

## Настройка политики безопасности Windows

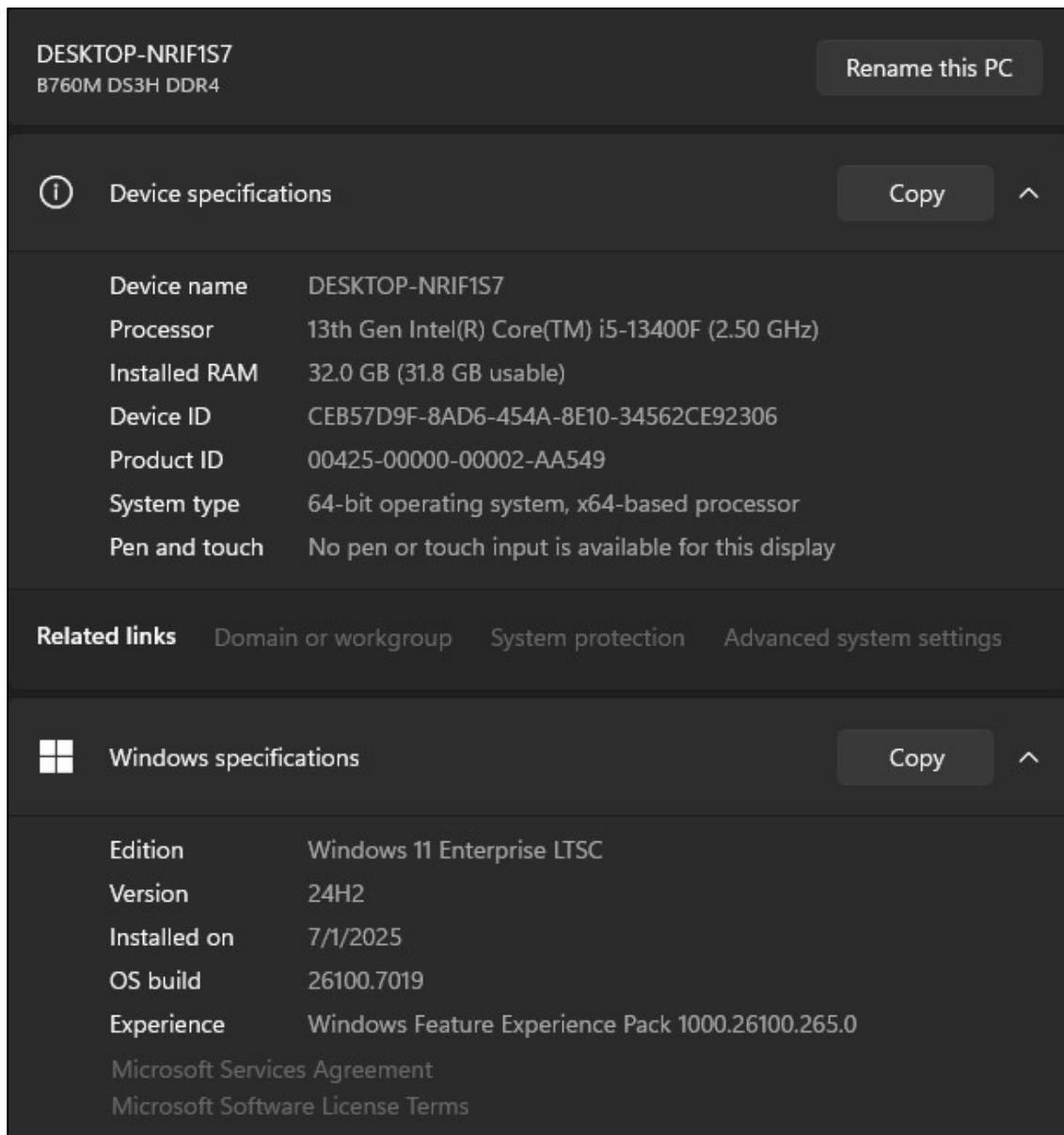


Рисунок 1 – О системе

### 1 Настройка реестра

Реестр Windows — центральное хранилище конфигурации. Настройка через regedit (с правами администратора).

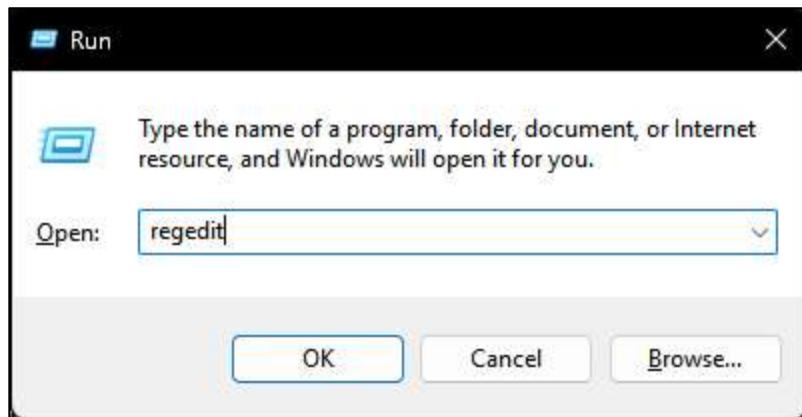


Рисунок 2 – Открываем реестр

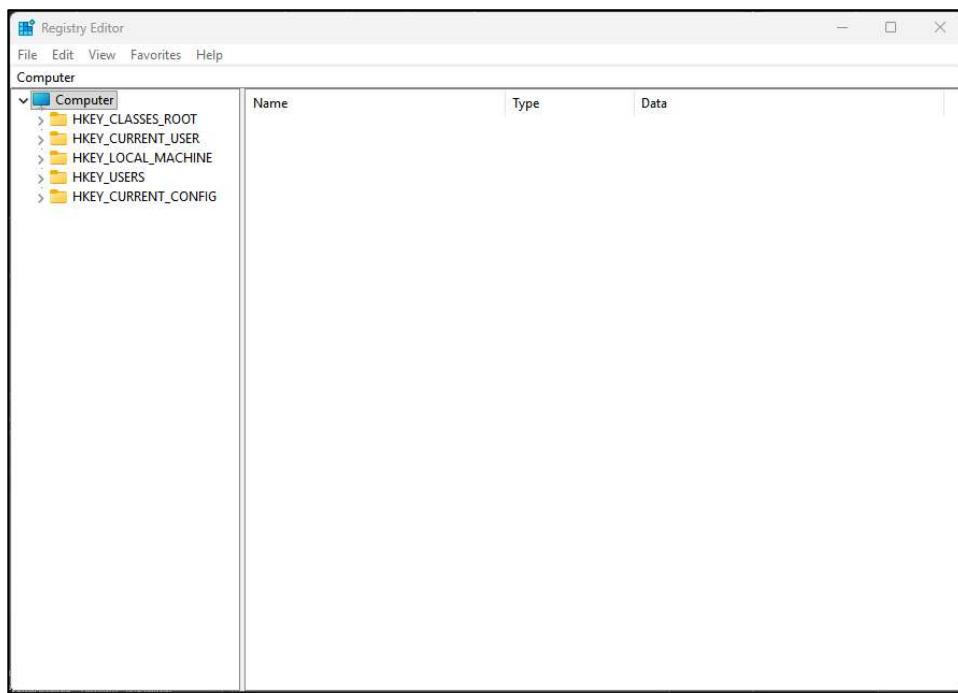


Рисунок 3 – Реестр Windows

Создаём резервную копию файла реестра (Файл → Экспорт).

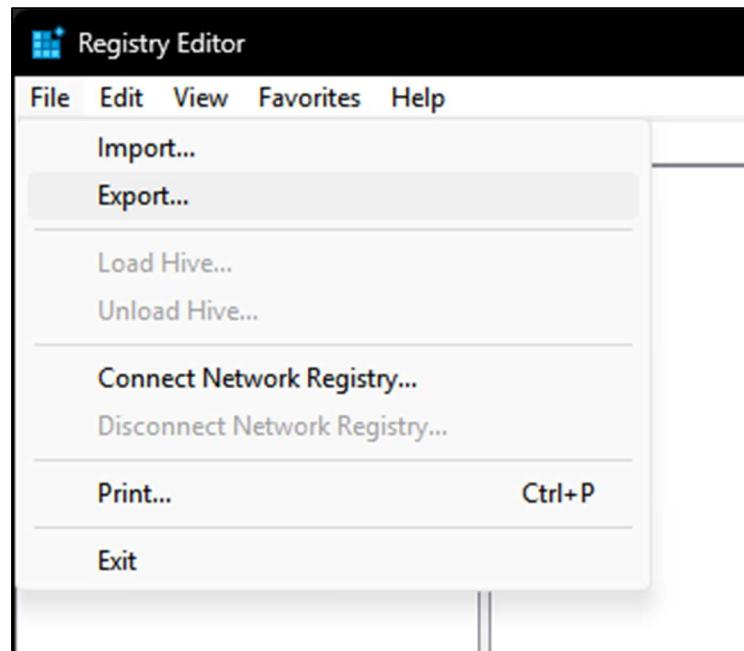


Рисунок 4 – Меню файл

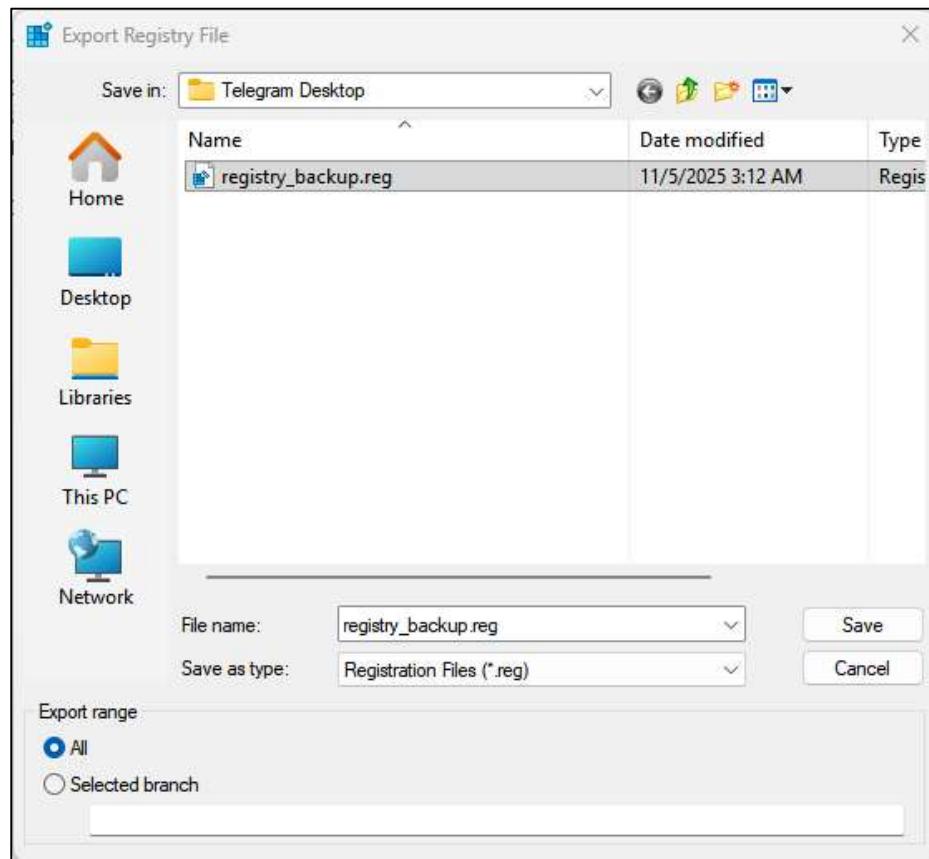


Рисунок 5 – Окно экспорта файла реестра

Отключение автозапуска с внешних носителей. Открываем Computer\HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\USBSTOR.

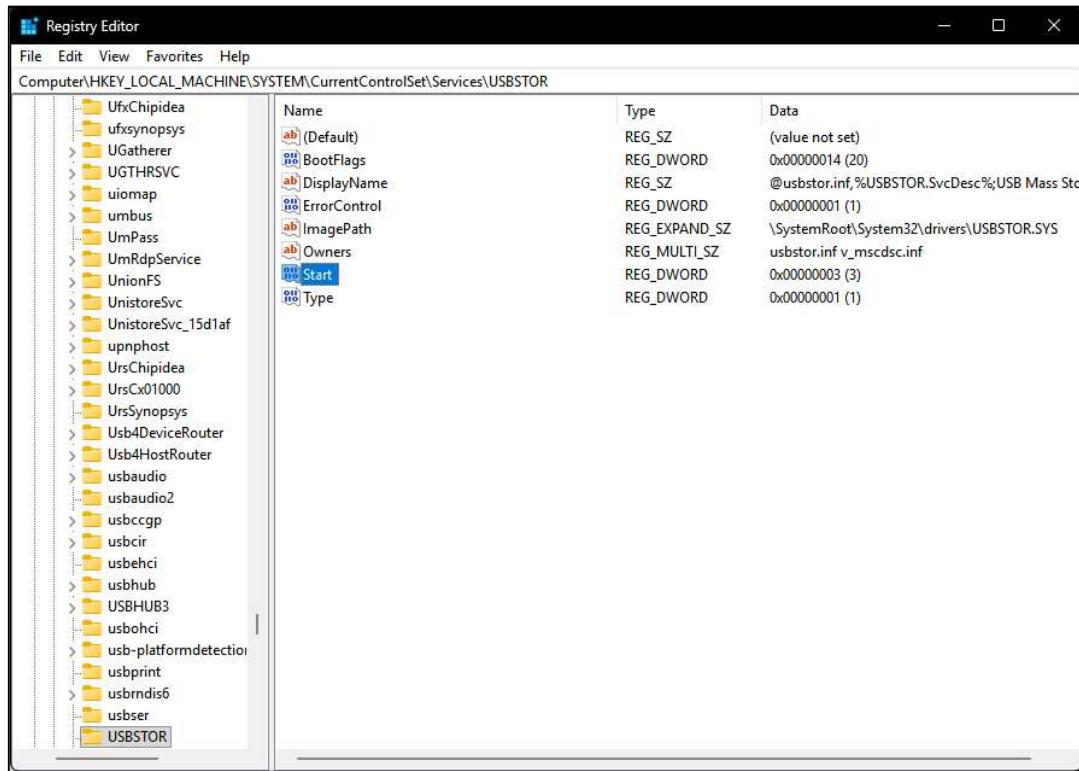


Рисунок 6 – Раздел USBSTOR

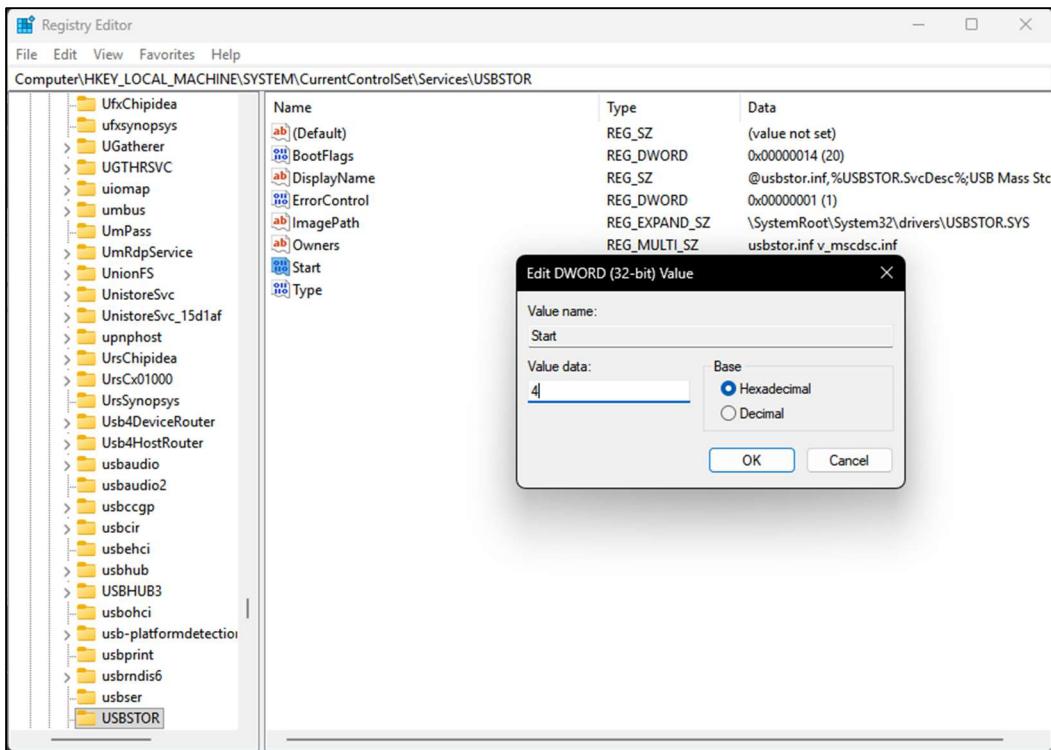


Рисунок 7 – Меняем значение Start на 4

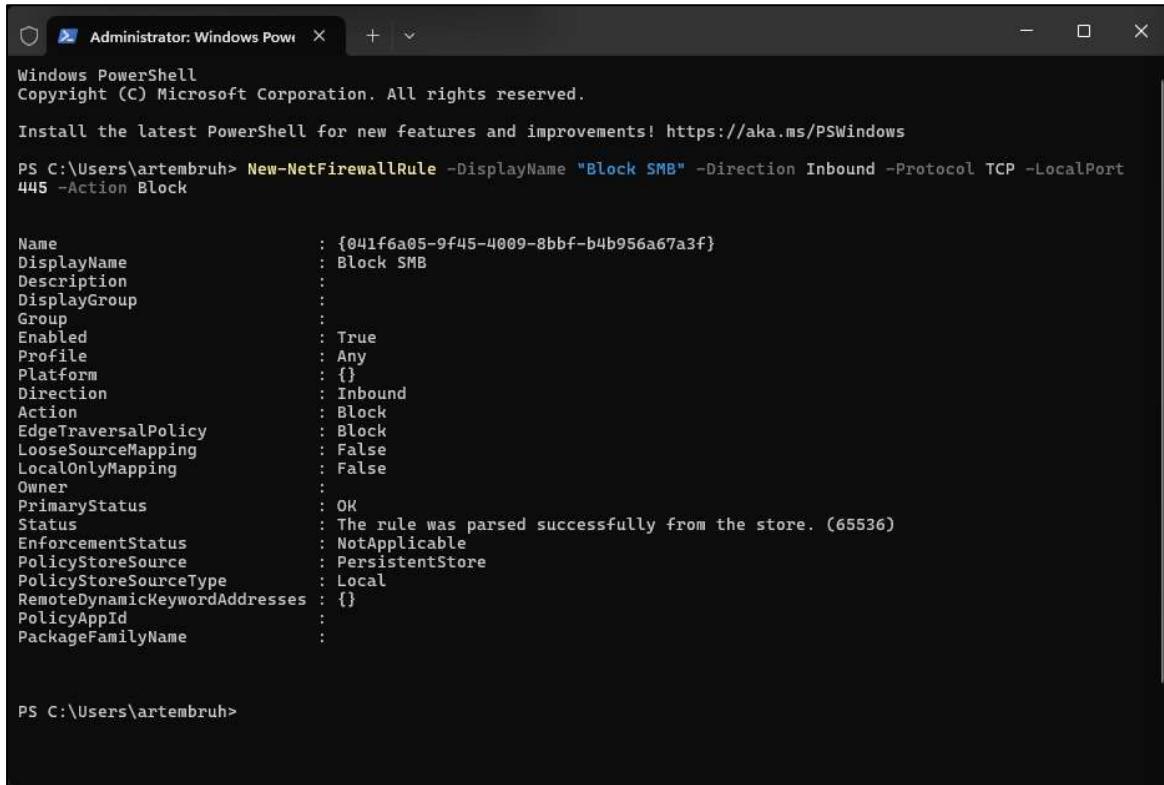
## 2 Настройка брандмауэра Windows

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\artembruh> Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled True
PS C:\Users\artembruh> |
```

Рисунок 8 – Включаем брандмауэр для всех профилей



```
Administrator: Windows Pow X + v
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\artembruh> New-NetFirewallRule -DisplayName "Block SMB" -Direction Inbound -Protocol TCP -LocalPort 445 -Action Block

Name : {041f6a05-9f45-4009-8bbf-b4b956a67a3f}
DisplayName : Block SMB
Description :
DisplayGroup :
Group :
Enabled : True
Profile : Any
Platform : {}
Direction : Inbound
Action : Block
EdgeTraversalPolicy : Block
LooseSourceMapping : False
LocalOnlyMapping : False
Owner :
PrimaryStatus : OK
Status : The rule was parsed successfully from the store. (65536)
EnforcementStatus : NotApplicable
PolicyStoreSource : PersistentStore
PolicyStoreSourceType : Local
RemoteDynamicKeywordAddresses : {}
PolicyAppId :
PackageName :

PS C:\Users\artembruh>
```

Рисунок 9 – Блокируем 445 порт который является целью Ransomware

### 3 Настройка служб Windows

Открыть cmd и ввести команду “services.msc” для открытия служб Windows.

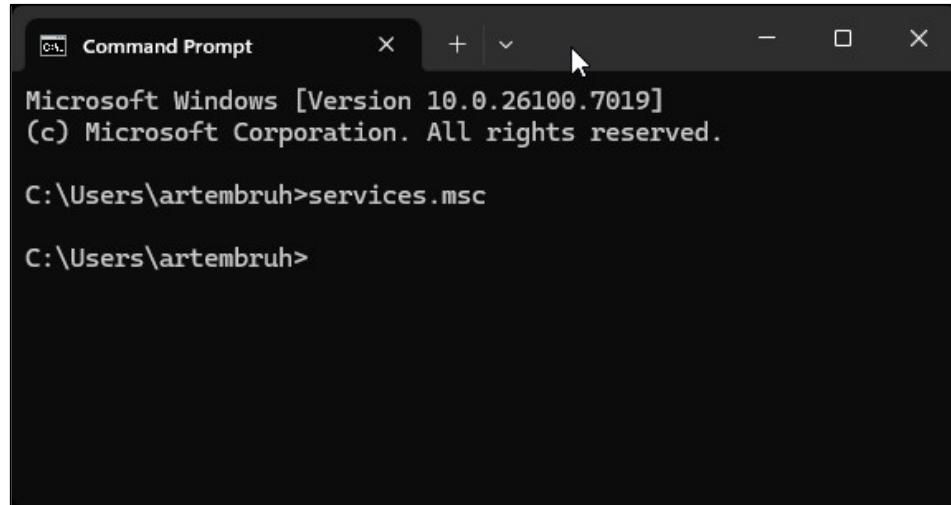


Рисунок 10 – Командная строка

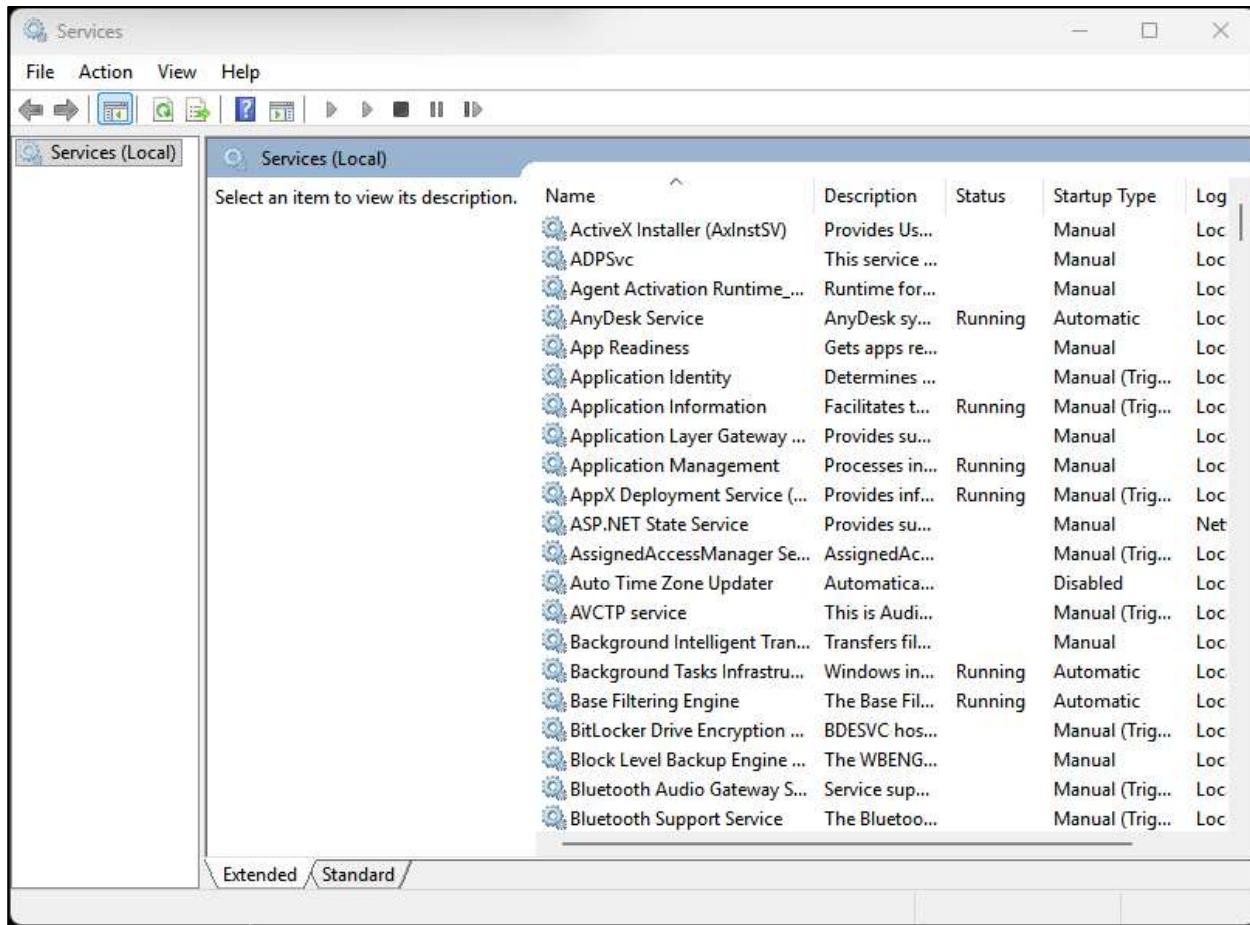


Рисунок 11 – Службы Windows

Отключаем не нужные службы, такие как “Print Spooler”

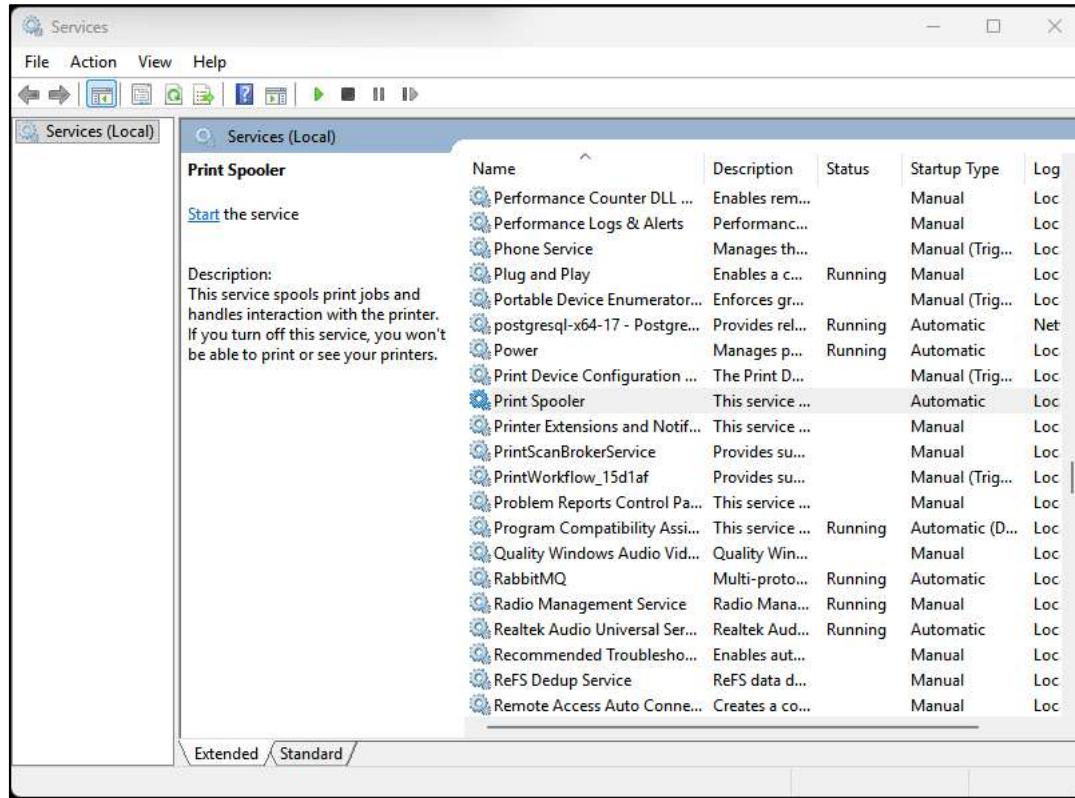


Рисунок 12 – Отключаем службу

## Вывод

Мы настроили реестр и брандмауэр, а также выключили не нужные службы.