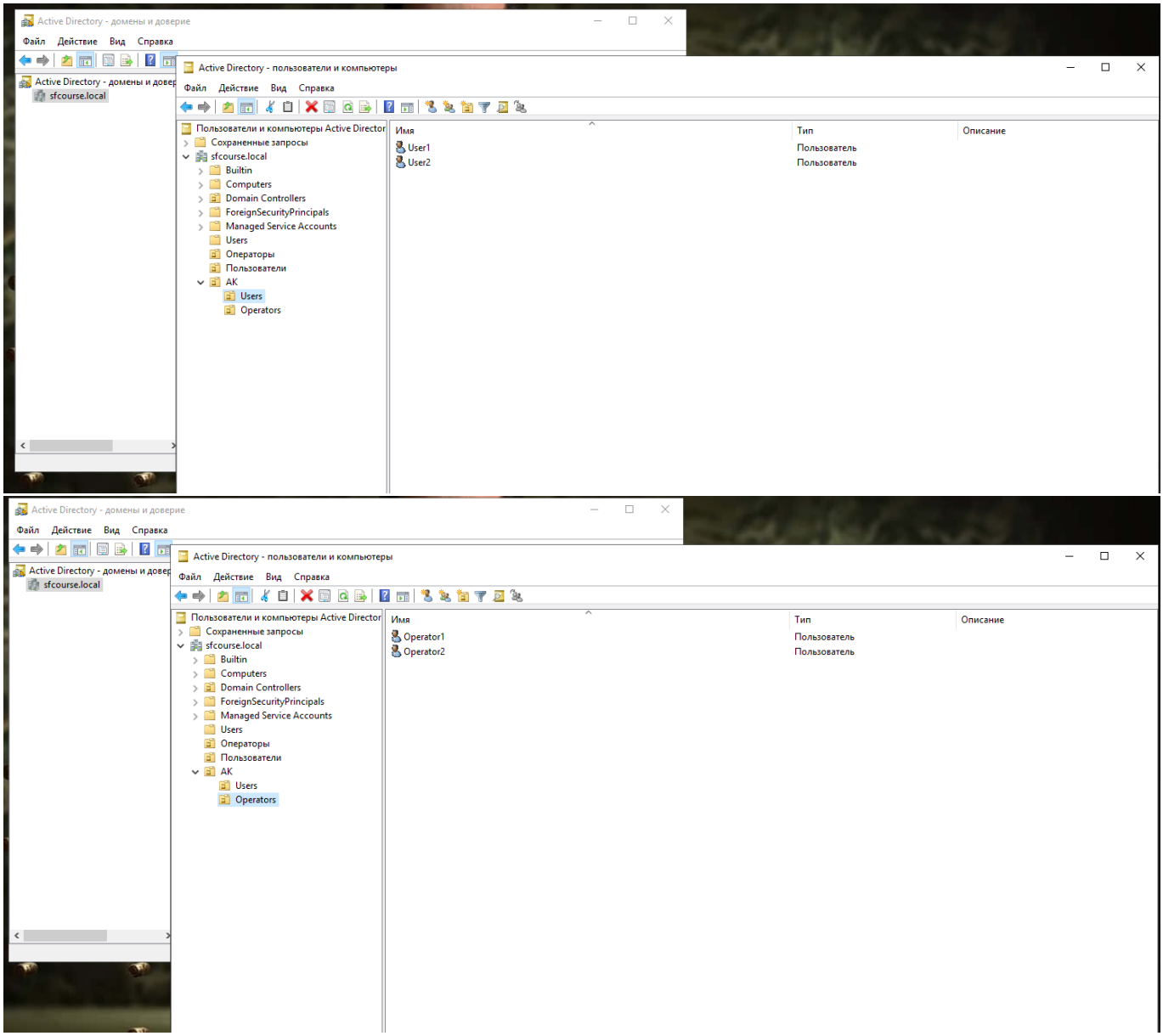
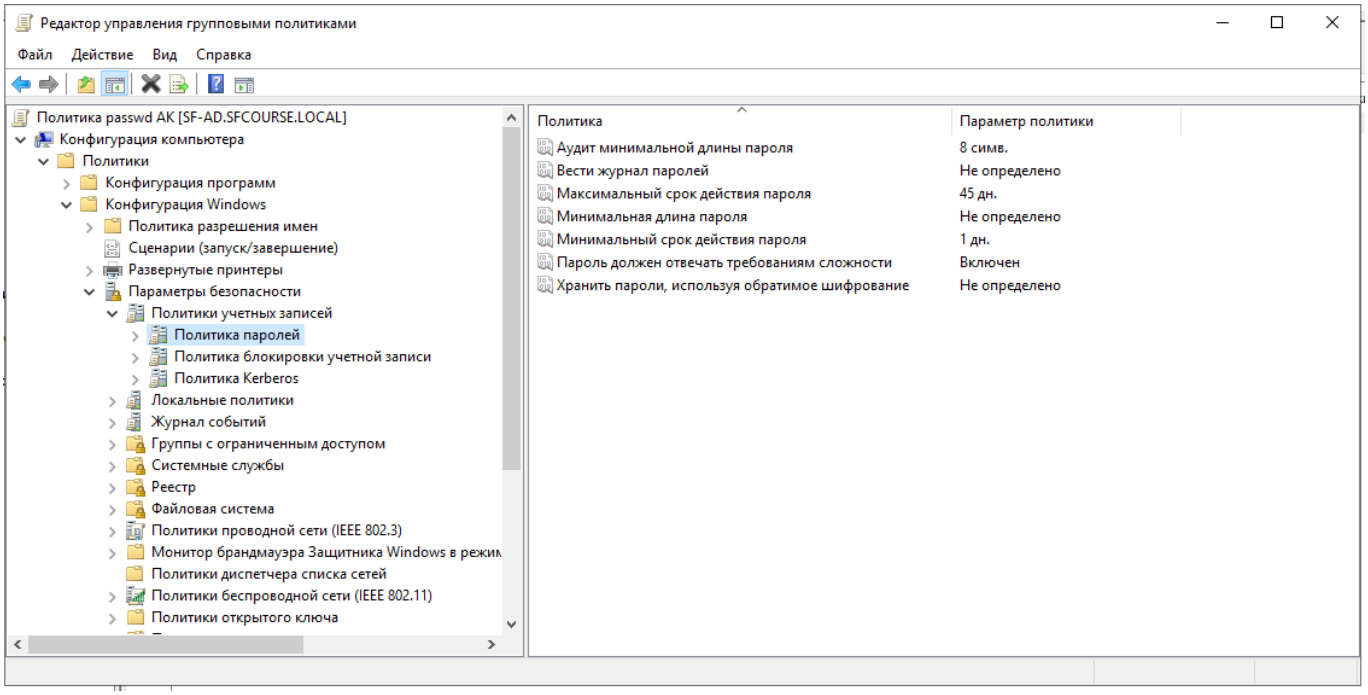
Практическое задание «Управление Active Directory»

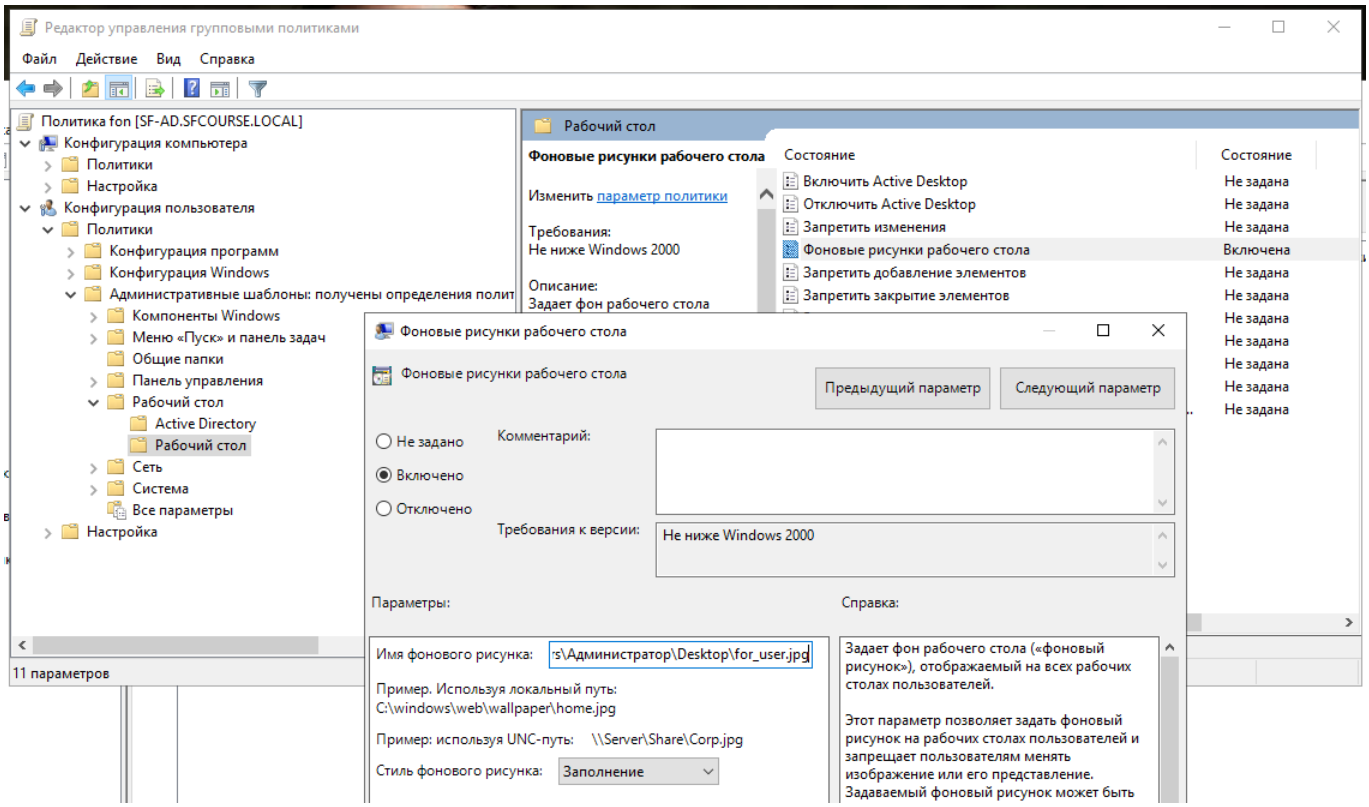
Создал организационное подразделение АК и группы Users, Operators с пользователями.



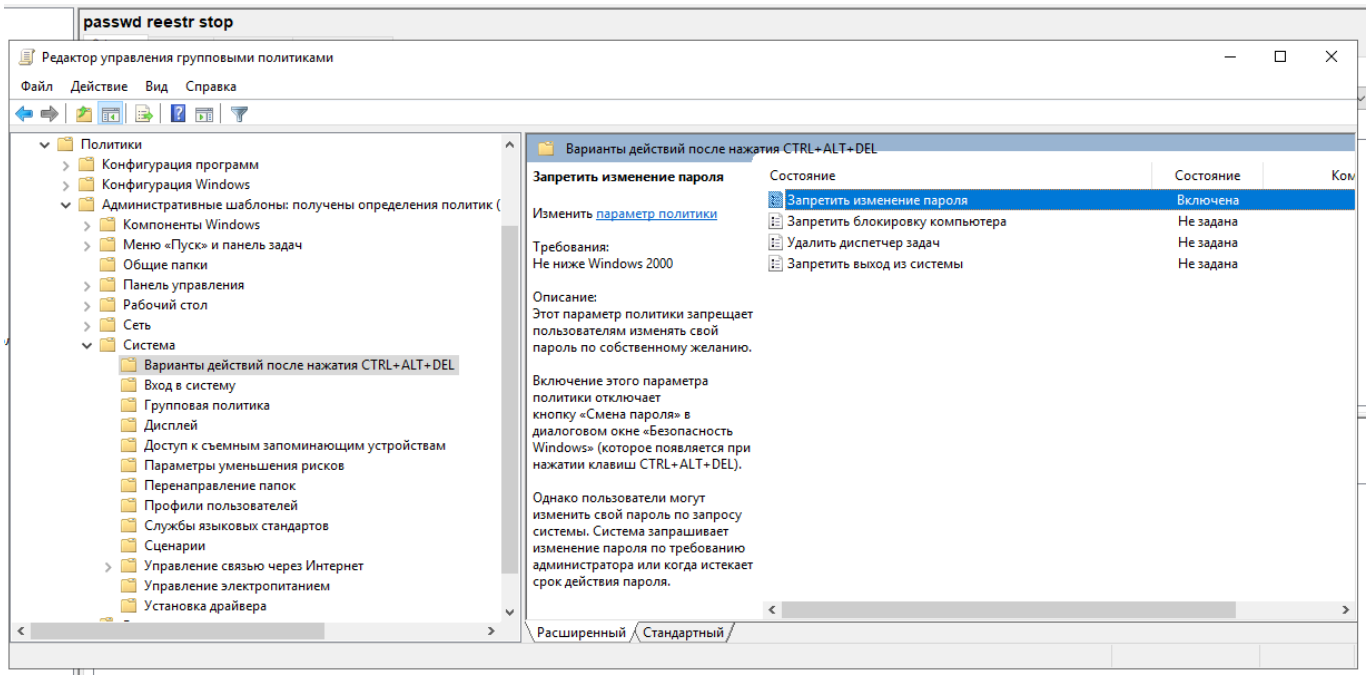
Создал групповую политику с общими правилами для паролей

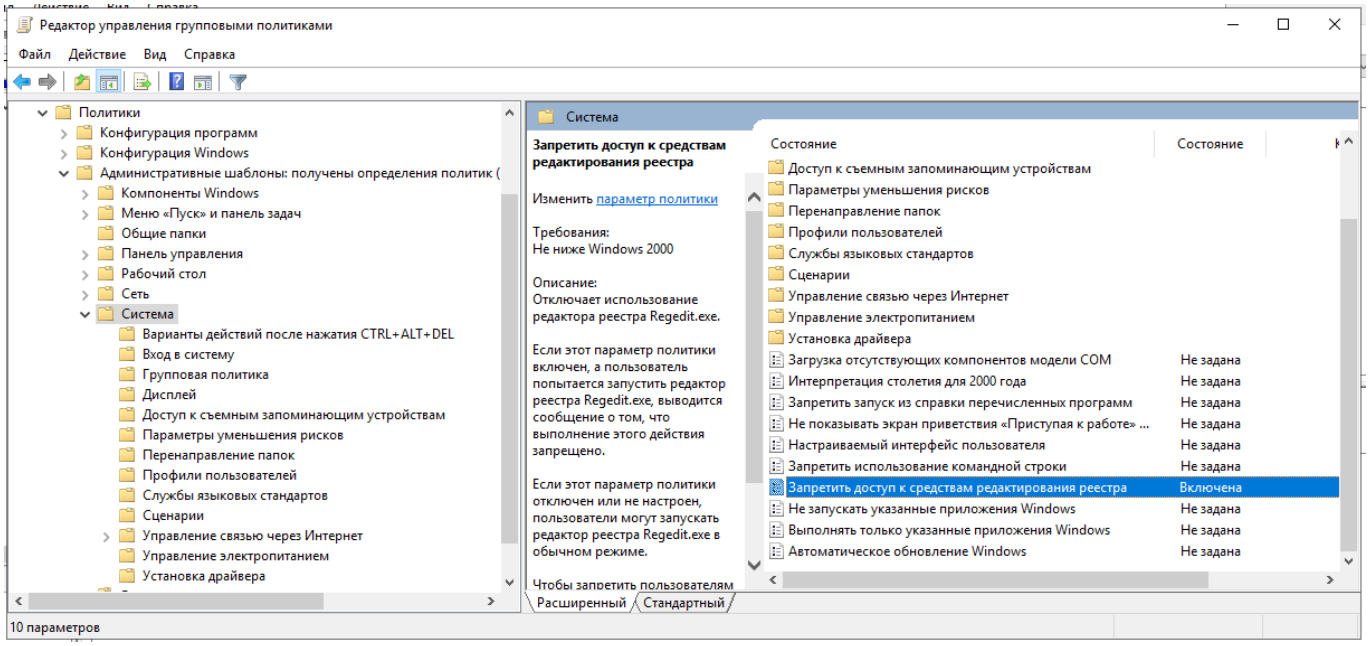


Для users установил рисунок рабочего стола через созданную политику fon

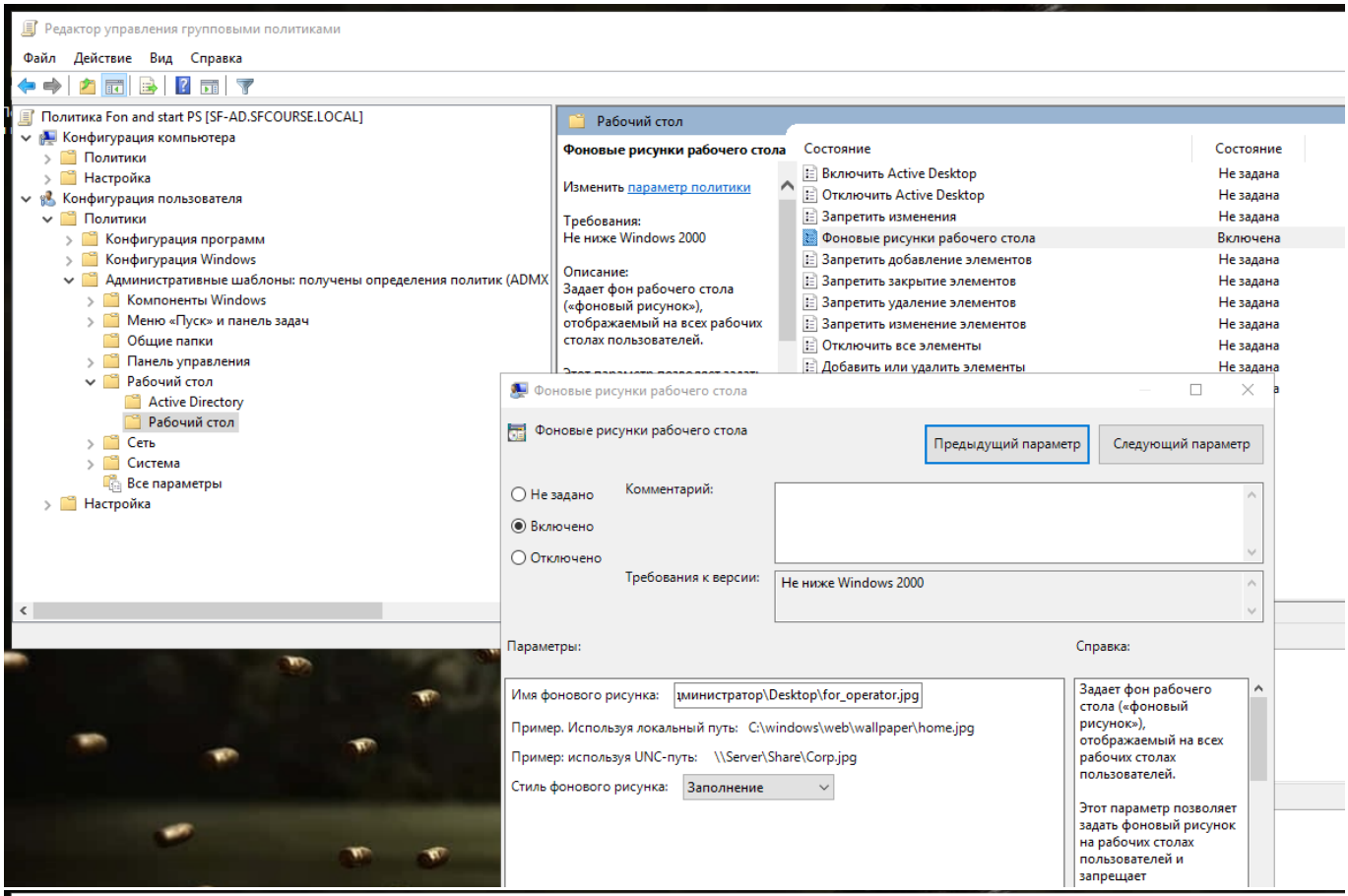


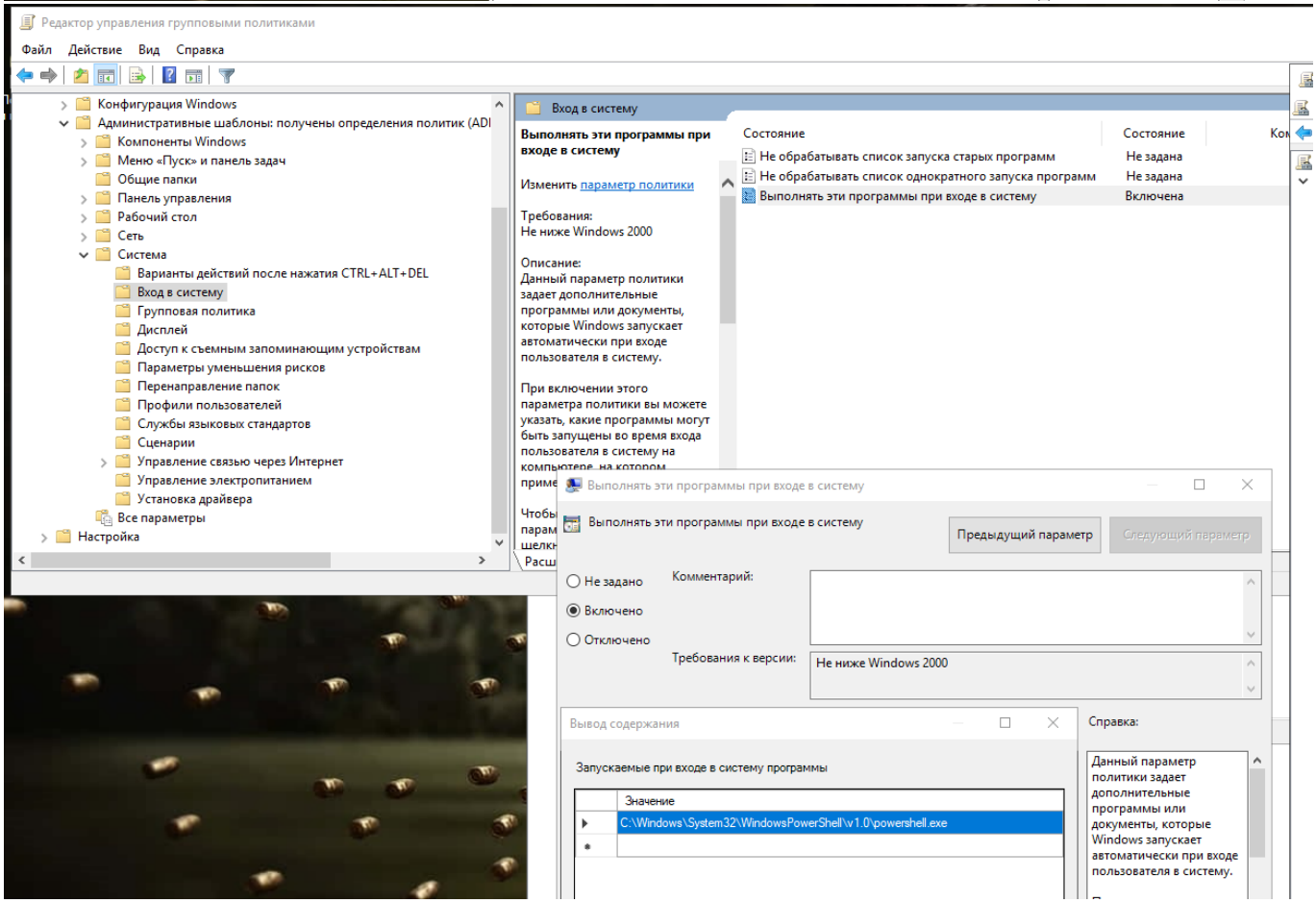
А также отключил возможность смены пароля и поставил запрет на редактирование реестра через созданную политику passwd reestr stop



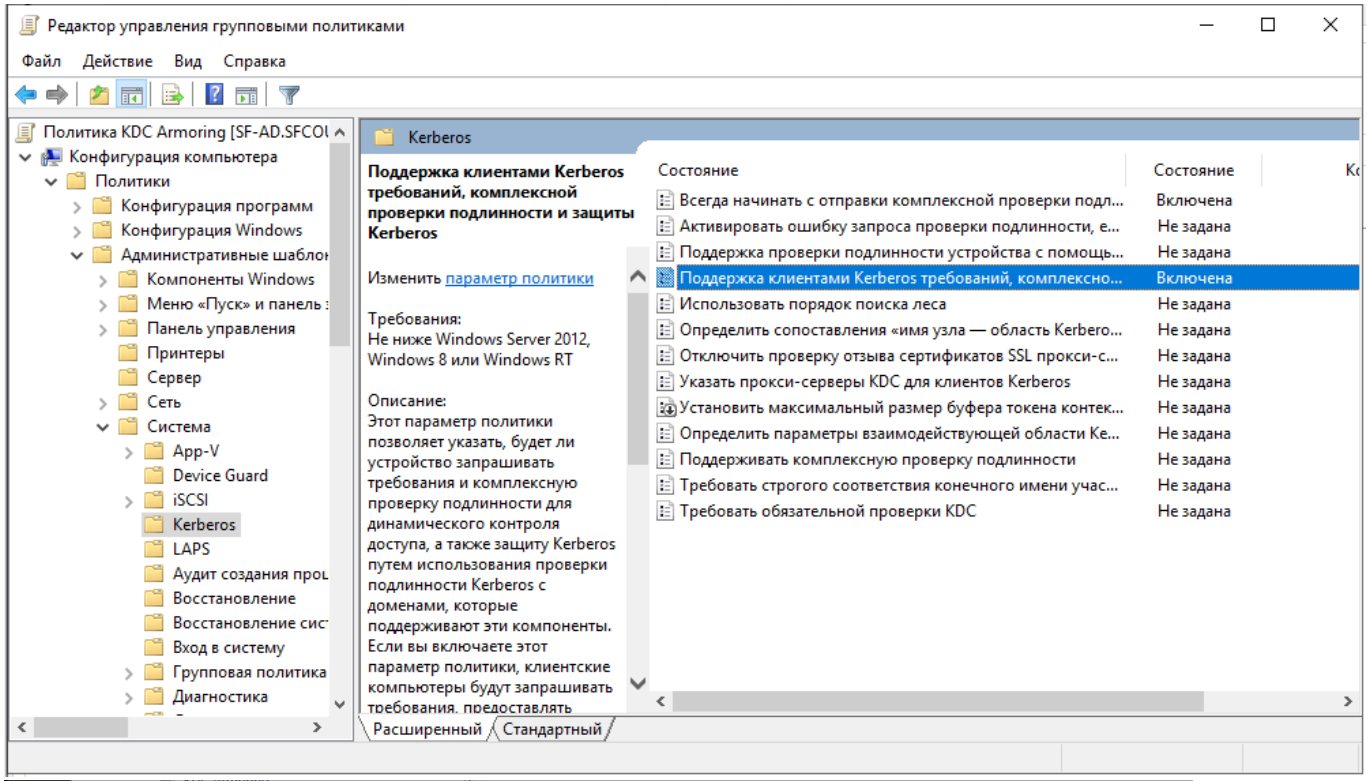


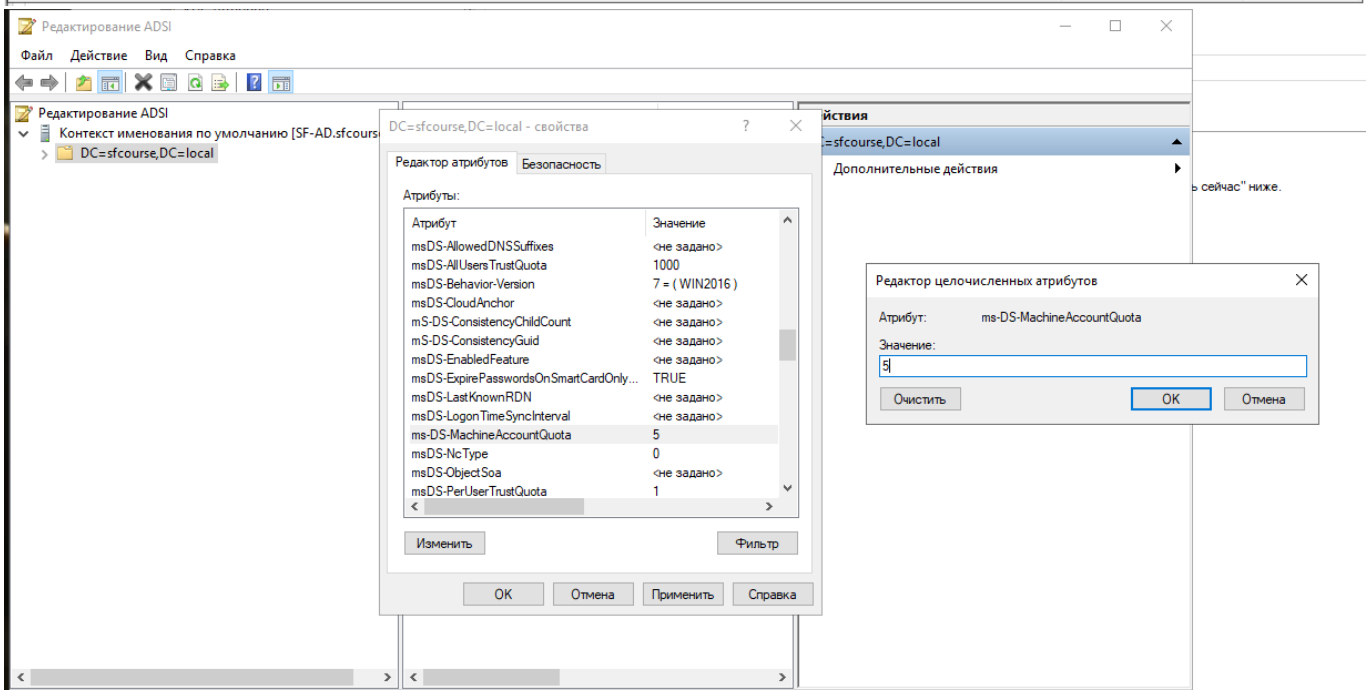
Для operators через созданную групповую политику Fon and start установил фон рабочего стола и открытие PS при входе



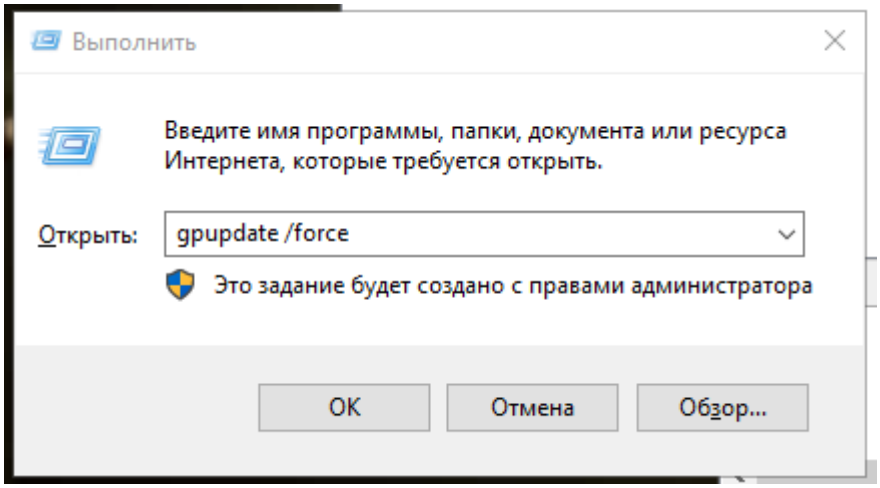


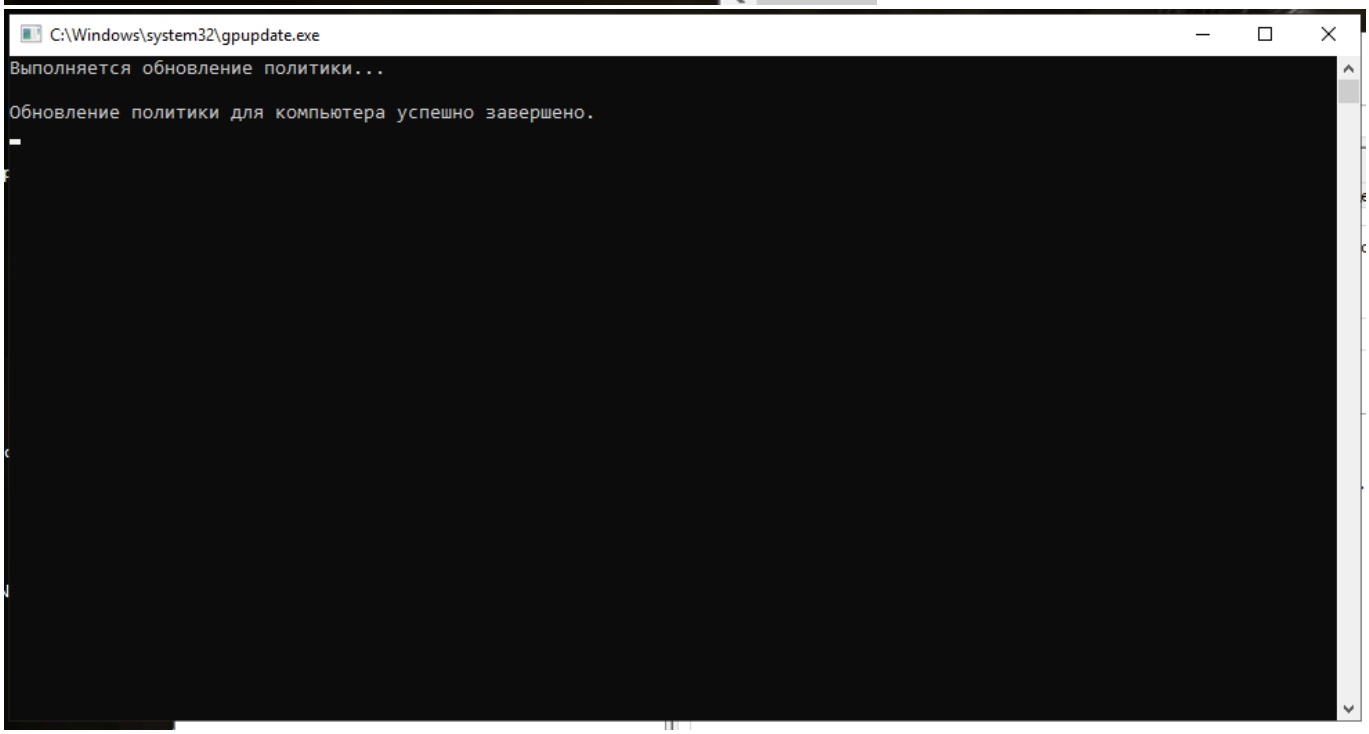
Включил KDC Armoring и поставил значение TheMachineAccountQuota на «5»





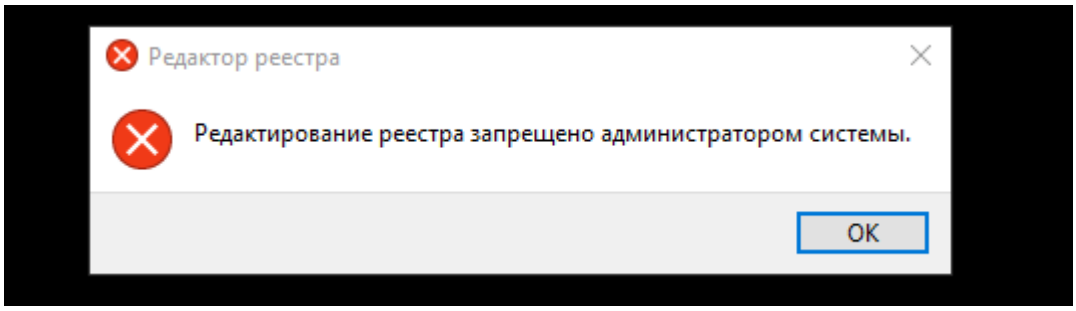
Применил политики



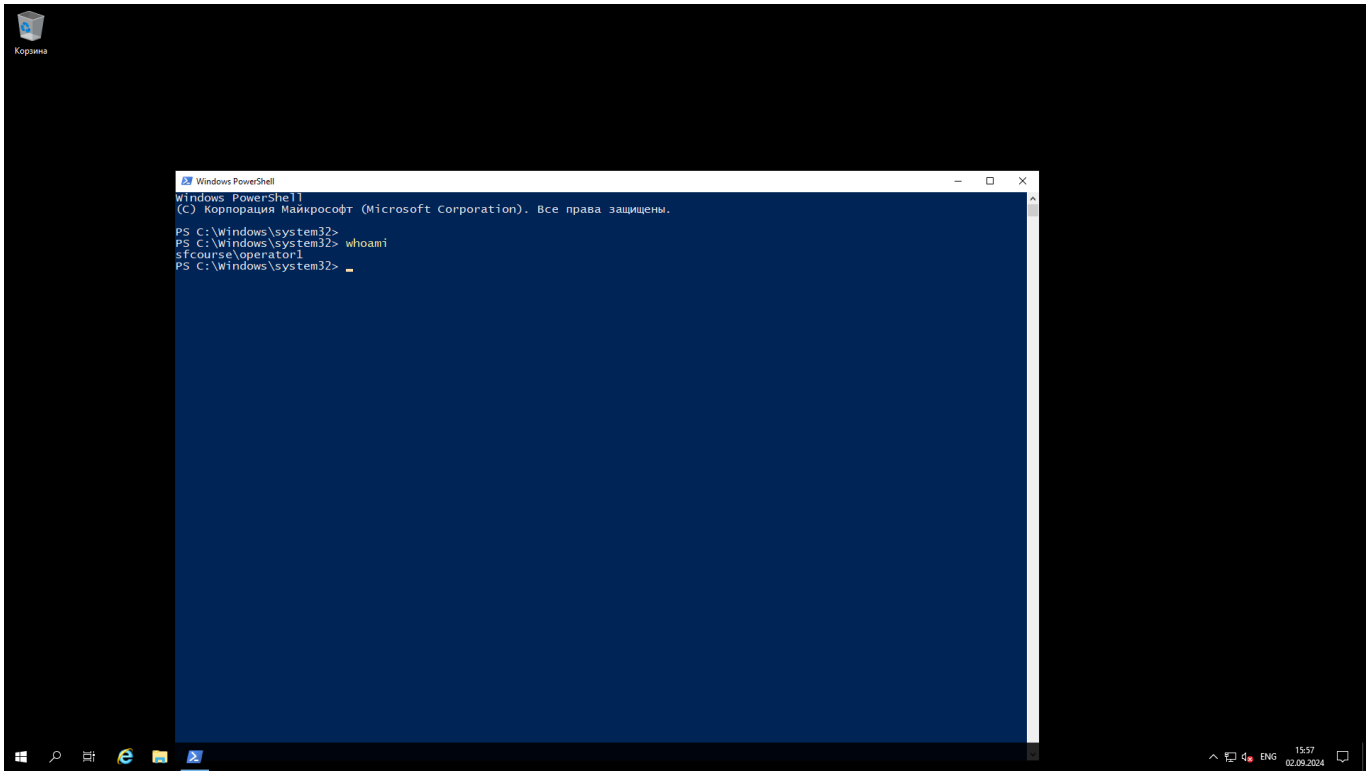


Добавил пользователей удаленного рабочего стола и зашёл на SF_CLIENT:

Под user1, с последующей попыткой редактирования реестра



И под operator1, где при входе запустился PS



**С обоями, честно говоря, так и не понял, почему не применилось ни у пользователя, ни у оператора. Хотя вроде в настройках выставлял.*

Созданные политики в текстовом виде:
PS 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 02.09.2024 в 16:23:15

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: 02.09.2024 в 16:20:25

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

Политика паролей

KDC Armoring

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

GPO: Политика паролей

Политика: MaximumPasswordAge

Параметры компьютера: 45

GPO: Политика паролей

Политика: MinimumPasswordAge

Параметры компьютера: 30

GPO: Политика паролей

Политика: MinimumPasswordLength

Параметры компьютера: 8

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

LOCAL SERVICE

NETWORK SERVICE

Администраторы

Прошедшие проверку

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 архива

Операторы сервера

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 архива

Операторы сервера

Операторы печати

GPO: Default Domain Controllers Policy

Политика: AuditPrivilege

Параметры компьютера: LOCAL SERVICE

NETWORK SERVICE

GPO: Default Domain Controllers Policy

Политика: InteractiveLogonRight

Параметры компьютера: Администраторы

Операторы архива

Операторы учета

Операторы сервера

Операторы печати

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

Администраторы

Прошедшие проверку

КОНТРОЛЛЕРЫ ДОМЕНА ПРЕДПРИЯТИЯ

Пред-Windows 2000 доступ

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 архива

Операторы сервера

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

GPO: Политика паролей

Политика: PasswordComplexity

Параметры компьютера: Включено

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\RequireSecuritySignature

Параметры компьютера: 1

GPO: Default Domain Controllers Policy

Политика: @wsecedit.dll,-59044

Параметр: MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature

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: Политика паролей

Идентификатор папки:
Software\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos\Parameters\KdcValidation

Значение: 2, 0, 0, 0

Состояние: Включено

GPO: KDC Armoring

Идентификатор папки:
Software\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos\Parameters\EnableCbacAndArmor

Значение: 1, 0, 0, 0

Состояние: Включено

GPO: KDC Armoring

Идентификатор папки:
Software\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos\Parameters\AlwaysSendCompoundId

Значение: 1, 0, 0, 0

Состояние: Включено

PS C:\Users\Администратор>

PS C:\Users\Администратор> gpresult /scope user /Z

Программа формирования отчета групповой политики операционной системы

Microsoft (R) Windows (R) версии 2.0

Создано 02.09.2024 в 16:25:53

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: 02.09.2024 в 14:50:11

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

PS C:\Users\Администратор>