МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ 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: студент группы ВТ-41

Ковалёв И. Д.

Проверил:

Федотов Е. А.

Белгород 2020

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

**Задания к работе:**

1. Создание и изменение группы.

В консоли Active Directory — пользователи и компьютеры раскройте контейнер Users и создайте в нем глобальную группу распространения Agents и выберите Свойства.

Можете ли вы изменить область действия и тип этой группы? Почему?

Если вы не можете изменить тип и область действия группы, ваш домен работает в смешанном режиме Windows 2000 или в промежуточном режиме Windows Server 2003. Чтобы изменить тип или область действия группы, необходимо перевести домен в

основной режим Windows 2000 или в режим Windows Server 2003.

2. Напишите сценарии, которые позволят выполнить операции:

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

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

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

4) Добавление User1, User2 и User3 в группу Group1.

5) Просмотр членов группы Group1.

6) Перемещение Group1 в группу Group2.

Какие группы теперь можно преобразовать в универсальные? Проверьте свои теоретические знания (вы должны без проблем преобразовать две из трех этих групп).

3. Управление учетными записями групп с помощью команды LDIFDE

3.1. Вывести список доступных параметров команды LDIFDE

3.2. Экспорт сведений о пользователях из одного ОП.

В домене создайте ОП Marketing. Добавьте в ОП Marketing двух или трех пользователей. Дайте им произвольные имена.

Экспортируете содержимое ОП Marketing из состава вашего домена.

3.3. Создание группы командой LDIFDE

С помощью команды LDIFDE добавить группу Management в ОП Marketing из состава вашего домена. В консоли Active Directory — пользователи и компьютеры проверьте, что новая группа создана.

4. Работа с политиками

4.1. Настройка политик

В консоли Active Directory — пользователи и компьютеры щелкните узел домена и выберите его свойства. На вкладке Групповая политика выберите Default Domain Policy и щелкните Изменить. Раскройте узлы Конфигурация компьютера, Конфигурация Windows, Параметры безопасности, Политики учетных записей и Политика блокировки учетной записи.

Дважды щелкните политику Блокировка учетной записи на. Установите флажок Определить следующий параметр политики. Установите продолжительность периода в 0. Убедитесь, что значение политики Блокировка учетной записи на — 0, пороговое значение — 5 и сброс политики счетчика произойдет через 30 минут.

Щелкните контейнер Контроллеры домена, расположенный по иерархии ниже узла домена и выберите Свойства. На вкладке Групповая политика выберите Default Domain Controllers Policy и щелкните Изменить.

Раскройте узлы Конфигурация компьютера, Конфигурация Windows, Параметры безопасности, Локальные политики и Политика аудита.

Дважды щелкните политику Аудит событий входа в систему. Выберите Определить следующий параметр политики, установите флажки Успех и Отказ.

Дважды щелкните политику Аудит входа в систему. Выберите Определить следующий параметр политики, установите флажки Успех и Отказ.

Дважды щелкните политику Аудит управления учетными записями. Выберите Определить следующий параметр политики, установите флажок Успех.

4.2. Генерация событий входа в систему

Завершите сеанс на Server1.

Сгенерируйте два события неудачного входа в систему, дважды попытавшись войти с именем пользователя petr.petrov и неверным паролем. Войдите в систему правильно (как пользователь petr.petrov). Выйдите из системы.

4.3. Генерация событий управления учетными записями

Войдите в систему как Администратор. Откройте консоль Active Directory — пользователи и компьютеры и выберите ОП Employees.

Выберите объект пользователя Петр Петров и раскройте меню Действие, в котором выберите команду Смена пароля. Введите и подтвердите новый пароль для Петр Петров.

4.4. Анализ событий безопасности, сгенерированных проверкой подлинности

Откройте консоль Управление компьютером из группы Администрирование.

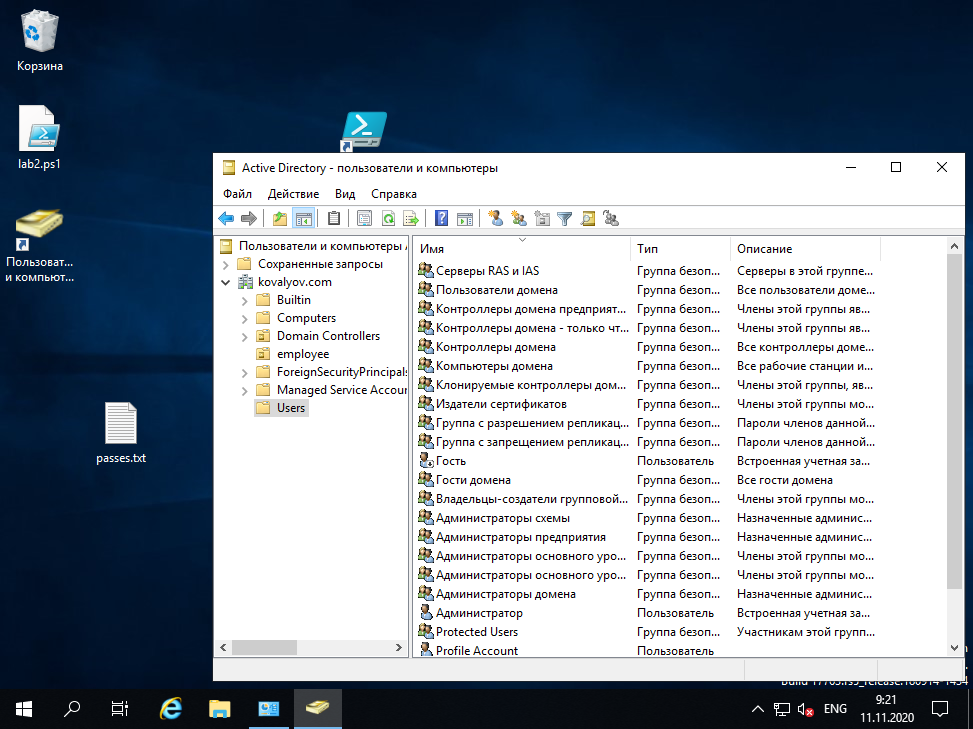
Раскройте узел Просмотр событий и щелкните Безопасность. Расширьте столбец Категория, чтобы видеть типы зарегистрированных событий.

Изучите события, сгенерированные действиями, которые вы только что выполнили. Обратите внимание на события неудачного и удачного входа в систему, а также на смену пароля для пользователя Петр Петров.

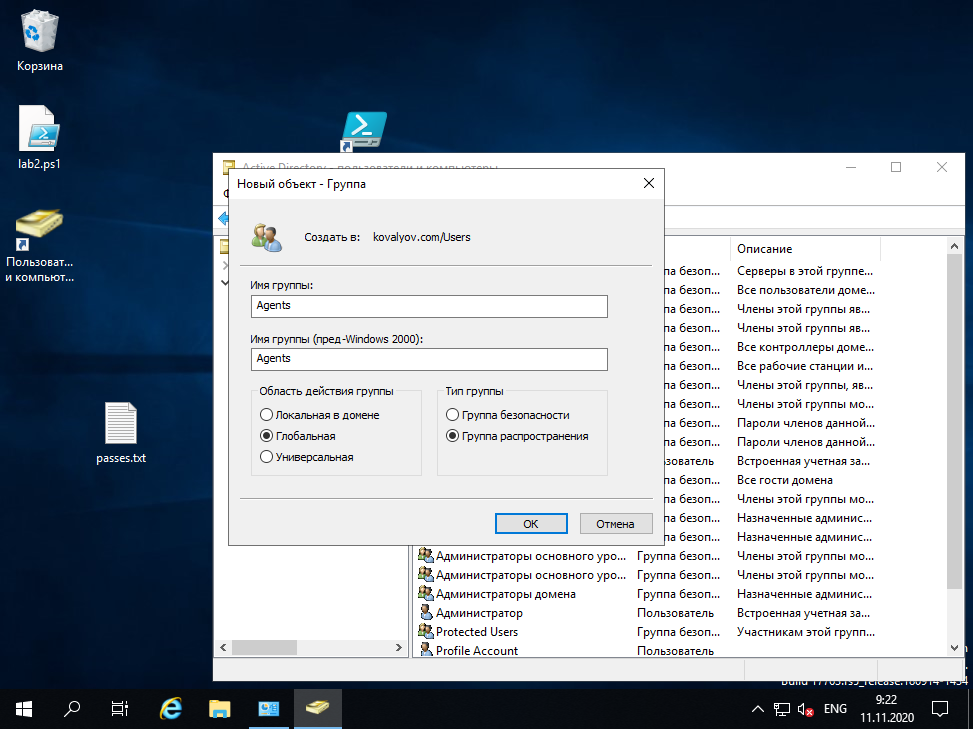
**Выполнение**

1. Создание и изменение группы.

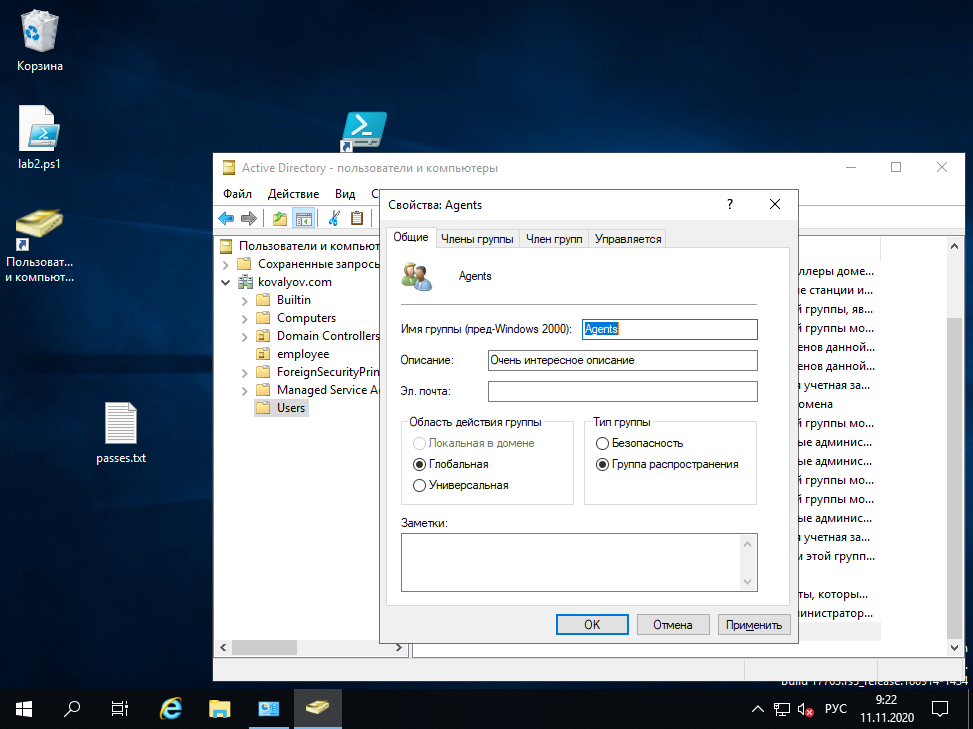
Откроем консоль Active Directory – пользователи и компьютеры:

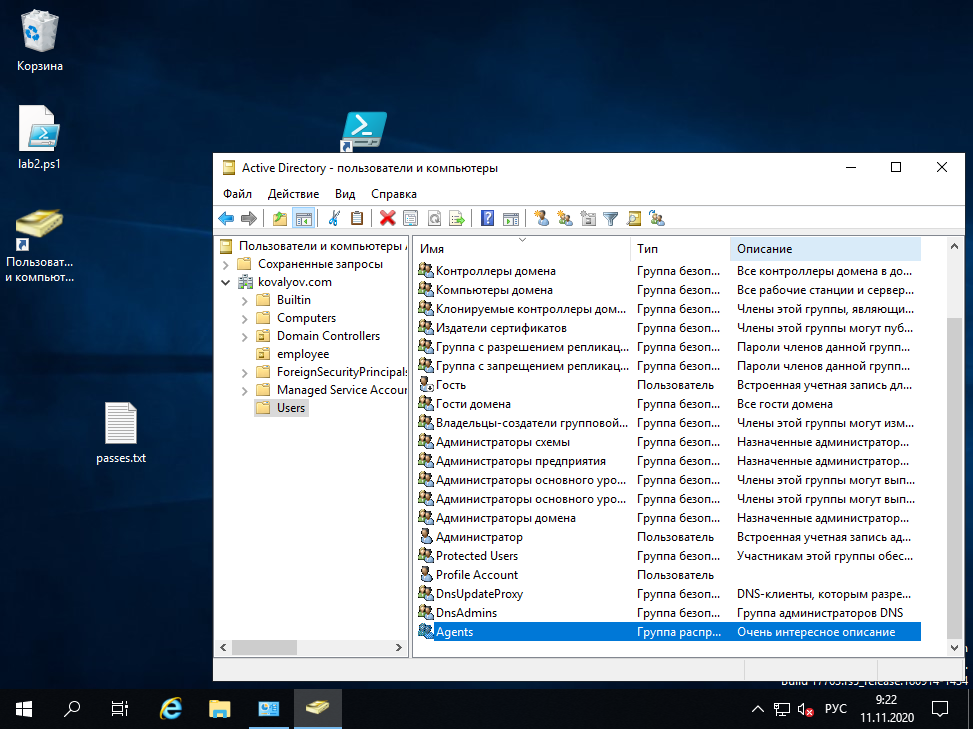


И раскроем контейнер Users и создадим в нем глобальную группу распространения Agents



Просмотрим свойства данного объекта и попробуем изменить:





Изменение описания прошло успешно, поскольку сервер работает в качестве контроллера домена и никаких ограничений на него не наложено.

2. Напишем сценарии, которые позволят выполнить операции:

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

2) 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

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

New-ADUser "User1" -Verbose

New-ADUser "User2" -Verbose

New-ADUser "User3" -Verbose

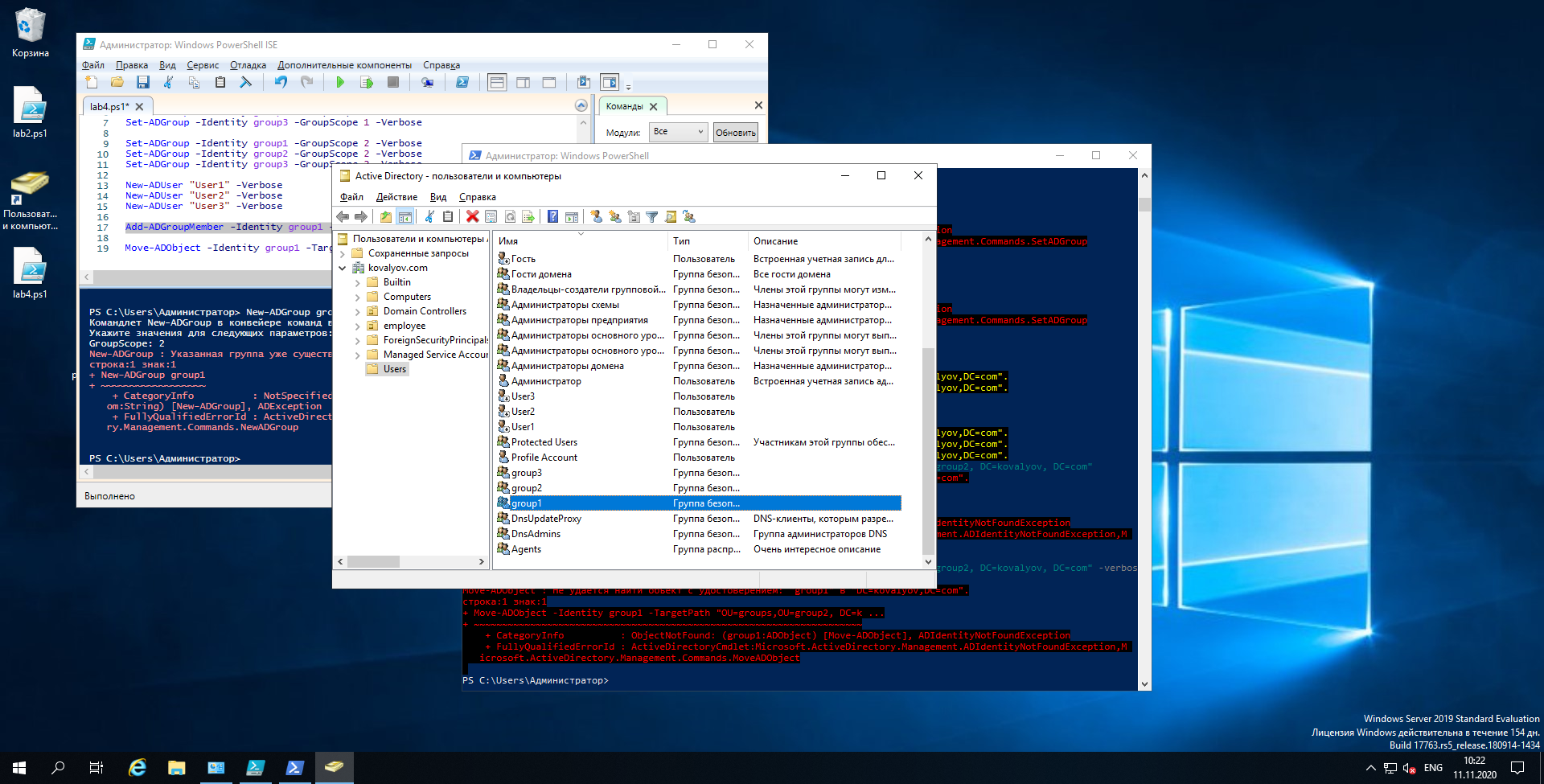
4) Добавление User1, User2 и User3 в группу Group1.

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

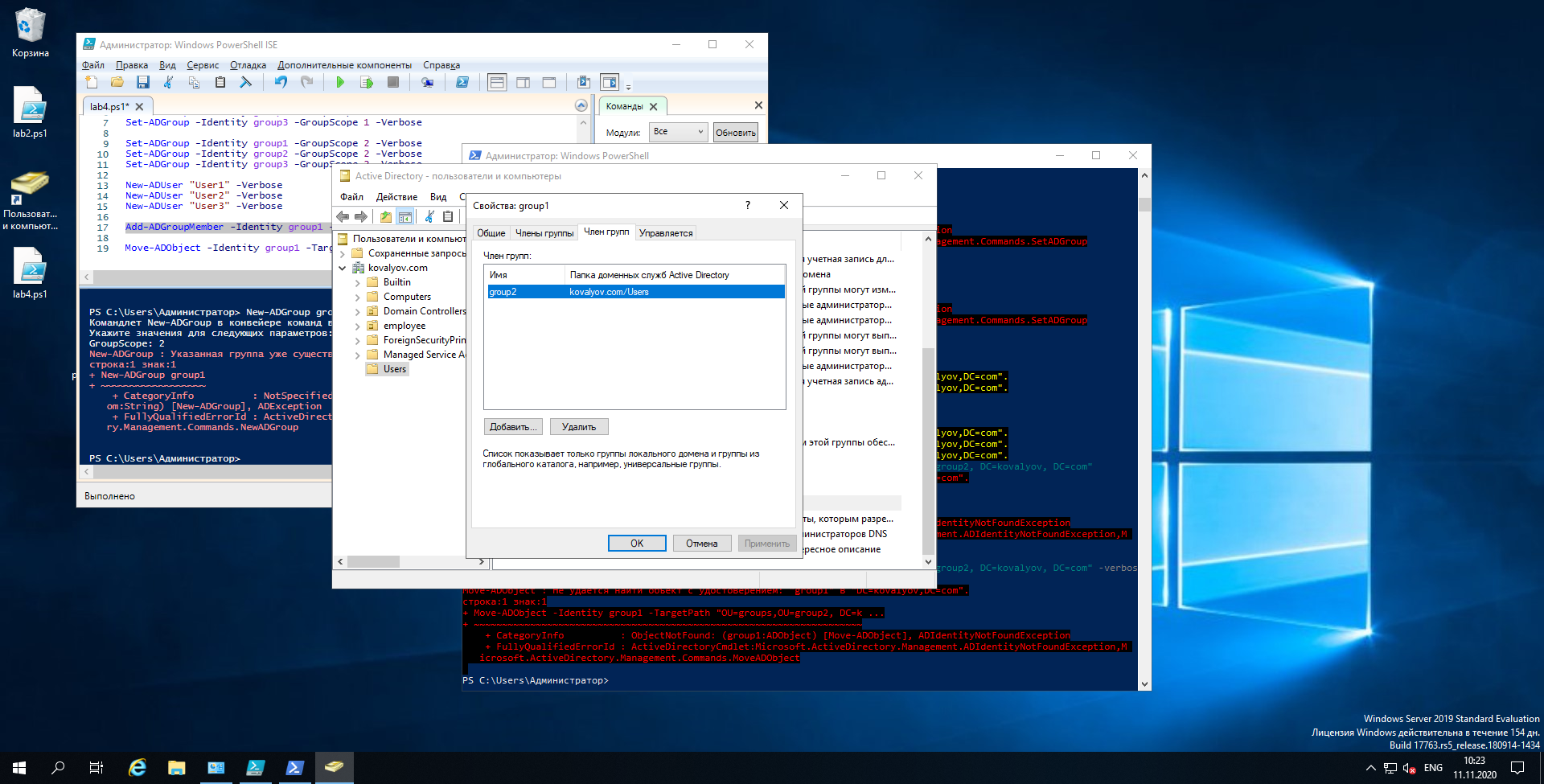
5) Перемещение Group1 в группу Group2.

Move-ADObject -Identity group1 -TargetPath "OU=groups,OU=group2, DC=kovalyov, DC=com" -verbose

Проверим результаты работы скриптов:



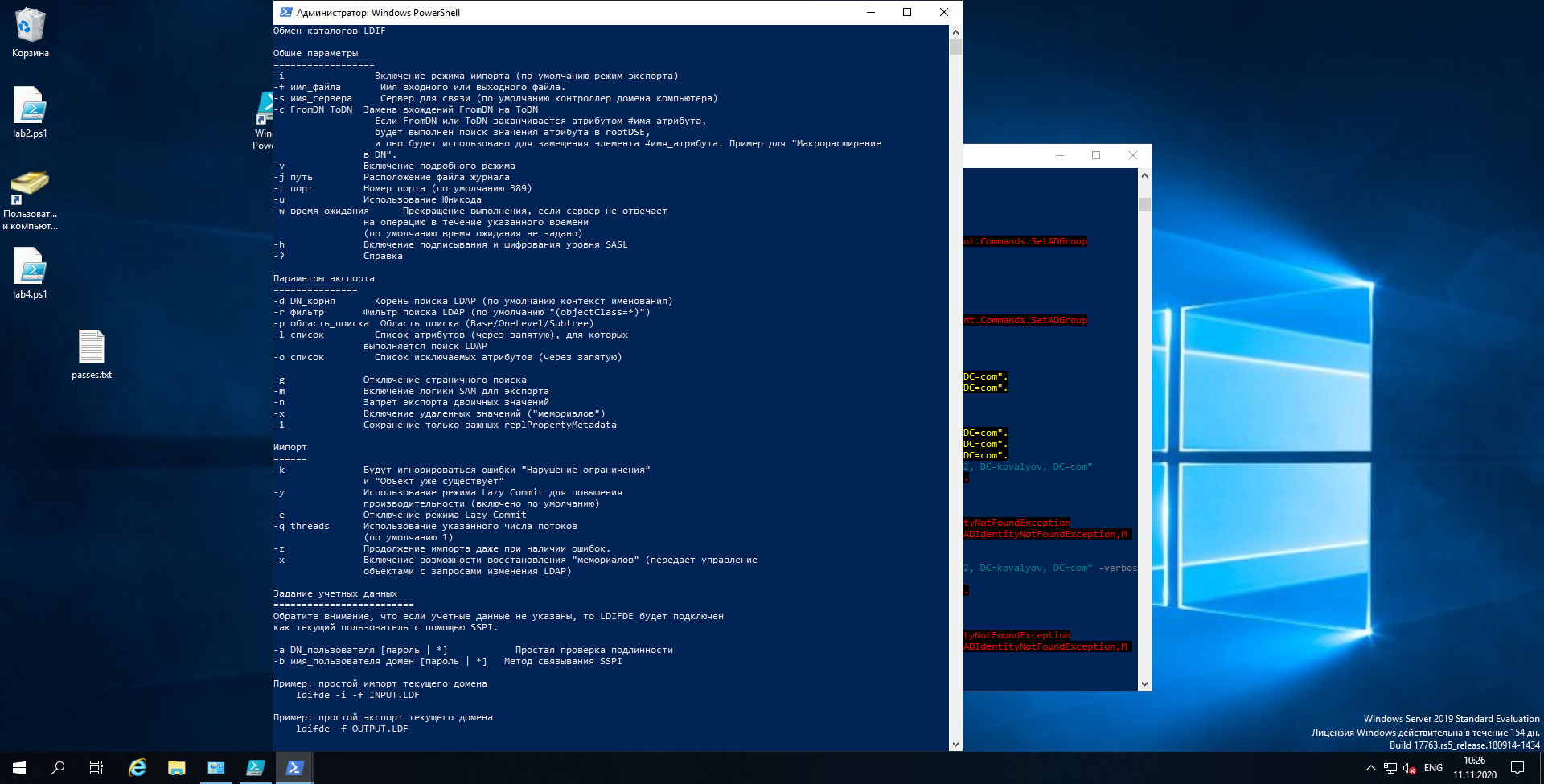
Группы и пользователи были созданы.



Group1 была перемещена в Group2.

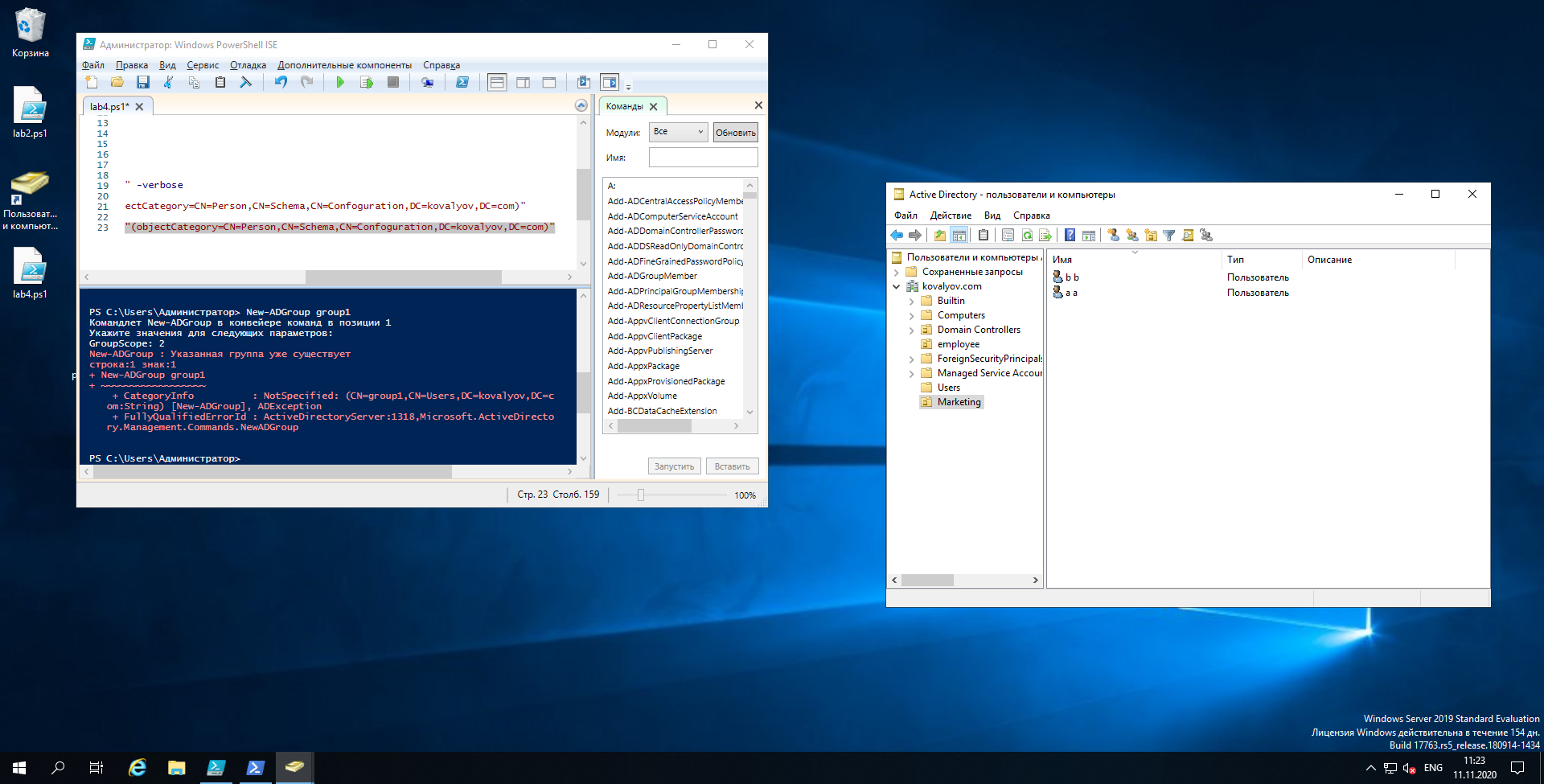
3. Управление учетными записями групп с помощью команды LDIFDE

3.1. Выведем список доступных параметров команды LDIFDE

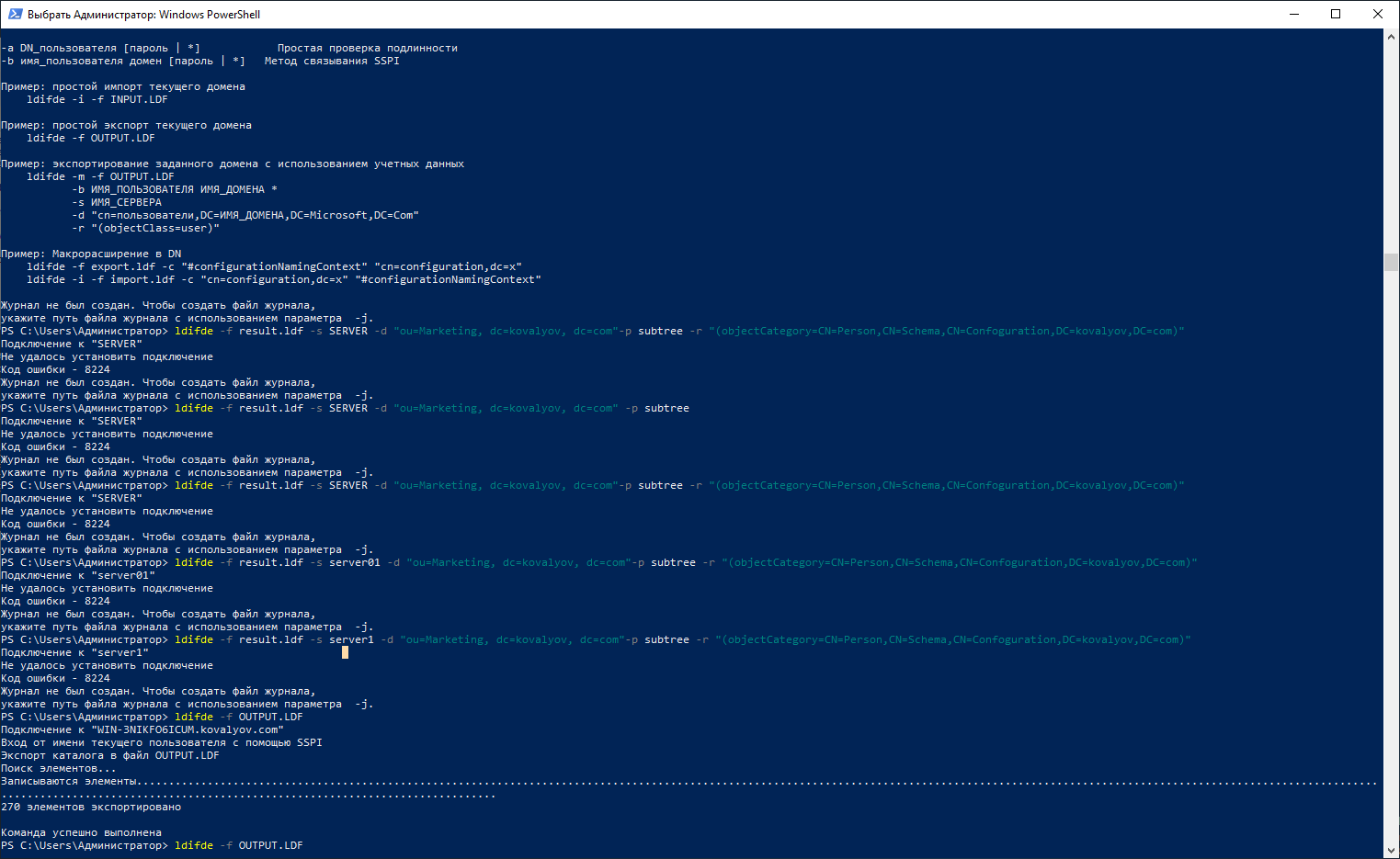


3.2. Экспорт сведений о пользователях из одного ОП.

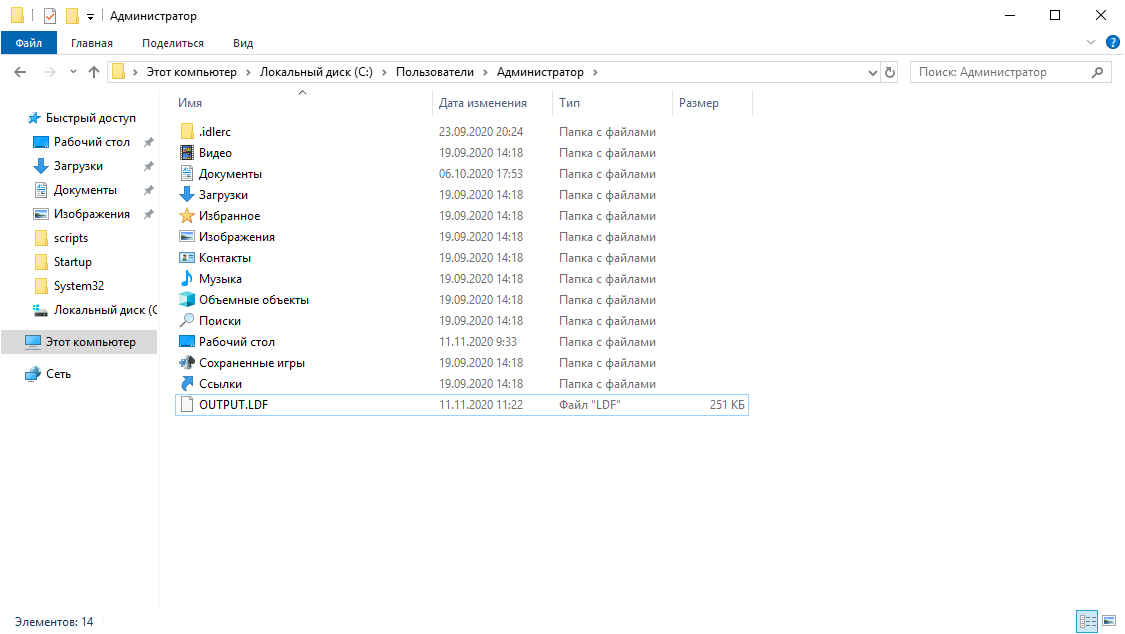
В домене был создан ОП Marketing, в него добавлены два пользователя:



Экспортируем содержимое домена с помощью команды ldifde -f OUTPUT.LDF:

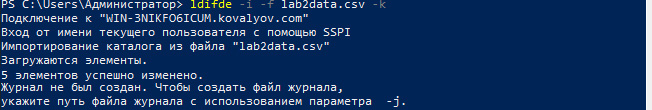


Полученный результат:



3.3. Импорт с помощью LDIFDE

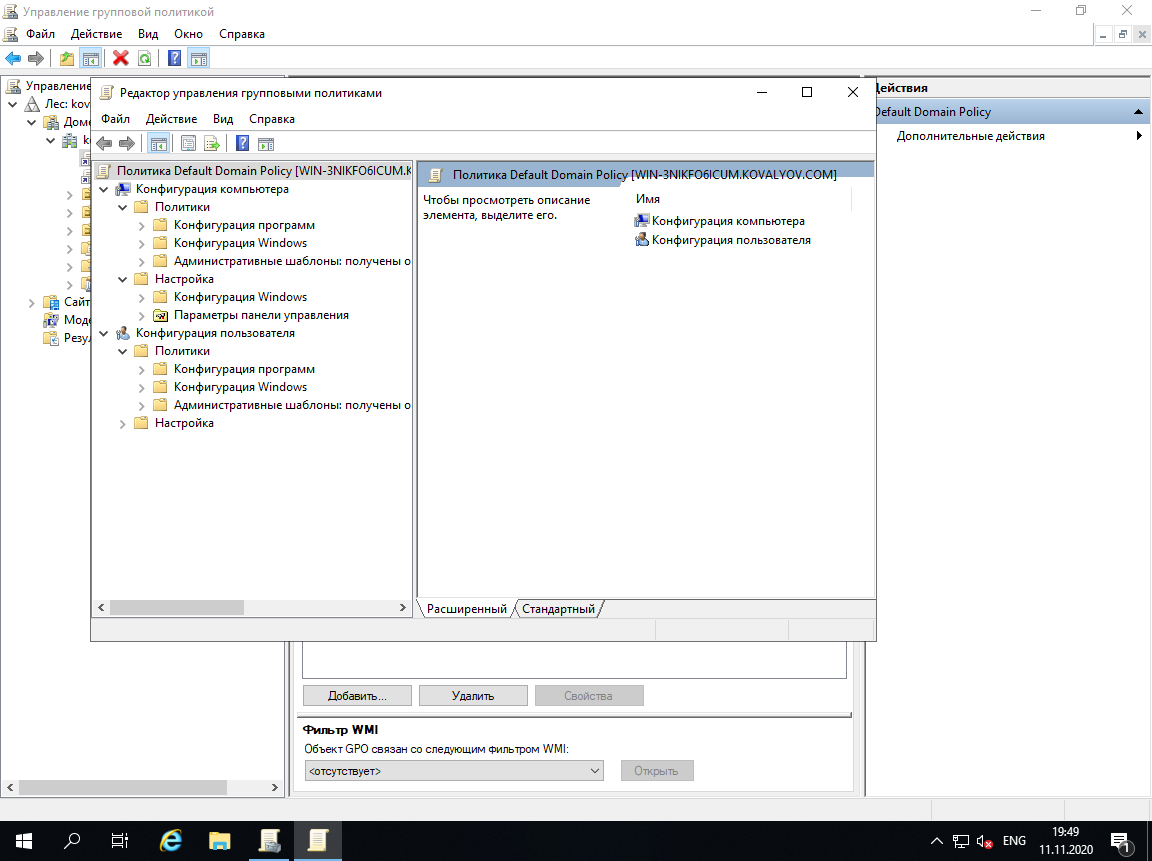
Загрузим данные из полученного ранее файла, содержащего информацию о содержимом одного из ОП:



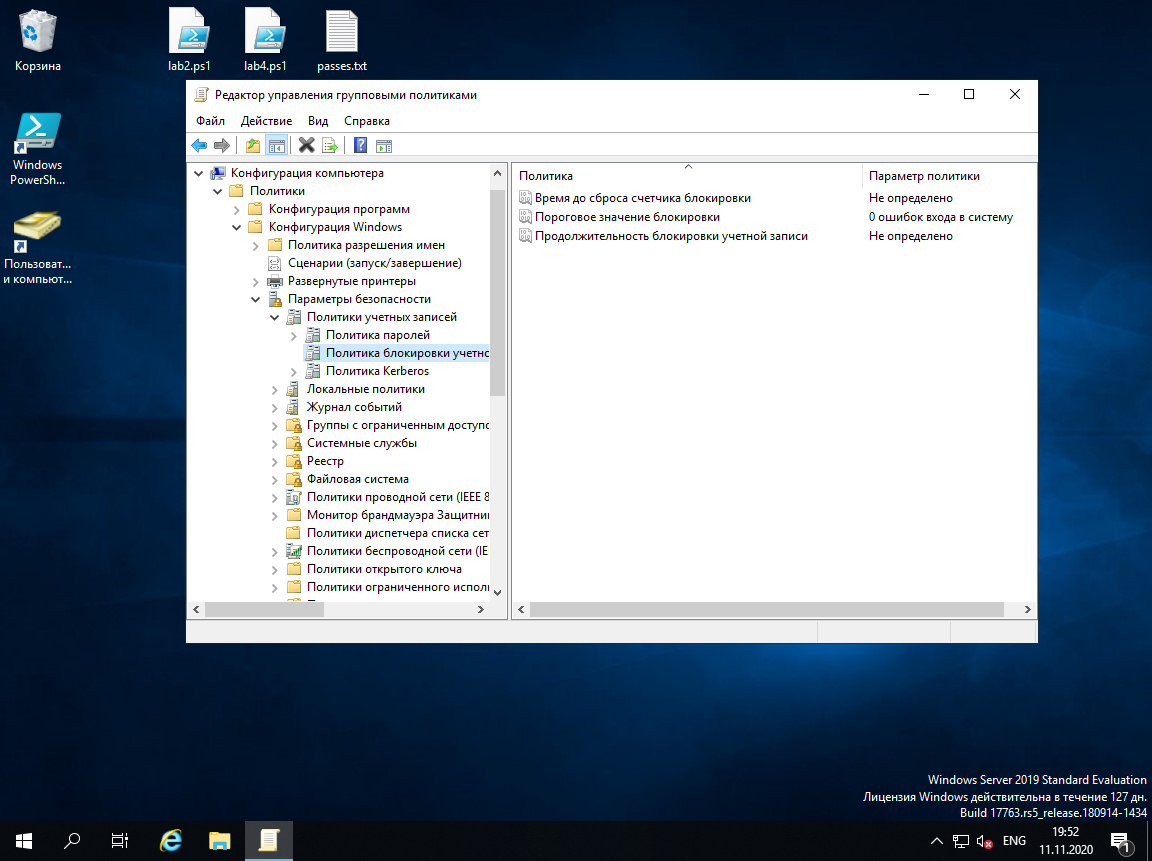
4. Работа с политиками

4.1. Настройка политик

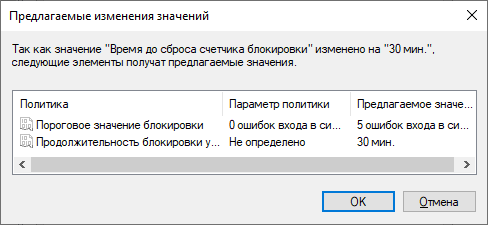
В консоли Active Directory — пользователи и компьютеры щелкнем узел домена Kovalyov.com и выберите его свойства.



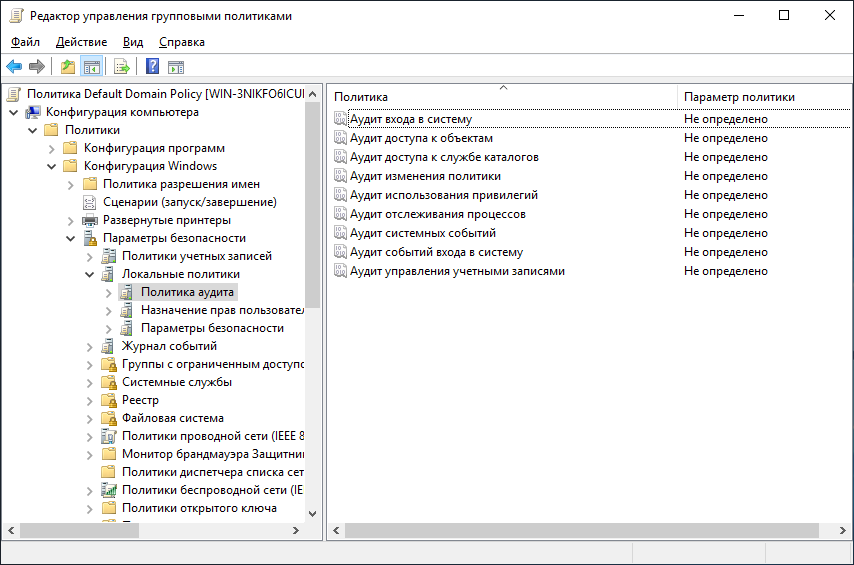
На вкладке Групповая политика выберем Default Domain Policy и щелкнем Изменить. Раскроем узлы Конфигурация компьютера, Конфигурация Windows, Параметры безопасности, Политики учетных записей и Политика блокировки учетной записи.



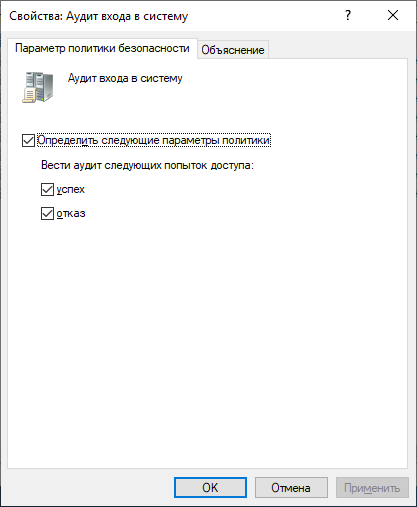
Установим флаг Определить следующий параметр политики. Установим необходимые параметры:



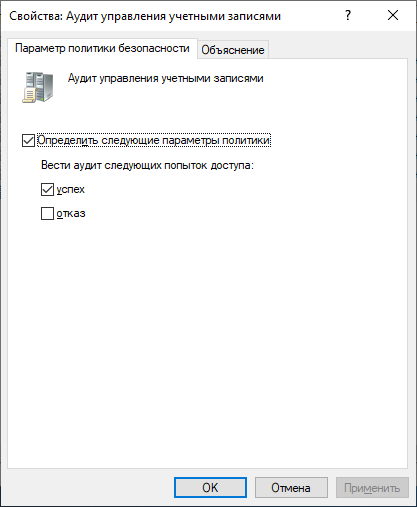
Откроем политики аудита:



Настроим политику Аудит событий входа в систему, выбрав Определить следующий параметр политики, и установим флажки Успех и Отказ.



Настроим Аудит управления учетными записями:

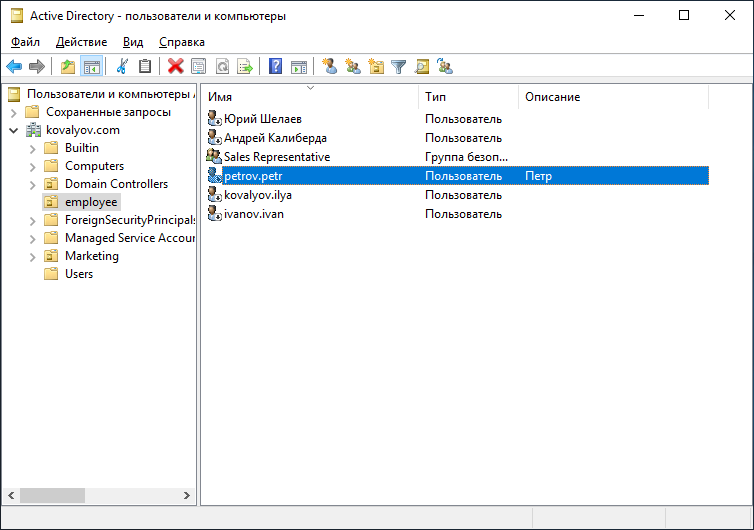


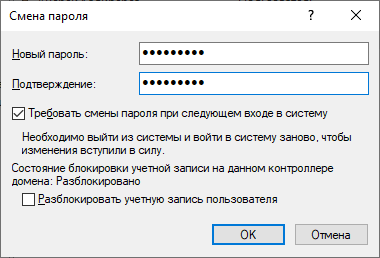
4.2. Генерация событий входа в систему

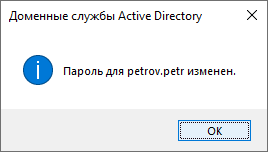
Завершим сеанс на SERVER и сгенерируем два события неудачного входа в систему, введя неверный пароль у пользователя.

4.3. Генерация событий управления учетными записями

Создадим новый пароль для пользователя petr.petrov:

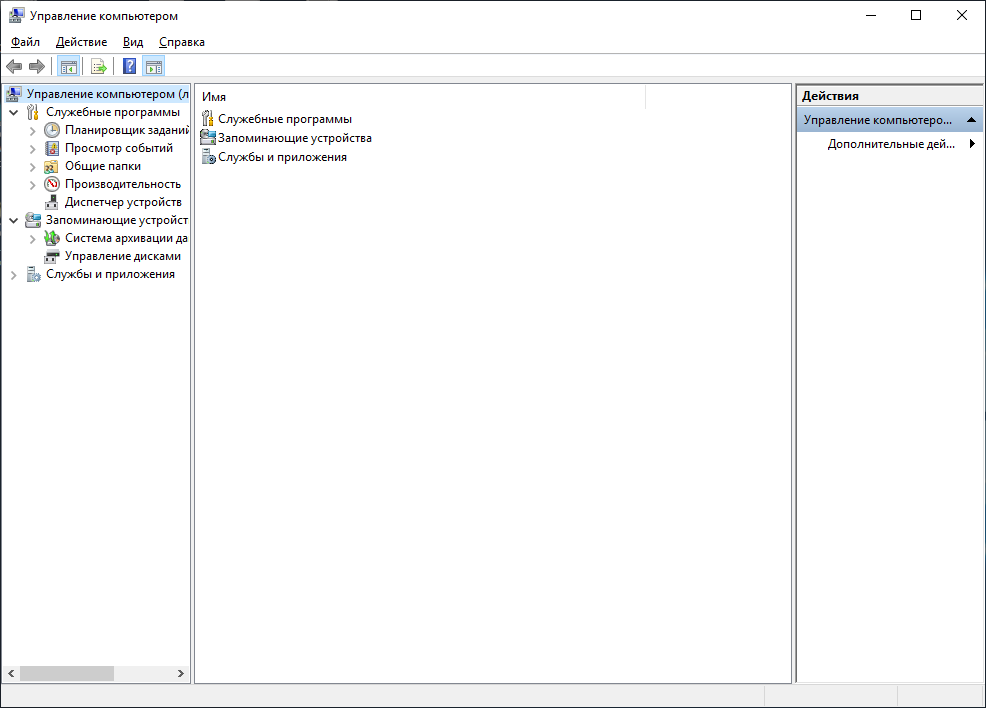




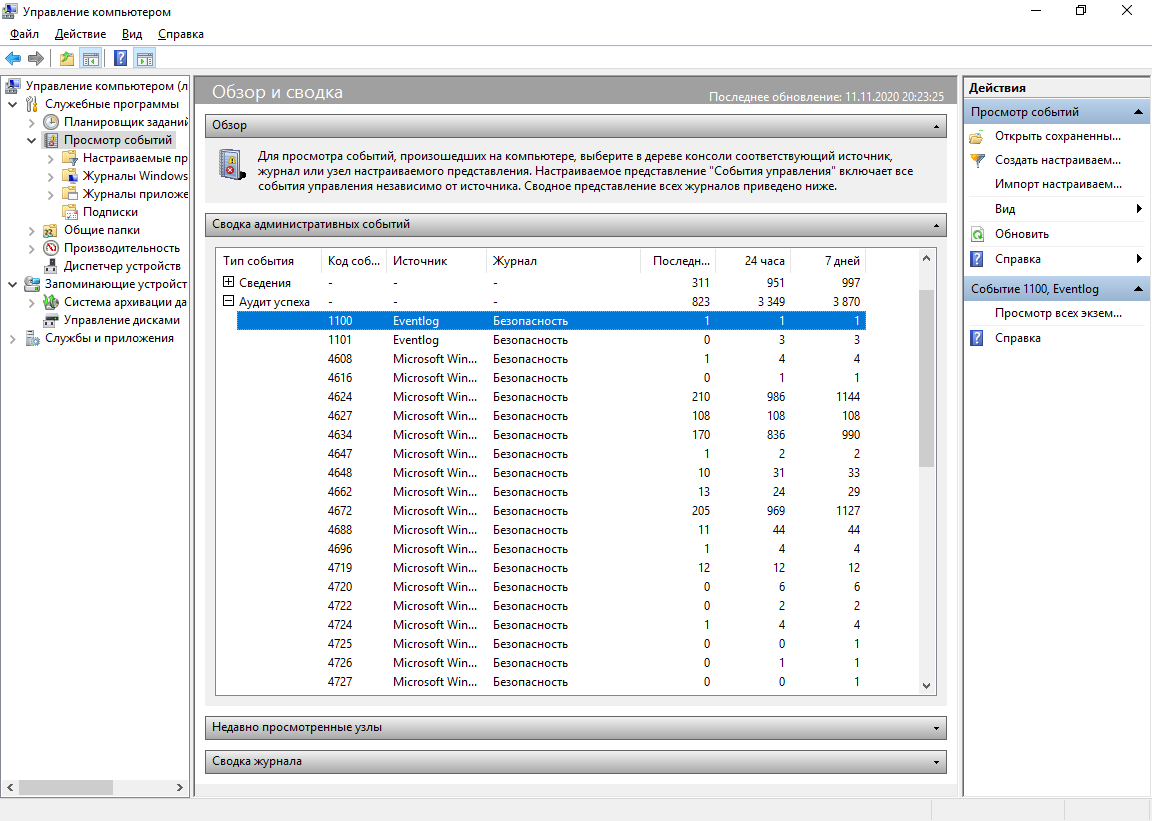


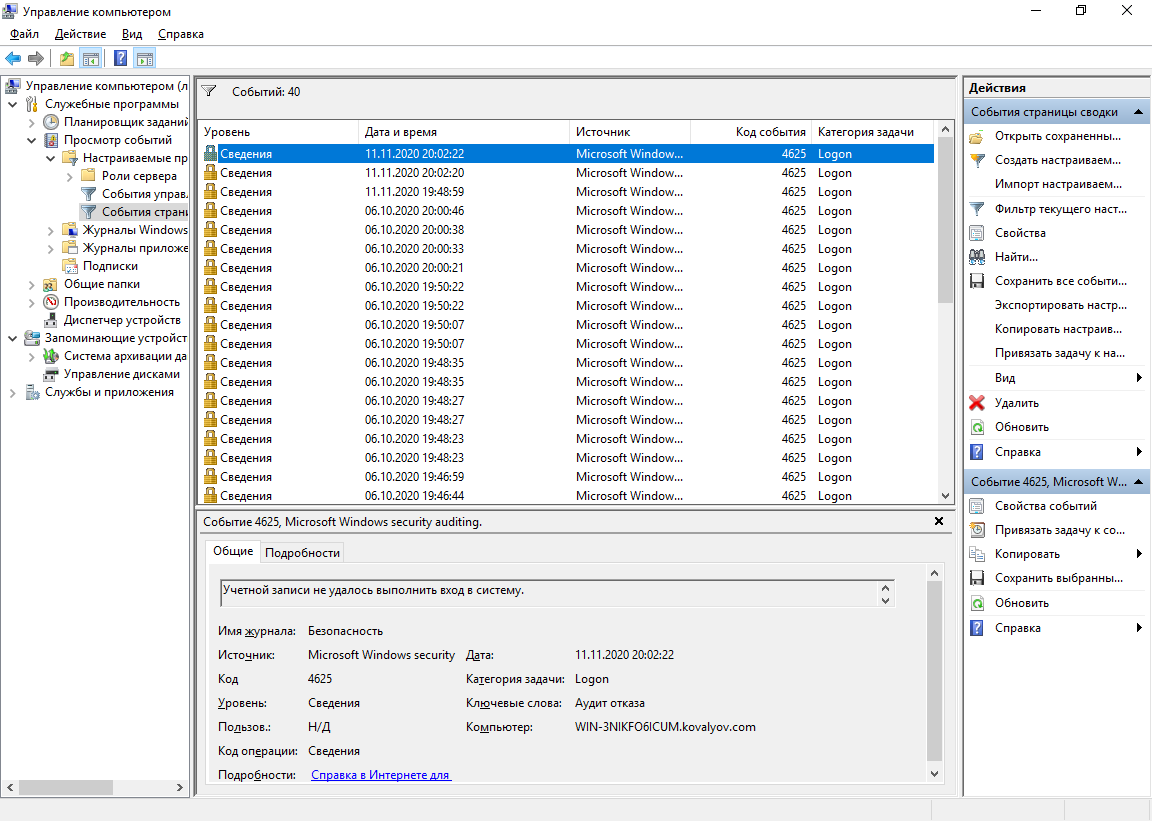
4.4. Анализ событий безопасности, сгенерированных проверкой подлинности

Откроем консоль Управление компьютером из группы Администрирование:



Раскрыв узел Просмотр событий увидим события, сгенерированные сменой пароля:





**Вывод:** в процессе выполнения лабораторной работы были получены навыки работы с такими объектами Active Directory, как группы с помощью сценариев powershell, команды LDIFDE. Так же были настроены политики и связанные с ними события, рассмотрен аудит, который позволяет отслеживать различные события, происходящие в рамках домена.

**Контрольные вопросы**

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 в домене:

* Локальная в домене – используется для управления разрешениями доступа к ресурсам только для того домена, в котором была создана.
* Глобальная в домене – может быть использована для предоставления доступа к ресурсам другого домена.
* Универсальная группа – рекомендуется использовать в лесах из множества доменов.

1. Перечислите политики паролей. Что они определяют?

Существуют такие политики паролей:

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

Из их названия очевидно, что они определяют.

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

* Блокировка ввода пароля на определенное время
* Восстановление счетчика блокировки

Данные политики применяются для защиты учетной записи пользователя от злоумышленника, который не придумал ничего лучше, чем перебирать все пароли.

1. Что такое аудит? Перечислите политики аудита.

Аудит – процесс отслеживания различных действий, выполняемых ОС.

Существуют такие политики аудита:

* 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
* и так далее.

1. Что содержит журнал событий безопасности?

Журнал событий Безопасность содержит события, влияющие на безопасность системы. Это попытки (иудачные и неудачные) входа в аккаунты системы, использование ресурсов (файлов, реестра, устройств), управление учетными записями, изменения прав и привилегий аккаунтов, запуск и остановка процессов (программ) и т.д. Администратор может сконфигурировать какие категории событий необходимо регистрировать. Например, по умолчанию система сконфигурирована регистрировать события управления учетными записями, события входа в систему, а аудит доступа к объектам не включен. Стоит быть осторожным при настройке аудита доступа к файлам, то это может привести к появлению большого количества событий, что в свою очередь может негативно отразиться на общей производительности системы и быстрому переполнению журнала безопасности.