**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
ВЫСШЕГО ОБРАЗОВАНИЯ  
«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ  
ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Г.ШУХОВА»  
(БГТУ им. В.Г.Шухова)**

**Лабораторная работа №4**

дисциплина «Администрирование распределенных вычислительных систем»

тема: «Группы. Настройка политик и событий»

Выполнил: ст. группы ВТ-42  
Воскобойников И. С.  
Проверил: Федотов Е.А.

**Белгород 2021**

**Лабораторная работа № 4**

**Группы. Настройка политик и событий**

**Цель работы:** получить навыки создания групп и работы с ними при помощи сценариев и команды LDIFDE, а также настройки политик и событий.

**Краткие сведения**

Группы Active Directory — это гибкие структуры, которые могут включать объекты практически любых типов и используются для самых разных целей, в том числе для управления доступом пользователей к ресурсам и определения фильтров в случае применения групповых политик.

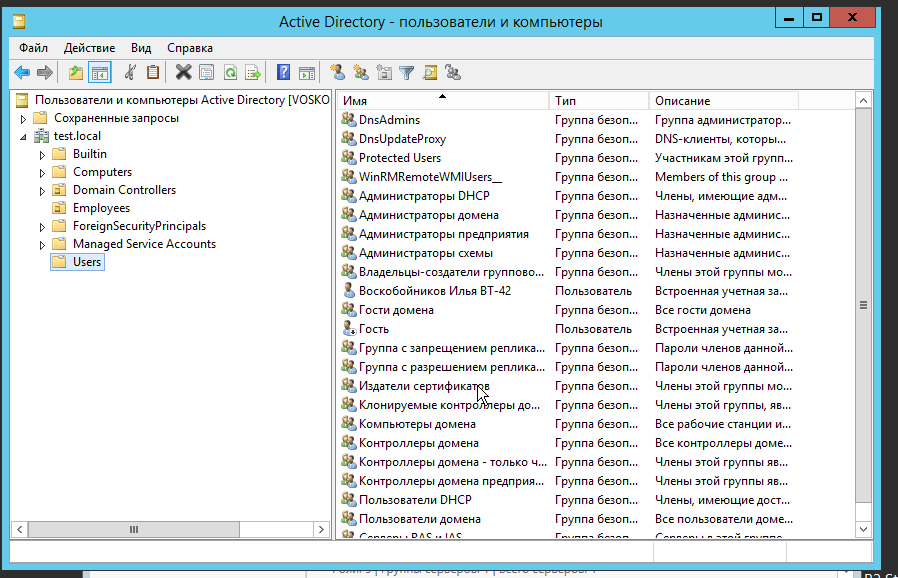
Каждая группа имеет определенную область действия и относится к одному из двух типов: безопасности или распространения. Группы безопасности используются для ограничения доступа к ресурсам, а группы распространения — просто как механизм группировки объектов. Область действия группы может быть глобальной, универсальной или локальной доменной. Она определяет, в какой части леса располагаются включаемые в группу объекты и в какой части леса группа используется в списках контроля доступа. Члены универсальных и локальных доменных групп могут относиться к любым доменам леса, но при этом первым разрешения обычно

предоставляются в любом домене леса, а вторым — только в локальном. Глобальные группы включают пользователей из того же домена, к которому относится группа, но зато им могут быть предоставлены разрешения в любом домене леса.

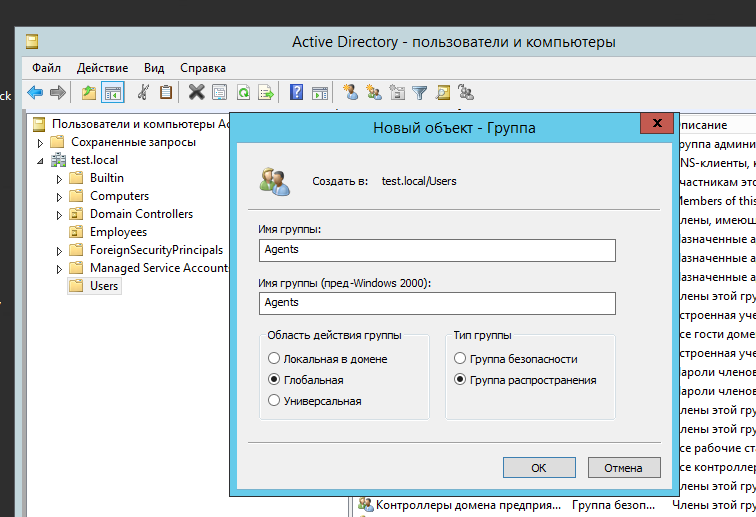
**Выполнение работы:**

1. **Создание и изменение группы**

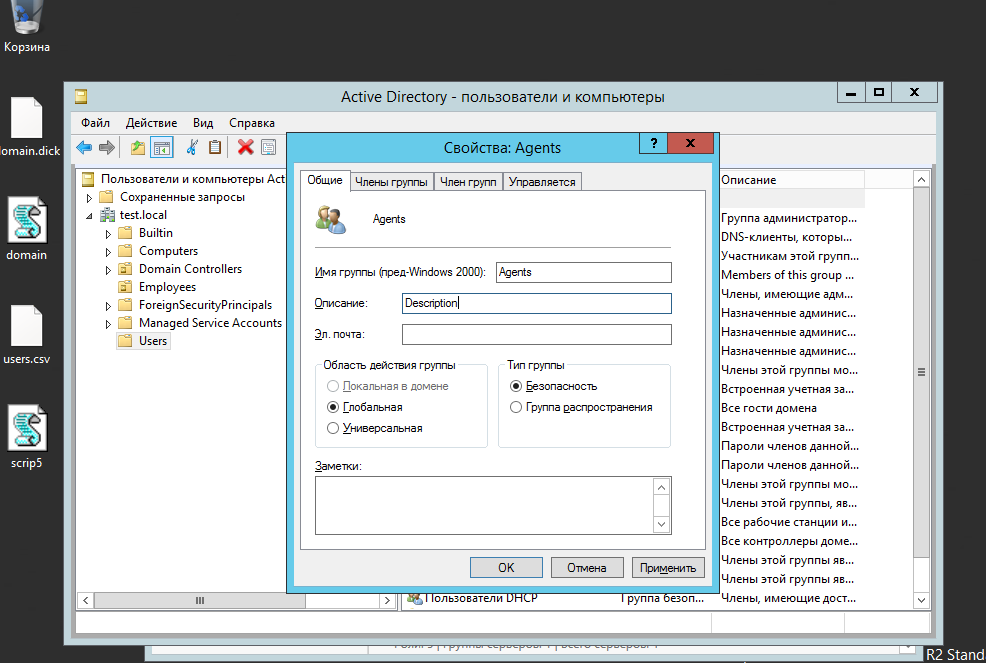
Открыл консоль Active Directory – пользователи и компьютеры.

****

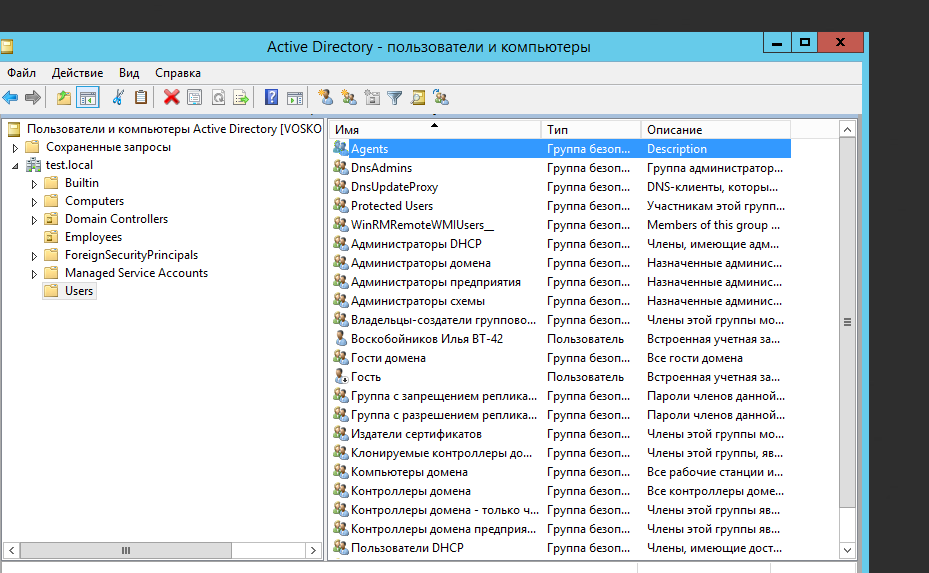
В контейнере Users создал глобальную группу распространения Agents



Просмотрел свойства, попробовал изменить их.



Свойства действительно изменились, т.к. сервер работает в качестве контроллера домена и не имеет ограничений на изменение.



1. **Написание сценариев**

Описал сценарии, которые выполняют:

1. Создание трех локальных групп в ОП Groups: Group1, Group2 и Group3.

New-ADGroup "Group1" -GroupScope 0 -PassThru -Verbose

New-ADGroup "Group2" -GroupScope 0 -PassThru -Verbose

New-ADGroup "Group3" -GroupScope 0 -PassThru -Verbose

1. Изменение области действия созданных групп на глобальную (сначала на универсальную, а затем на глобальную).

Set-ADGroup -Identity "Group1" -GroupScope 1 -Verbose

Set-ADGroup -Identity "Group2" -GroupScope 1 -Verbose

Set-ADGroup -Identity "Group3" -GroupScope 1 -Verbose

Set-ADGroup -Identity "Group1" -GroupScope 2 -Verbose

Set-ADGroup -Identity "Group2" -GroupScope 2 -Verbose

Set-ADGroup -Identity "Group3" -GroupScope 2 -Verbose

1. Создание трех учетных записей пользователей: User1, User2 и User3.

New-ADUser "User1" -Verbose

New-ADUser "User2" -Verbose

New-ADUser "User3" -Verbose

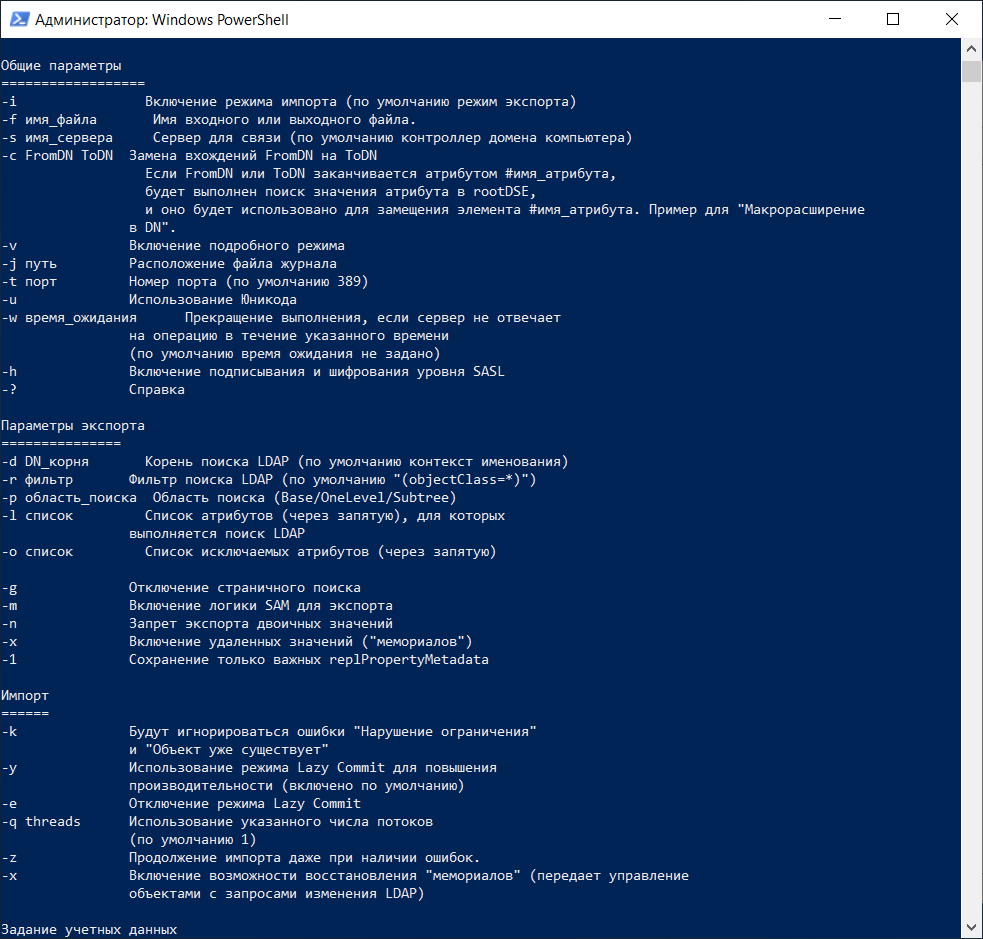
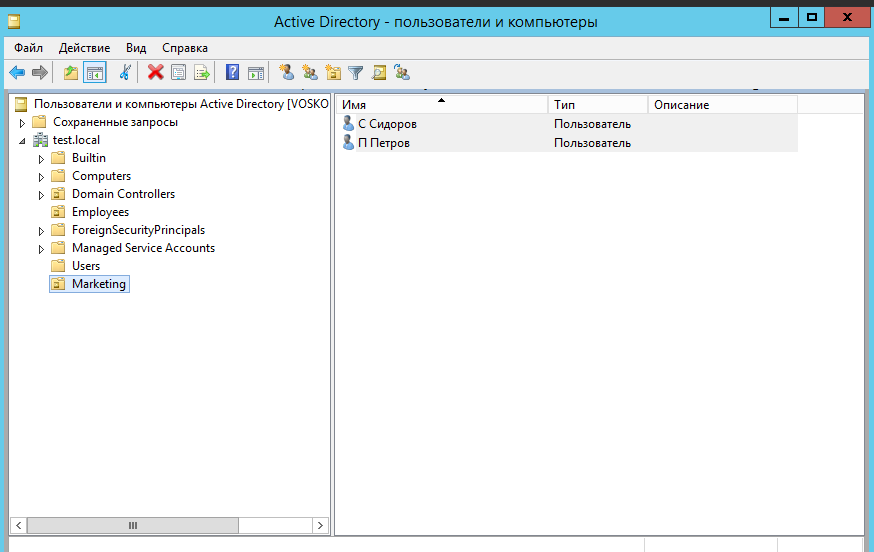
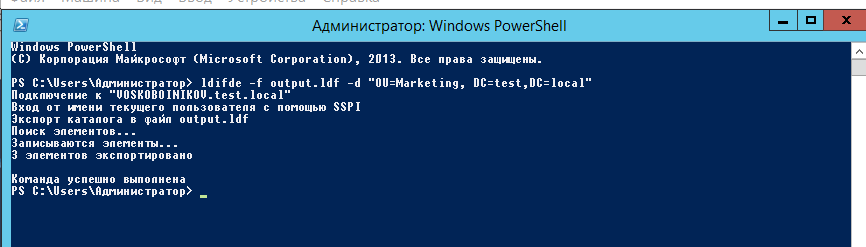
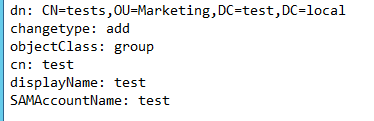
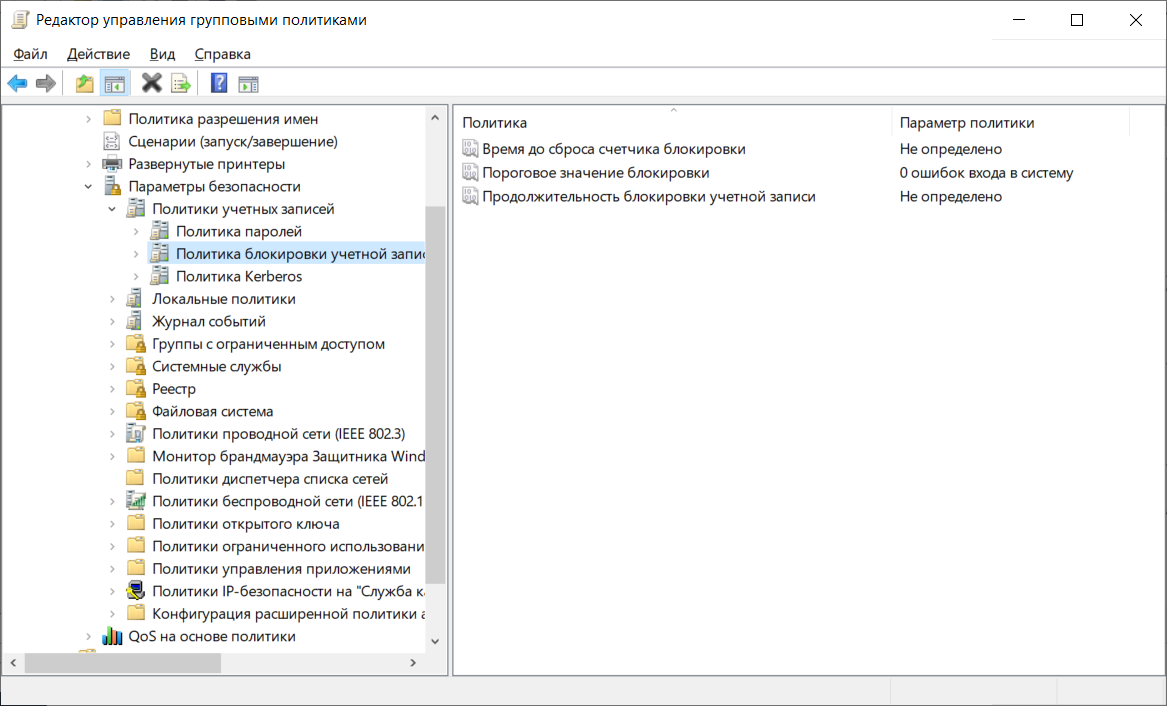
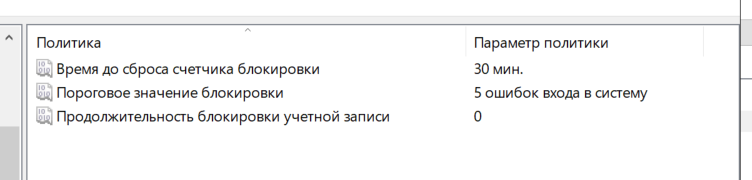
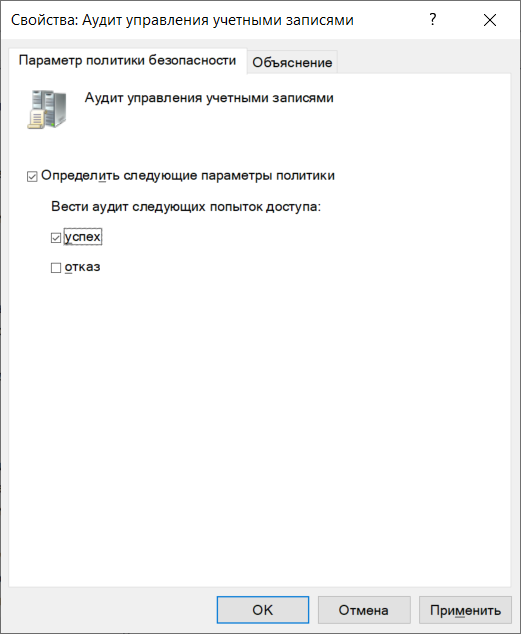
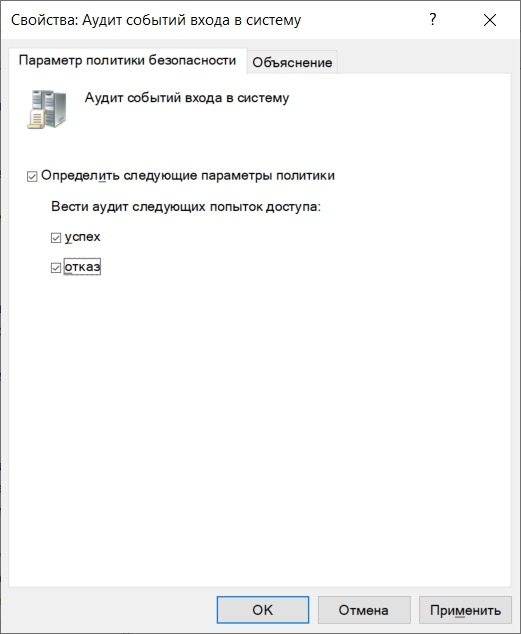
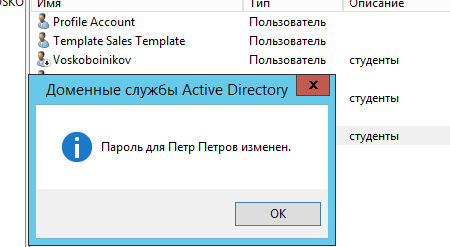
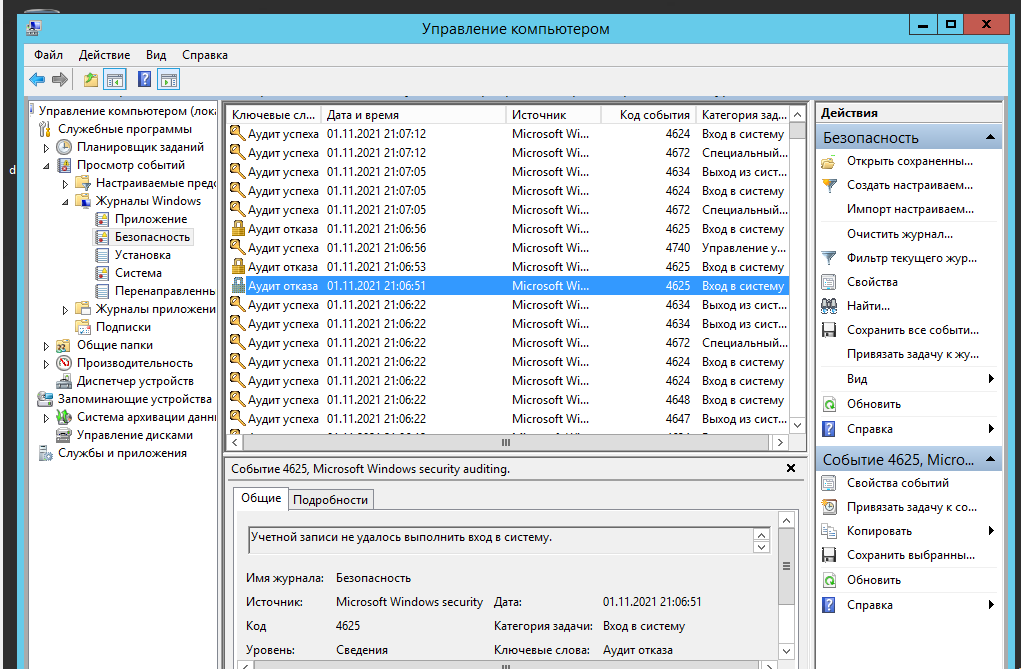
1. Добавление User1, User2 и User3 в группу Group1

Add-ADGroupMember -Identity group1 -Members User1, User2, User3 -Verbose

1. Перемещение Group1 в группу Group2.

Move-ADObject -Identity group1 -TargetPath "OU=groups,OU=Group2, DC=test, DC=local" -verbose

После выполнения сценария будет возможно преобразовать без промежуточных действий в универсальные группы Group1, Group3.

1. **Управление учетными записями групп с помощью команды LDIFDE**
   1. **Вывести список доступных параметров команды LDIFDE**
   2. **Экспорт сведений о пользователях из одного ОП.**Создал ОП Marketing, содержащий двух пользователей  
      Выполнил экспорт содержимого домена с помощью ldifde -f output.ldf -d "OU=Marketing,DC=test,DC=local"  
      
   3. **Создание группы командой LDIFDE**Создал файл с описанием создаваемой группы.  
        
      Импортировал его с помощью ldifde -I -f input.ldf -k  
      C:\Users\500a5\Desktop\01-11-2021 20-41-51.png
2. **Работа с политиками**
   1. **Настройка политик**Открыл редактор управления групповыми политиками; нашел раздел Политика блокировки учетной записи.  
        
      Изменил политики в соответствии с заданием  
        
      Изменил политики аудита в соответствии с заданием  
      
   2. **Генерация событий входа в систему**Произвел несколько попыток войти под учетной записью petr.petrov с неверным паролем; затем вошел с верным паролем.
   3. **Генерация событий управления учетными записями**В панели управления Active Directory сменил пароль пользователя petr.petrov.  
      ****
   4. **Анализ событий безопасности, сгенерированных проверкой подлинности**В разделе Просмотр событий открыл журнал безопасности Windows. Нашел записи, относящиеся к сгенерированным событиям удачных и неудачных входов и смены пароля.  
      ****

**Вывод:** в процессе выполнения лабораторной работы получил навыки работы с группами Active Directory с помощью сценариев PowerShell и команды LDIFDE. Научился настраивать политики и связанные с ними события, изучил функцию аудита, т.е., отслеживания различных событий, происходящих внутри домена.

1. Что такое группы Active Directory? Типы групп.

Active Directory – службы каталогов корпорации Microsoft для операционных систем семейства Windows server. Первоначально создавалась как LDAP-совместимая реализация службы каталогов.

Существует три типа групп:

* Локальная
* Глобальная
* Универсальная

2. Перечислите политики паролей. Что они определяют?

* Минимальные и максимальные длины паролей
* Минимальные и максимальные сроки действия этих паролей
* Требования к сложности пароля
* Хранения паролей с помощью реверсируемого шифрования

3. Перечислите политики блокировки учетной записи. Что они определяют?

* Блокировка после некоторого количества неудачных попыток входа
* Время, на которое устанавливается блокировка
* Время, через которое сбрасывается счетчик неудачных входов

4. Что такое аудит? Перечислите политики аудита.

Аудит – процесс отслеживания различных действий, выполняемых ОС. Политики аудита объединены в группы:

* Аудит проверки учетных данных
* Аудит службы проверки подлинности Kerberos
* Аудит операций с билетами службы Kerberos
* Аудит других событий входа учетных записей
* Управление учетными записями
* Аудит управления группами приложений
* Аудит управления группами распространения
* Аудит других событий управления учетными записями
* Аудит управления группами безопасности
* Аудит управления учетными записями пользователей

5. Что содержит журнал событий безопасности?

Журнал событий безопасности содержит события, относящиеся к обеспечению безопасности системы.

* попытки входа в учетную запись
* использование ресурсов (файлов, реестра, устройств)
* управление учетными записями
* изменения прав и привилегий аккаунтов
* запуск и остановка процессов (программ)

Типы регистрируемых событий можно сконфигурировать с помощью редактора политик.