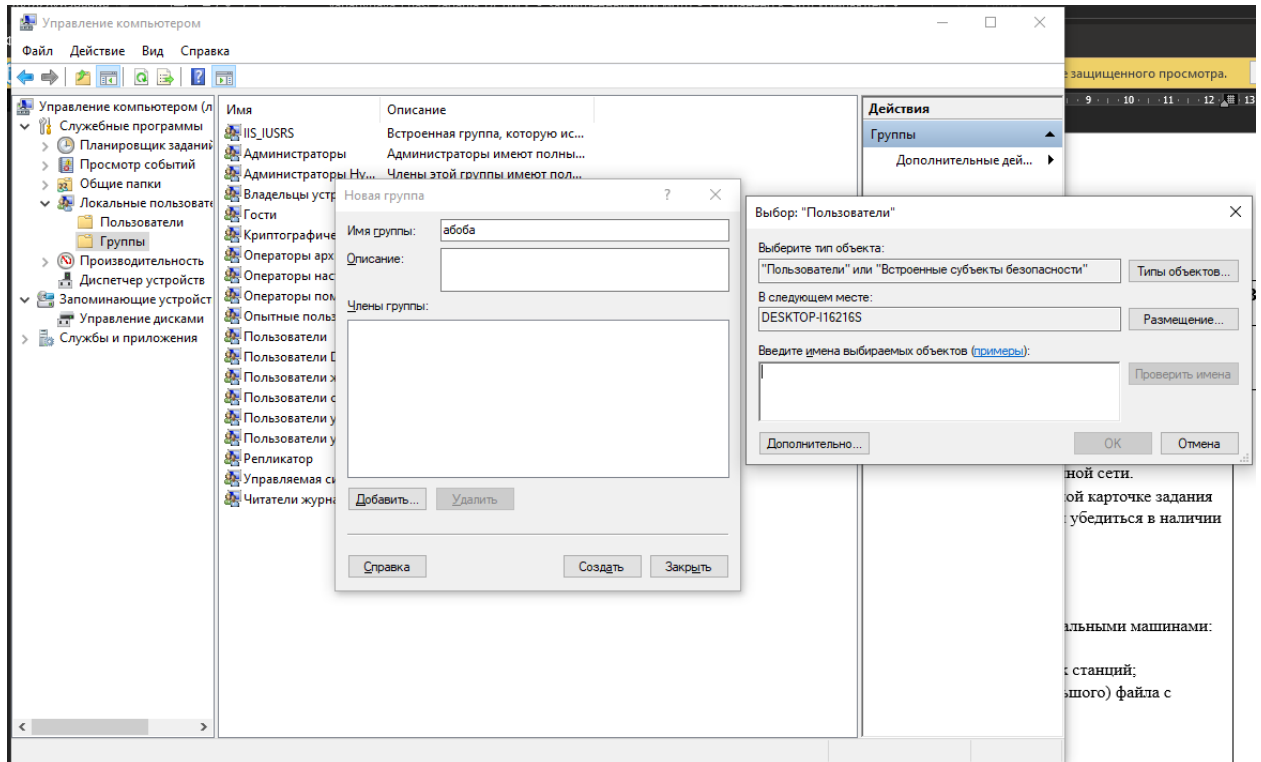


## Задание 2.

Зайти в управление компьютером, локальные пользователи.

Создать 3 пользователей

Создать группу и добавить туда пользователей



## Задание 3.

Определить доступность сетевого узла и ip-адрес с помощью командной строки и команды ping

```
C:\Users\pallexx818>ping minobrnauki.gov.ru

Обмен пакетами с minobrnauki.gov.ru [217.107.75.18] с 32 байтами данных:
Ответ от 217.107.75.18: число байт=32 время=62мс TTL=60
Ответ от 217.107.75.18: число байт=32 время=60мс TTL=60
Ответ от 217.107.75.18: число байт=32 время=60мс TTL=60
Ответ от 217.107.75.18: число байт=32 время=60мс TTL=60

Статистика Ping для 217.107.75.18:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потеря)
Приблизительное время приема-передачи в мс:
    Минимальное = 60мсек, Максимальное = 62 мсек, Среднее = 60 мсек
```

Определить путь до сетевого узла с помощью командной строки и команды tracert

```
C:\Users\pallexx818>tracert minobrnauki.gov.ru

Трассировка маршрута к minobrnauki.gov.ru [217.107.75.18]
с максимальным числом прыжков 30:

 1      1 ms      1 ms      1 ms  192.168.0.1
 2      2 ms      2 ms      2 ms  krsn-bras3.sib.ip.rostelecom.ru [213.228.116.37]
 3      2 ms      2 ms      2 ms  ae0.krsn-rgr5.sib.ip.rostelecom.ru [213.228.110.24]
 4     61 ms     62 ms     62 ms  185.140.151.255
 5     61 ms     61 ms     61 ms  194.190.247.82
 6     62 ms     61 ms     61 ms  217.107.75.18

Трассировка завершена.
```

Установить IP-адрес и MAC-адрес используемого вами ПК, IP-адрес шлюза, IP-адрес сервера службы DNS, IP-адрес сервера DHCP.

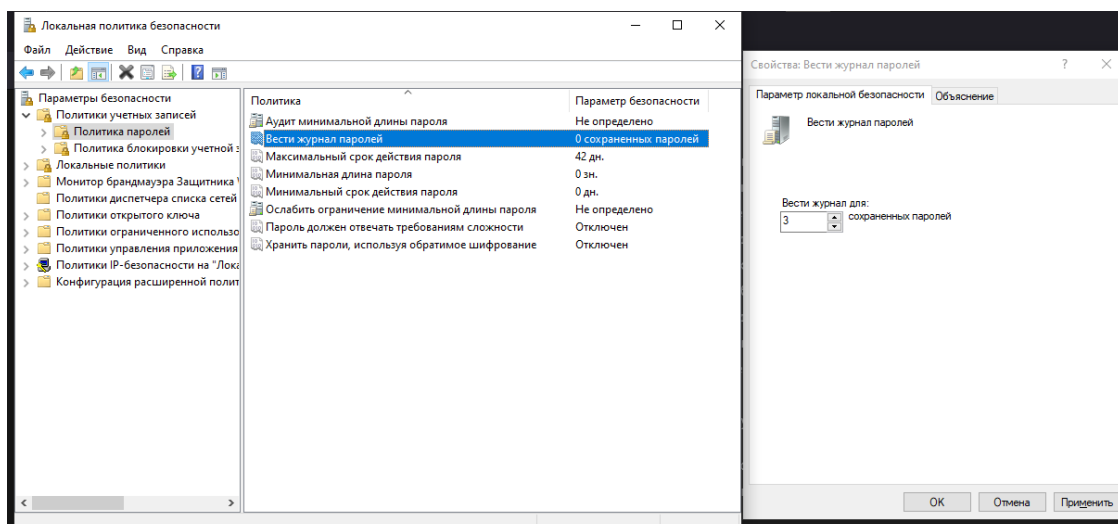
Выполняется с помощью командной строки и команды `ipconfig /all`

```
Адаптер беспроводной локальной сети Беспроводная сеть:

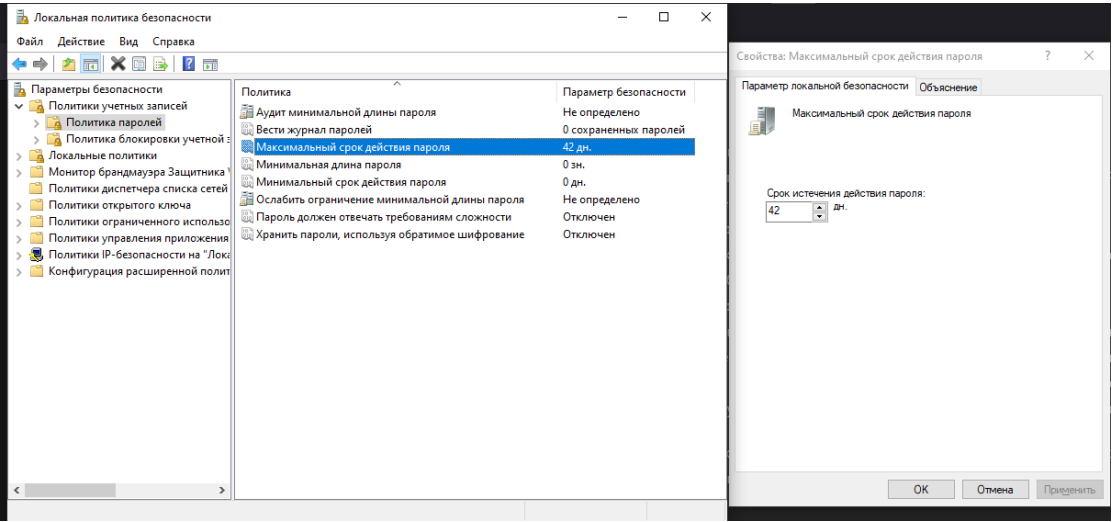
DNS-суффикс подключения . . . . . :
Описание. . . . . : Realtek RTL8822CE 802.11ac PCIe Adapter
Физический адрес. . . . . : C0-E4-34-AC-43-8B
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да
Локальный IPv6-адрес канала . . . : fe80::782a:b7e9:23da:f8ae%9(Основной)
IPv4-адрес. . . . . : 192.168.0.18(Основной)
Маска подсети . . . . . : 255.255.255.0
Аренда получена. . . . . : 16 апреля 2024 г. 18:02:13
Срок аренды истекает. . . . . : 17 апреля 2024 г. 4:56:22
Основной шлюз. . . . . : fe80::4a29:e4ff:fe34:e271%9
                        192.168.0.1
DHCP-сервер. . . . . : 192.168.0.1
IAID DHCPv6 . . . . . : 96527412
DUID клиента DHCPv6 . . . . . : 00-01-00-01-2C-C3-34-C4-E8-D8-D1-52-3D-64
DNS-серверы. . . . . : 192.168.0.1
NetBios через TCP/IP. . . . . : Включен
```

Задание 4. Зайти в командную строку и ввести команду `secpol.msc`

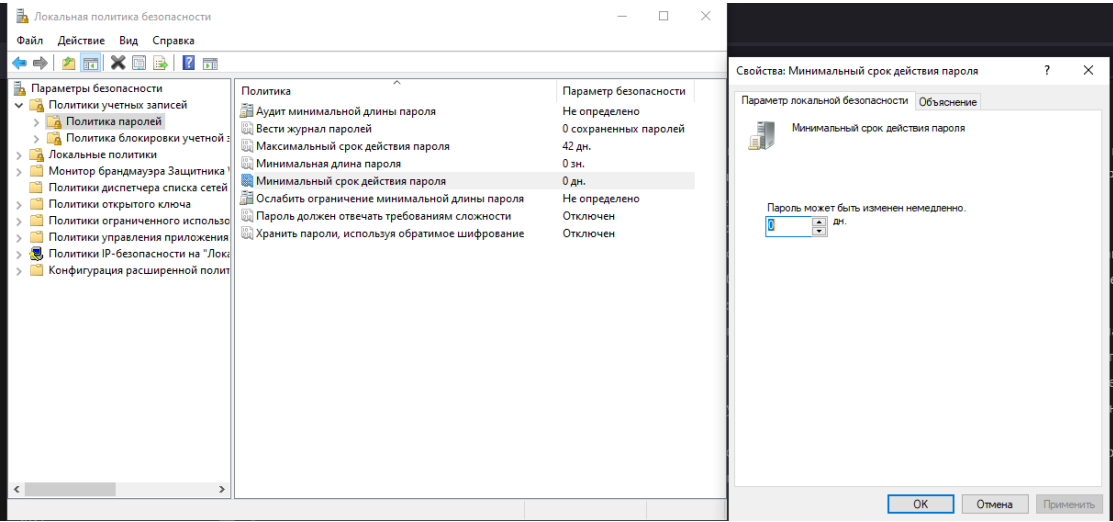
Длина журнала паролей



Максимальный срок действия пароля

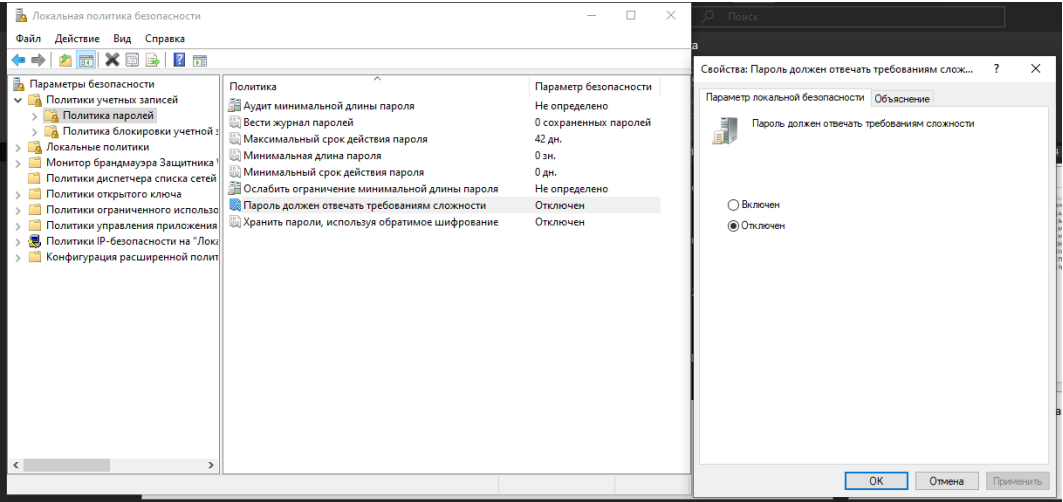


Минимальный срок действия пароля

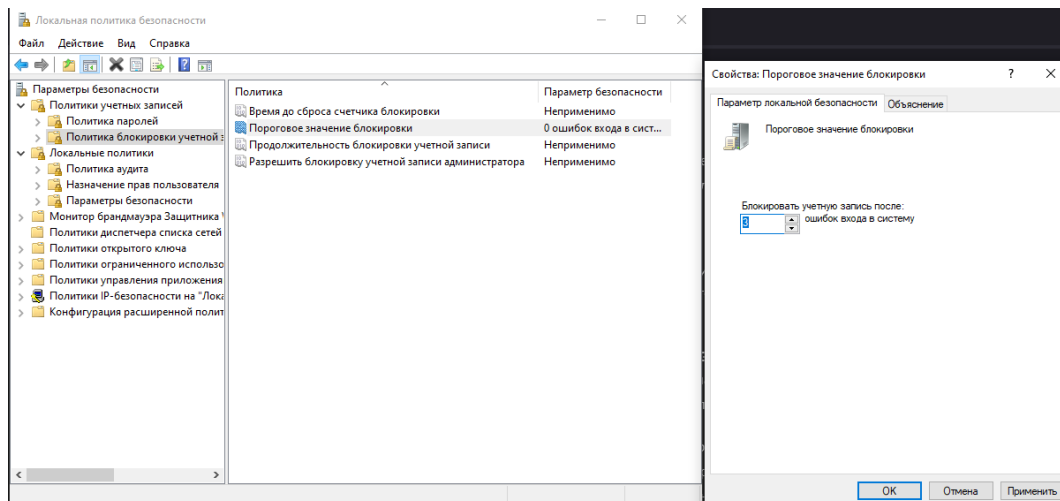


Минимальная длина пароля – X символов

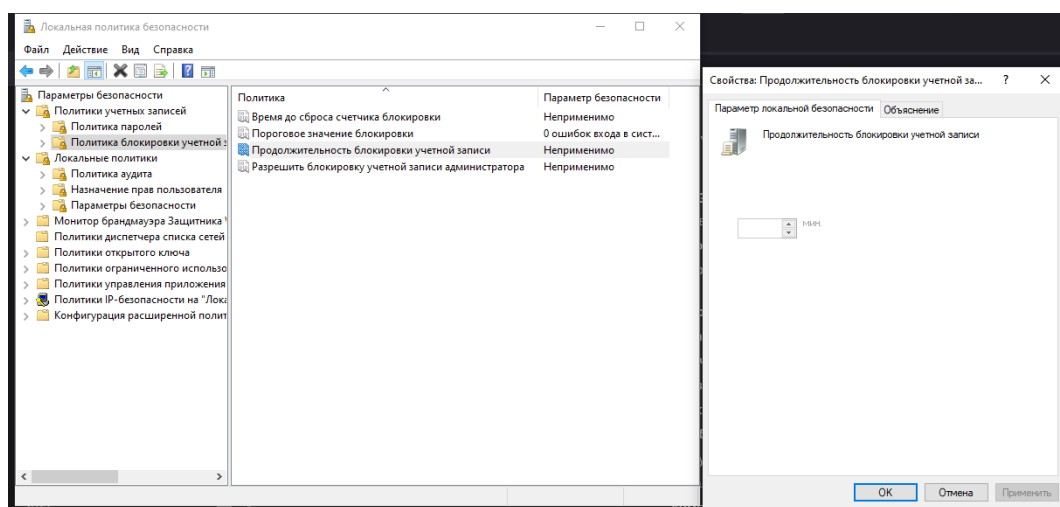
Включите требования к сложности пароля.



Блокировка учетной записи после трех ошибочных вводов пароля



Продолжительность блокировки учетной записи – X минут

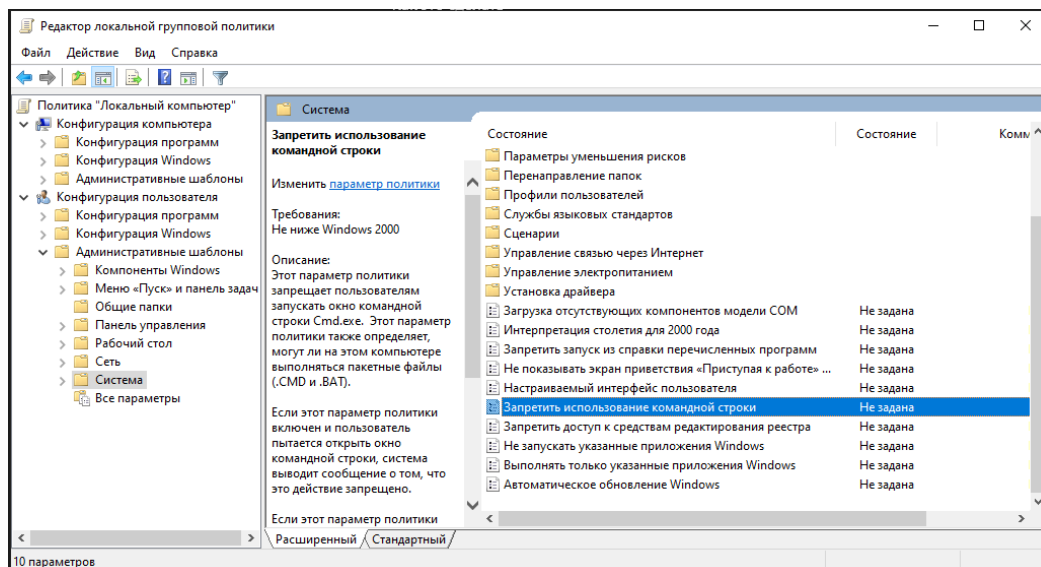


Подтвердите выполнение задачи скриншотом окна политик безопасности

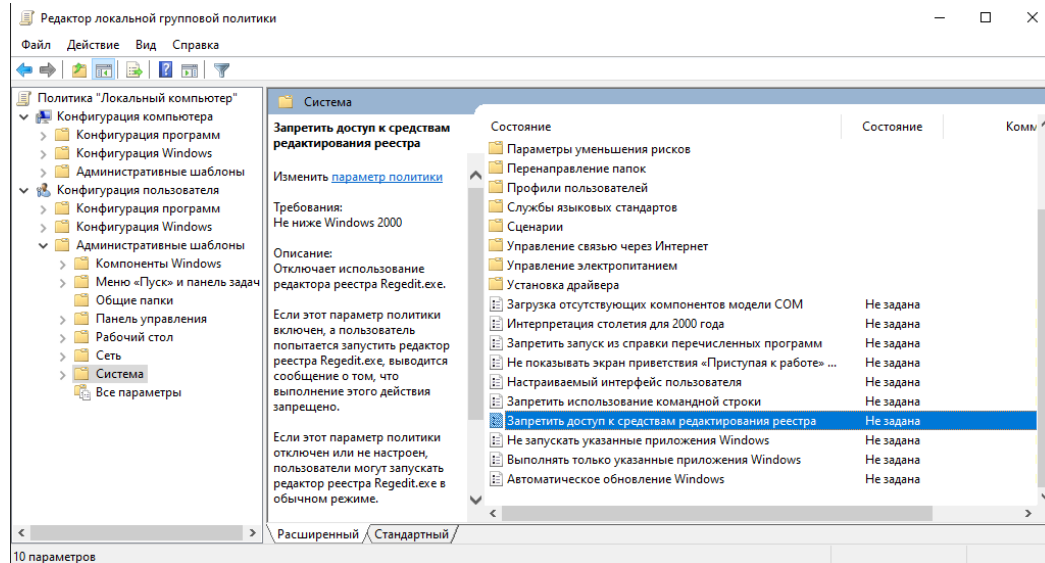
Сделать скриншоты Политики паролей и Политики блокировки учетной записи

Задание 5. Зайти в командную строку и ввести gredit.msc

Запретить использование командной строки



## Запрет редактирования реестра



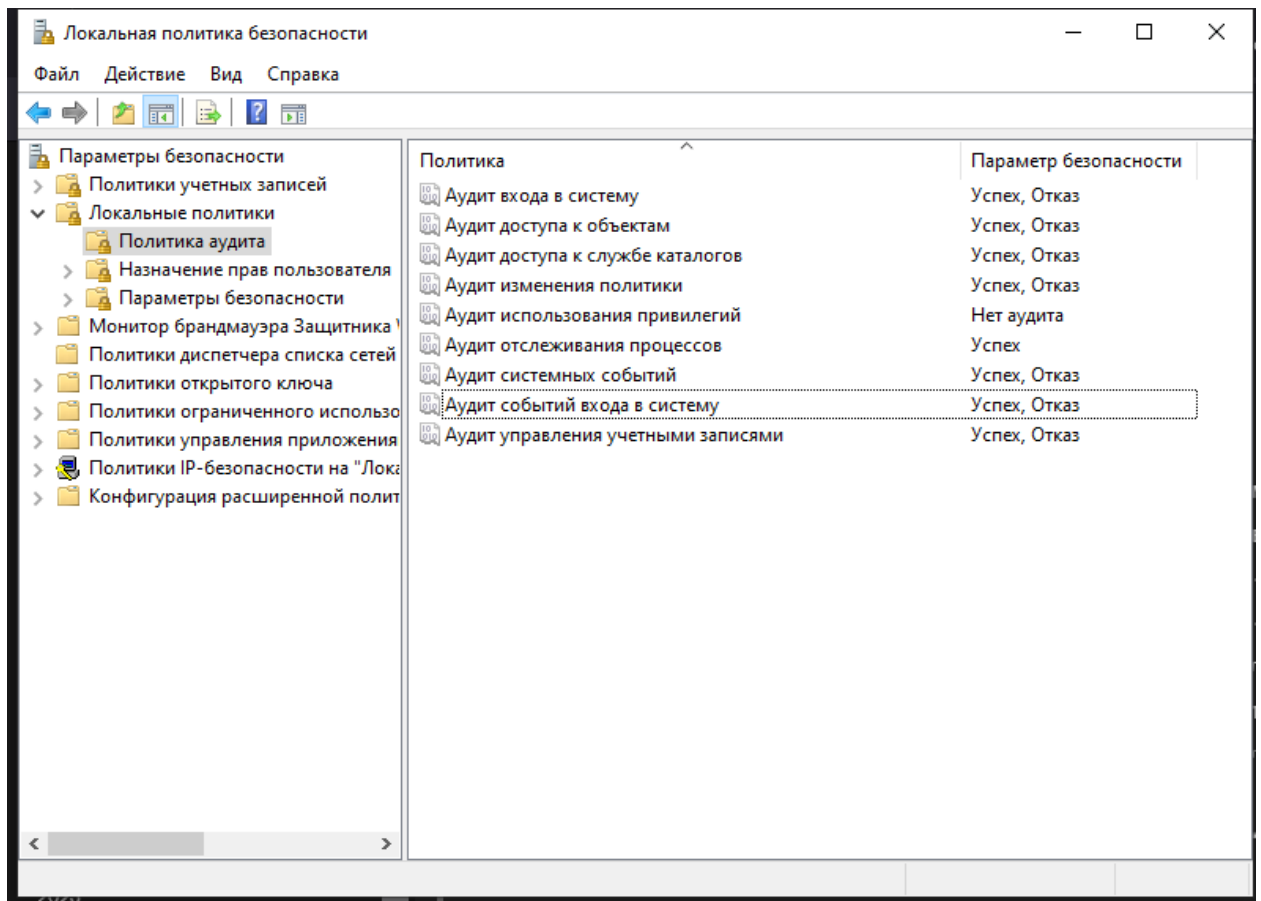
### Задание 6.

При помощи локальной групповой политики скройте из панели задач следующие элементы: Шифрование диска BitLocker, Центр управления сетями и общим доступом, Система, Учетные записи пользователей, Администрирование, Программы и компоненты, Параметры проводника. Проверьте работу политики выполнив скриншот окна панели управления

### Задание 7.

Настройте политики аудита: регистрация успешных входов и отказов входа в систему, аудит доступа к объектам, службе каталогов, изменения политики, системных событий, управления учетными записями, событий входа в систему.

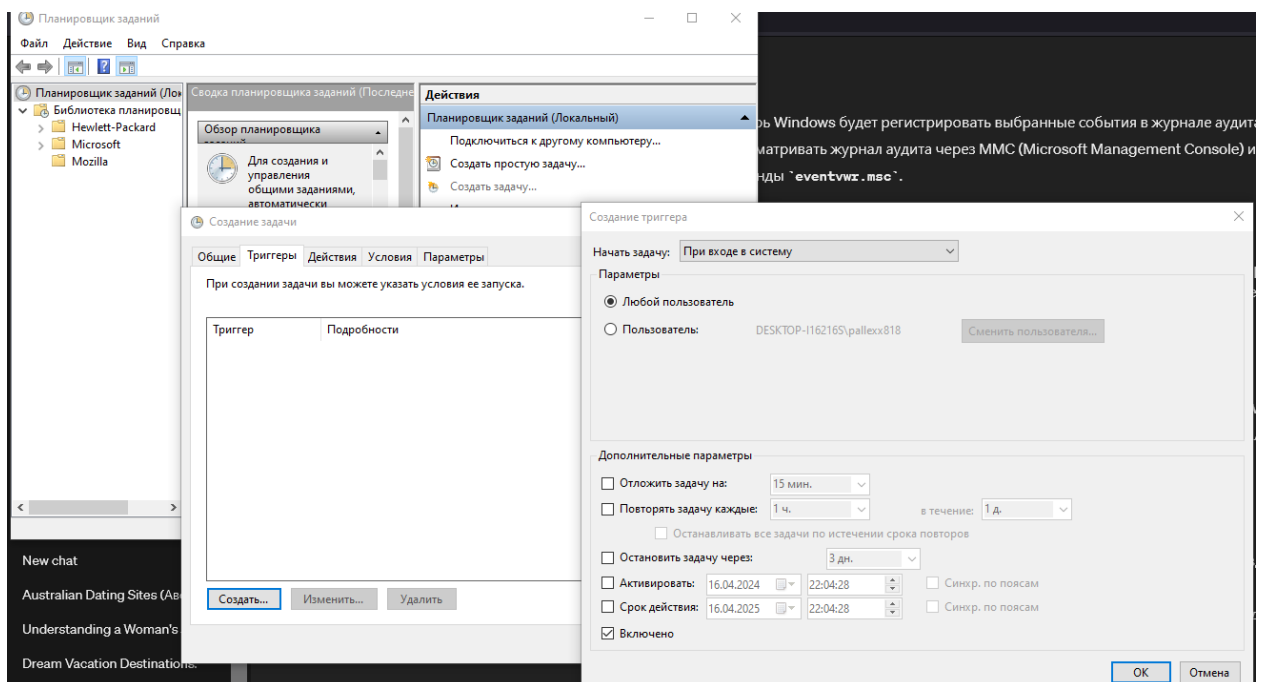
Зайти в командную строку и ввести secpol.msc



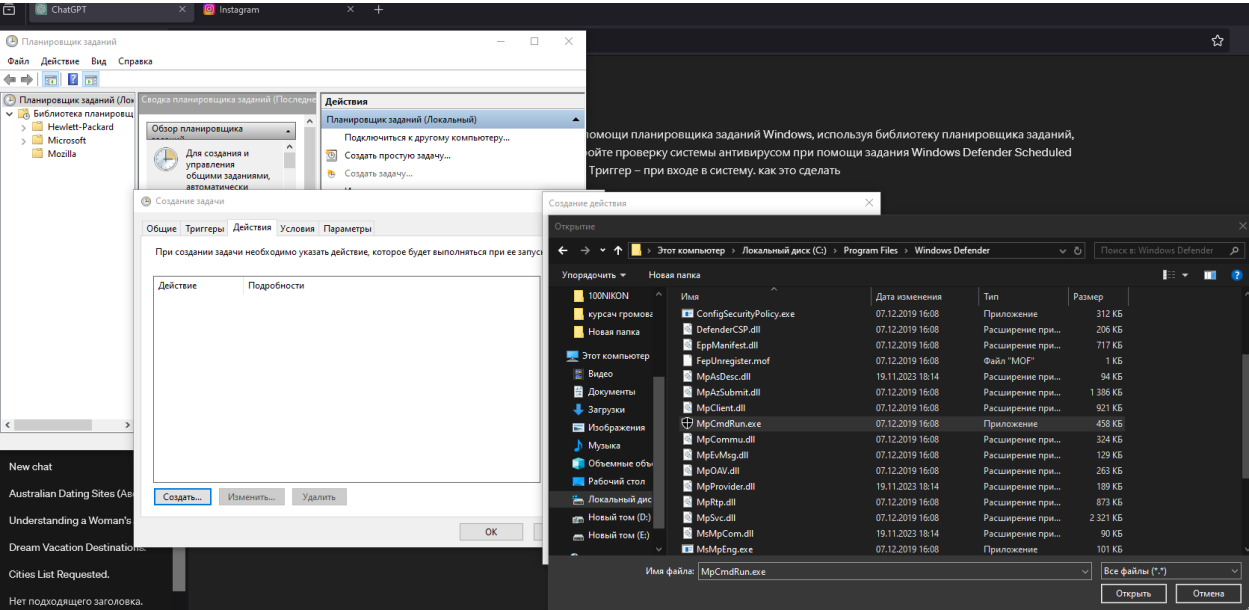
## Задание 8.

При помощи планировщика заданий Windows, используя библиотеку планировщика заданий, настройте проверку системы антивирусом при помощи задания Windows Defender Scheduled Scan: Триггер – при входе в систему.

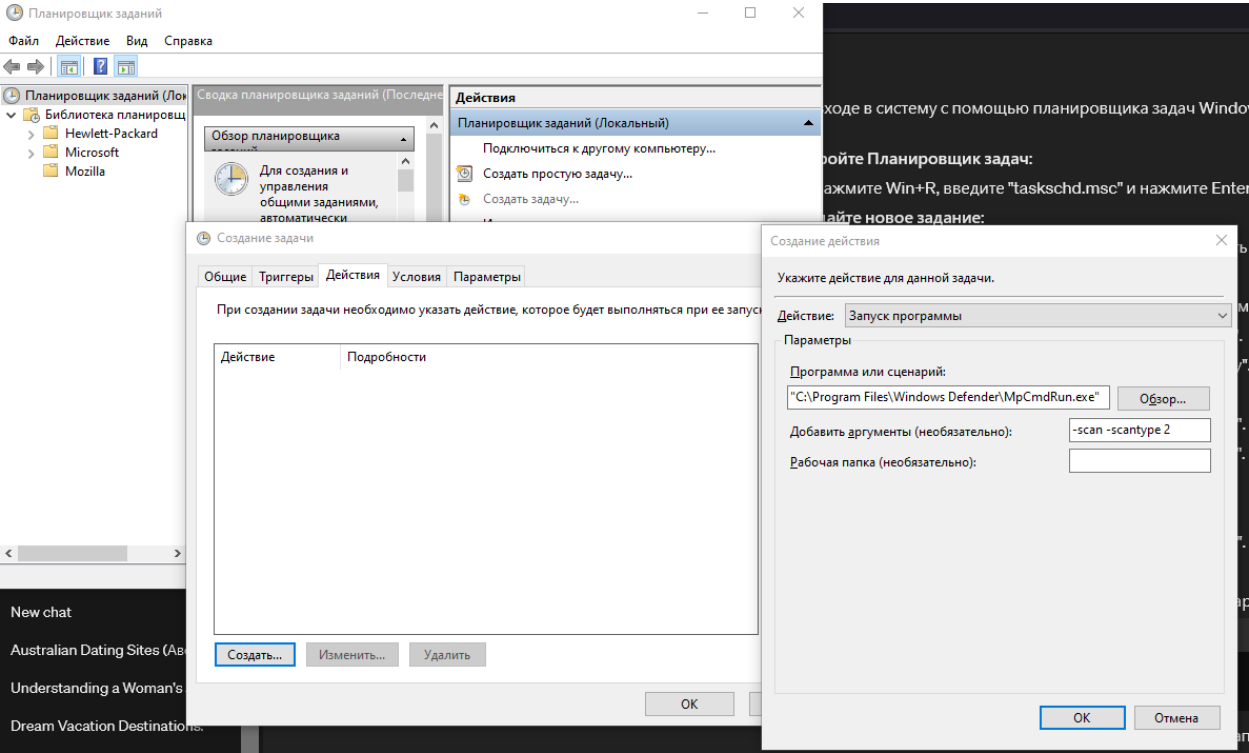
Ввести название в «общие», создать триггер выбрать «при входе в систему»



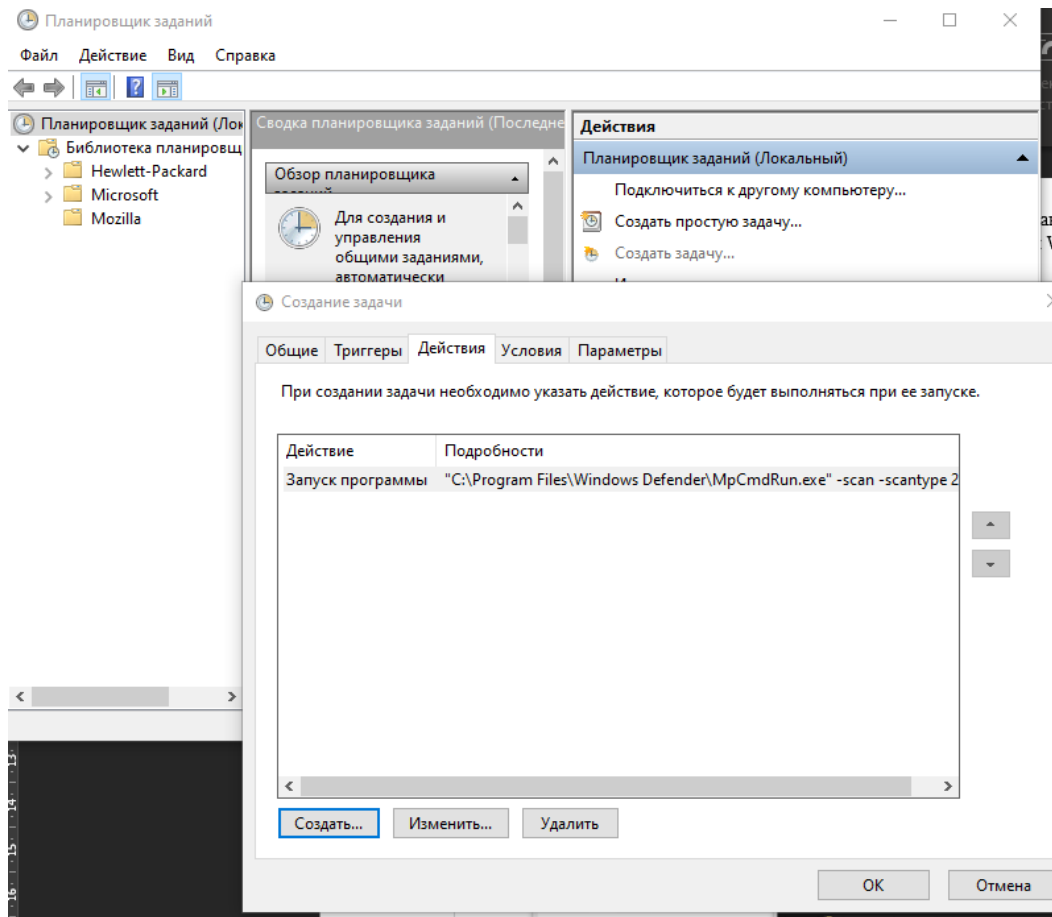
Создание действия и выбор программы



Создание аргумента



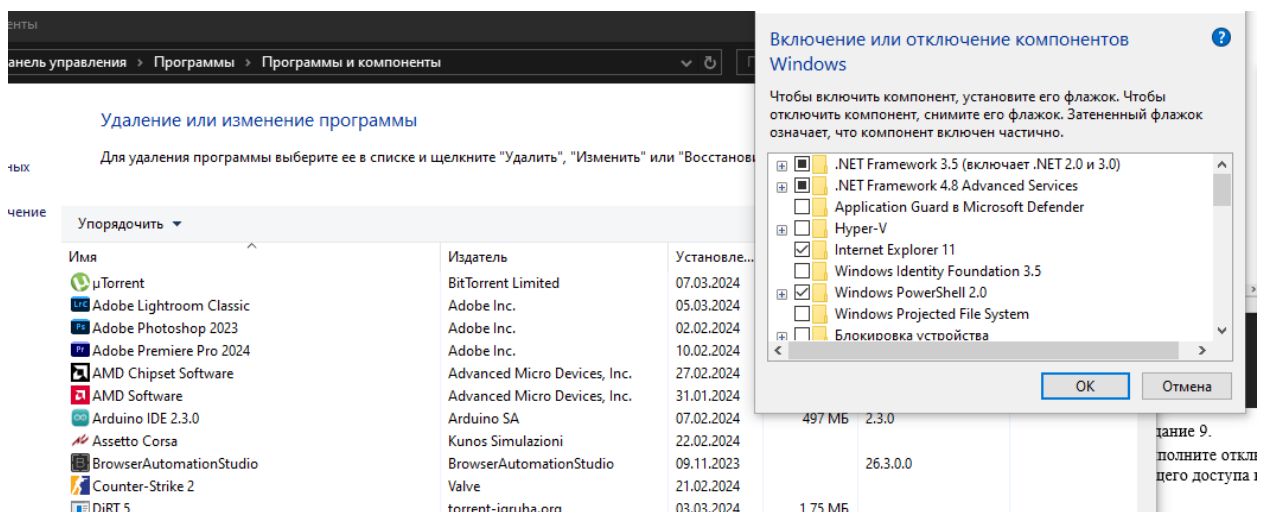
Завершение



#### Задание 9.

Выполните отключение компонентов Windows: клиент Telnet, клиент TFTP, поддержка общего доступа к файлам SMB 1.0, служба SMB Direct.

Зайти в панель управления, программы, программы и компоненты, включение и отключение, затем выбрать нужные компоненты и отключить их



#### Задание 10.

Создайте точку восстановления операционной системы Windows.

В поиске написать создание точки восстановления, Система защиты, Создать.