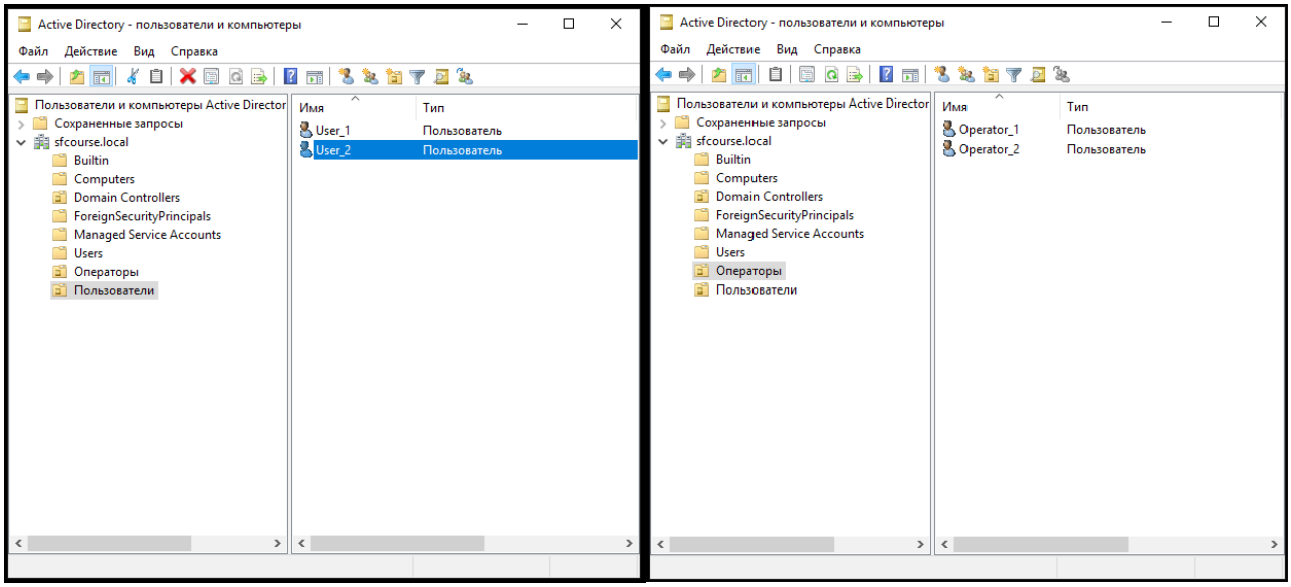
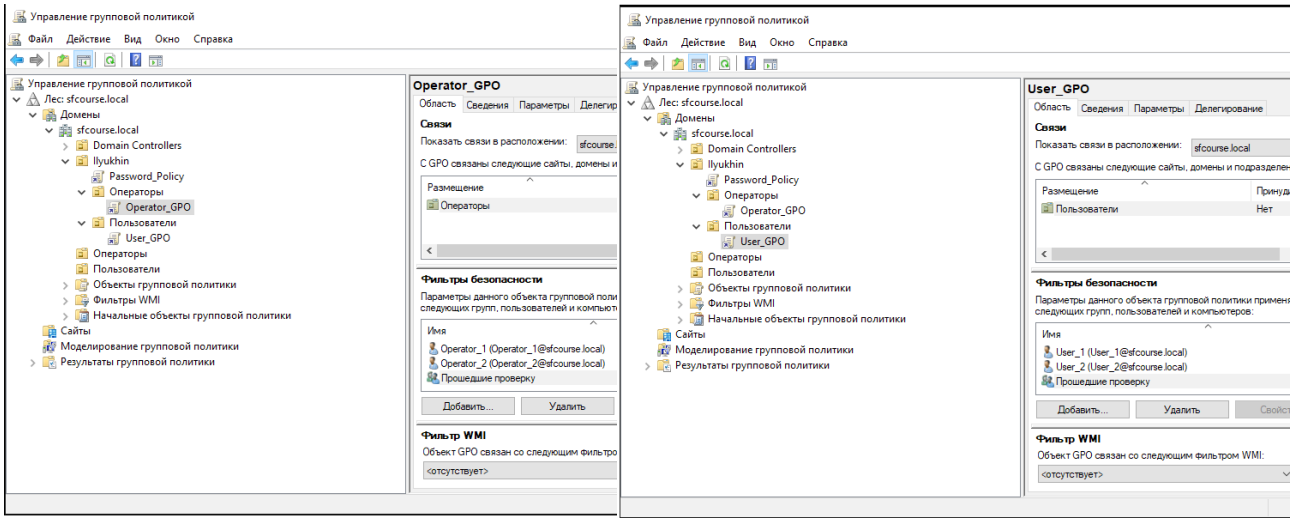
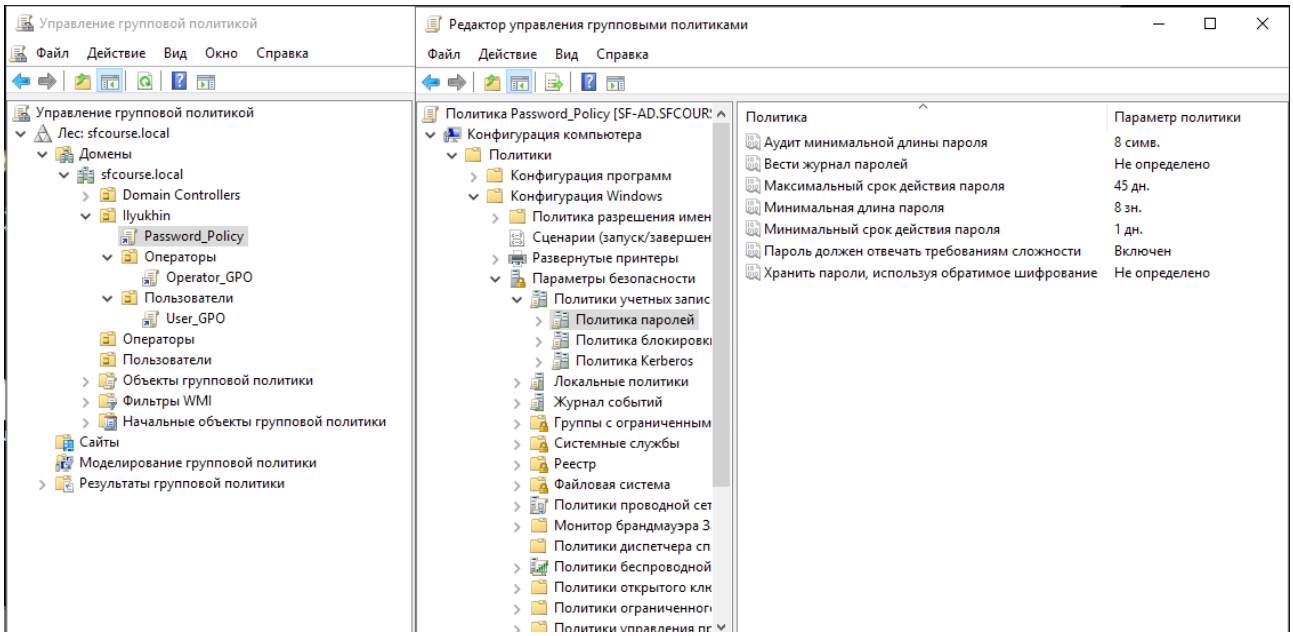
1. Созданы 4 пользователя с двумя функциональными ролями: «пользователи» и «операторы».



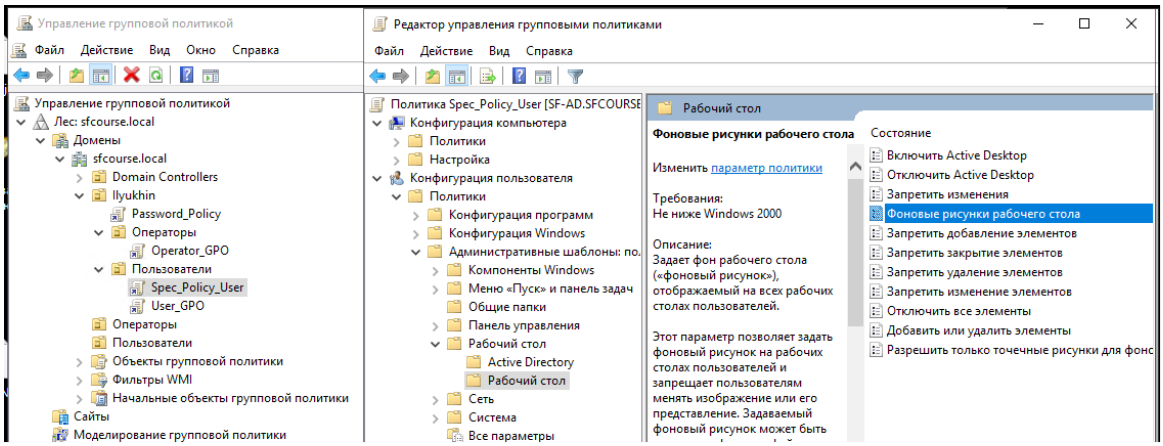
2. Для каждой группы создана групповая политика «Operator_GPO» и «User_GPO».

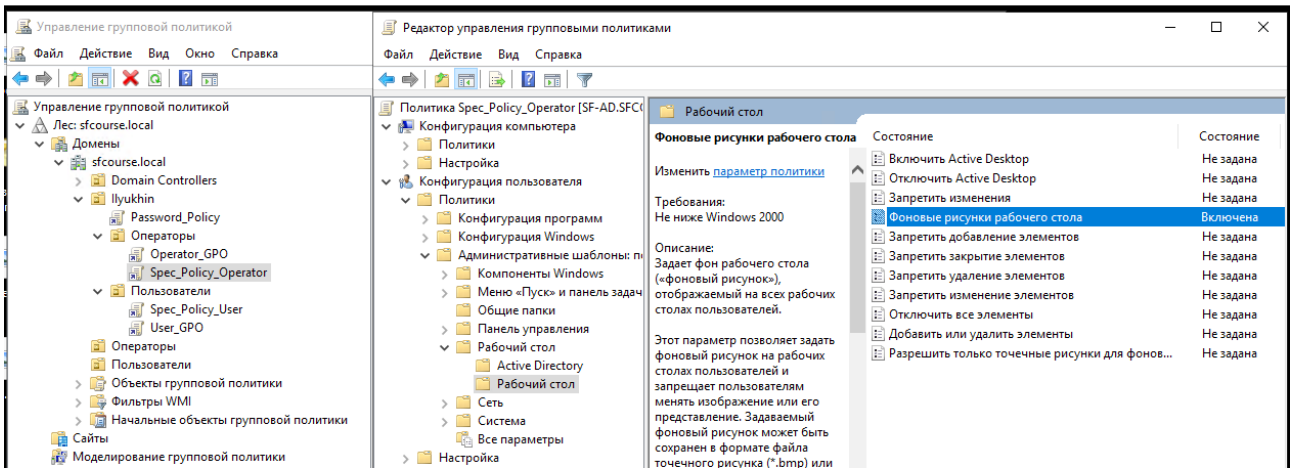


3. Для всех ролей настройка групповой политик паролей.

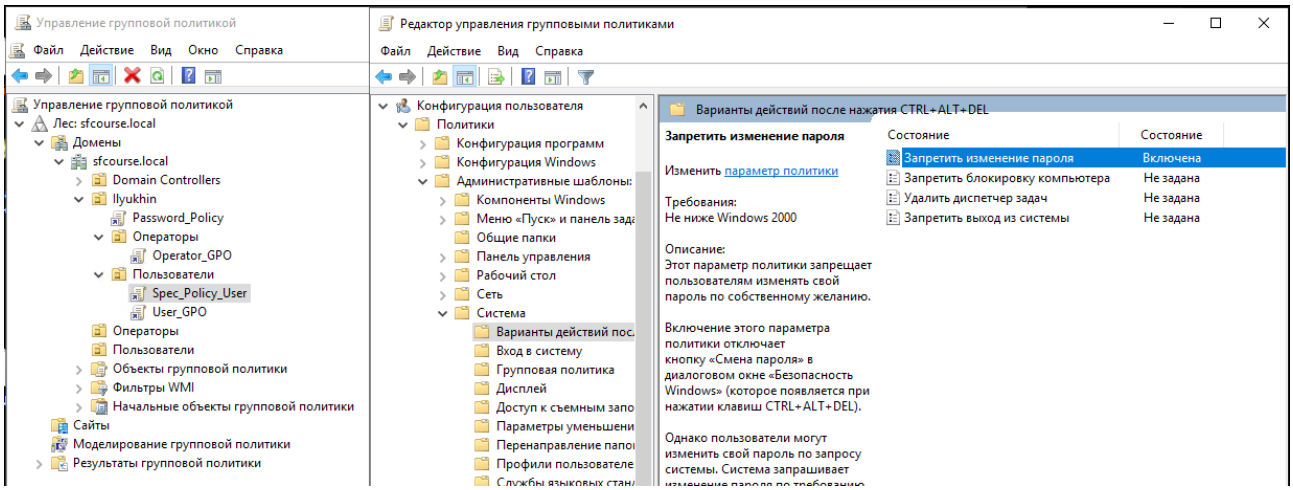


4.1 и 5.1. Установка фона для рабочего стола через групповую политику для ролей «Операторы» и «Пользователи».

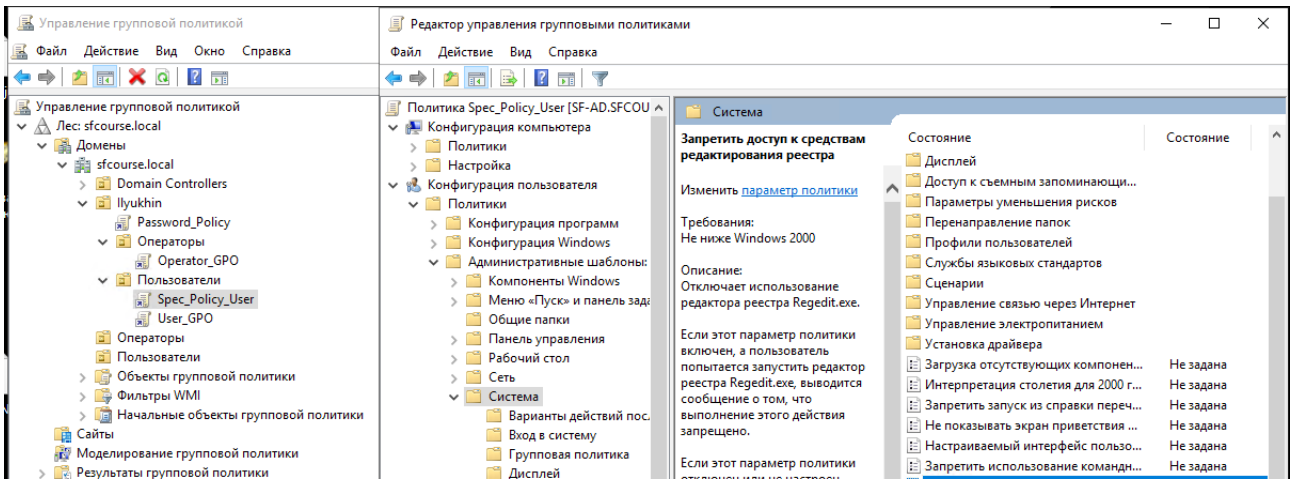


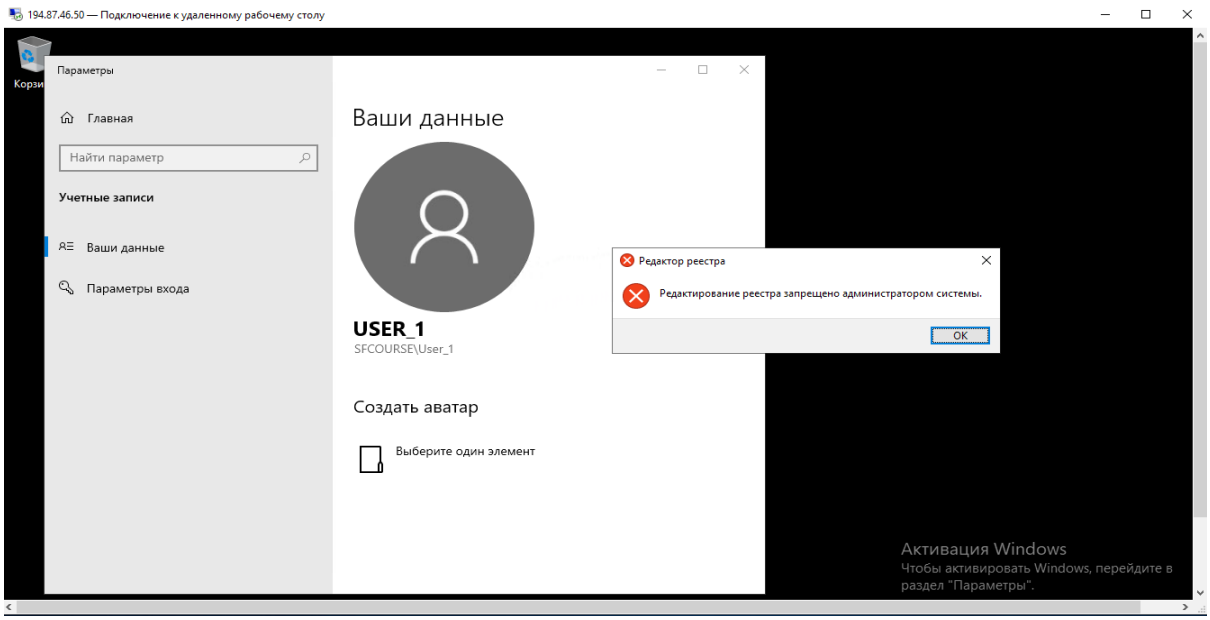


4.2. Отключение возможности изменения пароля для роли «Пользователи» через групповую политику.

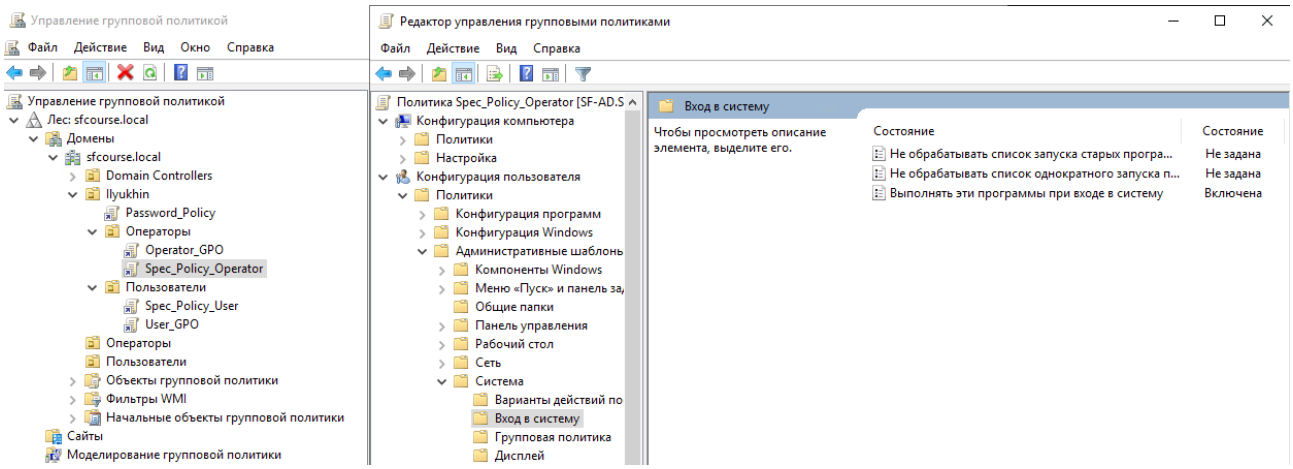


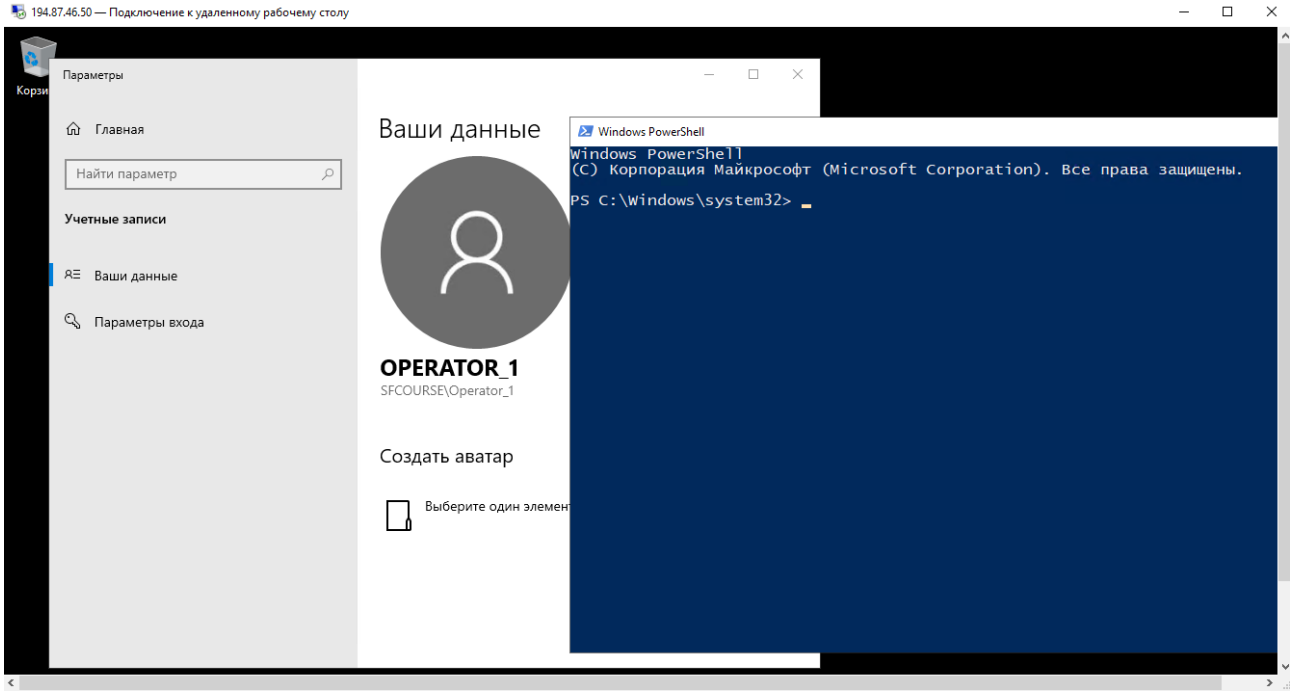
4.3. Запрет на редактирование реестра Windows.



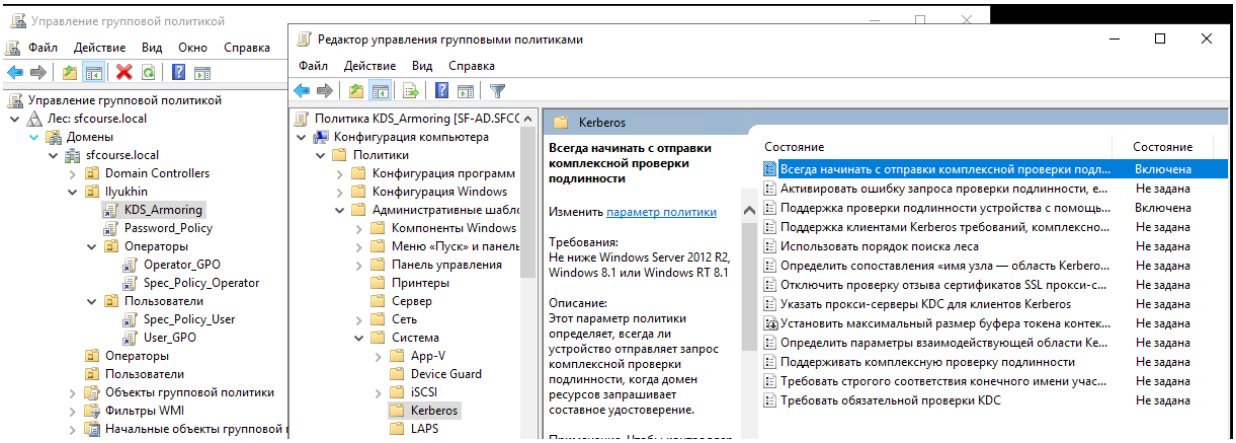


5.2. Настройка автозапуска MS PowerShell при входе в систему пользователей группы «Операторы».

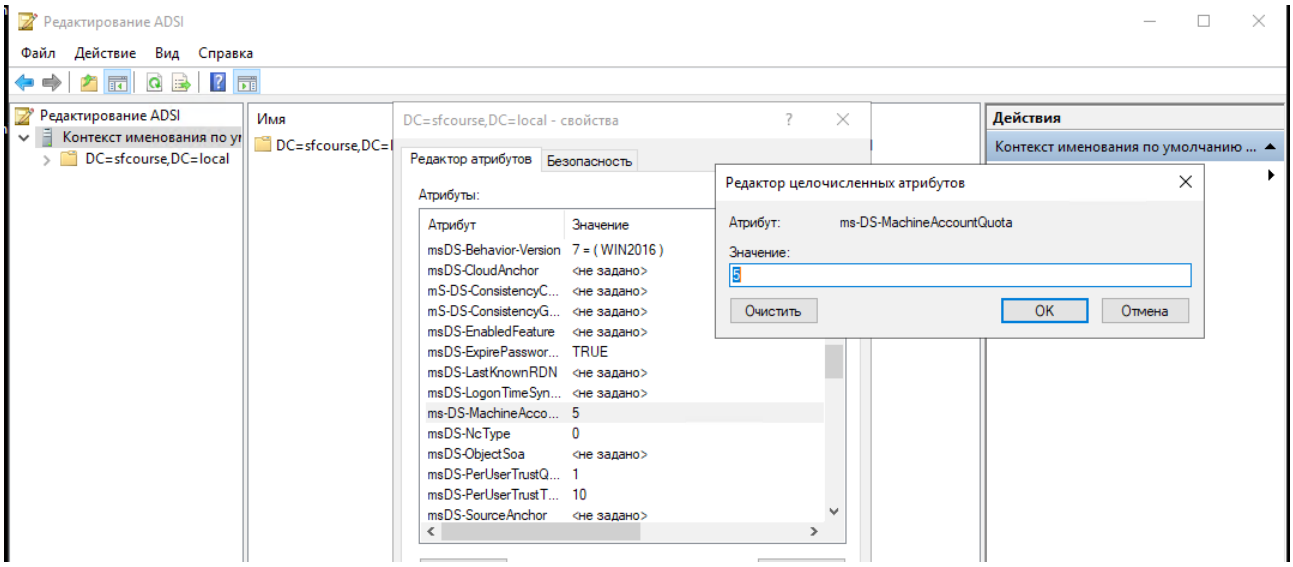




6. Включение KDC Armoring



Настройка ms-MachineAccountQuota.



Вывод команды gpresult /scope user

```
C:\Users\Администратор>gpresult /scope user /z

Программа формирования отчета групповой политики операционной системы
Microsoft (R) Windows (R) версии 2.0
© Корпорация Майкрософт (Microsoft Corporation), 2018. Все права защищены.

Создано ?21.?10.?2023 в 23:35:28

Данные RSOP для SFCOURSE\Administrator на SF-AD : Режим ведения журнала
-----------------------------------------------------------------------------
Конфигурация ОС:            Основной контроллер домена
Версия ОС:                  10.0.17763
Имя сайта:                  Н/Д
Перемещаемый профиль:                   Н/Д
Локальный профиль:          C:\Users\Администратор
Подключение по медленному каналу: Нет

Конфигурация пользователя
-------------------------
    CN=Administrator,CN=Users,DC=sfcourse,DC=local
    Последнее применение групповой политики:  21.10.2023 в 22:14:30
    Групповая политика была применена с:      SF-AD.sfcourse.local
    Порог медленного канала для групповой политики: 500 kbps
    Имя домена:                         SFCOURSE
    Тип домена:                         Windows 2008 или более поздняя версия

    Примененные объекты групповой политики
    --------------------------------------
        Н/Д

    Следующие политики GPO не были применены, так как они отфильтрованы
    --------------------------------------------------------------------
        Local Group Policy
            Фильтрация:  Не применено (причина неизвестна)
```

```
      Пользователь является членом следующих групп безопасности
      ----------------------------------------------------------
        Пользователи домена
        Все
        Администраторы
        Пользователи
        Пред-Windows 2000 доступ
        REMOTE INTERACTIVE LOGON
        ИНТЕРАКТИВНЫЕ
        Прошедшие проверку
        Данная организация
        ЛОКАЛЬНЫЕ
        Администраторы домена
        Владельцы-создатели групповой политики
        Администраторы схемы
        Администраторы предприятия
        Подтвержденное центром проверки подлинности удостоверение
        Группа с запрещением репликации паролей RODC
        Высокий обязательный уровень

    Привилегии безопасности данного пользователя
    --------------------------------------------
        Обход перекрестной проверки
        Управление аудитом и журналом безопасности
        Архивация файлов и каталогов
        Восстановление файлов и каталогов
        Изменение системного времени
        Завершение работы системы
        Принудительное удаленное завершение работы
        Смена владельцев файлов и других объектов
        Отладка программ
        Изменение параметров среды изготовителя
        Профилирование производительности системы
        Профилирование одного процесса
        Увеличение приоритета выполнения
        Загрузка и выгрузка драйверов устройств
        Создание файла подкачки
        Настройка квот памяти для процесса
        Отключение компьютера от стыковочного узла
        Выполнение задач по обслуживанию томов
        Имитация клиента после проверки подлинности
        Создание глобальных объектов
        Изменение часового пояса
        Создание символических ссылок
        Получить маркер олицетворения для другого пользователя в том же сеансе
        Разрешение доверия к учетным записям компьютеров и пользователей при
делегировании
        Увеличение рабочего набора процесса
        Добавление рабочих станций к домену

    Результирующий набор политик для пользователя
    ---------------------------------------------

        Установка программ
        ------------------
            Н/Д

        Сценарии входа
        --------------
            Н/Д

        Сценарии выхода
        ---------------
            Н/Д
```

```
Политики открытого ключа
------------------------
    Н/Д

Административные шаблоны
------------------------
    Н/Д

Перенаправление папок
---------------------
    Н/Д

Пользовательский интерфейс браузера Internet Explorer
-----------------------------------------------------
    Н/Д

Подключения Internet Explorer
-----------------------------
    Н/Д

URL-адреса Internet Explorer
----------------------------
    Н/Д

Безопасность Internet Explorer
------------------------------
    Н/Д

Программы Internet Explorer
---------------------------
    Н/Д
```

Вывод команды gpresult /scope computer.

```
C:\Users\Администратор>gpresult /scope computer /z

Программа формирования отчета групповой политики операционной системы
Microsoft (R) Windows (R) версии 2.0
© Корпорация Майкрософт (Microsoft Corporation), 2018. Все права защищены.

Создано ?21.?10.?2023 в 23:37:35


Данные RSOP для  на SF-AD : Режим ведения журнала
-------------------------------------------------

Конфигурация ОС:            Основной контроллер домена
Версия ОС:                  10.0.17763
Имя сайта:                  Default-First-Site-Name
Перемещаемый профиль:
Локальный профиль:
Подключение по медленному каналу: Нет


Конфигурация компьютера
-----------------------
    CN=SF-AD,OU=Domain Controllers,DC=sfcourse,DC=local
    Последнее применение групповой политики:  21.10.2023 в 23:34:33
    Групповая политика была применена с:      SF-AD.sfcourse.local
```

```
Порог медленного канала для групповой политики: 500 kbps
Имя домена:                         SFCOURSE
Тип домена:                         Windows 2008 или более поздняя версия

Примененные объекты групповой политики
--------------------------------------
    Default Domain Controllers Policy

Следующие политики GPO не были применены, так как они отфильтрованы
---------------------------------------------------------------------
    Local Group Policy
        Фильтрация:  Не применяется (пусто)

Компьютер является членом следующих групп безопасности
------------------------------------------------------

Результирующий набор политик для компьютера
-------------------------------------------

    Установка программ
    ------------------
        Н/Д

    Сценарии запуска
    ----------------
        Н/Д

    Сценарии завершения работы
    --------------------------
        Н/Д

    Политики учетных записей
    ------------------------
        Н/Д

    Политика аудита
    ---------------
        Н/Д

    Права пользователя
    ------------------
        GPO: Default Domain Controllers Policy
            Политика:             MachineAccountPrivilege
            Параметры компьютера: Прошедшие проверку

        GPO: Default Domain Controllers Policy
            Политика:             ChangeNotifyPrivilege
            Параметры компьютера: Все
                                  Прошедшие проверку
                                  LOCAL SERVICE
                                  NETWORK SERVICE
                                  Администраторы
                                  Пред-Windows 2000 доступ

        GPO: Default Domain Controllers Policy
            Политика:             IncreaseBasePriorityPrivilege
            Параметры компьютера: Администраторы
                                  Window Manager\Window Manager Group

        GPO: Default Domain Controllers Policy
            Политика:             TakeOwnershipPrivilege
            Параметры компьютера: Администраторы

        GPO: Default Domain Controllers Policy
```

```
    Политика:             RestorePrivilege
    Параметры компьютера: Администраторы
                          Операторы сервера
                          Операторы архива

GPO: Default Domain Controllers Policy
    Политика:             DebugPrivilege
    Параметры компьютера: Администраторы

GPO: Default Domain Controllers Policy
    Политика:             SystemTimePrivilege
    Параметры компьютера: LOCAL SERVICE
                          Администраторы
                          Операторы сервера

GPO: Default Domain Controllers Policy
    Политика:             SecurityPrivilege
    Параметры компьютера: Администраторы

GPO: Default Domain Controllers Policy
    Политика:             ShutdownPrivilege
    Параметры компьютера: Администраторы
                          Операторы сервера
                          Операторы печати
                          Операторы архива

GPO: Default Domain Controllers Policy
    Политика:             AuditPrivilege
    Параметры компьютера: LOCAL SERVICE
                          NETWORK SERVICE

GPO: Default Domain Controllers Policy
    Политика:             InteractiveLogonRight
    Параметры компьютера: Администраторы
                          Операторы учета
                          Операторы сервера
                          Операторы печати
                          Операторы архива
                          КОНТРОЛЛЕРЫ ДОМЕНА ПРЕДПРИЯТИЯ

GPO: Default Domain Controllers Policy
    Политика:             CreatePagefilePrivilege
    Параметры компьютера: Администраторы

GPO: Default Domain Controllers Policy
    Политика:             BatchLogonRight
    Параметры компьютера: Администраторы
                          Операторы архива
                          Пользователи журналов производительности
                          IIS_IUSRS

GPO: Default Domain Controllers Policy
    Политика:             NetworkLogonRight
    Параметры компьютера: Все
                          Прошедшие проверку
                          Администраторы
                          Пред-Windows 2000 доступ
                          КОНТРОЛЛЕРЫ ДОМЕНА ПРЕДПРИЯТИЯ

GPO: Default Domain Controllers Policy
    Политика:             SystemProfilePrivilege
    Параметры компьютера: Администраторы
                          NT SERVICE\WdiServiceHost
```

```
            GPO: Default Domain Controllers Policy
                Политика:             RemoteShutdownPrivilege
                Параметры компьютера: Администраторы
                                      Операторы сервера

            GPO: Default Domain Controllers Policy
                Политика:             BackupPrivilege
                Параметры компьютера: Администраторы
                                      Операторы сервера
                                      Операторы архива

            GPO: Default Domain Controllers Policy
                Политика:             EnableDelegationPrivilege
                Параметры компьютера: Администраторы

            GPO: Default Domain Controllers Policy
                Политика:             UndockPrivilege
                Параметры компьютера: Администраторы

            GPO: Default Domain Controllers Policy
                Политика:             SystemEnvironmentPrivilege
                Параметры компьютера: Администраторы

            GPO: Default Domain Controllers Policy
                Политика:             LoadDriverPrivilege
                Параметры компьютера: Администраторы
                                      Операторы печати

            GPO: Default Domain Controllers Policy
                Политика:             IncreaseQuotaPrivilege
                Параметры компьютера: LOCAL SERVICE
                                      NETWORK SERVICE
                                      Администраторы

            GPO: Default Domain Controllers Policy
                Политика:             ProfileSingleProcessPrivilege
                Параметры компьютера: Администраторы

            GPO: Default Domain Controllers Policy
                Политика:             AssignPrimaryTokenPrivilege
                Параметры компьютера: LOCAL SERVICE
                                      NETWORK SERVICE

        Параметры безопасности
        ----------------------
            Н/Д

            GPO: Default Domain Controllers Policy
                Политика:             @wsecedit.dll,-59013
                Параметр:
MACHINE\System\CurrentControlSet\Services\NTDS\Parameters\LDAPServerIntegrity
                Параметры компьютера: 1

            GPO: Default Domain Controllers Policy
                Политика:             @wsecedit.dll,-59043
                Параметр:
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecurit
ySignature
                Параметры компьютера: 1

            GPO: Default Domain Controllers Policy
                Политика:             @wsecedit.dll,-59044
```

```
                Параметр:
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecurity
Signature
                Параметры компьютера: 1

            GPO: Default Domain Controllers Policy
                Политика:             @wsecedit.dll,-59018
                Параметр:
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSignOrSeal
                Параметры компьютера: 1

        Параметры журнала событий
        -------------------------
            Н/Д

        Группы с ограниченным доступом
        ------------------------------
            Н/Д

        Системные службы
        ----------------
            Н/Д

        Параметры реестра
        -----------------
            Н/Д

        Параметры файловой системы
        --------------------------
            Н/Д

        Политики открытого ключа
        ------------------------
            Н/Д

        Административные шаблоны
        ------------------------
            GPO: Default Domain Controllers Policy
                Идентификатор папки:
Software\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos\Parameters\En
ableCbacAndArmor
                Значение:    1, 0, 0, 0
                Состояние:       Включено
```