Настройка локальной сети с выделенным сервером Windows Server 2025

Инструкция Антона Севостьянова

Итак, добрый день! Меня зовут Севостьянов Антон.

В данной инструкции я расскажу, как настроить локальную сеть с выделенным сервером.

Вот какие темы нам предстоит изучить:

Ну что, не будем терять времени и приступим к изучению…

Загрузка оригинальных образов (Windows 7, 10, 11, 2025 Server)

Для начала работы нам потребуется скачать установочные образы операционных систем, с которыми мы будем работать.

А в частности, это образ Windows Server 2025, и образы для клиентских машин 7, 10 и 11, так как они на данный момент наиболее распространенные в корпоративных средах.

Но не стоит забывать, что версии клиентских операционных систем должны быть как минимум профессиональные. Так как, в обычных версиях для домашних пользователей отсутствует возможность подключения компьютера к домену и ряд других, не мало важных функций.

Скачать дистрибутив **Windows Server 2025** можно тут

Переходим в раздел Russian \ ISO download \ 64-bit edition \ Путь для сохранения ISO образа

Скачать дистрибутив **Windows 11** можно тут

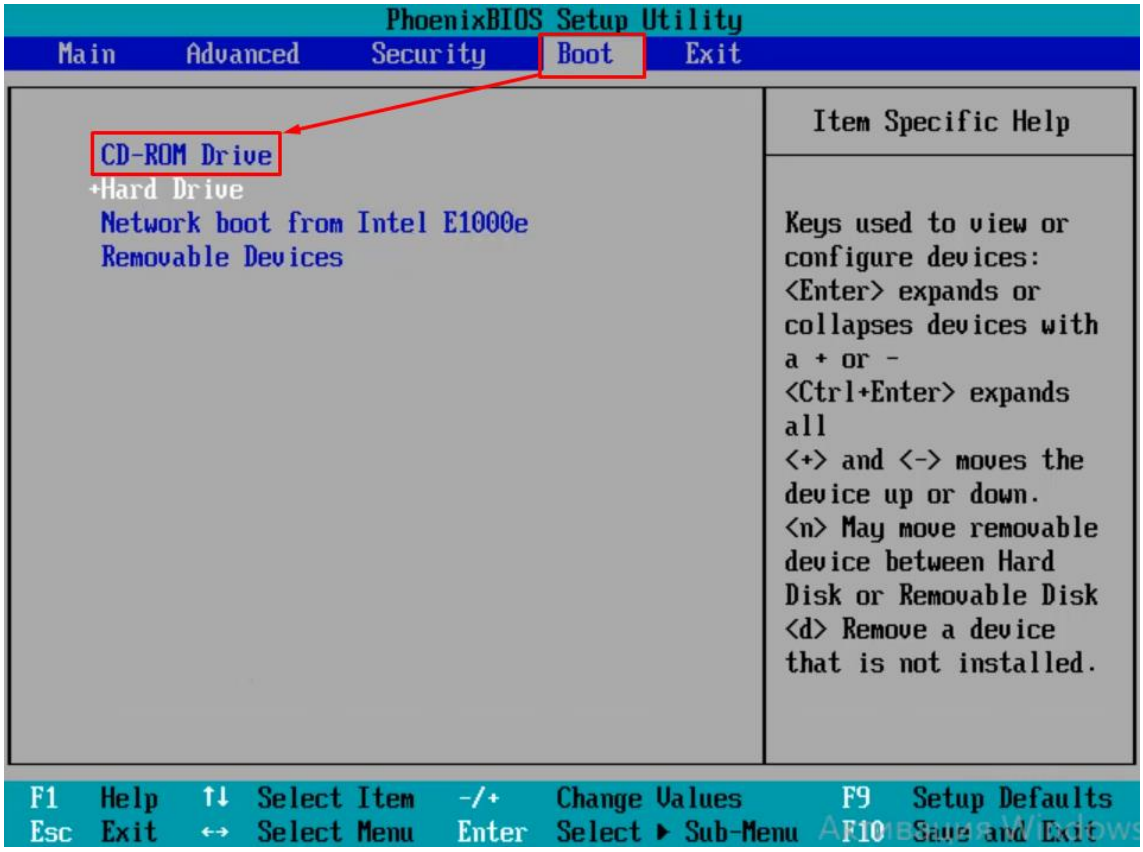
Скачать дистрибутив **Windows 10** можно тут

А вот **Windows 7** уже скачать с официального сайта не получится, так как Microsoft активно продвигает свои новые продукты и уже не дает скачивать мою любимую 7. Поэтому 7 вам придется искать самим, и советую скачивать оригинальный образ, а не какую-нибудь сборку.

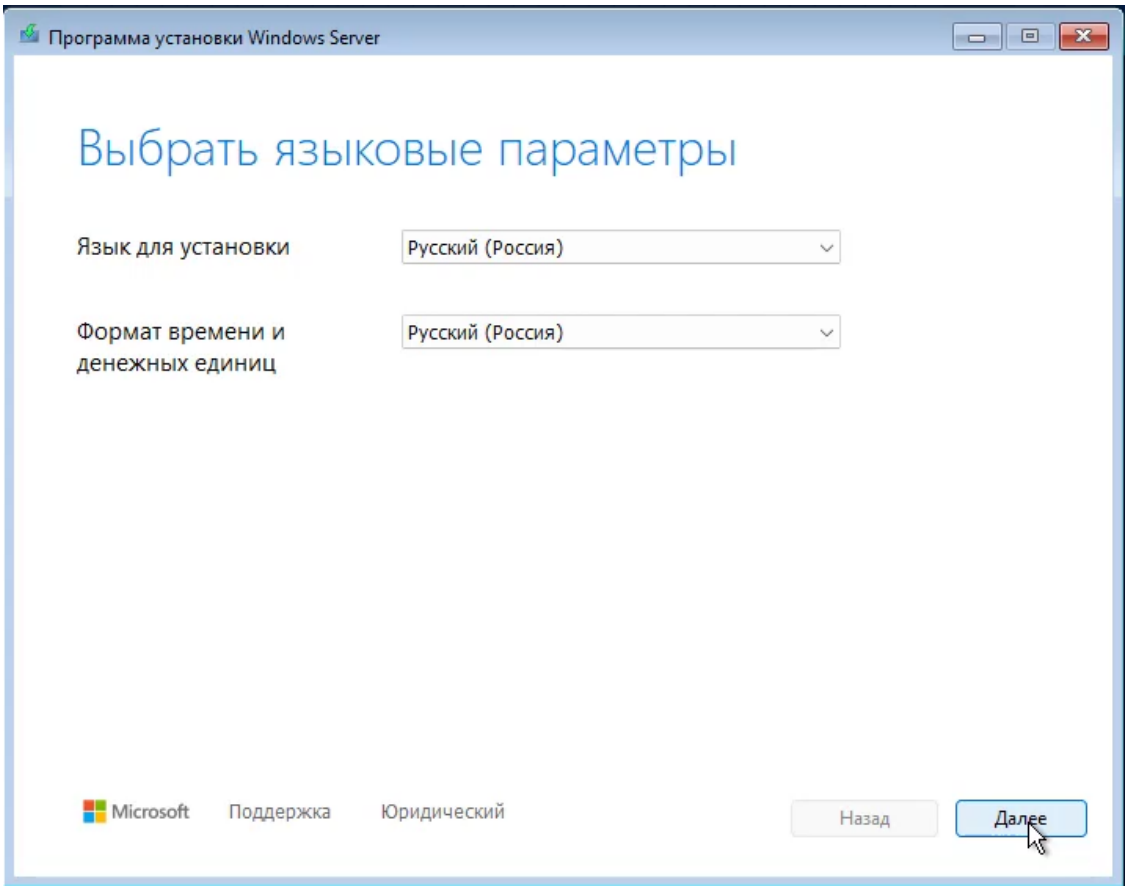
Установка операционных систем Windows 7, 10, 11 и 2025 Server

Надеюсь, что вам уже ни раз приходилось устанавливать операционную систему Windows, так что особо подробно я не буду на этом останавливаться. Расскажу лишь о нюансах установки Windows Server 2025 (видеоинструкция по установке).

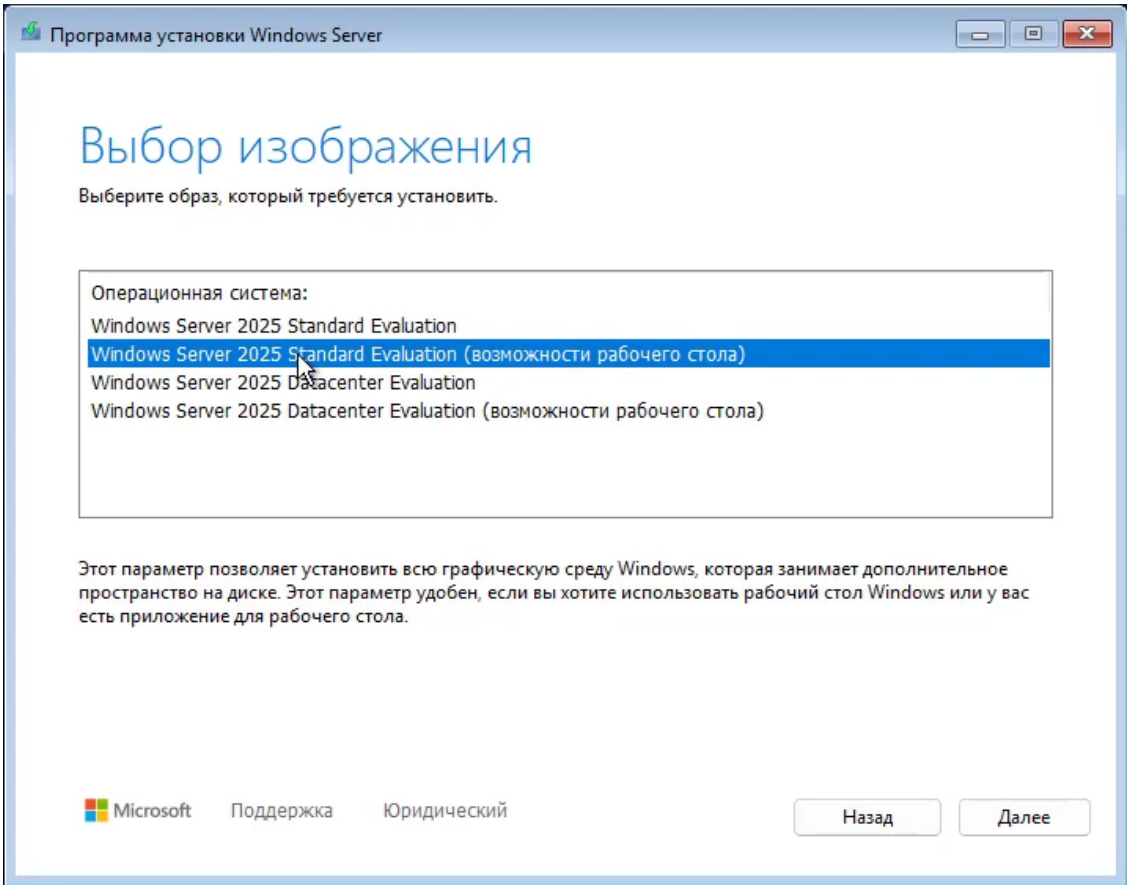
Монтируем загрузочный диск (флешку) с дистрибутивом Windows Server 2025 и указываем его первым в очередности загружаемых устройств.



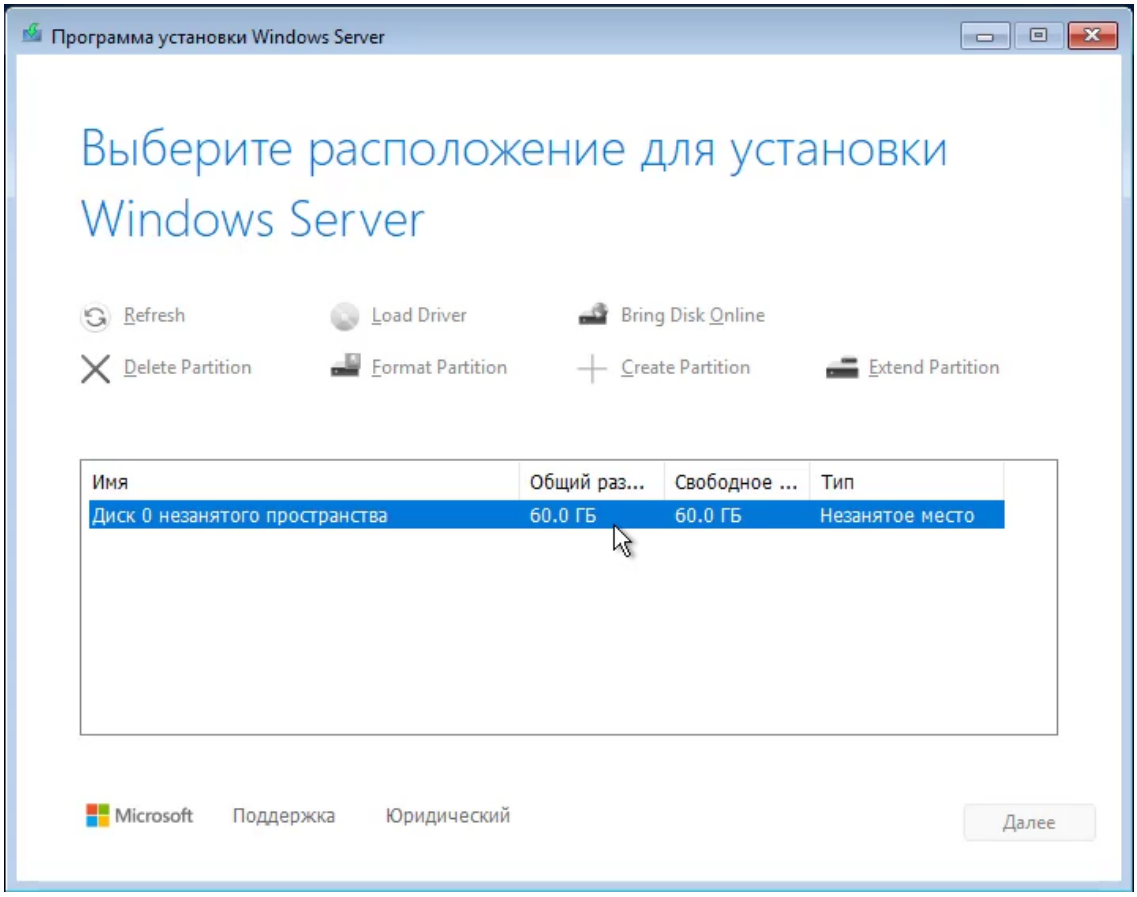
Везде русский (если вы русский :-D)



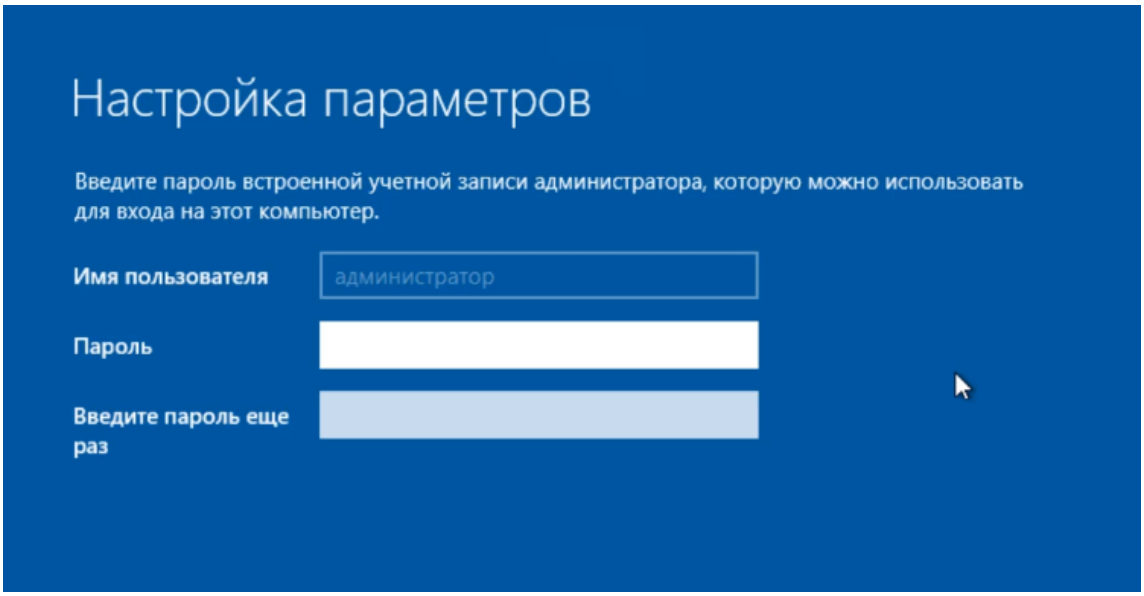
Выбираем версию **Standard Evaluation (возможности рабочего стола)**. В этом варианте нам будет доступен графический интерфейс, если выбрать обычную версию, то управление ОС будет выполняться через командную строку, как в Linux системах.



Установим на не занятое пространство диска (не будем разбирать диск на разделы) \ Далее



После нескольких перезагрузок вводим пароль администратора, подходящий под требования сложности (цифры, большие буквы и маленькие).



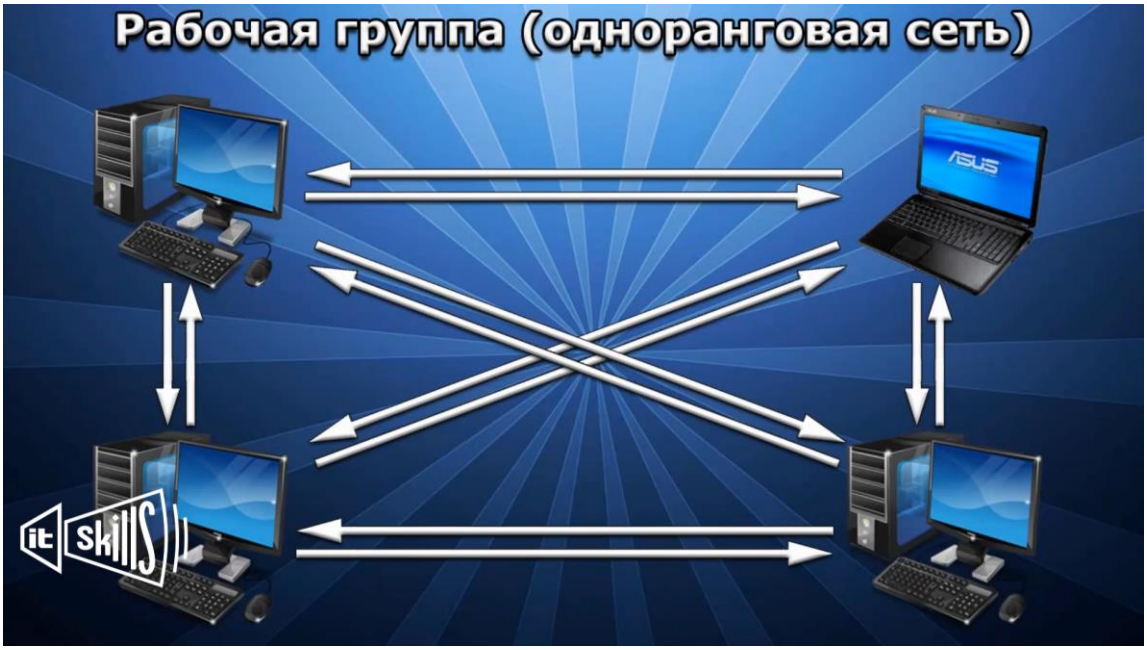
С Windows 7, 10 и 11 все аналогично

Поднятие контроллера домена (Active Directory + DNS)

Основной особенность Windows Server является работа с Active Directory (Активная директория или AD) которая позволяет эффективно управлять правами доступа в локальной сети.

Но, для начала давайте разберемся в чем заключается разница в работе одноранговой сети (сеть с рабочей группой) и сети с Active Directory (доменной сети).

В сети, основанной на рабочей группе (или одноранговая сеть), каждый компьютер является одновременно и клиентом и сервером.

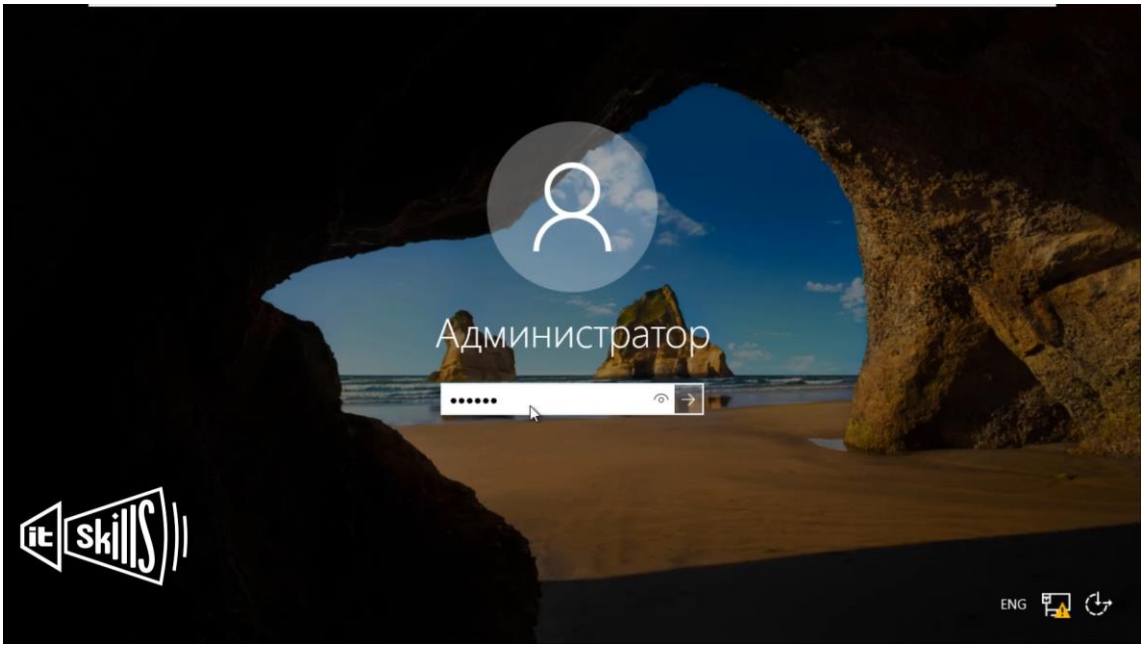


Т.е. для того, чтобы получить доступ к определенным ресурсам компьютера в сети, необходимо присутствуя за ним физически, выполнить все необходимые настройки и так с каждым компьютером. Конечно, это можно сделать через удаленный доступ, но в любом случае, настраивать его придется, физически присутствуя за машиной. И в случае, если вам нужно выполнить какие-либо настройки (настроить систему безопасности, создать нового пользователя, установить программу, прописать сетевой принтер и .т.д.) придется каждый компьютер настраивать по отдельности.

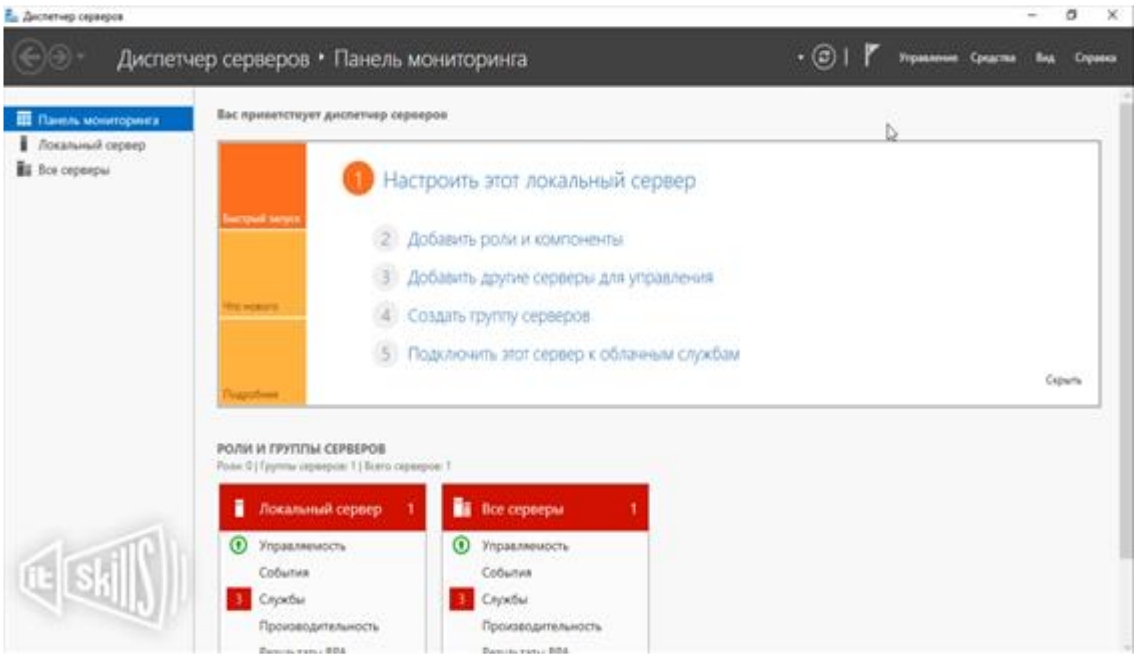
В сети с доменом, есть сервер, а остальные машины являются клиентами и взаимодействие в сети между компьютерами осуществляется через контроллер домена, т.е. он определяет, кому и куда давать доступ.

Таким образом, имея доступ к одному только контроллеру домена, вы можете выполнять 95% задач, в удаленном режиме, так как сервер имеет полные права на любом компьютере в домене. А при помощи групповых политик, можно за несколько минут настроить все компьютеры в домене, не бегая от компьютера к компьютеру.

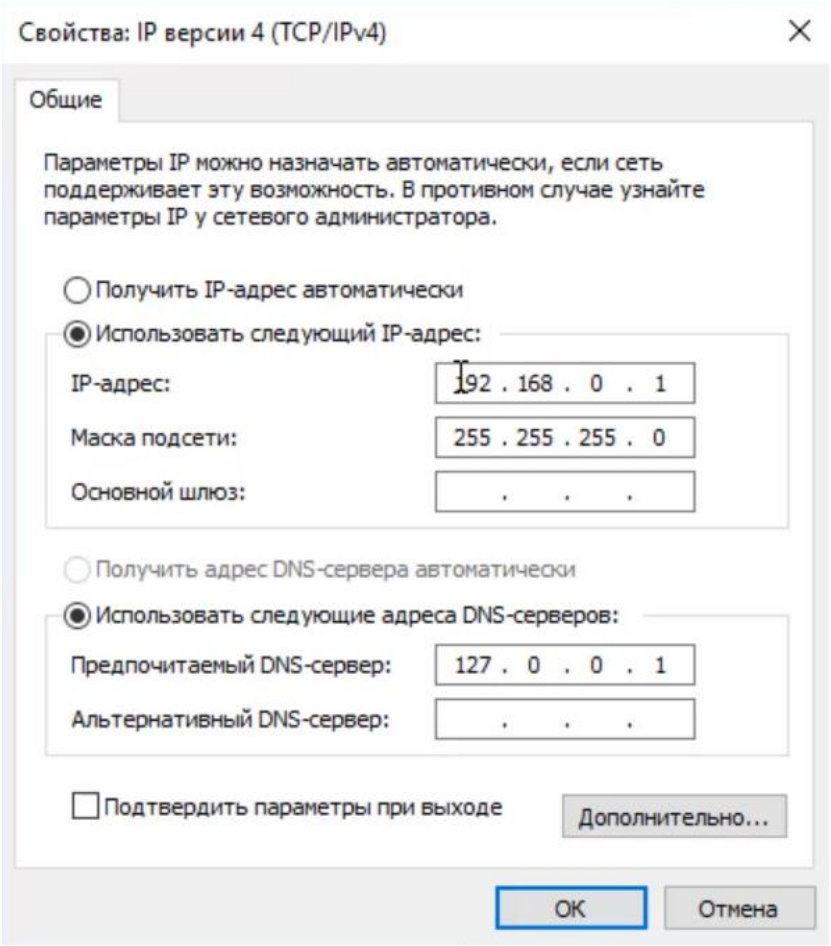
С теорией покончено, перейдем к практике. Выполним вход в систему через комбинацию клавиш Ctrl+Alt+Del, в виртуальной среде эту комбинацию можно отправить через (**Виртуальная машина \ Отправить команду Ctrl+Alt+Del**)



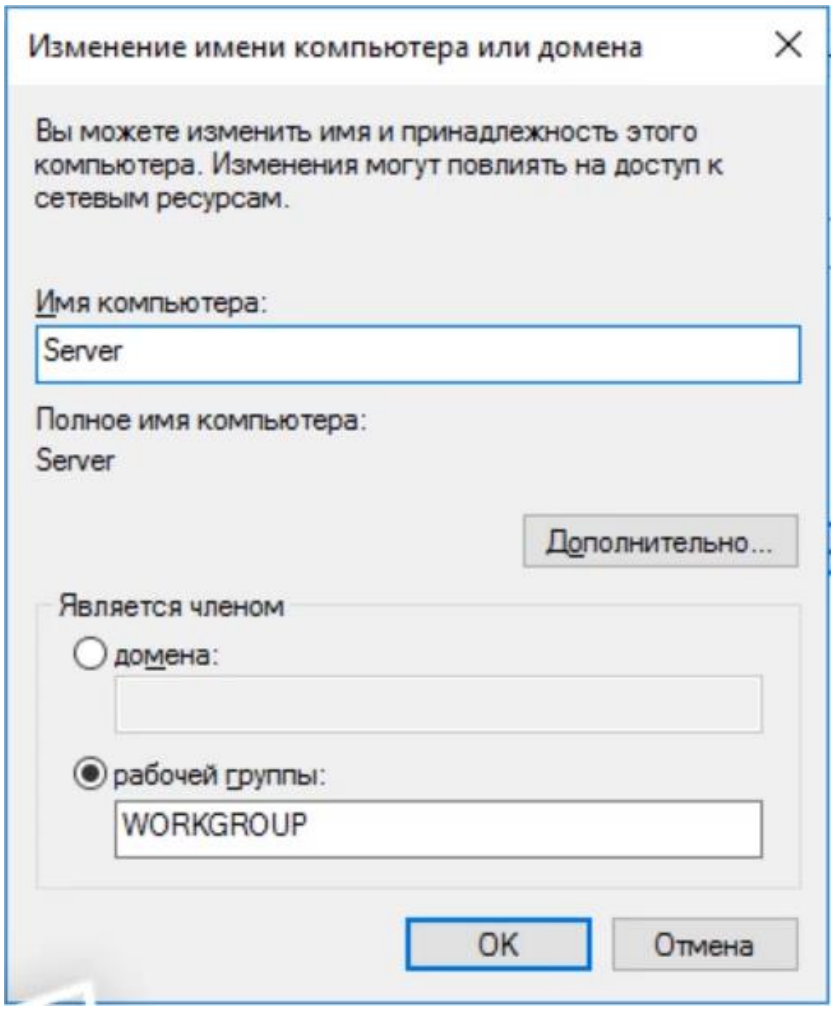
Автоматически запускается Диспетчер серверов, собственно в нем и будет проходить вся основная работа. Если вы его закрыли, вновь открыть можно через **Пуск \ Диспетчер серверов**



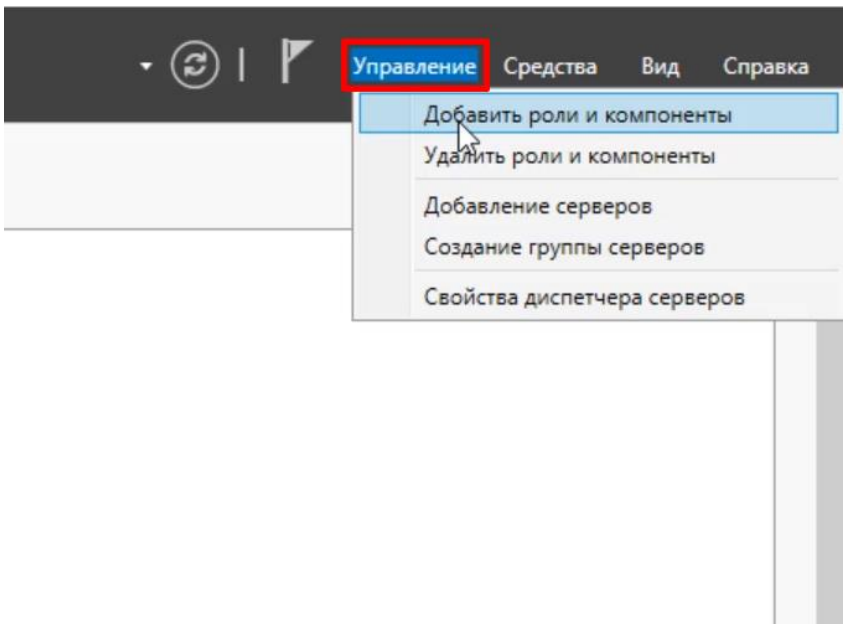
Первым делом нужно прописать все необходимые настройки для сетевого подключения (**Панель управления \ Центр управления сетями и общим доступом \ Сетевое подключение \ Свойства \ IP v4 \Свойства \ Использовать следующий IP адрес: 192.168.0.1; Маска: 255.255.255.0; DNS: 127.0.0.1**)



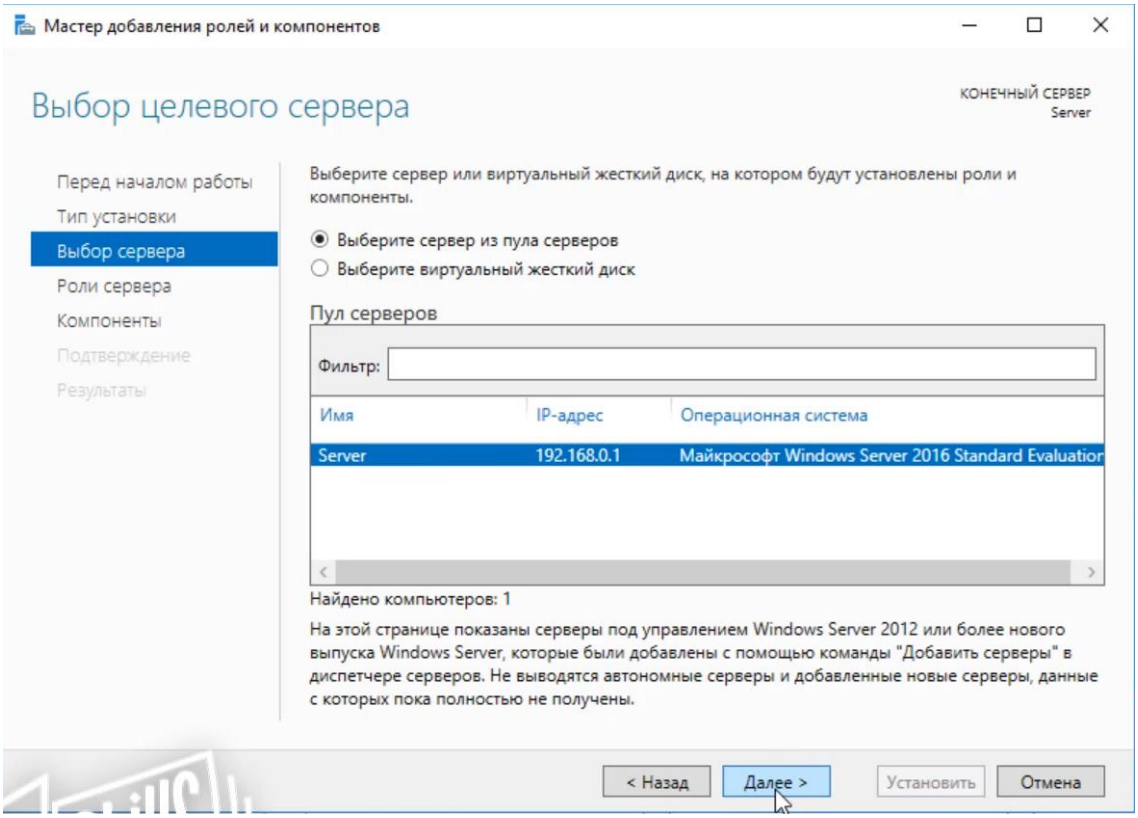
Так же давайте изменим имя сервера, чтобы его можно было легко распознать в сетевом окружении (**Этот компьютер \ ПКМ \ Свойства \ Изменить \ Изменить \ server \ Перезагружаемся**).



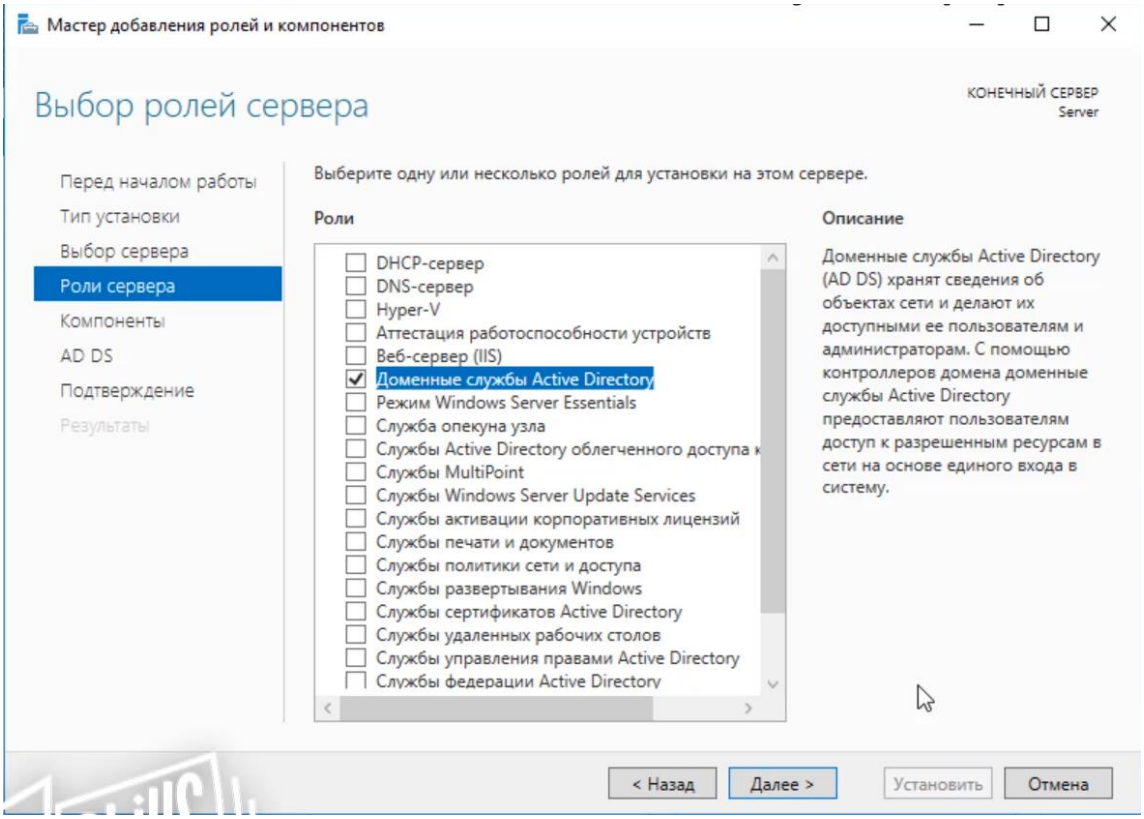
Перейдем к установке ролей AD и DNS (**Диспетчер серверов \ Управление \ Добавить роли и компоненты**



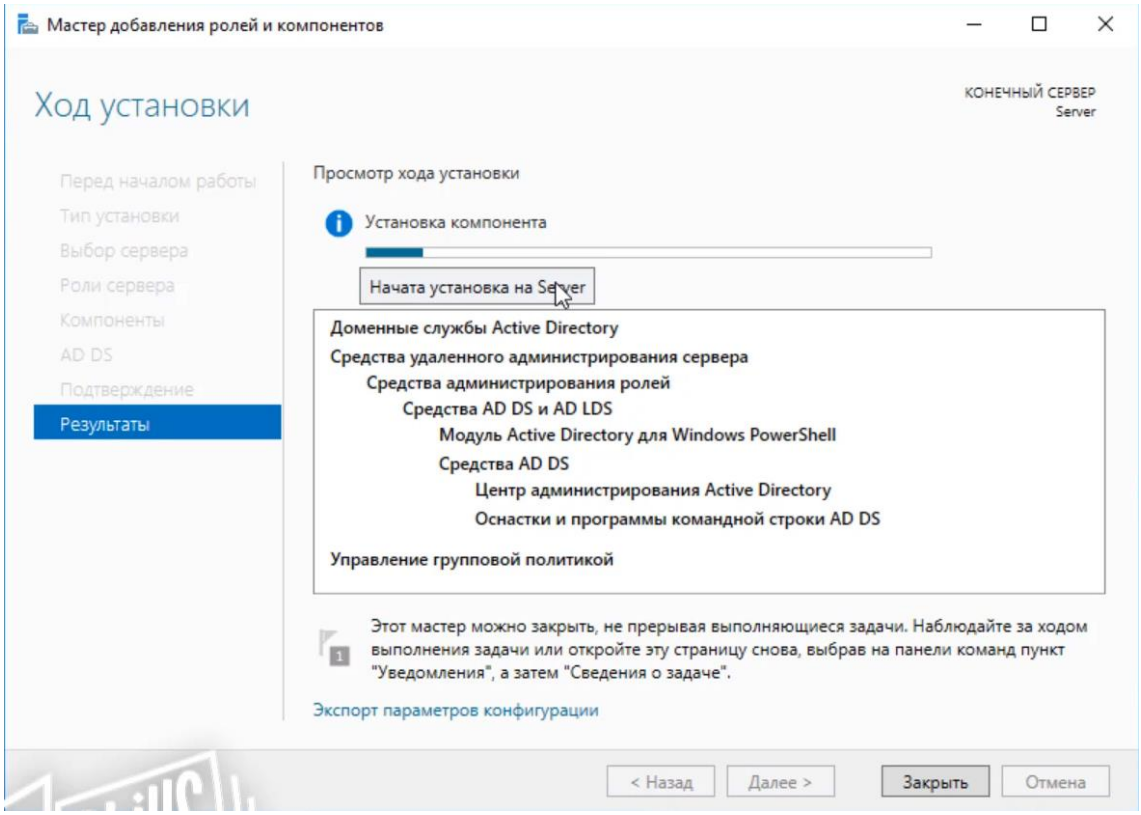
Далее \ Установка ролей или компонентов \ Далее \ Выбираем наш сервер, он у нас один



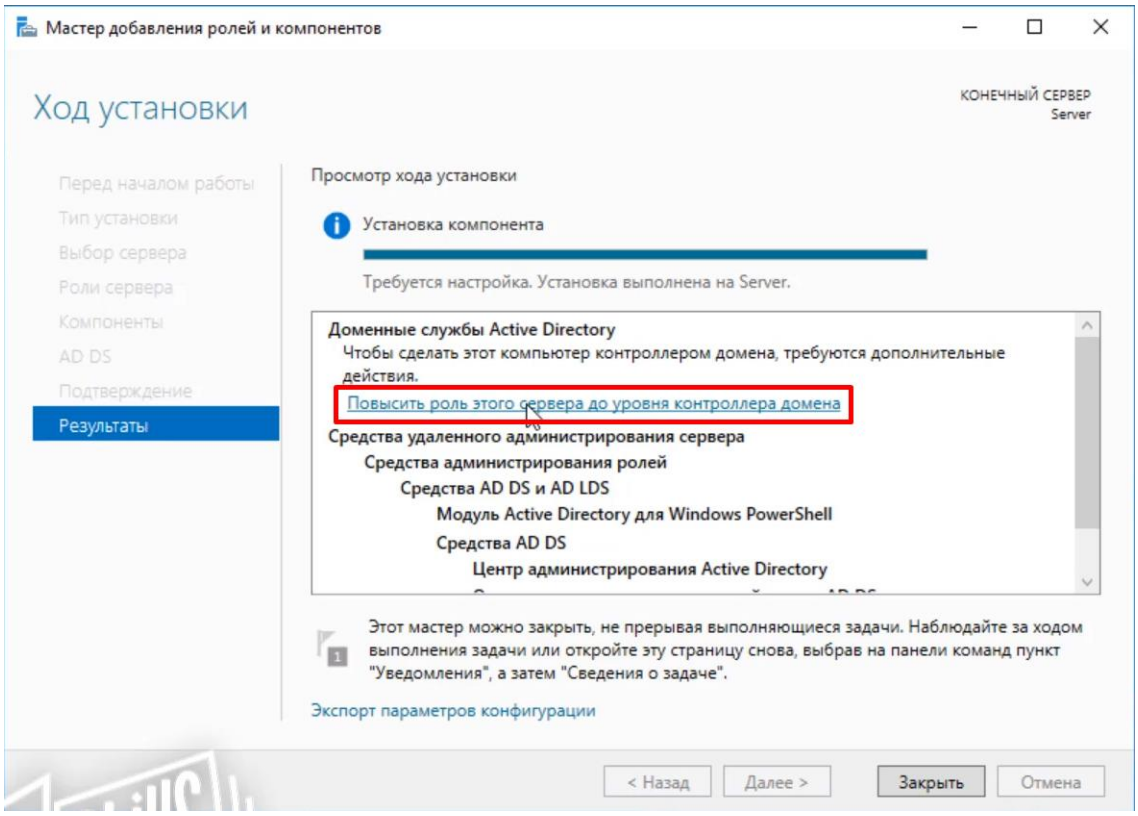
Далее \ Доменные службы Active Directory \



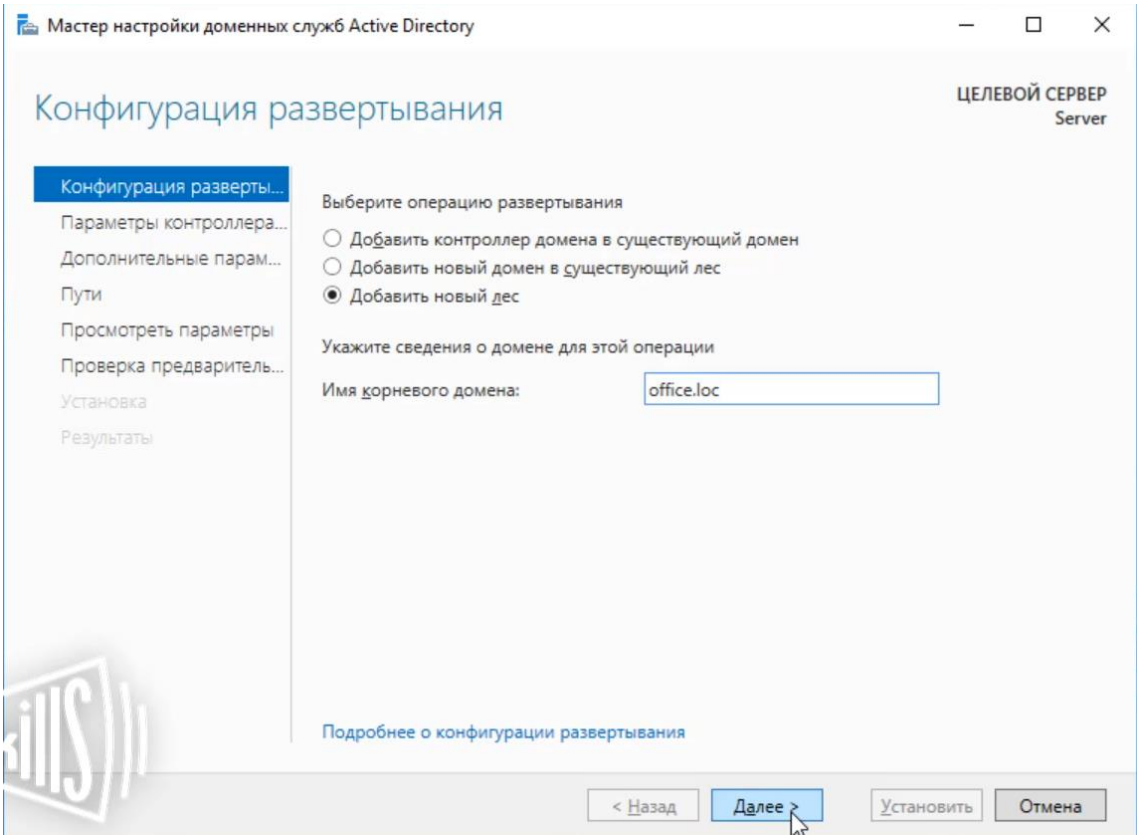
Добавить компоненты \ Далее \ Необходимые компоненты уже должны были выбраться, как было сказано в прошлом окне \ Далее \ Говорится что будет установлен и DNS \ Далее \ Установить



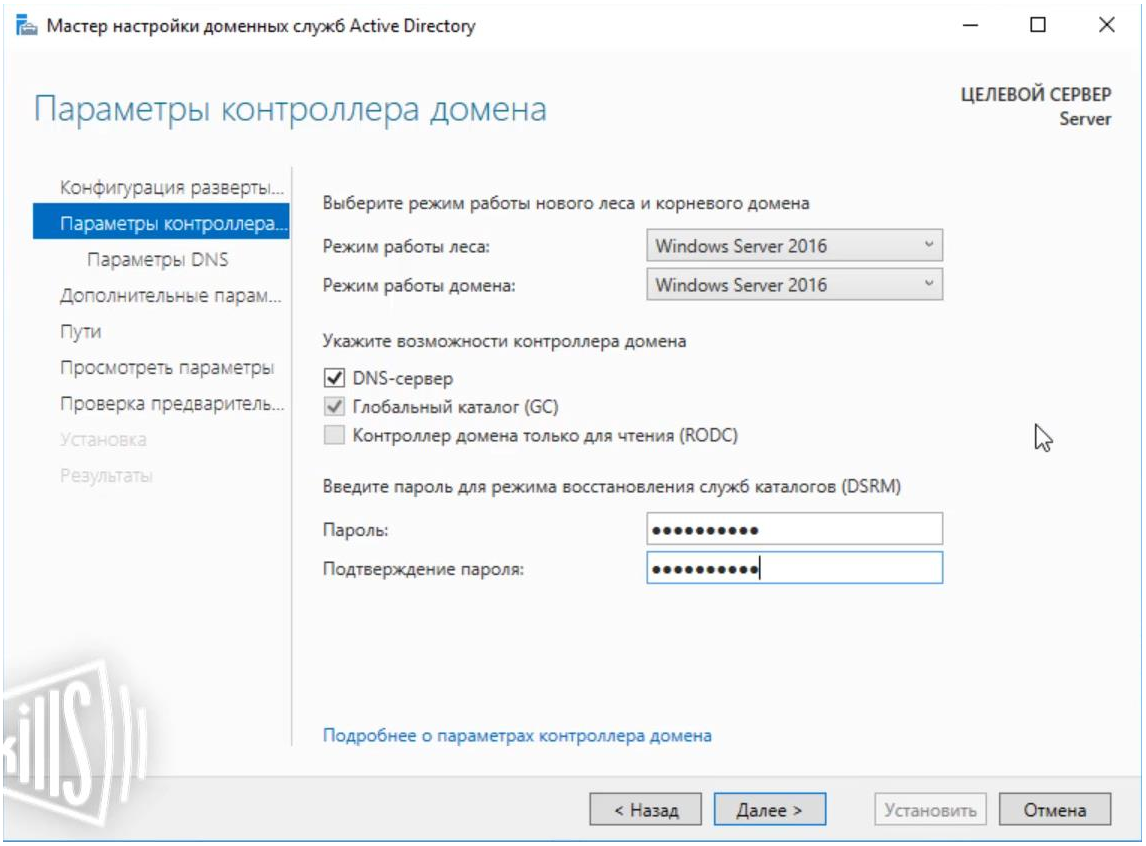
После установки нажимаем **Повысить роль этого сервера до уровня контроллера домена**, т.е. он будет главным в нашей доменной сети.



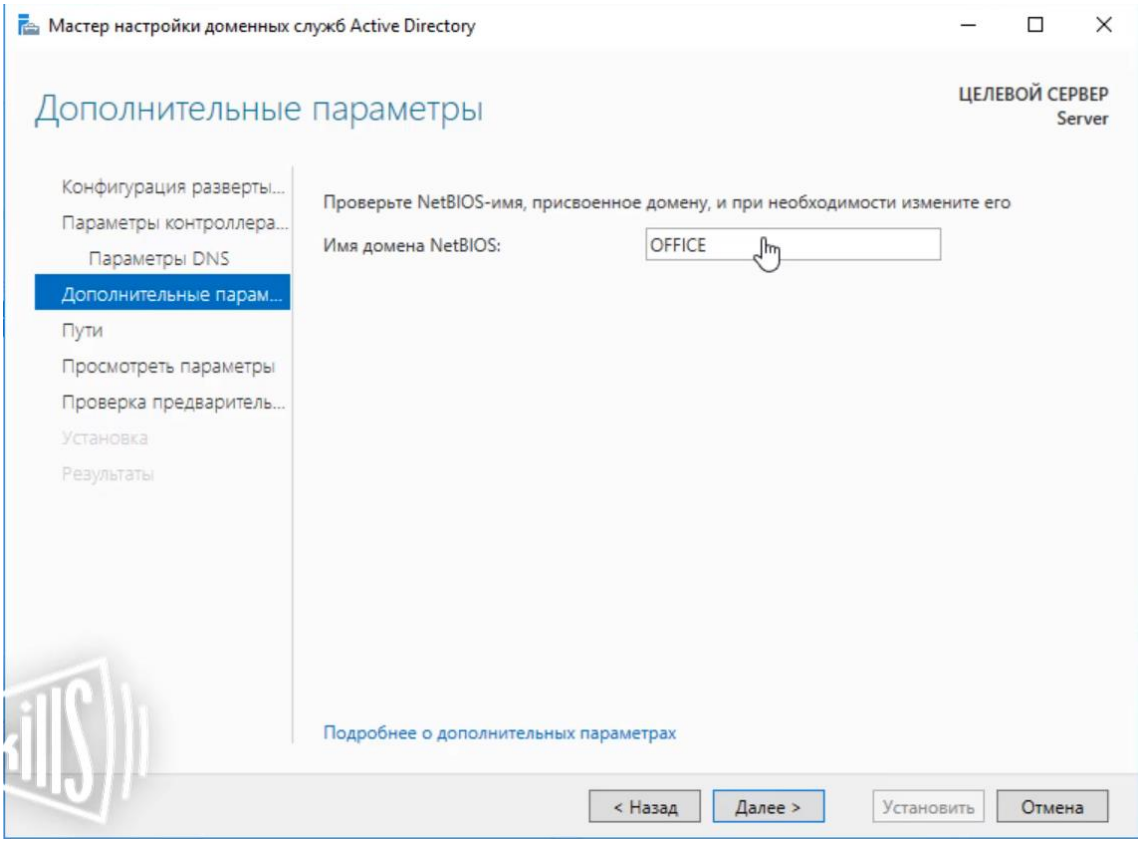
Так как у нас домен новый и других доменов у нас нет (так называемого леса), то мы добавим новый лес и именем корневого домена office.loc



Оставляем по умолчанию и вводим пароль для режима восстановления (можете такой же пароль, как и для администратора)



Параметры DNS, он у нас будет один, по этому мы не можем создать делегирование (**Далее \ NetBIOS имя (это сокращённое имя домена без .loc) \ Далее \ Далее \ Далее \ Установить \ Сервер перезагрузится**)



На этом, первоначальная настройка сервера завершена.

Настройка DNS

В прошлом разделе мы немного забежали вперед, установив роль DNS вместе с Active Directory, но, по сути, не выяснив что это за роль и зачем она нужна.

Поэтому сейчас рассмотрим зачем вообще DNS нужен и немного его до настроим.

Компьютеры и люди воспринимают информацию совершенно по-разному. Компьютеру удобнее работать с числами, так как он работает с двоичными значениями, а людям проще воспринимаются слова. Так вот DNS сервер предназначен для того, чтобы цифровые значения преобразовывать в текст.

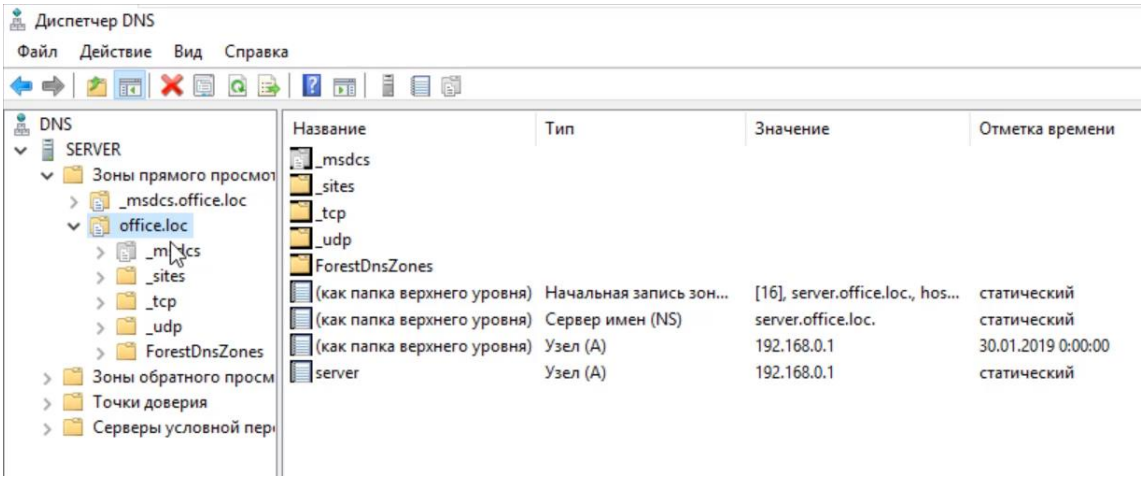
Хорошей аналогией DNS могут служить телефонные справочники, чтобы понять, в чем сходства, рассмотрим принцип их работы.

В городе Москва есть телефонный справочник и чтобы нам найти номер телефона Иванова Ивана Ивановича, мы находим его имя в справочнике, где его имени соответствует номер телефона.

В DNS в качестве названия города создается зона DNS (office.loc), в качестве имени – имя компьютера (director.office.loc), а в качестве телефона IP-адрес (192.168.0.213).

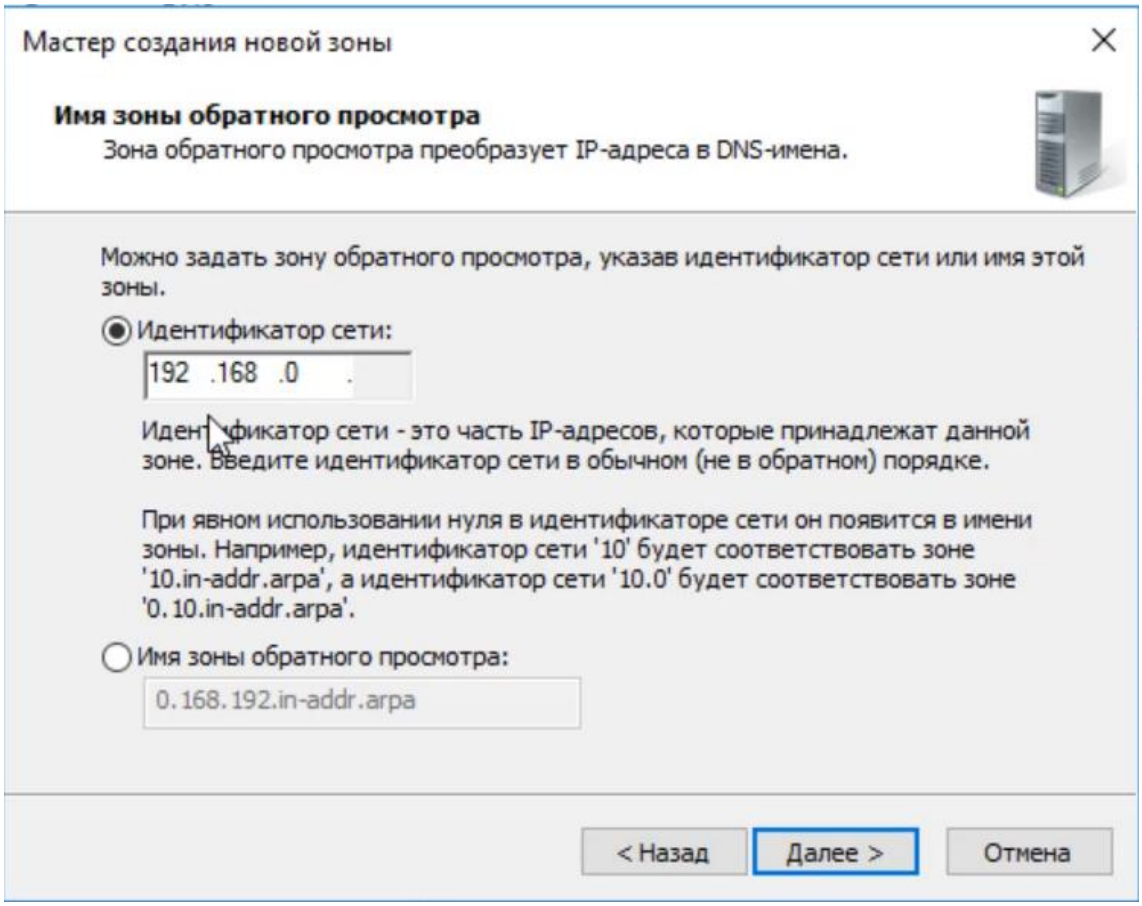
Так вот работа DNS сервера заключается в преобразовании имен в IP-адреса и наоборот, IP-адреса в имена. Причем, соответствие между именем и адресом, называется записью ресурса (Resource Record или RR записью)

Посмотрим, что у нас происходит в DNS (**Средства \ DNS \ Server \ Зоны прямого просмотра \ office.loc**)



Зона прямого просмотра содержит записи, по которым выполняется преобразование имени компьютера в IP адрес, а зона обратного просмотра – преобразование IP адреса в имя компьютера.

Зона прямого просмотра у нас создалась автоматически, а зоны обратного просмотра у нас нет, поэтому мы её создадим вручную (**Зона обратного просмотра \ ПКМ \ Создать новую зону \ Далее \ Далее \ Далее \ Далее \ Идентификатор сети 192.168.0 \ Далее \ Далее \ Готово**)



Теперь, когда мы будем подключать новые компьютеры к домену, у нас будут появляться записи в прямой и обратной зонах DNS.

Доменные учетные записи

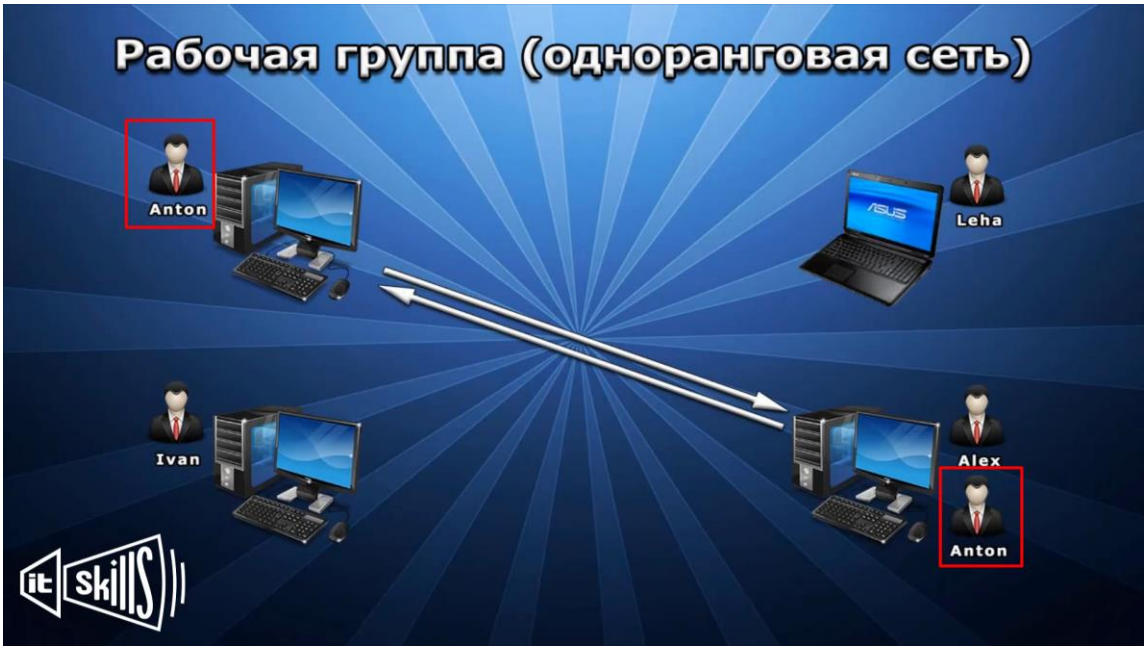
Одной из основных задач системного администратора в доменной сети, является управление учетными записями компьютеров и пользователей. Но, для этого нужно иметь представление о логике взаимодействия этих элементов.

Для этого, рассмотрим взаимодействие учетных записей компьютеров и пользователей в рабочей группе и в домене.

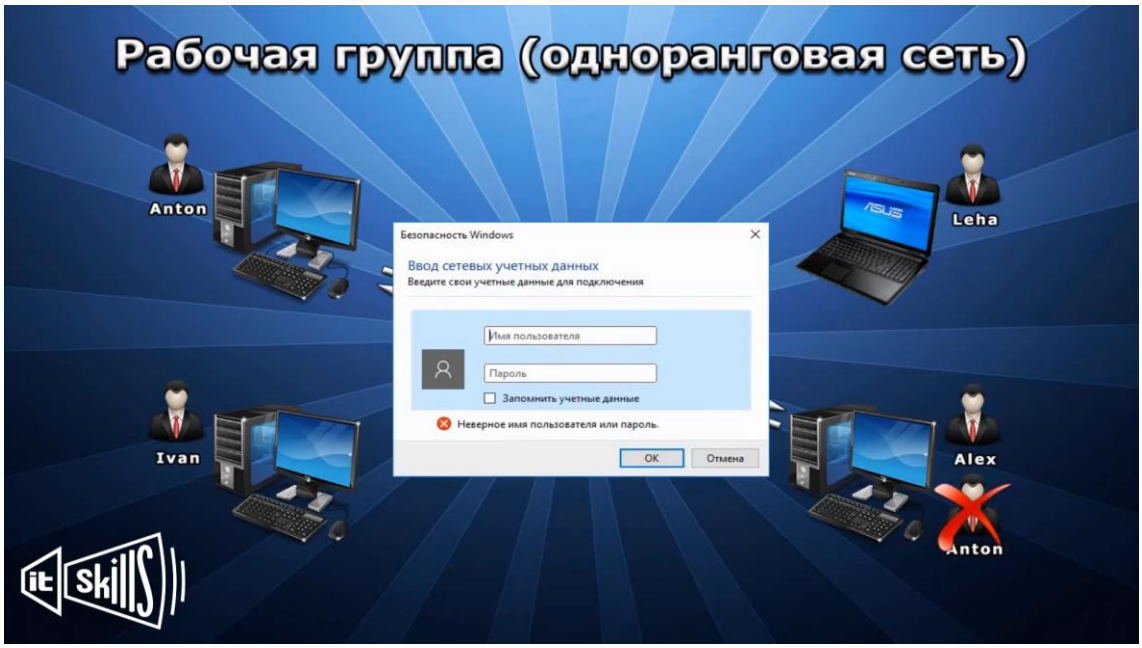
Как я говорил ранее, в рабочей группе каждый компьютер одновременно является и сервером, и клиентом. В результате чего, их взаимодействие выполняется напрямую.

На каждой рабочей станции существуют локальные учетные записи пользователей и взаимодействие между компьютерами выполняется как раз через учетные записи пользователей.

Допустим, нам необходимо с одного компьютера, получить доступ к файлам другого. В данной ситуации отправляется запрос к нужной машине. В свою очередь, она проверяет, из-под какой учетной записи выполняется запрос. И если учетная запись данного пользователя существует, т.е. имя пользователя и пароль одинаковы на обеих машинах, то авторизация проходит успешно, и мы можем получить доступ к ресурсам.



Если такой учетной записи не существует, то система попросит ввести данные пользователя, который есть на компьютере.



Таким образом, нам нужно либо знать имена пользователей и пароли на всех компьютерах, либо создать единую учетную запись на всех рабочих станциях. Как раз в рабочей группе принцип взаимодействия основан на использовании учетной записи рабочей группы на всех компьютерах, через которую и выполняется взаимодействие в сети.

Такая сеть дешевле, но сложнее в администрировании, так как требует вашего непосредственного вмешательства в процесс настройки.

В сети с доменом все взаимодействие выполняется через сервер и для того, чтобы получить доступ к ресурсам сети достаточно подключить компьютер к домену, а также создать пользователя, который будет работать за этим компьютером. Но, так как пользователь создается на контроллере домена, то он сможет работать за любым компьютером в этом домене, конечно же, если это не запрещено политикой безопасности.

И благодаря этому, имея доступ к контроллеру домена, мы сможем управлять любым компьютером в сети, а используя групповые политики можно в автоматическом режиме на всех компьютерах в домене настроить: удаленный доступ, безопасность, антивирусную защиту, устанавливать или удалять программы, настроить принтеры, внести изменения в реестр и многое другое.

Поэтому, далее, нам потребуется подключить компьютеры к домену и создать первого пользователя.

Подключение компьютеров к домену

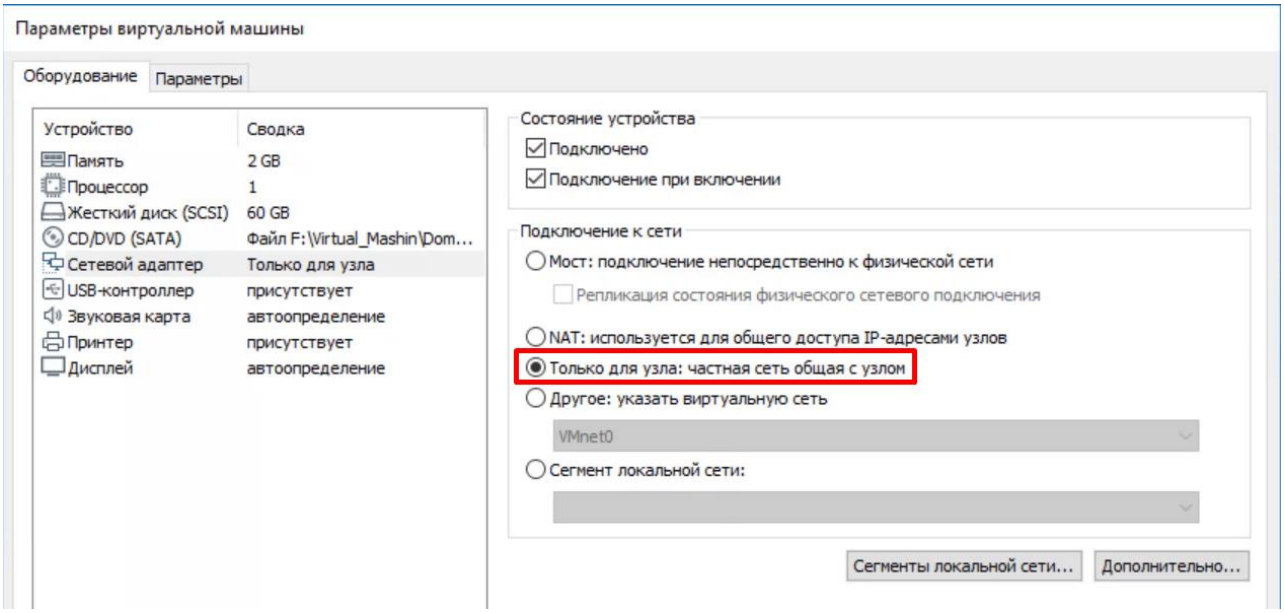
Для того, чтобы начать централизованно управлять компьютерами и иметь к ним доступ, нам необходимо эти компьютеры подключить к домену.

Предварительно вы уже должны были создать клиентские виртуальные машины и установить на них Windows 7, 10 и 11. Данные версии операционных систем наиболее часто используются. Хотя кто-то считает 7 устаревшей операционной системой, но на практике они до сих пор используются.

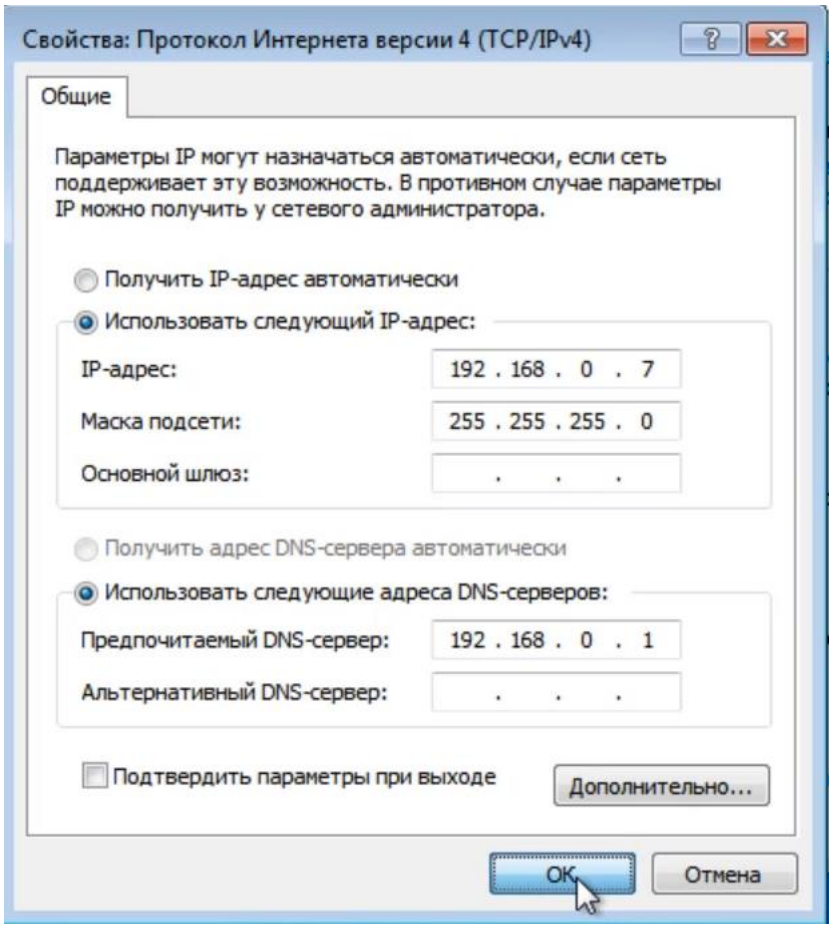
Подключение к домену Windows 7

Для начала нам потребуется наладить связь между контроллером домена и рабочей станцией, поэтому вручную пропишем настройки сетевого подключения для той же сети, что и контроллер домена.

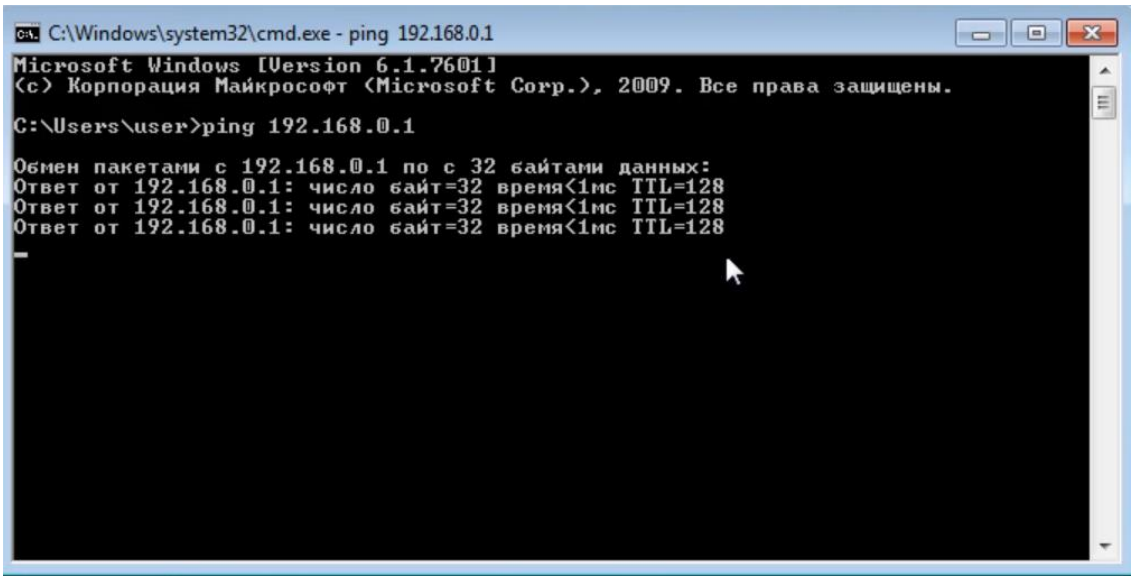
Если настройка проходит в виртуальной среде, то нужно удостовериться, что сетевая карта настроена на общую сеть с контроллером (**Виртуальная машина \ Параметры \ Сетевой адаптер \ Только для узла: частная сеть общая с узлом**)



Теперь настроим сетевое подключение (**Центр управления сетями и общим доступом \ Подключение по локальной сети \ Свойства \ Протокол интернета версии 4 \ Использовать следующие параметры**)



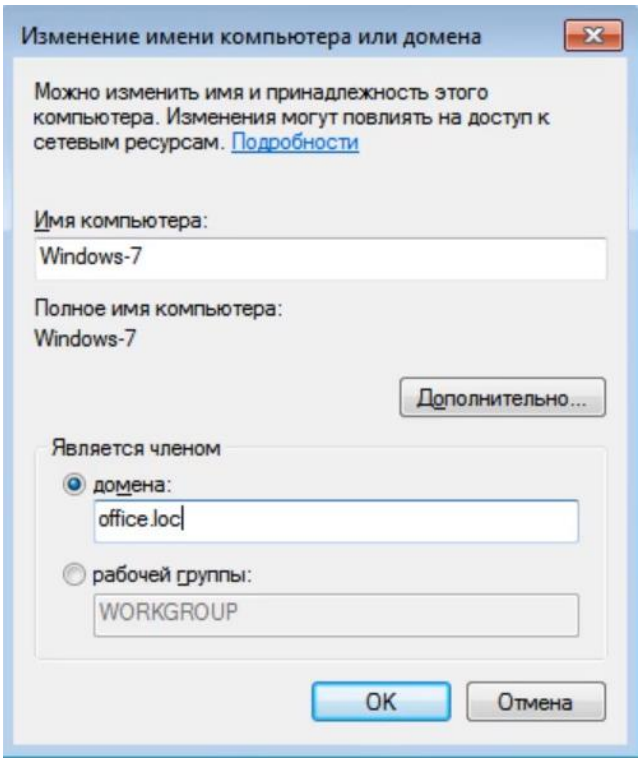
Проверим, есть ли связь с контроллером домена (**Выполнить \ cmd \ ping 192.168.0.1**).



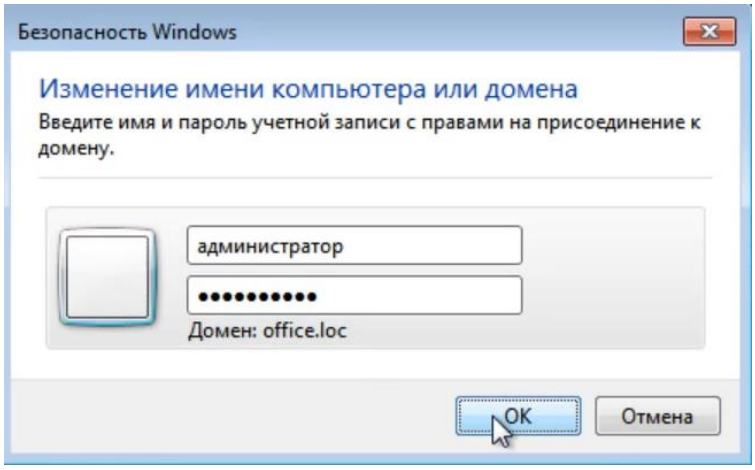
«Пинги» пошли, связь есть, значит можем двигаться дальше.

Так же стоит проверить часовой пояс и время, так как из-за этого могут быть проблемы с взаимодействием в сети. Все должно быть одинаково на всех компьютерах в сети.

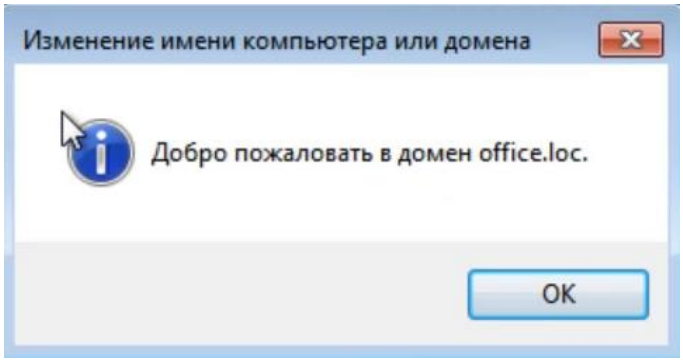
Далее необходимо указать уникальное имя компьютера, так как в домене, не может быть 2 компьютеров с одинаковыми именами или IP адресами. Точнее это может произойти, но, в данной ситуации корректность работы компьютеров в сети будет нарушена (**Пуск \ Мой компьютер \ ПКМ \ Свойства \ Имя компьютера, имя домена и параметры рабочей группы \ Изменить параметры \ Изменить \ Имя компьютера** – в реальной сети я называю компьютеры согласно должности работника, который будет за ним сидеть. Так проще в сети найти тот или иной компьютер. Однако, в тестовой сети, я назову его согласно установленной на нем операционной системе, чтобы аутентифицировать его в сети Windows-7 **\ Является членом домена: office.loc**)



Если появилось окно с вводом данных учетной записи имеющей права на присоединение компьютера к домену, то связь на логическом уровне с контроллером есть. Вводим данные администратора домена, так как в данный момент у нас только один пользователь в домене, это Администратор и его пароль.



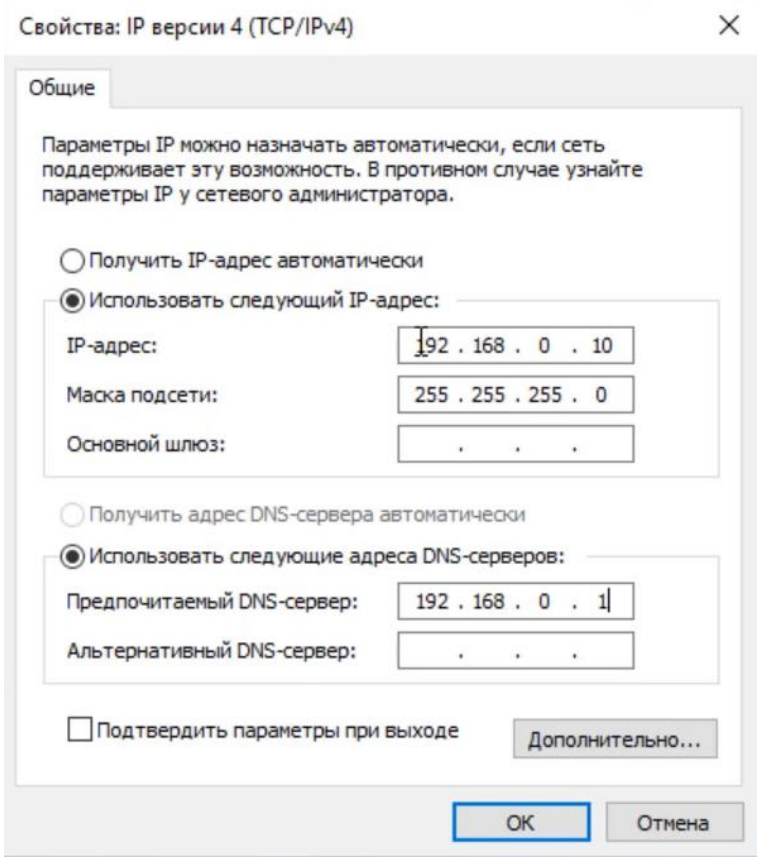
Если все прошло удачно, то появится сообщение Добро пожаловать в домен office.loc.



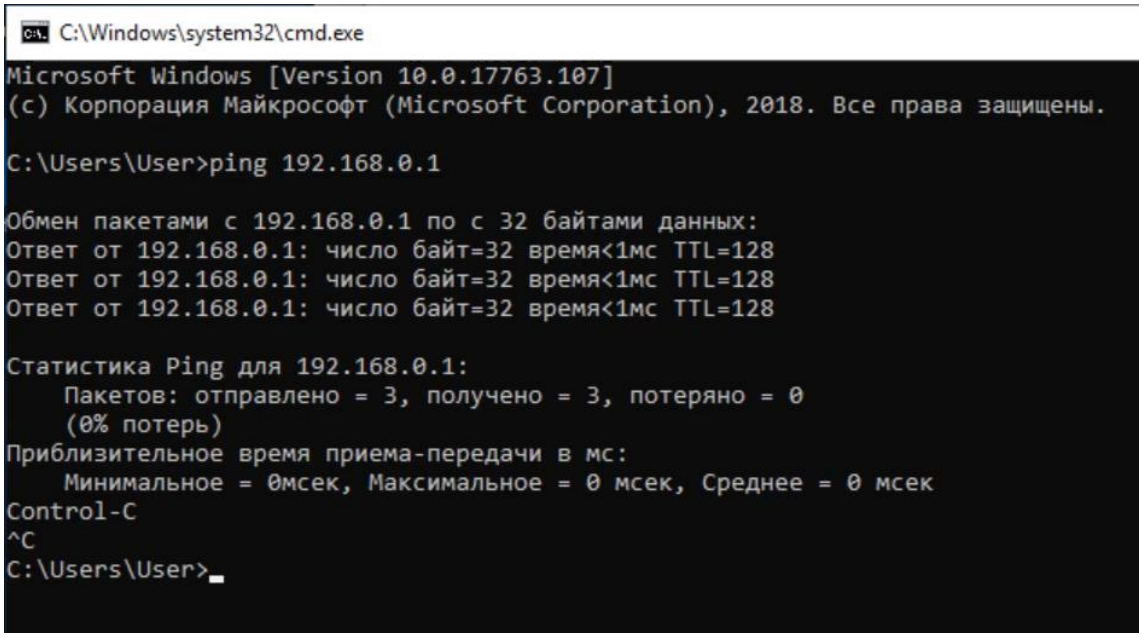
После перезагрузки рабочей станции, нам предлагается нажать Ctrl+Alt+Del и ввести учетные данные пользователя, который будет работать на данном компьютере. А так как у нас его еще нет, то перейдем к созданию пользователя в домене в следующем разделе, а сейчас подключим к домену Windows 10.

Подключение к домену Windows 10

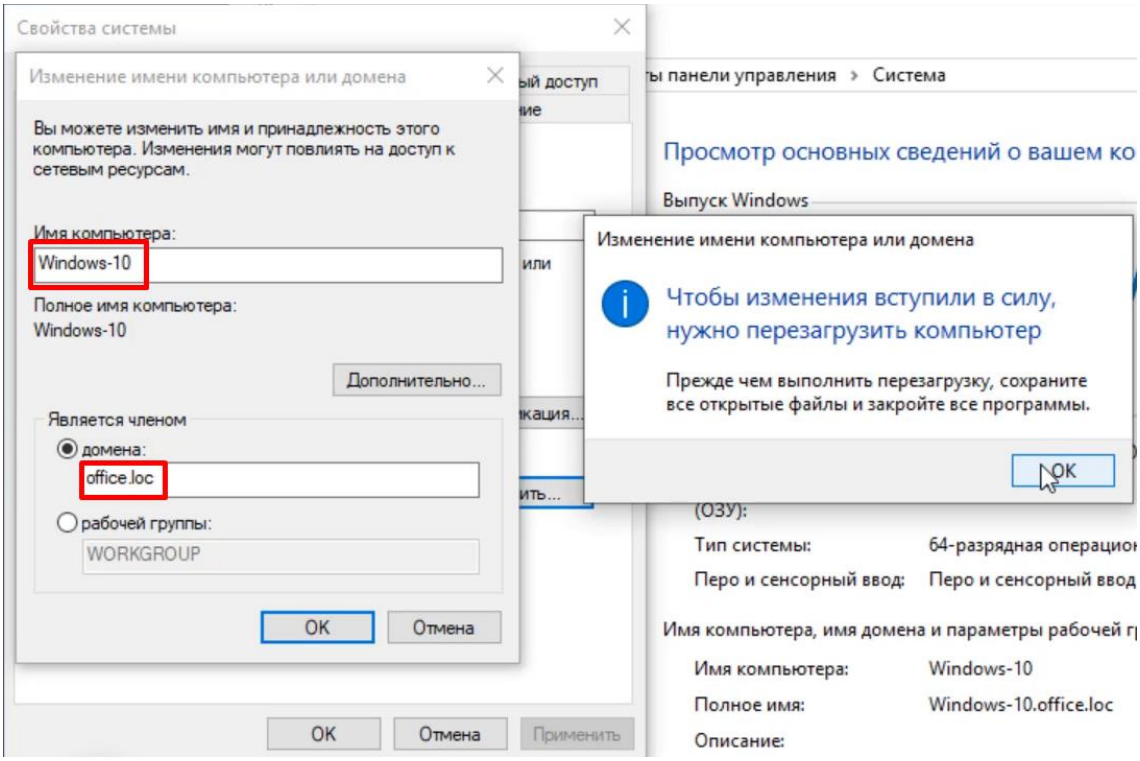
Назначим компьютеру следующие сетевые настройки (Центр управления сетями и общим доступом \ Подключение по локальной сети \ Свойства \ Протокол интернета версии 4 \ Использовать следующие параметры)



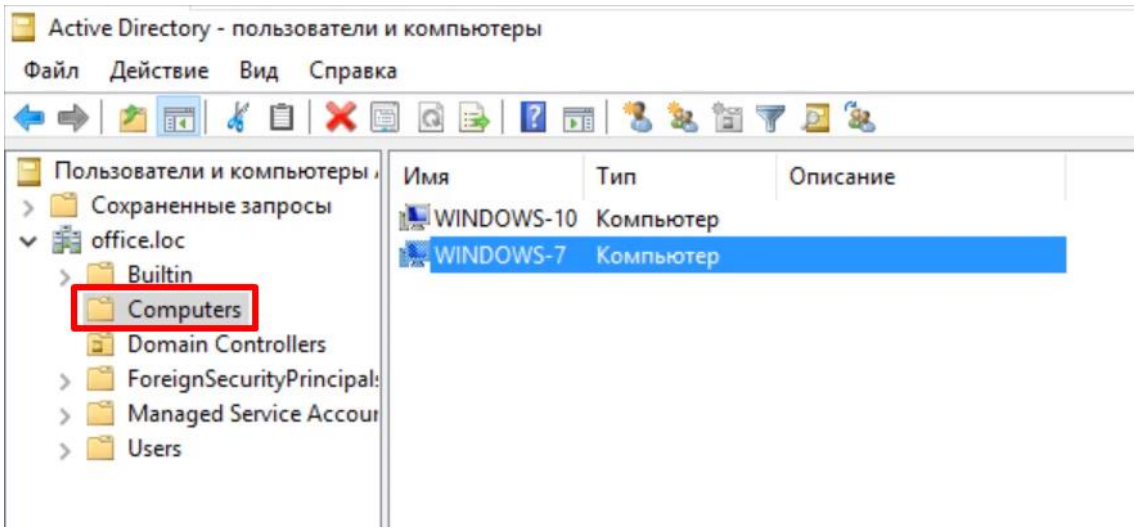
Так же проверим, есть ли связь с контроллером домена (Выполнить \ cmd \ ping 192.168.0.1).



Указываем имя компьютера и домен (**Проводник \ Этот компьютер \ ПКМ \ Свойства \ Имя компьютера, имя домена и параметры рабочей группы \ Изменить параметры \ Изменить \ Имя компьютера \ Windows-10 \ Является членом домена: office.local \ Перезагрузка**)



Можем посмотреть на контроллере домена, появились ли компьютеры в домене (**Пуск \ Администрирование \ AD пользователи и компьютеры \ office.local \ Computers \ Windows-7 и Windows-10**)



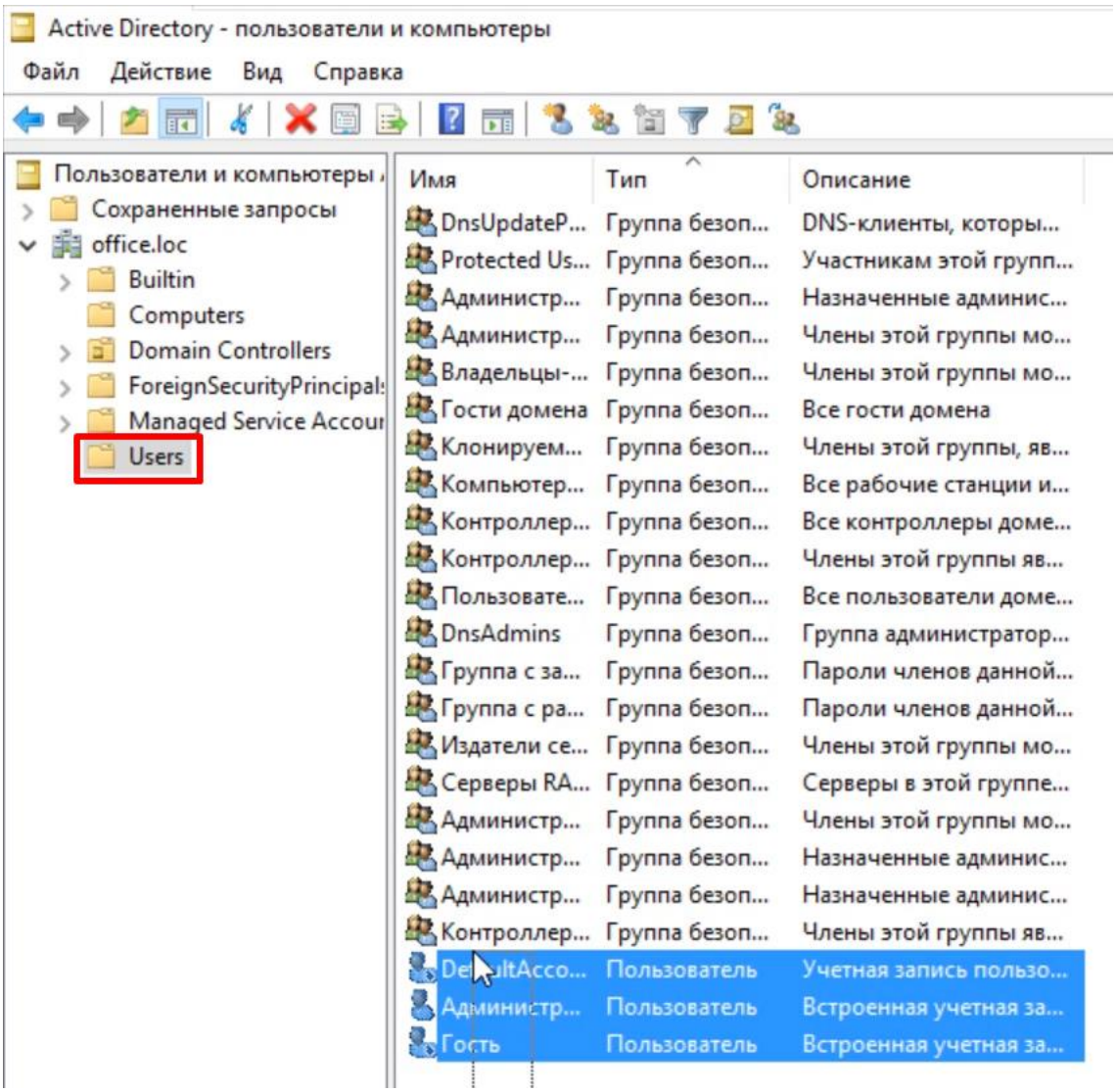
Аналогичным образом подключаем к домену Windows 11.

Создание пользователей

Теперь нам нужно научиться работать с учетными записями пользователей домена, чтобы управлять доступом сотрудников в нашей сети.

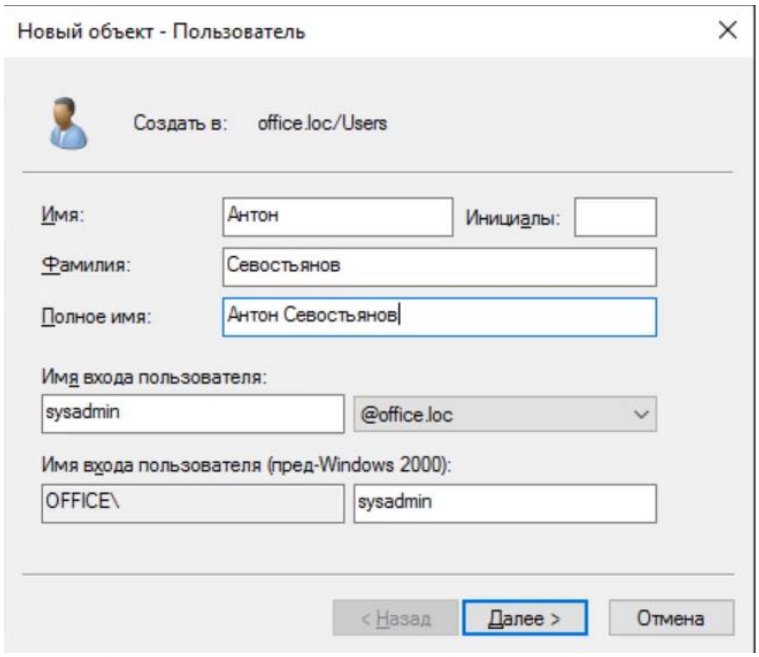
Давайте создадим учетную запись пользователя, под которой сотрудник будет получать доступ к ресурсам домена.

Для этого зайдем в (**Диспетчер серверов \ Средства \ Пользователи и компьютеры Active Directory**)



С категорией «Компьютеры» мы уже разобрались, поэтому, разберемся с категорией Пользователи (Users). В данной категории у нас располагаются учетные записи пользователей и группы пользователей. Как вы видите, на данный момент у нас 2 пользователя, это Администратор – администратор домена и Гость – отключенная учетная запись.

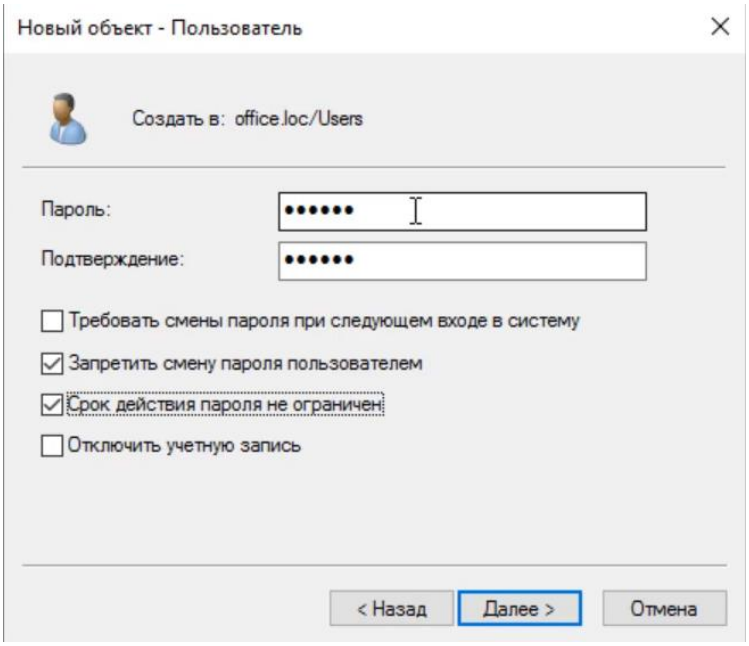
Именно здесь нам и нужно создать первого пользователя (**Users \ Создать \ Пользователь** - к примеру пользователь у нас будет **Севостьянов Антон Геннадьевич и логин sysadmin**.



Как правило, для каждого сотрудника в компании создается отдельная учетная запись с его ФИО, допустим у меня это было бы sevostyanov_ag. Однако на практике это часто не удобно, так как у вас может быть большая текучка (как правило этим грешит отдел продаж), в результате чего вам каждый раз нужно создавать нового пользователя, переносить документы старого сотрудника в профиль нового пользователя.

Поэтому лучше указывать должность сотрудника, чтобы не создавать и удалять учетные записи каждый раз, можно просто поменять пароль.

Так же при задании пароля мы видим надписи, напротив которых можно поставить галочки:



Требовать смену пароля при следующем входе в систему – пользователю, который будет выполнять вход на компьютер входящий в данный домен, при вводе пароля, который мы задаем, будет предложено сменить пароль, где потребуется ввести старый пароль и новый. Это нужно для того, чтобы пароль, который введет пользователь, знал только он.

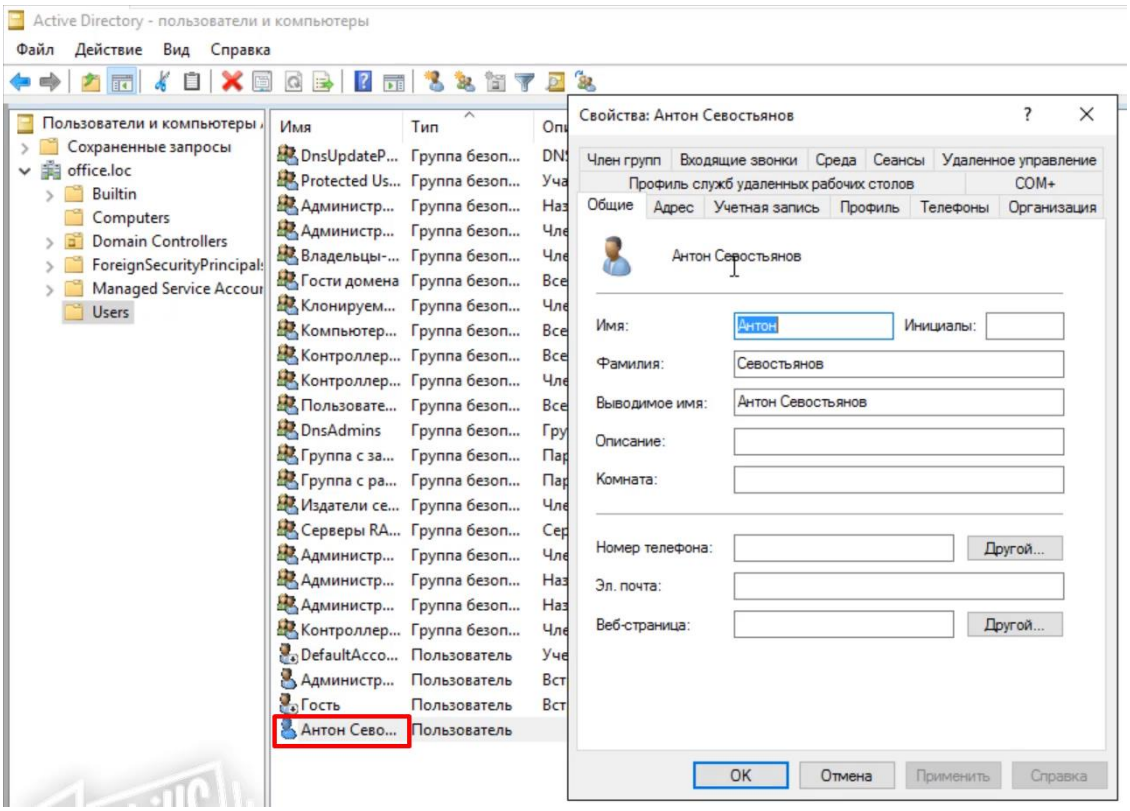
Запретить смену пароля пользователем – пароль можете менять только вы, т.е. администратор.

Срок действия пароля не ограничен – так же в политике безопасности паролей есть такой параметр как срок действия пароля, это означает, что по истечении указанного срока, так же пользователю будет предложено поменять пароль на новый. По умолчанию этот срок равен 42 дням, вы так же его можете менять. Так же есть параметр в политике о повторе паролей, по умолчанию 24 пароля. Это означает, что если при смене пароля вы введете один из 24 ранее использованных паролей, то пароль не будет изменен. Этот параметр так же можно редактировать в политике безопасности домена.

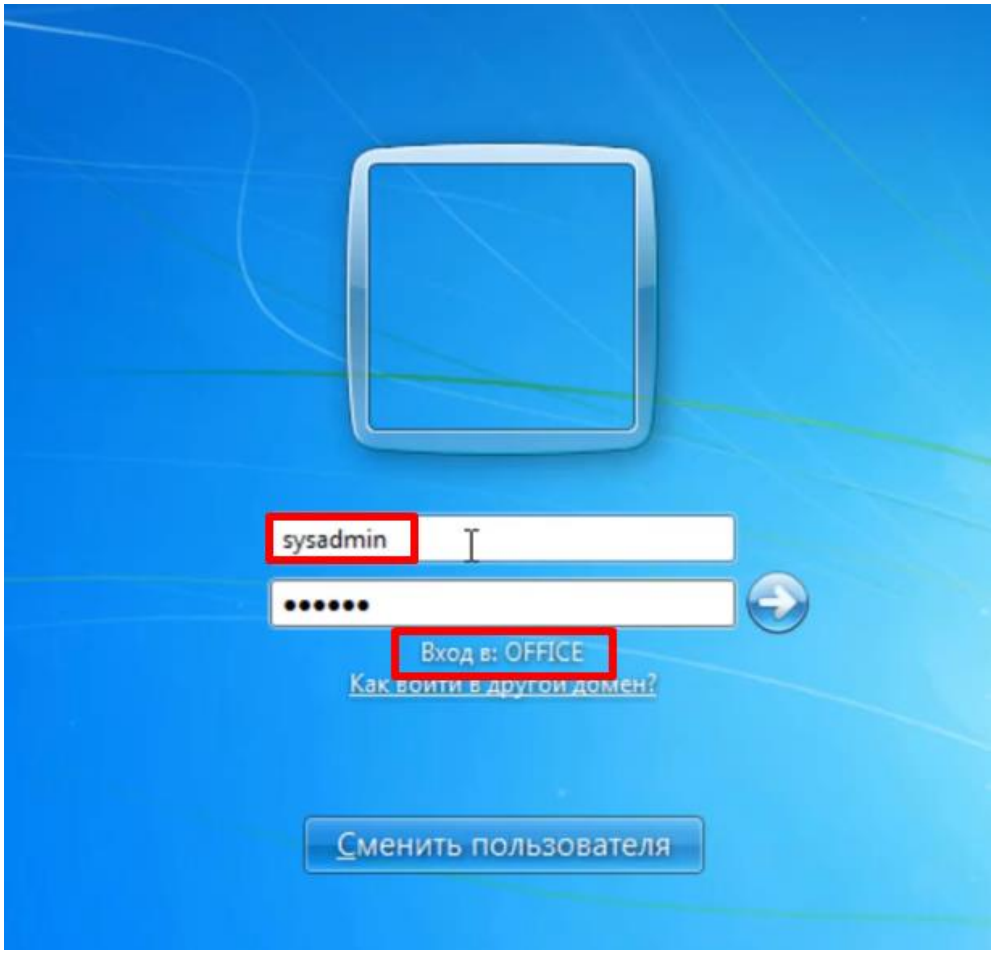
Отключить учетную запись – после создания учетной записи ей воспользоваться не удастся, так как она будет отключена.

Я же выбираю вариант «Запретить смену пароля пользователем» и «Срок действия не ограничен» **\ Далее \ Готово**.

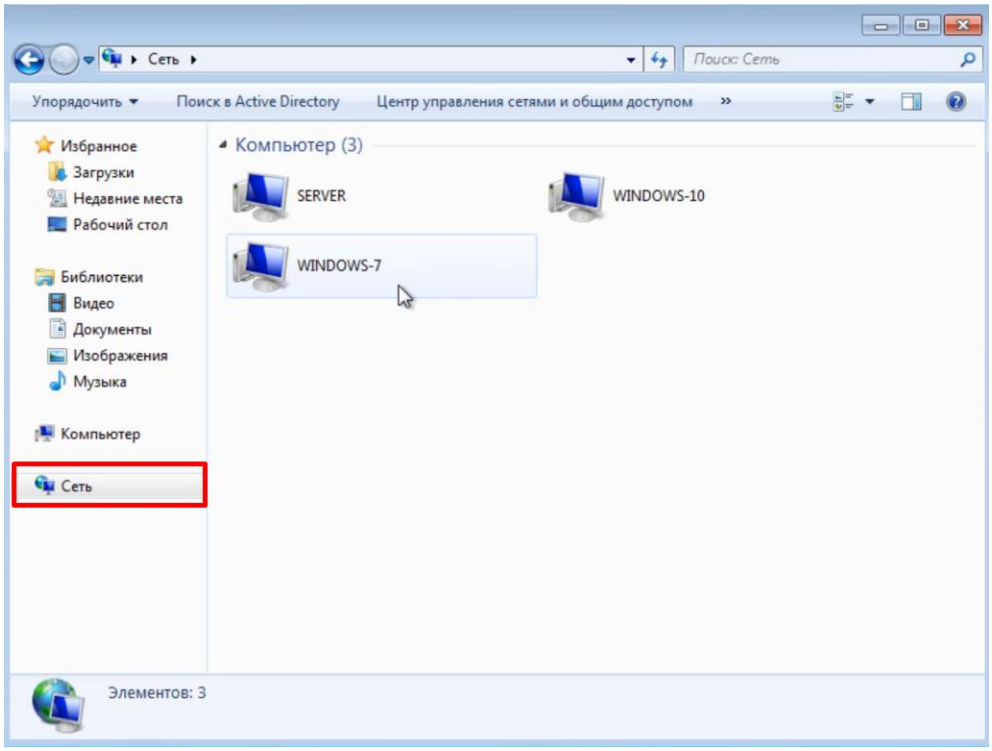
Теперь видим, что пользователь Севостьянов Антон появился у нас в правой части окна. Можно щелкнуть на нем два раза, чтобы добавить какую-либо дополнительную информацию.



Попробуем выполнить вход под данной учетной записью на компьютеры и зайти по сети на какой-либо компьютер.

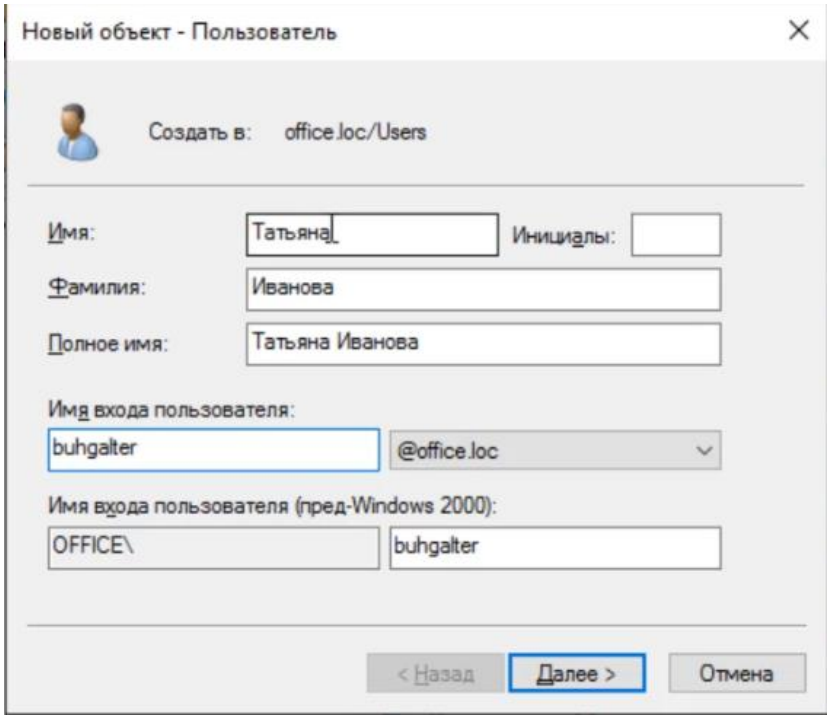


Зайдем в сетевое окружение, чтобы посмотреть какие компьютеры присутствуют в сети.



Настройка общего доступа к файлам

Теперь попробуем по экспериментировать с правами доступа для различных пользователей на разных рабочих станциях. Для этого создадим еще одного пользователя (buhgalter – Иванова Татьяна) и посмотрим, как они будут взаимодействовать между собой.



Теперь выполним вход на клиентские машины под разными учетными записями:

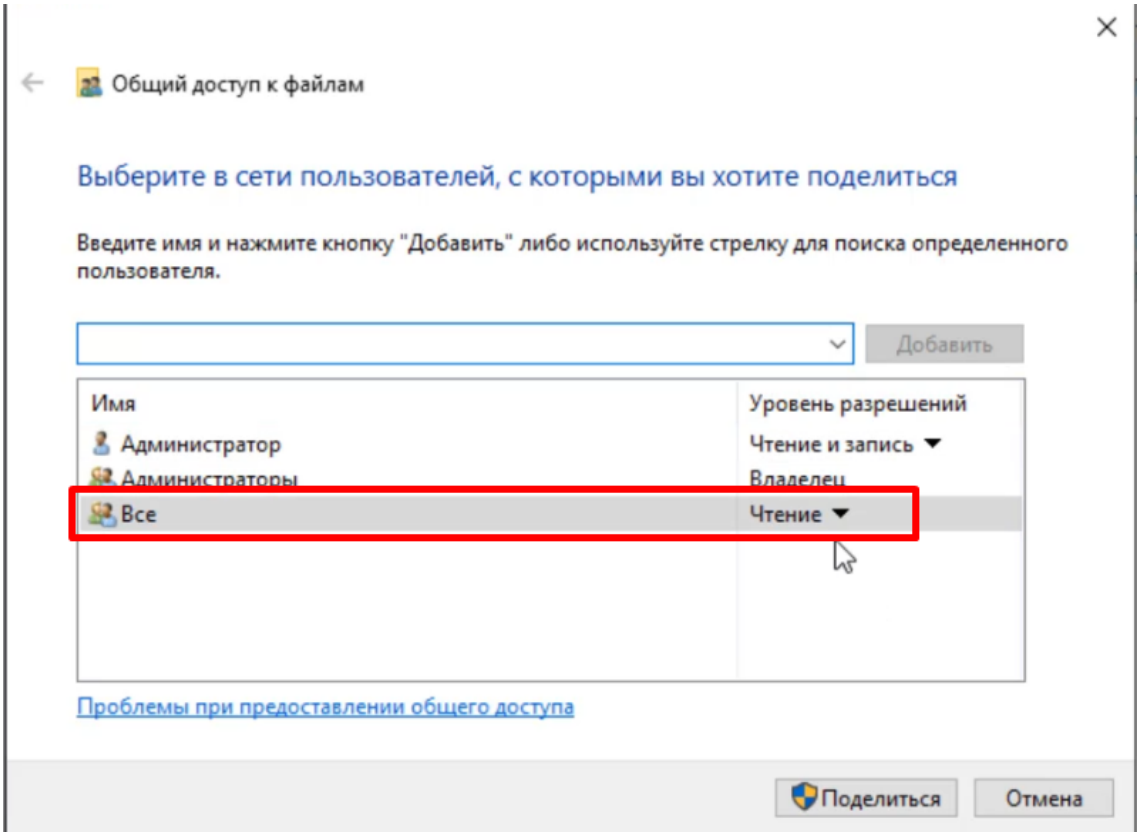
Windows-7 – buhgalter;

Windows-10 – sysadmin.

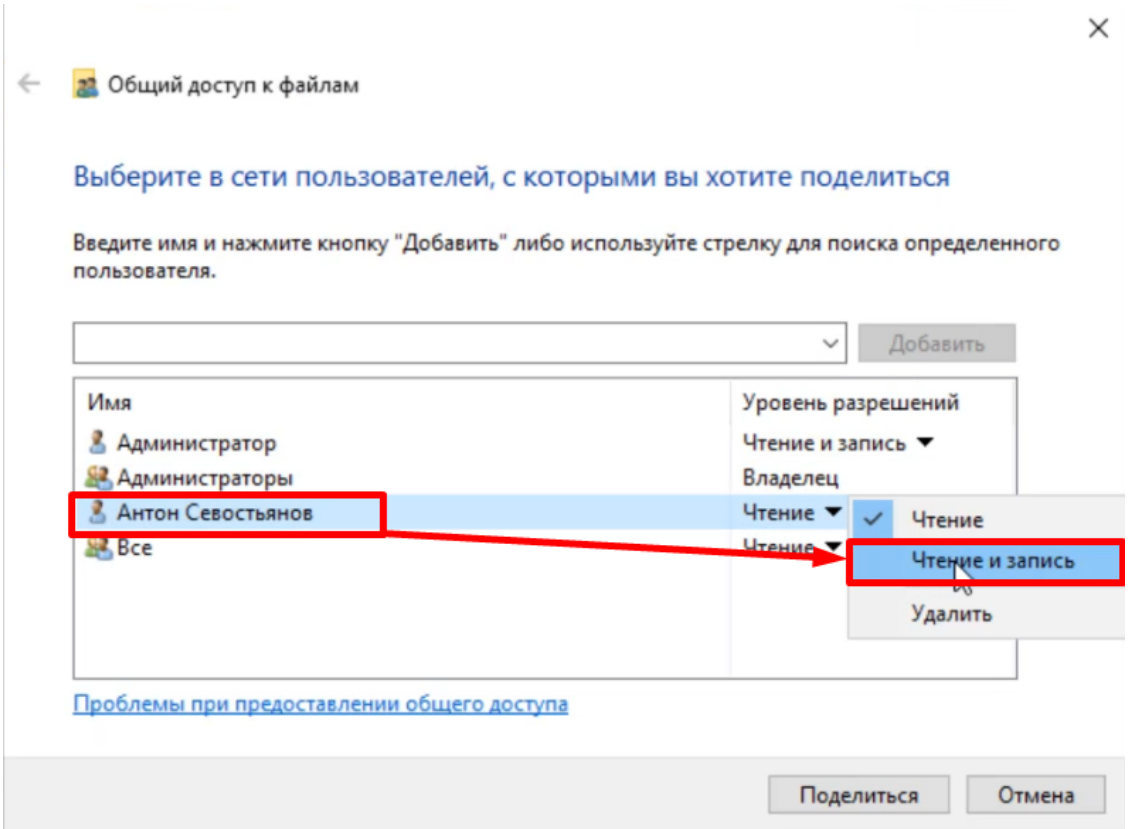
Допустим, перед нами стоит следующая задача. На сервере требуется создать папку Обмен, через которую, пользователи смогут обмениваться нужной им информацией между собой. Однако, нужно настроить права доступа таким образом, чтобы у каждого пользователя был отдельный ресурс с полными правами, а остальные могли только просматривать файлы на этом ресурсе.

В общем, создаем папку ОБМЕН на сервере, а внутри неё отдельную папку для каждого пользователя (sysadmin и buhgalter).

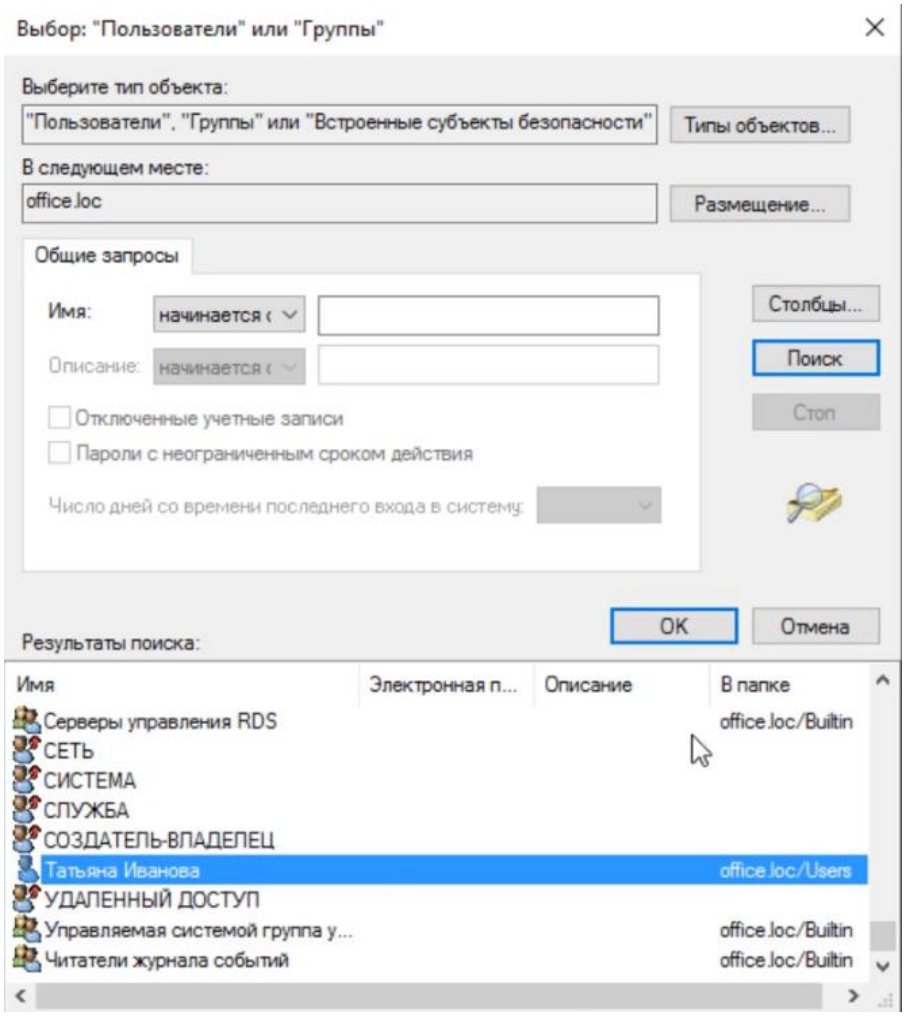
Папке обмен, разрешим всем доступ только для чтения (**ОБМЕН \ ПКМ \ Свойства \ Доступ \ Общий доступ \ Все \ Добавить \ Чтение**)



Папке sysadmin дадим полный доступ только для пользователя sysadmin или Севостьянов Антон (**sysadmin \ ПКМ \ Свойства \ Доступ \ Общий доступ \ Поиск пользователей \ Дополнительно \ Тип объекта «Пользователи» \ Поиск \ Севостьянов Антон \ ОК \ Чтение и запись \ Общий доступ**)



Папке buhgalter дадим полный доступ только для пользователя buhgalter или Иванова Татьяна (**buhgalter \ ПКМ \ Свойства \ Доступ \ Общий доступ \ Поиск пользователей \ Дополнительно \ Тип объекта «Пользователи» \ Поиск \ Иванова Татьяна \ ОК \ Чтение и запись \ Общий доступ**)



И теперь посмотрим, что будет выдаваться на стороне клиента:

Windows-7 – buhgalter – может копировать и просматривать любые документы, однако, удалять и изменять только в папке Обмен \ buhgalter

Windows-10 – sysadmin - может копировать и просматривать любые документы, однако, удалять и изменять только в папке Обмен \ sysadmin

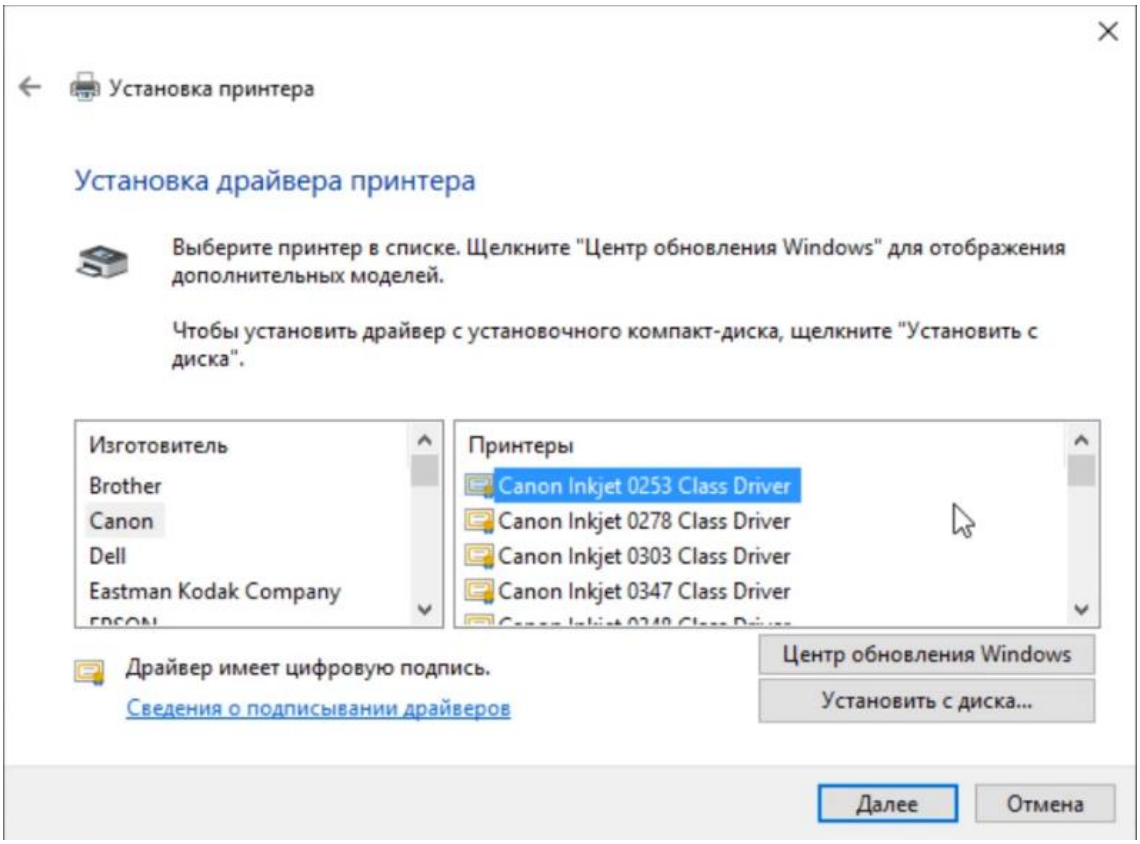
Таким образом, в зависимости от поставленной задачи, вы можете управлять правами доступа к ресурсам сети.

Но, это самая примитивная настройка, в Windows Server можно круто распределять права и работать с файловым сервером.

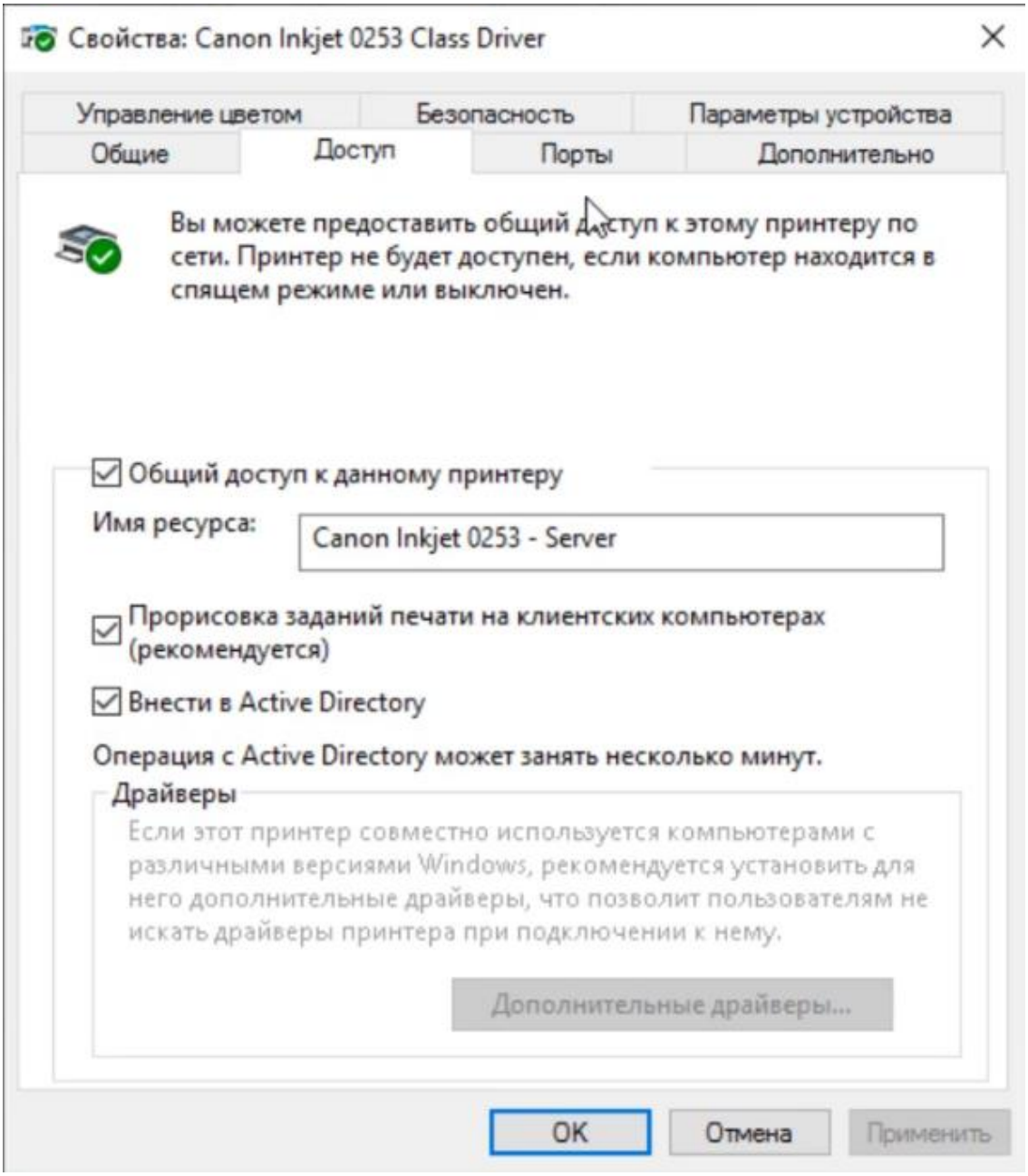
Настройка общего доступа к принтерам

Ни одна компания не может обойтись без принтера, поэтому в этом разделе разберемся как предоставлять общий доступ к принтерам.

Так как у меня нет физического принтера, я настрою что-то типа виртуального, т.е. на самом деле он не подключен, но в системе он отображаться будет. Этого будет достаточно чтобы разобраться с процессом предоставления и управления доступом к принтеру (**Панель управления \ Устройства и принтеры \ Добавление принтера \ Необходимый принтер отсутствует в списке \ Локальный \ LPT \ Canon \ Не предоставлять общий доступ, его мы настроим вручную**)

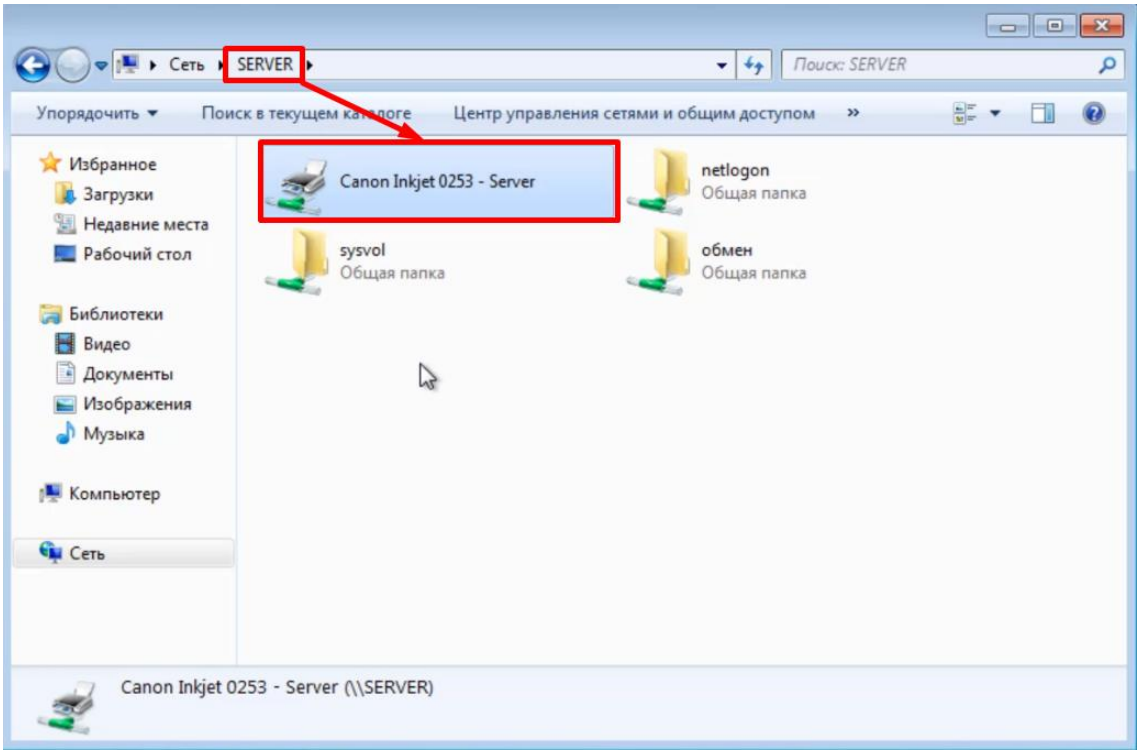


Выполним настройку доступа (**Устройства и принтеры \ ПКМ \ Свойства принтера \ Доступ \ Общий доступ,** Внести в Active Directory, чтобы мы могли его видеть в каталоге, дальше это рассмотрим при подключении принтера к клиентскому компьютеру **\ Безопасность \ Разрешить управление принтером и управление документами,** часто бывает так, что что-то пошло не так и пользователю нужно отменить печать и если мы не укажем данный доступ, то они не смогут это сделать)

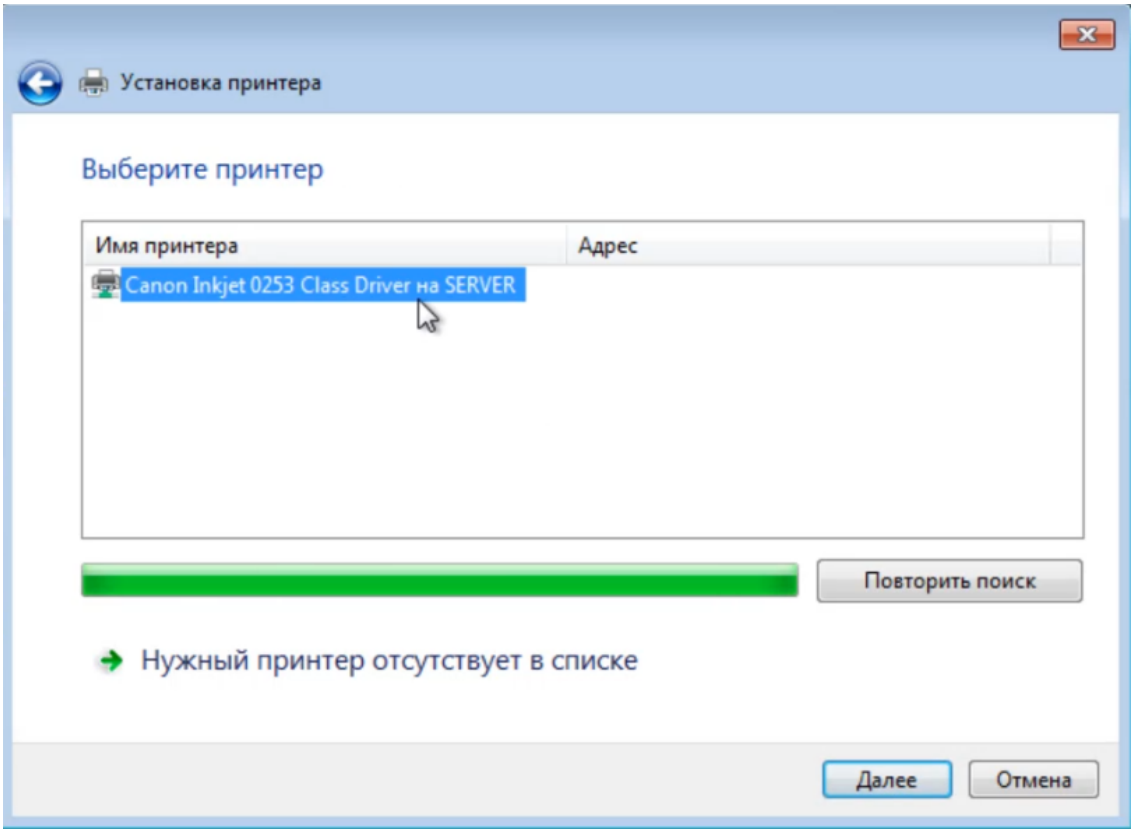


Теперь попробуем подключить принтер к клиентской машине. Это можно сделать двумя способами:

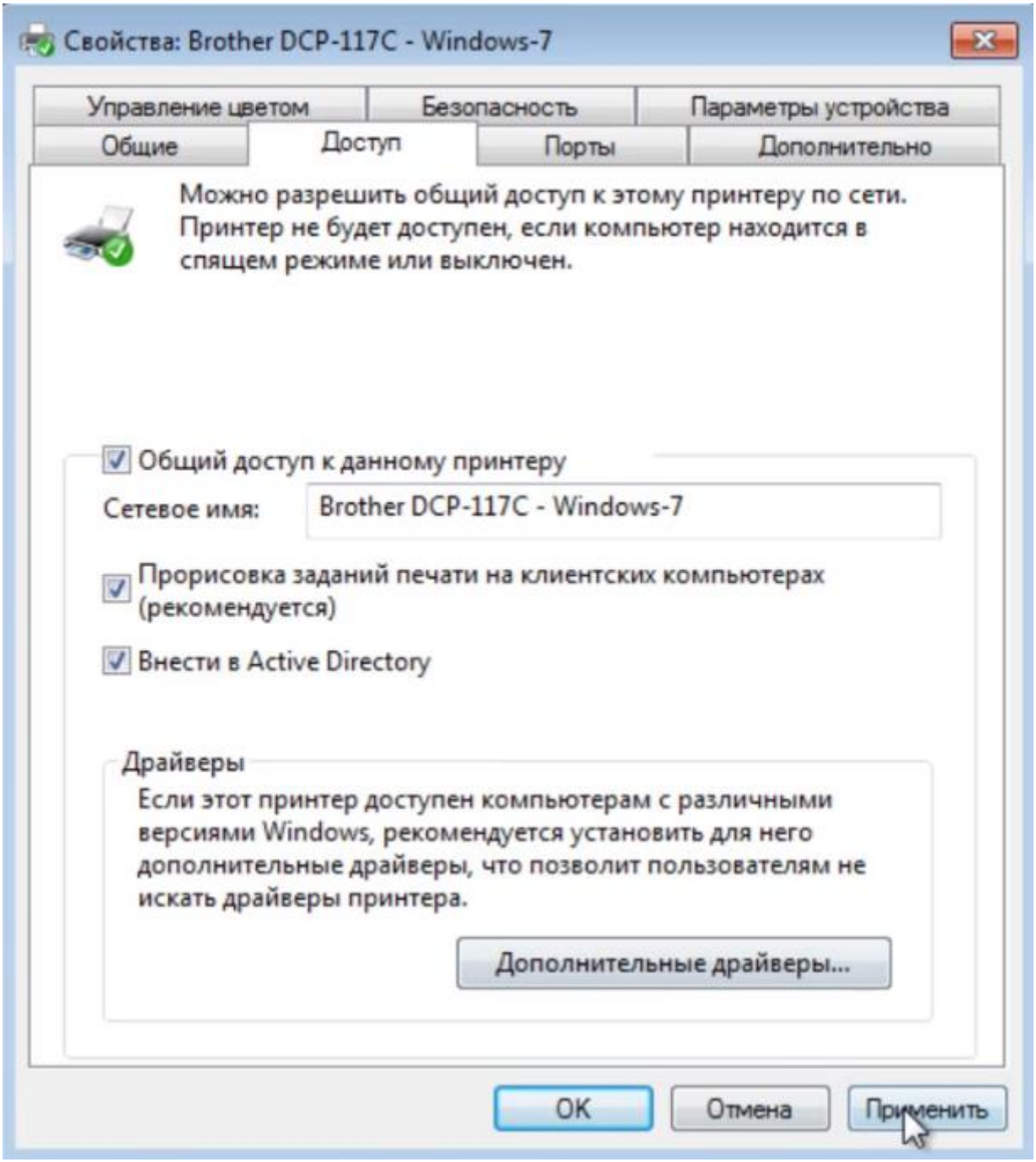
1) Заходим в сетевое окружение на компьютер к которому подключен принтер и который предоставляет общий доступ к нему **\ ПКМ \ Подключить**



2) **Панель управления \ Устройства и принтеры \ ПКМ \ Добавить принтер \ Добавить сетевой принтер \ Далее**



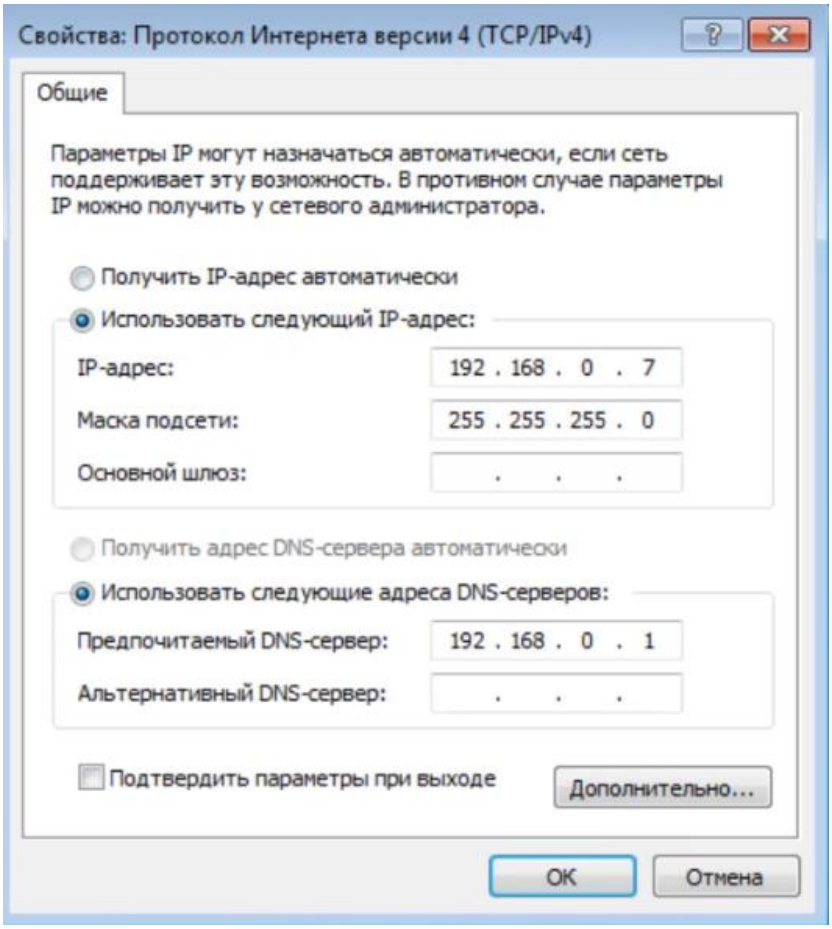
Таким же образом мы можем предоставить доступ к принтеру который подключен к обычной рабочей станции (**Панель управления \ Устройства и принтеры \ ПКМ \ Добавить принтер \ Локальный \ LPT \ Brother \ Не предоставлять общий доступ \ ПКМ \ Свойства принтера \ Доступ \ Общий доступ, Внести в Active Directory \ Безопасность \ Разрешить управление принтером и управление документами \ Применить**)



На другом компьютере подключаем нужный нам принтер.

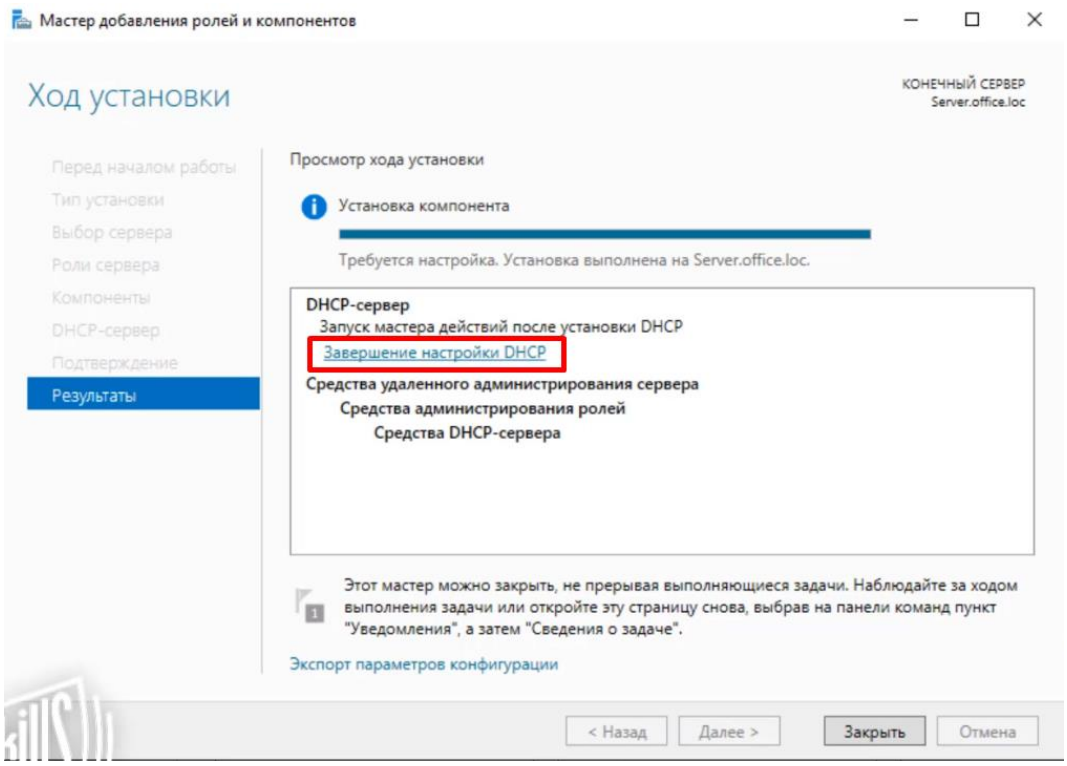
Настройка DHCP сервера

Как вы помните для того, чтобы настроить компьютер для работы в сети, нам требовалось вручную указать сетевые настройки (**Центр управления сетями и общим доступом \ Подключение по локальной сети \ Свойства \ Протокол интернета версии 4 \ Свойства**)

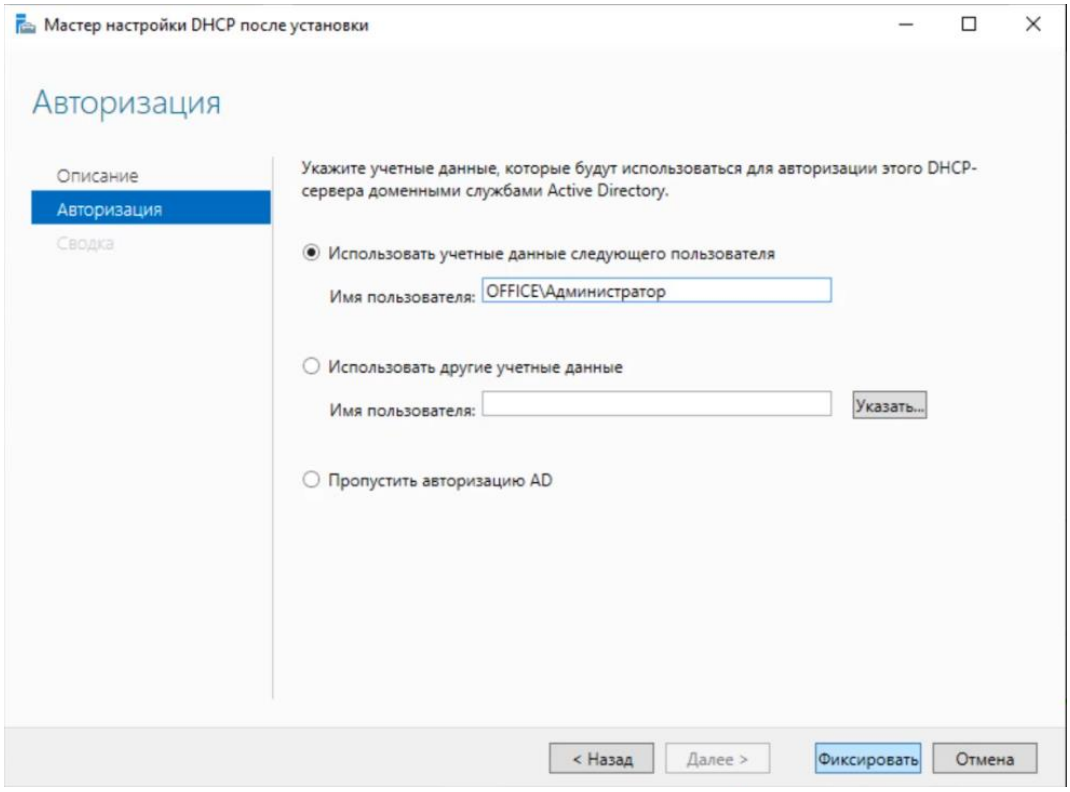


Для того чтобы не выполнять эти настройки вручную, а, чтобы система автоматически получала соответствующие настройки сети. Нужно поднять службу **DHCP**, что в расшифровке **D**ynamic **H**ost **C**onfiguration **P**rotocol или протокол динамической конфигурации хоста.

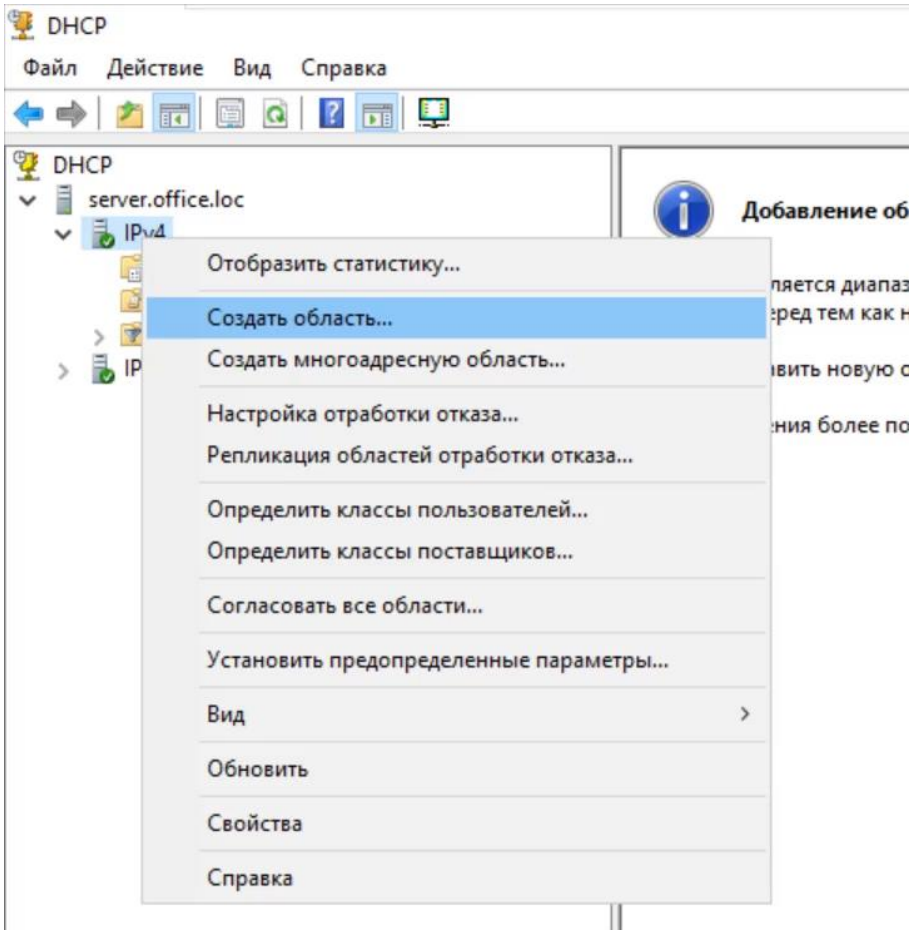
Перед настройкой DHCP сервера потребуется добавить роль DHCP для нашего сервера (**Диспетчер серверов \ Управление \ Добавить роли и компоненты \ Далее \ Далее \ Далее \ DHCP сервер \ Добавить компоненты \ Далее \ Средства удаленного администрирования сервера \ Средства администрирование ролей \ Средства DHCP сервера \ Далее \ Далее \ Установить \ Установка выполнена \ Завершение настройки DHCP**



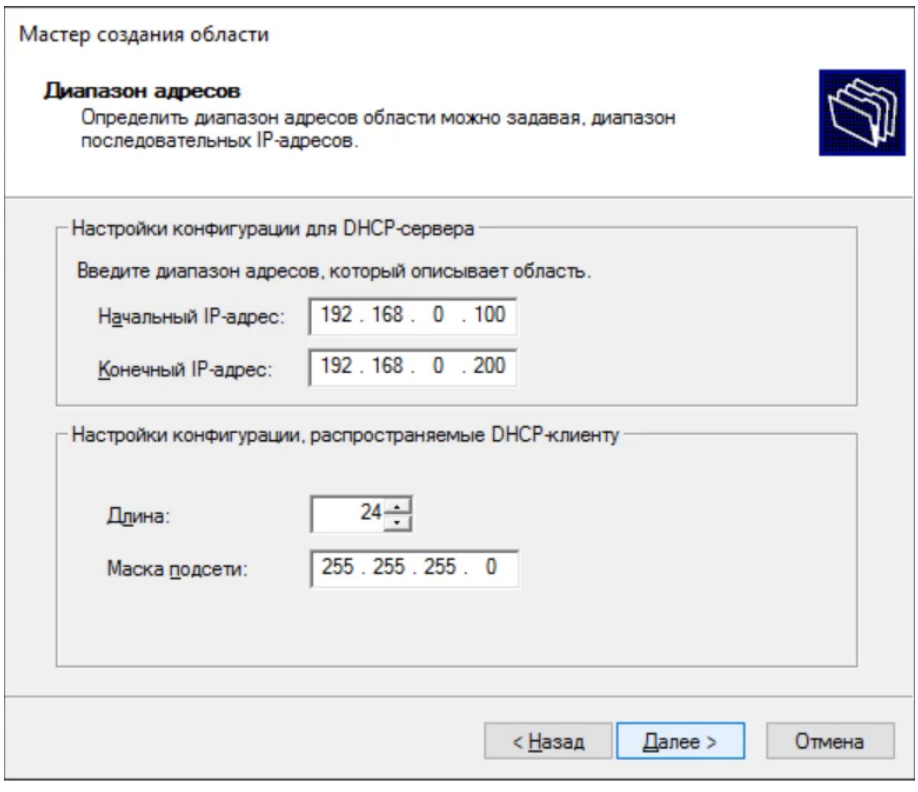
Авторизация \ Office\администратор \ Фиксировать \ Закрыть



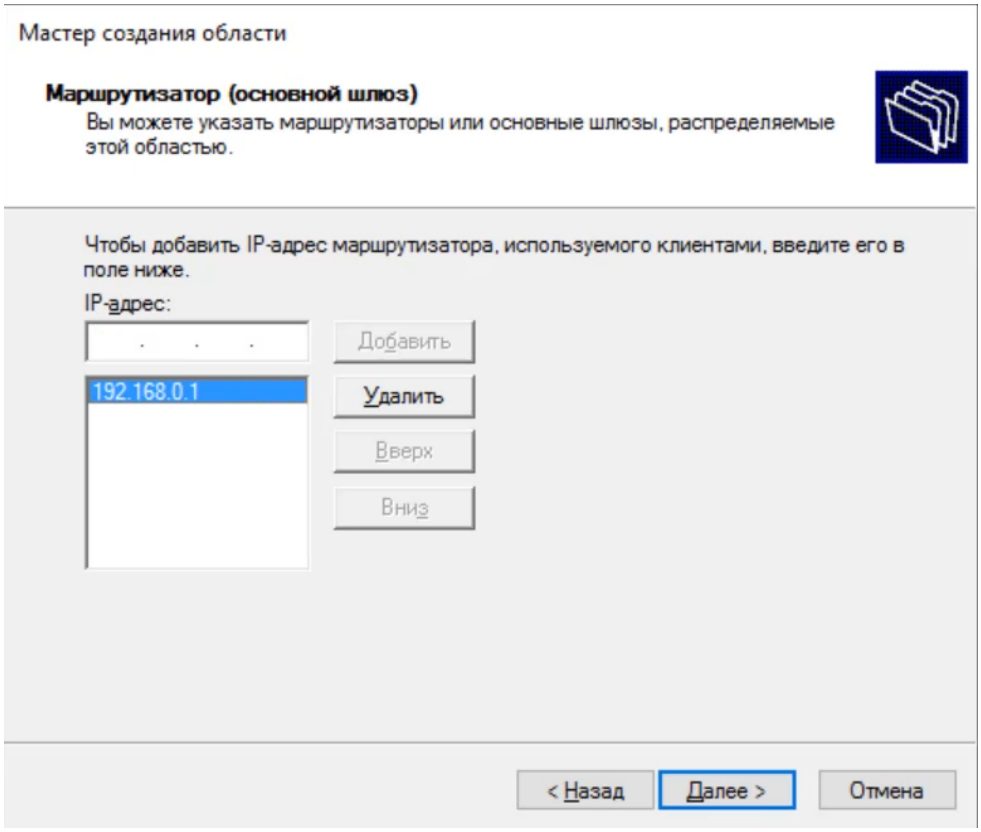
Настроим DHCP (**Диспетчер серверов \ Средства \ DHCP \ IPv4 \ ПКМ \ Создать область**



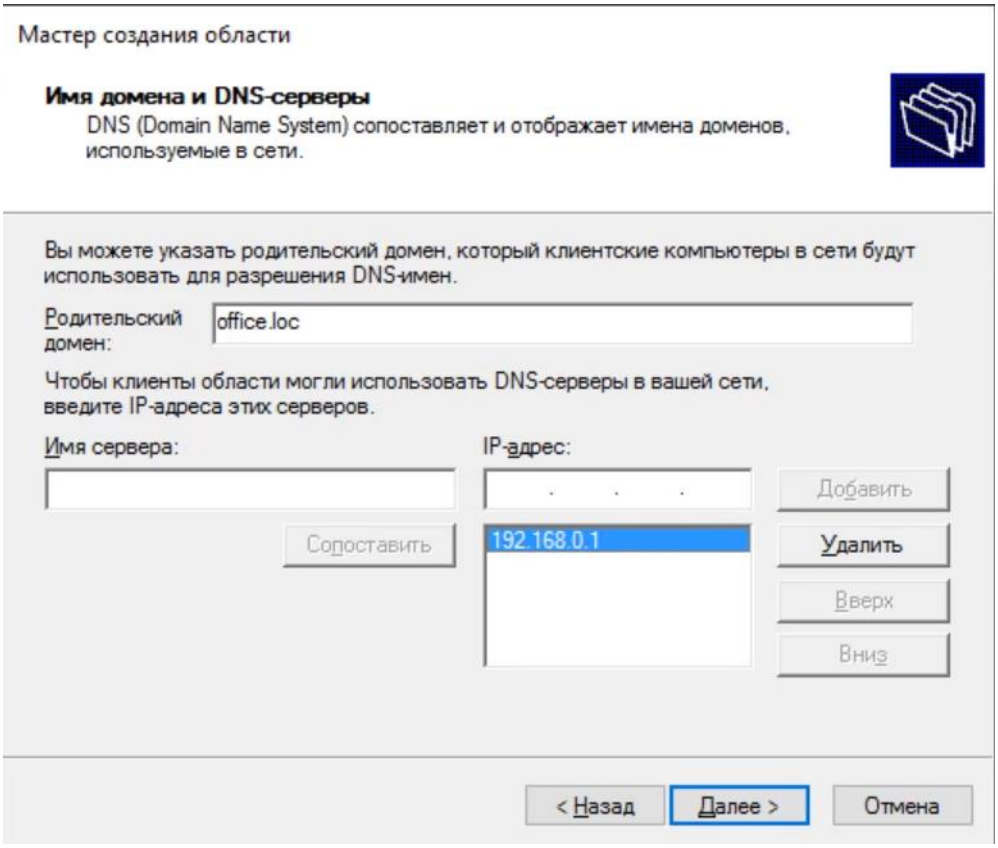
Далее \ Имя \ Рабочие станции, так как указанные далее настройки будут применяться к рабочим станциям **\ Настройки конфигурации DHCP сервера**



Далее \ Без исключений \ Далее \ Далее \ Да, настроить параметры сейчас \ Маршрутизатор 192.168.0.1, этот параметр используется для подключение рабочих станций к сети интернет через наш сервер, настраивать мы его будем позже, но уже сейчас укажем в настройках DHCP

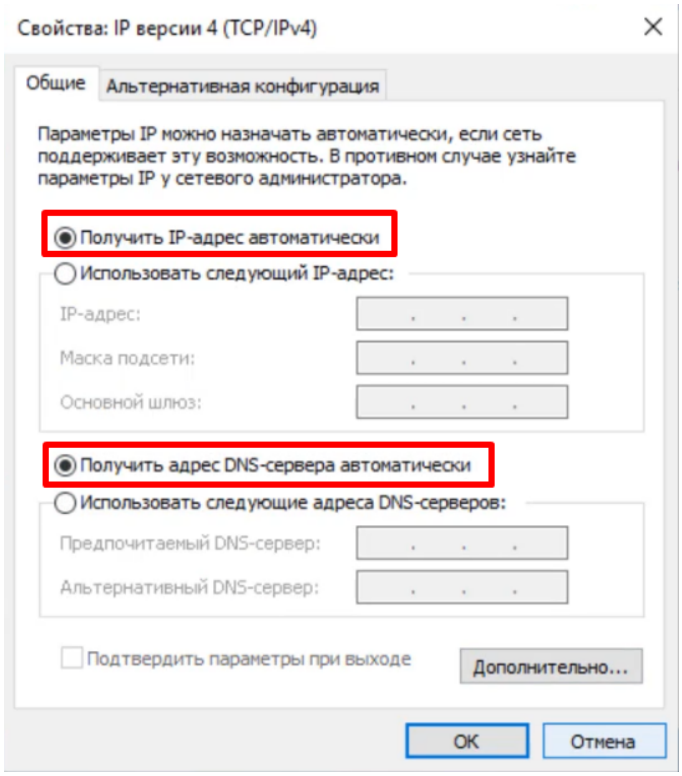


DNS у нас свой 192.168.0.1

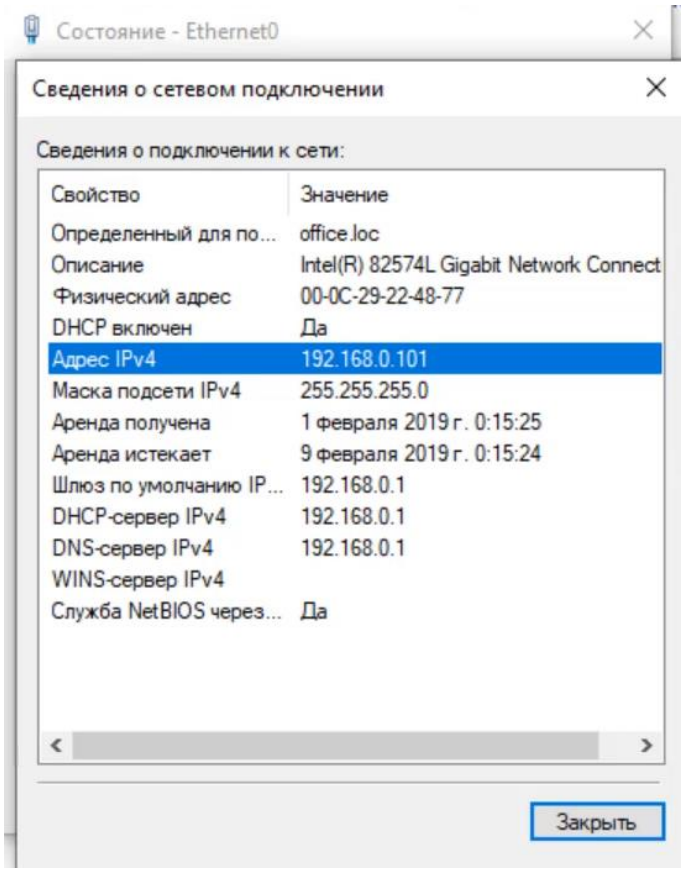


Далее \ WINS не будем использовать \ Да, я хочу активировать эту область \ Готово

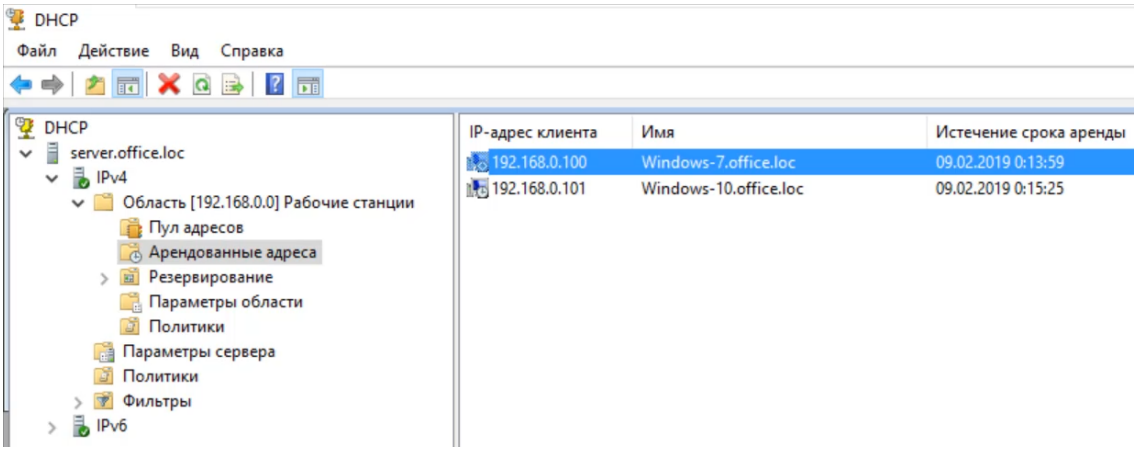
Проверим работу, для этого на клиентской машине в свойствах сетевого подключения IPv4 укажем получить автоматически.



Отключим и подключим сетевое подключение на рабочей станции, чтобы вновь выполнить запрос на получение IP адреса или перезагрузим компьютер.



Все ОК, так же можем посмотреть в настройках DHCP что был выдан в аренду данный IP адрес. Аналогичным образом указываем на остальных рабочих станциях автоматическое получение параметров сети.



Таким образом, DHCP сервер исключает возможность присваивания двум машинам одного IP адреса, так как он проверяет, какие адреса уже выдавались.

Хотя, в ситуации, если компьютер долго не включался и у него адрес был прописан вручную, то DHCP может подумать, что данный адрес никому не присвоен и назначить автоматически. А когда компьютер включат, то произойдет конфликт IP адресов, но, это уже исключения, которые не так часто встречаются.

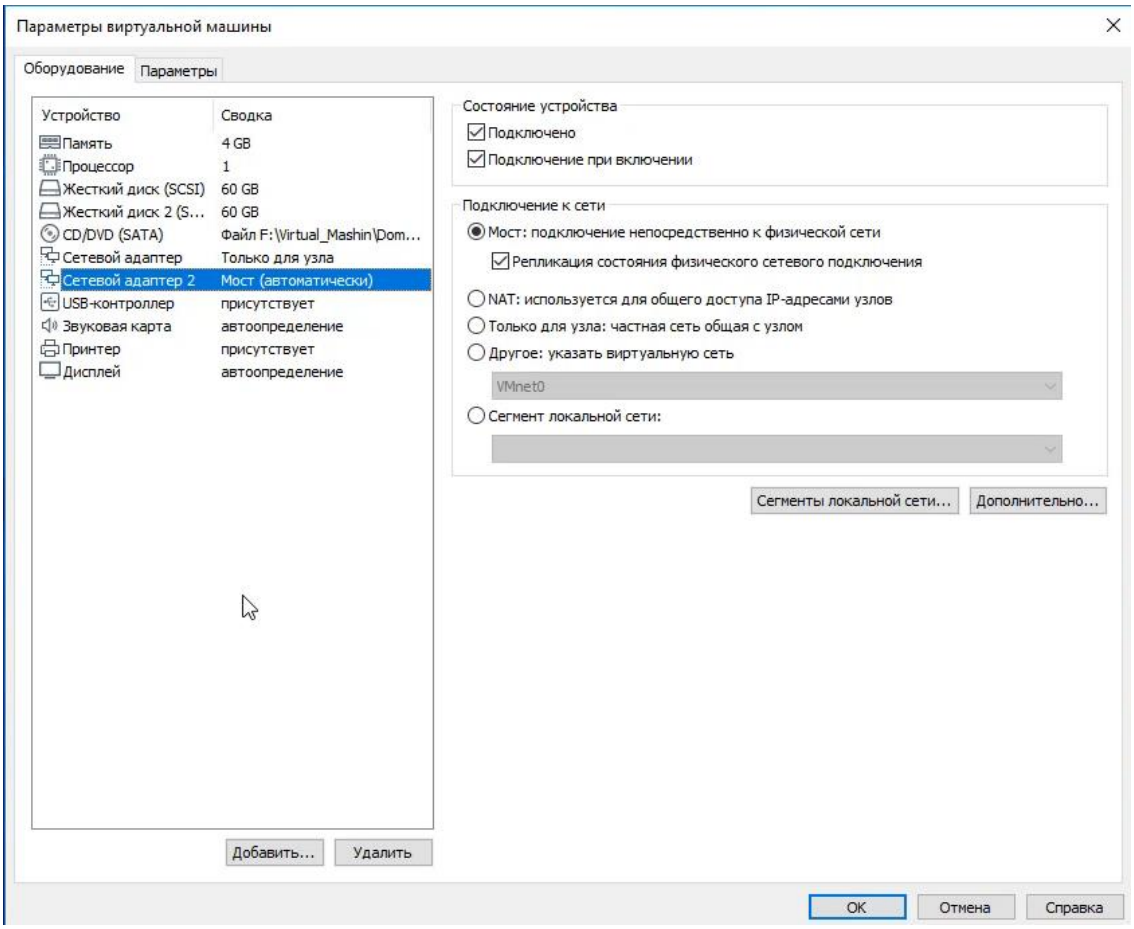
Настройка маршрутизатора (NAT)

Какая современная организация может обойтись без интернета, да никакая, поэтому разберемся с вопросом подключения нашей сети к Интернету. Несмотря на то, что мы все будем выполнять в виртуальной среде, в реальной сети настройки будут выполняться аналогично.

И первым делом нам необходимо подключить Интернет к серверу, а через него будем раздавать Интернет на остальные рабочие станции. Это позволит, используя специализированные программы, контролировать доступ в сеть Интернет.

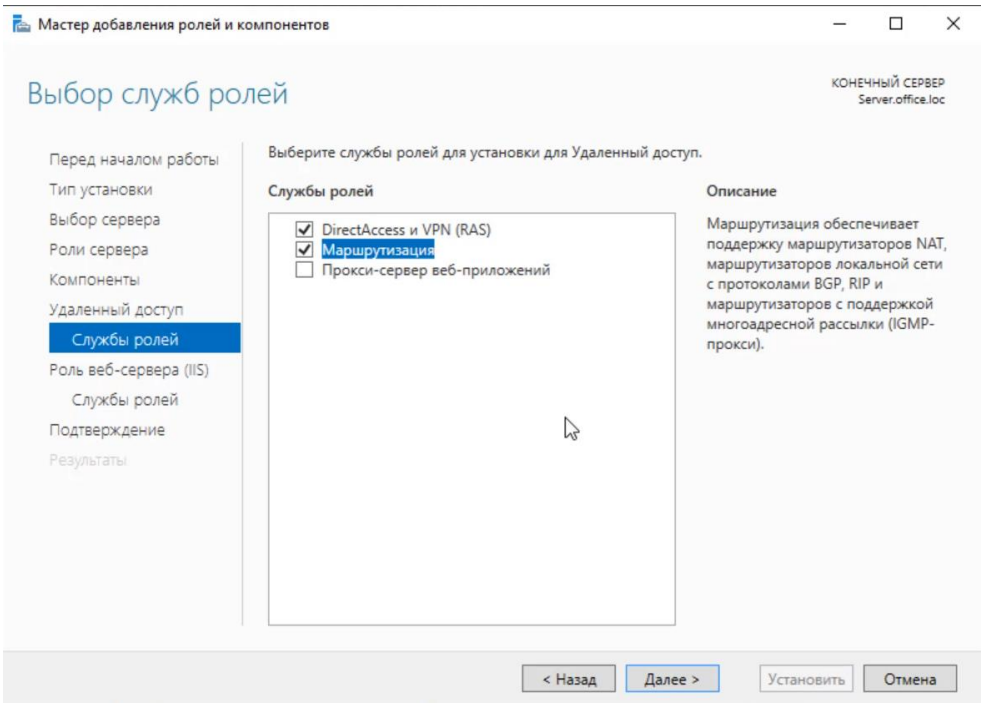
Как правило, провайдер дает выделенную линию, а вы уже подключаете их кабель к своему оборудованию, в данном случае, мы будем подключать его к серверу Windows Server 2025.

Для этого, нам потребуется добавить виртуальную сетевую карту, которая будет смотреть в Интернет (**Виртуальная машина \ Параметры \ Оборудование \ Добавить \ Сетевой адаптер \ Далее \ Мост,** данный вариант подключения предоставляет доступ в вашу физическую сеть, а значит интернет виртуальная машина будет брать с роутера **\ Готово**)

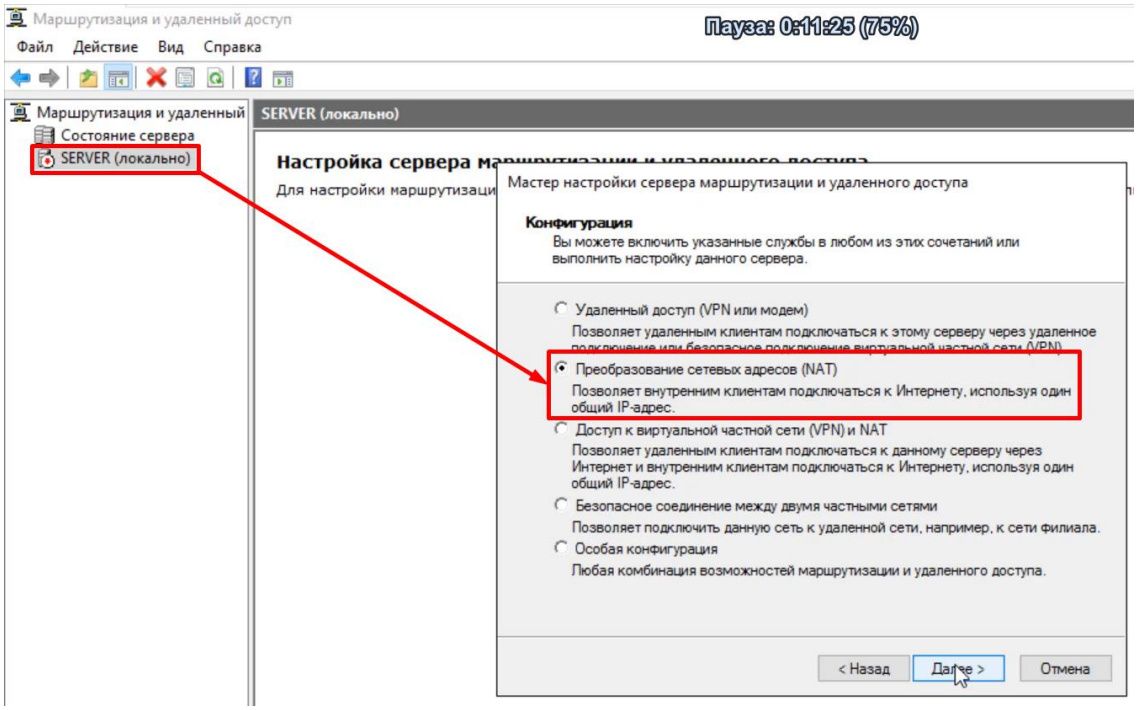


Отключим обновления, чтобы потом они не выносили мозг, но после настройки нужно их включить обратно (**Службы \ Отключить службу Центр обновления Windows**).

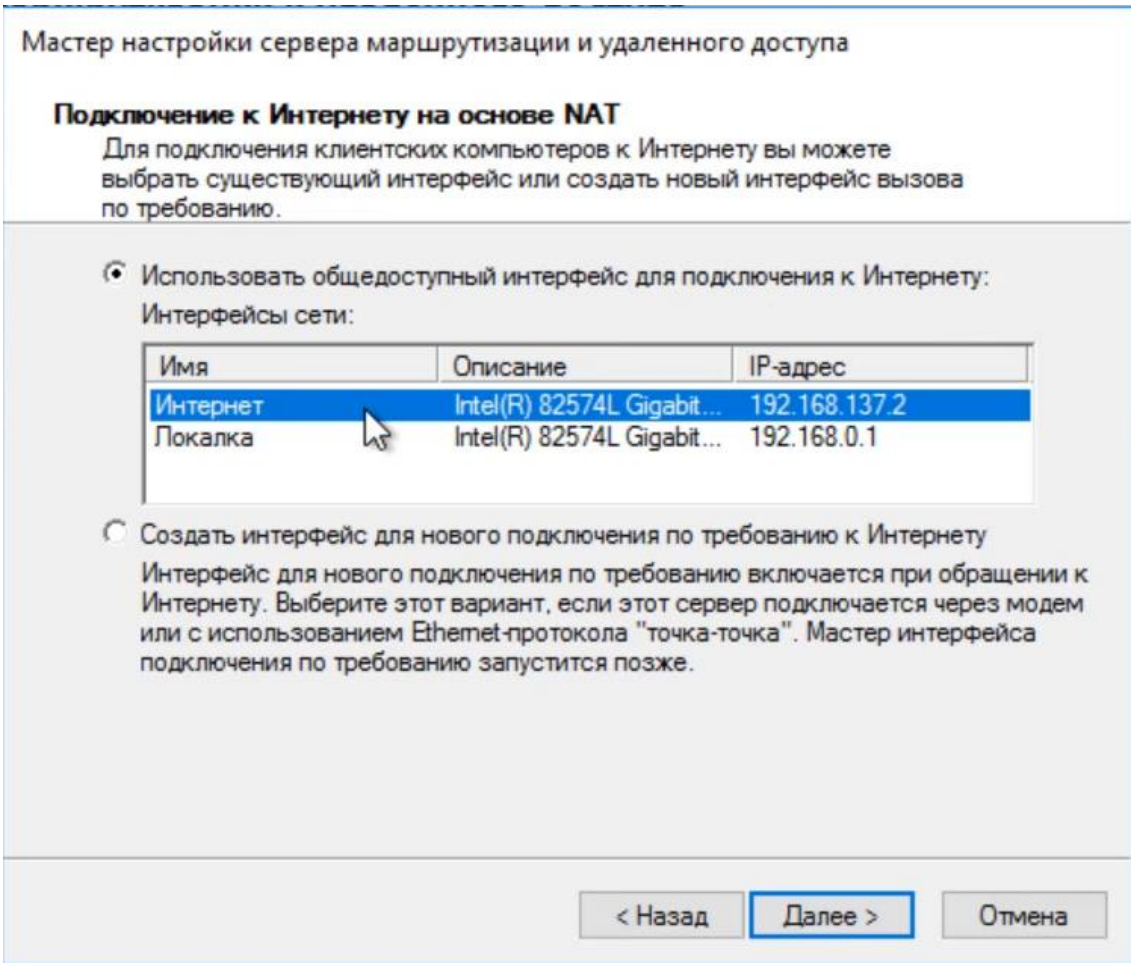
Теперь нам нужно поднять роль маршрутизатора на сервере, чтобы через него можно было раздавать интернет на рабочие станции (**Диспетчер серверов \ Управление \ Добавить роль \ Удаленный доступ \ Далее \ Далее \ Маршрутизация \ Установить \ Закрыть \ Перезагрузиться**)



Настроим маршрутизацию (**Диспетчер серверов \ Средства \ Маршрутизация и удаленный доступ \ SERVER \ ПКМ \ Настроить и включить маршрутизацию и удаленный доступ \ Далее \ Преобразование адресов NAT**

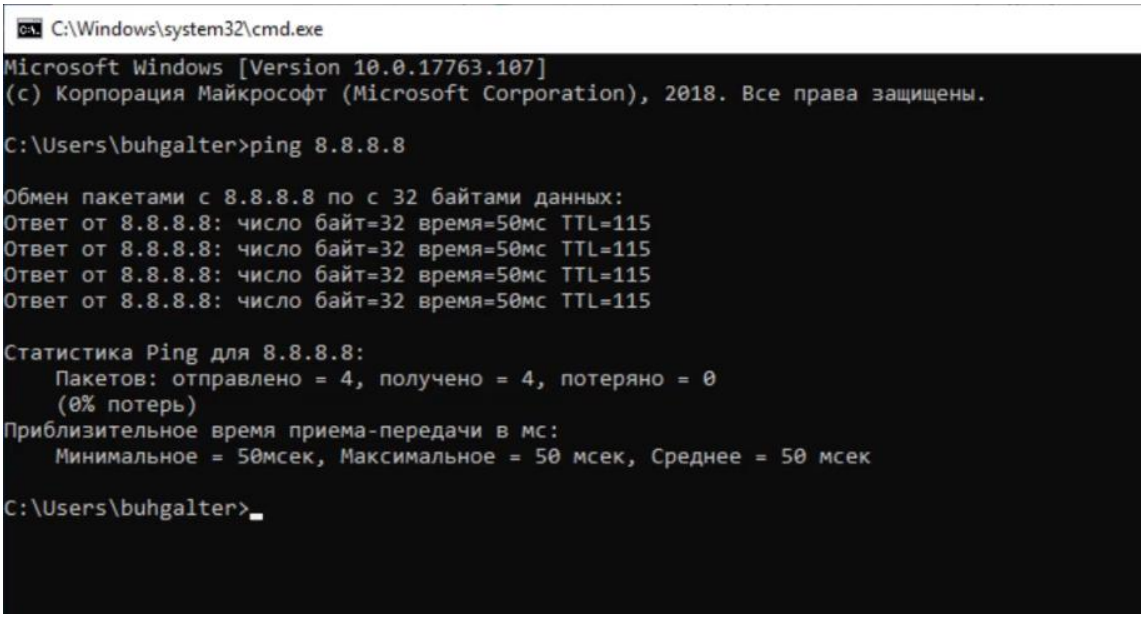


Выбираем сетевую карту, которая подключена к интернету \ Далее \ Готово)



Адрес маршрутизатора в DHCP мы уже настроили ранее, поэтому интернет на рабочих станциях должен появиться автоматически.

Проверяем на рабочих станциях появился ли интернет.

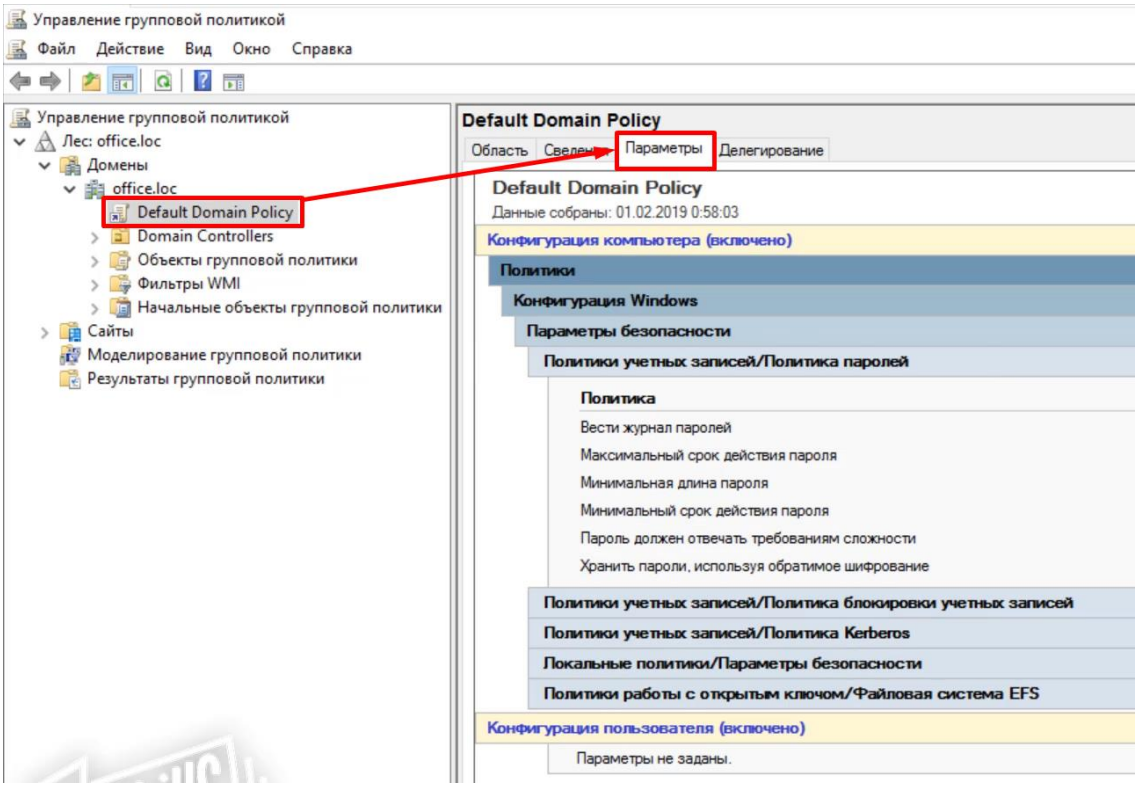


Настройка групповой политики (GPO)

Для того, чтобы облегчишь жизнь системному администратору в Windows Server были разработаны групповые политики. Суть работы которых заключается в том, чтобы можно было определенные настройки применить ко всем или определенным компьютерам в домене. Что позволяет в считанные минуты настроить рабочее пространство пользователя и систему безопасности.

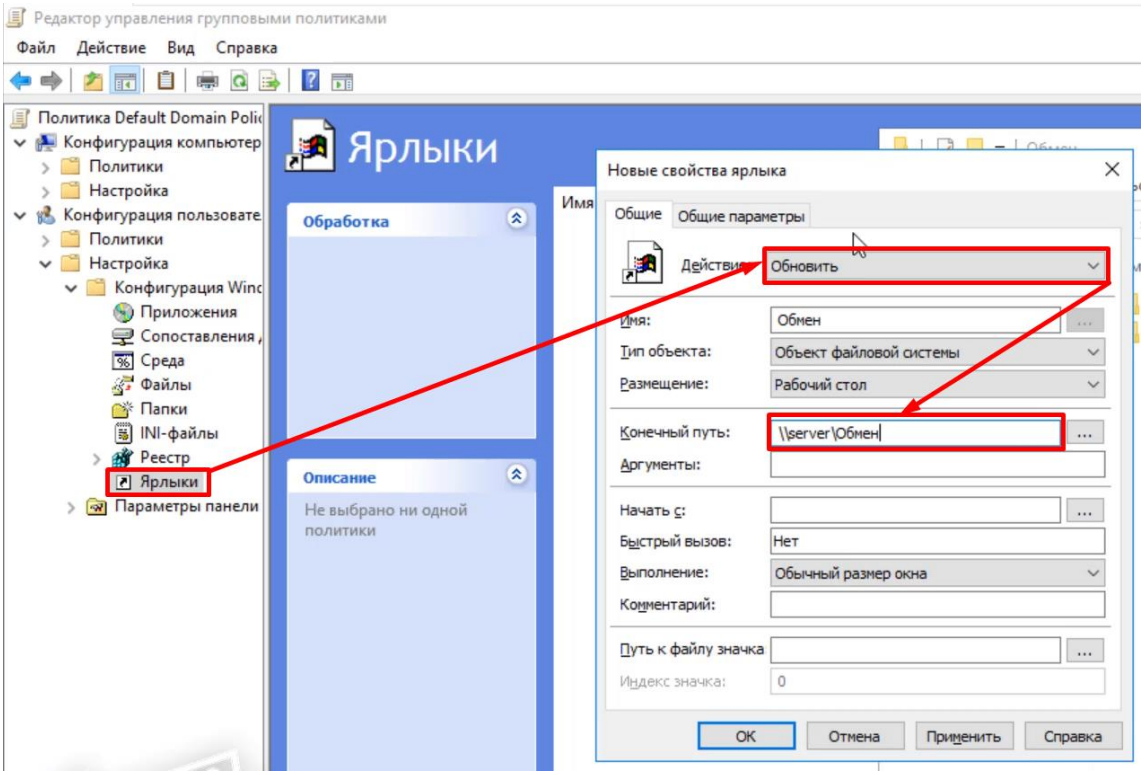
Давайте попробуем у всех пользователей в домене, на рабочем столе сделать ярлык для сетевого ресурса «Обмен», чтобы им не приходилось его постоянно искать. (**Диспетчер серверов \ Средства \ Управление групповой политикой \ Пуск \ Администрирование \ Управление групповой политикой \ Default Domain Policy** – групповая политика домена по умолчанию. Изменения, которые мы будем вносить в эту политику, будут применяться ко всем компьютерам в домене. Поэтому, следует с осторожностью относиться к данной политике.

Параметры – здесь создается отчет, какие параметры на данный момент уже настроены в политике

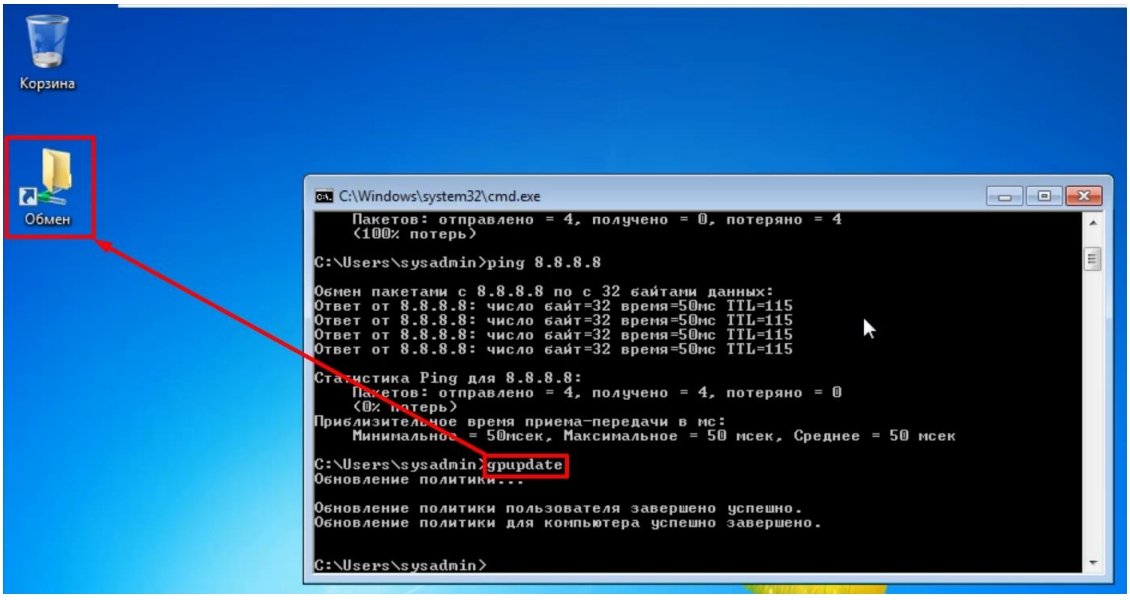


Так как мы не вносим серьезные изменения, а всего лишь прописываем ярлык, то можно сделать это и в политике для домена по умолчанию. В иных случаях, рекомендуется создать отдельную политику, применить её к определенным компьютерам, для тестирования, а уже потом применять для всех компьютеров.

\ Параметры – здесь создается отчет, какие параметры на данный момент уже настроены в политике **\ ПКМ \ Изменить \ Конфигурация пользователя \ Настройка \ Конфигурация Windows \ Ярлыки \ ПКМ \ Создать \ Ярлык \ Действие: Обновить \ Имя: Обмен \ Размещение: Рабочий стол; Конечный путь: \\server\0БМЕН \ ОК**).



Теперь, у всех пользователей в домене OFFICE на рабочем столе появится ярлык Обмен, который ведет на общий сетевой ресурс на сервере. Это можно проверить, перезагрузив компьютер или выполнив команду gpupdate. Данная команда обновляет политику на конечной рабочей станции. Данная команда работает не всегда, так как для некоторых задач требуется перегрузить компьютер. Но, для такой мелочи как создание ярлыка она вполне подойдет.



Подводим итоги...

Принимай мои поздравления, ты все таки осилил этот «талмуд» ☺

Есть ты выполнял все на практике, то в результате у тебя получился мощный домашний полигон, в котором ты сможешь тестировать абсолютно любые технологии.

Так что, смотри какие требования предъявляются к интересующей тебя вакансии и внедряй это в тестовой среде, чтобы с уверенность сказать на собеседовании, что ты с этим работал!!!

А если ты хочешь пройти обучение системному администрированию под моим руководством, то буду рад тебя видеть на курсе «Комплексное обучение системному администрированию»

Вот как проходит обучение у нас:

Комплексное обучение системному администрированию проходит в следующей форме:

✓ обучение проходит в онлайн школе IT-Skills;

✓ все видеоуроки записаны и вы можете приступить к изучению в любой момент после оплаты курса;

✓ изучаете в удобное для вас время, но, чтобы изучить программу в 3 месяца нужно каждый день изучать по 2 видеоурока (примерно 30 минут контента);

✓ сопровождение и ответы на вопросы во время обучения;

✓ закрытый чат для студентов;

✓ проводим стримы для студентов с целью разбора различных вопросов.

P.S. Узнать подробное описание курса, вплоть до каждого видеоурока и или оформить бесплатный демо-доступ, можно по этой ссылке

Если у тебя возникнут какие-либо вопросы по поводу обучения, напиши мне по контактам ниже и я расскажу все более подробно:

Telegram: https://t.me/it_skills_bot

VK: http://vk.me/club34272024

Желаю удачи и достижения поставленных целей, уверен, что мои материалы в этом помогут. ;-)