Создание виртуальной сети вымышленного предприятия «COMPANY» на базе Windows Server 2016.

Часть 2. Создание подразделений и знакомство с групповой политикой.

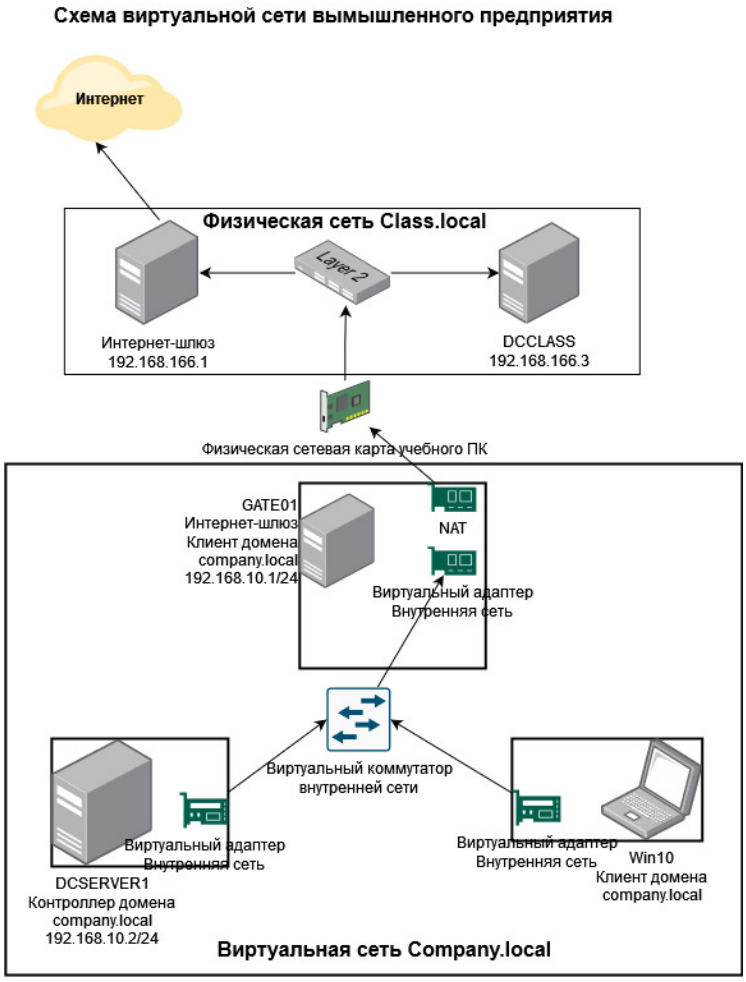
Задание.

На базе развернутой в предыдущей работе виртуальной сети (контроллера домена, интернет-шлюза и клиента) необходимо настроить групповую политику (ГП) для двух подразделений («Buhg» – бухгалтерия и «Managers» – менеджеры).

Схема сети представлена на рис.1.

При необходимости образы дисков VM скачать с «Рабочий стол\Материалы для студентов\VM\» (уточнить у преподавателя).

Рис.1



Этапы работы

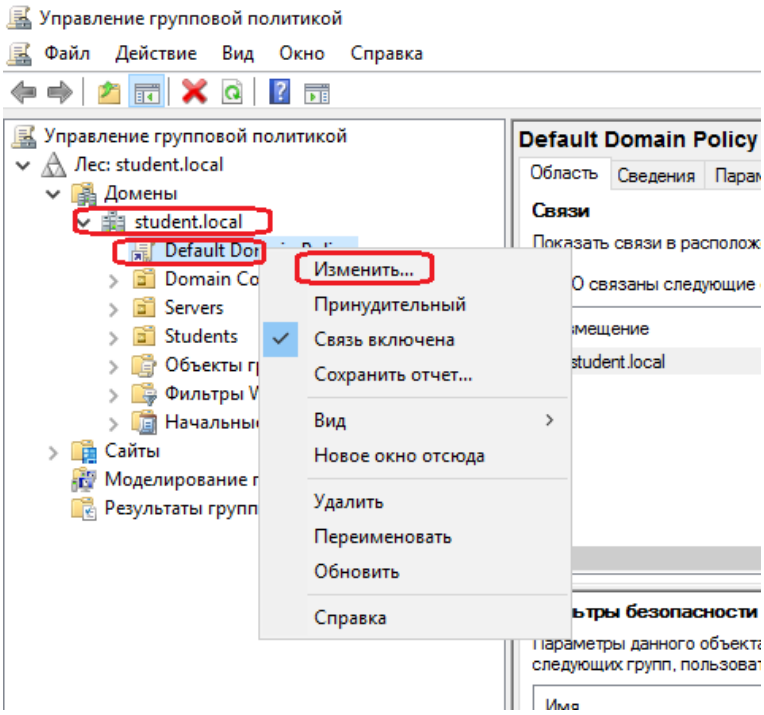
Этап 1. Создание подразделений и пользователей.

Задача 1. Делаем возможным создание простых паролей пользователям и отключаем службу обновлений Windows во всем домене Company.local.

Для того чтобы иметь возможность задавать пользователям простые пароли с длиной от 5 символов, необходимо предварительно отредактировать параметры групповой политики домена. А именно, «**политику домена по умолчанию**»/ «**Default Domain Policy**».

Открываем оснастку «**Управление групповой политикой**» в «Диспетчере серверов – Средства».

Затем, «**Default Domain Policy**» - **Изменить:**

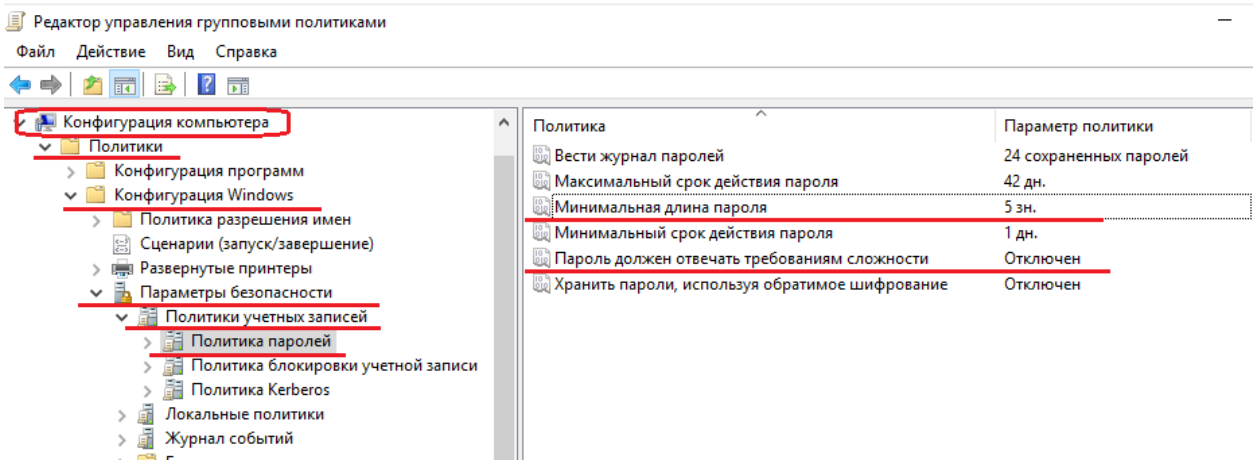


Примечание: в реальной рабочей сети упрощений политики паролей вносить крайне не желательно!!! В данном случае это делается для упрощения создания паролей пользователям.

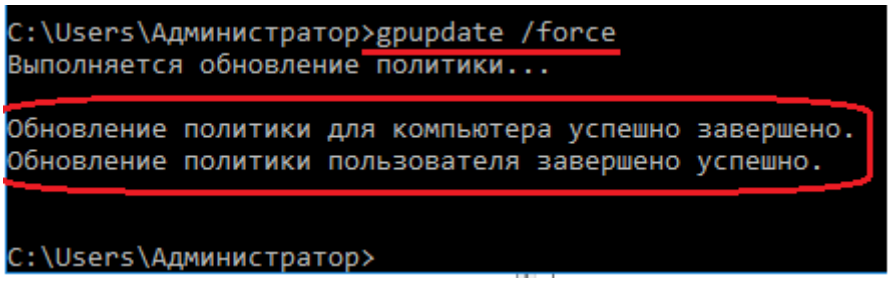
Далее, открываем: **Конфигурация компьютера – Политики – Конфигурация Windows – Параметры безопасности – Политики учетных записей – Политики паролей.**

В них меняем значения «**Минимальная длина пароля**» – **5**;

«**Пароль должен отвечать требованиям сложности**» - **отключен.**



После чего закрываем оснастку и открываем командную строку CMD и форсируем обновление новых политик на контроллере домена с помощью команды **gpupdate /force** :



Отключаем службу обновлений Windows во всем домене Company.local для ускорения работы серверов и клиентов.

В оснастке «Управление групповой политикой» открываем политику «**Default Domain Policy**»

Далее, открываем: «**Конфигурация компьютера – Политики – Конфигурация Windows – Параметры безопасности – Системные службы**». Затем находим службу «**Центр обновления Windows**» и меняем режим запуска службы на «**запрещен**».

После чего закрываем оснастку и открываем командную строку CMD и форсируем обновление новых политик на контроллере домена с помощью команды **gpupdate /force**.

Аналогичным образом форсируем обновление групповых политик на остальных серверах и клиентах.

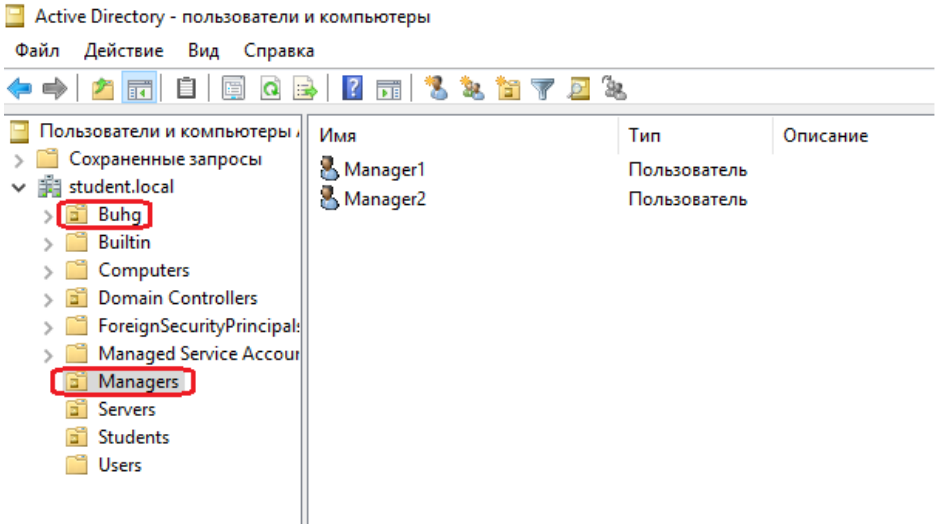
Для проверки применения политик перезагружаем клиент Win10. Открываем оснастку «Управление компьютером - Службы и приложения - Службы». Находим службу «Центр обновления Windows» и убеждаемся что данная служба отключена.

Примечание: Изменения в объекте групповой политики (ГП) «Default Domain Policy» влияют на весь домен и все сервера и рабочие станции в нем!!! Потому будьте внимательны и не меняйте что-либо если точно не знаете на что это повлияет!!!

Неверное изменение ГП может нарушить работу всего домена или отдельных подразделений!!!

Задача 2. Создание подразделений и пользователей, перемещение компьютеров между подразделениями.

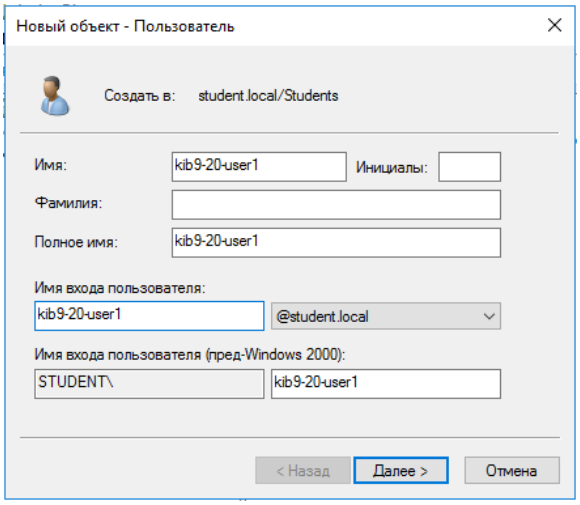
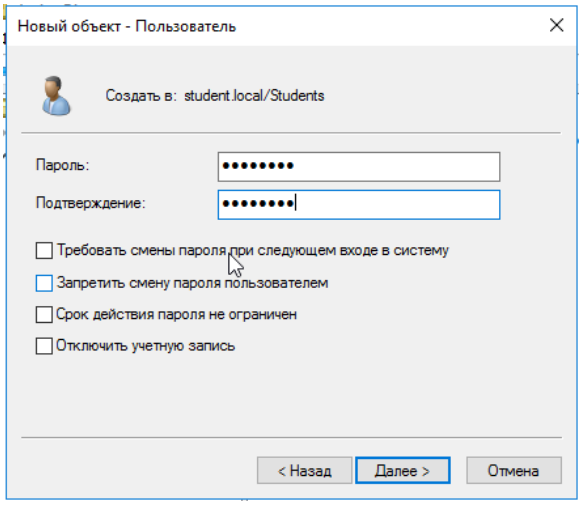
С помощью оснастки **«Active Directory – пользователи и компьютеры»** создаем подразделения **«Buhg» и «Managers»:**



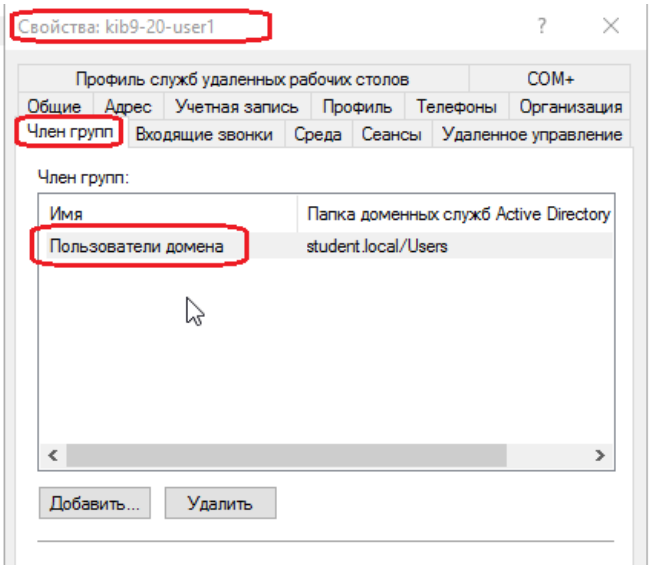
В соответствующих подразделениях (OU –organization unit) создаем пользователей:

Подразделение **Buhg**	
Пользователь	Пароль

buhg1	**buhg1**
buhg2	**buhg2**
Подразделение **Managers**	
manager1	**manager1**
manager2	**manager2**

Задаем имя нового пользователя:	Задаем пароль пользователя:
	

Откроем свойства любого из данных пользователей и удостоверимся, что он входим в группу Пользователи домена (не имеет прав администратора):

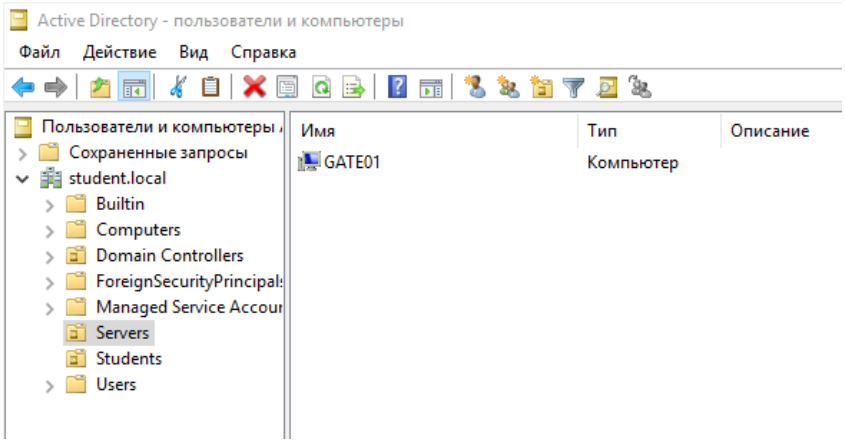


Примечание: по умолчанию, все вновь созданные пользователи домена входят в группу Пользователи домена.

Затем **переместите компьютер «Win10»** из подразделения «**Computers**» в недавно созданное подразделение «**Buhg**».

Примечание: по умолчанию, все подключенные к домену компьютеры по умолчанию попадают в подразделение «Computers».

Аналогичным образом создайте подразделение «**Servers**» и перенесите туда сервер **GATE01** из подразделения «**Computers»**.

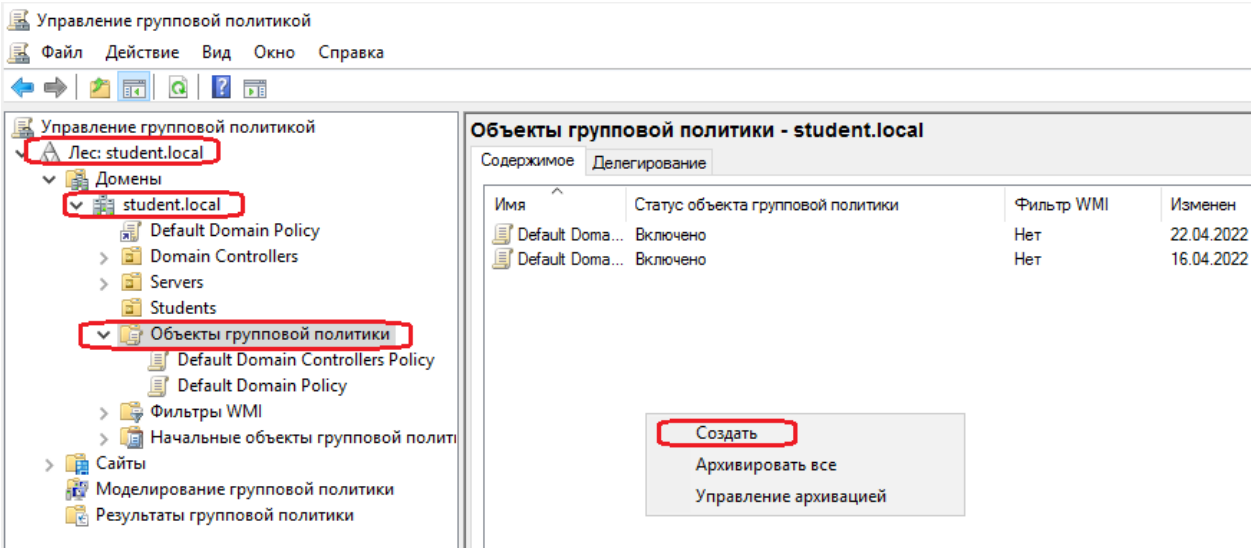


Этап 2. Создание объектов групповой политики и их применение для отдельного подразделения

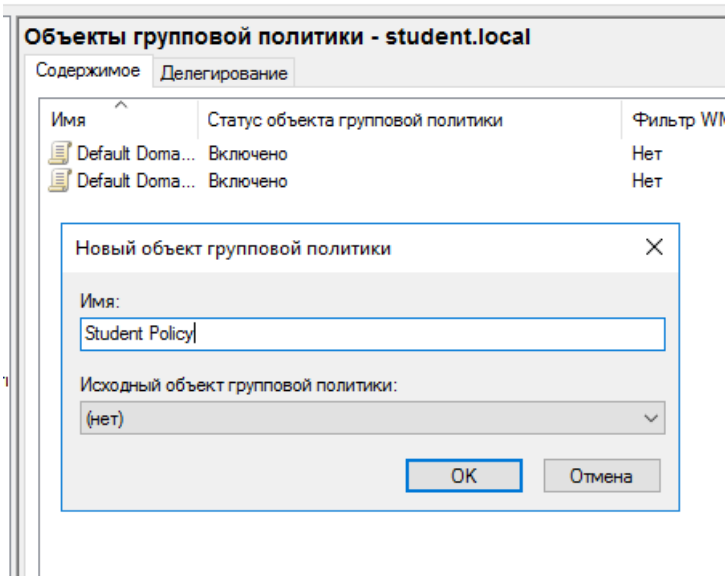
Задача 3. Внести изменения в режим запуска (настройки) служб на компьютерах входящих в подразделения «Buhgs» и «Managers», для включения возможности обнаруживать в «Сетевом окружении» проводника соседних компьютеров.

Данная политика будет применяться к компьютерам, а не пользователям входящим в данные подразделения (OU)

Откройте в диспетчере серверов оснастку «Управление групповой политикой»

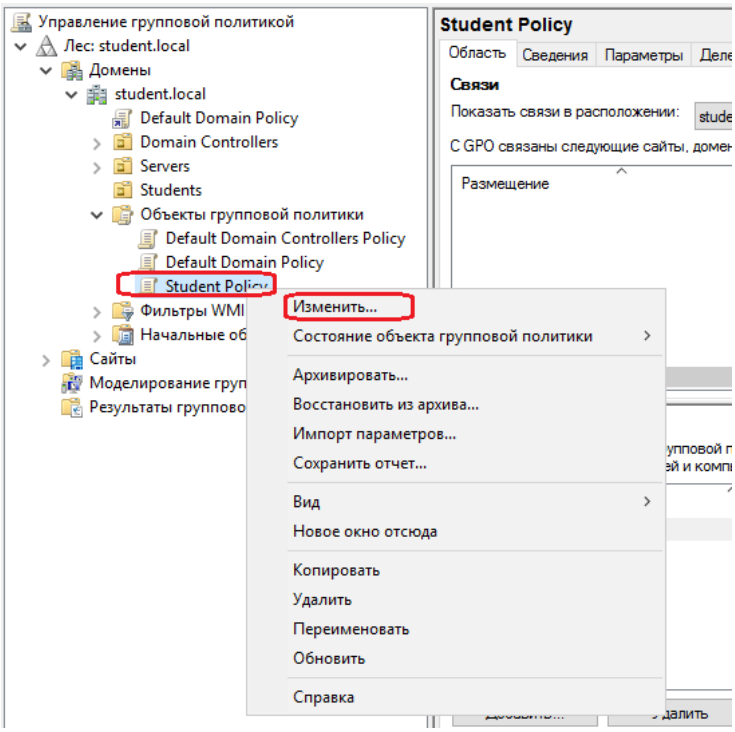


Создайте в «**Объекты групповой политики**» текущего домена объекты групповой политики «**Buhg Policy**» и «**Managers Policy**».

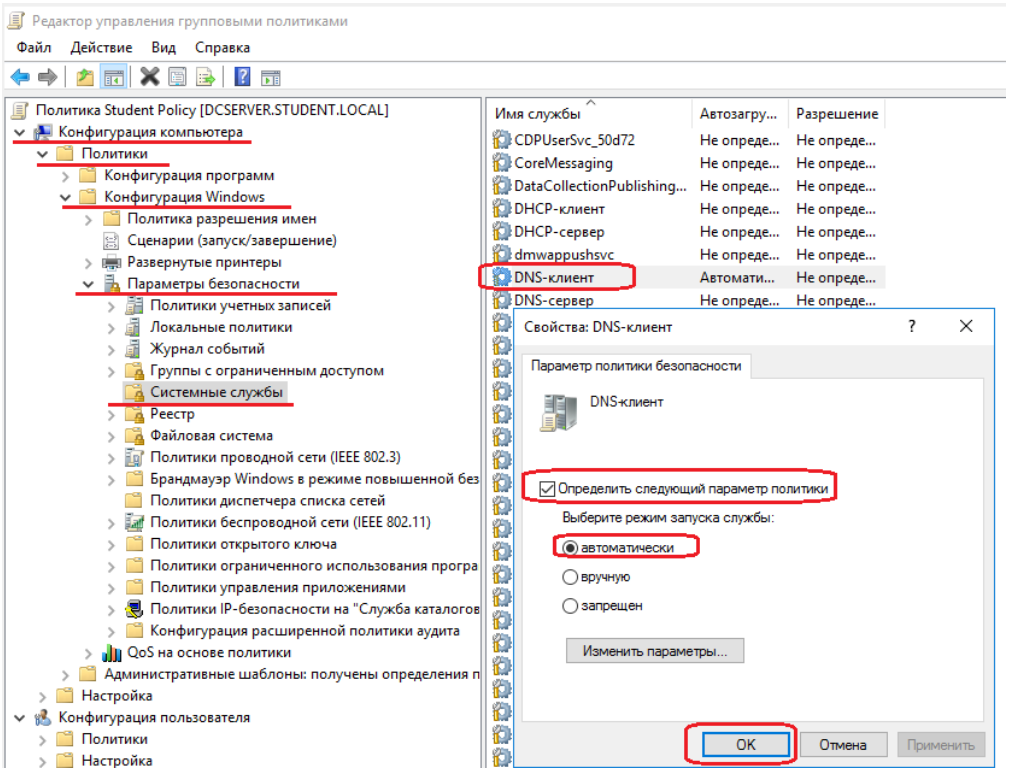


Приступим к редактированию объекта групповой политики.

Выберем «Изменить»:



Далее, открываем: **Конфигурация компьютера – Политики – Конфигурация Windows – Параметры безопасности –Системные службы**



Меняем режим запуска на «**автоматически» в следующих службах:**

1. **DNS-клиент (DNS Client);**
2. **Обнаружение SSDP (SSDP Discovery);**
3. **Публикация ресурсов обнаружения функции (Function Discovery Resource Publication);**
4. **Узел универсальных PNP-устройств (UPnP Device Host).**

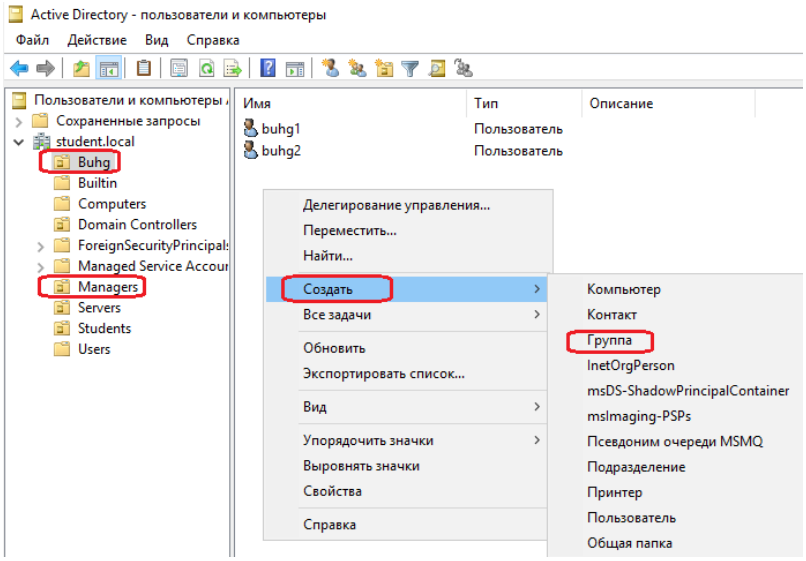
Редактируем данные параметры в обоих политиках («Buhg Policy» и «Managers Policy»).

Задача 4. Опубликовать сетевые папки «Общая папка бухгалтерии» и «Общая папка менеджеров», находящиеся на сервере DCSERVER1, на рабочих столах пользователей в виде ярлыков.

Выполним данную задачу в несколько этапов.

1. **В подразделении «Buhg» создадим группу безопасности «Buhg» в которую включим пользователей buhg1 и buhg2.**

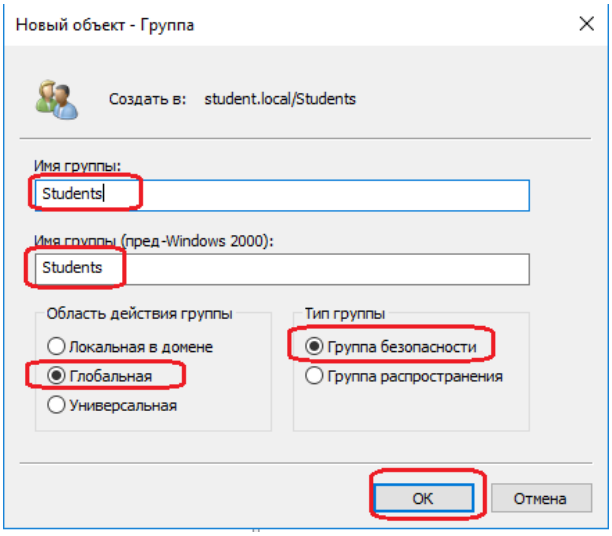
В подразделении «Managers» создадим группу безопасности «Managers» в которую включим пользователей Manager1 Manager2.



Имя группы – Buhg,

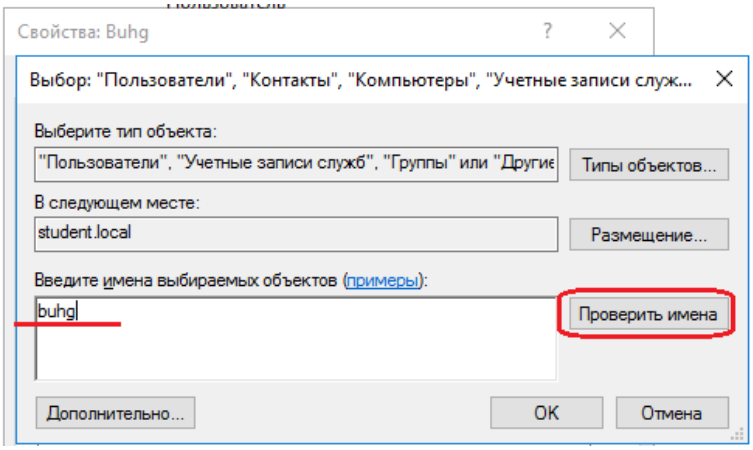
Область действия группы – Глобальная,

Тип группы – Группа безопасности:

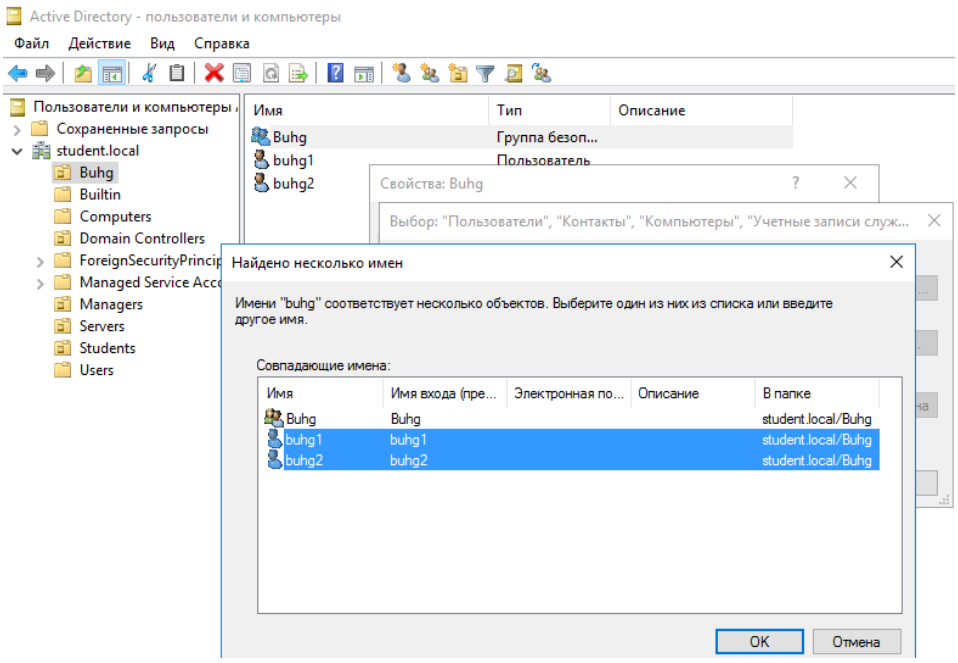


Открываем свойства группы и во вкладке «Члены группы» жмем «Добавить».

Вбиваем первые буквы имени пользователей buhg и жмем «Проверить имена».

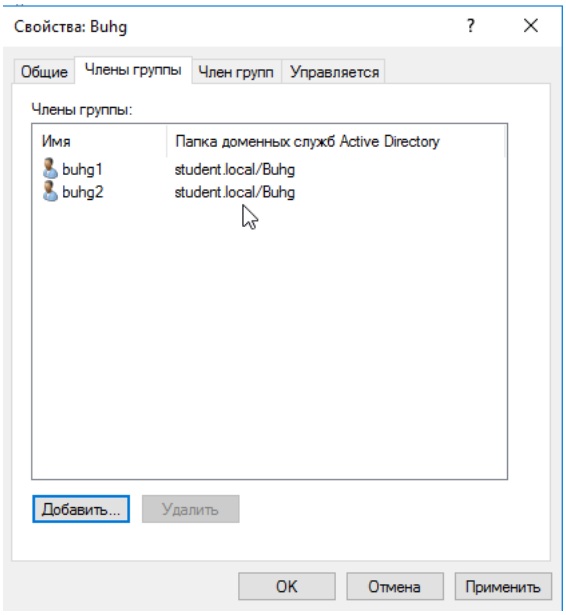


Выделяем, зажав Shift и щелкая левой кнопкой мыши нужных пользователей и жмем «ОК»:



В последнем окне проверяем правильность введенных пользователей и жмем «ОК»

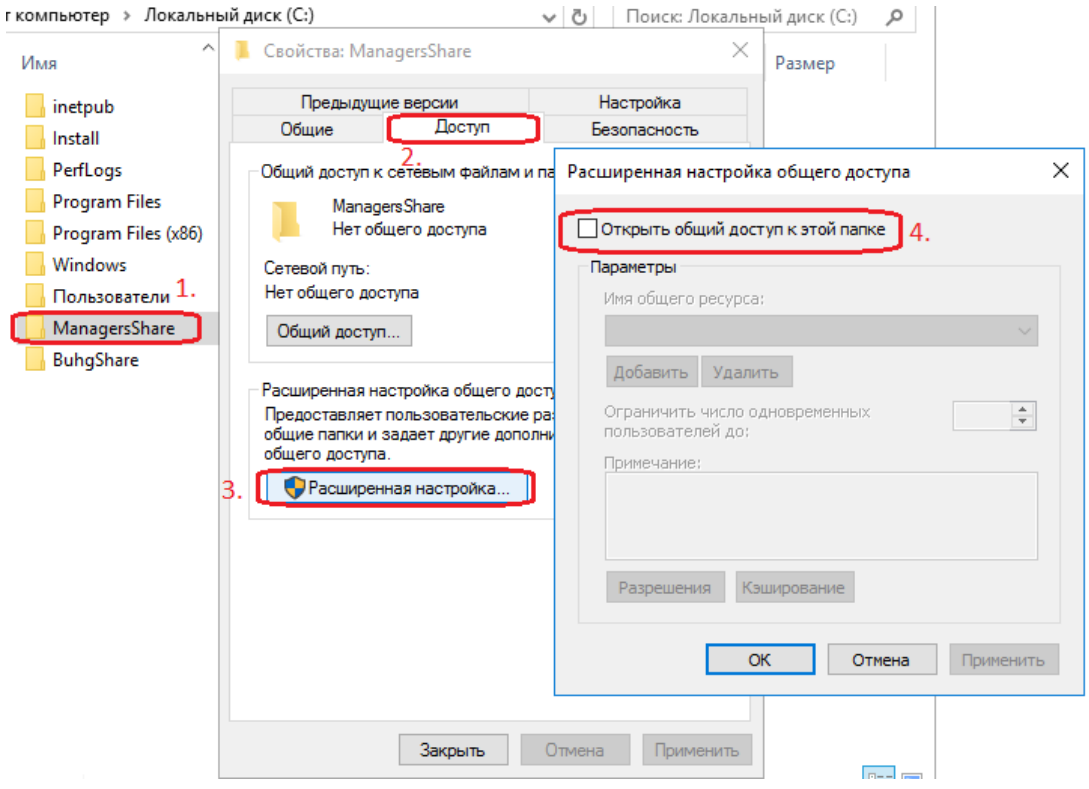
В результате во вкладке «Члены группы» в свойствах группы Buhg должны отображаться входящие в нее пользователи (buhg и buhg2).



Аналогичным образом добавляем в группу Managers пользователей manager1 и manager2.

2. **В корне диска C: создадим папки «ManagersShare» и «BuhgShare» и предоставим право на изменение для соответствующих групп безопасности Managers или Buhg.**

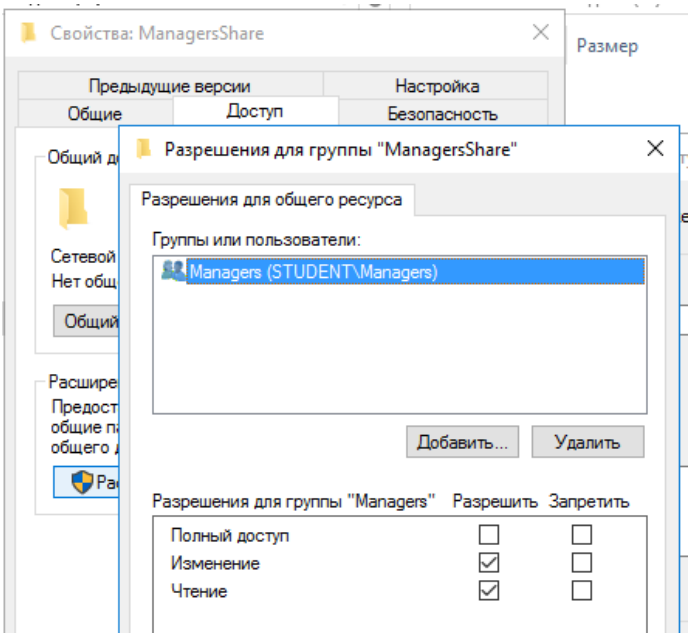
В свойствах созданных папок, открываем вкладку «**Доступ**», затем открываем «**Расширенная настройка**»



Далее, открываем общий доступ к этой папке.

Жмем «**Разрешения**» и настраиваем сетевой доступ необходимой группе безопасности (Managers или Buhg).

Удаляем группу «**Все**» из списка имеющих разрешение на сетевой доступ.



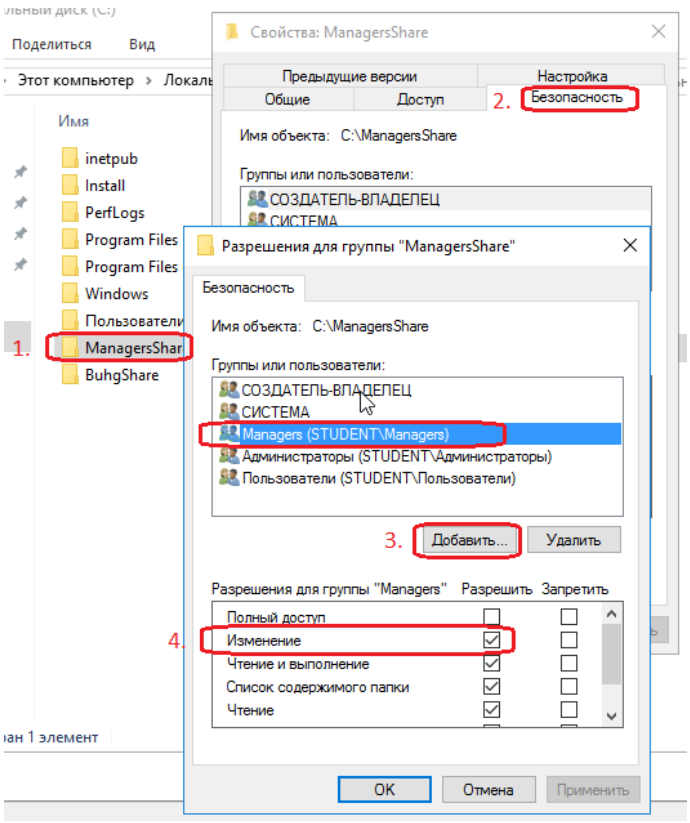
Далее, назначаем права **«Изменение»** для нужной группы.

Подтверждаем изменения и закрываем окно «Расширенная настройка доступа».

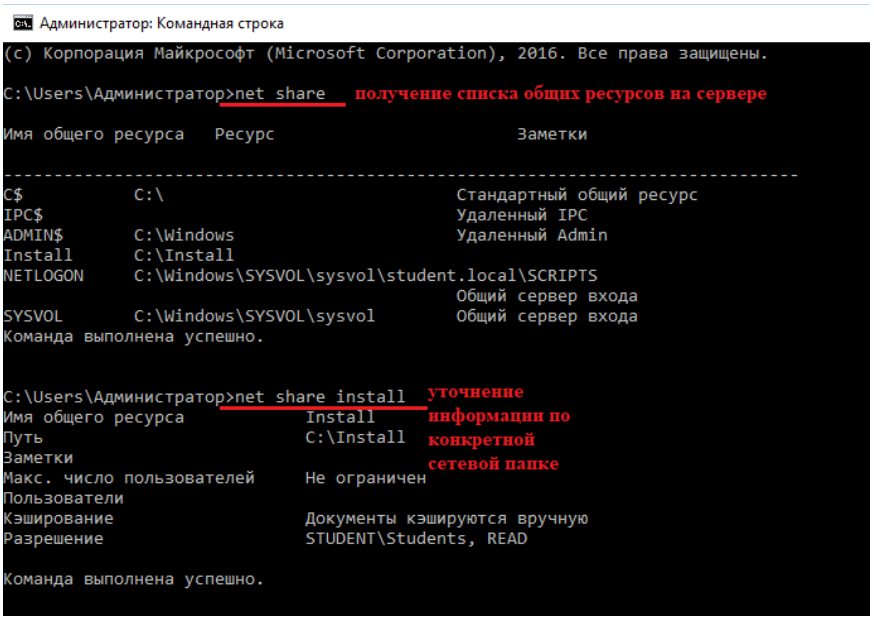
Затем, необходимо настроить права доступа во вкладке «**Безопасность**». В которой жмем «**Изменить**» для внесения изменений в настройки безопасности для данной папки.

Жмем «**Добавить**» и находим нужную группу безопасности (Buhg или Managers). Затем задаем права на «**Изменение».**

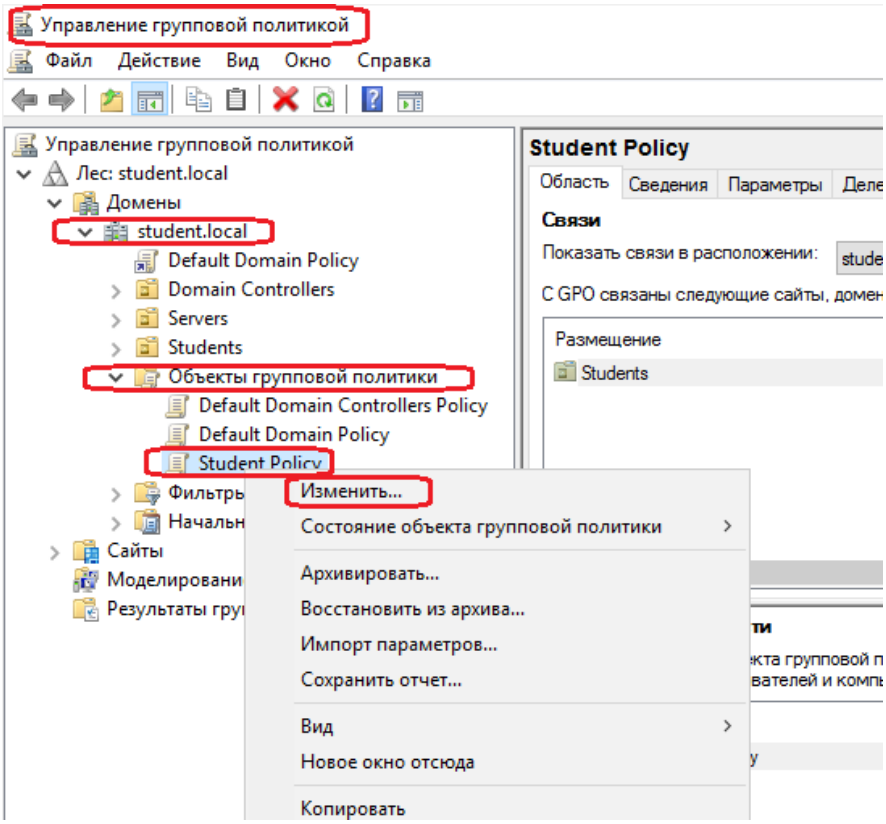
Подтверждаем изменения и закрываем окно «Разрешения для группы», затем подтверждаем изменения и закрываем окно свойств папки



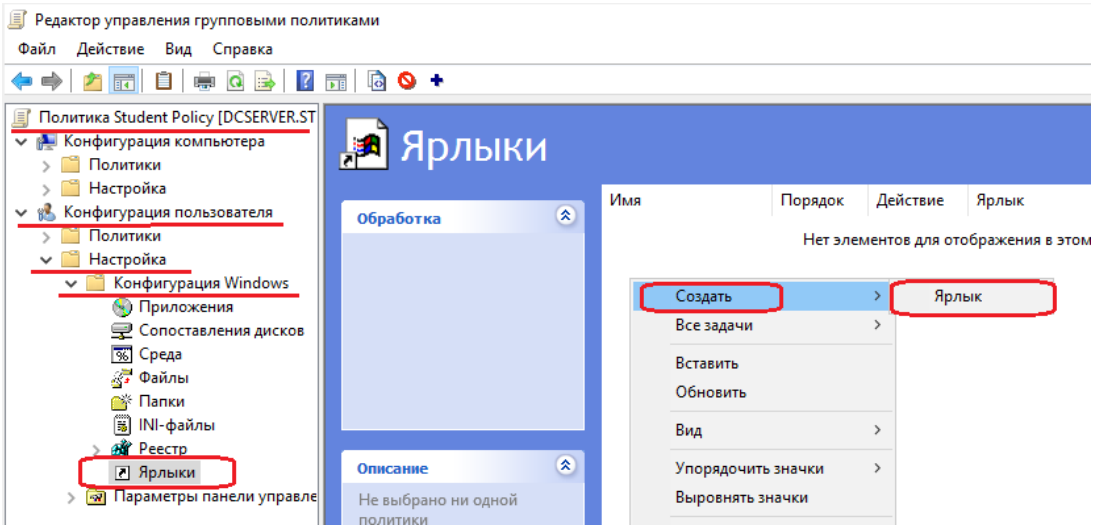
С помощью команд **net share** и **net share имя_ресурса**, запущенным в **командной строке с правами администратора** можно узнать список общих сетевых ресурсов и уточнить информацию по интересующей нас сетевой папке Install.



3. **Редактируем объекты групповой политики «Buhg Policy» и «Manager Policy».**



В данном объекте ГП открываем **«Конфигурация пользователя – Настройка – Конфигурация Windows – Ярлыки»**



В нем создаем ярлык со следующими параметрами:

Действие – Заменить (ярлык будет обновляться каждый раз при входе пользователя);

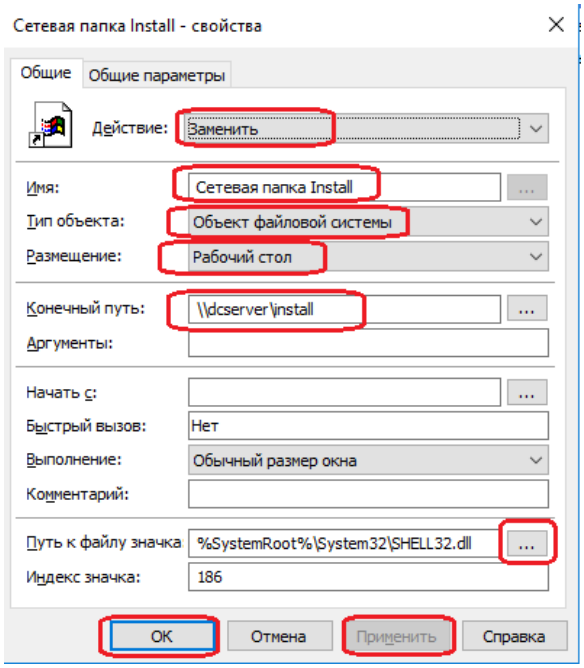
Имя – Общая папка бухгалтерии (Название ярлыка);

Тип объекта – Объект файловой системы (на что указывает ярлык);

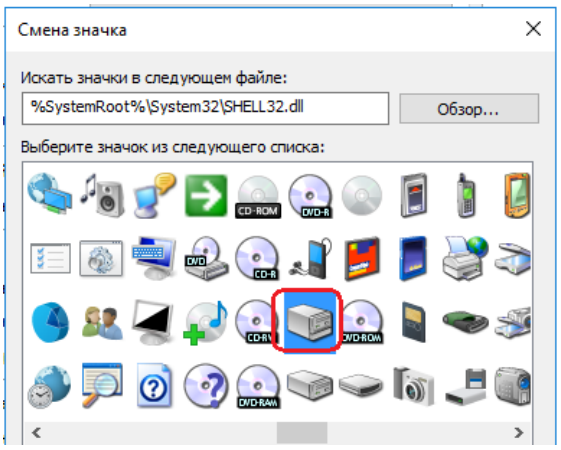
Размещение – Рабочий стол (место расположения ярлыка);

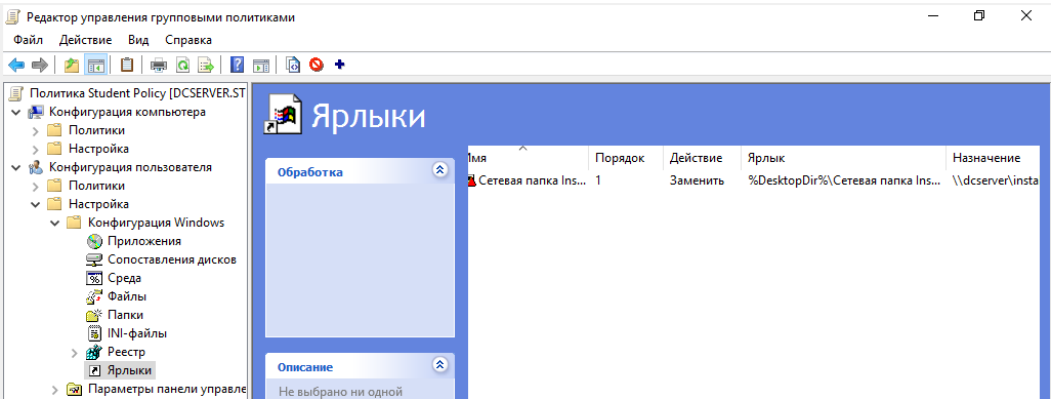
Конечный путь - \\dcserver1\buhgshare (сетевая папка на которую ссылается ярлык);

Путь к файлу значка (выбираем персональный значок для ярлыка).

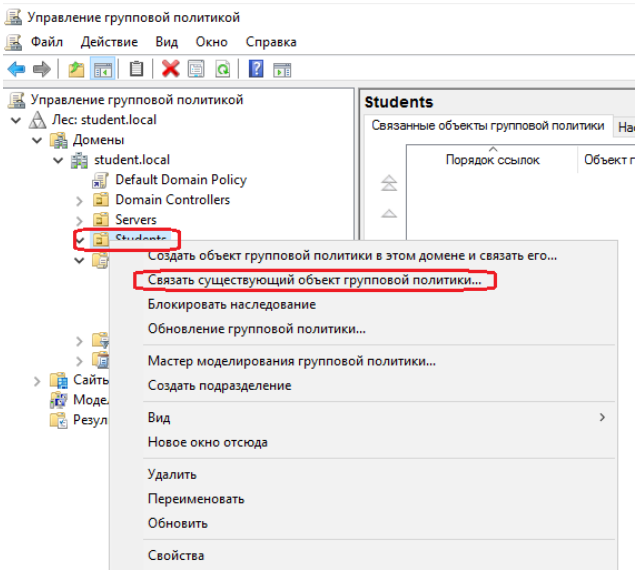


Выбор значка.

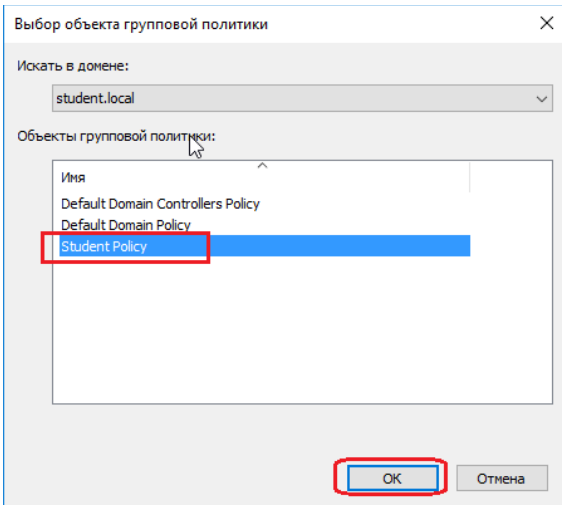




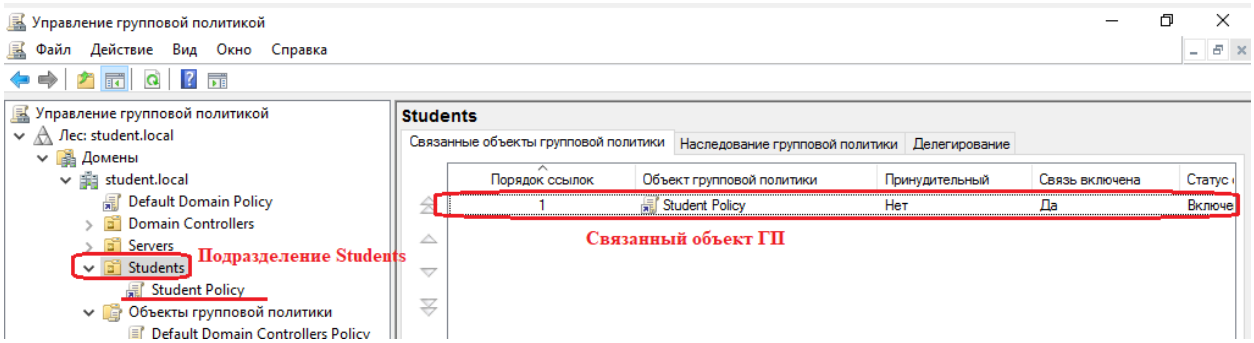
После чего необходимо **связать** вновь созданный **объект ГП «Buhg Policy» с подразделением «Buhg»**



Выбираем искомый объект ГП «Bung Policy».



В результате должна отобразиться связь объекта ГП с подразделением.



Примечание: если объект ГП был ранее уже связан с подразделением, повторно связывать не требуется.

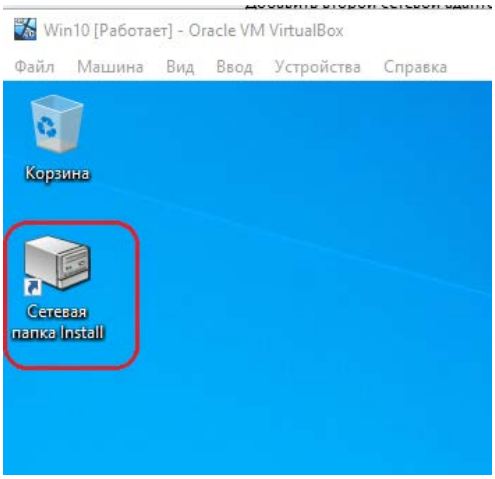
Аналогичным образом создаем и редактируем второй объект ГП **«Manager Policy».** В нем создаем создам ярлык **«Общая папка менеджеров»** с необходимыми параметрами.

После чего вводим в командной строке **gpupdate /force** для формирования изменений в ГП.

Задача 5. Проверка результатов редактирования ГП.

Входим на компьютере **Win10** под учетной записью **buhg1.**

1. Удостоверяемся в успешном создании ярлыка на Рабочем столе и соответственно в успешном применении изменений ГП.



Затем проверяем возможность создания/редактирования/удаления файлов/папок в данной папке. Для этого создадим произвольное количество папок или файлов. Скопируем и удалим.

2. Затем, с помощью оснастки **«Active Directory – пользователи и компьютеры» перенесем компьютер Win10** из подразделения **«Buhg»** в подразделение **«Managers».**

Форсируем применение новых правил ГП на клиенте Win10 с помощью команды **gpupdate /force** и перезагружаем его. Затем входим под учетной записью **Manager1.**

В результате на новом рабочем столе пользователя должен появиться новый ярлык **«Общая папка менеджеров»** созданная ранее для подразделения **«Managers».**

Проверяем возможность создания/редактирования/удаления файлов/папок в данной папке.

3. Проверяем видимость сетевого окружения в проводнике на Win10. Видны ли сервера DCSERVER1 и GATE01?