

Политика безопасности в ОС Microsoft Windows 11

Настройка политики безопасности в операционной системе Microsoft Windows 11 будет состоять из 3 основных пунктов:

1. Ограничение политики выполнения скриптов
2. Контроль учётных записей
3. Управление удалённым способом

Они позволят оптимизировать и обезопасить систему от несанкционированных действий вредоносного ПО или пользователей.

1. Ограничение политики выполнения скриптов

- 1.1. Открытие терминала Windows. Откройте программу «Выполнить» нажатием сочетания клавиш WIN + R и введите в поле ввода команду wt, и выполните команду.

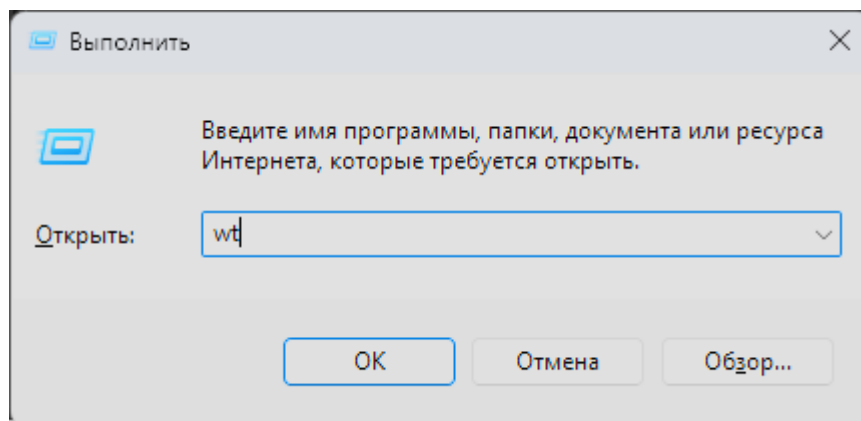


Рисунок 1 – Окно выполнения команд

- 1.2. После выполнения команды должен быть открыт терминал Windows.

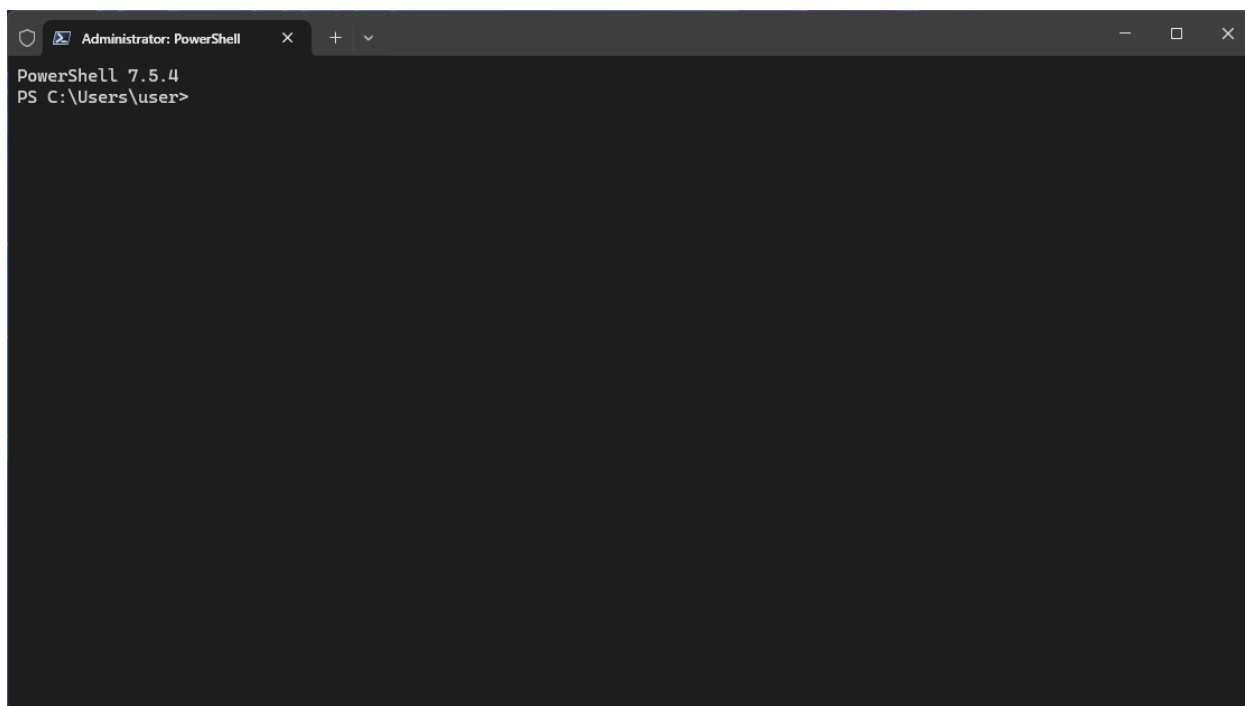


Рисунок 2 – Окно программы «Терминал Windows»

- 1.3. Введите команду `Get-ExecutionPolicy -List` для получения настройки выполнения скриптов для всех областей

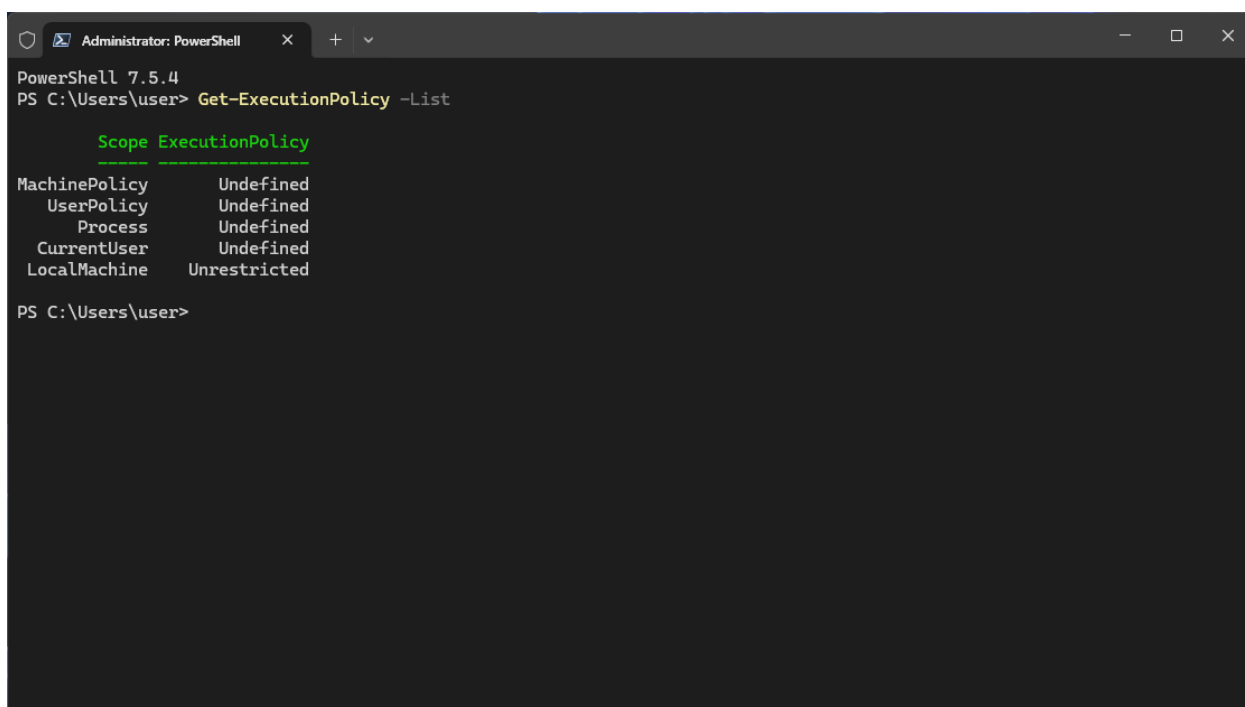


Рисунок 3 – Список настройки выполнения скриптов для всех областей

- 1.4. Введите команду `Set-ExecutionPolicy RemoteSigned -Force` для разрешения выполнения только подписанных скриптов

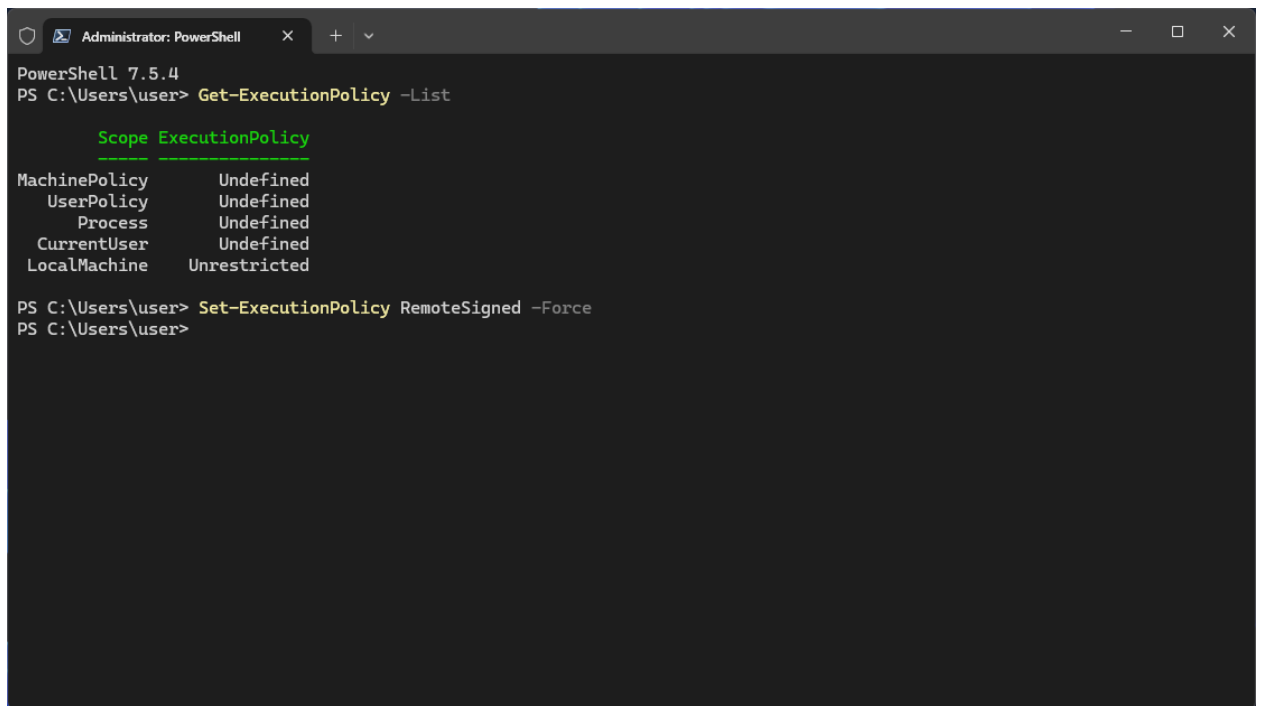


Рисунок 4 – Выполненная команда.

2. Контроль учётных записей

- 2.1. Откройте программу «Выполнить» нажатием сочетания клавиш WIN + R и введите в поле ввода команду gpedit.msc, и выполните команду.

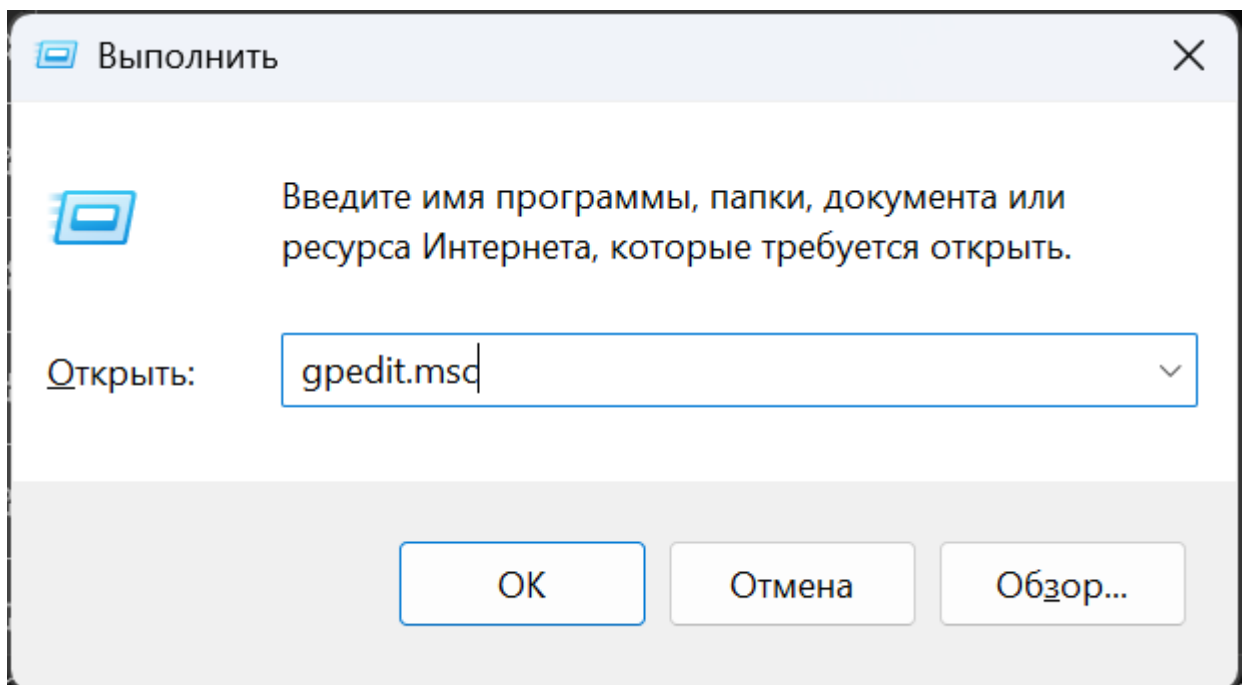


Рисунок 5 – Окно выполнения команд

- 2.2. После открытия программы откройте параметры безопасности (Конфигурация компьютера – Конфигурация Windows – Параметры безопасности – Локальные политики – Параметры безопасности)

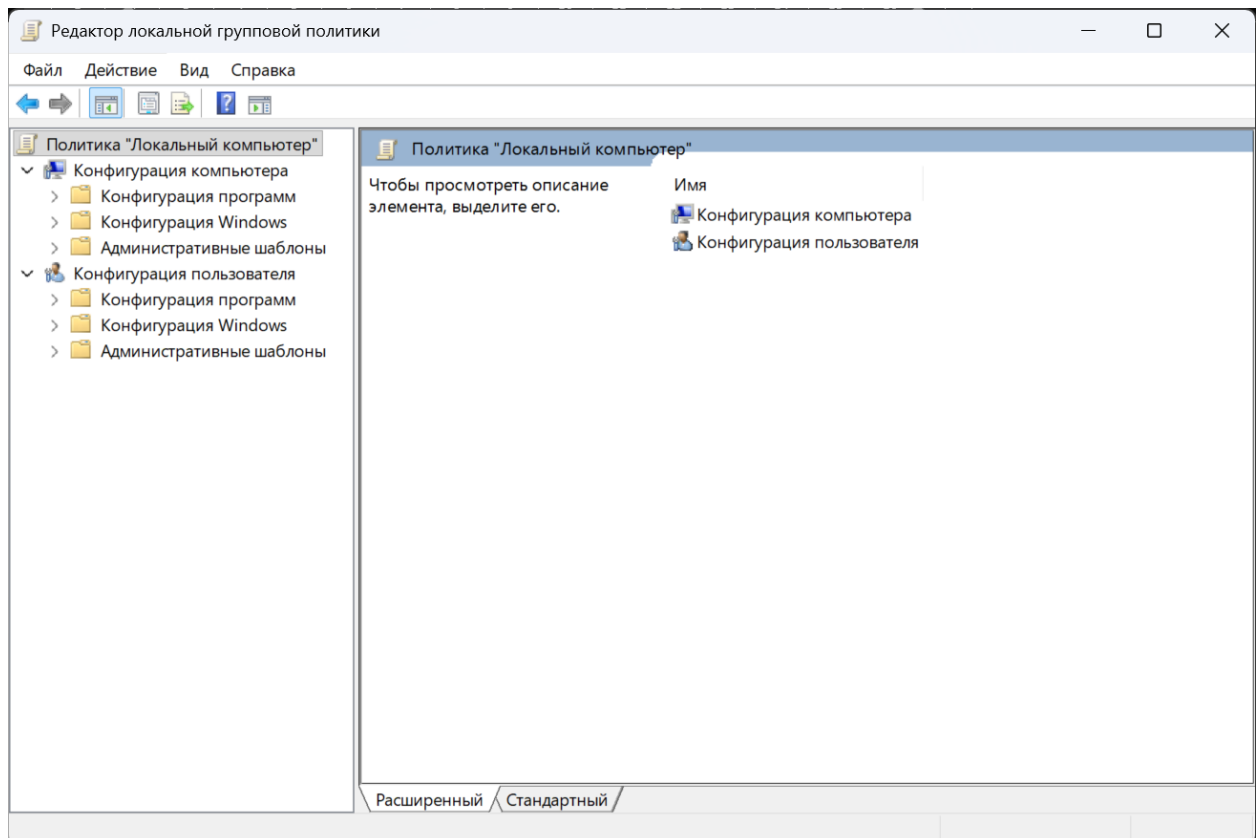


Рисунок 6 – Редактор локальной групповой политики

2.3. Найдите следующие параметры и выставите следующие значения:

Контроль учётных записей: все администраторы работают в режиме одобрения — «Включён»

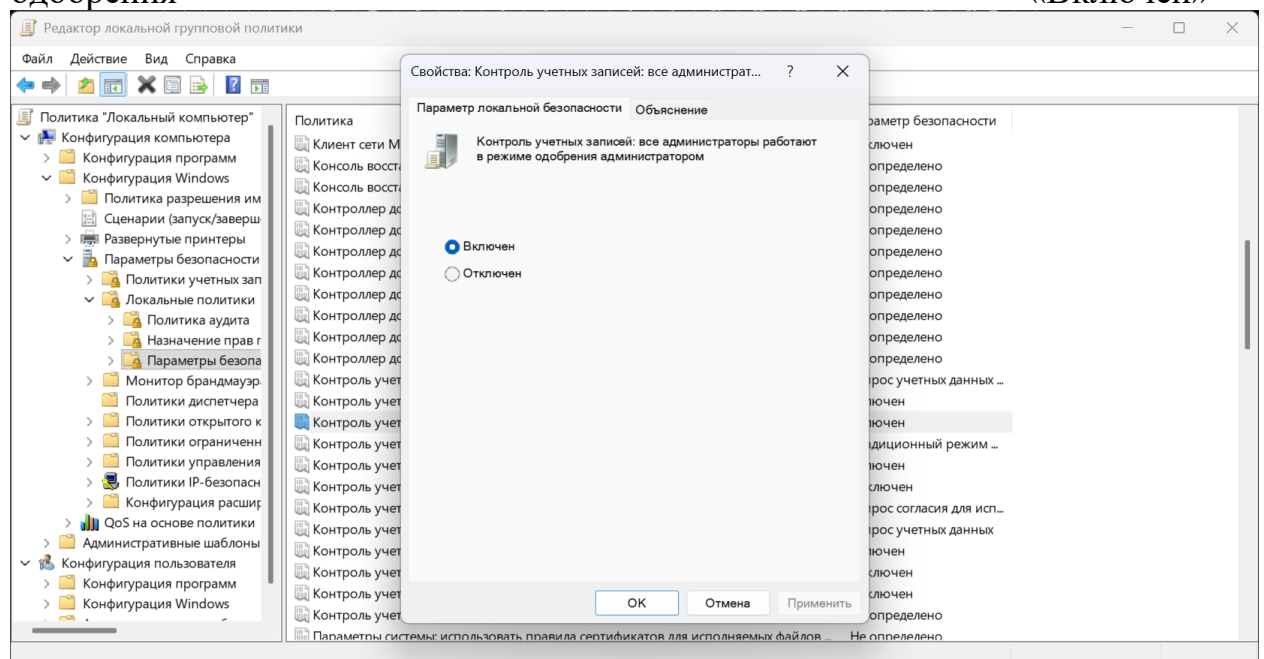


Рисунок 7 – Конфигурация параметров в редакторе групповой политики

Контроль учётных записей: поведение запроса на повышение для администраторов – «Запрашивать согласие»

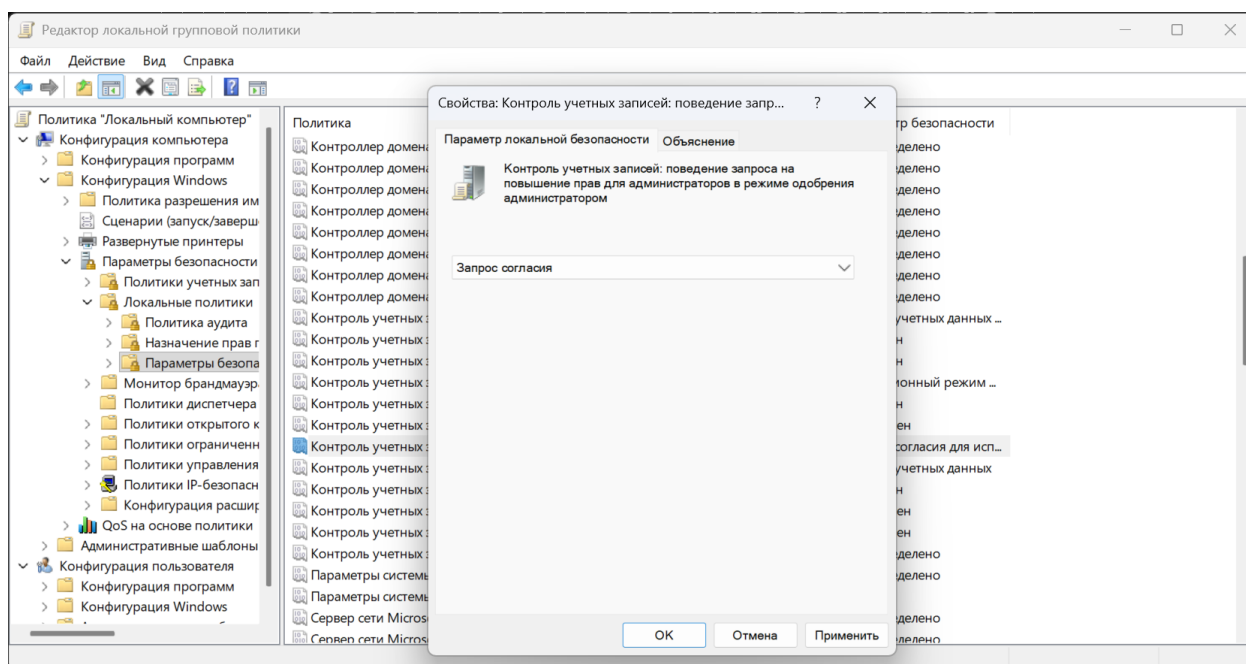


Рисунок 8 - Конфигурация параметров в редакторе групповой политики

Контроль учётных записей: переключение к безопасному рабочему столу при выполнении запроса на повышение прав – «Включён»

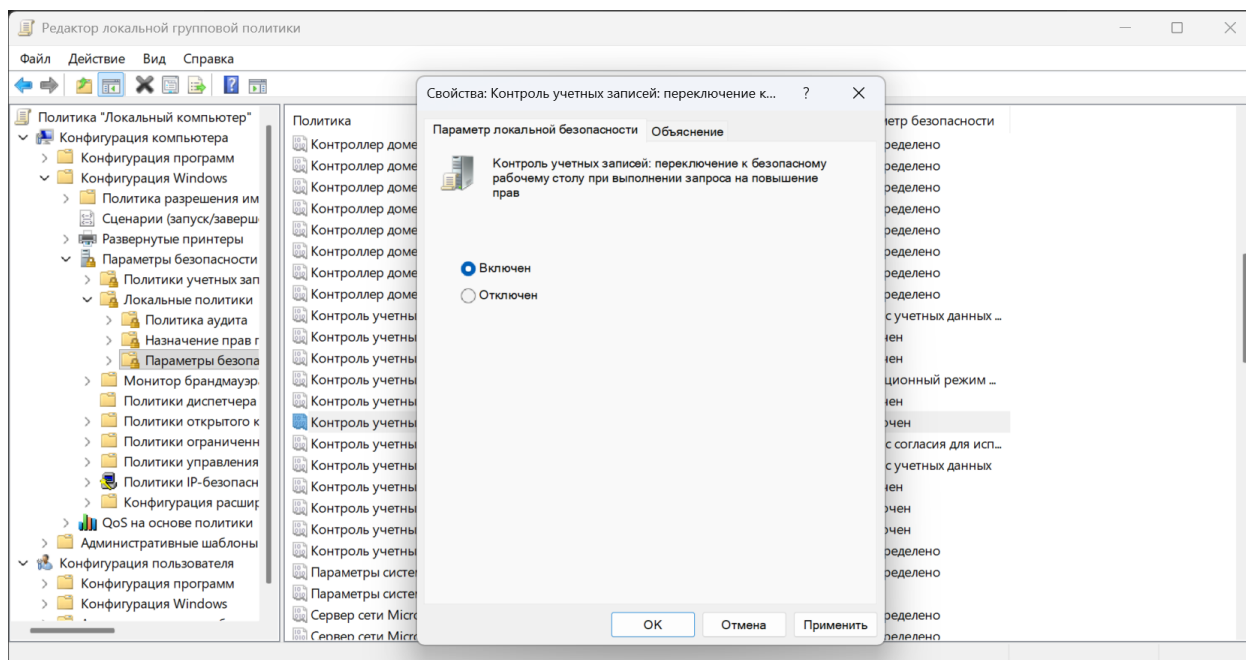


Рисунок 9 - Конфигурация параметров в редакторе групповой политики

2.4. После применения параметров перезагрузите компьютер.

3. Управление удалённым способом

- 3.1. Откройте программу «Выполнить» нажатием сочетания клавиш WIN + R и введите в поле ввода команду wt, и выполните команду.

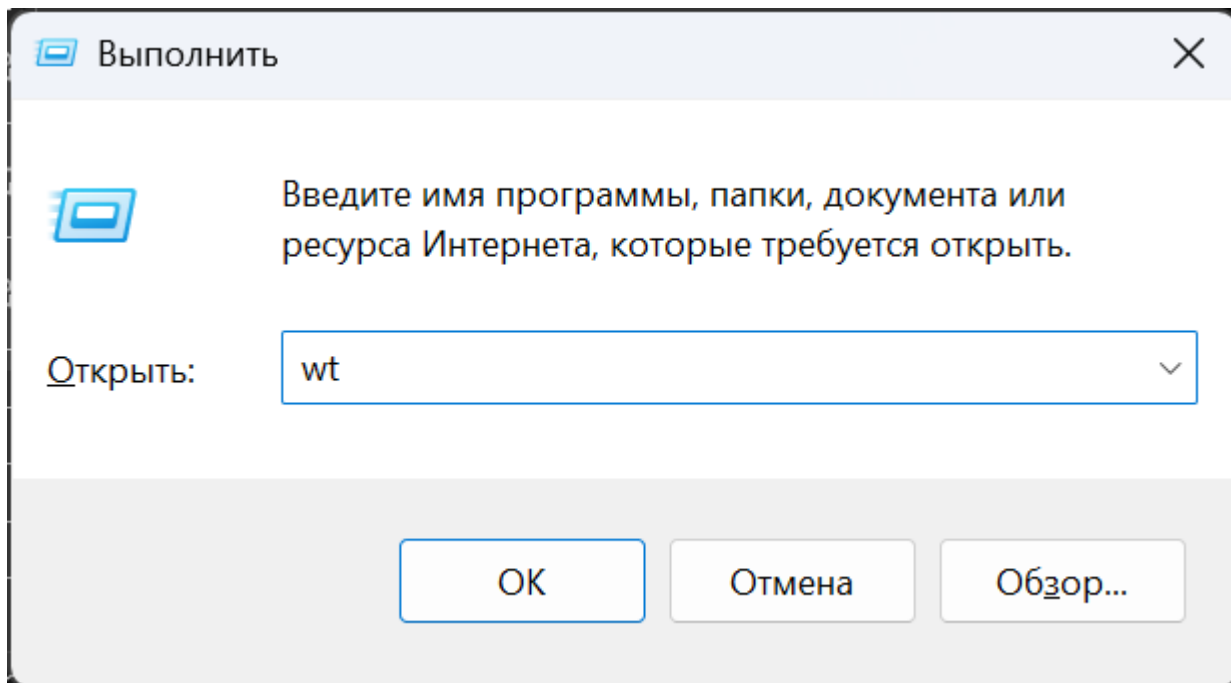


Рисунок 10 – Окно выполнения команд

3.2. Включите PowerShell Remoting

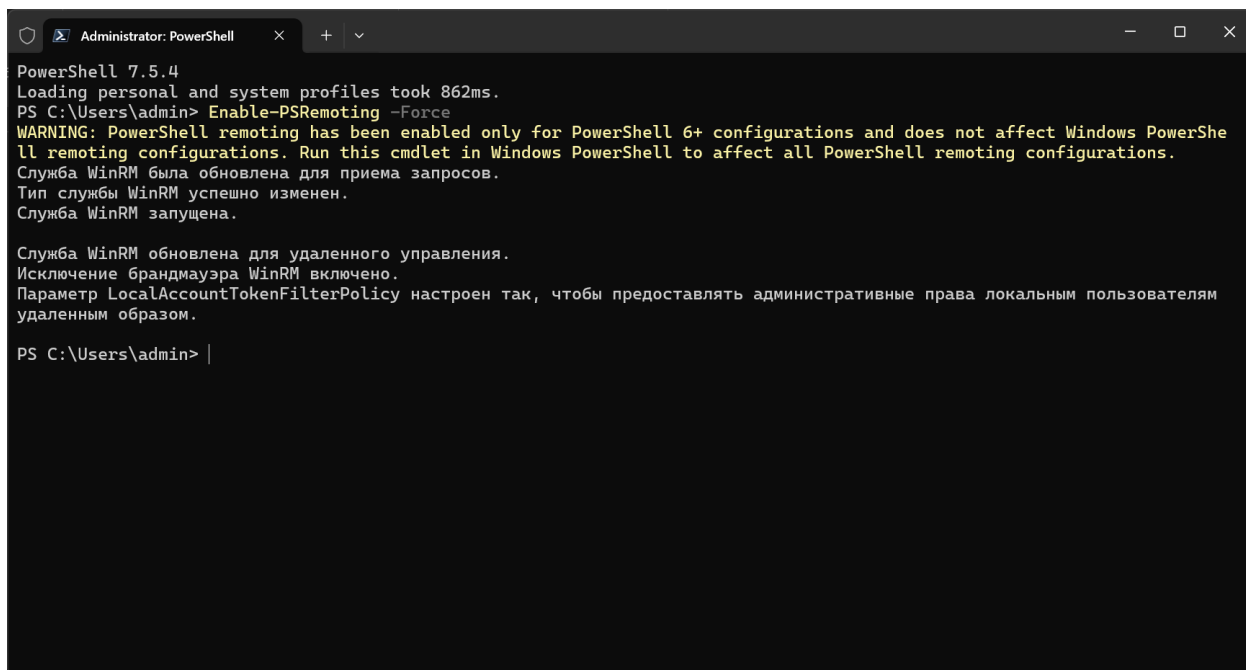
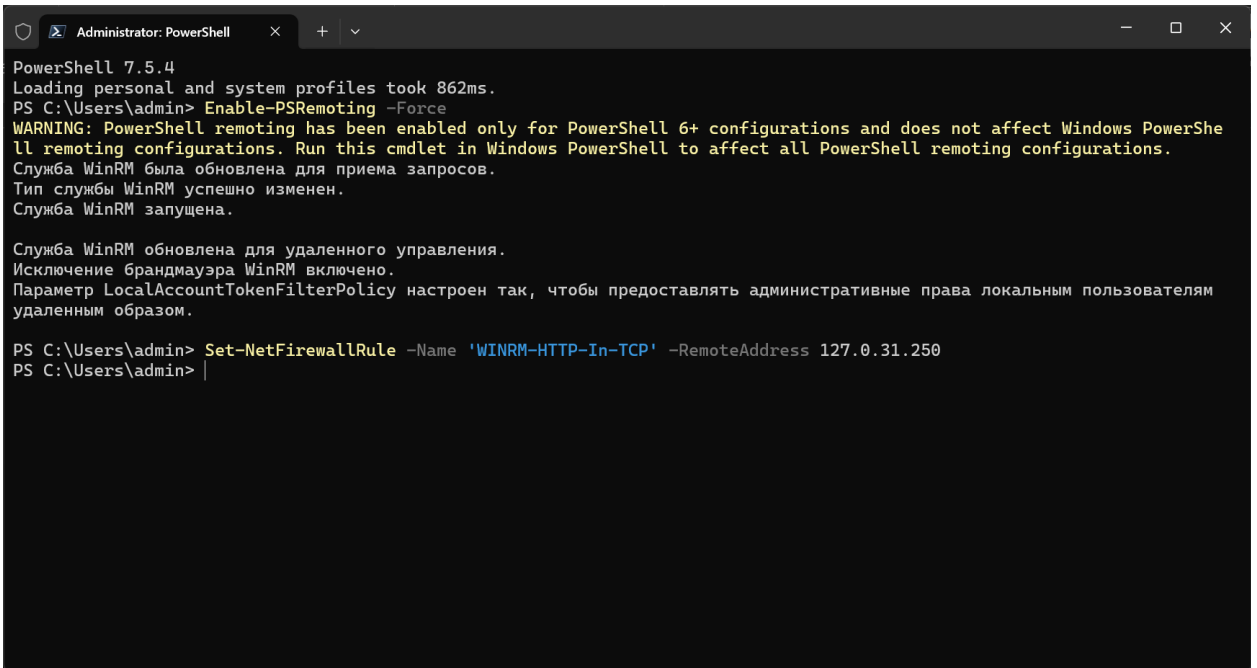


Рисунок 11 – Результат включения PowerShell Remoting

3.3. Введите команду Set-NetFirewallRule -Name 'WINRM-HTTP-In-TCP' -RemoteAddress X.X.X.X для разрешения только определённым IP



```
PowerShell 7.5.4
Loading personal and system profiles took 862ms.
PS C:\Users\admin> Enable-PSRemoting -Force
WARNING: PowerShell remoting has been enabled only for PowerShell 6+ configurations and does not affect Windows PowerShell remoting configurations. Run this cmdlet in Windows PowerShell to affect all PowerShell remoting configurations.
Служба WinRM была обновлена для приема запросов.
Тип службы WinRM успешно изменен.
Служба WinRM запущена.

Служба WinRM обновлена для удаленного управления.
Исключение брандмауэра WinRM включено.
Параметр LocalAccountTokenFilterPolicy настроен так, чтобы предоставлять административные права локальным пользователям удаленным образом.

PS C:\Users\admin> Set-NetFirewallRule -Name 'WINRM-HTTP-In-TCP' -RemoteAddress 127.0.31.250
PS C:\Users\admin> |
```

Рисунок 12 – Результат разрешения подключения только определённых IP адресов