | STOP | TIME | USE | USER | VIEW ]

C:\Users\Администратор>net view
^C
C:\Users\Администратор>net start SstpSvc
Служба "Служба SSTP" запускается.
Служба "Служба SSTP" успешно запущена.

```

протокола SSTP (Secure Socket Tunneling Protocol) для подключения к удаленным

Служба SSTP
 Служба Windows Admin Center

Обеспечи...
 Служба ве...

Администратор: Командная строка

```

C:\Users\Администратор>net stop SstpSvc
Служба "Служба SSTP" останавливается.
Служба "Служба SSTP" успешно остановлена.

```

Задание_3:

Сожмите том, создайте раздел, потом верните в исходное состояние

Управление компьютером

Файл Действие Вид Справка

Управление компьютером (локальным)

- Службные программы
 - Планировщик заданий
 - Просмотр событий
 - Общие папки
- Локальные пользователи и группы
 - Пользователи
 - Группы
- Производительность
- Диспетчер устройств
- Запоминающие устройства
 - Система архивации данных Windows
 - Управление дисками
- Службы и приложения

Том	Расположение	Тип	Файлова...	Состояние	Действия
(C:)	Простой	Базовый	NTFS	Исправен (Загрузка, Файл по	Управление ди... Дополните...
Зарезервировано сист...	Простой	Базовый	NTFS	Исправен (Система, Активен	

Диск 0

Базовый
50,00 ГБ
В сети

Зарезервировано	(C:)	6,05 ГБ
549 МБ NTFS Исправен (Систе	43,41 ГБ NTFS Исправен (Загрузка, Файл под	Не распределена

CD-ROM 0

CD-ROM (D:)

Нет носителя

Не распределена Основной раздел

Управление компьютером

Файл Действие Вид Справка

Просмотр событий

- Настраиваемые представления
- Журналы Windows
- Журналы приложений и служб
- Подписки

Общие папки

- Общие ресурсы
- Сеансы
- Открытые файлы

Локальные пользователи и группы

- Пользователи
- Группы

Производительность

Диспетчер устройств

Запоминающие устройства

- Система архивации данных Windows
- Управление дисками

Службы и приложения

- Маршрутизация и удаленный доступ
- Службы
- Управляющий элемент WMI

Том	Расположение	Тип	Файловая система	Состояние
(C:)	Простой	Базовый	NTFS	Исправен (Загрузка, Файл по
Зарезервировано системой	Простой	Базовый	NTFS	Исправен (Система, Активен
Новый том (E:)	Простой	Базовый	ReFS	Исправен (Основной раз

Диск 0

Базовый
50,00 ГБ
В сети

Зарезервировано	(C:)	Новый том (E:)
549 МБ NTFS Исправен (Систе	43,41 ГБ NTFS Исправен (Загрузка, Файл под	6,05 ГБ ReFS Исправен (Основной раз

CD-ROM 0

CD-ROM (D:)


Нет носителя

Том	Расположение	Тип	Файловая система	Состояние
(C:)	Простой	Базовый	NTFS	Исправен (Загрузка)
Зарезервировано системой	Простой	Базовый	NTFS	Исправен (Системный)
Новый том (E:)	Простой	Базовый	ReFS	Исправен (Основной раз)

Диск 0	Зарезервировано	(C:)	Новый том (E:)
Базовый 50,00 ГБ В сети	549 МБ NTFS Исправен (Системный)	43,41 ГБ NTFS Исправен (Загрузка, Файл под)	6,05 ГБ ReFS Исправен (Основной раз)

CD-ROM 0
CD-ROM (D:)
Нет носителя

Диспетчер виртуальных дисков

 Уменьшение тома невозможно, так как не поддерживается файловой системой.

OK

■ Не распределена ■ Основной раздел

тр событий

раиваемые представлени

налы Windows

наде

тиск

папки

ие р

исы

ыты

ые п

зова

пы

дите

ер у

щие

арх

ние

трил

диза

1

Том	Расположение	Тип	Файловая система	Состояние
(C:)	Простой	Базовый	NTFS	Исправен (Загрузка)
Зарезервировано системой	Простой	Базовый	NTFS	Исправен (Системный)
Новый том (E:)	Простой	Базовый	NTFS	Исправен (Основной раз)


Сжать E:

Общий размер до сжатия (МБ): 6197

Доступное для сжатия пространство (МБ): 3075

Размер сжимаемого пространства (МБ): **3075**

Общий размер после сжатия (МБ): 3122

 Невозможно сжать том дальше области расположения неподвижных файлов. Дополнительные сведения об этой операции см. после ее завершения в описании события "defrag" в журнале приложения.

Дополнительные сведения см. в разделе "Сжатие базового тома" из справки по управлению дисками

Сжать Отмена

Дей

Упр

Том	Расположение	Тип	Файловая система	Состояние
(C:)	Простой	Базовый	NTFS	Исправен (Загрузка, Файл)
Зарезервировано системой	Простой	Базовый	NTFS	Исправен (Система, Активный)
Новый том (E:)	Простой	Базовый	NTFS	Исправен (Основной раздел)

Диск 0	Зарезервировано	(C:)	Новый том (E:)	
Базовый 50,00 ГБ В сети	549 МБ NTFS Исправен (Система, Активный)	43,41 ГБ NTFS Исправен (Загрузка, Файл)	5,08 ГБ NTFS Исправен (Основной раздел)	1001 МБ Не распределено

Том	Расположение	Тип	Файловая система	Состояние
(C:)	Простой	Базовый	NTFS	Исправен (Загрузка, Файл)
Зарезервировано системой	Простой	Базовый	NTFS	Исправен (Система, Активный)
Новый том (E:)	Простой	Базовый	NTFS	Исправен (Основной раздел)
Новый том (F:)	Простой	Базовый	NTFS	Исправен (Логический)

Диск 0	Зарезервировано	(C:)	Новый том (E:)	Новый том (F:)
Базовый 50,00 ГБ В сети	549 МБ NTFS Исправен (Система, Активный)	43,41 ГБ NTFS Исправен (Загрузка, Файл)	5,08 ГБ NTFS Исправен (Основной раздел)	1000 МБ NTFS Исправен (Логический)

CD-ROM 0				
CD-ROM (D:)				
Нет носителя				

Удалить том, раздел ...

Том	Расположение	Тип	Файловая система	Состояние	Дей
(C:)	Простой	Базовый	NTFS	Исправен (Загрузка, Фа	Упр
Зарезервировано системой	Простой	Базовый	NTFS	Исправен (Система, Ак	

Диск 0 Базовый 50,00 ГБ В сети	Зарезервирован 549 МБ NTFS Исправен (Систем	(C:) 43,41 ГБ NTFS Исправен (Загрузка, Файл подка	6,05 ГБ Не распределена
CD-ROM 0 CD-ROM (D:) Нет носителя			

kali-linux-2022.1-virtualbox-amd64
Powered Off

w2019core01
Powered Off

w2019gui01
Powered Off

deb8vuln2
Powered Off

Metasploitable3-ub1404
Powered Off

DVL
Powered Off

General

System

Display

Storage

Audio

Network

Serial Ports

USB

Shared Folders

User Interface

Storage

Storage Devices

Controller: SATA

- w2019gui01.vdi
- Empty
- w2019gui01_2.vdi
- w2019gui01_1.vhd

Attributes

Hard Disk: SATA Port 3

- ☐ Solid-state Drive
- ☐ Hot-pluggable

Information

Type (Format): Normal (VHD)

Virtual Size: 1.07 GB

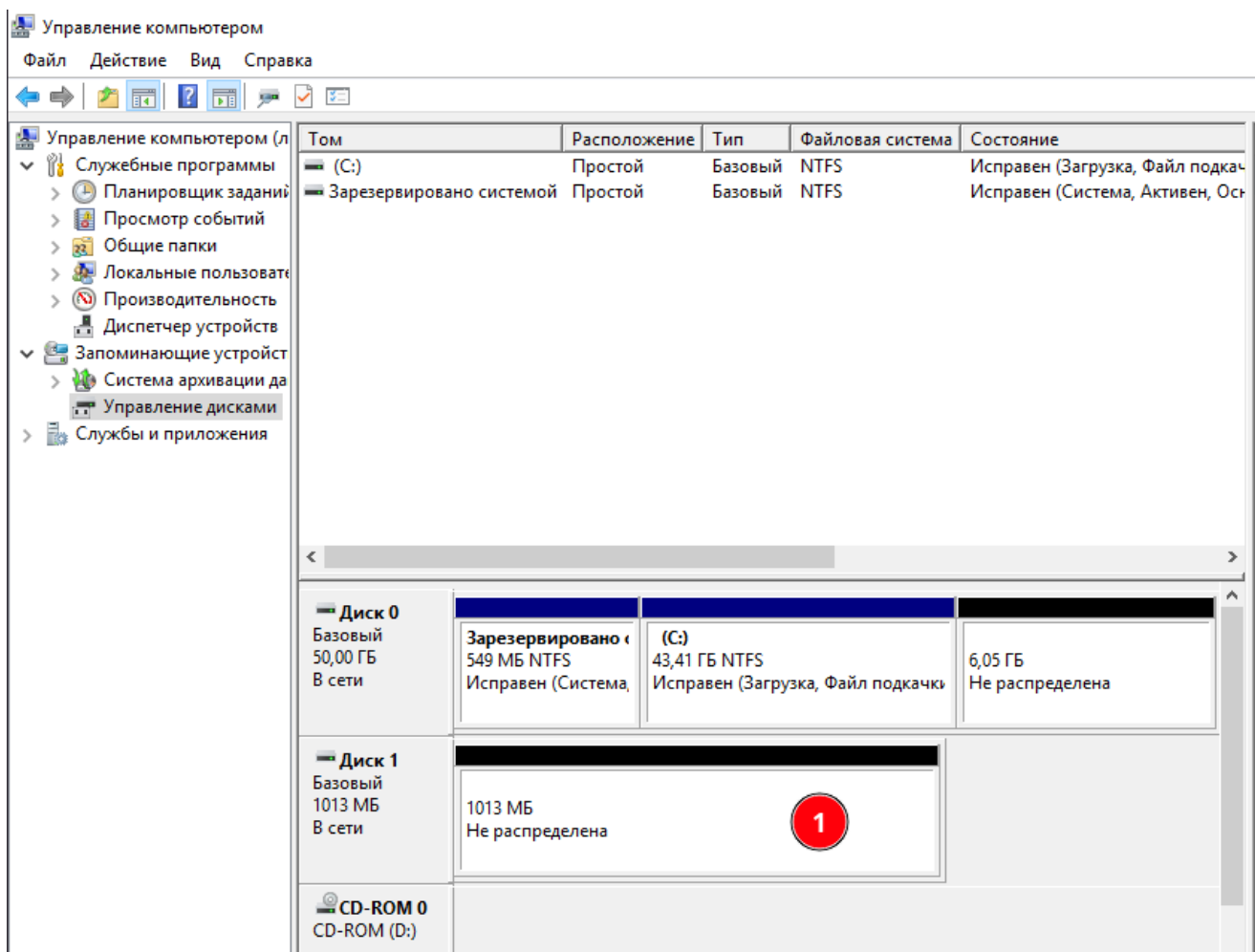
Actual Size: 4.50 KB

Details: Dynamically allocated storage

Location: /home/am/VirtualBox VMs/w201...

Attached to: --

Encrypted with key: --



С Диск 1 проведем те же действия, что и с Диск 0

Задание_4:

Подключите второй диск, преобразуйте его в GPT

- Для каждой секции или тома выберите элемент и удерживайте его (или щелкните правой кнопкой мыши) и выберите пункт "Удалить секцию" или "Удалить том".
- Выберите и удерживайте (или щелкните правой кнопкой мыши) диск МБ R для преобразования в формат GPT и выберите команду "Преобразовать в диск GPT".

Управление компьютером (л)

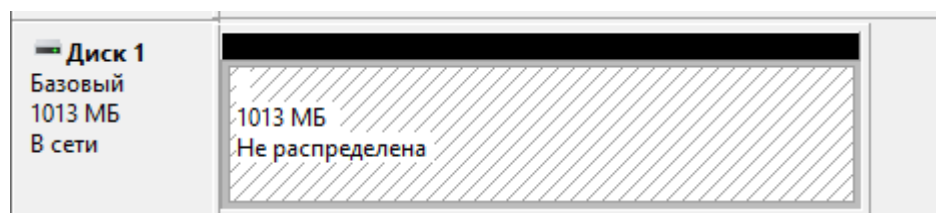
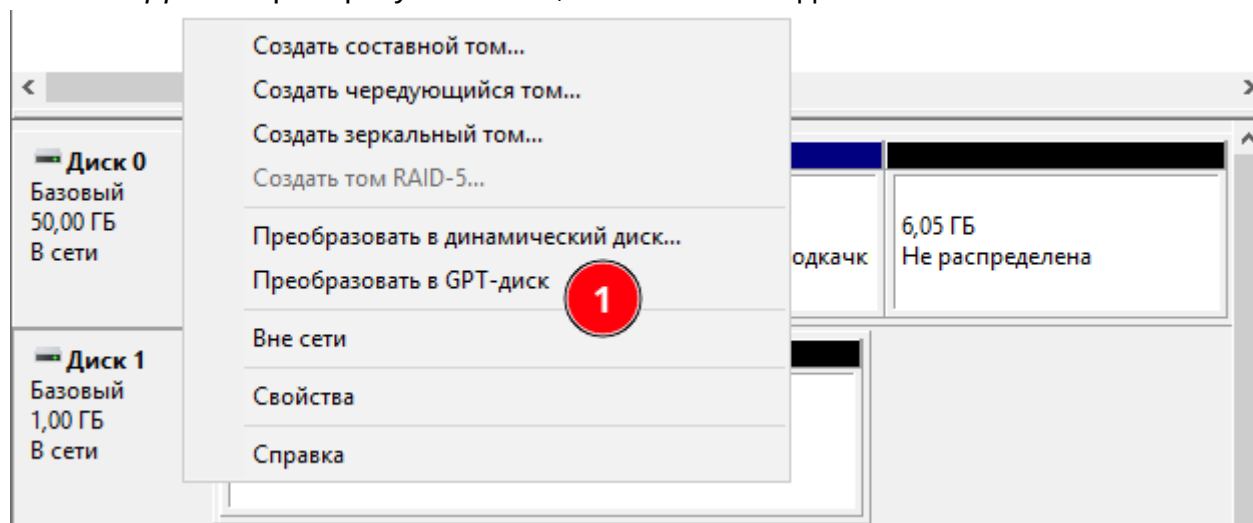
- Службные программы
 - Планировщик заданий
 - Просмотр событий
 - Общие папки
 - Локальные пользователи и группы
 - Производительность
 - Диспетчер устройств
- Запоминающие устройства
 - Система архивации данных
 - Управление дисками
- Службы и приложения

Том	Расположение	Тип	Файловая система	Состояние
(C:)	Простой	Базовый	NTFS	Исправен (Загрузка, Файл подкачки)
Зарезервировано системой	Простой	Базовый	NTFS	Исправен (Система, Активен, Остаток)
Новый том (E:)	Простой	Базовый	NTFS	Исправен (Основной раздел)

Диск	Тип	Объем	Состояние
Диск 0	Базовый	50,00 ГБ	В сети
Зарезервировано системой	549 МБ NTFS	Исправен (Система, Активен, Остаток)	
(C:)	43,41 ГБ NTFS	Исправен (Загрузка, Файл подкачки)	6,05 ГБ Не распределена
Диск 1	Базовый	1013 МБ	В сети
Новый том (E:)	1012 МБ NTFS	Исправен (Основной раздел)	
CD-ROM 0	CD-ROM (D:)	Нет носителя	

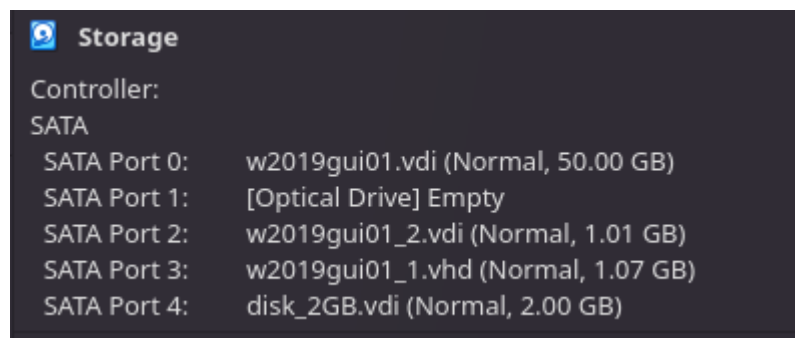
Диск	Тип	Объем	Состояние
Диск 0	Базовый	50,00 ГБ	В сети
Зарезервировано системой	549 МБ NTFS	Исправен (Система, Активен, Остаток)	
(C:)	43,41 ГБ NTFS	Исправен (Загрузка, Файл подкачки)	6,05 ГБ Не распределена
Диск 1	Базовый	1013 МБ	Вне сети
1013 МБ	Не распределена		
CD-ROM 0	CD-ROM (D:)	Нет носителя	

Сначала *Диск 1* преобразуем в MBR, а потом в GPT-диск.

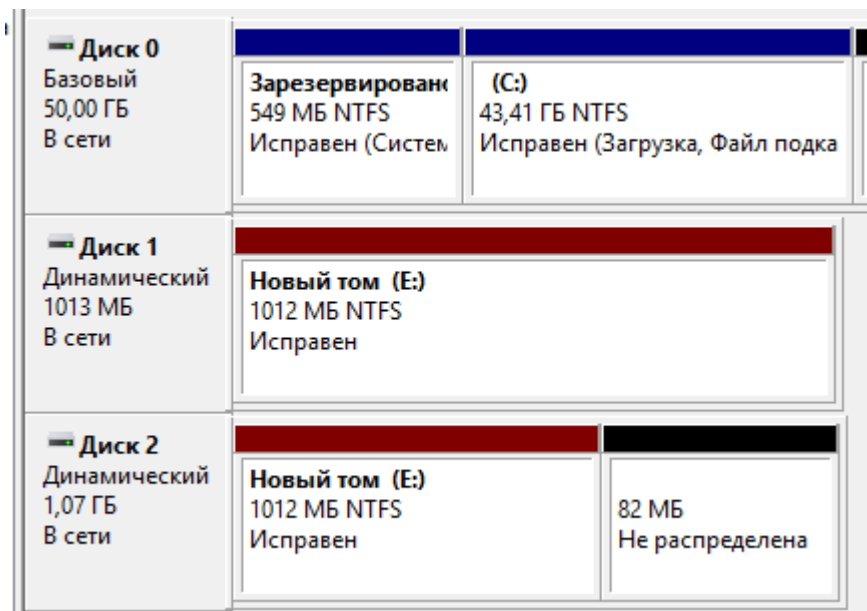
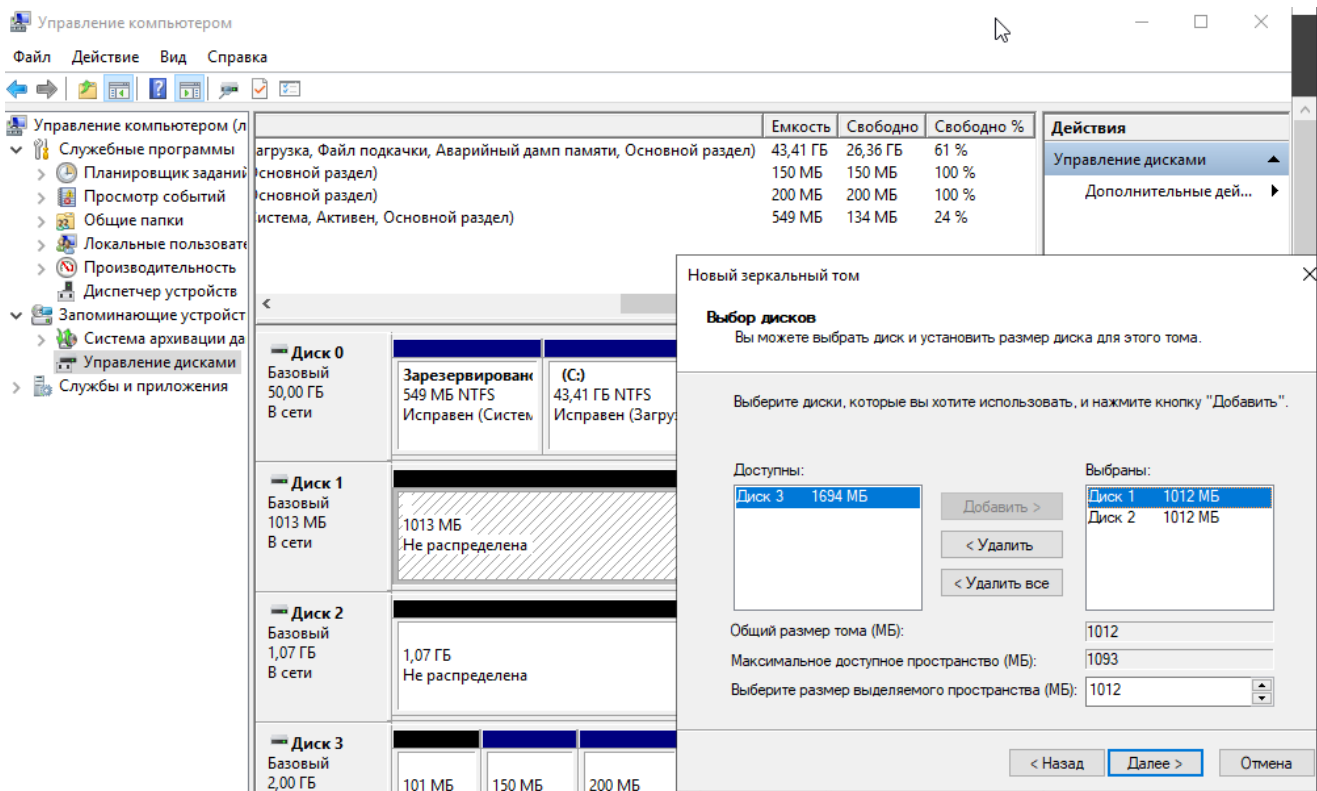


Задание_5:

Добавьте третий диск, создайте из 2 и 3 диска зеркальный том

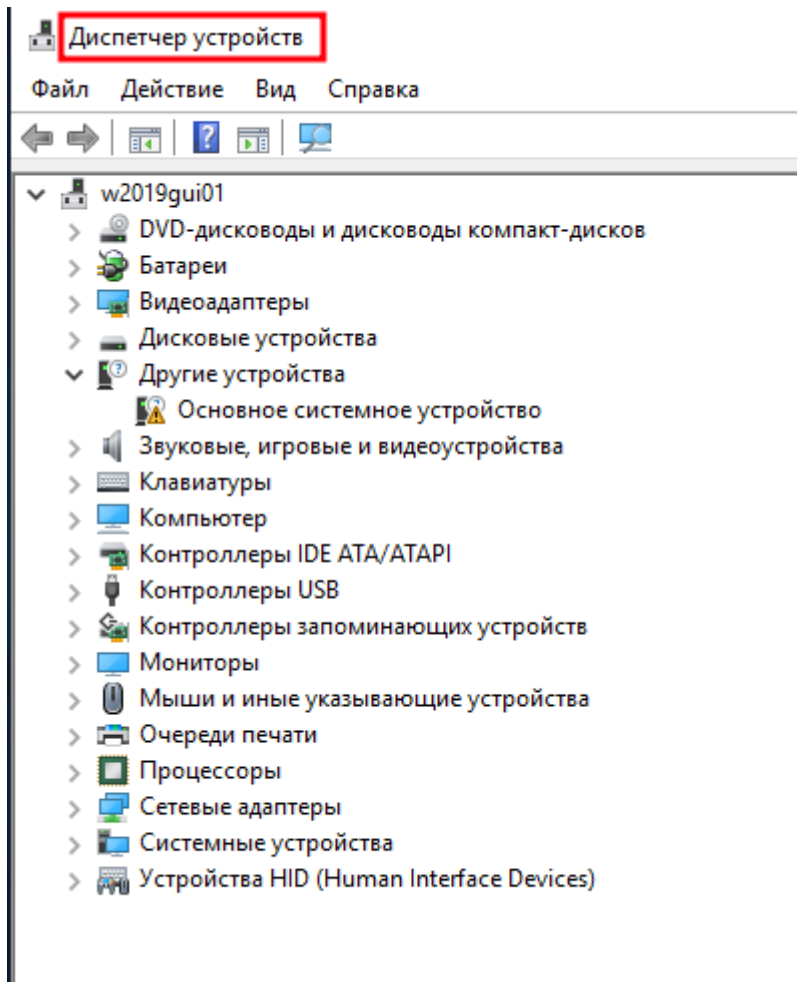


<div><div></div><div>Диск 0</div><div>Базовый</div><div>50,00 ГБ</div><div>В сети</div></div>	<div><div></div><div>Зарезервирован</div><div>549 МБ NTFS</div><div>Исправен (Систем</div></div>	<div><div></div><div>(C:)</div><div>43,41 ГБ NTFS</div><div>Исправен (Загрузка, Файл подка</div></div>	<div><div></div><div>6,05 ГБ</div><div>Не распределена</div></div>	
<div><div><div></div><div>Диск 1</div><div>Базовый</div><div>1013 МБ</div><div>В сети</div></div></div>	<div><div></div><div>1013 МБ</div><div>Не распределена</div></div>			
<div><div><div></div><div>Диск 2</div><div>Базовый</div><div>1,07 ГБ</div><div>В сети</div></div></div>	<div><div></div><div>1,07 ГБ</div><div>Не распределена</div></div>			
<div><div><div></div><div>Диск 3</div><div>Базовый</div><div>2,00 ГБ</div><div>В сети</div></div></div>	<div><div></div><div>101 МБ</div><div>Не распр</div></div>	<div><div></div><div>150 МБ</div><div>Исправен</div></div>	<div><div></div><div>200 МБ</div><div>Исправен (</div></div>	<div><div></div><div>1,56 ГБ</div><div>Не распределена</div></div>
<div><div><div></div><div>CD-ROM</div></div></div>				
<div><div></div> Не распределена</div> <div><div></div> Основной раздел</div>				

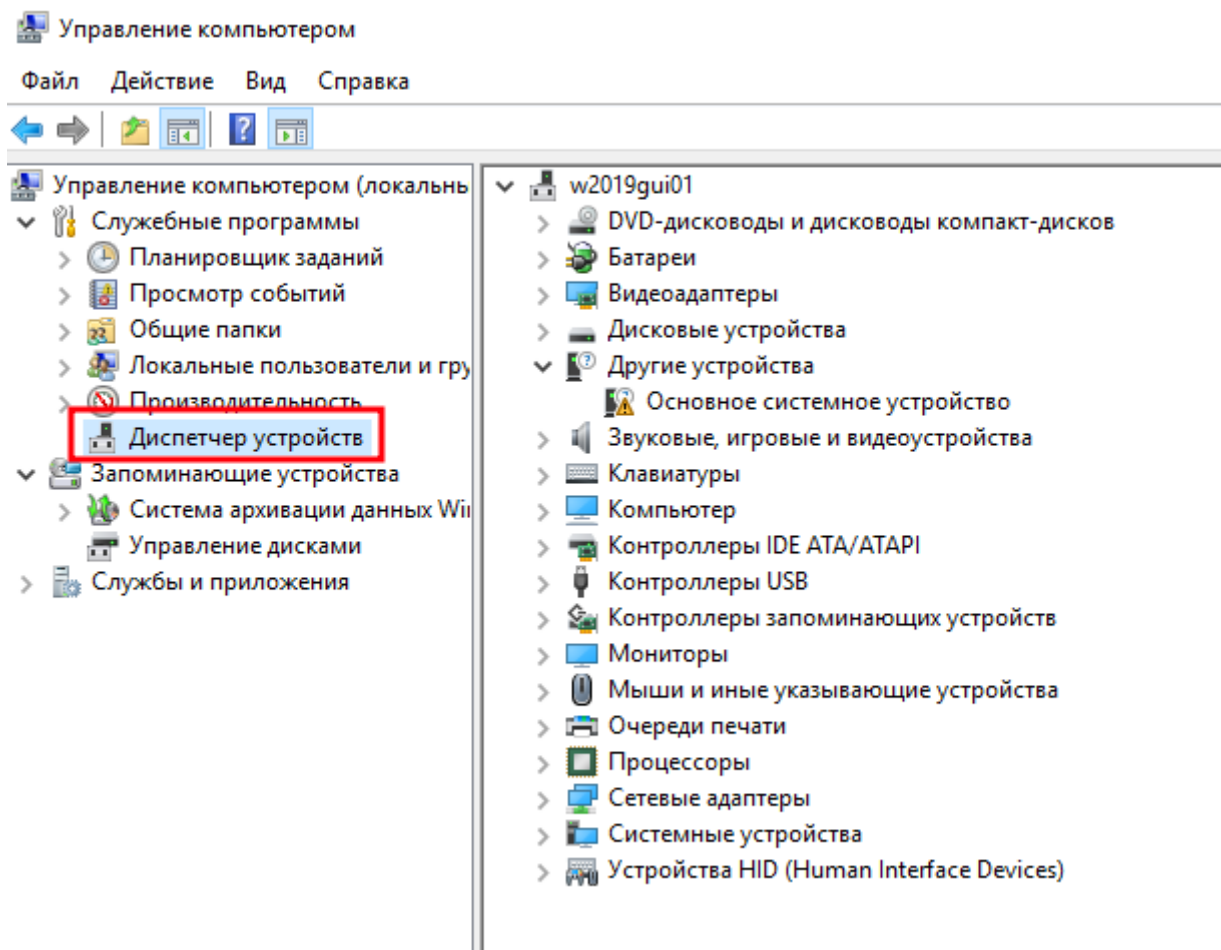


Задание_6:

Найдите ИД оборудования (`pci\ven` , например, контроллер жесткого диска или видеокарта) и сайт в интернете, откуда можно скачать драйвера для этого устройства



Или через Диспетчер устройств



Свойства: Базовый видеоадаптер (Майкрософт)

Общие | **Драйвер** | Сведения | События | Ресурсы

Базовый видеоадаптер (Майкрософт)

События

Метка времени	Описание
21.01.2024 20:48:27	Запрошена установка устройства
21.01.2024 20:48:30	Запрошена установка устройства
21.01.2024 20:48:49	Устройство настроено (display.inf)
21.01.2024 20:48:49	Устройство запущено (BasicDisplay)
21.01.2024 20:48:49	Устройство установлено (display.inf...)

Сведения

Устройству PCI
VEN_80EE&DEV_BEEF&SUBSYS_040515AD&REV_00\3&267a616
a&0&10 требуется дальнейшая установка.

Просмотреть все события...

OK Отмена

Сведения о файлах драйверов

Базовый видеоадаптер (Майкрософт)

Файлы драйверов:

basicdisplay.inf_amd64_5103ac179273be89\BasicDisplay.sy

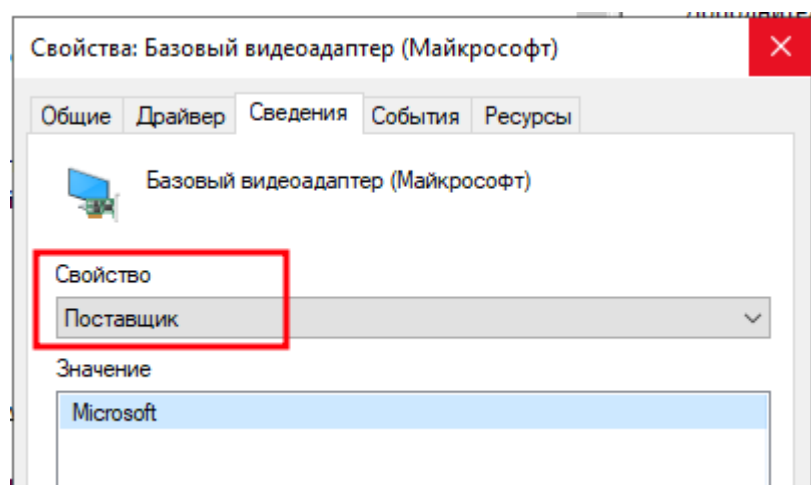
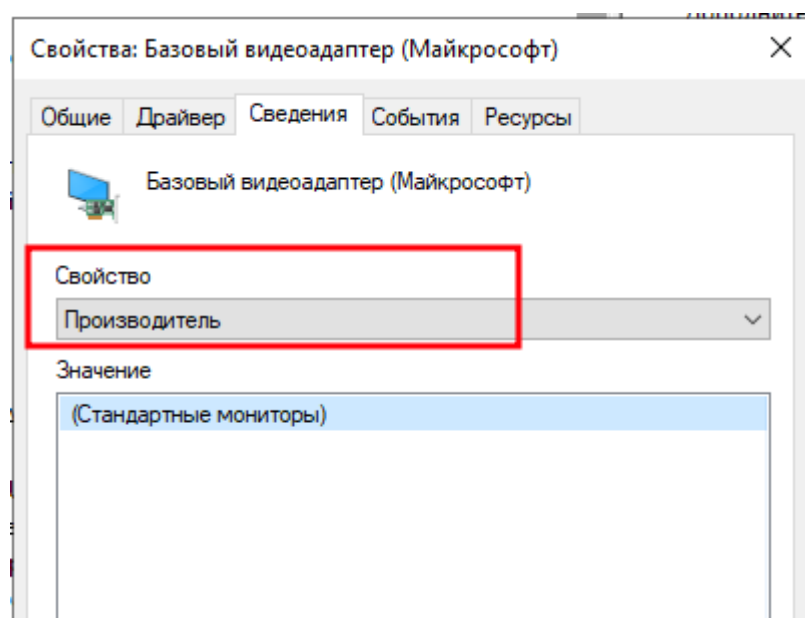
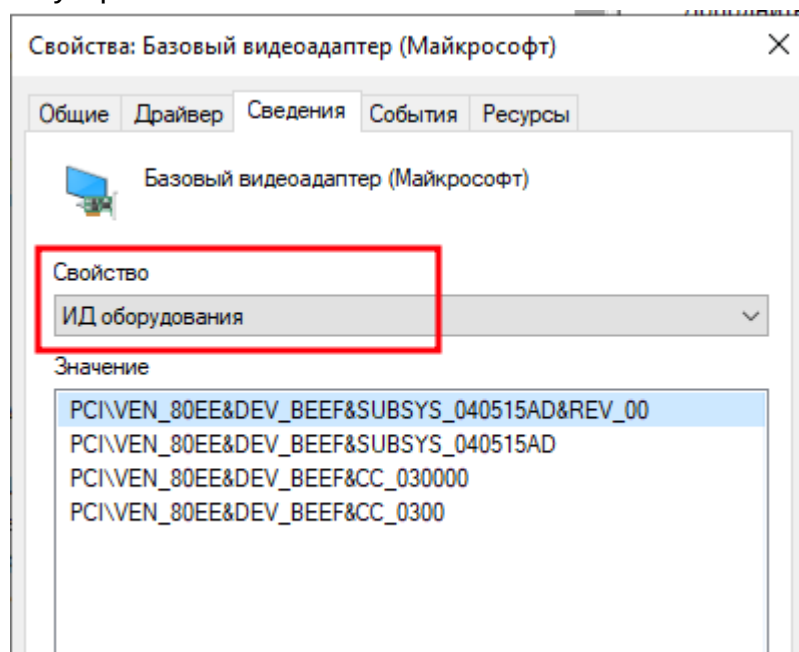
Поставщик: Microsoft Corporation

Версия файла: 10.0.17763.1 (WinBuild.160101.0800)


Авторские права: © Microsoft Corporation. All rights reserved.

Цифровая подпись: Microsoft Windows

ID-устройства



Пробуем обновить драйвер

←  Обновить драйверы — Базовый видеоадаптер (Майкрософт)


Наиболее подходящие драйверы для данного устройства уже установлены

Система Windows определила, что наиболее подходящий драйвер для этого устройства уже установлен. Более подходящие драйверы могут быть размещены в Центре обновления Windows или на веб-сайте изготовителя устройства.



Базовый видеоадаптер (Майкрософт)

→ Поиск обновленных драйверов в Центре обновления Windows

 Обновить драйверы — Базовый видеоадаптер (Майкрософт)

Выберите драйвер для этого устройства.



Выберите изготовителя устройства, его модель и нажмите кнопку "Далее". Если имеется установочный диск с драйвером, нажмите кнопку "Вы хотите установить с диска".

☒ Только совместимые устройства

Модель



Базовый видеоадаптер (Майкрософт)



Драйвер имеет цифровую подпись.

[Сведения о подписывании драйверов](#)

Установить с диска...

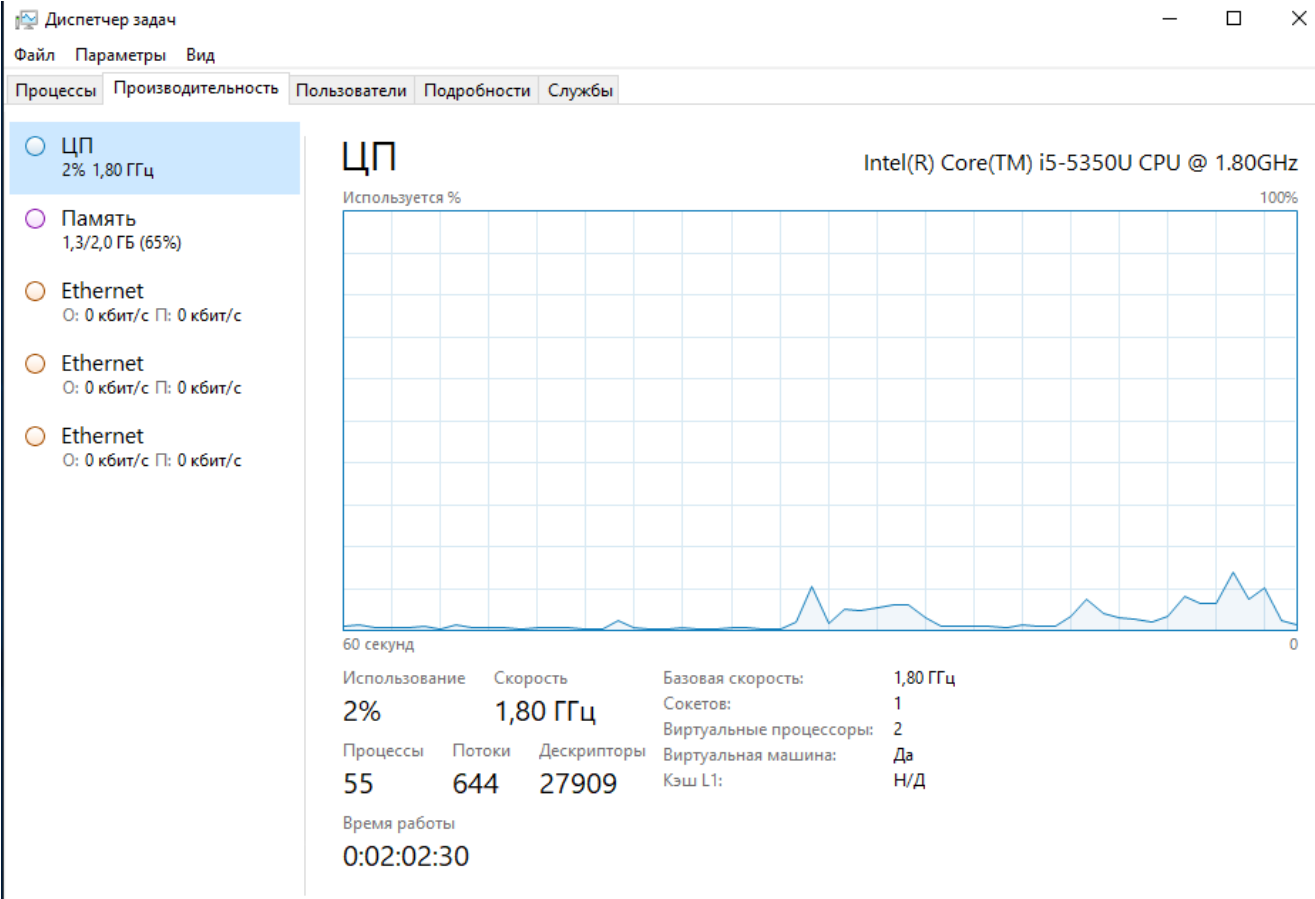
Перенаправляемся на интернет страничку

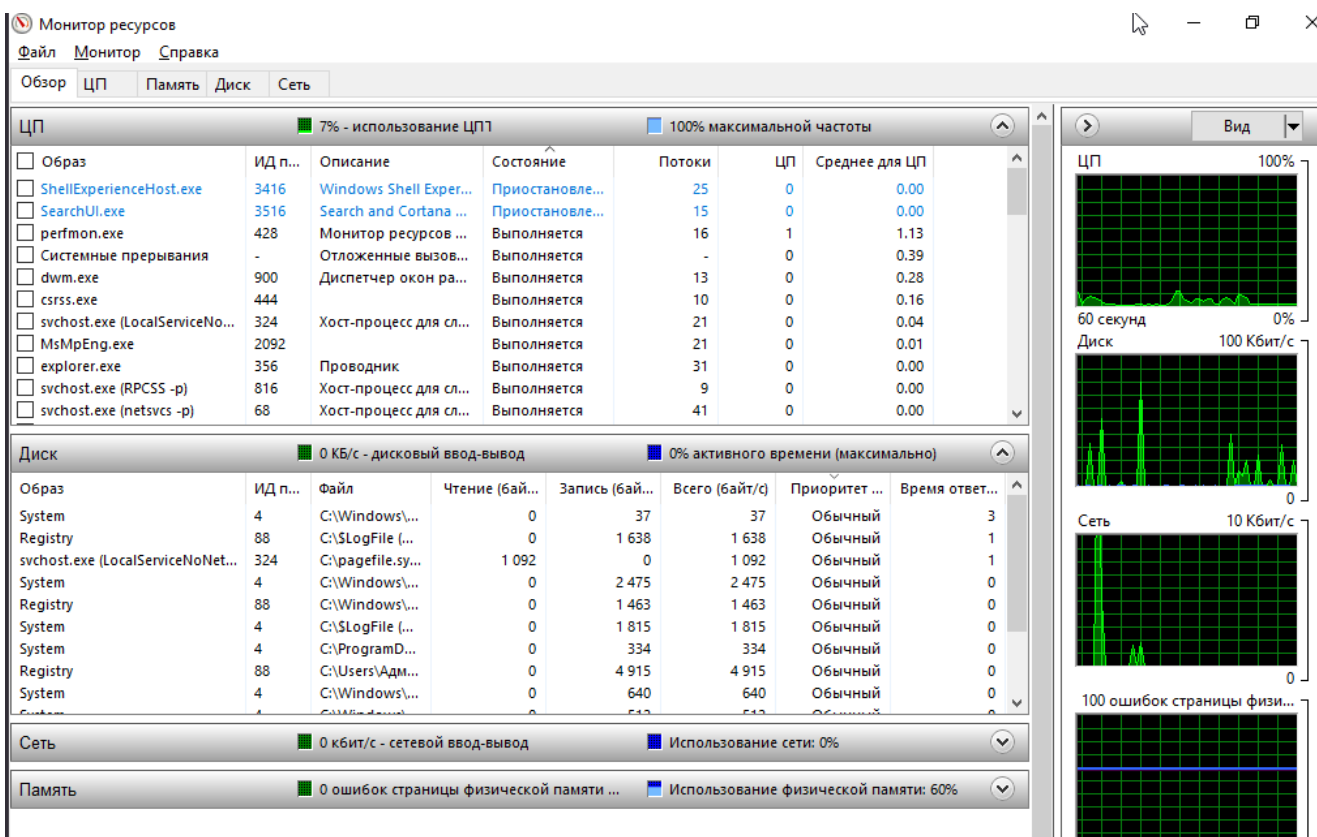
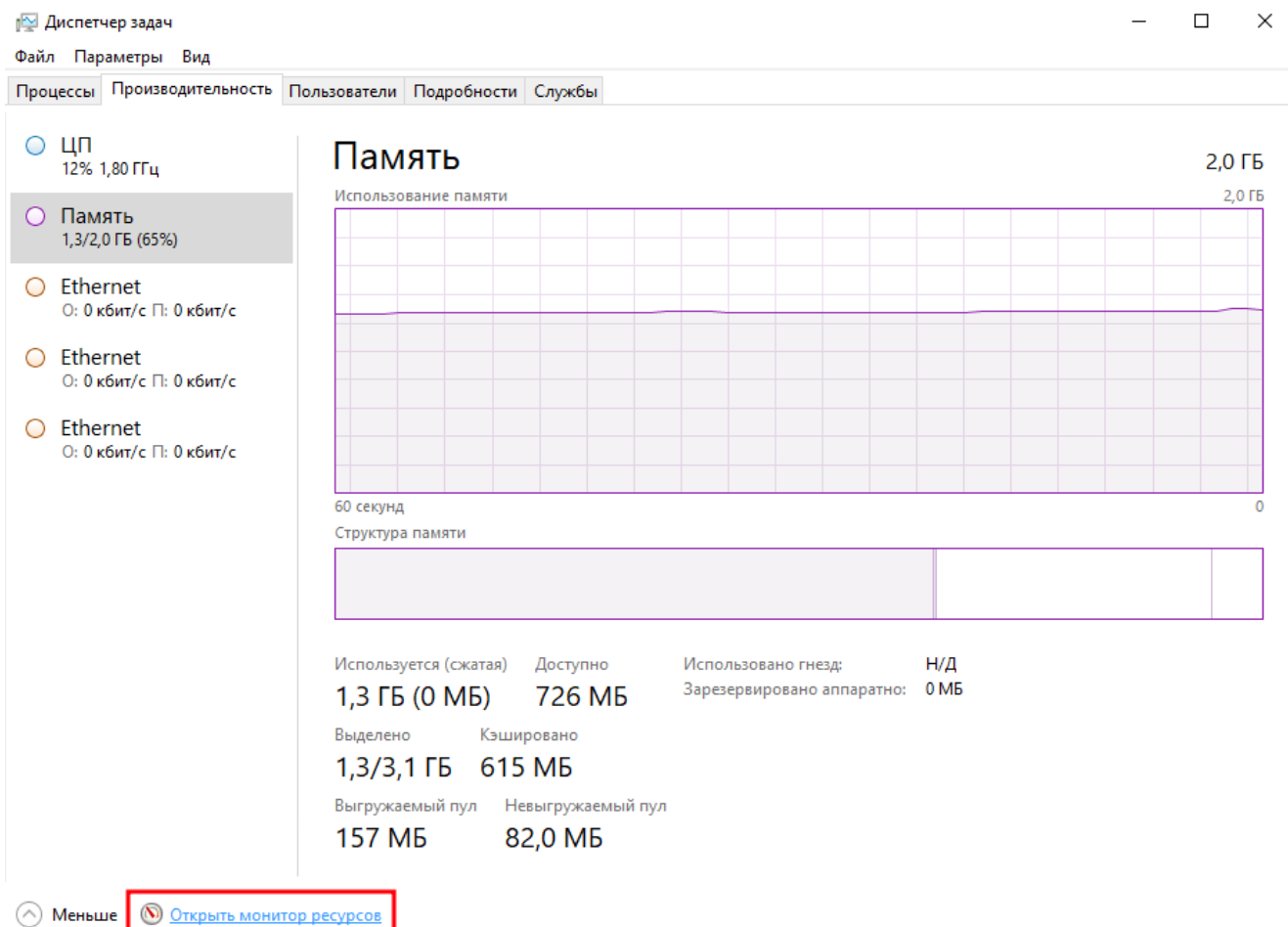
Задание_7:

В диспетчере задач отфильтруйте приложения которые больше всего потребляют ресурсов процессора и оперативную память

Диспетчер задач (Ctrl+Alt+Del)

Диспетчер задач			
Файл Параметры Вид			
Процессы Производительность Пользователи Подробности Службы			
Имя	Состояние	ЦП	Память
> Диспетчер задач		1,7%	14,1 МБ
Системные прерывания		1,1%	0 МБ
Диспетчер окон рабочего стола		0,7%	31,7 МБ
Процесс исполнения клиент-...		0%	1,4 МБ
> Antimalware Service Executable		0%	107,1 МБ
> Узел службы: локальная систе...		0%	36,0 МБ
> Windows Admin Center Windo...		0%	35,2 МБ
> Консоль управления (MMC)		0%	25,1 МБ
> Проводник		0%	23,3 МБ
> Поиск (2)		0%	20,0 МБ
> Узел службы: локальная служ...		0%	16,7 МБ
> Хост Windows Shell Experience		0%	16,6 МБ
> Узел службы: UtcSvc		0%	15,0 МБ





Монитор ресурсов

Файл Монитор Справка

Обзор ЦП Память Диск Сеть

ЦП 4% - использование ЦП 100% максимальной частоты

Образ	ИД п...	Описание	Состояние	Потоки	ЦП	Среднее для ЦП
perfmon.exe	428	Монитор ресурсов ...	Выполняется	21	3	1.73
Системные прерывания	-	Отложенные вызов...	Выполняется	-	2	1.03
ieexplore.exe	996	Internet Explorer	Выполняется	40	0	6.63
ieexplore.exe	3836	Internet Explorer	Выполняется	16	0	1.14
dwm.exe	900	Диспетчер окон ра...	Выполняется	12	0	0.66
MsMpEng.exe	2092		Выполняется	24	0	0.47
csrss.exe	444		Выполняется	10	0	0.16
taskhostw.exe	468	Хост-процесс для за...	Выполняется	8	0	0.16
explorer.exe	356	Пользоват...	Выполняется	38	0	0.13
lsass.exe						
svchost.exe						

https://www.bing.com/search?q=perfmon.exe

perfmon.exe - Поиск

Microsoft Bing

perfmon.exe

ВСЕ ИЗОБРАЖЕНИЯ ВИДЕО КАРТЫ НОВОСТИ ПОКУПКИ МОЙ BING

Приблизительное число результатов: 4.310.000

geekon.media
https://geekon.media/chto-takoe-perfmon-exe

Perfmon.exe: что это за процесс, почему грузит диск, ...

Интернет **Perfmon.exe** – это исполняющийся файл стандартного приложения Performance Monitor, который графически отображает загруженность ресурсов ПК. Для решения проблемы с загрузкой процессора нужно обновить ОС.

ЦП 100%

Диск 1 Мбит/с

10 Кбит/с

Управление компьютером

Файл Действие Вид Справка

Управление компьютером (л)

- Служебные программы
 - Планировщик заданий
 - Просмотр событий
 - Общие папки
 - Локальные пользователи и группы
 - Производительность
 - Средства наблюдения
 - Системный монитор
 - Группы сборщиков данных
 - Отчеты
 - Диспетчер устройств
 - Запоминающие устройства
 - Система архивации данных
 - Управление дисками
 - Службы и приложения

Системный монитор

Действия

Системный монитор

Дополнительные дей..

100

80

60

40

20

0

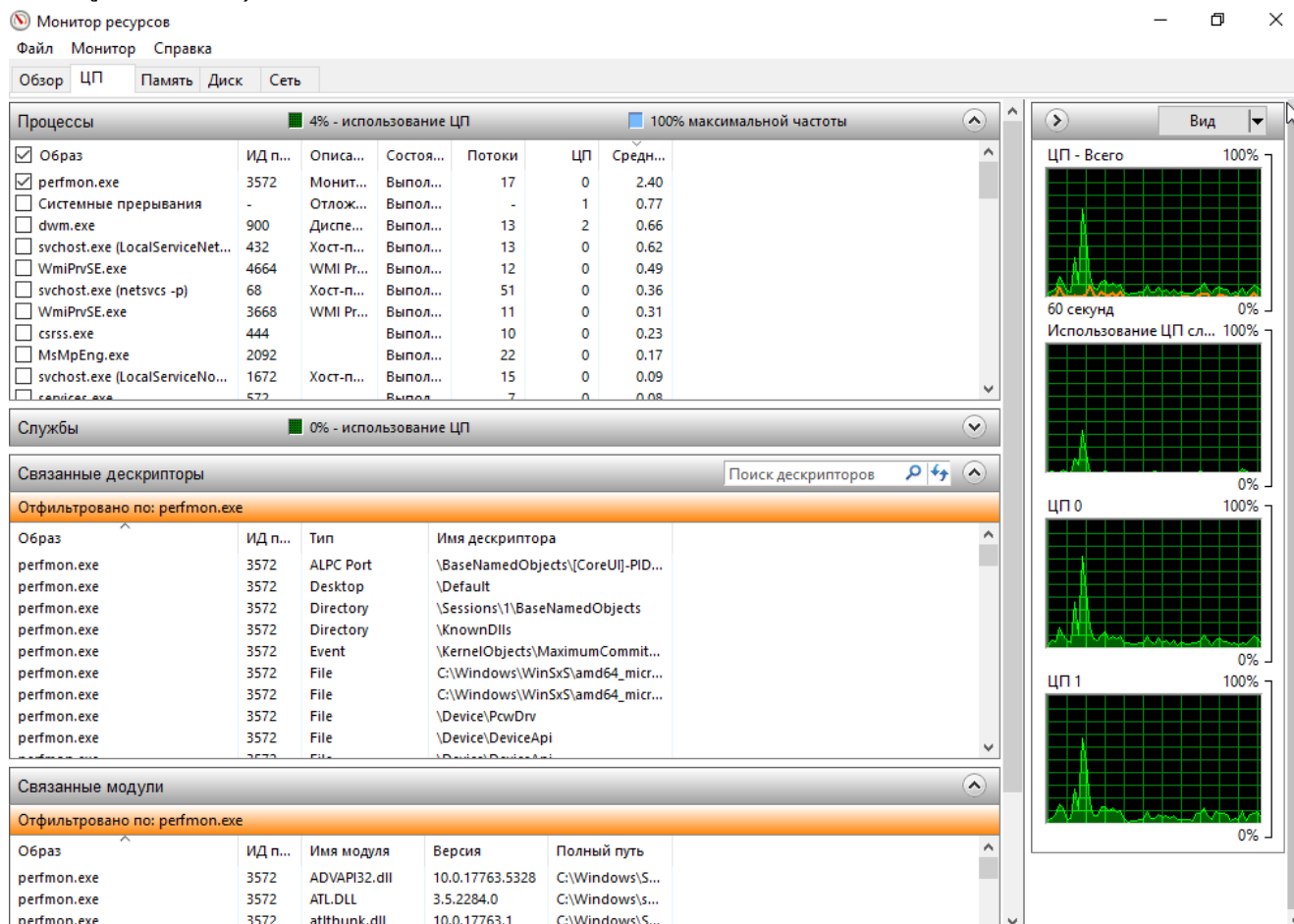
2:53:01 2:53:15 2:53:25 2:53:35 2:53:45 2:53:55 2:54:05 2:54:15 2:54:25 2:54:39

Последний Средний Минимум

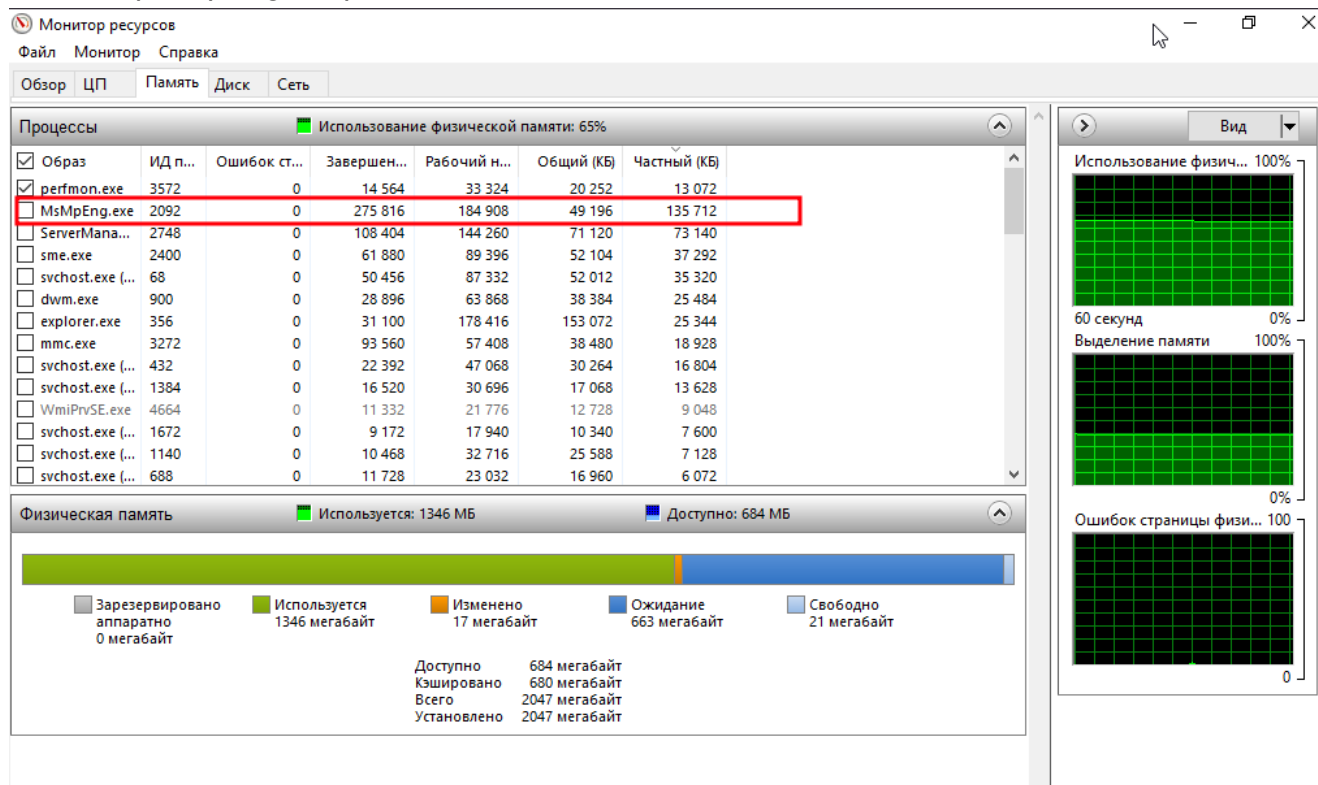
Максимум Длительность 1:40

Пок...	Цвет	Ша...	Счетчик	Экзем...	Родит...	Объект	Компьютер
✓	—	0,1	Ошибка страниц...	---	---	Память	\\W2019GUI0
✓	—	0,000...	Доступно байт	---	---	Память	\\W2019GUI0
✓	—	0,000...	Байт выделенной...	---	---	Память	\\W2019GUI0
✓	—	0,000...	Предел выделен...	---	---	Память	\\W2019GUI0
✓	—	1,0	Запись копий стр...	---	---	Память	\\W2019GUI0
✓	—	0,1	Ошибка транзит...	---	---	Память	\\W2019GUI0
✓	—	0,1	Ошибка кэш-па...	---	---	Память	\\W2019GUI0
✓	—	0,1	Ошибка запроса ...	---	---	Память	\\W2019GUI0

CPU (perfon.exe)

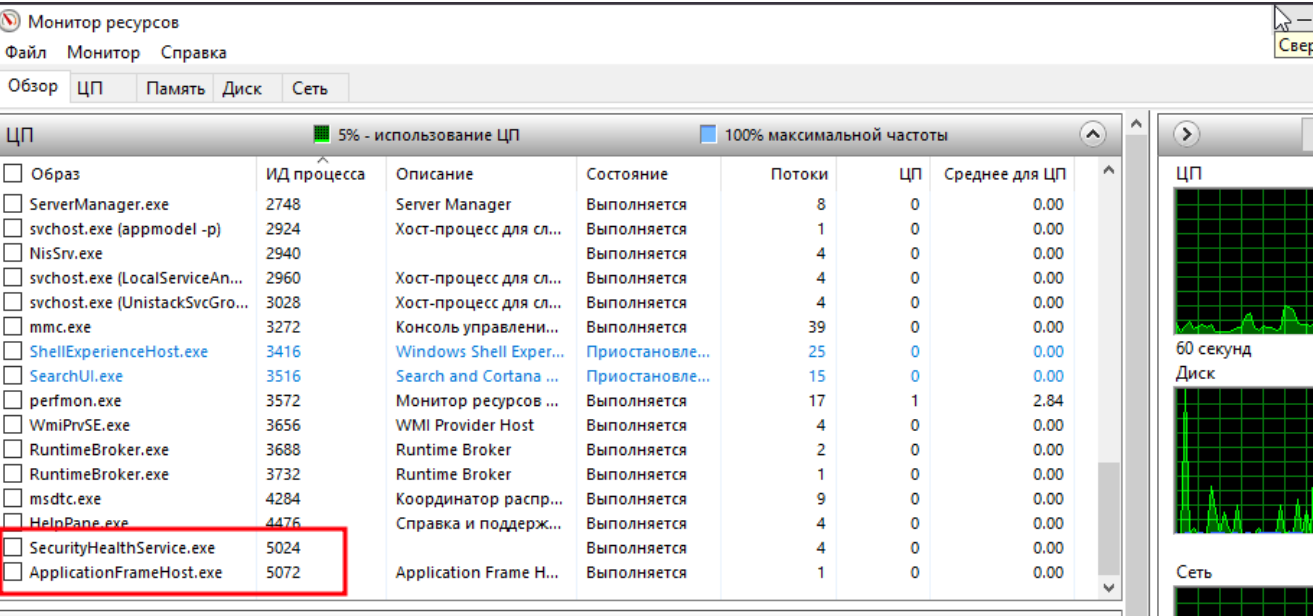


Память (MsMpEng.exe)



Задание_8:

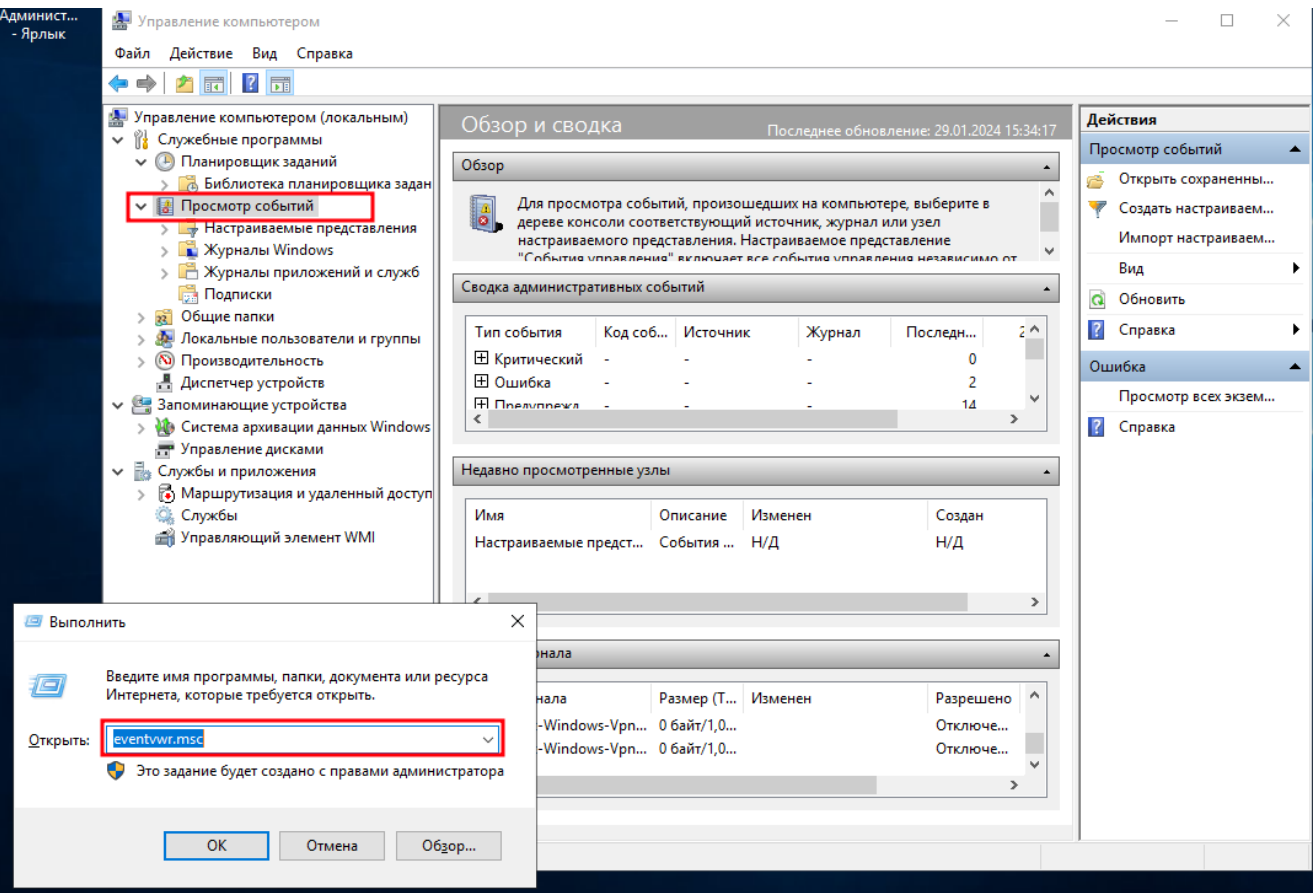
Отфильтруйте системные события с кодом 6013 или 7036



Здесь ID-процесса с 6013 и/или 7036 не наблюдаем.

Запускаем Просмотр событий

- eventvwr.msc



Настраиваемые представления

События: 7036, 6013

Управление компьютером

Файл Действие Вид Справка

Управление компьютером (локальным)

- Служебные программы
 - Планировщик заданий
 - Библиотека планировщика задан...
 - Просмотр событий
 - Настраиваемые представления
 - Роли сервера
 - События управления
 - Журналы Windows
 - Журналы приложений и служб
 - Подписки
 - Общие папки
 - Локальные пользователи и группы
 - Производительность
 - Диспетчер устройств
- Запоминающие устройства
 - Система архивации данных Windows
 - Управление дисками
- Службы и приложения
 - Маршрутизация и удаленный доступ
 - Службы

Событий: 305

Уровень	Дата и время	Источник	Код соб...	Кategori...
Ошибка	21.01.2024 23:44:08	NetBT	4321	Отсутств...
Ошибка	21.01.2024 23:26:59	NetBT	4321	Отсутств...
Ошибка	21.01.2024 23:44:10	NetBT	4321	Отсутств...
Ошибка	21.01.2024 23:26:55	NetBT	4321	Отсутств...
Предупрежде...	22.01.2024 1:26:44	Winlogon	6005	Отсутств...
Предупрежде...	22.01.2024 1:29:03	Winlogon	6006	Отсутств...
Ошибка	29.01.2024 13:18:19	EventLog	6008	Отсутств...
Ошибка	22.01.2024 0:02:00	EventLog	6008	Отсутств...
Ошибка	28.01.2024 15:16:42	EventLog	6008	Отсутств...
Ошибка	21.01.2024 23:44:04	EventLog	6008	Отсутств...
Ошибка	21.01.2024 20:48:46	Service C...	7023	Отсутств...
Ошибка	21.01.2024 20:48:46	Service C...	7023	Отсутств...
Ошибка	28.01.2024 17:31:01	Service C...	7023	Отсутств...
Ошибка	21.01.2024 22:49:16	Service C...	7030	Отсутств...
Ошибка	21.01.2024 23:44:20	Security-...	8198	Отсутств...

Событие 15301 HttpEvent

Смотрим Журнал Windows (6013, 7036)

Управление компьютером

Файл Действие Вид Справка

Управление компьютером (локальным)

- Служебные программы
 - Планировщик заданий
 - Библиотека планировщика задан...
 - Просмотр событий
 - Настраиваемые представления
 - Роли сервера
 - События управления
 - Журналы Windows
 - Приложение
 - Безопасность
 - Установка
 - Система
 - Перенаправленные события
 - Журналы приложений и служб
 - Подписки
 - Общие папки
 - Локальные пользователи и группы
 - Производительность
 - Диспетчер устройств
- Запоминающие устройства
 - Система архивации данных Windows
 - Управление дисками
- Службы и приложения

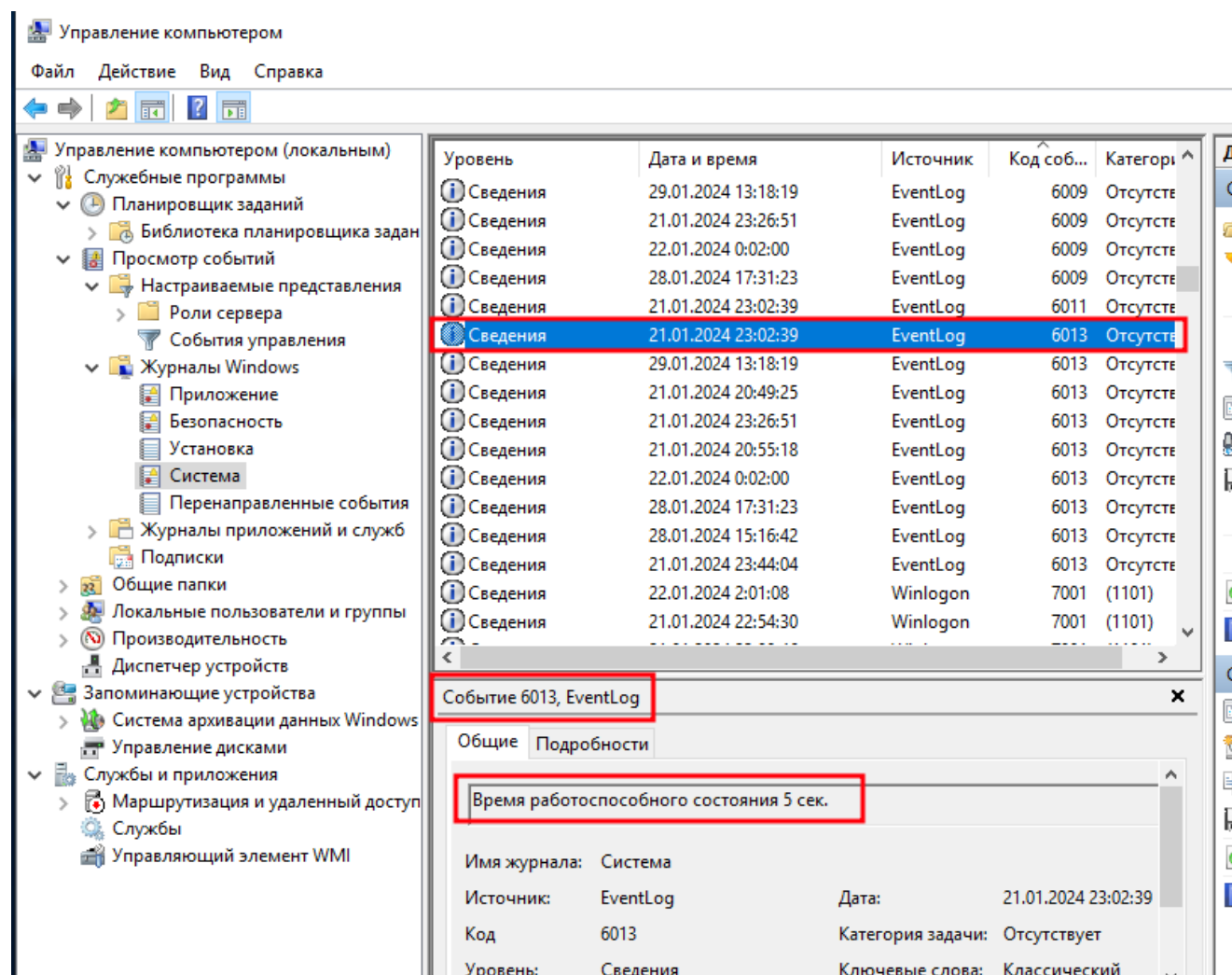
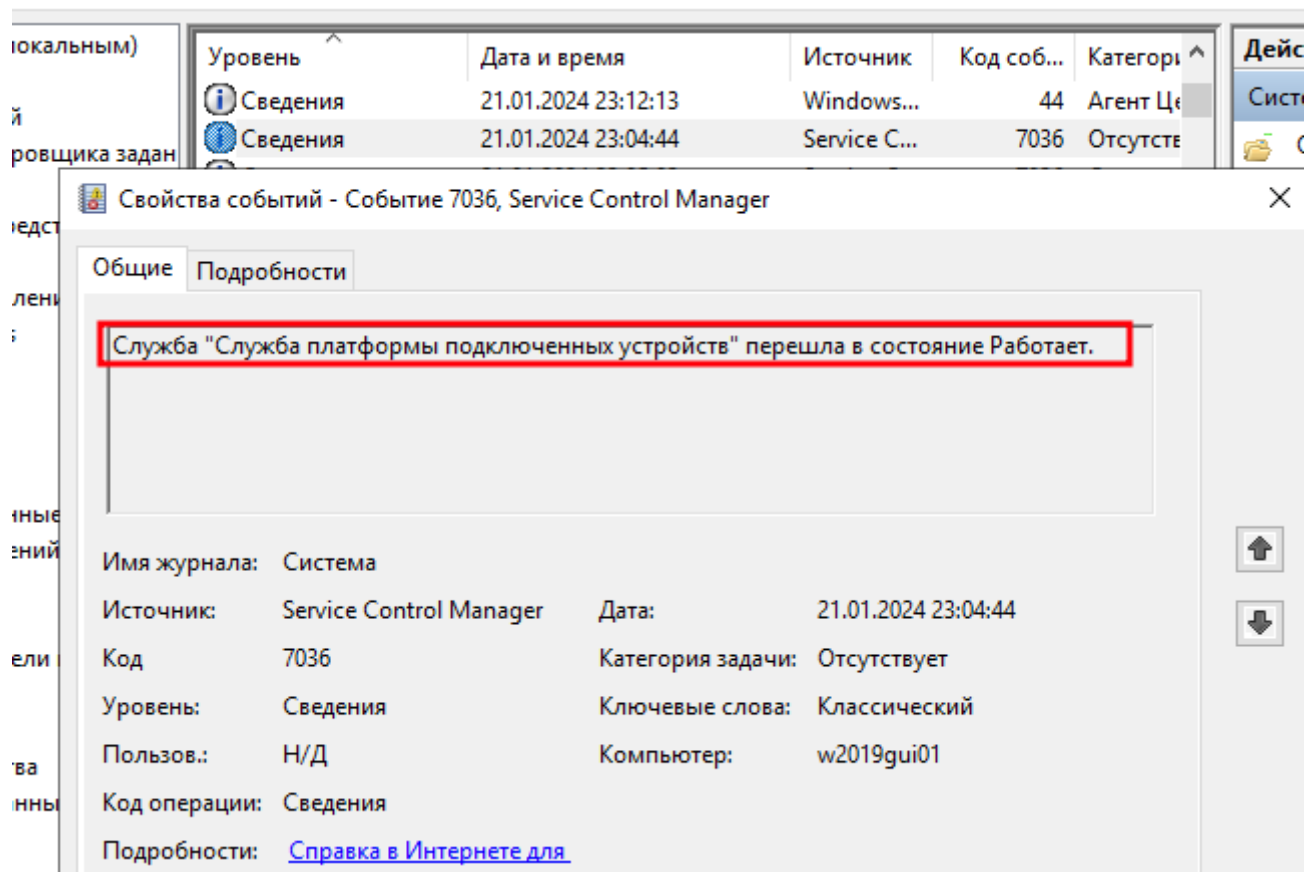
Уровень	Дата и время	Источник	Код соб...	Кategori...
Сведения	21.01.2024 22:50:44	Service C...	7040	Отсутств...
Сведения	21.01.2024 22:50:44	Service C...	7040	Отсутств...
Сведения	21.01.2024 22:50:44	Service C...	7040	Отсутств...
Сведения	22.01.2024 2:00:09	Service C...	7036	Отсутств...
Сведения	22.01.2024 0:02:01	Service C...	7036	Отсутств...
Сведения	22.01.2024 2:01:09	Service C...	7036	Отсутств...
Сведения	22.01.2024 2:00:41	Service C...	7036	Отсутств...
Сведения	22.01.2024 0:02:01	Service C...	7036	Отсутств...
Сведения	22.01.2024 2:00:09	Service C...	7036	Отсутств...
Сведения	22.01.2024 0:02:01	Service C...	7036	Отсутств...
Сведения	22.01.2024 0:02:16	Service C...	7036	Отсутств...
Сведения	22.01.2024 0:02:01	Service C...	7036	Отсутств...
Сведения	22.01.2024 0:02:01	Service C...	7036	Отсутств...
Сведения	22.01.2024 2:00:04	Service C...	7036	Отсутств...
Сведения	22.01.2024 0:02:16	Service C...	7036	Отсутств...
Сведения	22.01.2024 0:02:01	Service C...	7036	Отсутств...
Сведения	22.01.2024 0:02:01	Service C...	7036	Отсутств...
Сведения	22.01.2024 1:25:02	Service C...	7036	Отсутств...

Событие 7036, Service Control Manager

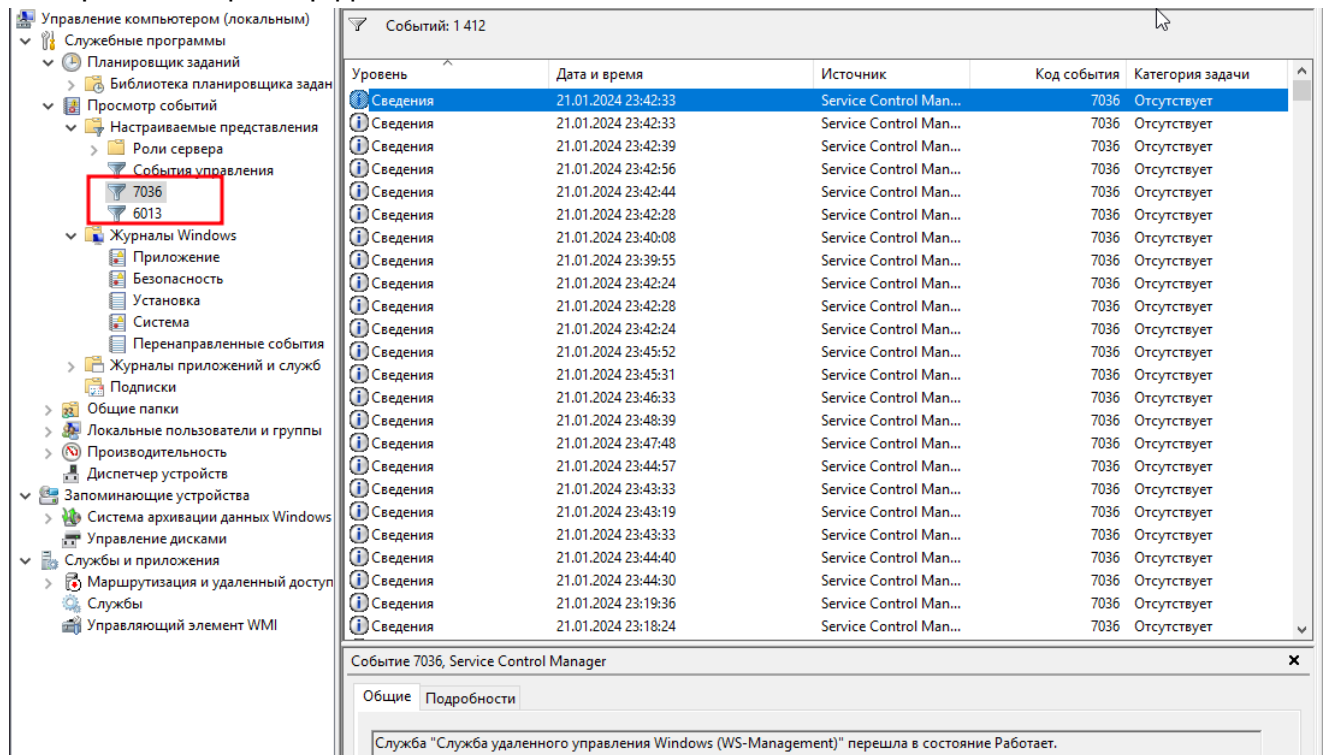
Общие Подробности

Действия

- Система
 - Открыть сохраненны...
 - Создать настраиваем...
 - Импорт настраиваем...
 - Очистить журнал...
 - Фильтр текущего жур...
 - Свойства
 - Найти...
 - Сохранить все событи...
 - Привязать задачу к жу...
- Вид
- Обновить
- Справка
- Событие 7036, Service Con...
- Свойства событий
- Привязать задачу к со...
- Копировать



Настраиваем фильтр для событий 6013 и 7036



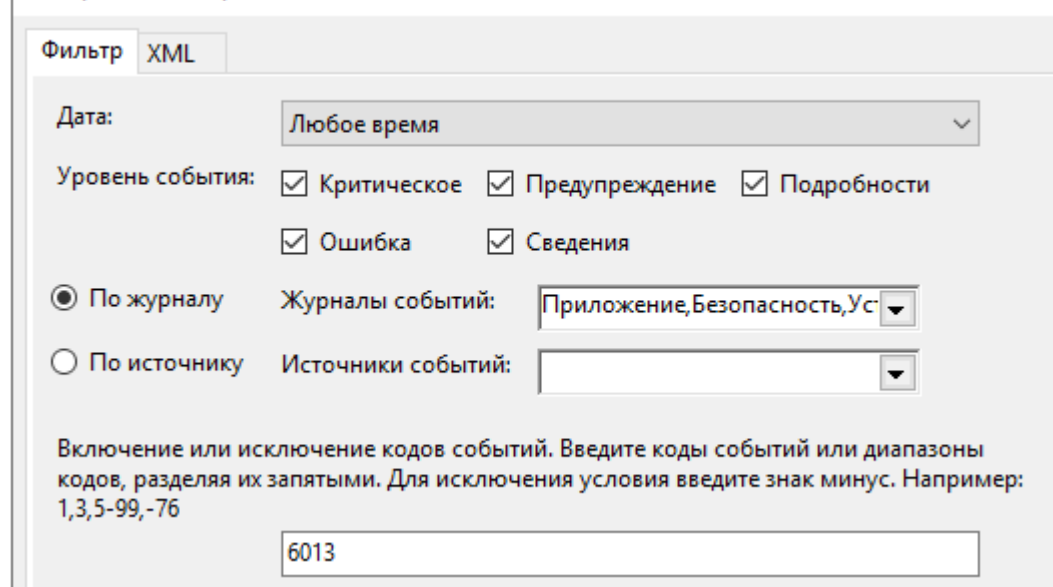
Уровень	Дата и время	Источник	Код события	Категория задачи
Сведения	21.01.2024 23:42:33	Service Control Man...	7036	Отсутствует
Сведения	21.01.2024 23:42:33	Service Control Man...	7036	Отсутствует
Сведения	21.01.2024 23:42:39	Service Control Man...	7036	Отсутствует
Сведения	21.01.2024 23:42:56	Service Control Man...	7036	Отсутствует
Сведения	21.01.2024 23:42:44	Service Control Man...	7036	Отсутствует
Сведения	21.01.2024 23:42:28	Service Control Man...	7036	Отсутствует
Сведения	21.01.2024 23:40:08	Service Control Man...	7036	Отсутствует
Сведения	21.01.2024 23:39:55	Service Control Man...	7036	Отсутствует
Сведения	21.01.2024 23:42:24	Service Control Man...	7036	Отсутствует
Сведения	21.01.2024 23:42:28	Service Control Man...	7036	Отсутствует
Сведения	21.01.2024 23:42:24	Service Control Man...	7036	Отсутствует
Сведения	21.01.2024 23:45:52	Service Control Man...	7036	Отсутствует
Сведения	21.01.2024 23:45:31	Service Control Man...	7036	Отсутствует
Сведения	21.01.2024 23:46:33	Service Control Man...	7036	Отсутствует
Сведения	21.01.2024 23:48:39	Service Control Man...	7036	Отсутствует
Сведения	21.01.2024 23:47:48	Service Control Man...	7036	Отсутствует
Сведения	21.01.2024 23:44:57	Service Control Man...	7036	Отсутствует
Сведения	21.01.2024 23:44:33	Service Control Man...	7036	Отсутствует
Сведения	21.01.2024 23:43:19	Service Control Man...	7036	Отсутствует
Сведения	21.01.2024 23:43:33	Service Control Man...	7036	Отсутствует
Сведения	21.01.2024 23:44:40	Service Control Man...	7036	Отсутствует
Сведения	21.01.2024 23:44:30	Service Control Man...	7036	Отсутствует
Сведения	21.01.2024 23:19:36	Service Control Man...	7036	Отсутствует
Сведения	21.01.2024 23:18:24	Service Control Man...	7036	Отсутствует

Событие 7036, Service Control Manager

Общие Подробности

Служба "Служба удаленного управления Windows (WS-Management)" перешла в состояние Работает.

Настраиваемое представление свойств



Фильтр XML

Дата: Любое время

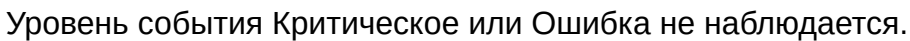
Уровень события: ☒ Критическое ☒ Предупреждение ☒ Подробности
☒ Ошибка ☒ Сведения

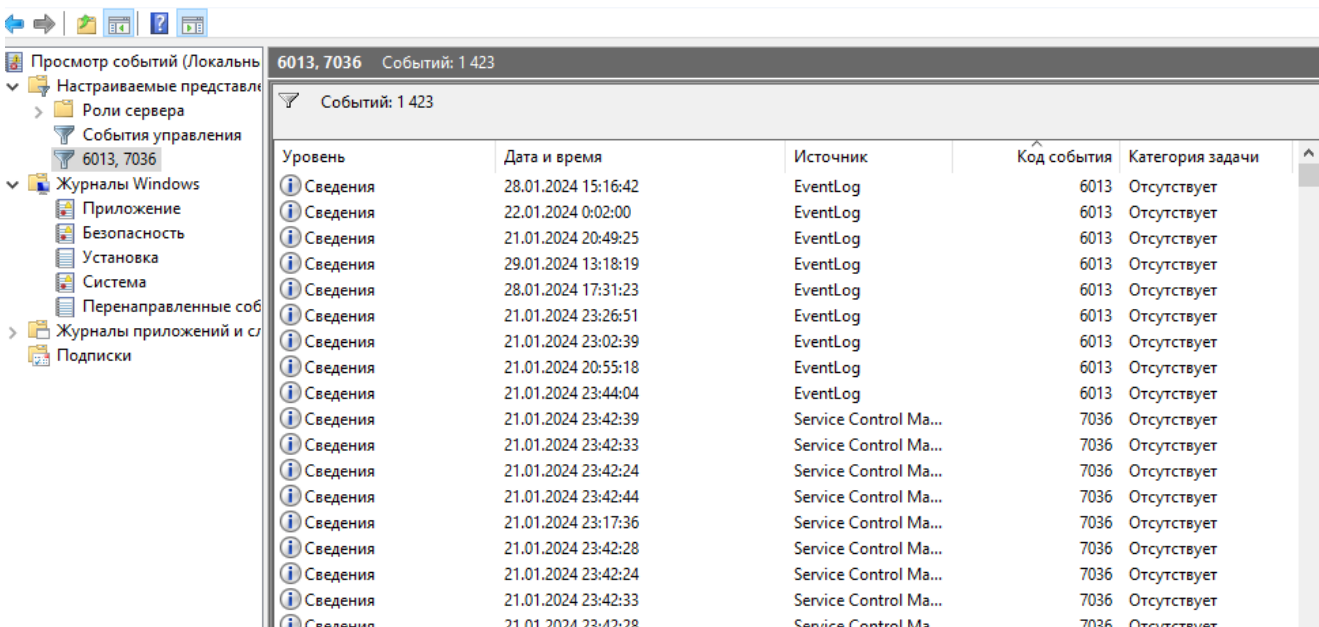
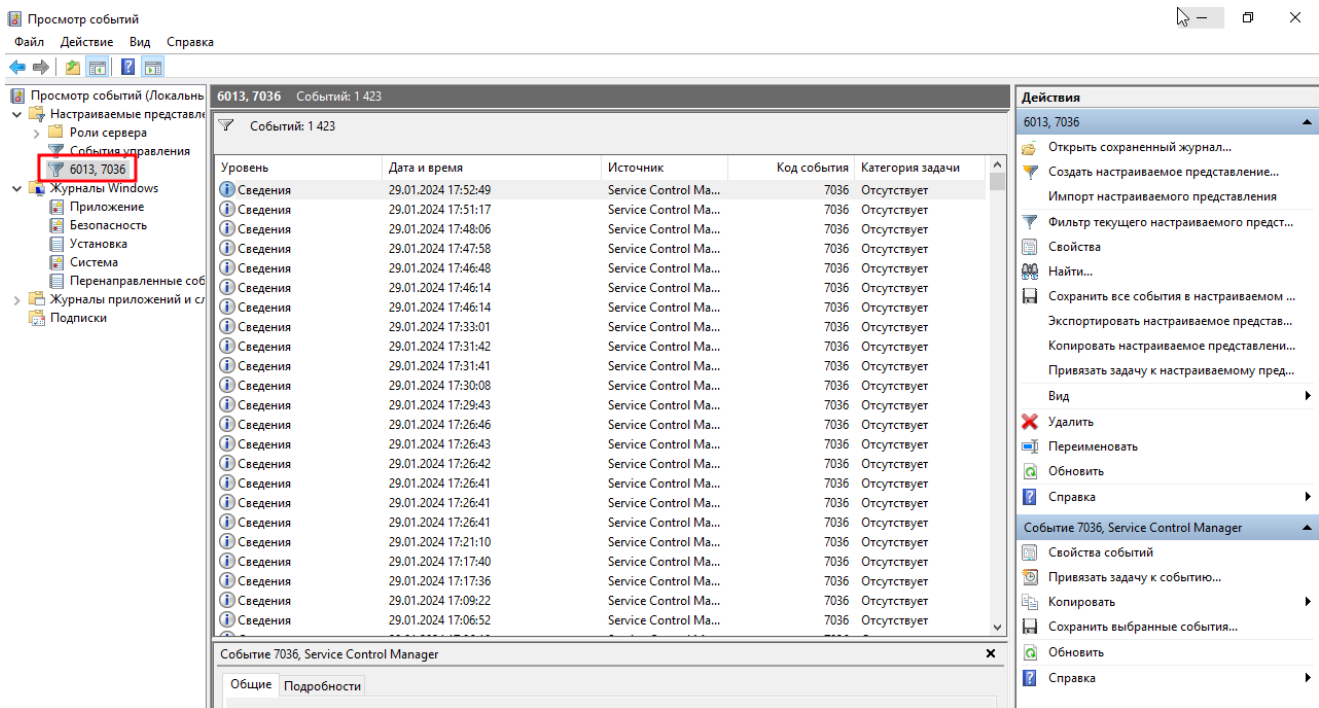
☒ По журналу Журналы событий: Приложение,Безопасность,Ус

☐ По источнику Источники событий:

Включение или исключение кодов событий. Введите коды событий или диапазоны кодов, разделяя их запятыми. Для исключения условия введите знак минус. Например: 1,3,5-99,-76

6013





Задание_9:

Создайте задание, которое будет в 14.00 в рабочие дни запускать команду ping 8.8.8.8

Общие Триггеры Действия Условия Параметры Журнал (отключен)

Имя: ping 8.8.8.8

Размещение: \

Автор: W2019GUI01\Администратор

Описание:

Параметры безопасности

При выполнении задачи использовать следующую учетную запись пользователя:

Администратор

Изменить...

☒ Выполнять только для пользователей, вошедших в систему

☐ Выполнять для всех пользователей

☐ Не сохранять пароль. Будут доступны ресурсы только локального компьютера.

☒ Выполнить с наивысшими правами

☐ Скрытая задача

Настроить для: Windows Vista™, Windows Server™ 2008

Общие **Триггеры** Действия Условия Параметры

Создание триггера

Начать задачу: По расписанию

Параметры

☐ Однократно

☒ Ежедневно

☐ Еженедельно

☐ Ежемесячно

Начать: 21.01.2024



14:00:00

☐ Синхр. по поясам

Повторять каждые: 1 дн.

Дополнительные параметры

☐ Отложить задачу на (произвольная задержка): 1 ч.

☐ Повторять задачу каждые: 1 ч.

в течение: 1 д.

☐ Останавливать все задачи по истечении срока повторов

☐ Остановить задачу через:

3 дн.

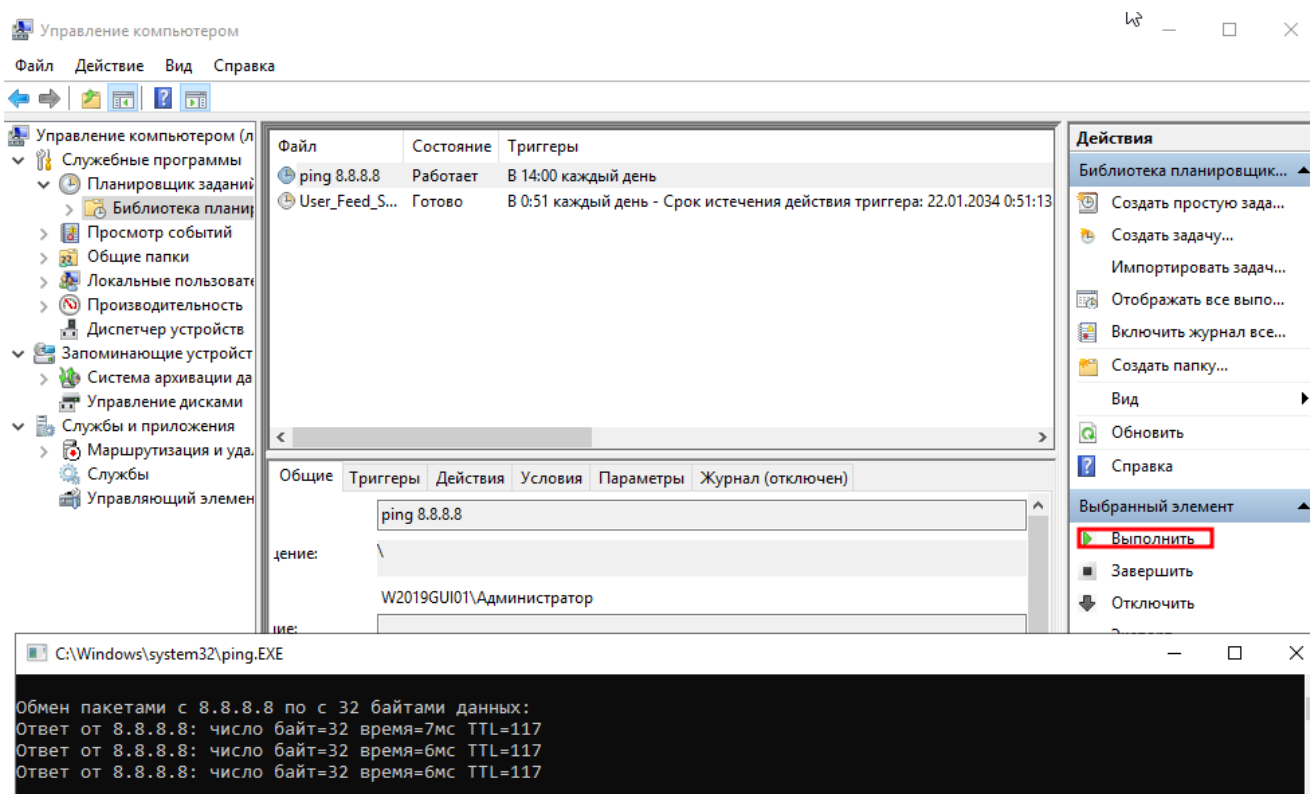
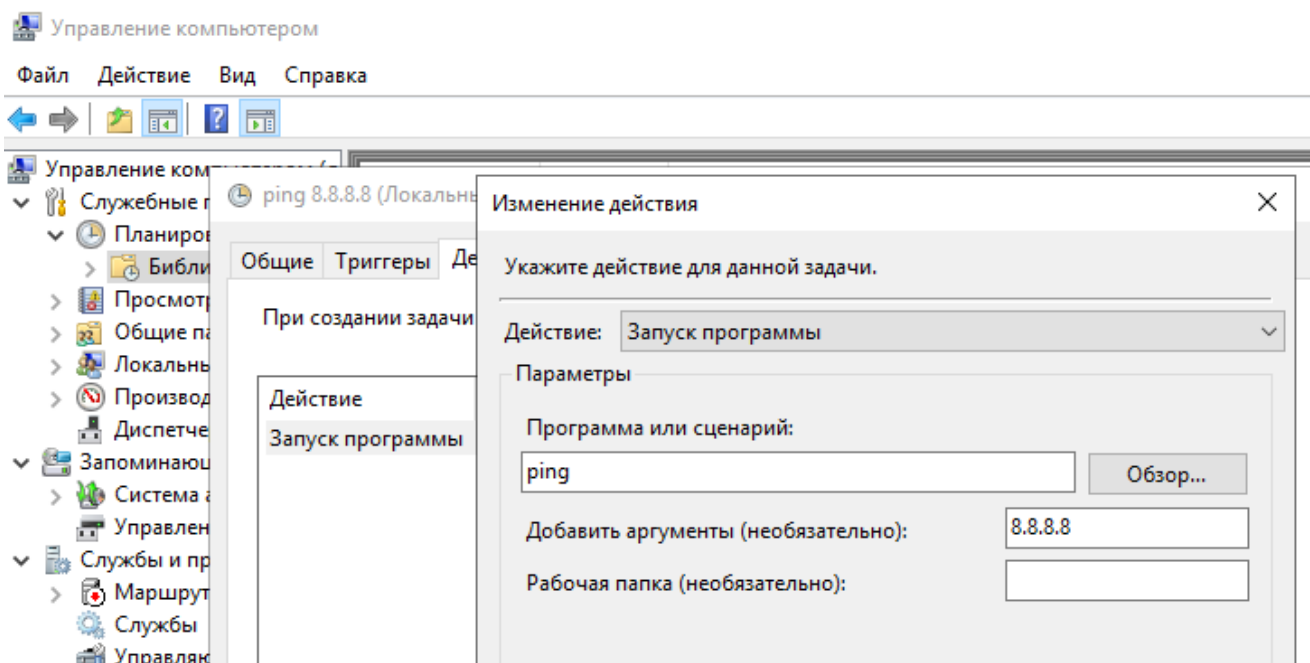
☐ Срок действия:

21.01.2025

20:17:31

☐ Синхр. по поясам

☒ Включено

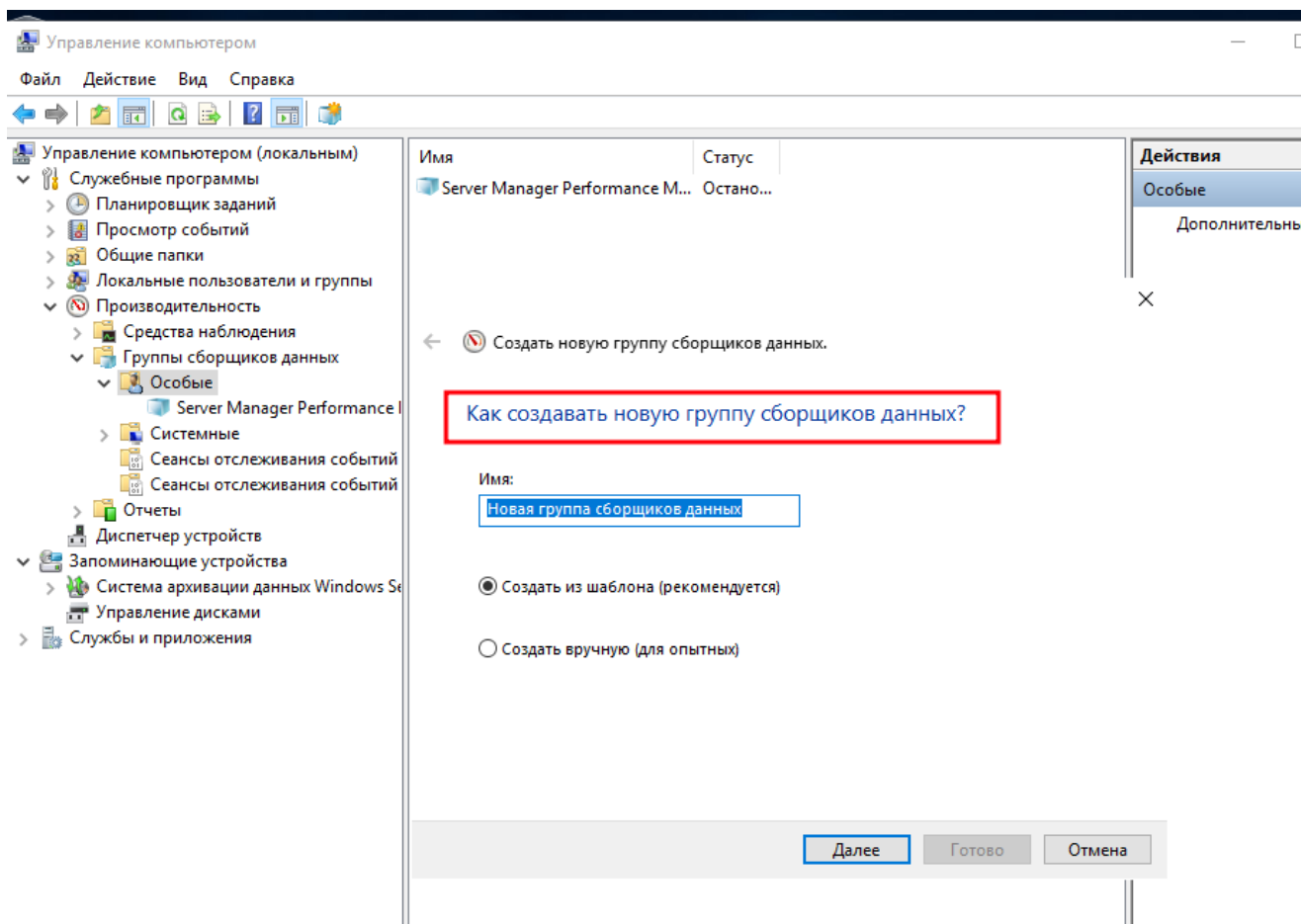


Или задаем:

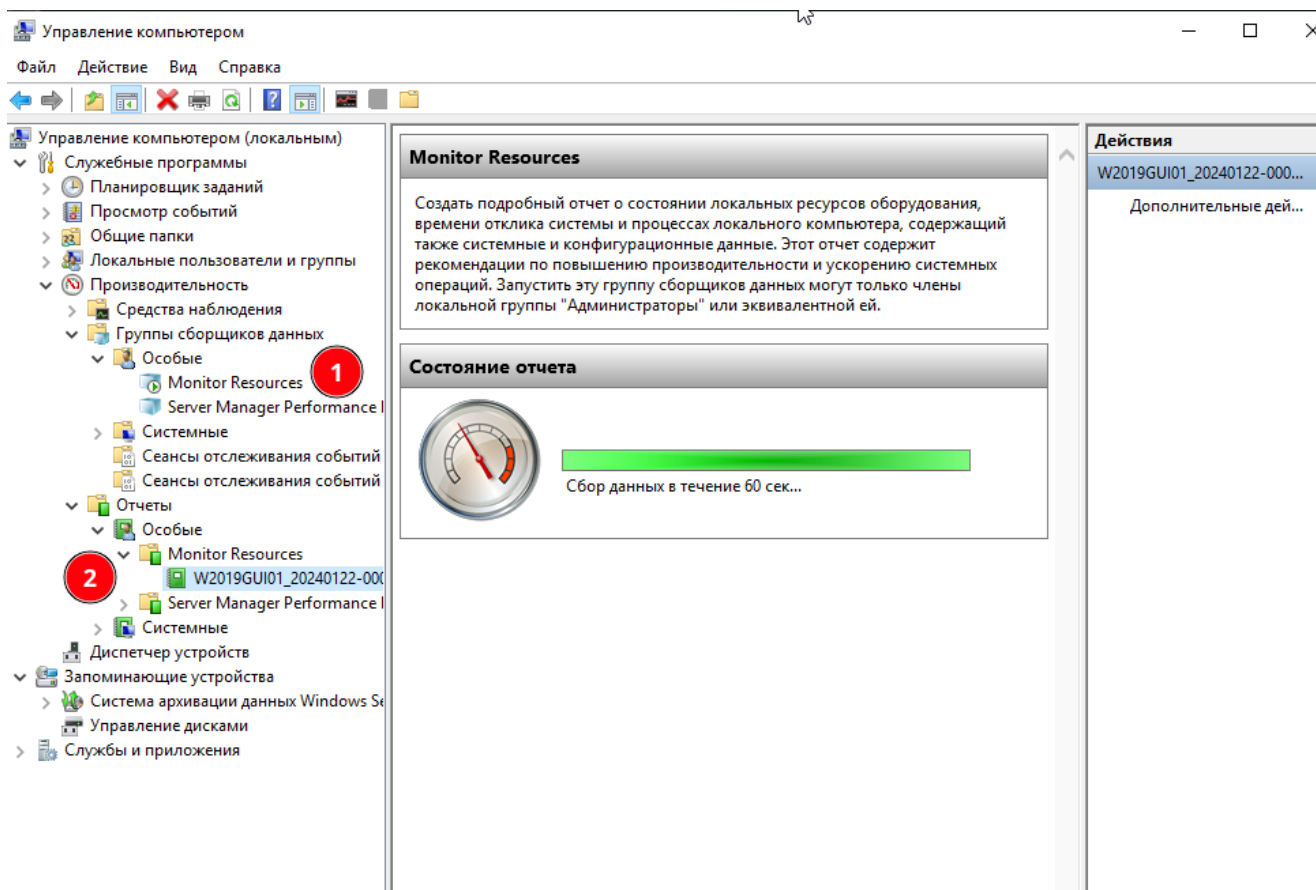
ping -n 8.8.8.8

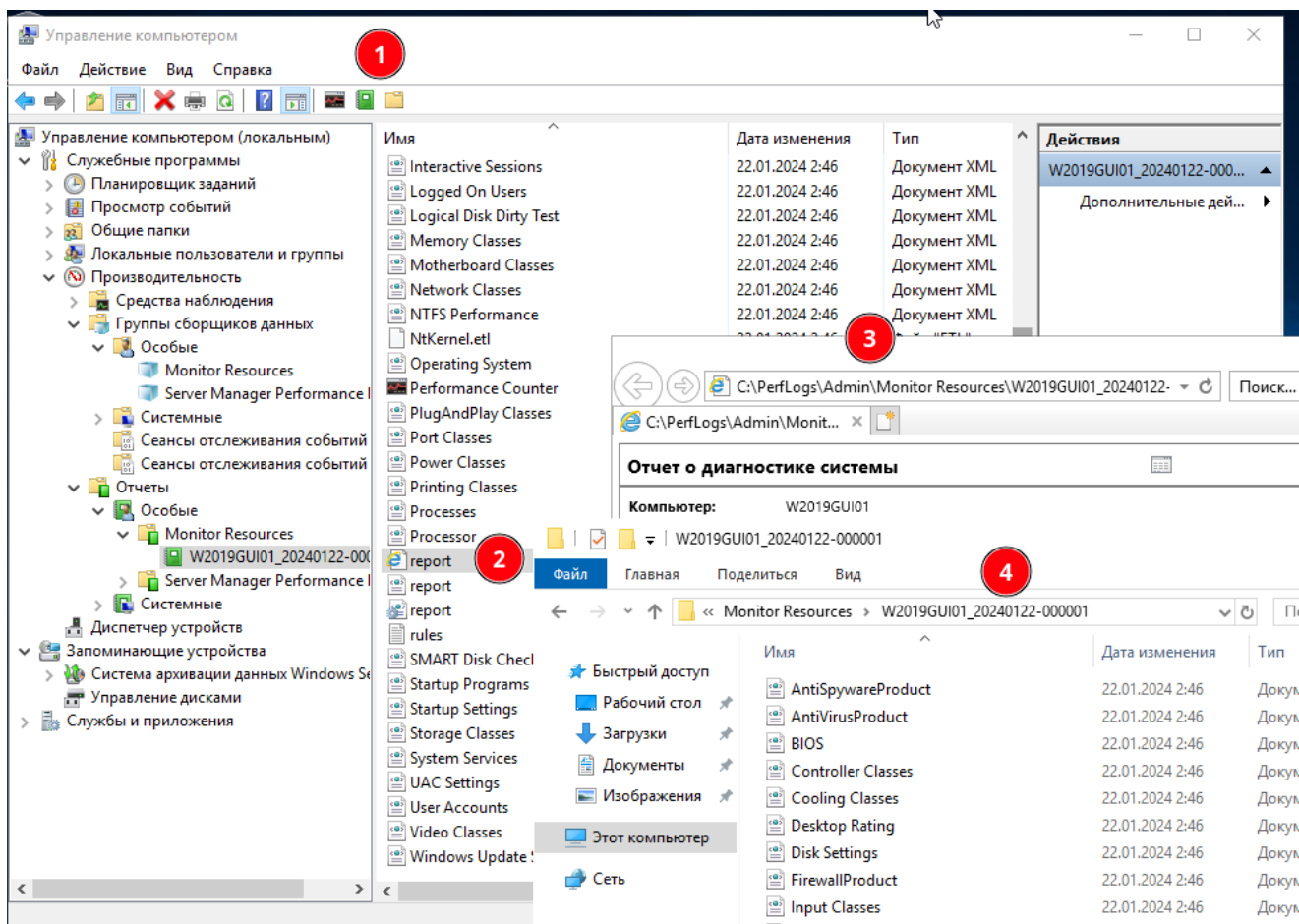
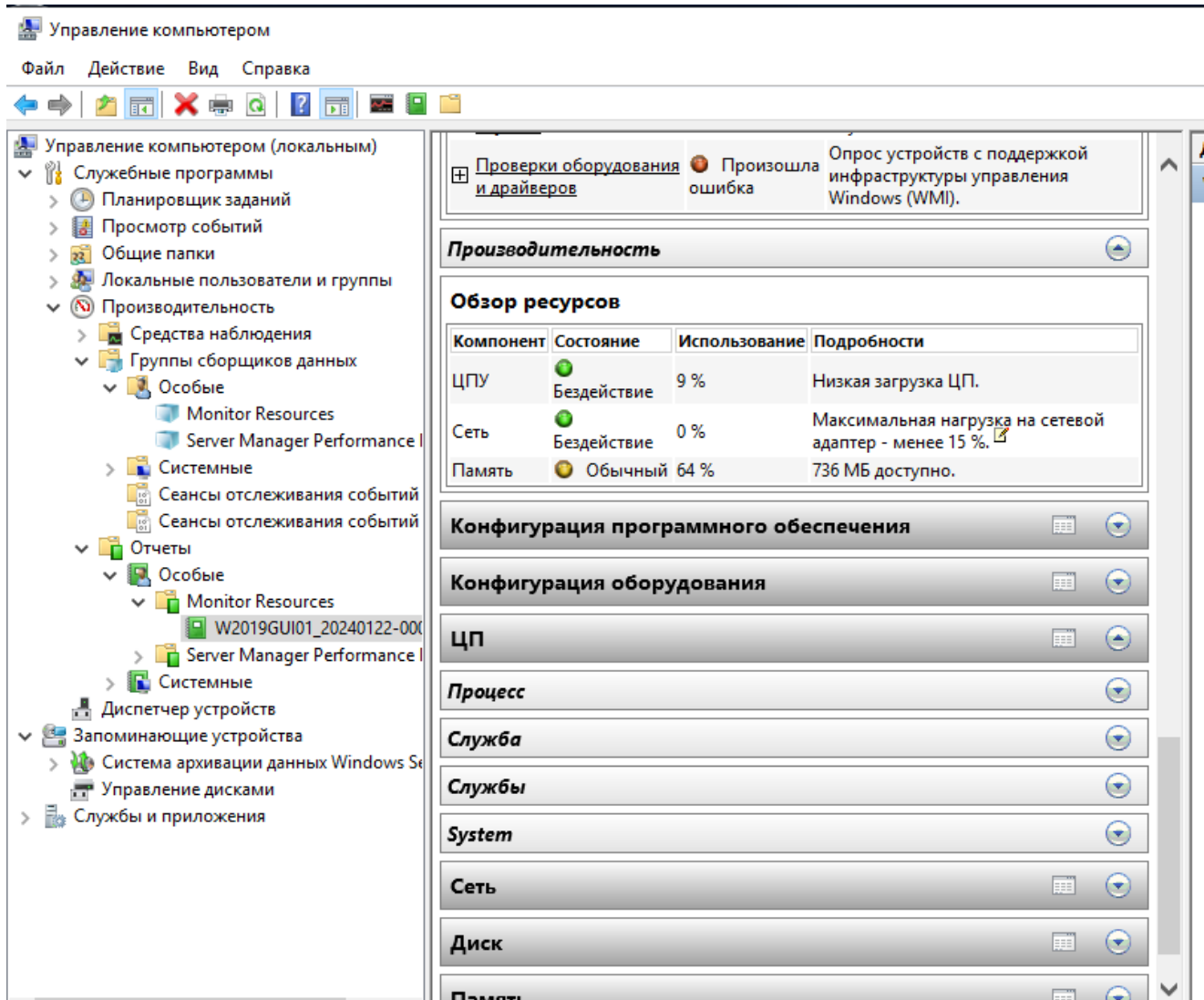
Задание_10:

Промониторьте через Системный монитор загрузку процессора и пришлите лог



- Выбираем нужное ...
- Запускаем





Задание_11:

Через Монитор ресурсов просмотрите в разделе Диск-Процессы с дисковой активностью-System какие используются файлы

The first image shows the Windows Administrative Tools window. The 'Resource Monitor' link is highlighted in the left sidebar. The main pane lists various system utilities, with 'Resource Monitor' selected and highlighted by a red rectangle.

The second image is a detailed view of the Resource Monitor window. The 'Disk' tab is selected, showing the following data:

Процессы с дисковой активностью				
Образ	ИД п...	Чтение (байт/с)	Запись (байт/с)	Всего (байт/с)
System	4	0	6 460	6 460
perfmom.exe	3956	25 839	0	25 839
Registry	88	0	2 985	2 985
svchost.exe (...)	1404	1 792	0	1 792

Работа диска							
Отфильтровано по: System							
Образ	ИД процесса	Файл	Чтение (байт/с)	Запись (байт/с)	Всего (байт/с)	Приоритет...	Время отв...
System	4	C:\Windows\System...	0	1 703	1 703	Обычный	0
System	4	C:\ProgramData\M...	0	2 114	2 114	Обычный	0
System	4	C:\ProgramData\M...	0	216	216	Обычный	0
System	4	C:\LogFile (Журн...	0	2 321	2 321	Обычный	0
System	4	C:\Mft (Основная...	0	750	750	Обычный	0
System	4	C:\Windows\System...	0	512	512	Обычный	0
System	4	C:\Windows\System...	0	186	186	Обычный	0
System	4	C:\Windows\Servic...	0	120	120	Обычный	0
System	4	C:\\$Extend\$\UsrJr...	0	120	120	Обычный	0
System	4	C:\\$BitMap (Карта ...)	0	272	272	Обычный	0
System	4	C:\Users\Админис...	0	174	174	Обычный	0

Запоминающие устройства					
Логический д...	Физически...	Активное ...	Свободно ...	Всего (MB)	Длина оче...
C:	0	0.01	26 781	44 451	0.00

On the right side of the Resource Monitor window, there are two graphs: 'Disk' showing a peak in activity around 100 Kbit/s, and 'Disk Queue Length' showing a peak around 0.01.

Глоссарий

Том англ. Volume — часть долговременной памяти компьютера, рассматриваемая как единое целое для удобства работы. Понятие тома обеспечивает для операционной системы абстракцию от физического расположения данных: том может быть компакт-диском, выделен как раздел жёсткого диска, как пространство имен или раздел на

флеш-накопителе, как раздел RAID-массива или LUN сети хранения данных.

Operating system environment, сокр. OSE – экземпляр Windows, запущенный на компьютере, может быть физическим или виртуальным.

Original equipment manufacturer, сокр. OEM — компания, которая производит детали и оборудование, которые могут быть проданы другим производителям под другой торговой маркой.

Just a bunch of disks, сокр. JBOD — дисковый массив, в котором единое логическое пространство распределено по жёстким дискам последовательно. Просто пачка дисков.

Дополнительные материалы

1. Craig Zacker "Installation, Storage and Compute with Windows Server 2016"
2. Сравнение редакций <https://docs.microsoft.com/en-us/windows-server/get-started/2016-edition-comparison>
3. Описание Nano-сервера <https://docs.microsoft.com/ru-ru/windows-server/get-started/getting-started-with-nano-server>

Используемые источники

1. Версии Windows Server
https://en.wikipedia.org/wiki/List_of_Microsoft_Windows_versions
2. Полный список системных требований <https://docs.microsoft.com/en-us/windows-server/get-started/system-requirements>
3. Обзор лицензирования Windows server 2016
<https://download.microsoft.com/download/7/2/9/7290EA05-DC56-4BED-9400-138C5701F174/WS20>

Выполнил: AndreiM