

Настройка политики безопасности Windows

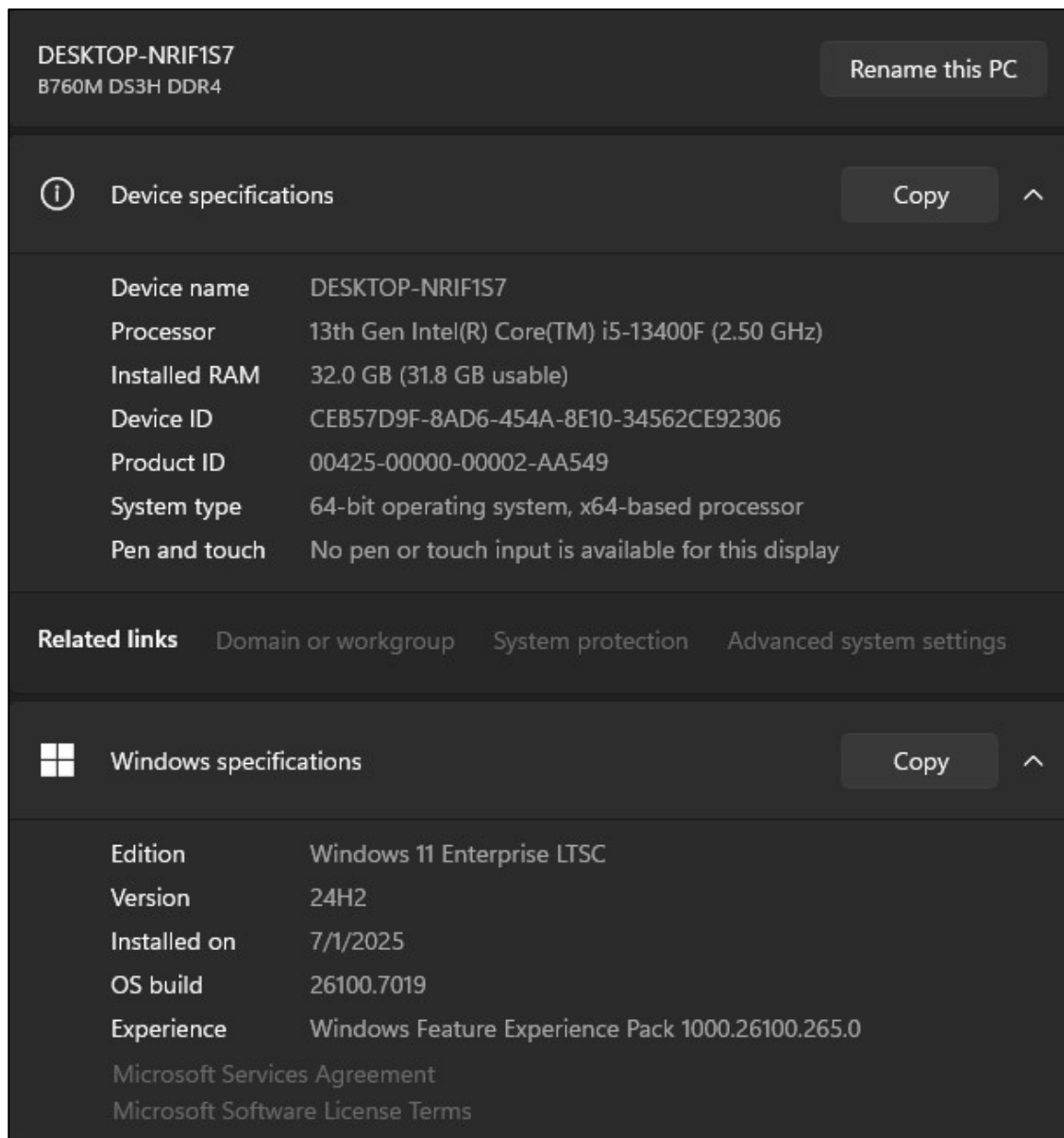


Рисунок 1 – О системе

1 Настройка реестра

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

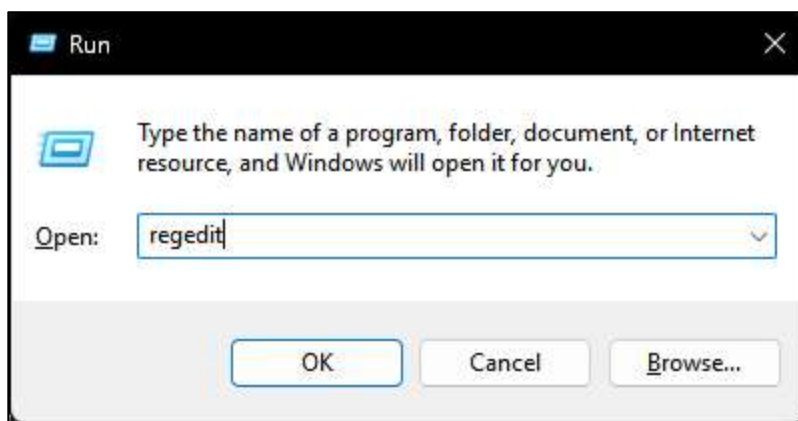


Рисунок 2 – Открываем реестр

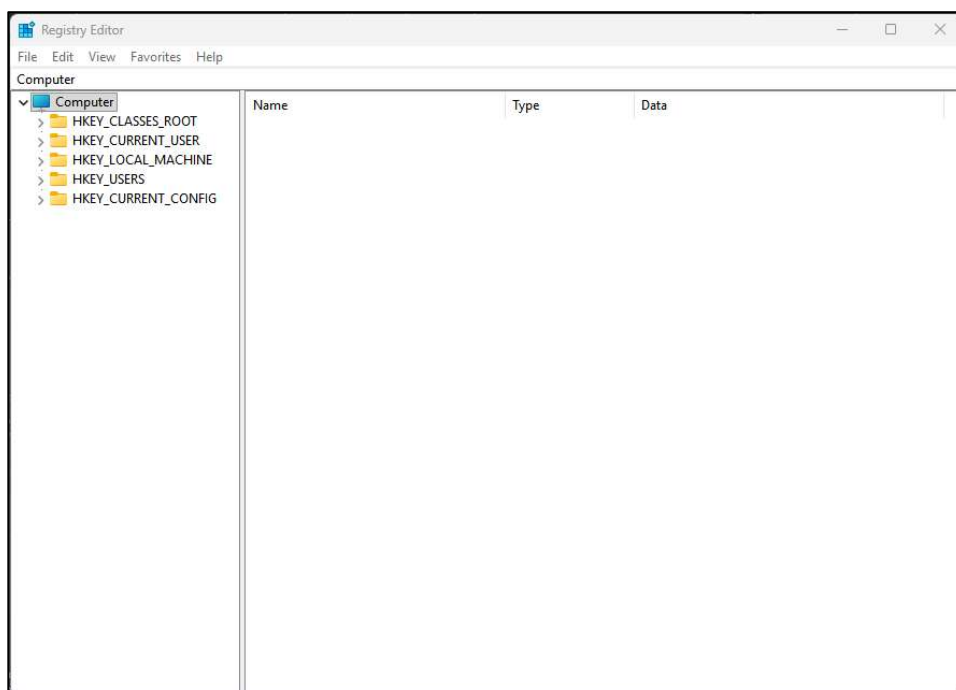


Рисунок 3 – Реестр Windows

Создаём резервную копию файла реестра (Файл → Экспорт).

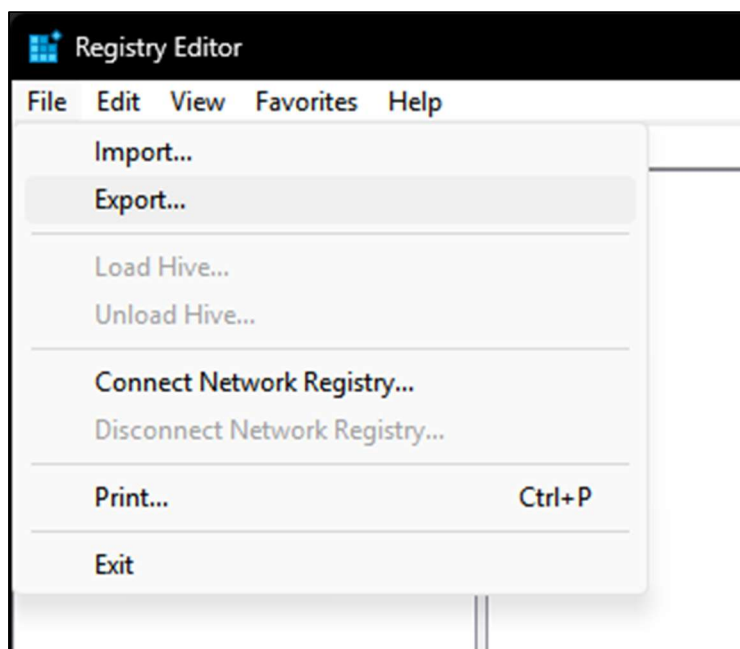


Рисунок 4 – Меню файл

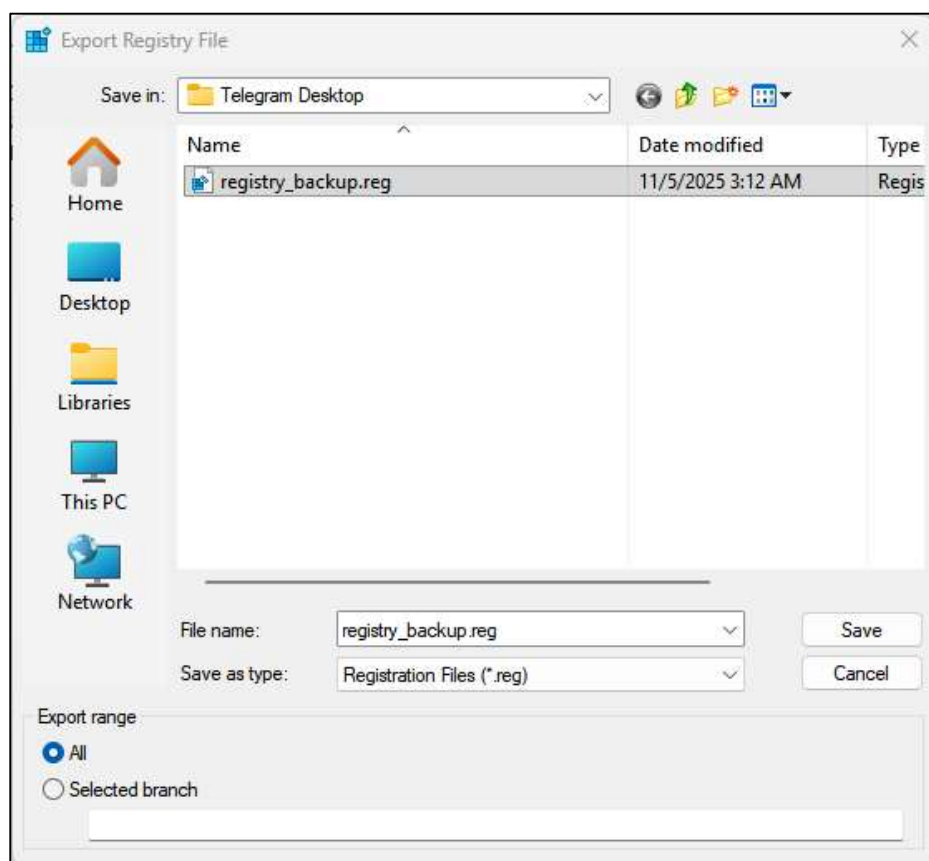


Рисунок 5 – Окно экспорта файла реестра

Отключение автозапуска с внешних носителей. Открываем Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\USBSTOR.

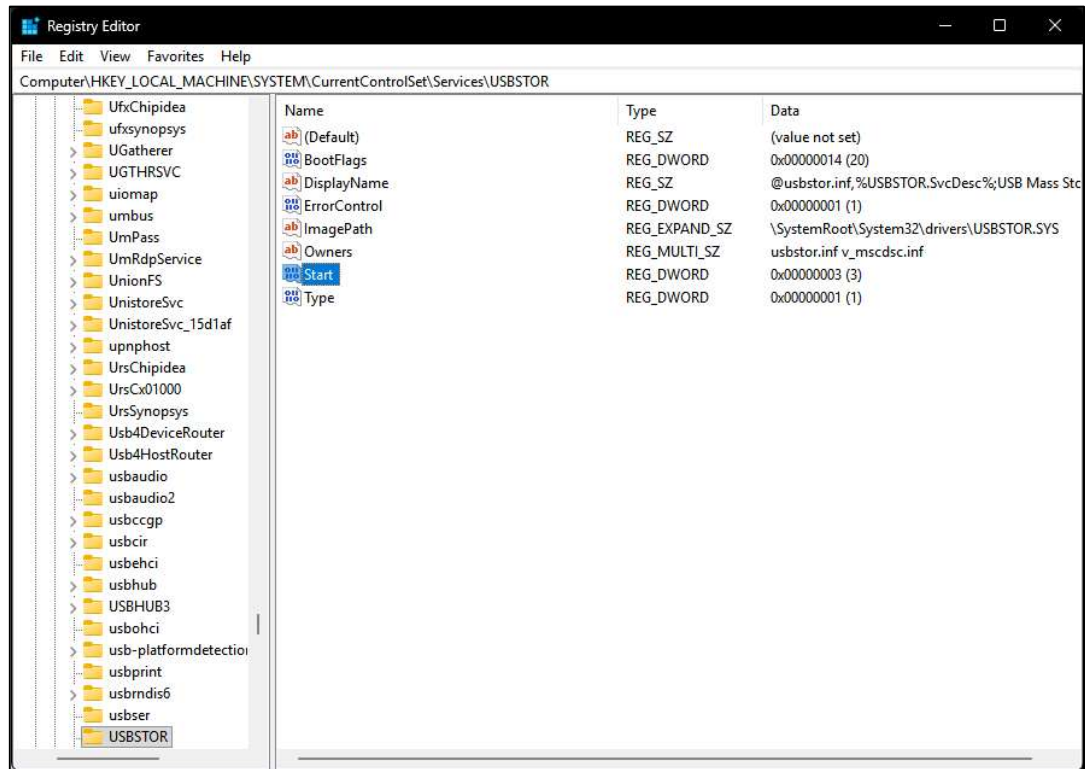


Рисунок 6 – Раздел USBSTOR

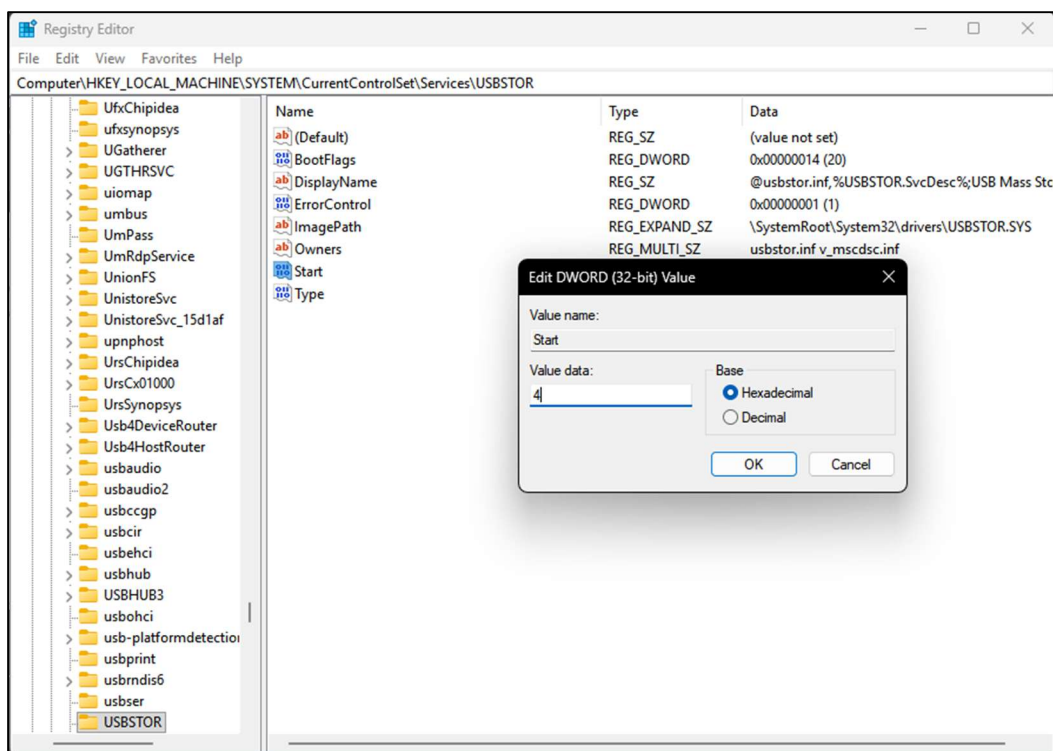


Рисунок 7 – Меняем значение Start на 4

2 Настройка брандмауэра Windows

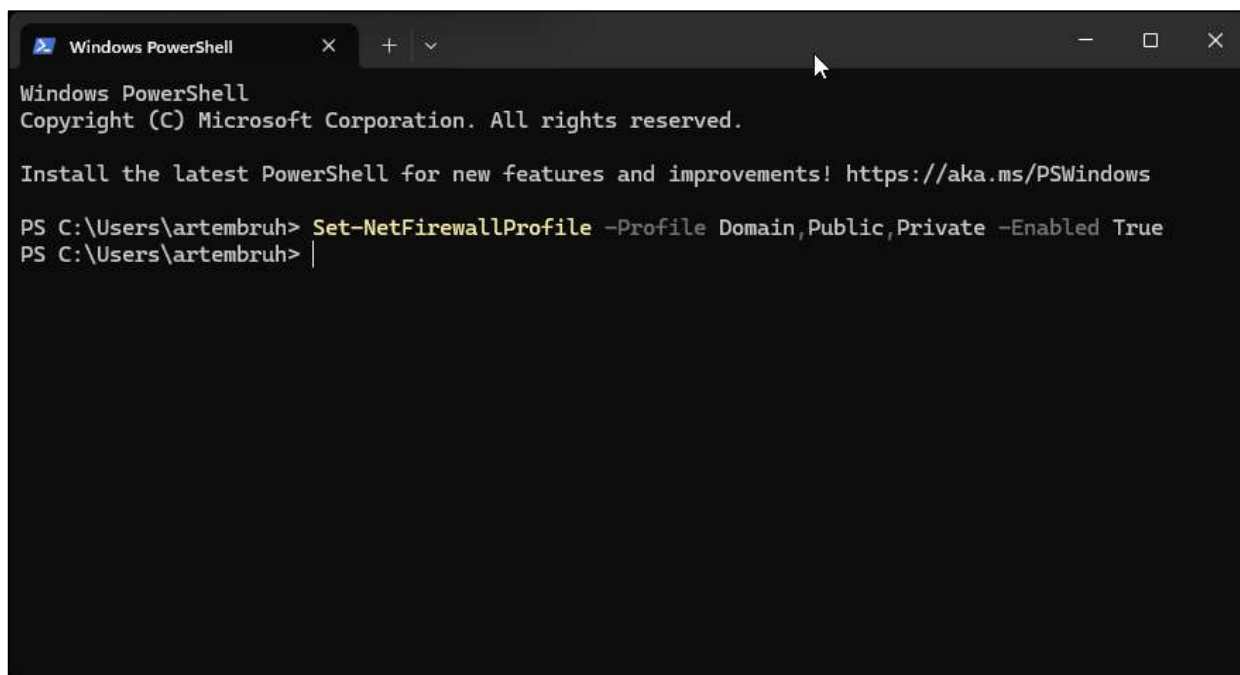
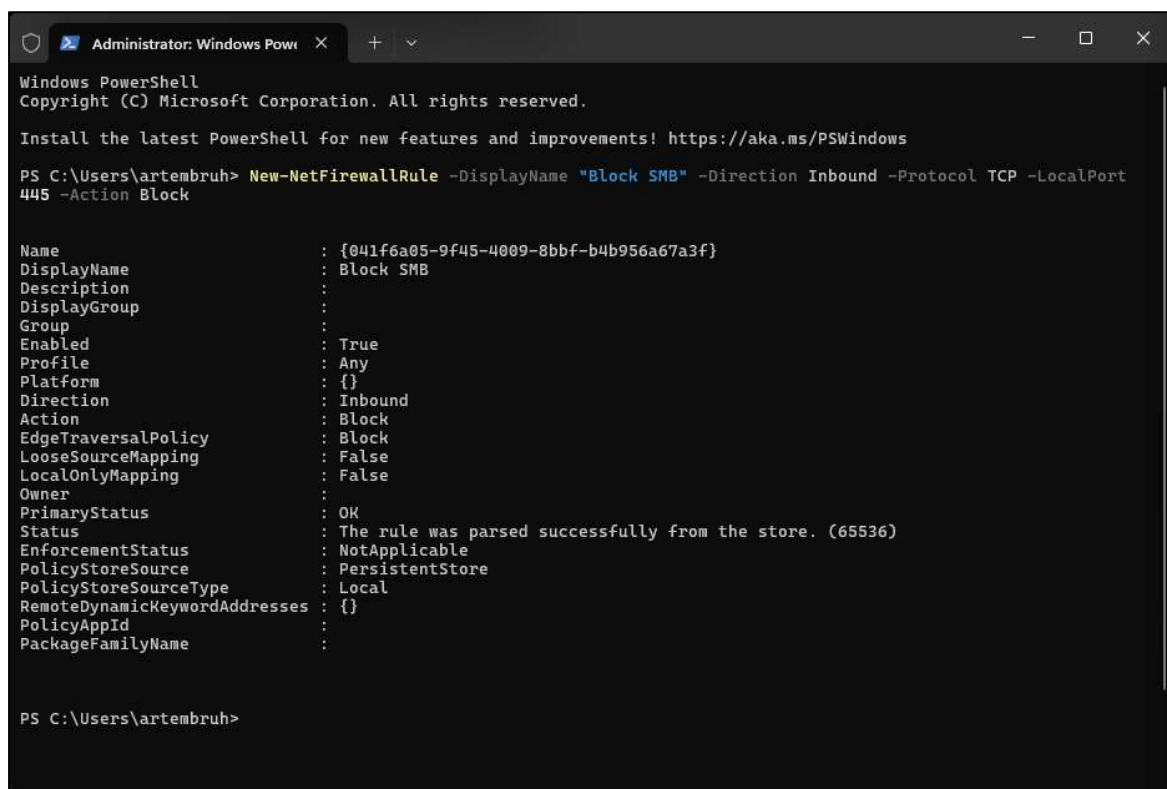


Рисунок 8 – Включаем брандмауэр для всех профилей



```
Administrator: Windows PowerShell
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\artembru> New-NetFirewallRule -DisplayName "Block SMB" -Direction Inbound -Protocol TCP -LocalPort 445 -Action Block

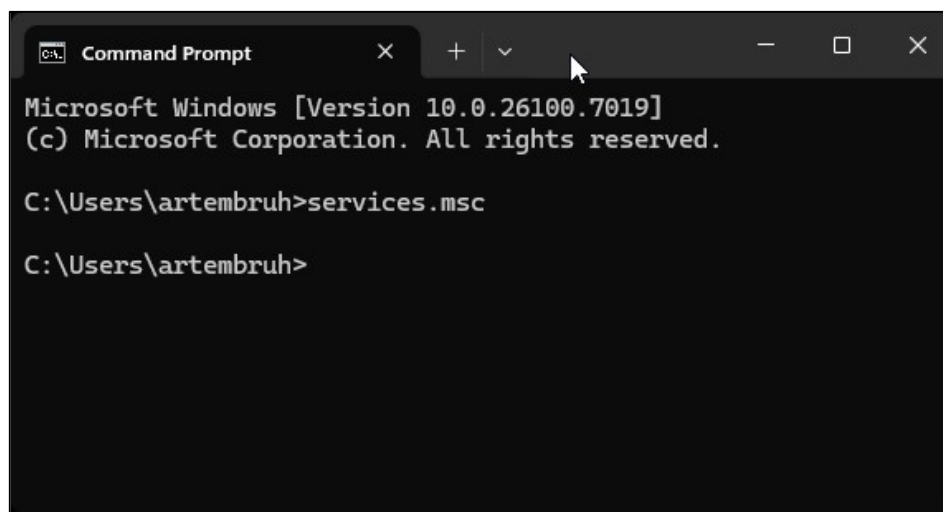
Name                               : {041f6a05-9f45-4009-8bbf-b4b956a67a3f}
DisplayName                         : Block SMB
Description                         :
DisplayGroup                        :
Group                               :
Enabled                             : True
Profile                             : 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                         :
PackageFamilyName                   :

PS C:\Users\artembru>
```

Рисунок 9 – Блокируем 445 порт который является целью Ransomware

3 Настройка служб Windows

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



```
Command Prompt
Microsoft Windows [Version 10.0.26100.7019]
(c) Microsoft Corporation. All rights reserved.

C:\Users\artembru>services.msc

C:\Users\artembru>
```

Рисунок 10 – Командная строка

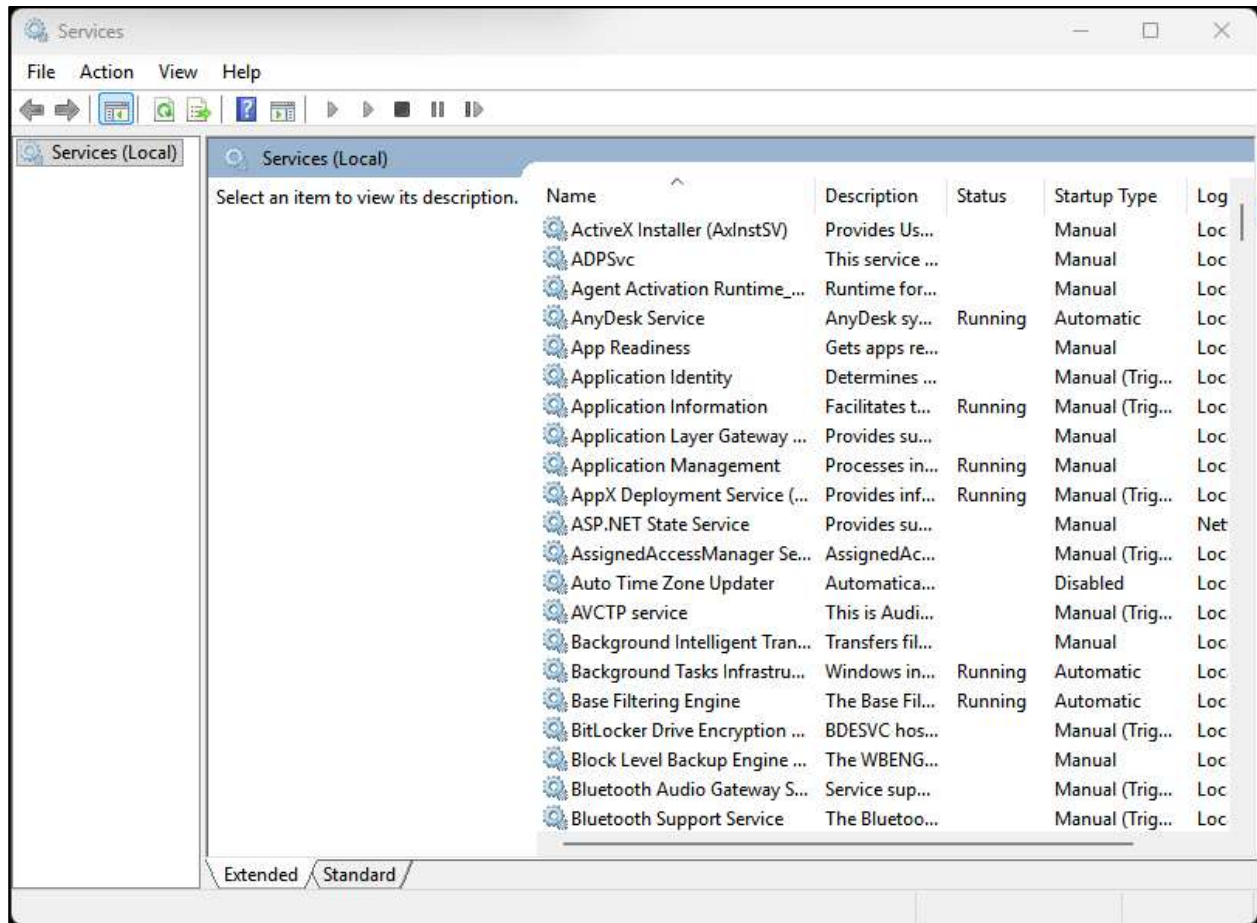


Рисунок 11 – Службы Windows

Отключаем не нужные службы, такие как “Print Spooler”

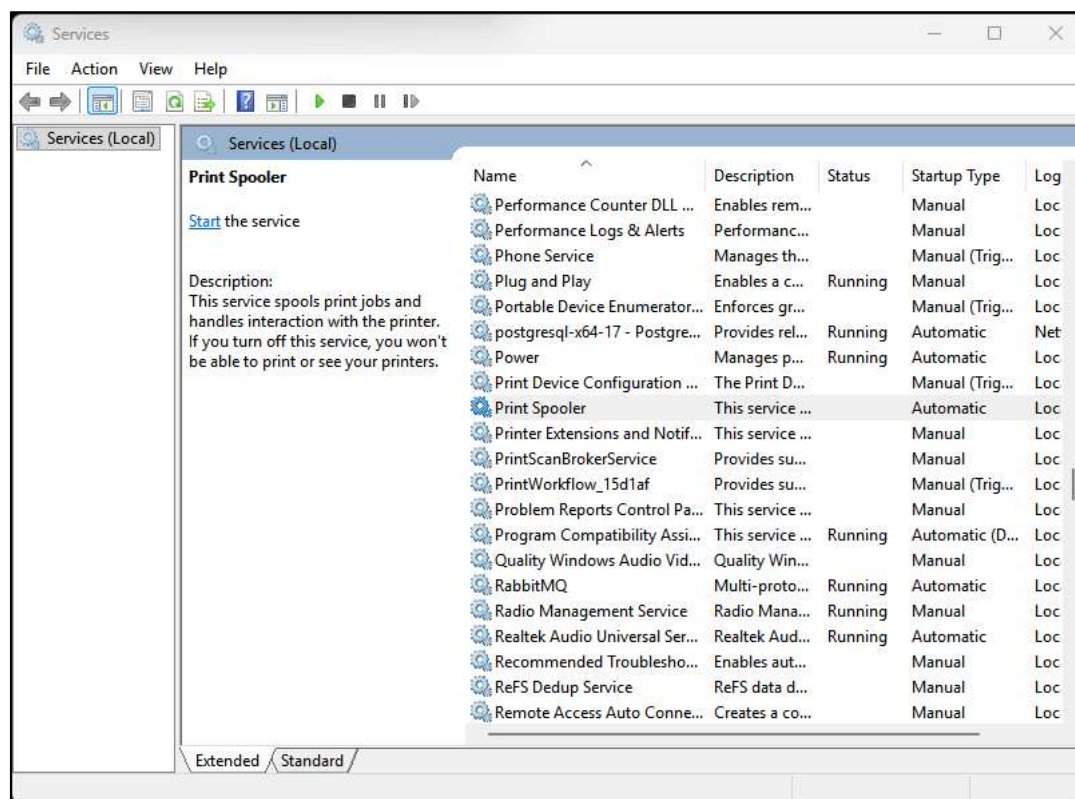


Рисунок 12 – Отключаем службу

Вывод

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