Санкт-Петербургский национальный исследовательский
университет информационных технологий, механики и оптики

Факультет инфокоммуникационных технологий

Направление подготовки 11.03.02

Лабораторная работа №5
«Развертывание и настройка домена на базе Microsoft Windows Server для пользователей корпоративной сети»

Выполнили:
Швалов Даниил Андреевич К34211
Кротова Милена Игоревна К34201
Проверила:
Казанова Полина Петровна

Санкт-Петербург

2024

1. Введение

Цель работы: в виртуальной машине v1 поднять домен class.local, создать организационные подразделения, пользователей и группы, подключить виртуальную машину v2 к домену как клиентский компьютер, предоставить разрешения на ресурсы с помощью доменных групп.

2. Ход работы

Упражнение 1. Создание домена и логической структуры подразделений

В данном упражнении необходимо было создать домен и логическую структуру подразделений. Сначала для этого было настроено использование собственного адреса в качестве DNS-сервера. Затем были установлены компоненты «DNS» и «Доменные службы Active Directory». После установки компонентов была повышена роль сервера до уровня контроллера домена. Данные действия показаны на рисунках 1-3.

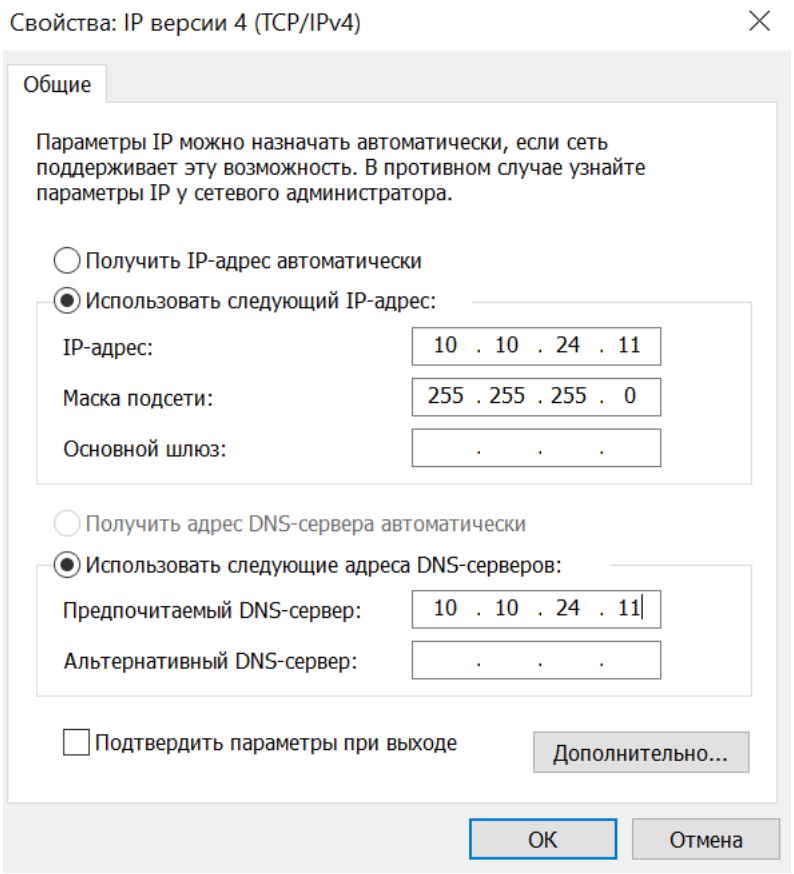

Рисунок 1 — Использование собственного адреса в качестве DNS-сервера

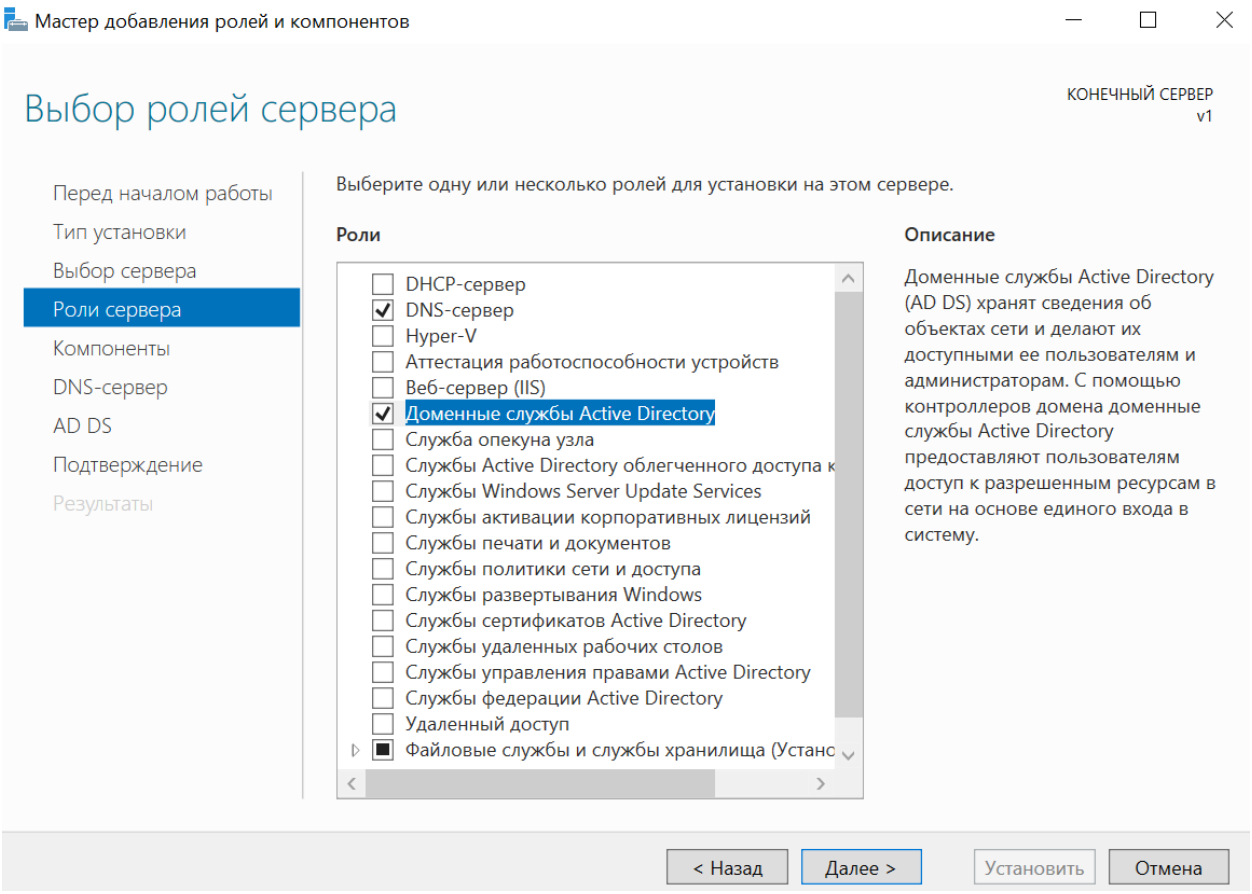

Рисунок 2 — Добавление компонентов «DNS» и «Доменные службы Active Directory»

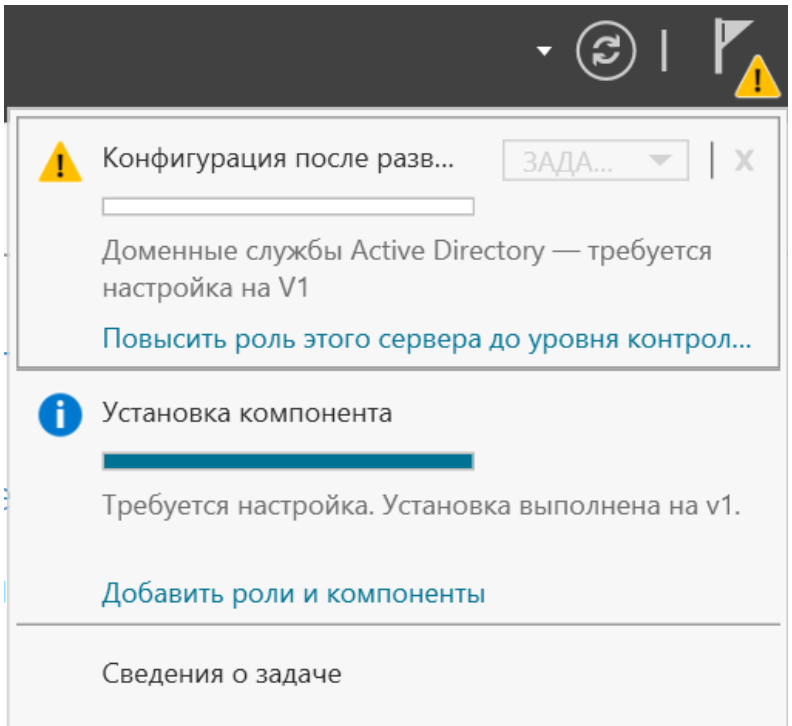

Рисунок 3 — Повышение роли сервера

После этого был добавлен новый лес с именем корневого домена «class. local». В качестве пароля для режима восстановления служб каталогов был использован пароль «Pa$$w0rd». В качестве режима работы домена и леса был выбран режим «Windows Server 2016». После этого было указано расположение базы данных, файлов журнала и папки SYSVOL согласно заданию. Процесс настройки представлен на рисунках 4-6.

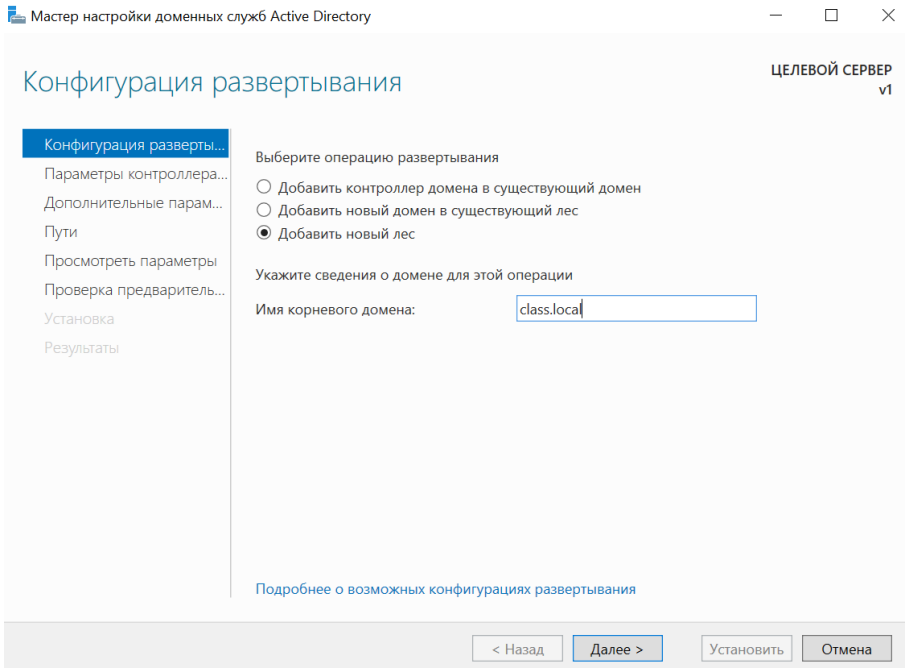

Рисунок 4 — Настройка имени корневого домена

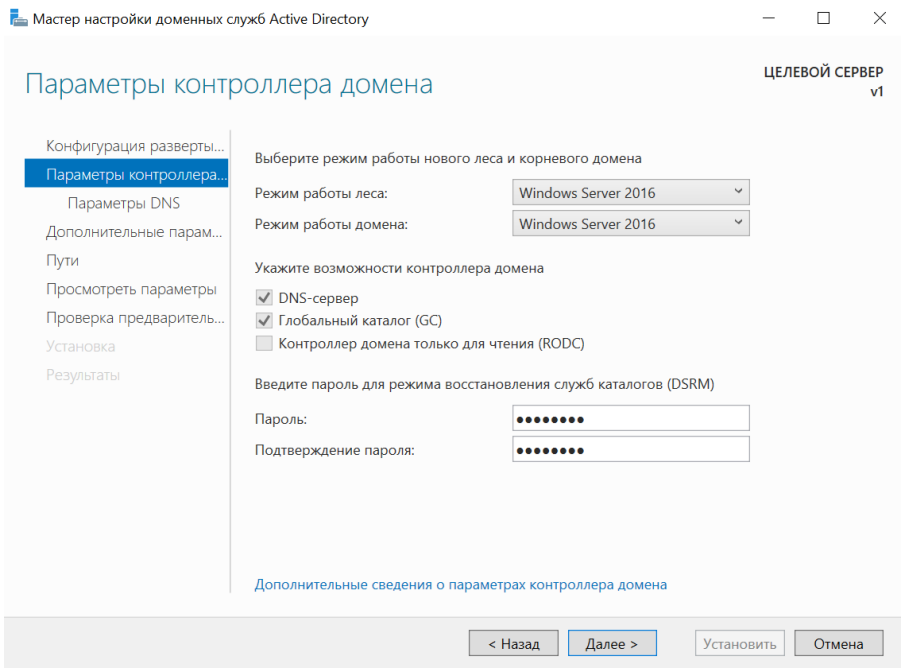

Рисунок 5 — Настройка параметров контроллера домена

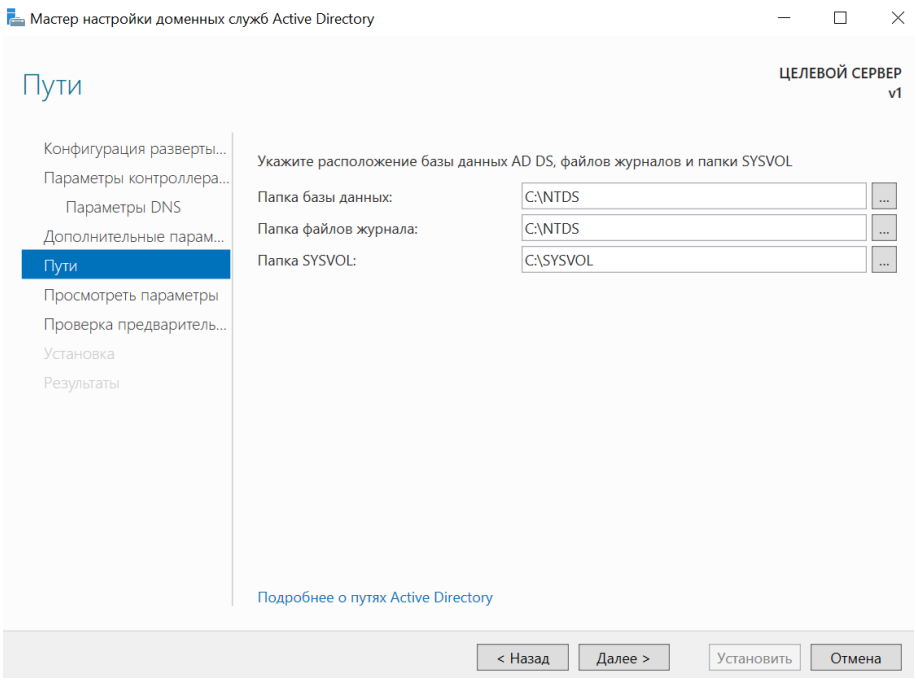

Рисунок 6 — Настройка путей

После завершения настройки были проверены журналы событий служб «AD DS» и «DNS». В журналах не было обнаружено ошибок, что свидетельствует о корректной настройке. Также была проверена доступность папки «SYSVOL» по сети, проверены записи ресурсов на DNS-сервере. Все работало корректно и без ошибок. Данные действия показаны на рисунках 7-10.

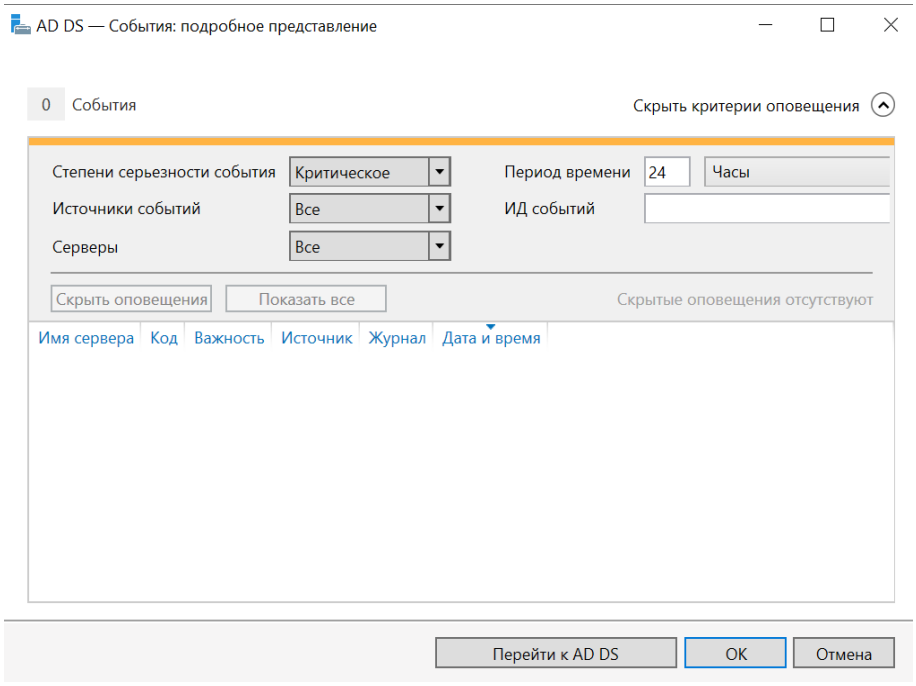

Рисунок 7 — Журнал событий AD DS

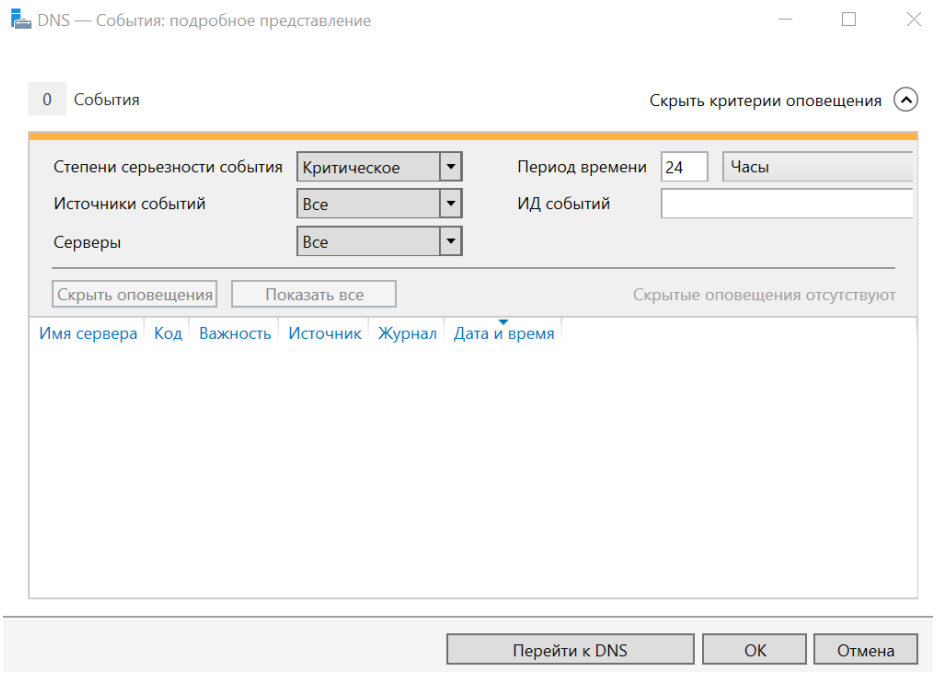

Рисунок 8 — Журнал событий DNS

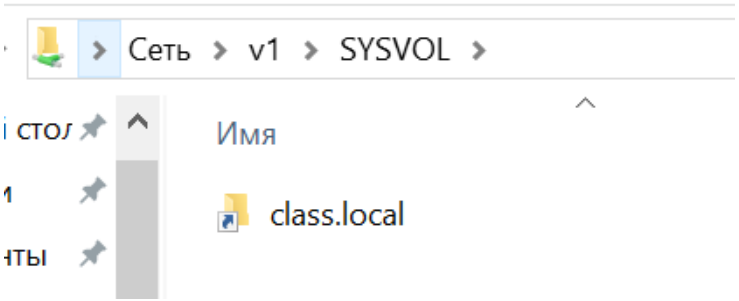

Рисунок 9 — Проверка доступности папки «SYSVOL» по сети

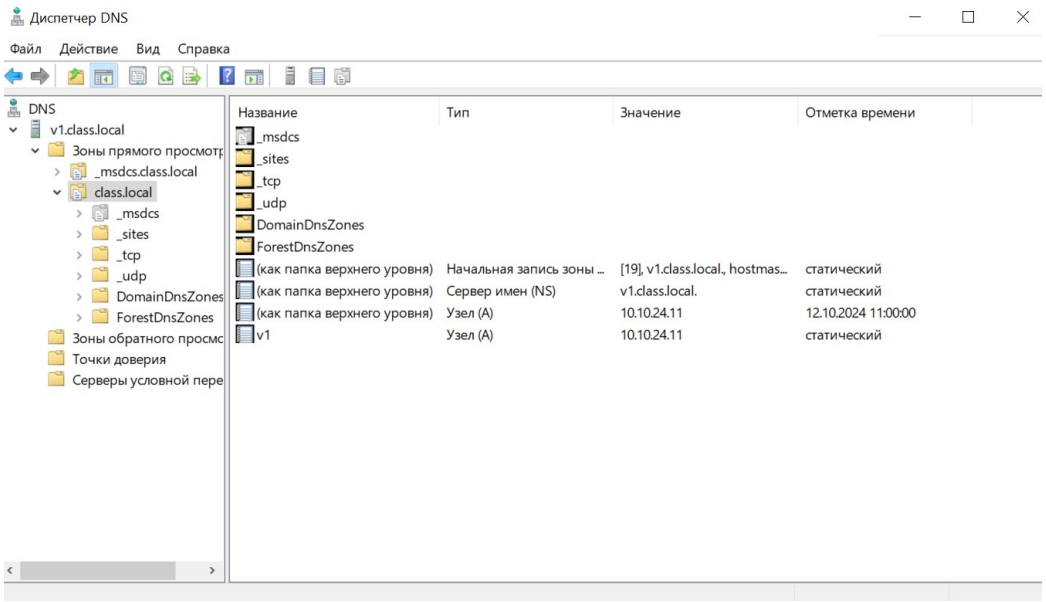

Рисунок 10 — Проверка записей на DNS-сервере

Затем была создана структура подразделений «admin», «comps», «office» с дочерними «buhgalters», «managers», «groups» согласно заданию. На рисунках 11-12 показан процесс и результат создания подразделений.

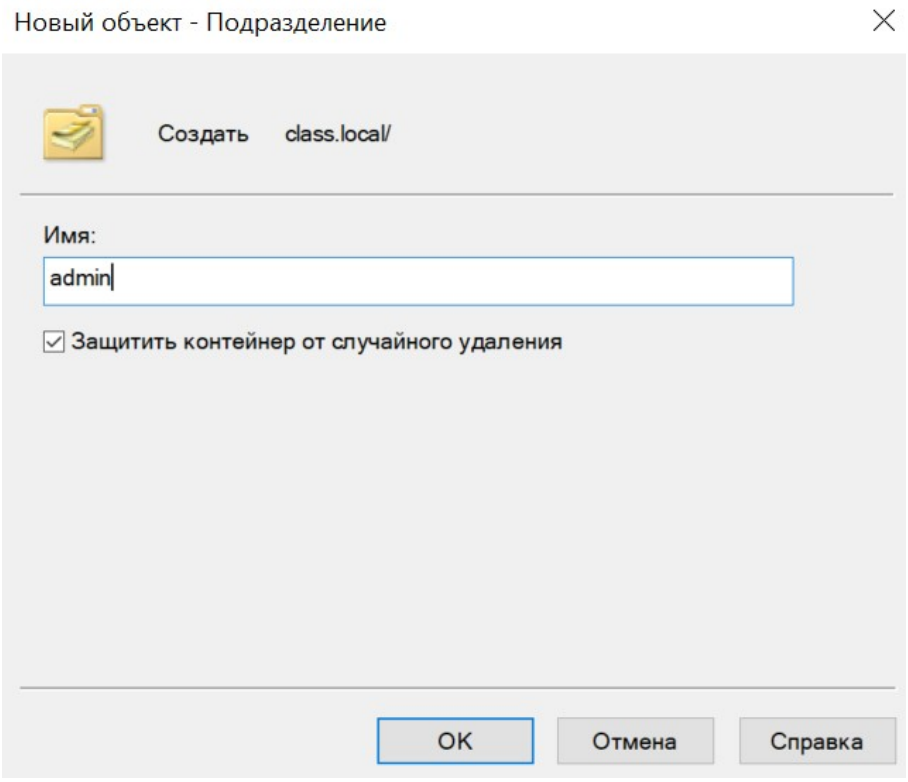

Рисунок 11 — Создание подразделения «admin»

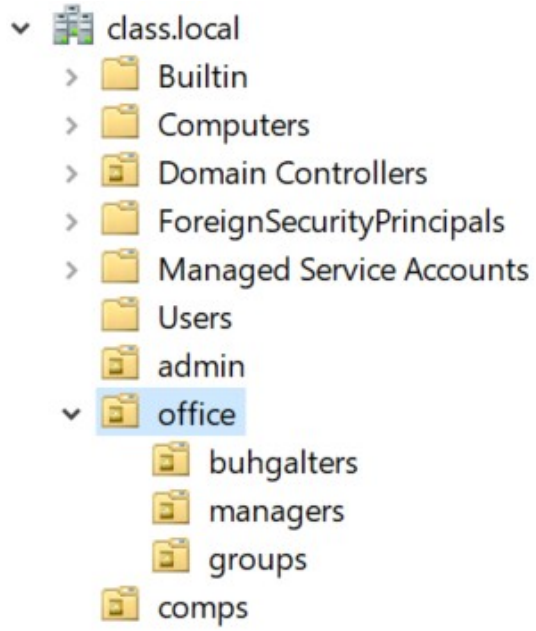

Рисунок 12 — Полученная структура подразделений

После этого была активирована корзина для удаленных объектов Active Directory. Это показано на рисунке 13.

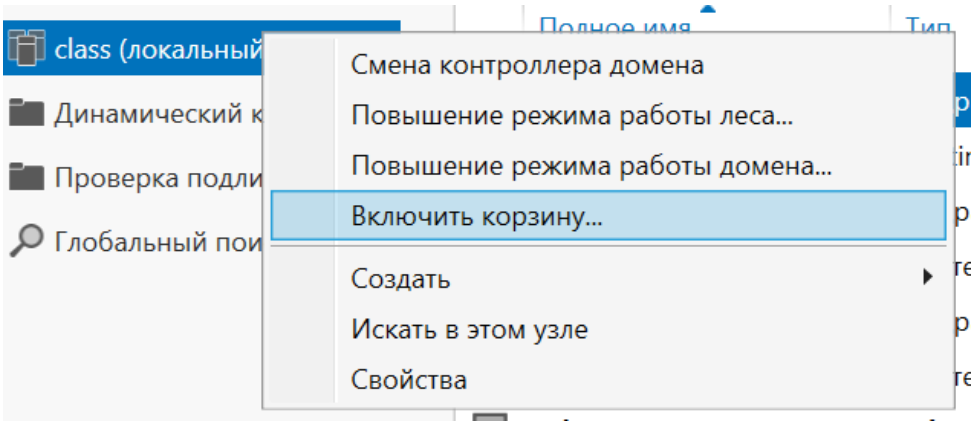

Рисунок 13 — Активация корзины для удаленных объектов AD

Затем были найдены учетные записи «bim» и «bom», созданные в предыдущих лабораторных работах. Они находились в контейнере «Users», т. к. это контейнер по умолчанию, в который помещаются новые учетные записи и группы. Это видно на рисунке 14. После этого старые пользователи были удалены.

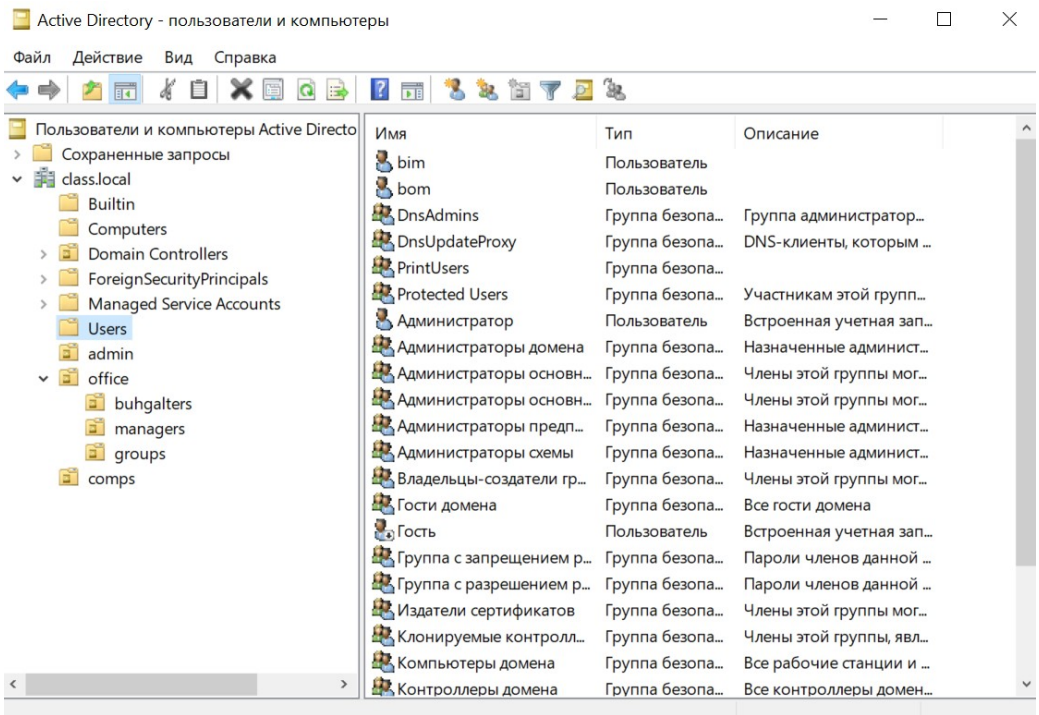

Рисунок 14 — Пользователи «bim» и «bom» в Active Directory

Упражнение 2. Присоединение компьютера к домену

В данном упражнении необходимо присоединить вторую виртуальную машину к домену. Для этого в качестве DNS-сервера был указан IP-адрес виртуальной машины v1. Также в диспетчере серверов в окне изменения имени компьютера был указан домен «class.local». Для проверки подключения виртуальной машины v2 к домену был выполнен вход в учетную запись «class/администратор». Вход был выполнен успешно, т. к. до этого виртуальная машина v2 была подключена к домену. Эти действия показаны на рисунках 15-17.

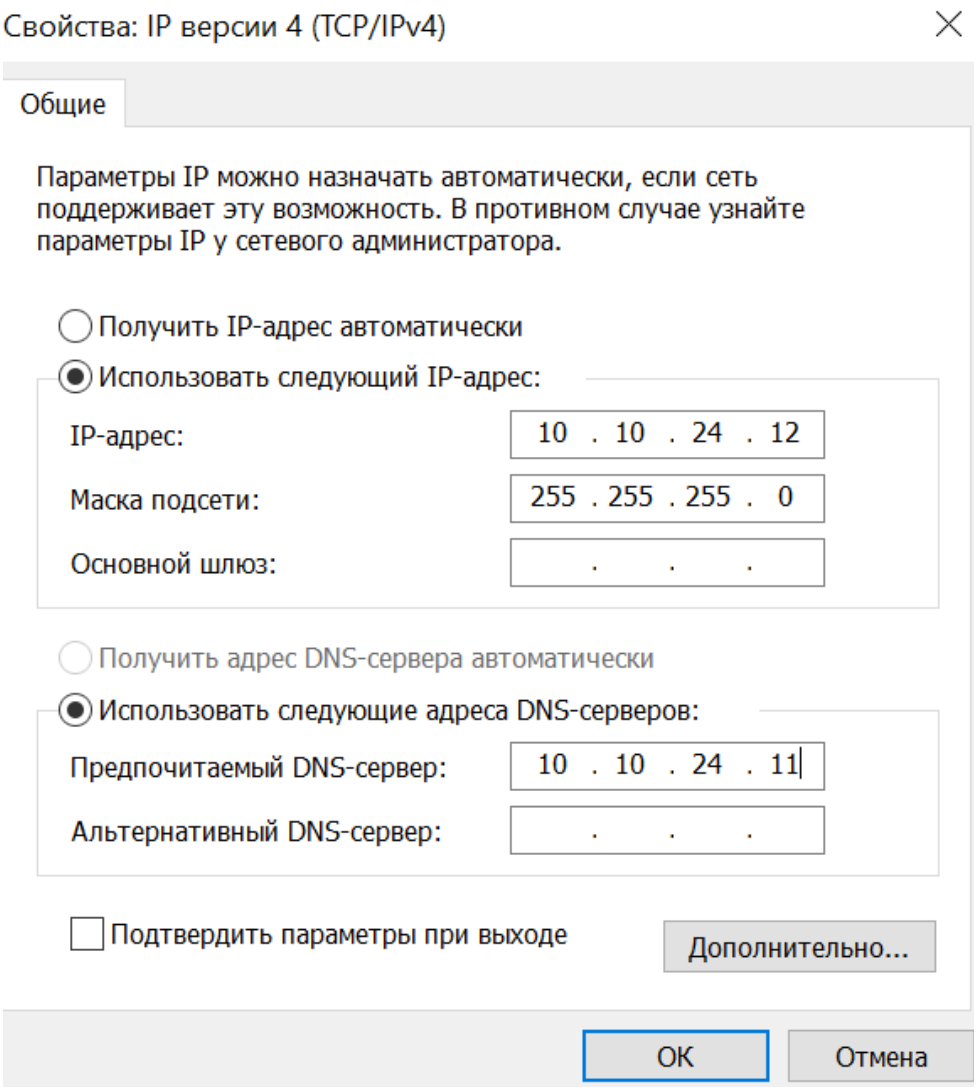

Рисунок 15 — Использование адреса виртуальной машины v1 в качестве DNS-сервера на виртуальной машине v2

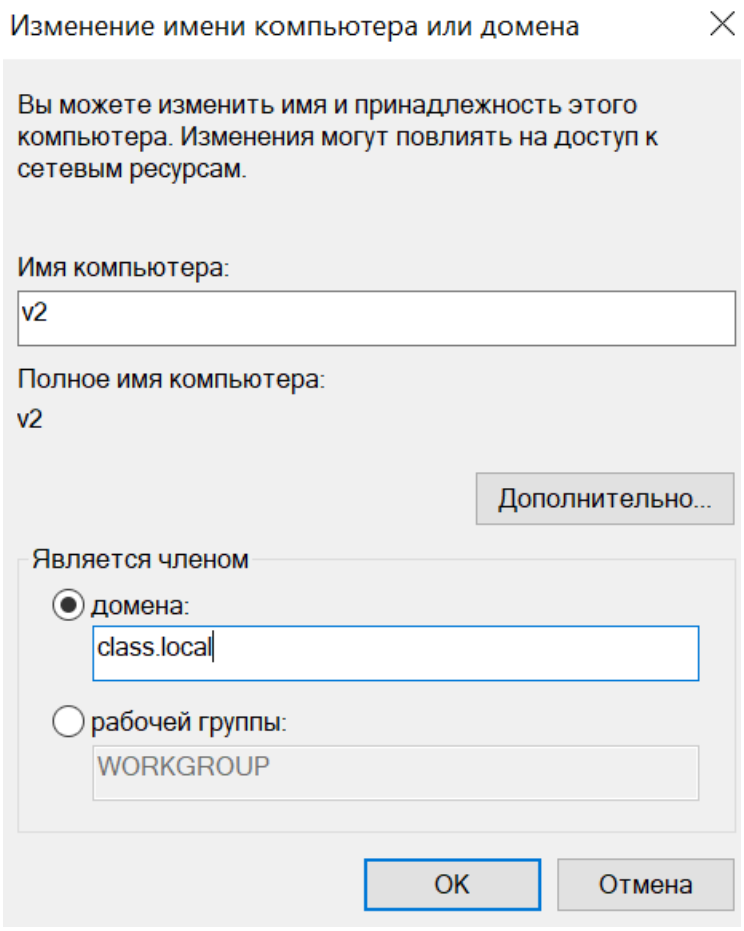

Рисунок 16 — Присоединение виртуальной машины v2 к домену «class.local»

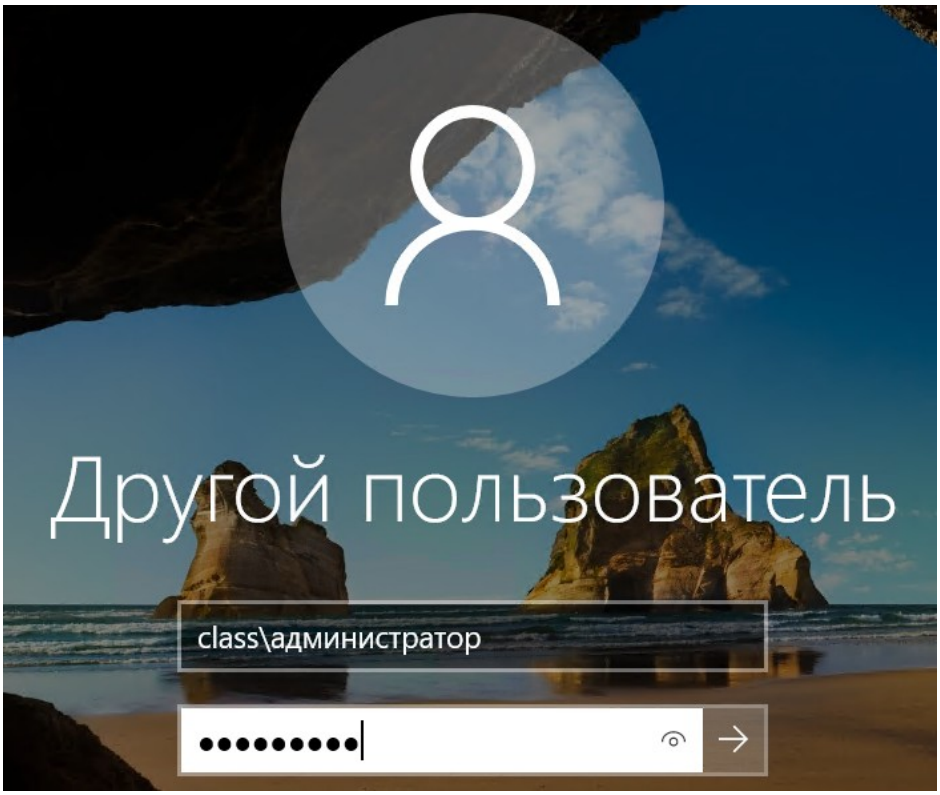

Рисунок 17 — Вход под учетной записью «class\администратор»

Упражнение 3. Перемещение учетной записи компьютера домена

В этом упражнении учетная запись компьютера «V2» была перемещена из контейнера «Computers» в подразделение «comps». Для этого сущность «компьютер» была перенесена с помощью перетягивания с одного места в другое. Это показано на рисунках 18-19.

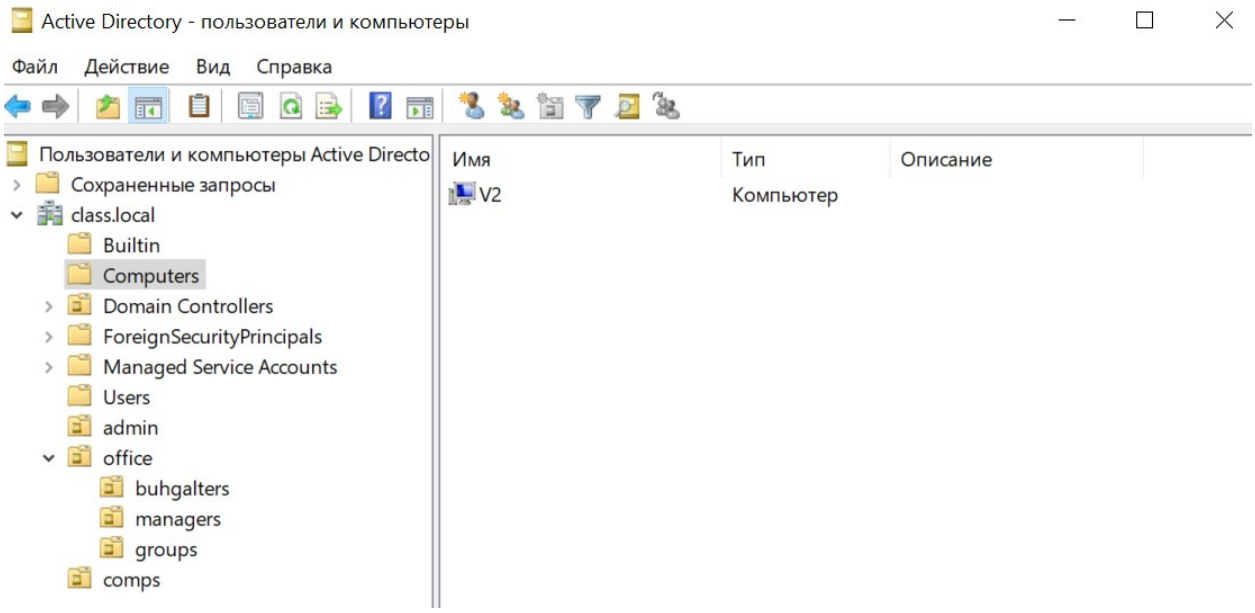

Рисунок 18 — Содержимое контейнера «Computers» в Active Directory

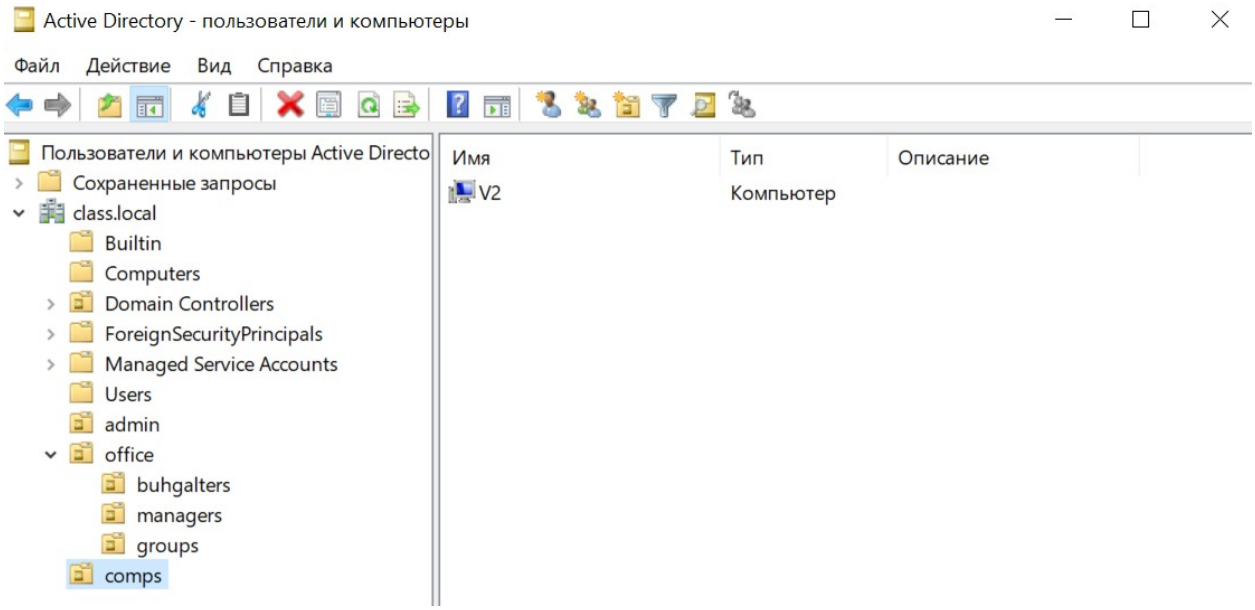

Рисунок 19 — Перемещение компьютера «V2» в подразделение «comps»

Упражнение 4. Создание и управление учетными записями пользователей домена

В данном упражнении необходимо создать учетные записи с помощью утилиты LDIFDE. Для этого был создан файл «c:\work\users.txt», в котором были описаны LDIF-записи для создания двух пользователей в ОП «admin», четверых пользователей в ОП «managers» и четверых пользователей в ОП «buhgalters» в соответствии с заданием. Эти LDIF-записи показаны на рисунках 20-22.

```
dn: cn=adm,ou=admin,dc=class,dc=local
changeType: add
objectClass: user
sAMAccountName: adm
userAccountControl: 2

dn: cn=helper,ou=admin,dc=class,dc=local
changeType: add
objectClass: user
sAMAccountName: helper
userAccountControl: 2
```

Рисунок 20 — Описание двух пользователей в ОП «admin» в формате LDIF

```
dn: cn=mmm,ou=managers,ou=office,dc=class,dc=local
changeType: add
objectClass: user
sAMAccountName: mmm
userAccountControl: 2
givenName: Мороз
sn: Морозов

dn: cn=mmm2,ou=managers,ou=office,dc=class,dc=local
changeType: add
objectClass: user
sAMAccountName: mmm2
userAccountControl: 2

dn: cn=mmm3,ou=managers,ou=office,dc=class,dc=local
changeType: add
objectClass: user
sAMAccountName: mmm3
userAccountControl: 2

dn: cn=mmm4,ou=managers,ou=office,dc=class,dc=local
changeType: add
objectClass: user
sAMAccountName: mmm4
userAccountControl: 2
```

Рисунок 21 — Описание четырех пользователей в ОП «managers» в формате LDIF

```
dn: cn=kkk,ou=buhgalters,ou=office,dc=class,dc=local
changeType: add
objectClass: user
sAMAccountName: kkk
userAccountControl: 2
givenName: Кащей
sn: Кащеев

dn: cn=kkk2,ou=buhgalters,ou=office,dc=class,dc=local
changeType: add
objectClass: user
sAMAccountName: kkk2
userAccountControl: 2

dn: cn=kkk3,ou=buhgalters,ou=office,dc=class,dc=local
changeType: add
objectClass: user
sAMAccountName: kkk3
userAccountControl: 2

dn: cn=kkk4,ou=buhgalters,ou=office,dc=class,dc=local
changeType: add
objectClass: user
sAMAccountName: kkk4
userAccountControl: 2
```

Рисунок 22 — Описание четырех пользователей в ОП «buhgalters» в формате LDIF

После этого был изучен синтаксис утилиты ldifde. Затем утилита была запущена с ключами «-i -f c:\work\users.txt». После запуска утилиты все пользователи были успешно созданы. Этот процесс показан на рисунках 23-25.

```
C:\Users\Администратор>ldifde /?
Неизвестный параметр

Обмен каталогов LDIF

Общие параметры
==================
-i                Включение режима импорта (по умолчанию режим экспорта)
-f имя_файла       Имя входного или выходного файла.
-s имя_сервера     Сервер для связи (по умолчанию контроллер домена компьютера)
-c FromDN ToDN  Замена вхождений FromDN на ToDN
                  Если FromDN или ToDN заканчивается атрибутом #имя_атрибута,
                  будет выполнен поиск значения атрибута в rootDSE,
                  и оно будет использовано для замещения элемента #имя_атрибута. Пример для "Макрорасширение
               в DN".
-v              Включение подробного режима
-j путь         Расположение файла журнала
-t порт         Номер порта (по умолчанию 389)
-u              Использование Юникода
-w время_ожидания      Прекращение выполнения, если сервер не отвечает
               на операцию в течение указанного времени
               (по умолчанию время ожидания не задано)
-h              Включение подписывания и шифрования уровня SASL
-?              Справка
```

Рисунок 23 — Синтаксис утилиты ldifde

```
C:\Users\Администратор>ldifde -i -f c:\work\users.txt
Подключение к "v1.class.local"
Вход от имени текущего пользователя с помощью SSPI
Импортирование каталога из файла "c:\work\users.txt"
Загружаются элементы.....
10 элементов успешно изменено.

Команда успешно выполнена
```

Рисунок 24 — Результат запуска команды «ldifde -i -f c:\work\users.txt»

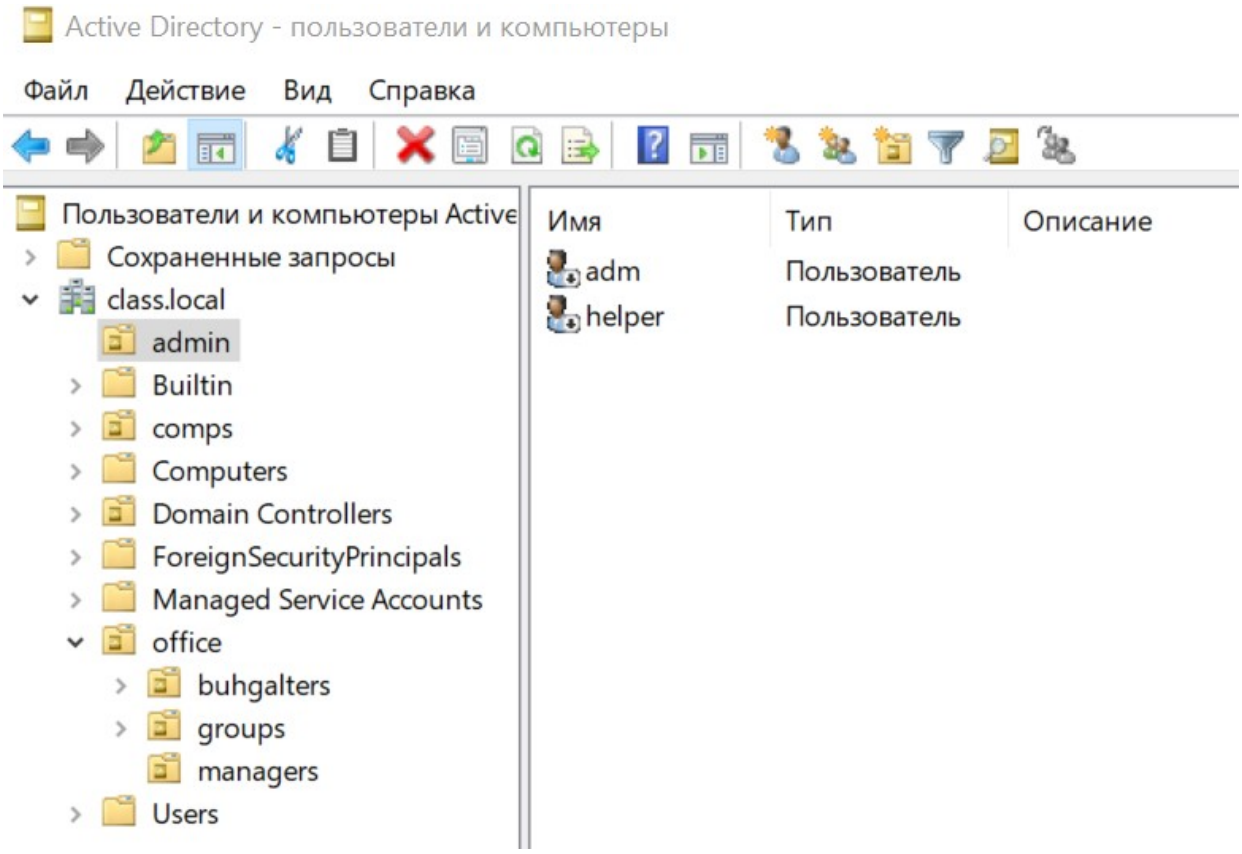

Рисунок 25 — Созданные пользователи в Active Directory

Затем для всех учетных записей был установлен пароль «Pa$$w0rd», а также были включены учетные записи «adm», «mmm» и «kkk». Это показано на рисунках 26-27.

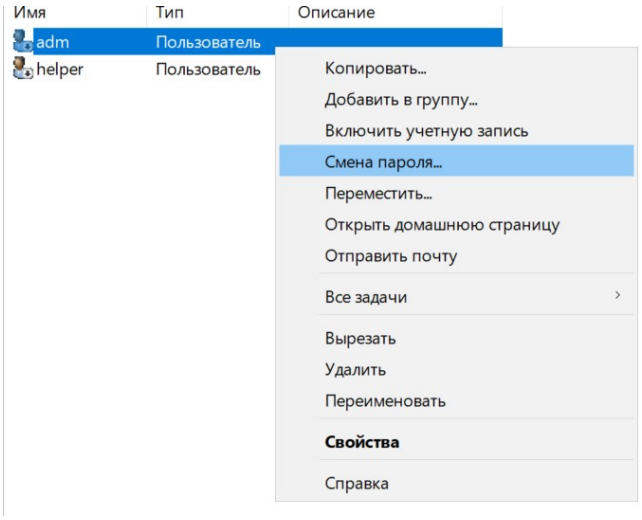

Рисунок 26 — Изменение пароля учетных записей

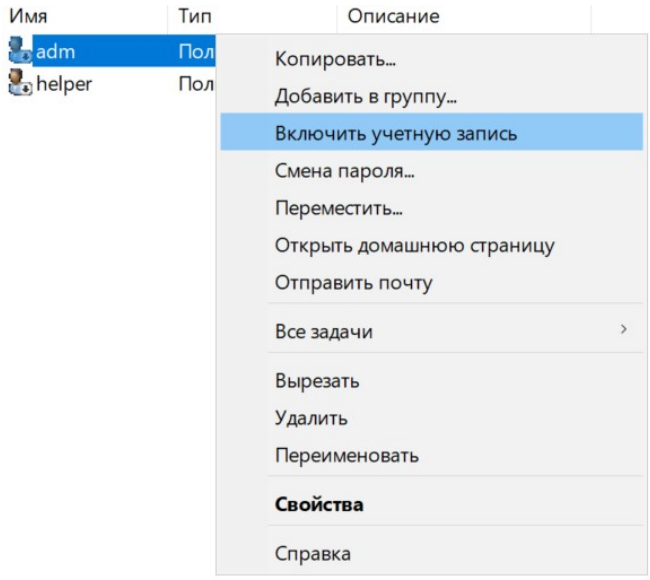

Рисунок 27 — Включение учетных записей

После этого учетная запись «adm» была добавлена в группу «Администраторы домена». Для учетной записи «Мороз Морозов» был указан номер телефона «123-45-67», установлено время входа «четверг с 8 до 12», подключена домашняя папка «\\v1\docs\%username%», установлена должность «Ведущий менеджер», выбран руководитель «adm», установлено ограничение активного сеанса «2 минуты», установлен флажок «Защитить объект от случайного удаления». Эти действия показаны на рисунках 28-35.

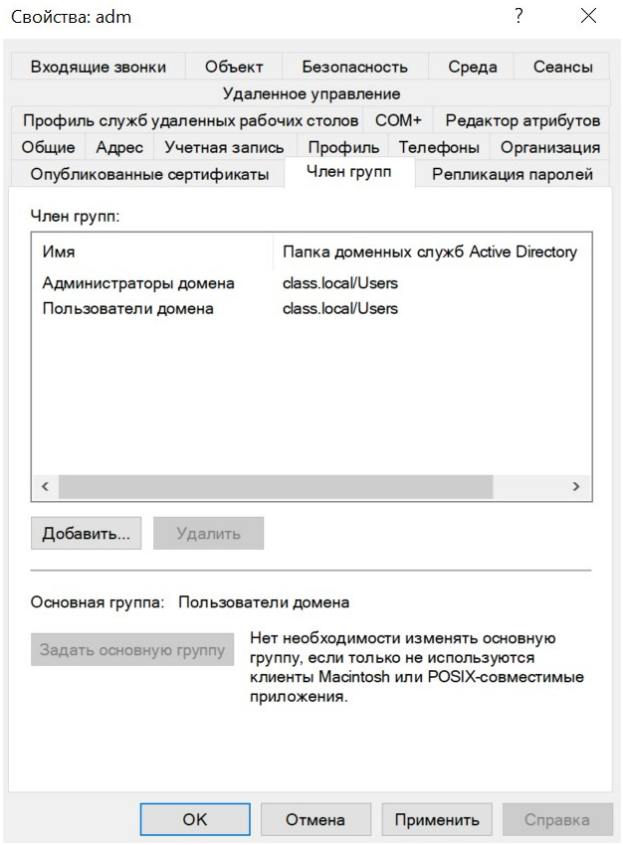

Рисунок 28 — Добавление учетной записи «adm» в группу «Администраторы домена»

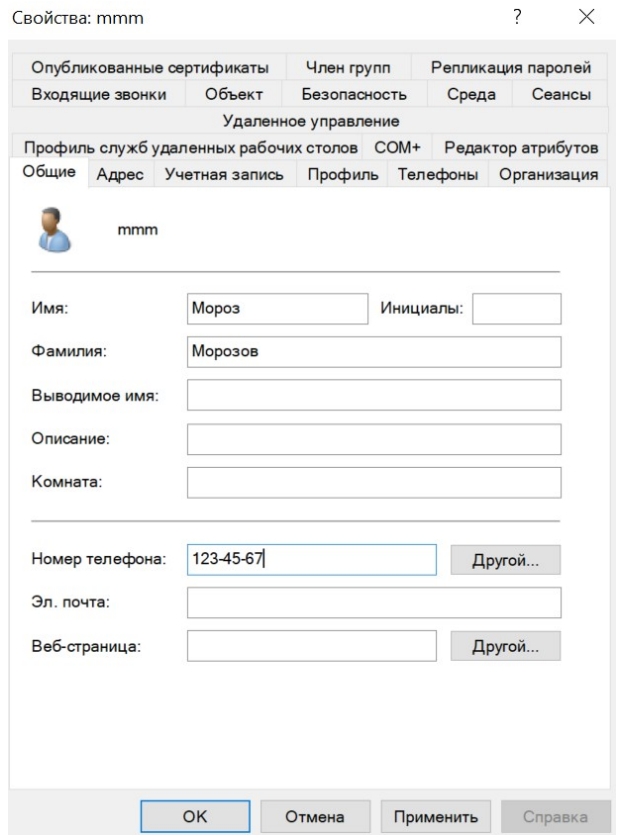

Рисунок 29 — Добавление номера телефона в учетную запись «mmm»

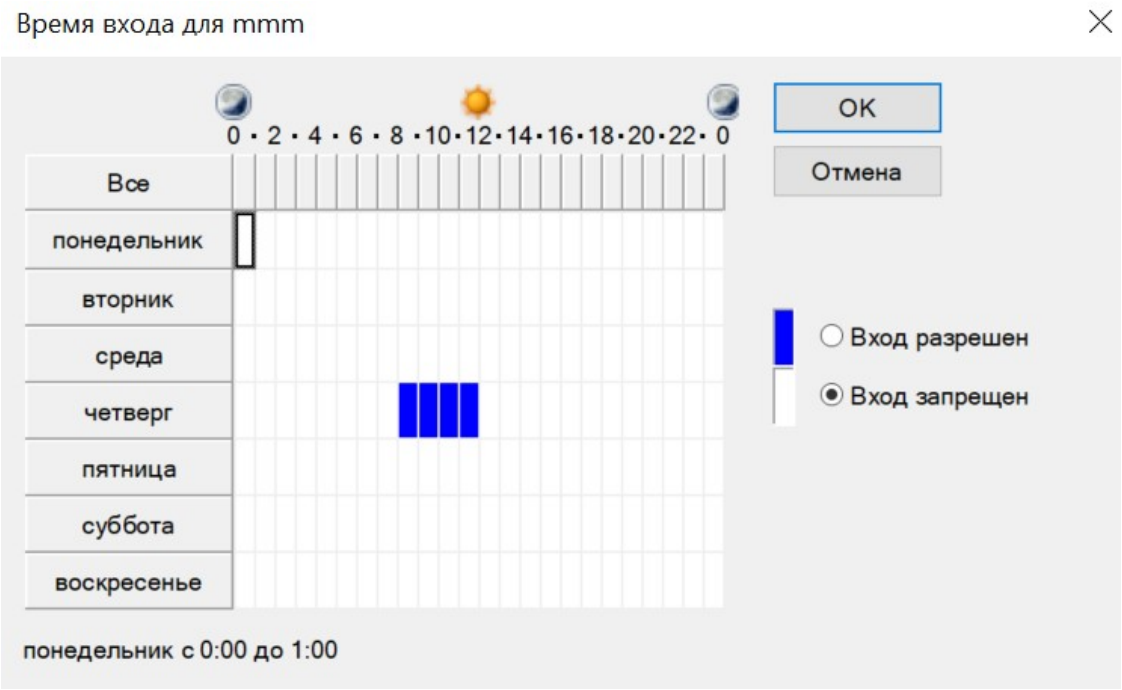

Рисунок 30 — Настройка времени входа для учетной записи «mmm»

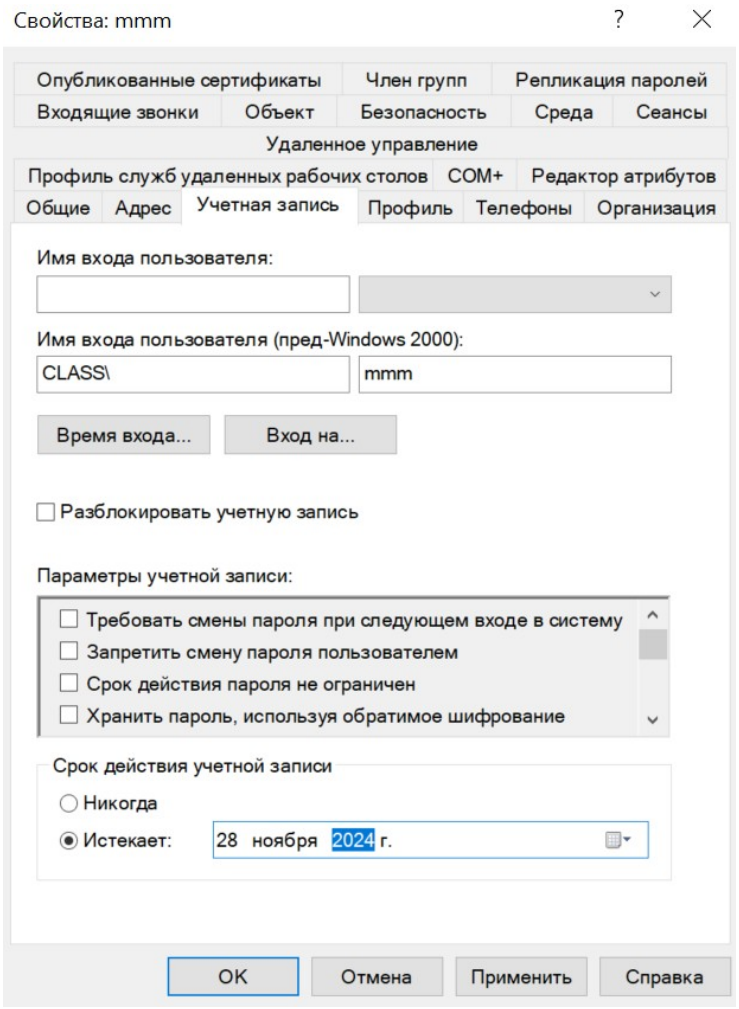

Рисунок 31 — Настройка срока действия учетной записи «mmm»

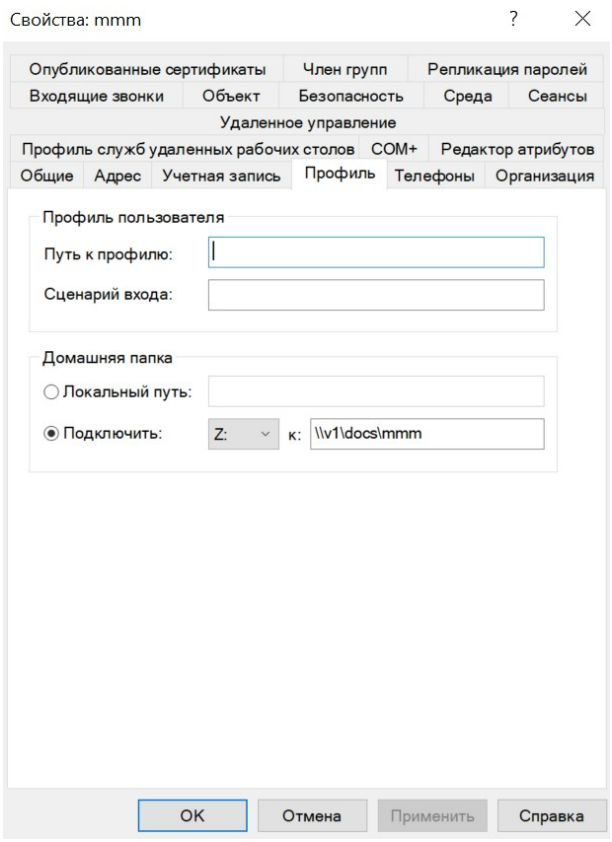

Рисунок 32 — Настройка домашней папки учетной записи «mmm»

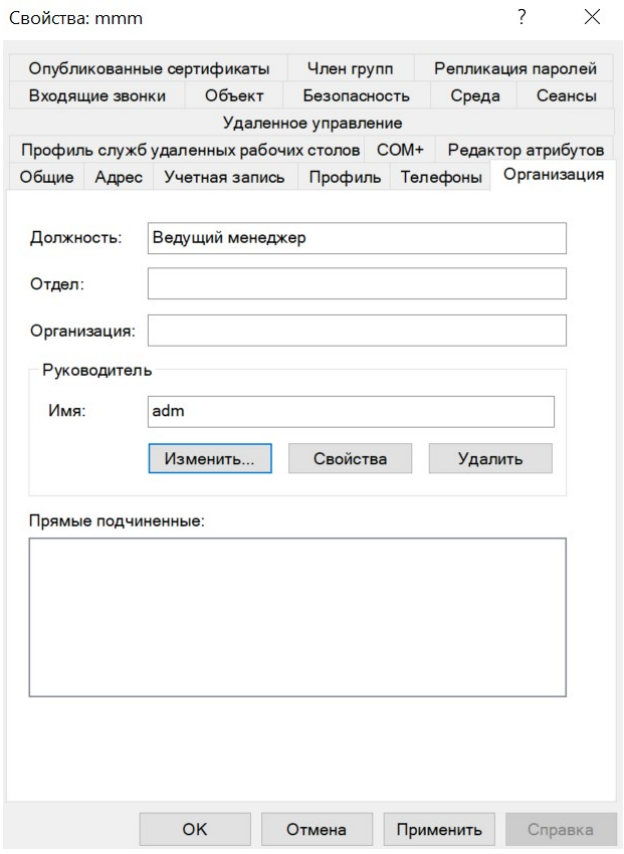

Рисунок 33 — Настройка должности и руководителя учетной записи «mmm»

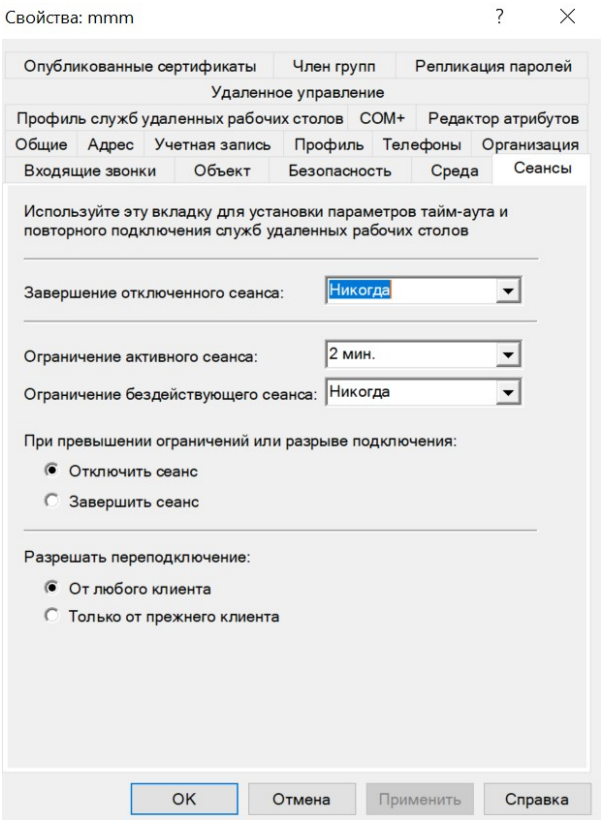

Рисунок 34 — Настройка ограничения активного сеанса учетной записи «mmm»

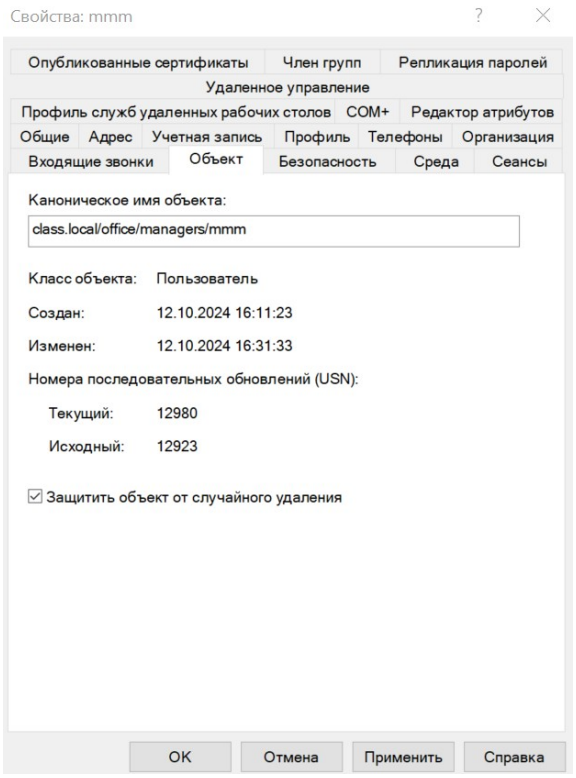

Рисунок 35 — Настройка защиты от случайного удаления учетной записи «mmm»

Затем в ОП «managers» было вызвано окно свойств для всех учетных записей. При этом была открыта одна вкладка, позволяющая задать какие-то общие свойства, например, должность, описание, адрес и т. п. После этого для выбранных учетных записей было установлено время входа «четверг с 9 до 15, суббота с 10 до 15», а также должность «Менеджер». Этот процесс показан на рисунках 36-39.

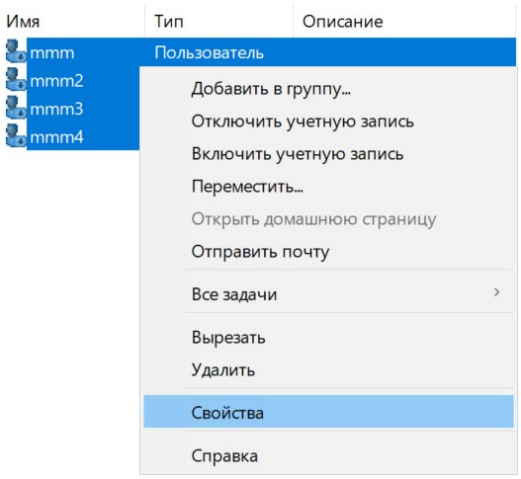

Рисунок 36 — Меню выбора настройки свойств для нескольких учетных записей

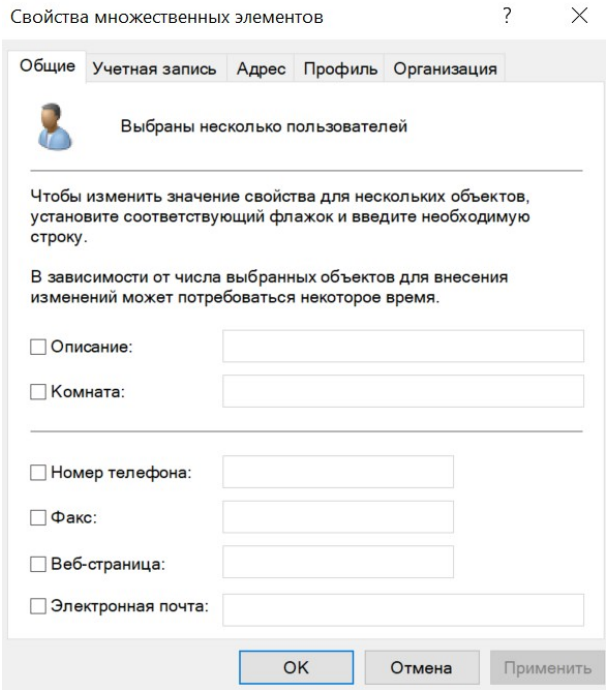

Рисунок 37 — Настройка свойств для нескольких учетных записей

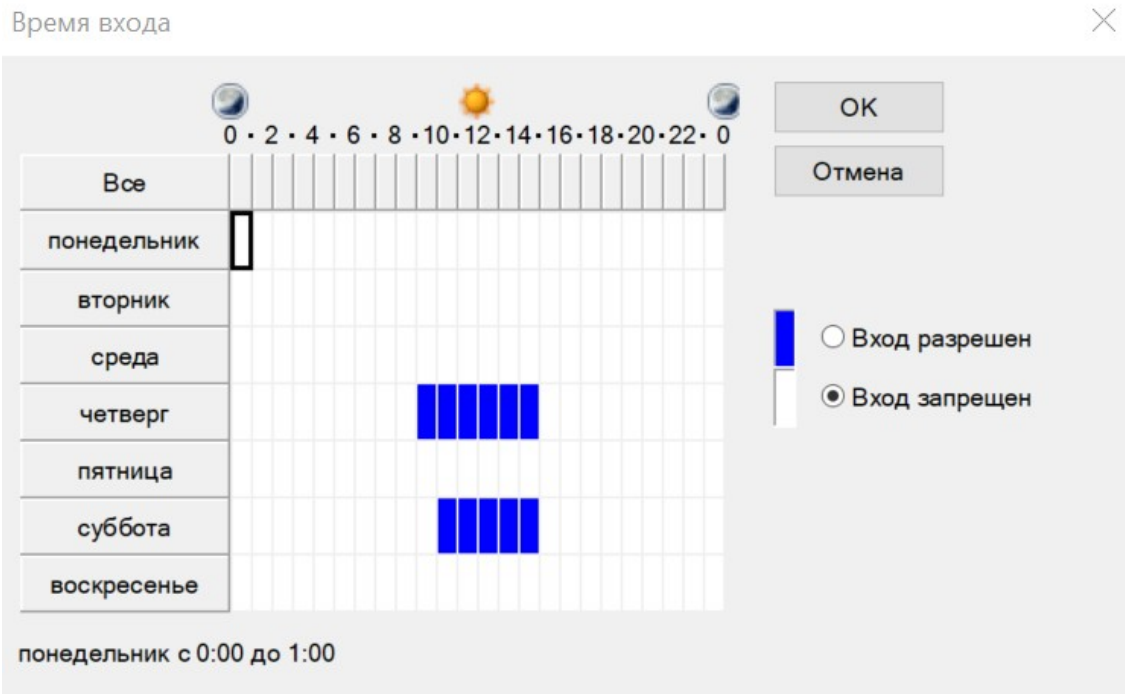

Рисунок 38 — Настройка времени входа для учетных записей из ОП «managers»

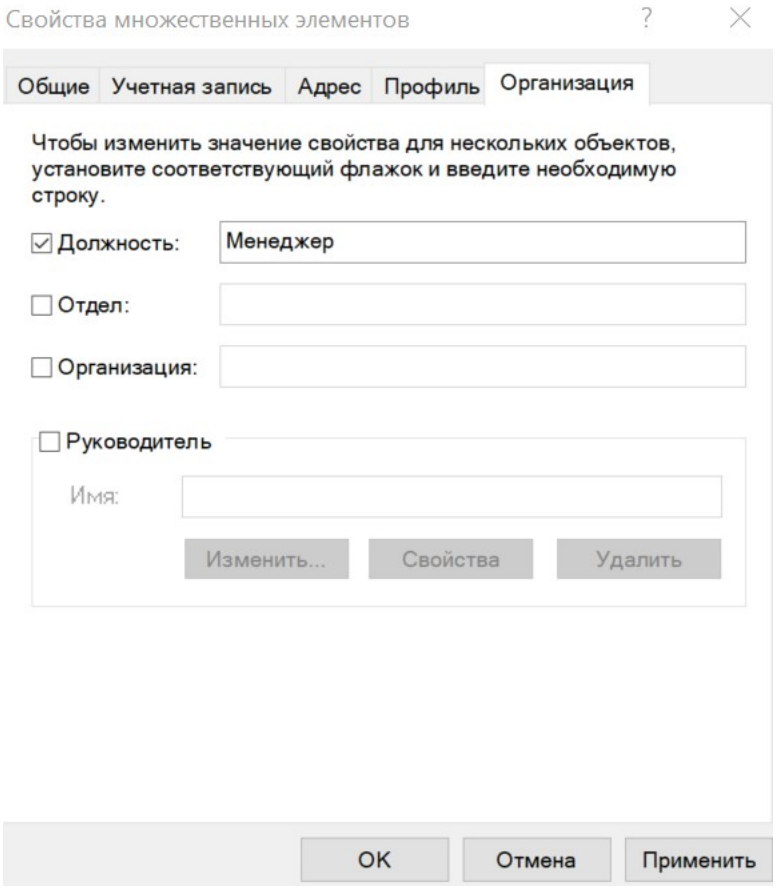

Рисунок 39 — Настройка должности для учетных записей из ОП «managers»

Похожие действия были сделаны для пользователей ОП «buhgalters»: было указано время входа «четверг с 10 до 15», а также установлена должность «Бухгалтер». Это продемонстрировано на рисунках 40-41.

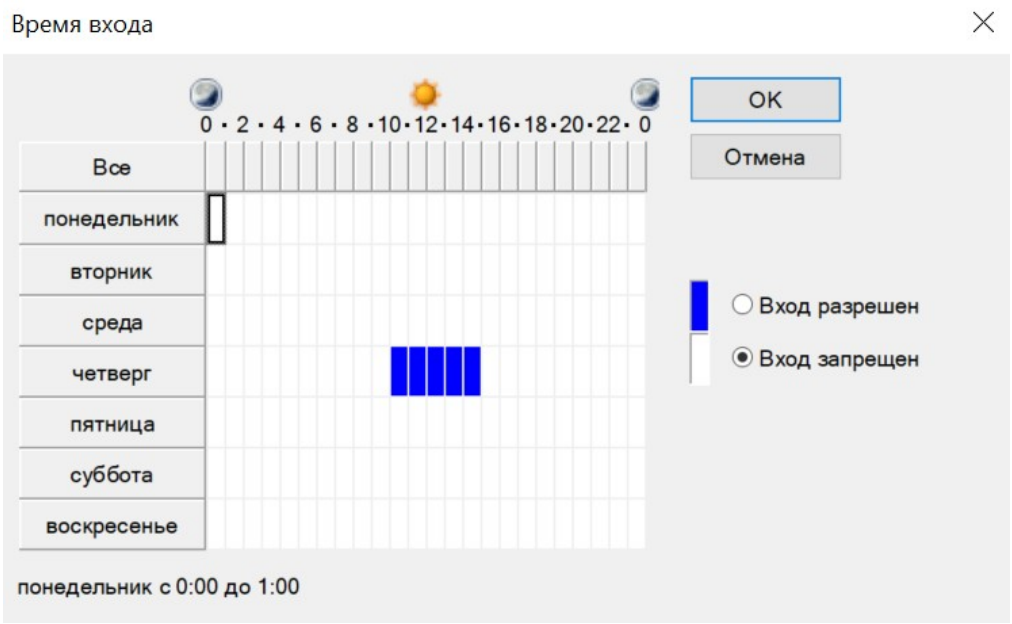

Рисунок 40 — Настройка времени входа для учетных записей из ОП «buhgalters»

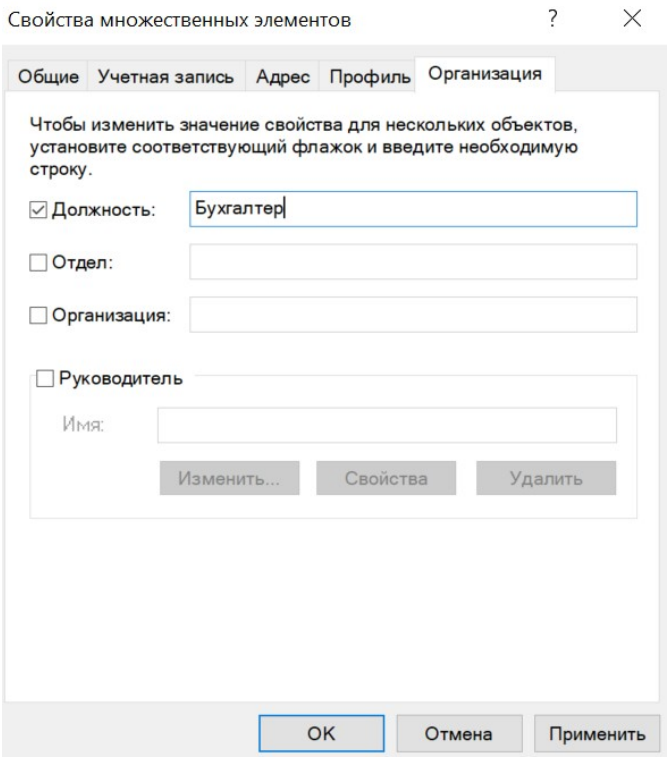

Рисунок 41 — Настройка должности для учетных записей из ОП «buhgalters»

После этого была протестирована возможность удаления учетной записи «mmm». При попытке удаления произошла ошибка, показанная на рисунке 42.

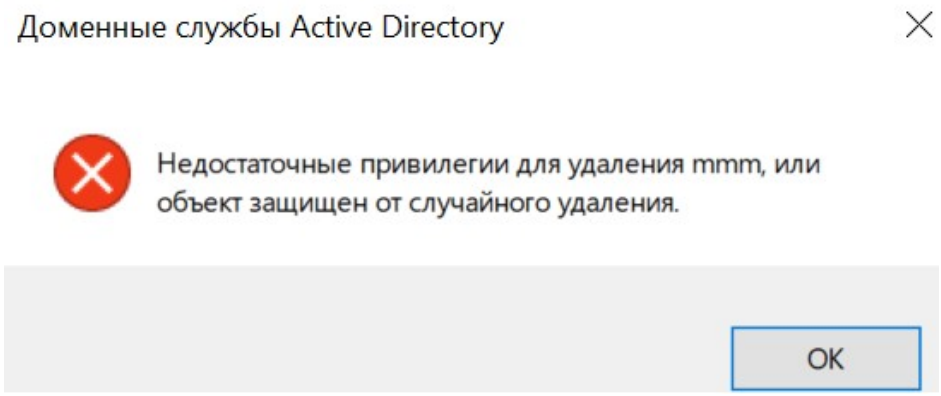

Рисунок 42 — Ошибка при удалении учетной записи «mmm»

Она произошла из-за того, что ранее для учетной записи «mmm» была включена защита от случайного удаления. Если попытаться удалить другую учетную запись без защиты от случайного удаления, например, учетную запись «kkk», то удаление произойдет успешно.

Упражнение 5. Создание и управление группами домена

В этом упражнении необходимо было создать группы домена. Для этого был изучен синтаксис утилиты «dsadd group». Затем, с помощью этой же утилиты были созданы следующие группы:

— глобальные группы домена «jAdmin_g», «jManagers_g», «jBuhgalters_g»;

— локальные группы домена «flDocsM_dl», «termV2_dl».

Синтаксис, команды для создания вышеперечисленных групп, а также результат выполнения команд в Active Directory продемонстрированы на рисунках 43-45.

```
C:\Users\adm>dsadd group /?
Описание:  добавление группы в каталог.

Синтаксис:  dsadd group <DN_группы> [-secgrp {yes | no}] [-scope {l | g | u}]
       [-samid <имя_SAM>] [-desc <описание>] [-memberof <группа ...>]
       [-members <член ...>] [{-s <сервер> | -d <домен>}] [-u <пользователь>]
       [-p {<пароль> | *}] [-q] [{-uc | -uco | -uci}]

Параметры:

Значение                Описание
<DN_группы>             Обязательный параметр. Различающееся имя (DN)
                        добавляемой группы.
                        Если конечный объект не задан, он будет взят
                        из стандартного ввода (STDIN).
-secgrp {yes | no}      Указывает, что группа является (yes) или не является
                       (no) группой безопасности. По умолчанию: yes.
-scope {l | g | u}      Указывает, что область действия группы является:
                        локальной (l), глобальной (g) или универсальной (u).
                        Для доменов со смешанным режимом универсальная область
                        действия не поддерживается. По умолчанию: global.
-samid <имя_SAM>        Задает имя SAM учетной записи группы <имя_SAM>
                        (например, операторы).
-desc <описание>        Задает описание группы <описание>.
-memberof <группа ...>  Добавляет группу в одну или несколько групп,
                        определяемых разделяемым пробелами списком
                        имен DN <группа ...>.
-members <член ...>     Добавляет одного или нескольких членов в эту группу.
                        Члены определяются разделяемым пробелами списком
                        имен DN <член ...>.
```

Рисунок 43 — Синтаксис команды «dsadd group»

```
C:\Windows\system32>dsadd group cn=jAdmin_g,ou=groups,ou=office,dc=class,dc=local -scope g
dsadd Успешно:cn=jAdmin_g,ou=groups,ou=office,dc=class,dc=local

C:\Windows\system32>dsadd group cn=jManagers_g,ou=groups,ou=office,dc=class,dc=local -scope g
dsadd Успешно:cn=jManagers_g,ou=groups,ou=office,dc=class,dc=local

C:\Windows\system32>dsadd group cn=jBuhgalters_g,ou=groups,ou=office,dc=class,dc=local -scope g
dsadd Успешно:cn=jBuhgalters_g,ou=groups,ou=office,dc=class,dc=local

C:\Windows\system32>dsadd group cn=flDocsM_dl,ou=groups,ou=office,dc=class,dc=local -scope l
dsadd Успешно:cn=flDocsM_dl,ou=groups,ou=office,dc=class,dc=local

C:\Windows\system32>dsadd group cn=termV2_dl,ou=groups,ou=office,dc=class,dc=local -scope l
dsadd Успешно:cn=termV2_dl,ou=groups,ou=office,dc=class,dc=local
```

Рисунок 44 — Создание глобальных и локальных групп домена

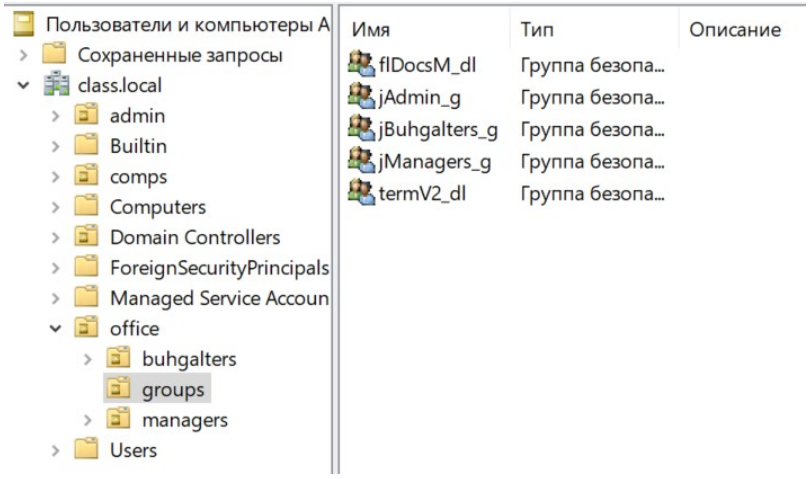

Рисунок 45 — Созданные группы в Active Directory

Затем все учетные записи менеджеров были добавлены в группу «jManagers_g», а учетные записи бухгалтеров — в группу «jBuhgalters_g». Также группа «jManagers_g» была добавлена членом групп «flDocsM_dl» и «termV2_dl». Затем учетные записи «adm» и «helper» были добавлены в группу «jAdmin_g», а группа «jAdmin_g» была добавлена членом встроенной группы «Администраторы домена». Эти действия показаны на рисунках 46-49.

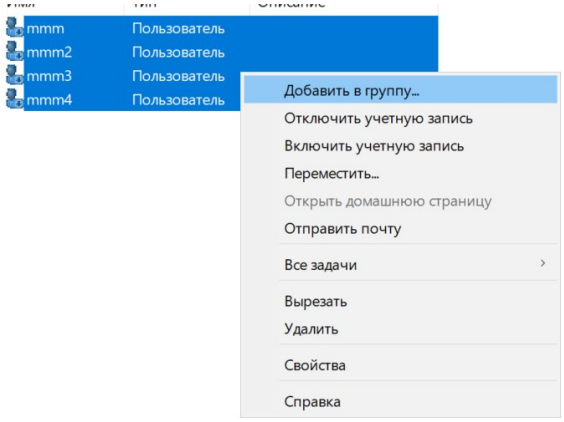

Рисунок 46 — Добавление учетных записей в группу

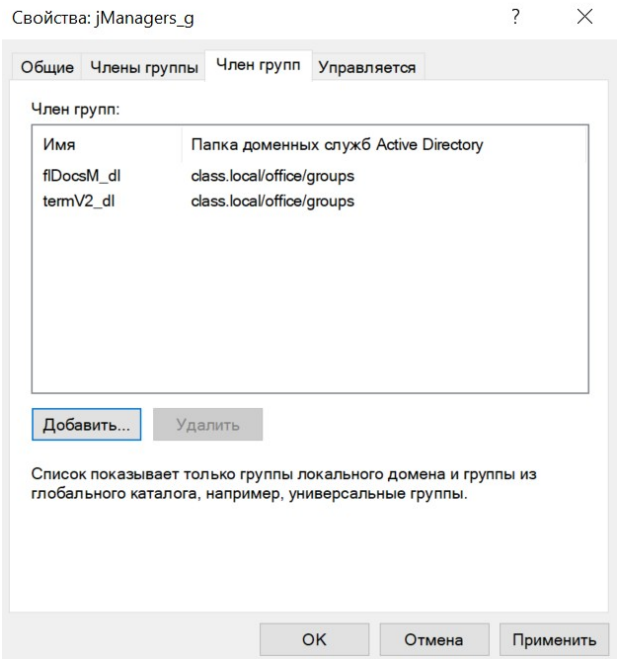

Рисунок 47 — Добавление группы «jManagers_g» членом групп «flDocsM_dl» и «termV2_dl»

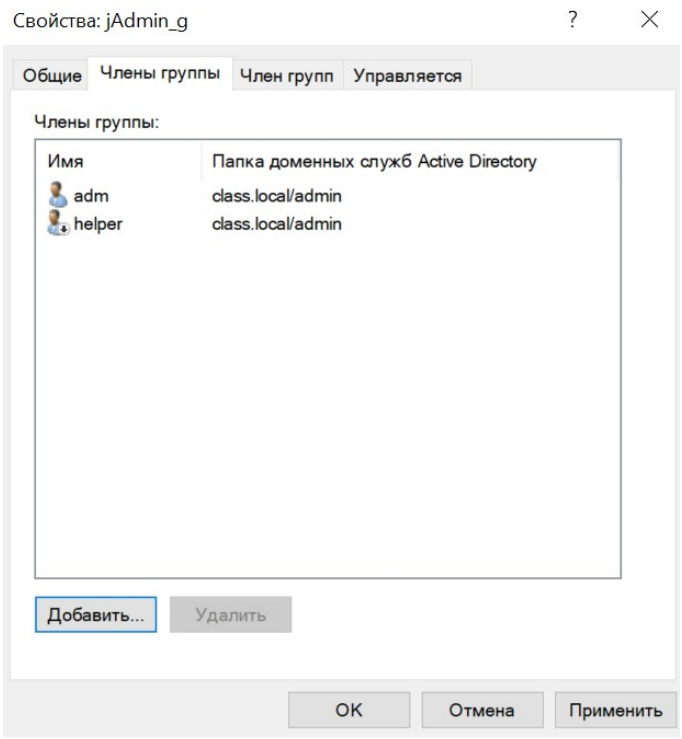

Рисунок 48 — Добавление учетных записей «adm» и «helper» в группу «jAdmin_g»

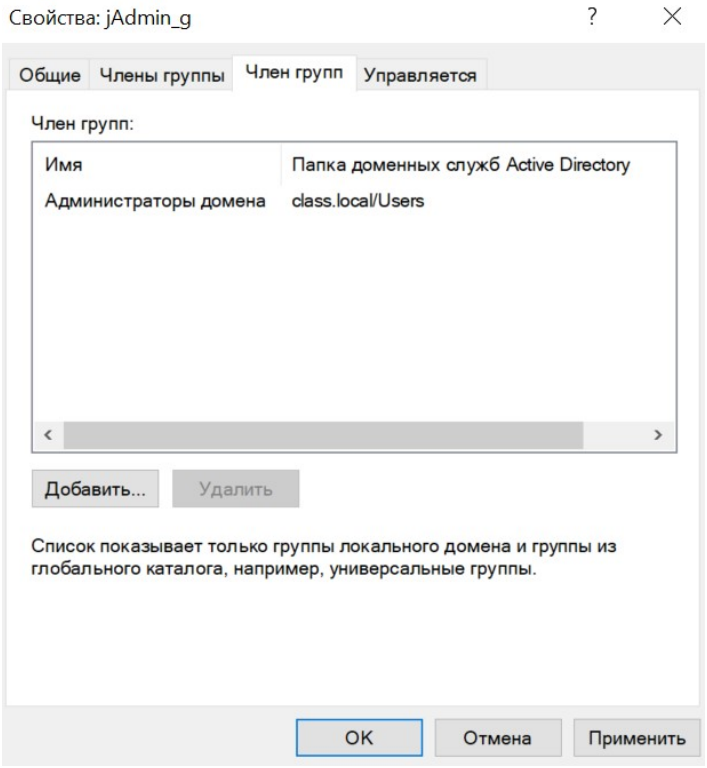

Рисунок 49 — Добавление группы «jAdmin_g» членом группы «Администраторы домена»

После этого были предоставлены разрешения на доступ к общим ресурсам папке Docs на виртуальной машине v1 и папке Public на виртуальной машине v2. Это показано на рисунках 50-51.

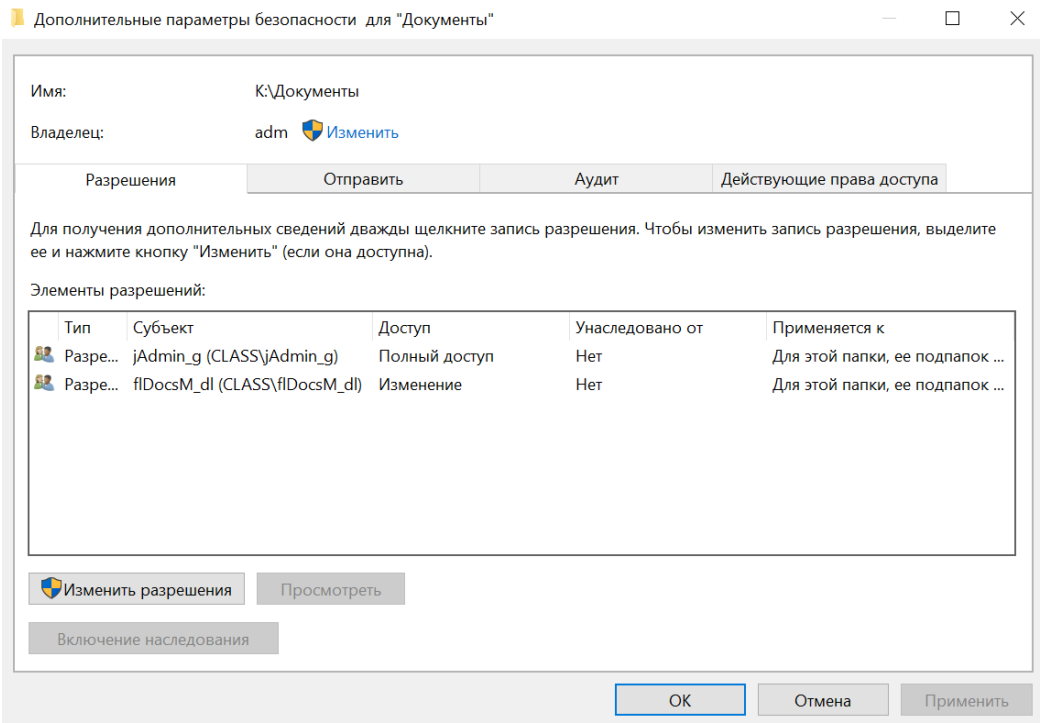

Рисунок 50 — Настройка доступа на виртуальной машине v1

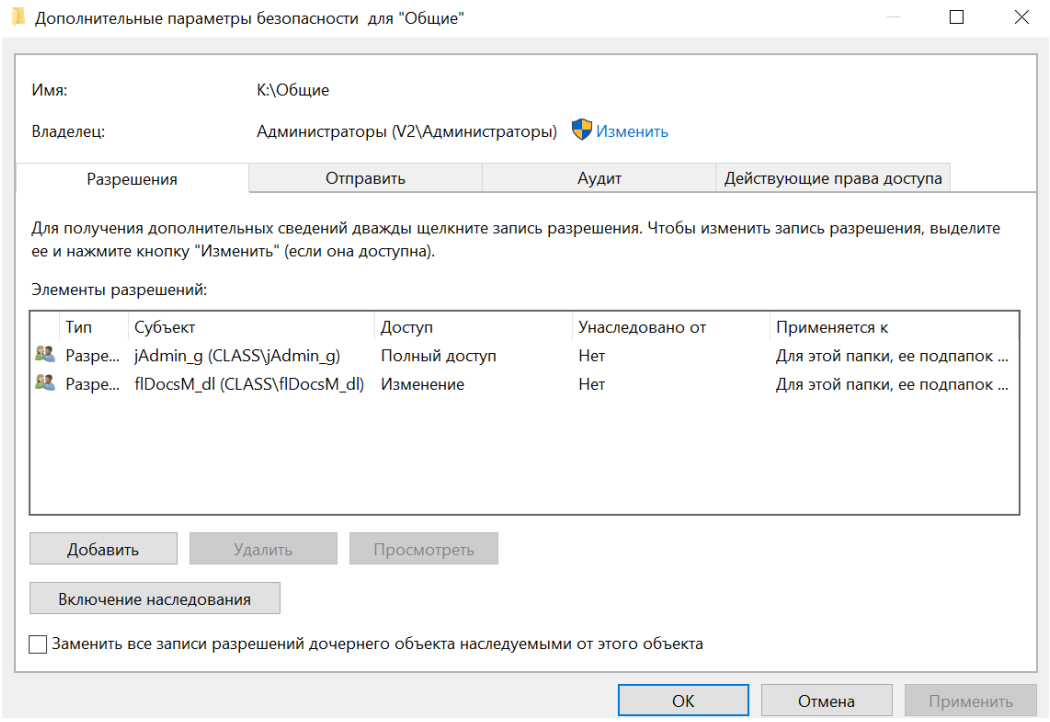

Рисунок 51 — Настройка доступа на виртуальной машине v2

После этого на виртуальной машине v2 в качестве пользователей удаленного рабочего стола была указана группа «termV2_dl», созданная ранее. Это показано на рисунке 52.

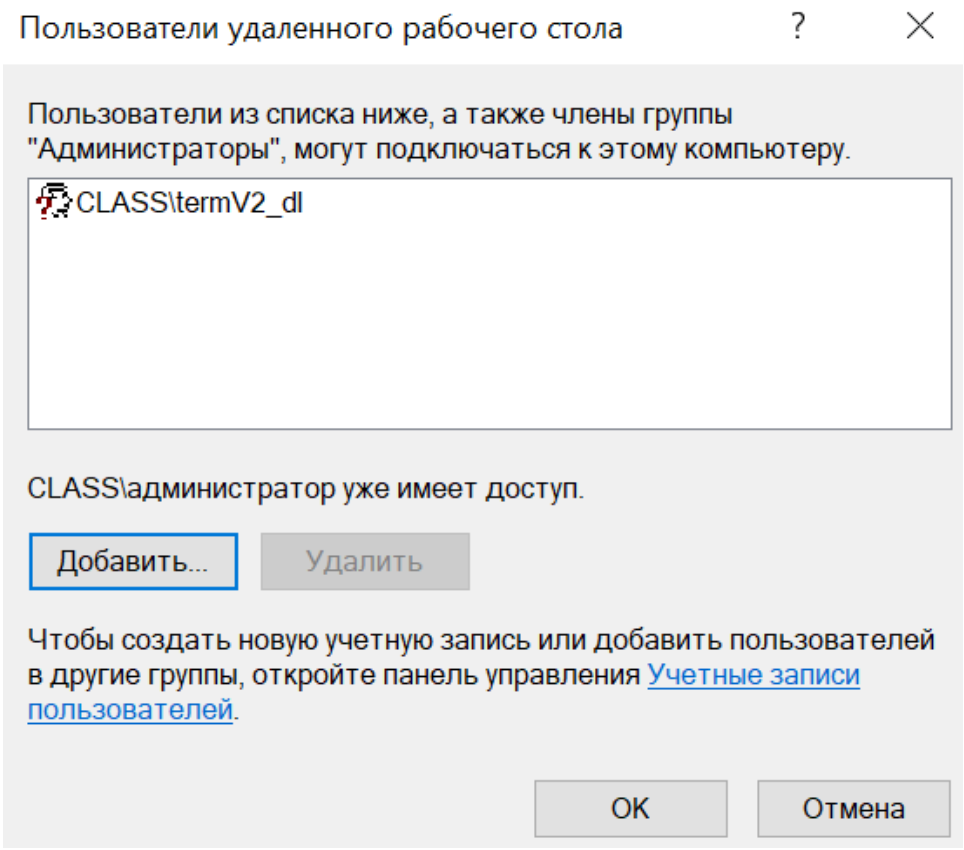

Рисунок 52 — Настройка пользователей удаленного рабочего стола

Затем на базовом сервере было запущено приложение подключения к удаленному рабочему столу. При попытке подключения под учетной записью «mmm» была выдана ошибка, показанная на рисунке 53.

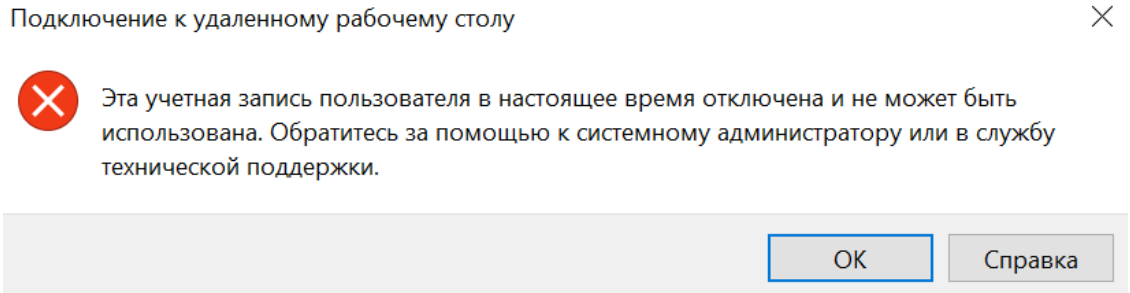

Рисунок 53 — Ошибка при подключении с помощью учетной записи «mmm»

Ошибка произошла, потому что ранее учетная запись «mmm» была отключена. Если включить учетную запись «mmm», то в случае входа во время, не соответствующее установленному ранее, будет выведена ошибка, показанная на рисунке 54.

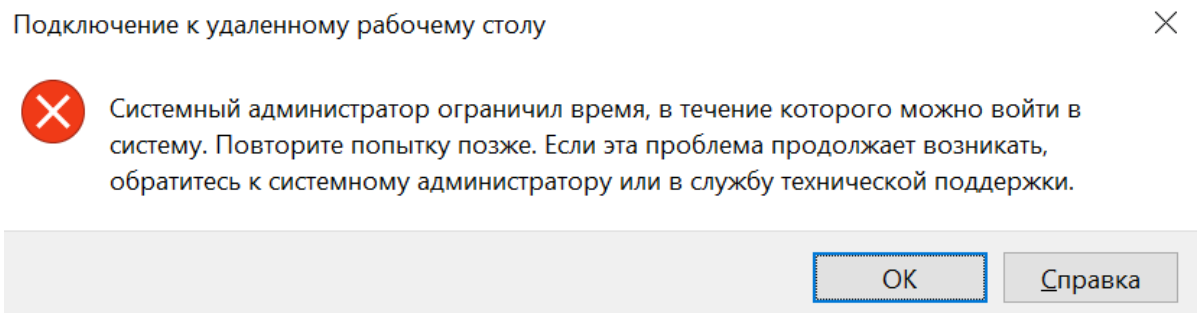

Рисунок 54 — Ошибка при подключении к учетной записи «mmm» в неподходящее время

Если попытаться войти во время, соответствующее ранее указанному в учетной записи, то вход будет успешно произведен.

3. Ответы на вопросы

1) Что такое протокол LDAP, для чего предназначен?

LDAP — это протокол доступа к каталогам, который позволяет получать и принимать через сеть данные из каталогов с иерархической структурой. LDAP может использоваться для чтения, записи, добавления новых данных или модификации существующих, а также для поиска данных.

2) Какие права должны быть у пользователя для добавления компьютера к домену?

Для добавления компьютера к домену у пользователя должны быть права администратора домена.

3) Для чего нужна учетная запись пользователя домена?

Учетные записи используются для:

— проверки подлинности пользователя с помощью уникальных учетных данных (т. е. с помощью имени пользователя и пароля);

— предоставления доступа к ресурсам на основе прав, выданных учетной записи;

— аудита действий, выполняемых пользователями.

4) Для чего предназначены организационные подразделения в AD?

Организационные подразделения предназначены для упрощения администрирования путем группировки объектов. Они позволяют создавать иерархическую структуру внутри домена, представляя собой объекты-контейнеры, которые могут содержать объекты службы каталогов (например, пользователи, группы и т. п.). Таким образом, владельцы подразделений могут создавать новые поддеревья и делегировать администрирование подразделений в этих поддеревьях.

5) Какого типа группы можно создать в домене?

Можно создать следующие типы групп:

— **группа безопасности** — используется для предоставления доступа к ресурсам;

— **группа распространения** — используется для создания групп почтовых рассылок.

6) Какая цель и задачи создания локальных групп домена (Domain Local)?

Локальные группы домена используются для управления разрешениями доступа к файлам, папкам и другим ресурсам только того домена, где группа была создана. Локальные группы нельзя использовать в других доменах. Также локальные группы могут входить в другие локальные группы, но не могут входить в глобальные группы домена.

7) Какая цель и задачи создания глобальных групп домена (Global)?

Глобальные группы домена используются для предоставления доступа к ресурсам другого домена. В эти группы можно добавить только учетные записи из того же домена, в котором создана группа. Глобальные группы могут входить в другие глобальные и локальные группы домена.

4. Вывод

В ходе выполнения данной лабораторной работы в виртуальной машине v1 был поднят домен class.local, созданы организационные подразделения, пользователи и группы, подключена виртуальная машина v2 к домену как клиентский компьютер, предоставлены разрешения на ресурсы с помощью доменных групп.