МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКИ  
ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра ПИ

Факультет КНТ

Лабораторная работа №8

Тема: «Планирование AD для своего предприятия. Управление объектами через консоль Active Directory».

Выполнил

ст. гр. ПИ-18Б

Моргунов А.Г.

Проверил:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Донецк – 2020

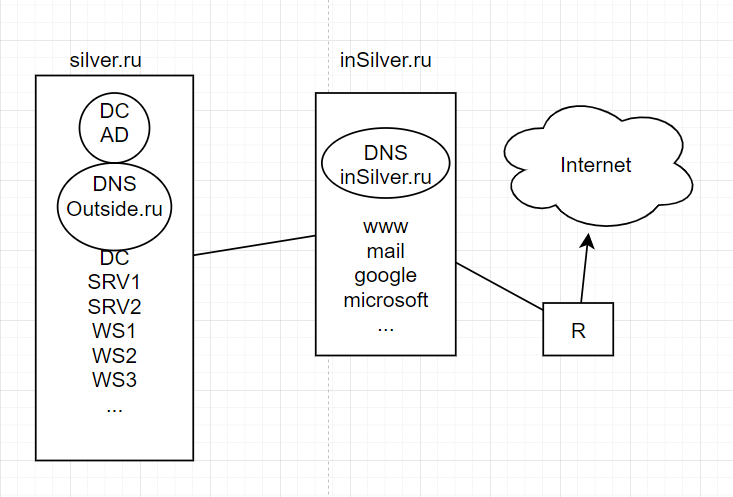
В ходе выполнения лабораторной работы необходимо ознакомиться со следующими вопросами и представить проект планирования AD для своего предприятия:

**- стратегия именования (механизм отличительных имен (Distinguished Name, DN), относительное отличительное имя (Relative Distinguished Name, RDN), основное имя объекта);**

Стратегия именования - основное имя объекта (UPN). Имя имеет следующий формат: <имя субъекта> @ <суффикс домена>

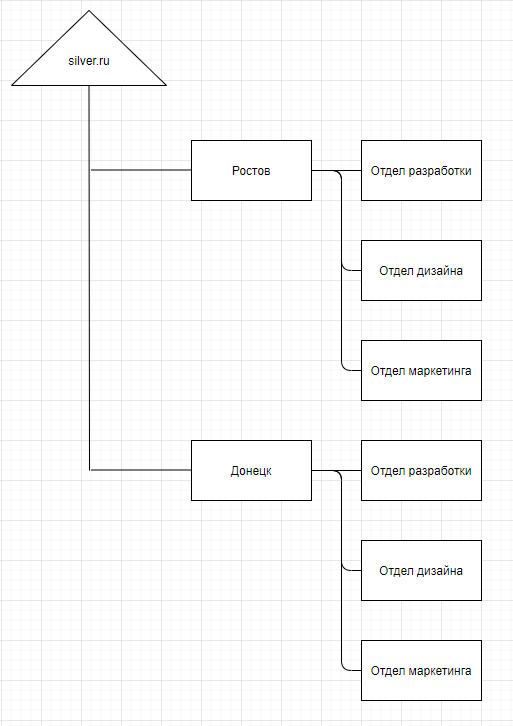
**- выбор схемы планирования пространства имен AD.**

Схема планирования пространства имен AD: Два различных домена DNS для внешних ресурсов и для AD.



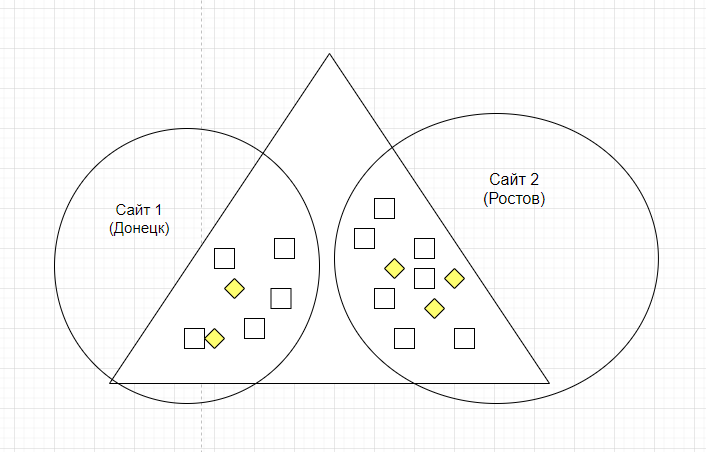
**- проектирование структуры OU, выбор модели классификации ОП в иерархии ОП;**

Модель структуры ОП – Смешанная (Сначала по местоположению, затем по структуре организации).



**- правила разбиения на сайты;**

Правило разбиения на сайты – в сайты помещаются контролеры доменов, в том числе глобальные каталоги, а также другое сетевое и пользовательское оборудование, которое соединены высокоскоростными каналами связи. В каждом городе находится свой сайт.



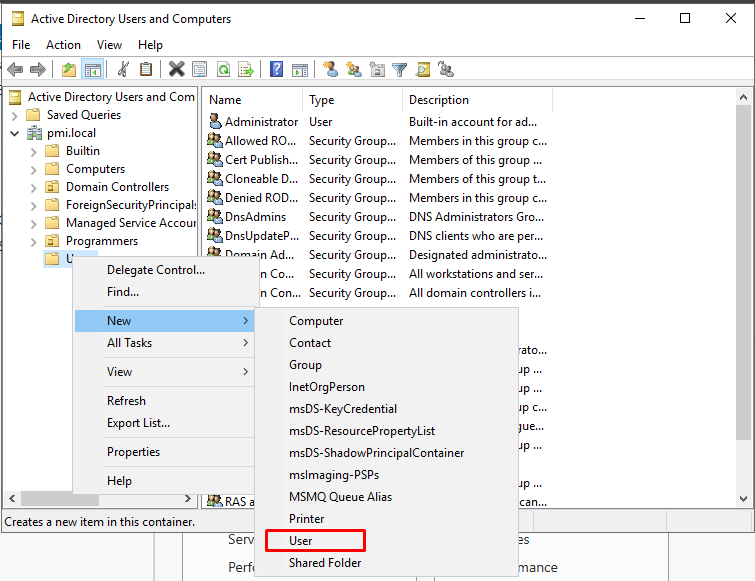
**- принципы размещения сетевых сервисов, глобальных каталогов (ГК) и других служб Active Directory;**

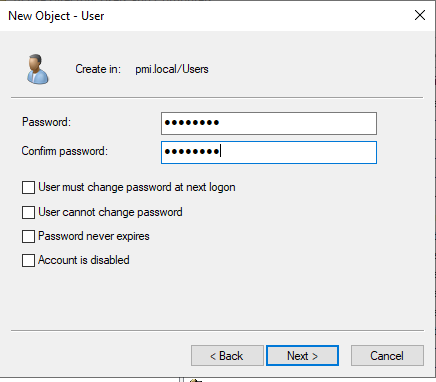
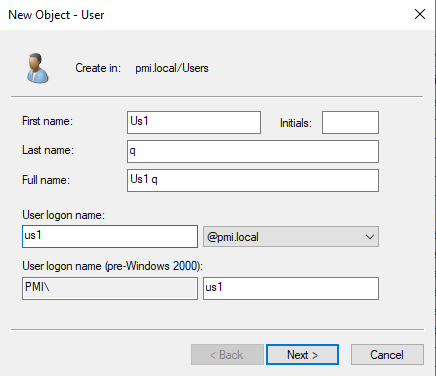
Принципы размещения сетевых сервисов, глобальных каталогов (ГК) и других служб Active Directory – в каждом сайте должен быть как минимум один глобальный каталог, и, желательно, контроллер домена. Сетевые сервисы располагаются по потребностям каждого отдела.

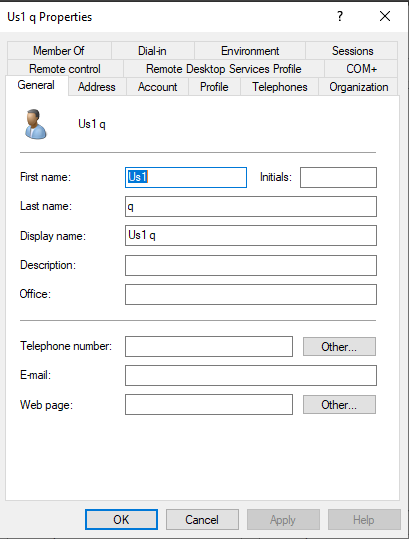
**- политика модификации схемы.**

Схема Active Directory представляет собой набор определений всех типов объектов каталога и связанных с ними атрибутов. Схема определяет способ хранения и конфигурирования в AD всех пользователей, компьютеров и других данных объек­тов, стандартизуя всю структуру Active Directory. Схема, защищенная с помощью списков разграничительного контроля доступа (Discretionary Access Control List – DACL), управляет возможными атрибутами каждого объекта из Active Directory. По существу, схема представляет собой базовое определение самого каталога и является основой функциональности среды домена. Делегировать управление схемой следует осторожно и лишь избранной группе администраторов, поскольку любые изменения схемы влияют на всю среду AD. Права на изменение схемы имеются только у главных админов городов.

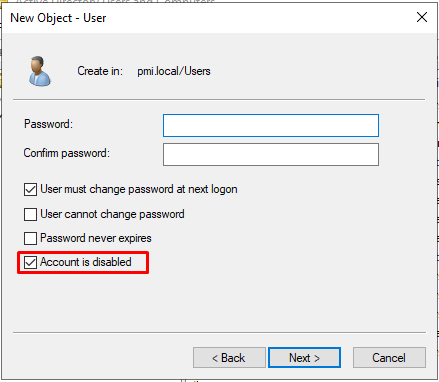
**- Создание и управление объектами пользователей в консоли Active Directory;**

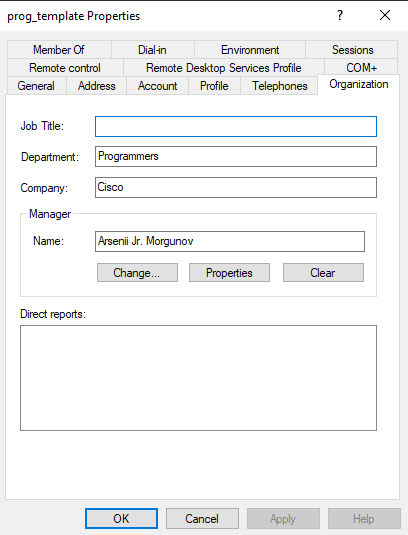
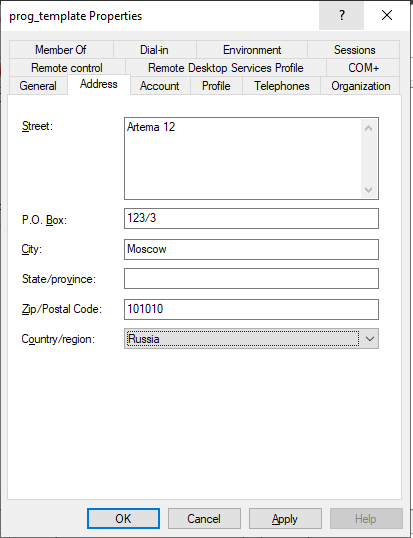


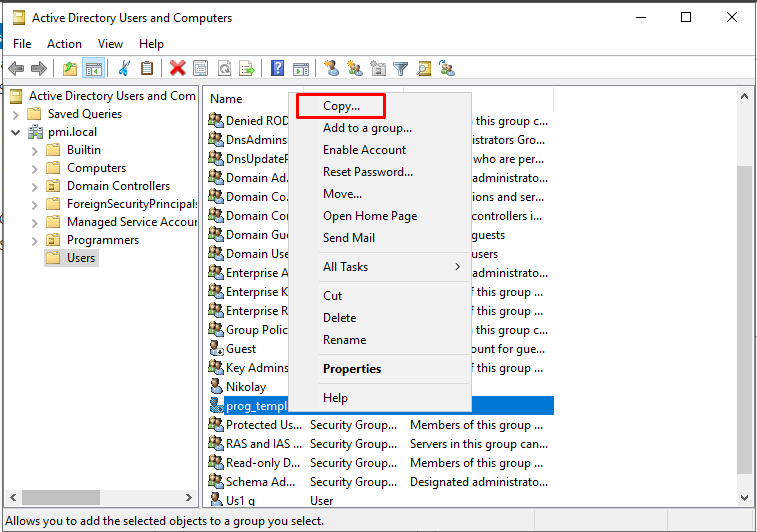


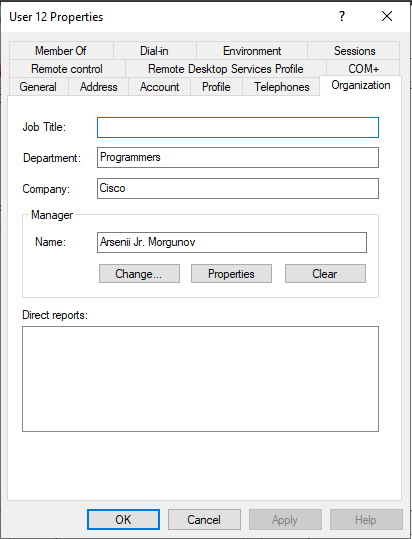
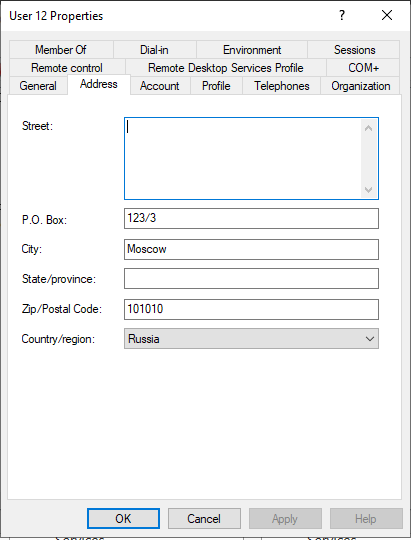


**- Создание и использование шаблонов объектов пользователей**

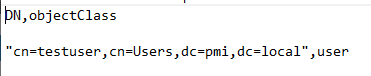


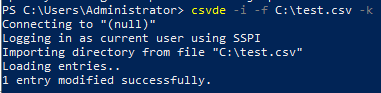






**- Импорт объектов пользователей при помощи CSVDE**





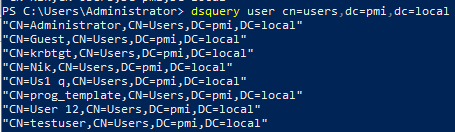
**- Использование DSADD, DSGET, DSMOD, DSMOVE, DSRM, DSQUERY для управления объектами пользователей.**













**- Управление профилями пользователей (локальные, преднастроенные, обязательные профили). Какими профилями можно в рамках лабораторной работы управлять?**

Управлять можно всеми типами пользователей. Различие состоит в том, что локальный профиль сохраняет изменения только на текущей машине. Преднастроенный пользователь сохраняет изменения на сервере, т.е. изменения будут применятся и на другие машины, на которых будет авторизоваться этот пользователь. Обязательные не сохраняют изменения во время сеанса, т.е. каждый новый сеанс будет начинаться с предопределенными настройками.

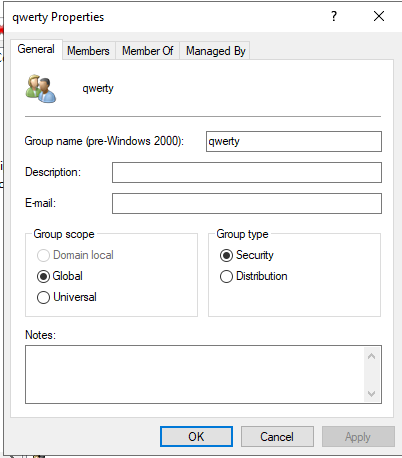
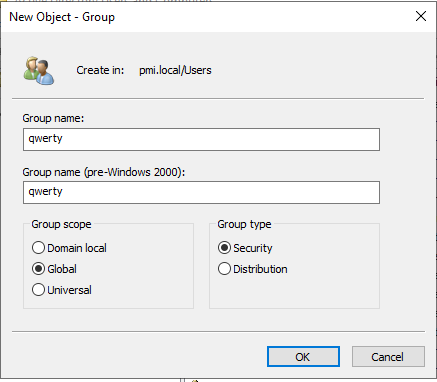
**- Работа с группами ( группа безопасности - 1)локальная доменная, 2) глобальная, 3) универсальная). Какие группы целесообразно назначать и когда?**

* **Локальная в домене** — используется для управления разрешениями доступа к ресурсам (файлам, папкам и другим типам ресурсам) только того домена, где она была создана. Локальную группу нельзя использовать в других доменах (однако в локальную группу могут входить пользователи другого домена). Локальная группа может входить в другую локальную группу, но не может входить в глобальную.
* **Глобальная группа** – данная группа может использоваться для предоставления доступа к ресурсам другого домена. В эту группу можно добавить только учетные записи из того же домена, в котором создана группа. Глобальная группа может входить в другие глобальные и локальные группы.
* **Универсальная группа** — рекомендуется использовать в лесах из множества доменов. С помощью нее можно определять роли и управлять ресурсами, которые распределены на нескольких доменах. В том случае, если в вашей сети имеется много филиалов, связанных медленными WAN каналами, желательно использовать универсальные группы только для редко изменяющихся групп. Т.к. изменение универсальной группы вызывает необходимость репликации глобального каталога во всем предприятии.

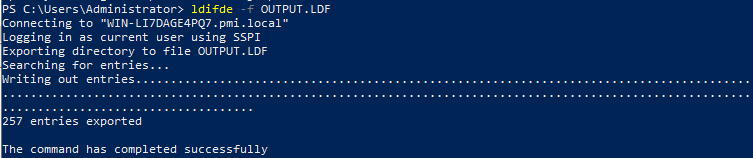
**- Изучить, какие специальные группы есть и их представление – обосновать, какие группы для чего используются.**

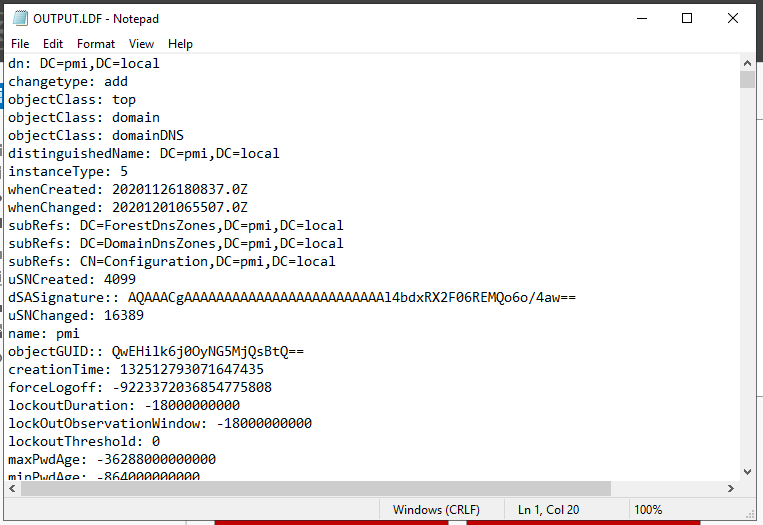
* **Группа безопасности** – этот тип группы используется для предоставления доступа к ресурсам. Например, вы хотите предоставить определенной группе доступ к файлам в сетевой папке. Для этого нужно создать группу безопасности.
* **Группа распространения** – данный тип групп используется для создания групп почтовых рассылок (как правило используется при установке Microsoft Exchange Server). Письмо, отправленное на такую группу, дойдет всем пользователям группы. Это тип группы нельзя использовать для предоставления доступа к ресурсам домена.

**- Управление учетными записями групп из консоли Active Directory**



**- Использование Ldifde.exe.**





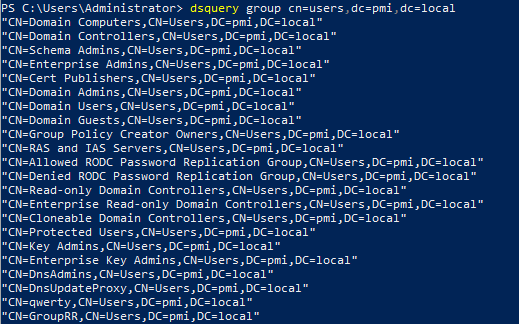
**- Использование DSADD, DSGET, DSMOD, DSMOVE, DSRM, DSQUERY для управления объектами групп.**





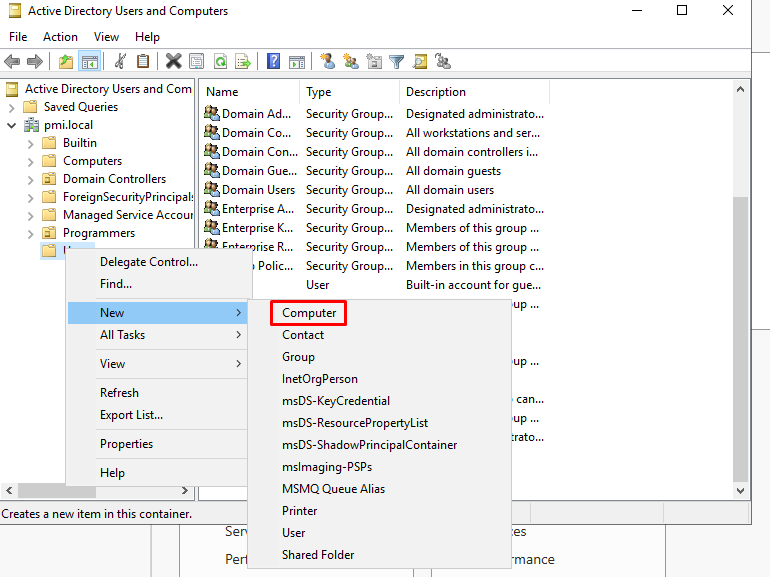


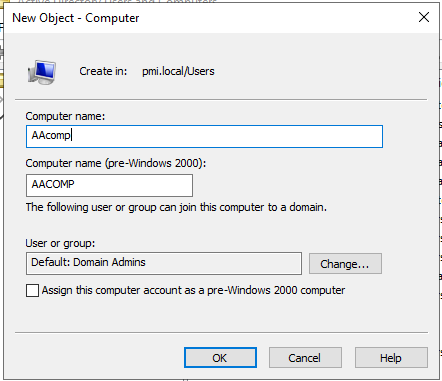






**- Создание учетных записей компьютеров из консоли Active Directory**





**- Использование DSADD, DSGET, DSMOD, DSMOVE, DSRM, DSQUERY для управления объектами компьютеров.**













**- Присоединение компьютера к домену**

