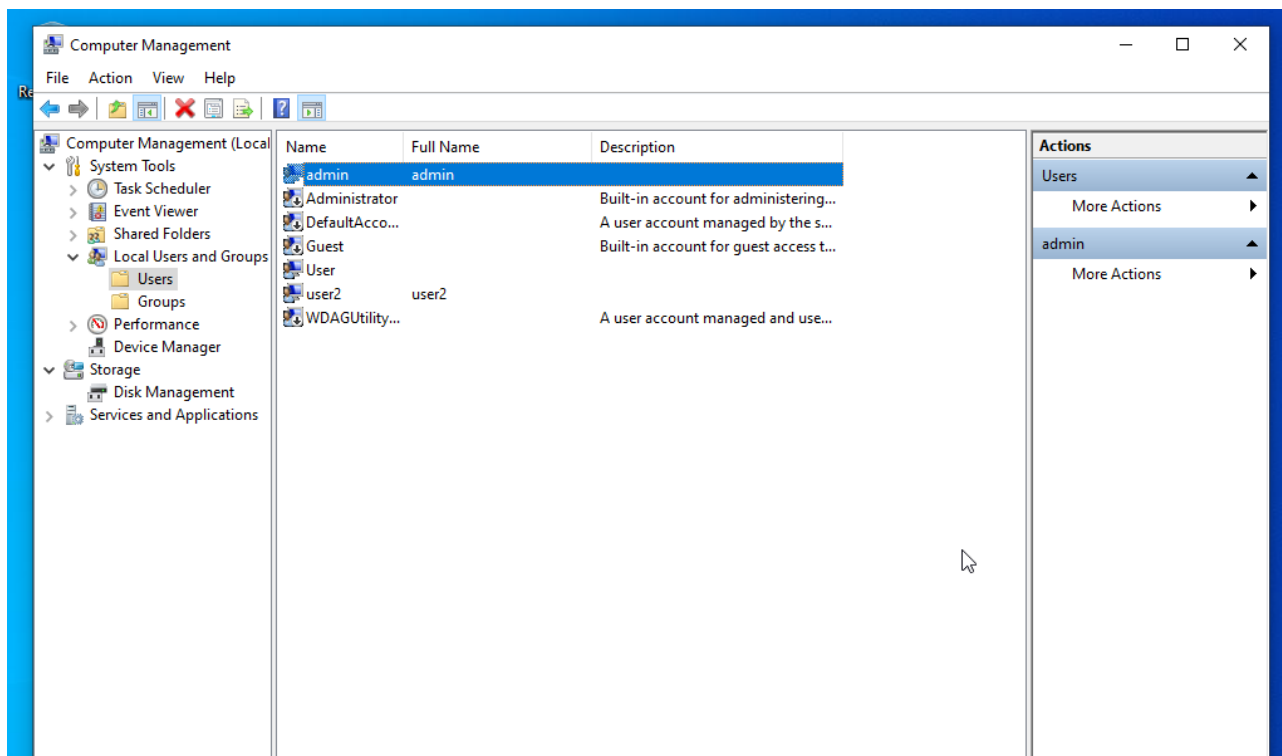
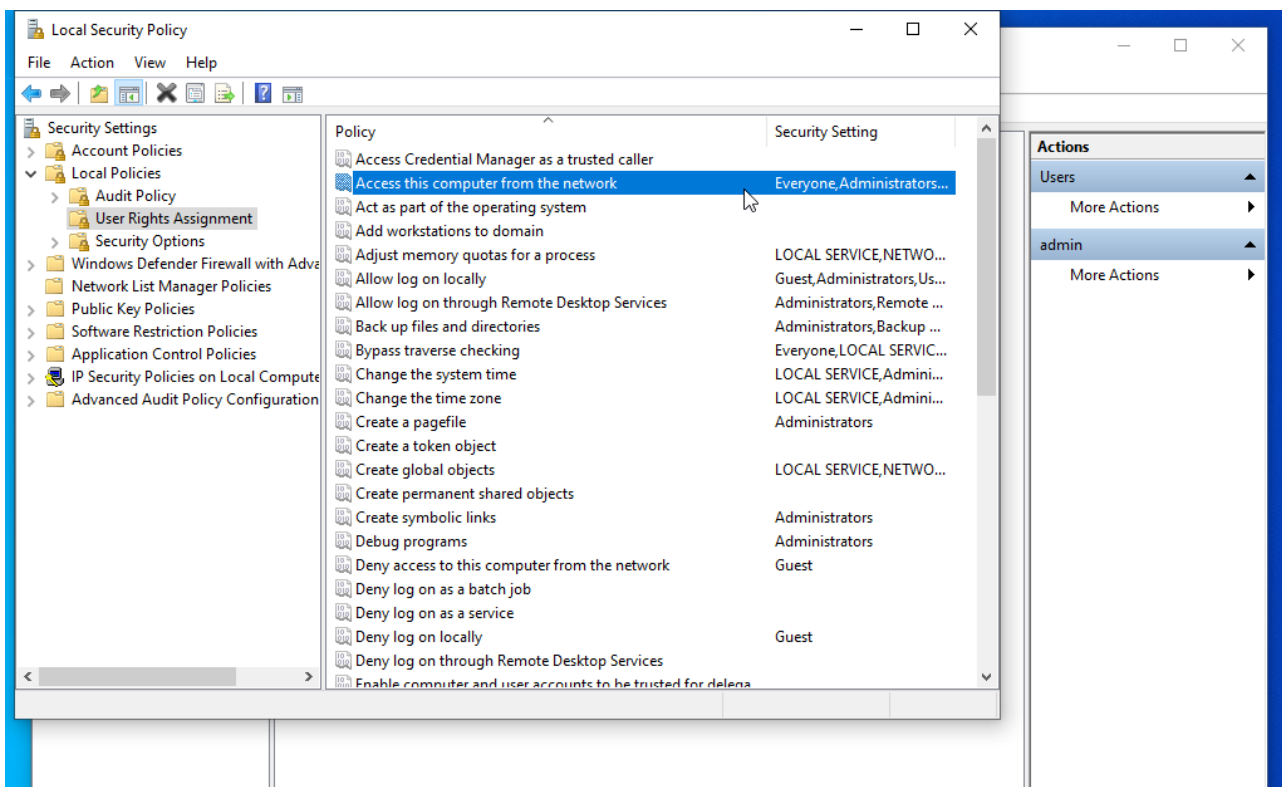


Step 1: Создать 2 учётные записи:

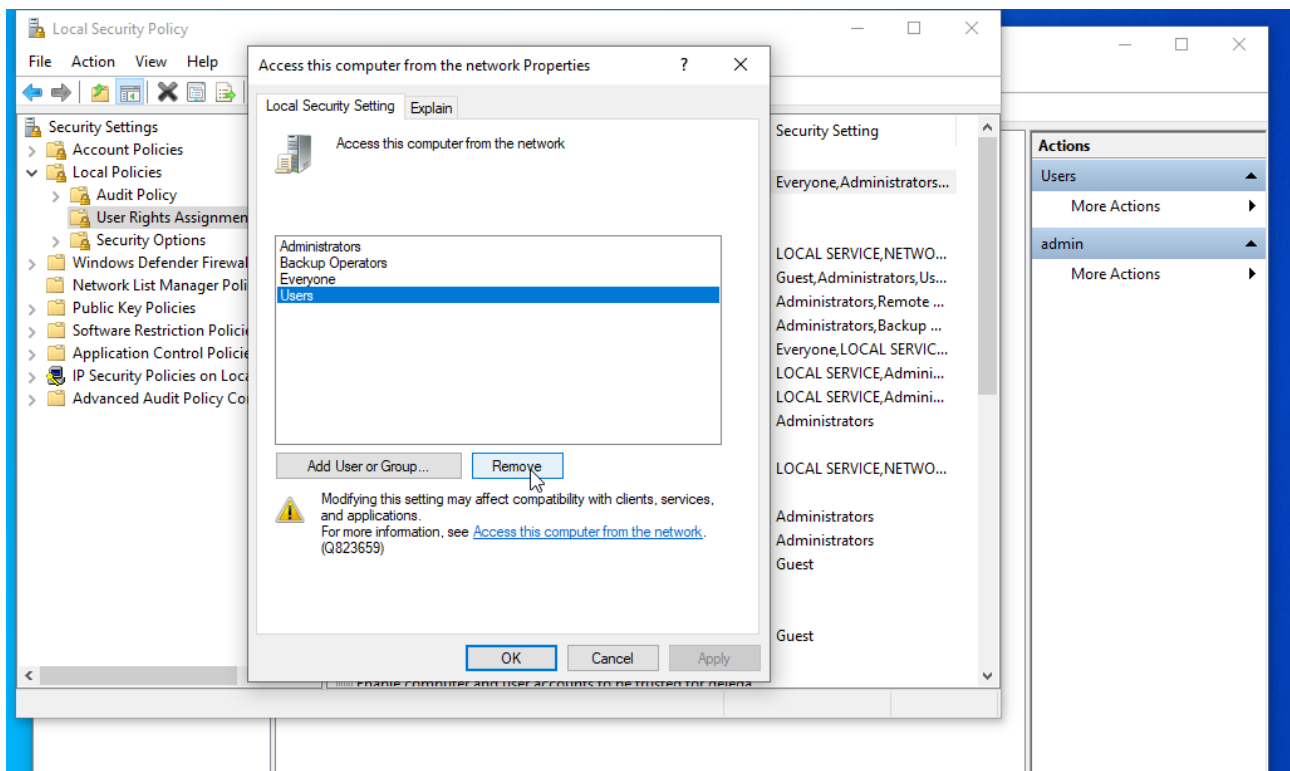
- с запретом доступа по сети к системе,
- с запретом удалённого доступа.



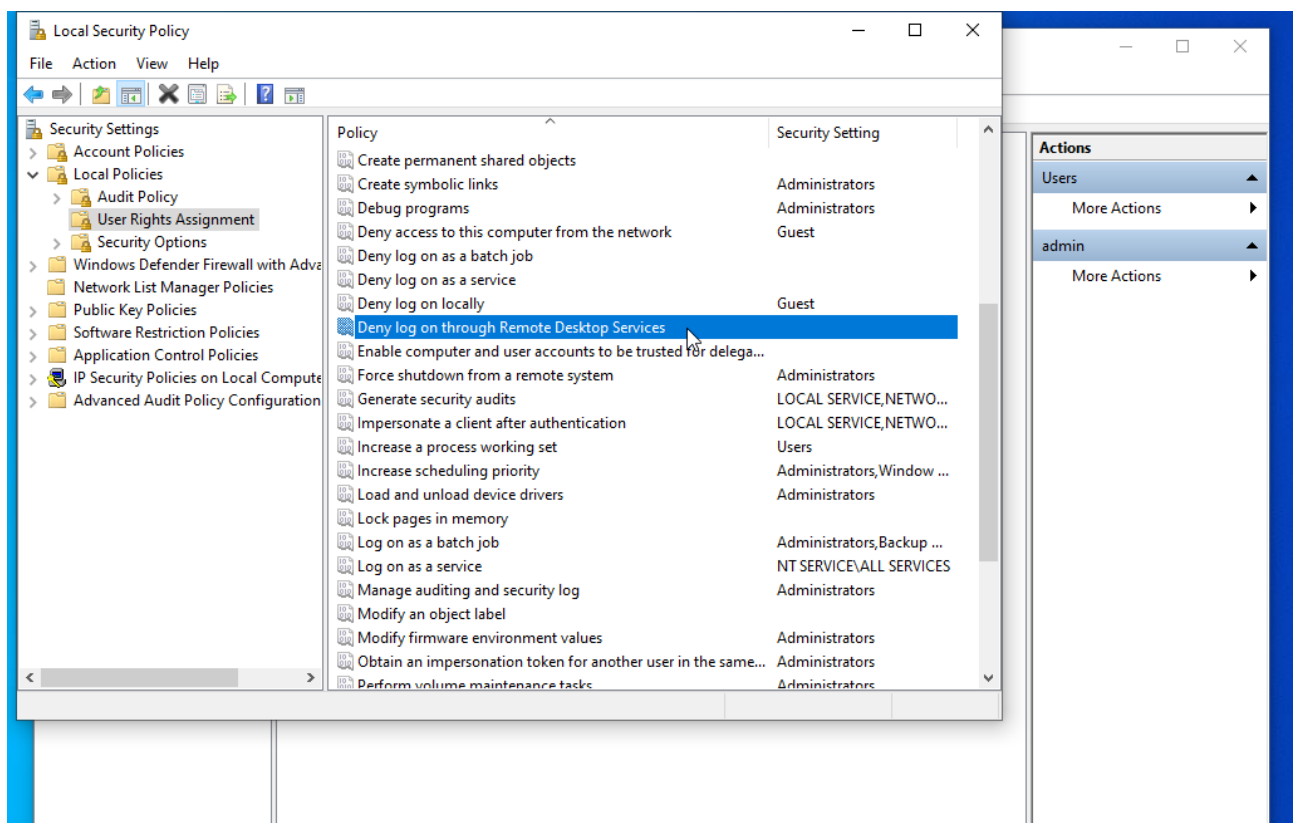
Тут я создал 2 аккаунта (в том случае admin и user2)



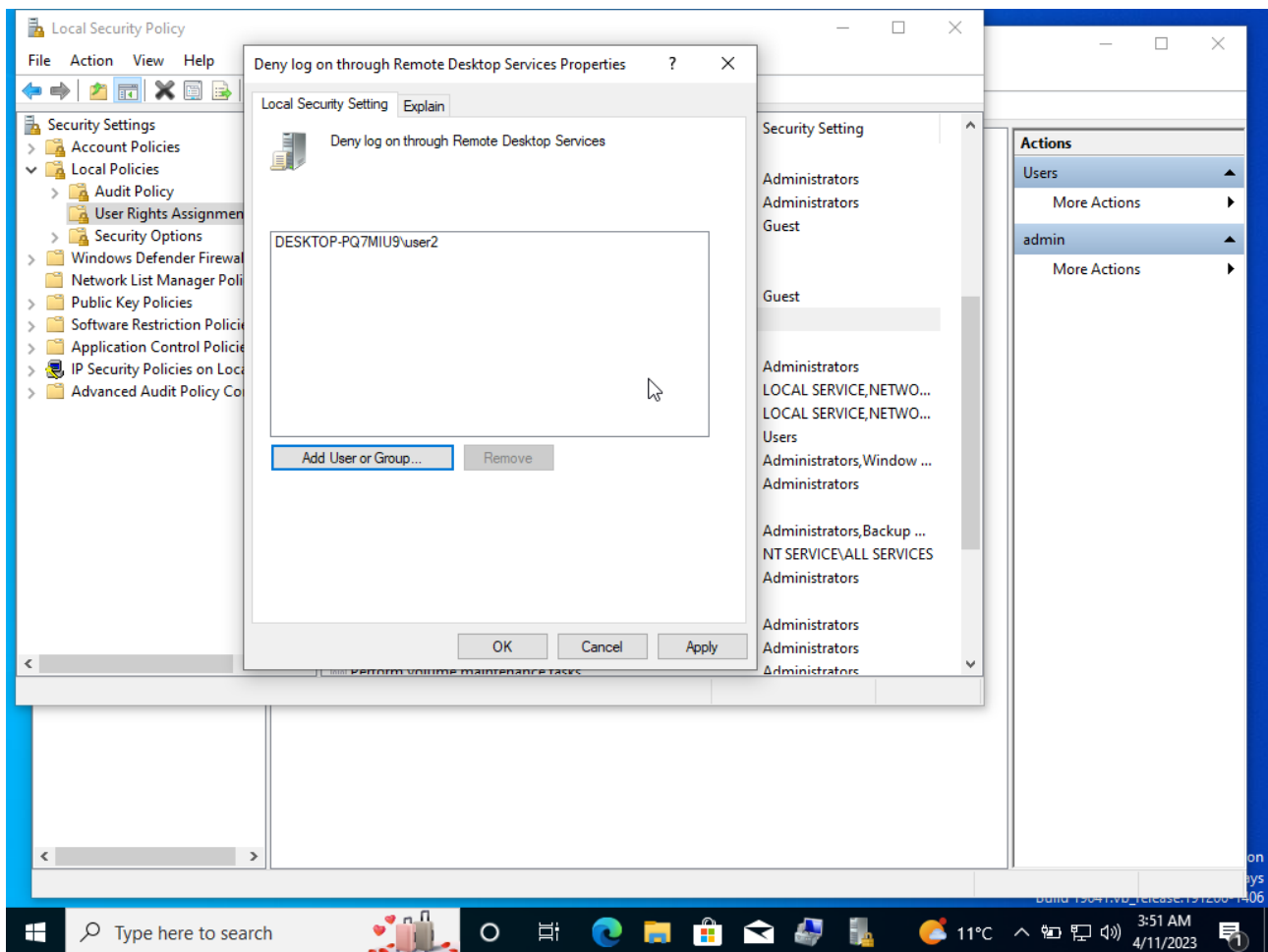
Вот тут в Локальной политике безопасности выбираю эту функцию.



Убираю группу пользователей (пользователи не смогут получать доступ к сети)

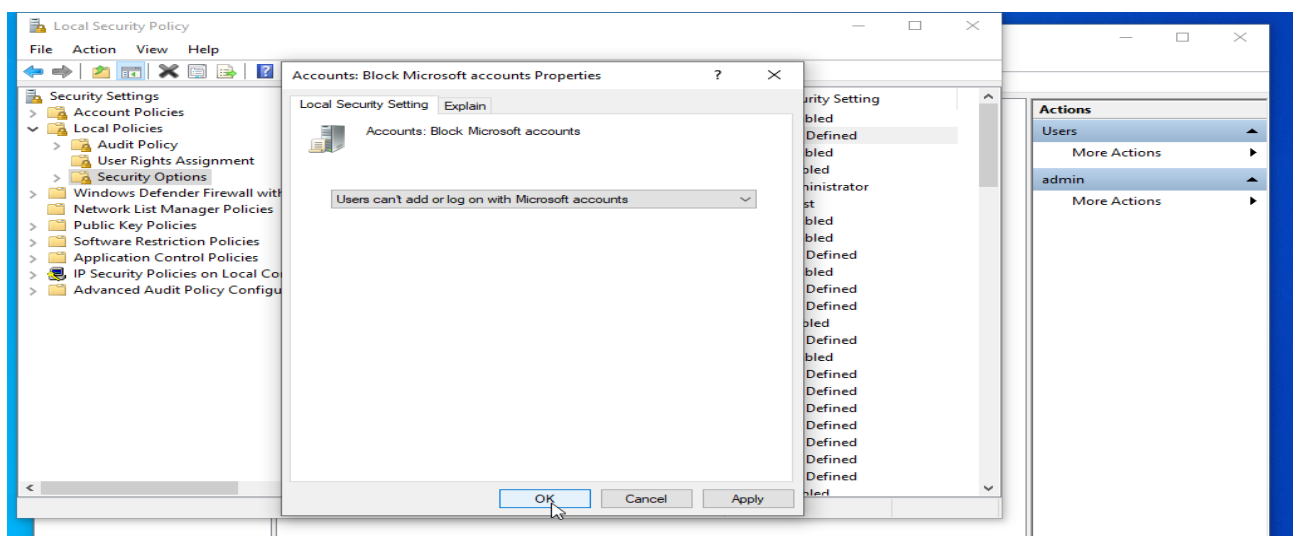


Для запрета для удалённого доступа я выбрал эту функцию



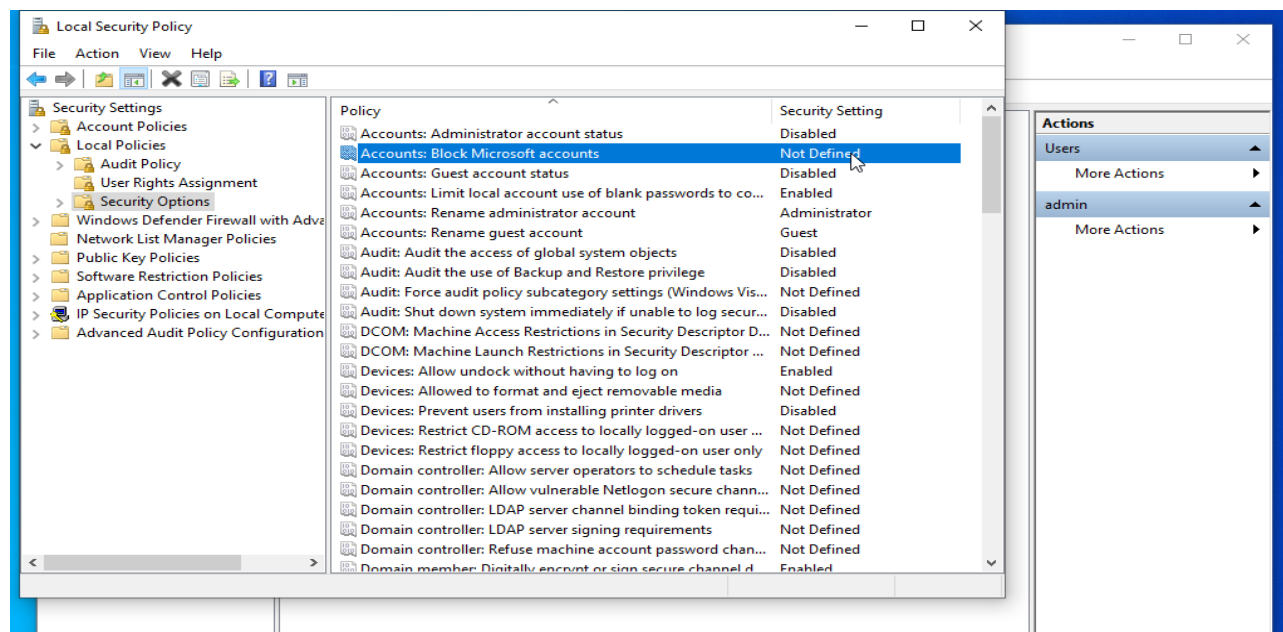
Добавил пользователя user2 в «черный список».

Step 2: Настроить с помощью GPO локально/в домене запрет аутентификации с помощью учётных записей Майкрософт.

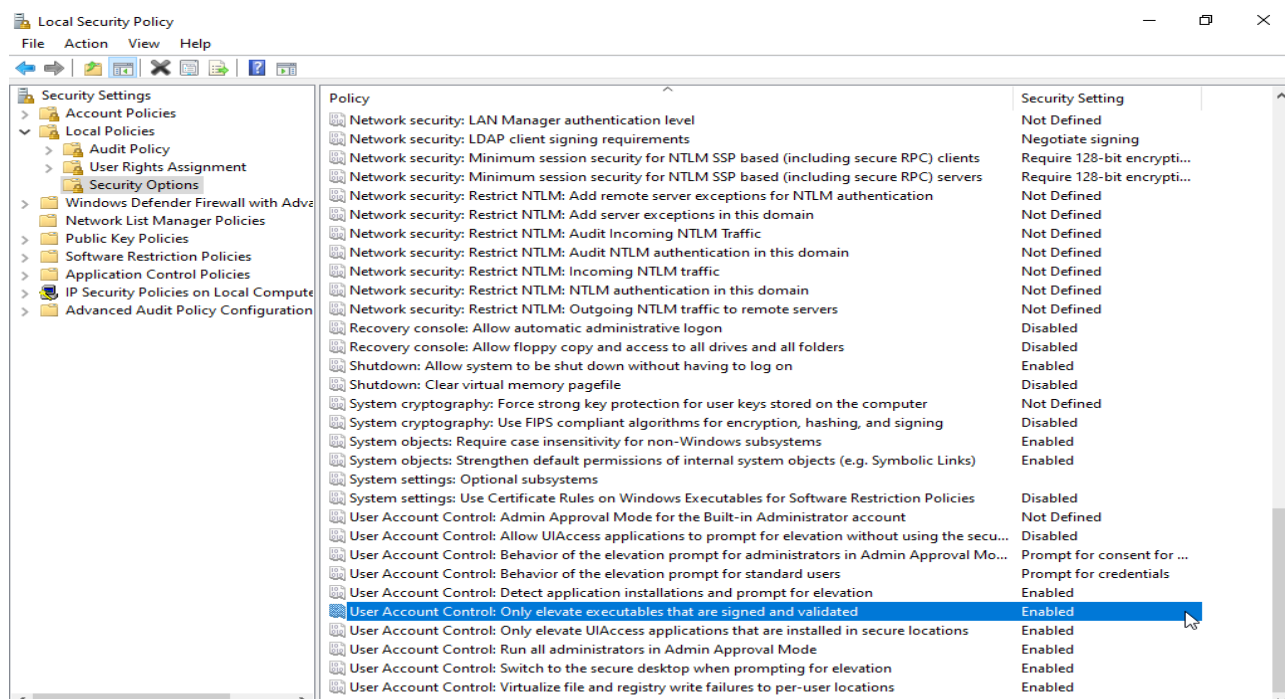


С помощью групповой политики выбрал опцию «Блокировать аккаунты Microsoft» (тип показано через LSP, но сделано именно через GPO)

Изначально сделал именно через локальную политику безопасности (не сразу понял надо было именно через групповую политику)

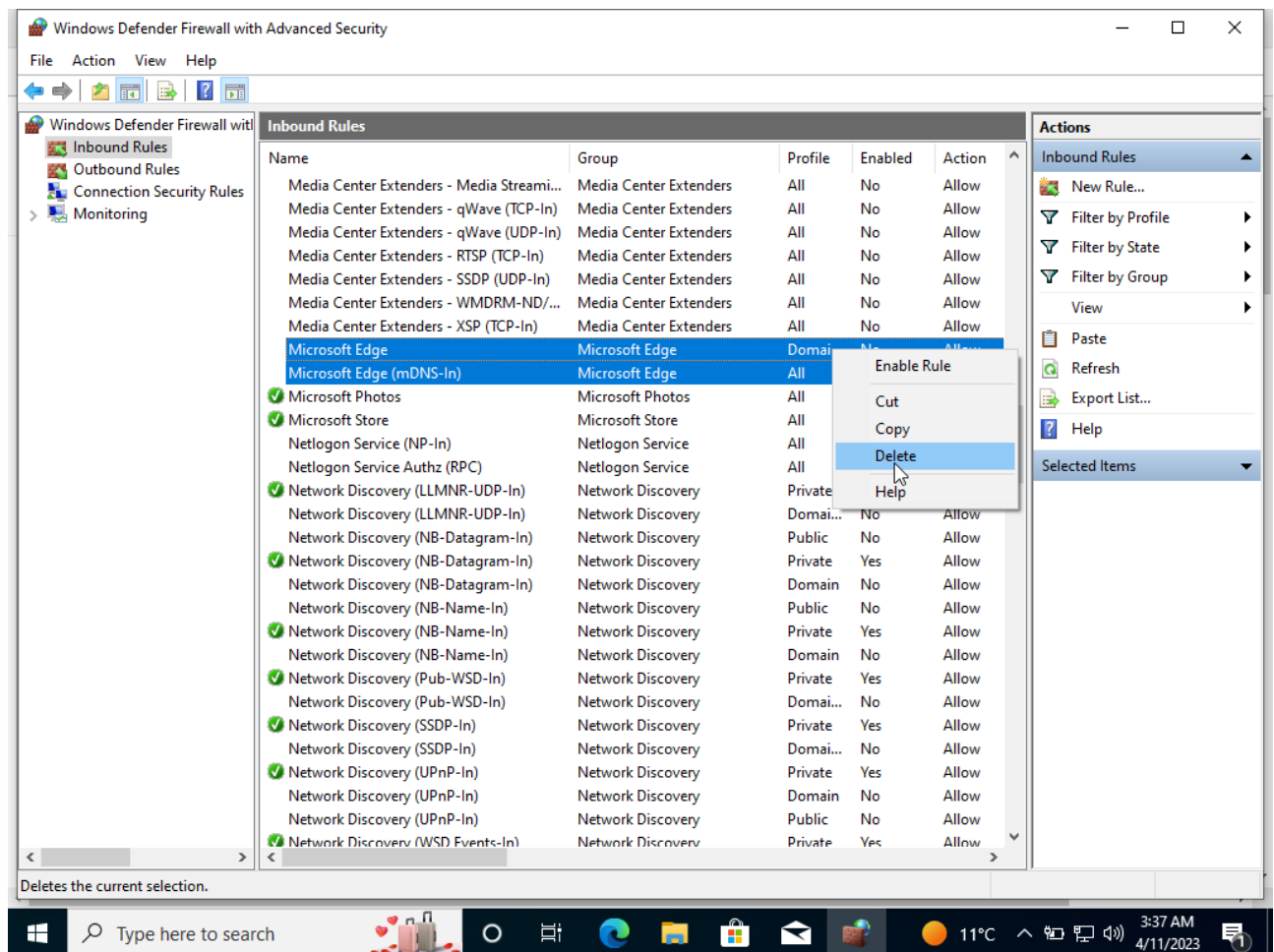


Step 3: Настроить контроль учётных записей так, чтобы у пользователей запрос на подтверждение действия с административными привилегиями автоматически отклонялся.

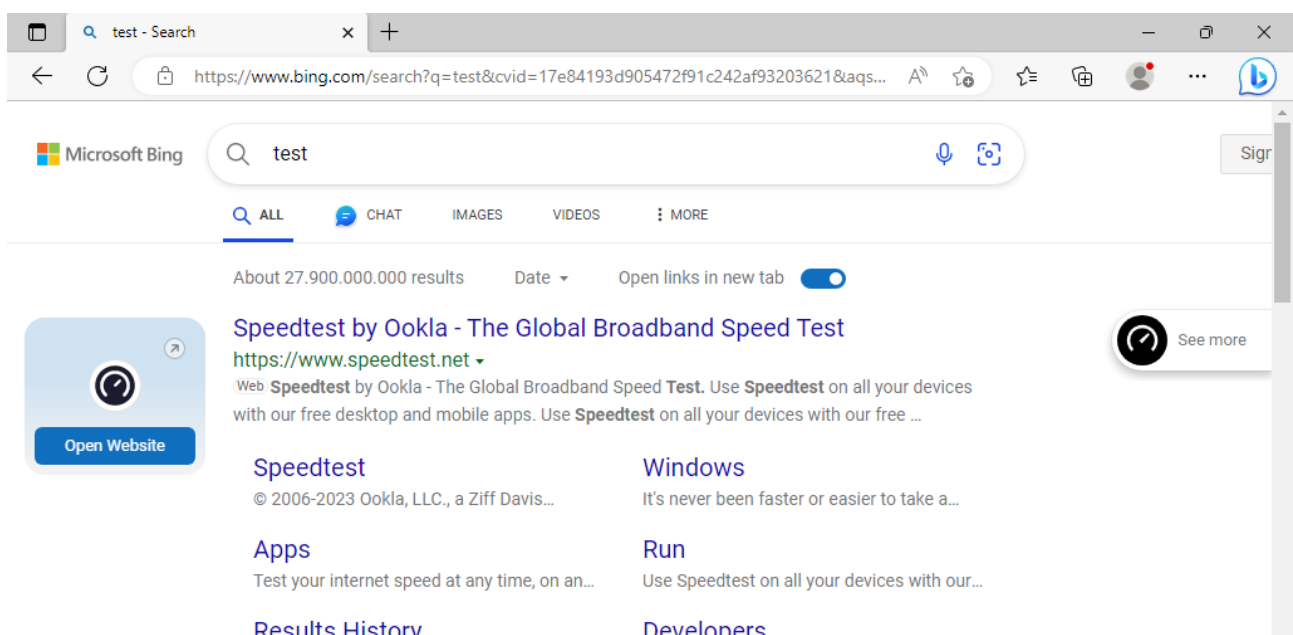


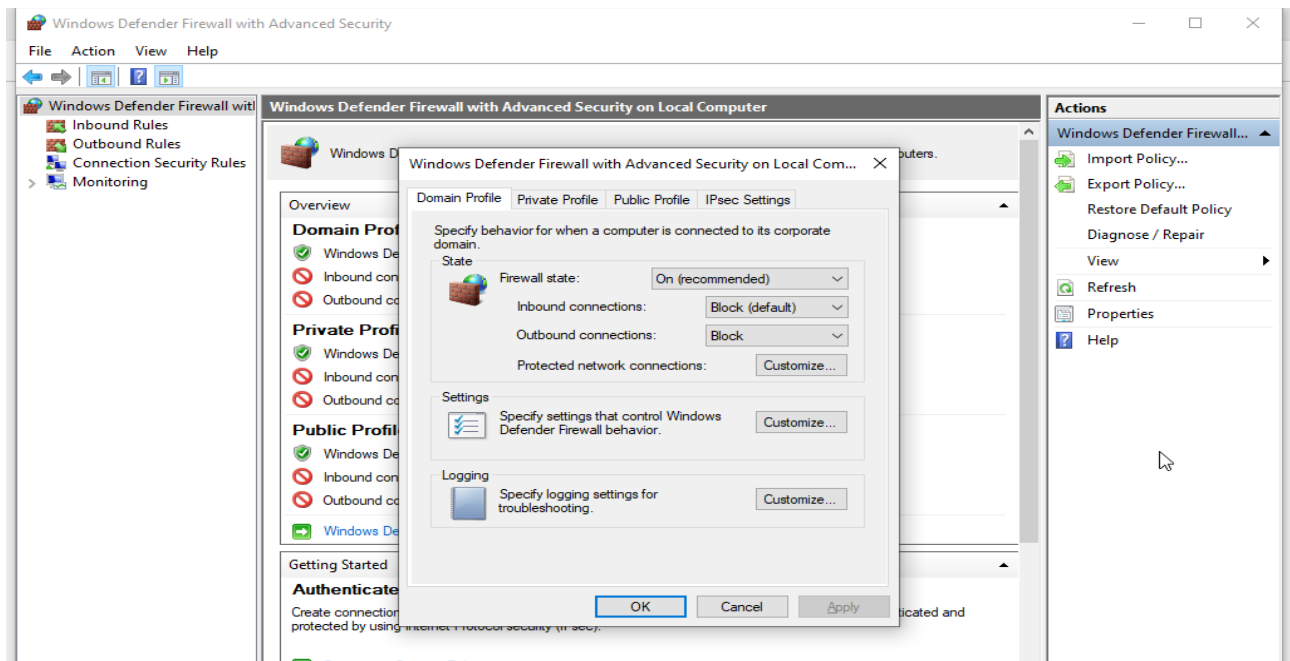
Включаю эту опцию, чтобы любой админ. процесс сразу отклонялся (будет ошибка — что данное действие было заблокировано политиков)

Step 4: Настроить «огненную стену» защитника Windows так, чтобы он запрашивал разрешение пользователя при установлении нового соединения программой или службой.



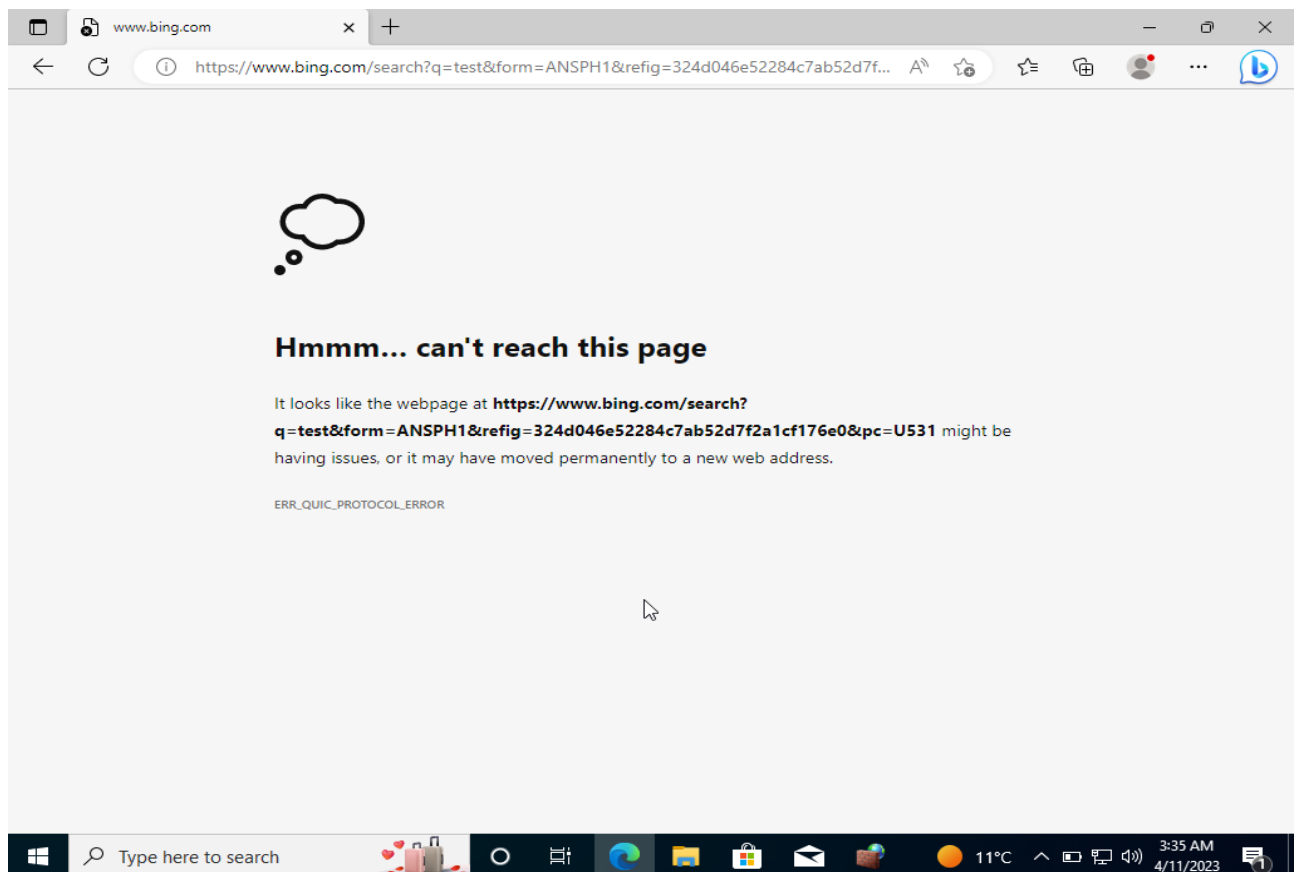
Для этого примера я решил удалить правила с Microsoft Edge



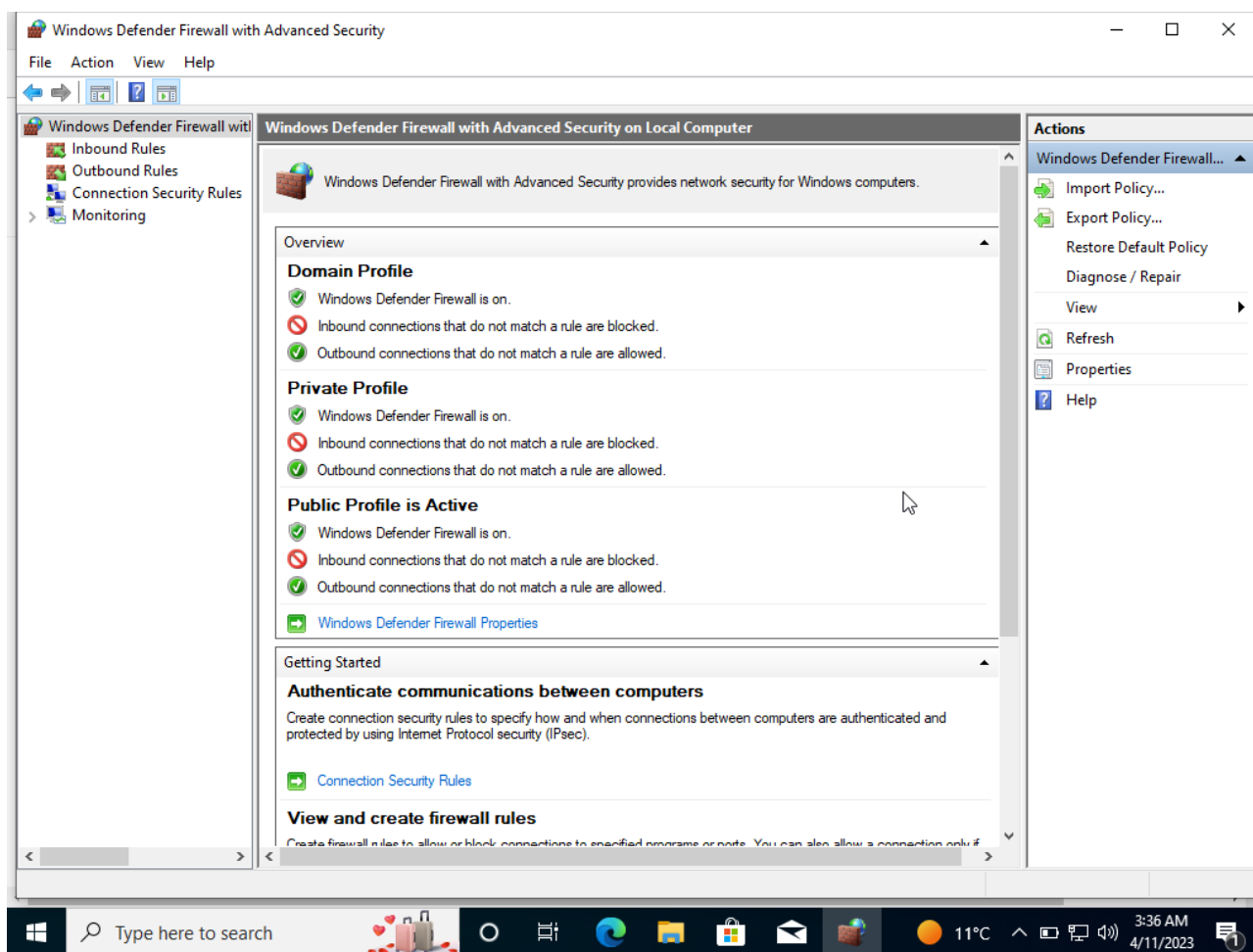


Я следовал шагам лекции, но почему то ничего не получилось.

Решил я попробовать вот так (знаю, что в лекции было не так).



У меня появилась ошибка об интернете, но никакого окна от «Огненной стены» о том, что можно создать новые правила — не появилось.



Вернул в первоначальное состояние, удалил пару правил (включая Edge) — но результат прежний. (P.S. Не удивлюсь если причиной этому станет — права пользователя)