Постановка задач:

1. Подготовить виртуальные машины к настройке;
2. Настроить прямую и обратную зону DNS сервера;
3. Протестировать прямую и обратную зону;
4. Подключить ПК к домену;
5. Создать настроить подразделения, группы и пользователей;
6. Создать необходимые папки и дать пользователям доступ к ним;
7. Протестировать авторизацию пользователей и доступ к папкам;
8. Защитить работу.

Входные данные:

1. Получить вариант задания у преподавателя. Уточнить наименование папок, пути к ним и пользователей с правами доступа к ним;
2. Домен – первая буква имени и фамилия полностью через точку указать группу. (Пример: Василий Пупкин, vpupkin.idb20-**.local);
3. IP Адрес – В виде числа подсети использовать число дня рождения. (Пример: 17.1.2000. – 10.10.17.1, 192.168.17.5);
4. Подразделения выбираются самостоятельно, минимум 3 подразделения.
5. Пользователи выбираются самостоятельно, минимум 6 пользователей.

Контрольные вопросы:

1) Для чего предназначены прямые и обратные запросы поиска?
2) Опишите назначение компонентов DNS: зона, сервер имен, доменное пространство имен.
3) Назовите основные типы зон и их назначение.
4) Назовите основные правила именования доменов.
5) Какова максимально допустимая длина имени домена?
6) Опишите различия между рабочей группой и доменом.
7) Перечислите известные Вам встроенные учетные записи пользователей и групп пользователей домена и опишите их назначение.
8) Можно ли установить Active Directory без установки DNS?
9) Как устанавливается и удаляется Active Directory?
10) Как происходит проверка прав доступа пользователя к ресурсам в ОС Windows?

Критерии оценки практической (лабораторной) работы:

«5» (отлично): выполнены все задания практической (лабораторной) работы, обучающийся четко и без ошибок ответил на все контрольные вопросы.

«4» (хорошо): выполнены все задания практической (лабораторной) работы; обучающийся ответил на все контрольные вопросы с замечаниями.

«3» (удовлетворительно): выполнены все задания практической (лабораторной) работы с замечаниями; обучающийся ответил на все контрольные вопросы с замечаниями.

«2» (не зачтено): обучающийся не выполнил или выполнил неправильно задания практической (лабораторной) работы; обучающийся ответил на контрольные вопросы с ошибками или не ответил на контрольные вопросы.

Теоретическая часть

Домен – область (ветвь) иерархического пространства доменных имён сети Интернет, которая обозначается уникальным доменным именем.

Доменное имя – символьное имя домена. Должно быть уникальным в рамках одного домена. Полное имя домена состоит из имён всех доменов, в которые он входит, разделённых точками. Например, полное имя www.tu-bryansk.ru. (с точкой в конце) обозначает домен третьего уровня www, который входит в домен второго уровня tu-bryansk, который входит в домен .ru, который входит в корневой домен. Доменное имя служит для адресации узлов сети Интернет и расположенных на них сетевых ресурсов (веб-сайтов, серверов электронной почты, сетевых сервисов) в удобной для человека форме.

Доменная зона – совокупность доменных имён определённого уровня, входящих в конкретный домен. Например, зона ctam.tu-bryansk.ru. означает все доменные имена третьего уровня в этом домене. Термин «доменная зона» в основном применяется в технической сфере, при настройке DNS-серверов (поддержание зоны, делегирование зоны, трансфер зоны).

Для обеспечения уникальности и защиты прав владельцев доменные имена 1-го и 2-го (в отдельных случаях и 3-го) уровней можно использовать только после их регистрации, которая производится уполномоченными на то регистраторами. Сведения о владельце (администраторе) того или иного регистрируемого домена общедоступны. Их можно узнать, воспользовавшись службой «whois.

Домены верхнего уровня общего назначения:

.aero – для субъектов авиатранспортной индустрии;

.biz – только коммерческие организации;

.cat – для использования каталанским языковым и культурным сообществом;

.com – коммерческие организации (без ограничений);

.coop – кооперативы;

.edu – высшие учебные заведения, признаваемые в качестве таковых Департаментом образования США;

.info – информационные ресурсы (без ограничений);

.jobs – кадровые агентства;

.mobi – для продавцов и поставщиков мобильного контента и услуг, связанных с мобильной связью;

.museum – музеи;

.name – физические лица;

.net – организации, имеющие отношение к функционированию Интернета (без ограничений);

.org – некоммерческие организации (без ограничений);

.pro – сертифицированные профессионалы и смежные темы;

.travel – для субъектов туристического бизнеса.

Для удобства распределения и назначения доменных имен для каждой из стран были выделены собственные (в основном двухсимвольные) домены верхнего уровня. Правда, это вовсе не означает обязательную привязку серверов в данных доменных к их географическому расположению. Примеры доменов первого уровня для стран:

.au – Australia (Австралия);

.be – Belgium (Бельгия);

.ru – Russia (Россия);

.ua – Ukraine (Украина);

.uk – United Kingdom (Англия).

Первоначально преобразование между доменными и IP-адресами производилось с использованием специального текстового файла DHOSTS.TXT, который составлялся централизованно и обновлялся вручную на каждой из машин сети. С ростом сети возникла необходимость в эффективном, автоматизированном механизме, которым и стала DNS (Domain Name System) – система доменных имен.

Примечание – На самом деле на каждой сетевой машине имеется текстовый файл hosts (Windows – %windir%\system32\drivers\etc\hosts; *nix – /etc/hosts), в котором можно самостоятельно сопоставлять с некоторым IP-адресом доменные имена. Правда, эти действия валидны только для текущей машины.

Функции DNS. Существуют два принципиально разных способа идентификации хостов: с помощью имен и с помощью IP-адресов. Имя хоста удобно для людей в силу своей мнемоничности, а IP-адрес, являющийся компактной числовой величиной фиксированного размера, проще обрабатывать прикладными программами и маршрутизаторами. Для того чтобы установить связь между этими двумя идентификаторами, используется система доменных имен. DNS представляет собой, с одной стороны, базу данных, распределенную между иерархически структурированными серверами имен, и, с другой стороны, протокол прикладного уровня, организующий взаимодействие между хостами и серверами имен для выполнения операций преобразования. DNS функционирует на принципе делегирования полномочий. Каждая машина либо знает ответ на вопрос, либо знает, кого спросить. При правильном функционировании система замкнута, т. е. если запрошенная информация имеется у кого-либо, то она будет найдена и сообщена клиенту, либо, если вопрос не имеет ответа, клиент получит сообщение о невозможности получения ответа на вопрос.

Обратный DNS-запрос (Reverce DNS). DNS используется в первую очередь для преобразования символьных имён в IP-адреса, но он также может выполнять обратный процесс. Для этого используются уже имеющиеся средства DNS. Дело в том, что с записью DNS могут быть сопоставлены различные данные, в том числе и какое-либо символьное имя. Существует специальный домен in-addr.arpa., записи в котором используются для преобразования IP-адресов в символьные имена. Например, для получения DNS-имени для адреса 192.168.128.5 можно запросить у DNS-сервера запись 5.128.168.192.in-addr.arpa, и тот вернёт соответствующее символьное имя. Обратный порядок записи частей IP-адреса объясняется тем, что в IP-адресах старшие биты расположены в начале, а в символьных DNS-именах старшие (находящиеся ближе к корню) части расположены в конце. Одна из проблем состоит в том, что обратную зону можно выделить только на сеть класса A, B или C (на 16777216, 65536 или 256 адресов соответственно) и никак иначе (маски здесь не работают).

Разграничение доступа

Разграничение доступа заключается в том, чтобы каждому зарегистрированному пользователю предоставить возможности

беспрепятственного доступа к информации в пределах его полномочий и исключить возможности превышения этих полномочий. Для каждого пользователя устанавливаются его полномочия в отношении файлов, каталогов, логических дисков и других системных ресурсов.

Для распределения полномочий субъектов по отношению к объектам используется матричная модель доступа, рассмотренная в параграфе. Разграничение может осуществляться:

- по уровням секретности (секретно, совершенно секретно и т.п.). Пользователю разрешается доступ только к данным своего или более низких уровней. Защищаемые данные распределяются по массивам таким образом, чтобы в каждом массиве содержались данные одного уровня секретности;
- специальным спискам. При этом разграничении доступа для каждого элемента защищаемых данных (файла, программы, базы) составляется список всех тех пользователей, которым предоставлено право доступа к соответствующему элементу. Возможен обратный вариант, когда для каждого зарегистрированного пользователя составляется список тех элементов защищаемых данных, к которым ему предоставлено право доступа;
- матрицам полномочий.

При организации доступа к оборудованию существенное значение имеют идентификация и аутентификация пользователей, а также контроль и автоматическая регистрация их действий. Для опознания пользователя могут быть использованы пароли и индивидуальные идентификационные карточки, а для управления доступом к оборудованию такие простые, но эффективные меры, как отключение питания или механические замки и ключи для устройств.

Организация доступа обслуживающего персонала к устройствам информационной системы отличается от организации доступа пользователей тем, что устройство освобождается от конфиденциальной информации и отключаются все информационные связи. Техническое обслуживание и восстановление работоспособности устройств выполняются под контролем должностного лица.

По виду управления доступом системы разграничения разделяют:

- на системы с дискреционным управлением, позволяющим контролировать доступ поименованных субъектов (пользователей) к поименованным объектам (файлам, программам и т.п.) в соответствии с матрицей доступа. Контроль доступа применим к каждому объекту и каждому субъекту (индивиду или группе равноправных индивидов). Кроме того, имеется возможность санкционированного изменения

списка пользователей и списка защищаемых объектов, предусмотрены средства управления, ограничивающие распространение прав на доступ как для явных, так и для скрытых действий пользователя;

- мандатные системы. Для реализации мандатного принципа управления доступом каждому субъекту и каждому объекту назначаются классификационные метки, отражающие их уровень (уязвимости, категории секретности и т.п.) в соответствующей иерархии. Эти метки служат основой мандатного разграничения доступа:
- субъект может читать объект, только если иерархическая классификация в классификационном уровне субъекта не меньше, чем иерархическая классификация в классификационном уровне объекта, и неиерархические категории в классификационном уровне субъекта включают в себя все иерархические категории в классификационном уровне объекта,
- субъект осуществляет запись в объект, только если классификационный уровень субъекта в иерархической классификации не больше, чем классификационный уровень объекта в иерархической классификации, и все иерархические категории в классификационном уровне субъекта включаются в неиерархические категории в классификационном уровне объекта.

Обеспечивающие средства для системы разграничения доступа выполняют идентификацию и аутентификацию субъектов; регистрацию действий субъекта и его процесса; изменение полномочий субъектов и включение новых субъектов и объектов доступа; тестирование всех функций защиты информации специальными программными средствами и ряд других функций.

Учету подлежат создаваемые защищаемые файлы, каталоги, тома, области оперативной памяти и другие объекты. Для каждого события должна регистрироваться информация (субъект, дата и время, тип события и др.) с выдачей печатных документов соответствующего образца. Кроме того, может автоматически оформляться учетная карточка документа с указанием даты выдачи, учетных реквизитов, наименования, вида, шифра, кода и уровня конфиденциальности документа.

Особенности реализации системы. В системе разграничения доступа должен быть использован диспетчер, осуществляющий разграничение доступа в соответствии с заданным принципом разграничения. Разграничение доступа к информационным объектам осуществляется в соответствии с полномочиями субъектов. Основой такого разграничения является выбранная модель управления доступом, реализуемая диспетчером доступа. Диспетчер обеспечивает выполнение правил разграничения доступа субъектов к объектам доступа, которые хранятся в базе полномочий и характеристик доступа. Запрос на доступ субъекта к некоторому объекту

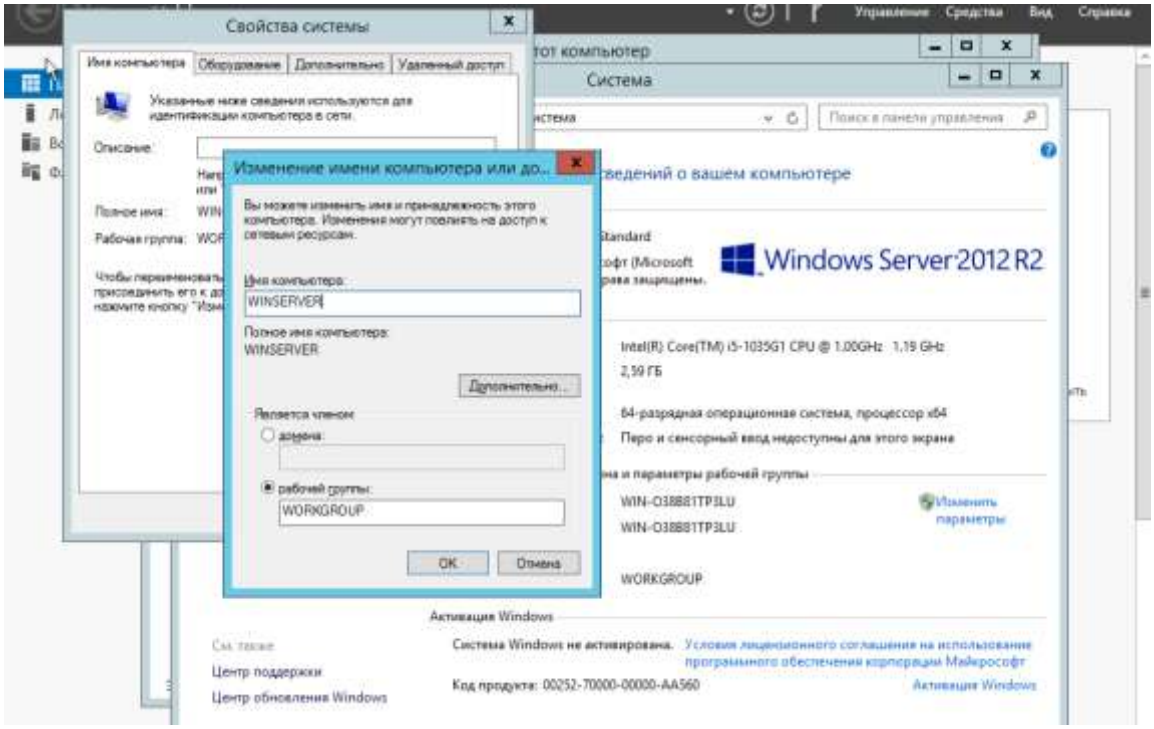
поступает в блок управления базой и регистрации событий. Полномочия субъекта и характеристики объекта анализируются в блоке принятия решений. По результатам анализа формируется сигнал разрешения или отказа в допуске ("Допустить", "Отказать"). Если число сигналов "Отказать" превысит заданный уровень (например, 5 раз), который фиксируется блоком регистрации, то блок принятия решений выдает сигнал "Несанкционированный доступ". На основании этого сигнала администратор системы безопасности может заблокировать работу субъекта для выяснения причины таких нарушений.

Подразделения (OU) в управляемом домене служб домен Active Directory Services (AD DS) позволяют логически группировать объекты, такие как учетные записи пользователей, учетные записи служб или учетные записи компьютеров. Затем можно назначить администраторов определенным подразделениям и применить групповую политику для применения целевых параметров конфигурации.

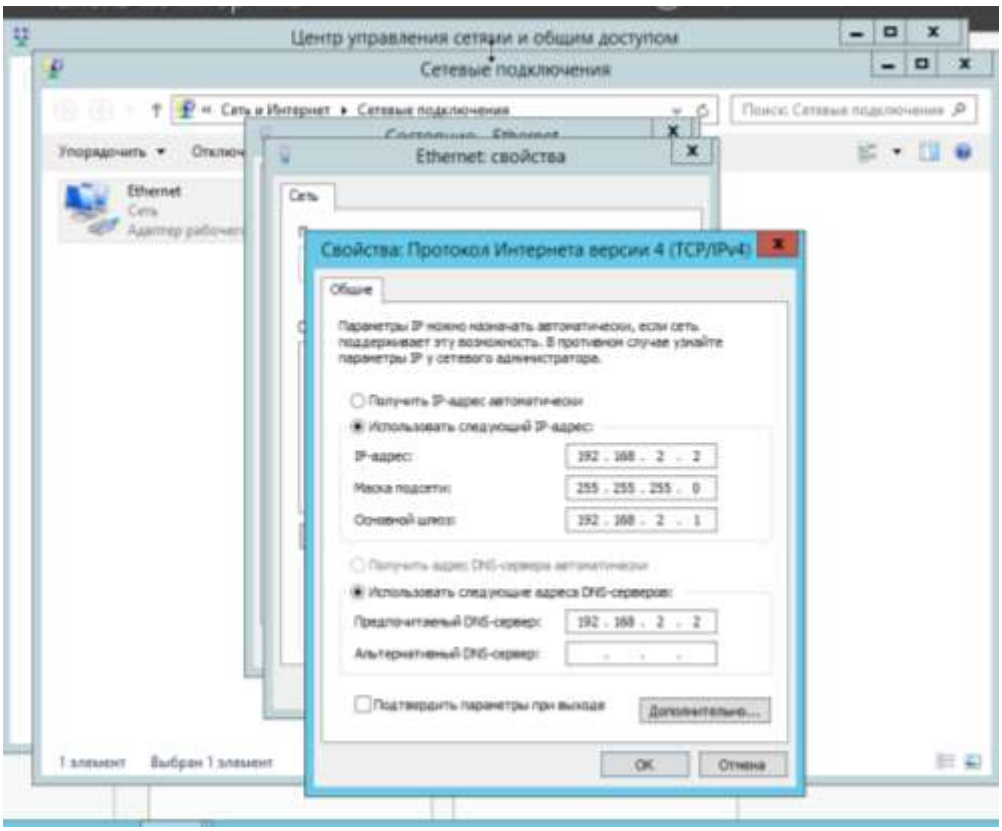
Подразделения (OU) в управляемом домене служб домен Active Directory Services (AD DS) позволяют логически группировать объекты, такие как учетные записи пользователей, учетные записи служб или учетные записи компьютеров. Затем можно назначить администраторов определенным подразделениям и применить групповую политику для применения целевых параметров конфигурации.

Практическая часть

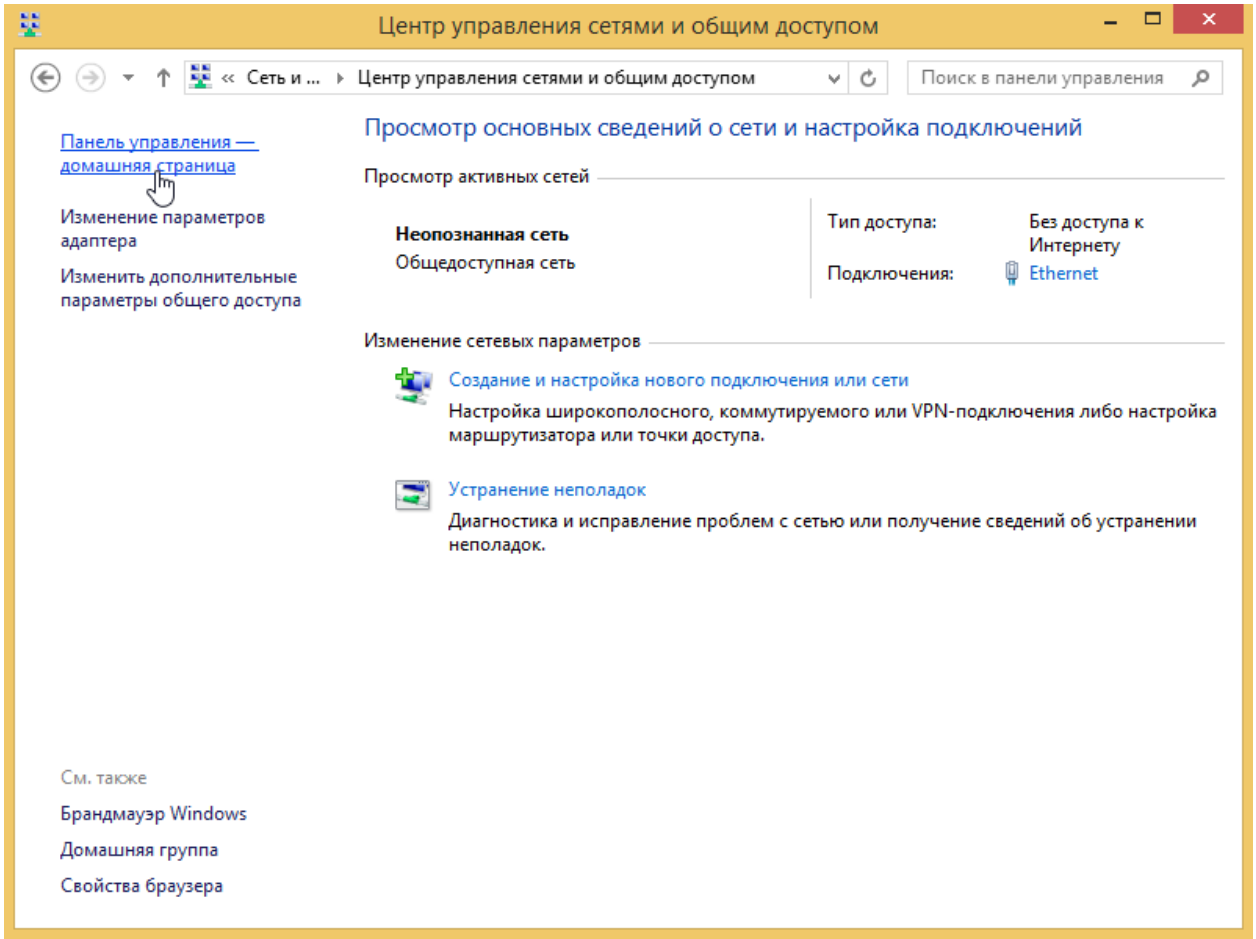
Первым делом необходимо переименовать имя сервера. Переходим в **Система, Изменить параметры**, **изменение имени компьютера или домена.** И указываем **Имя компьютера.**



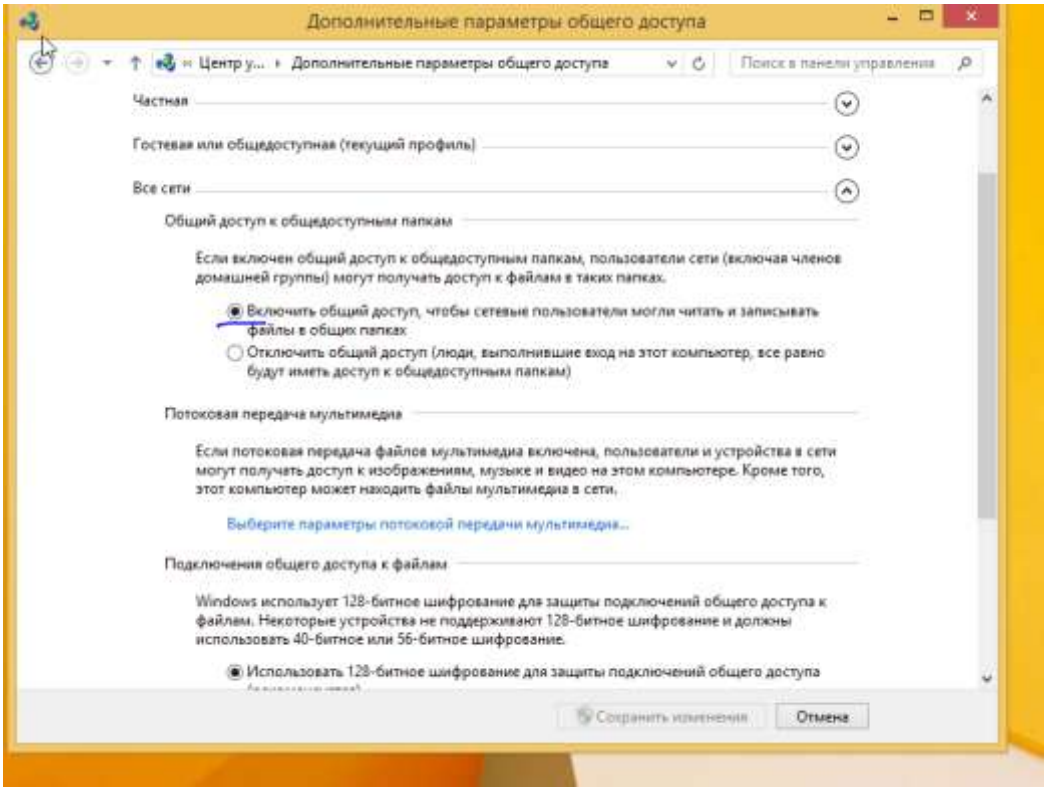
Далее необходимо назначить статический IP адрес. Статический IP адрес, необходим для настройки DNS и доменных зон**. Центр управления сетями и общий доступом**, **сетевые подключения**. Выбираем Сетевой адаптер и переходим в его свойства. Выбираем **IPv4** и прописываем статический IP.



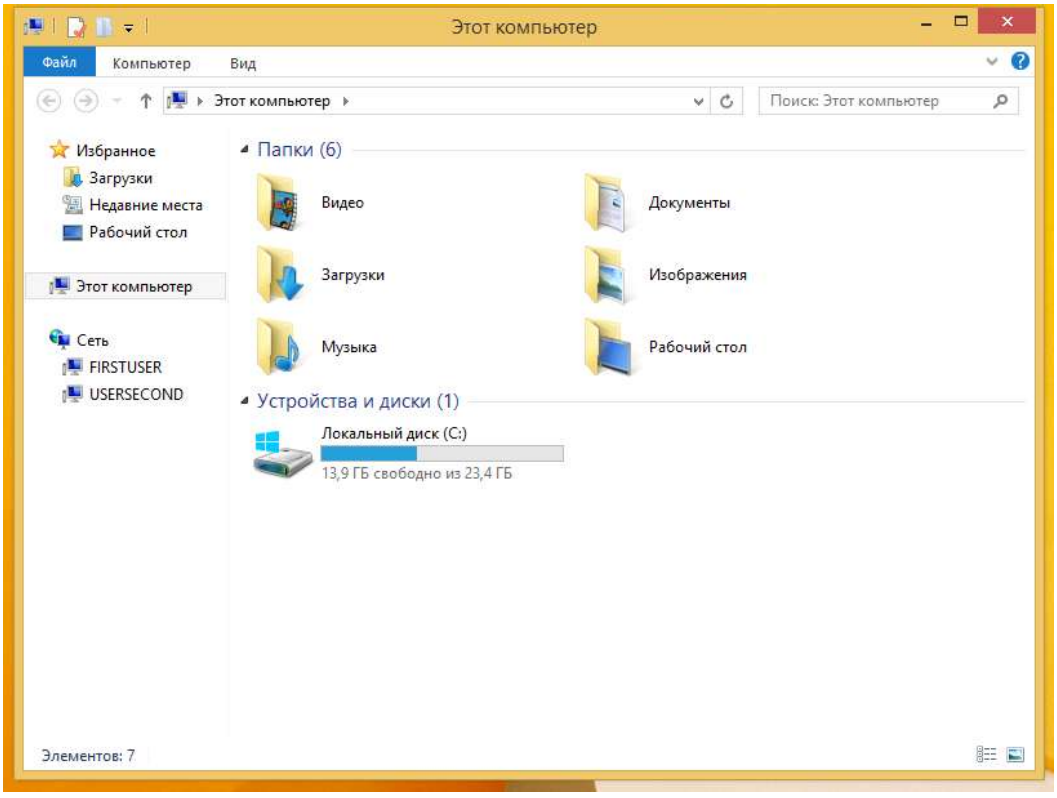
Далее рассмотрим одноранговую сеть. Переходим в **Центр управления сетями и общим доступом** и выбираем **Изменить дополнительные параметры общего доступа.**



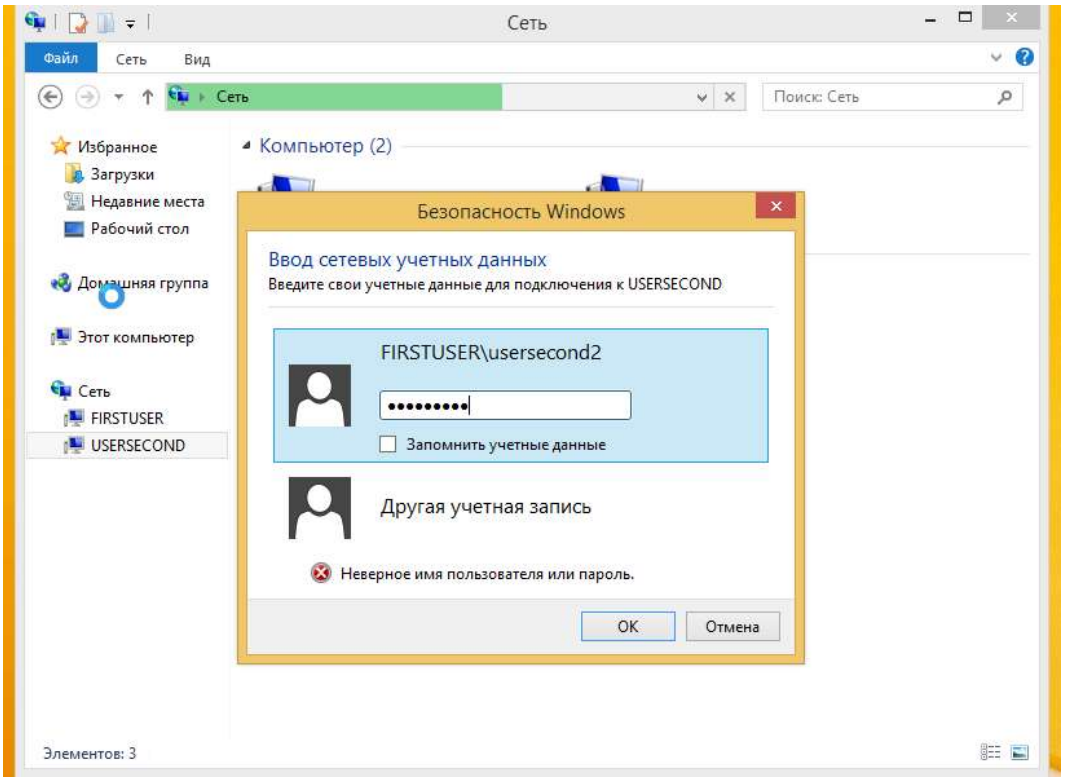
Далее необходимо выбрать в пункте **Все сети, Включить общий доступ, чтобы сетевые пользователи могли читать и записывать файлы в общих папках.**



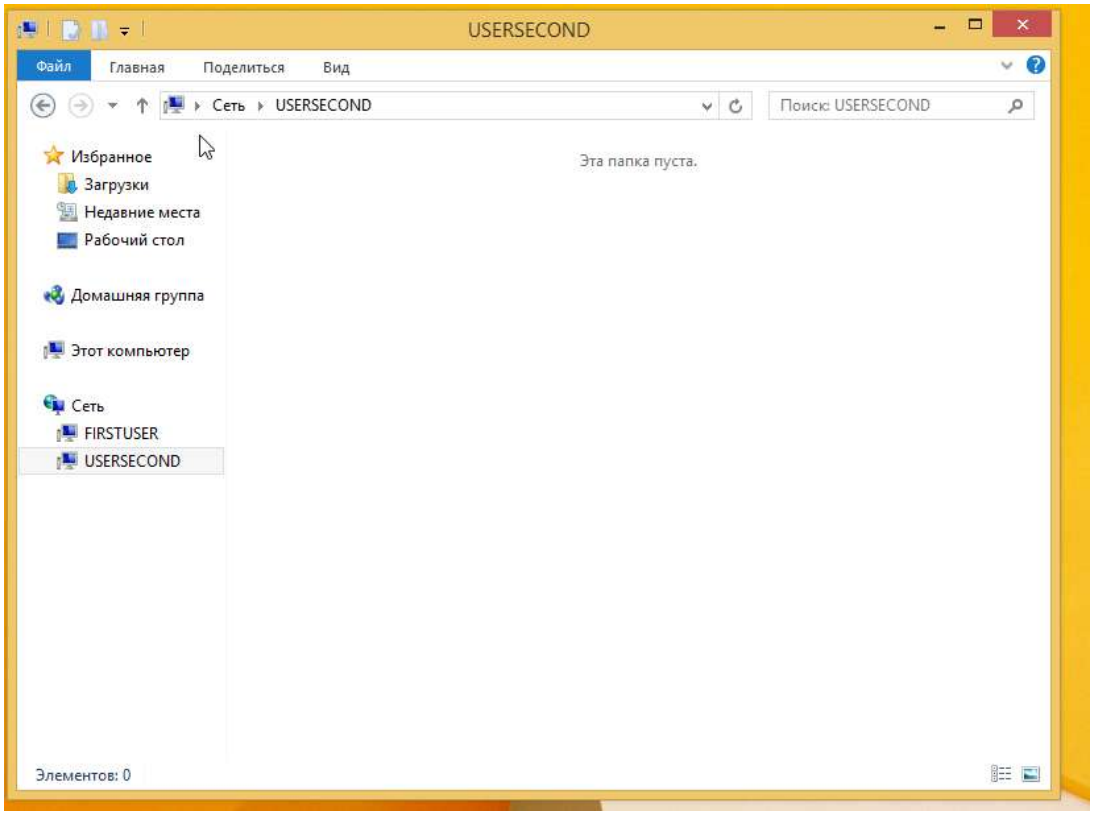
Далее переходим в **Этот компьютер**, выбираем пункт **Сеть** и необходимо увидеть компьютере в сети.



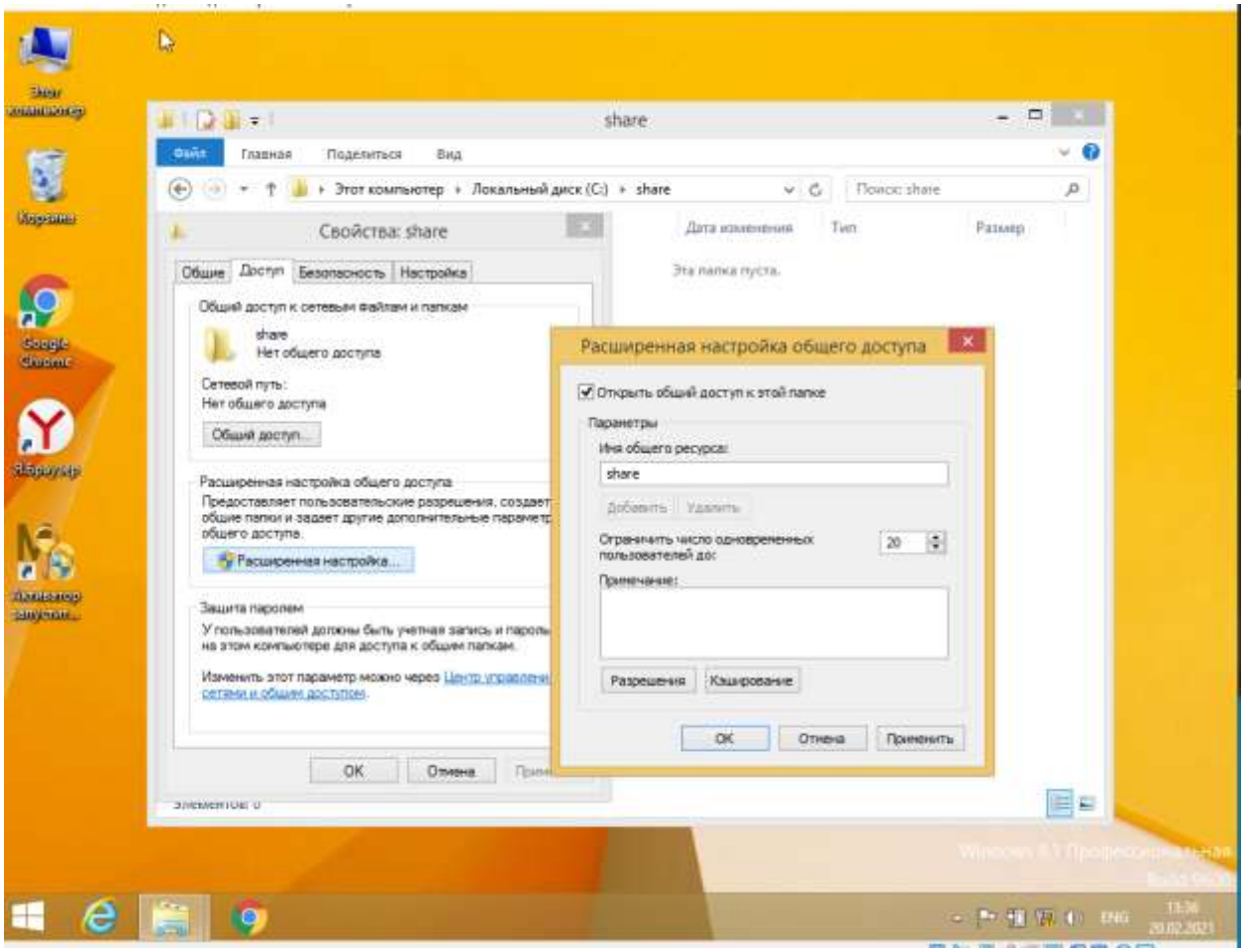
Далее в пункте **Сеть**, выбираем необходимый ПК. Далее вводим логин и пароль пользователя к которому подключаемся.



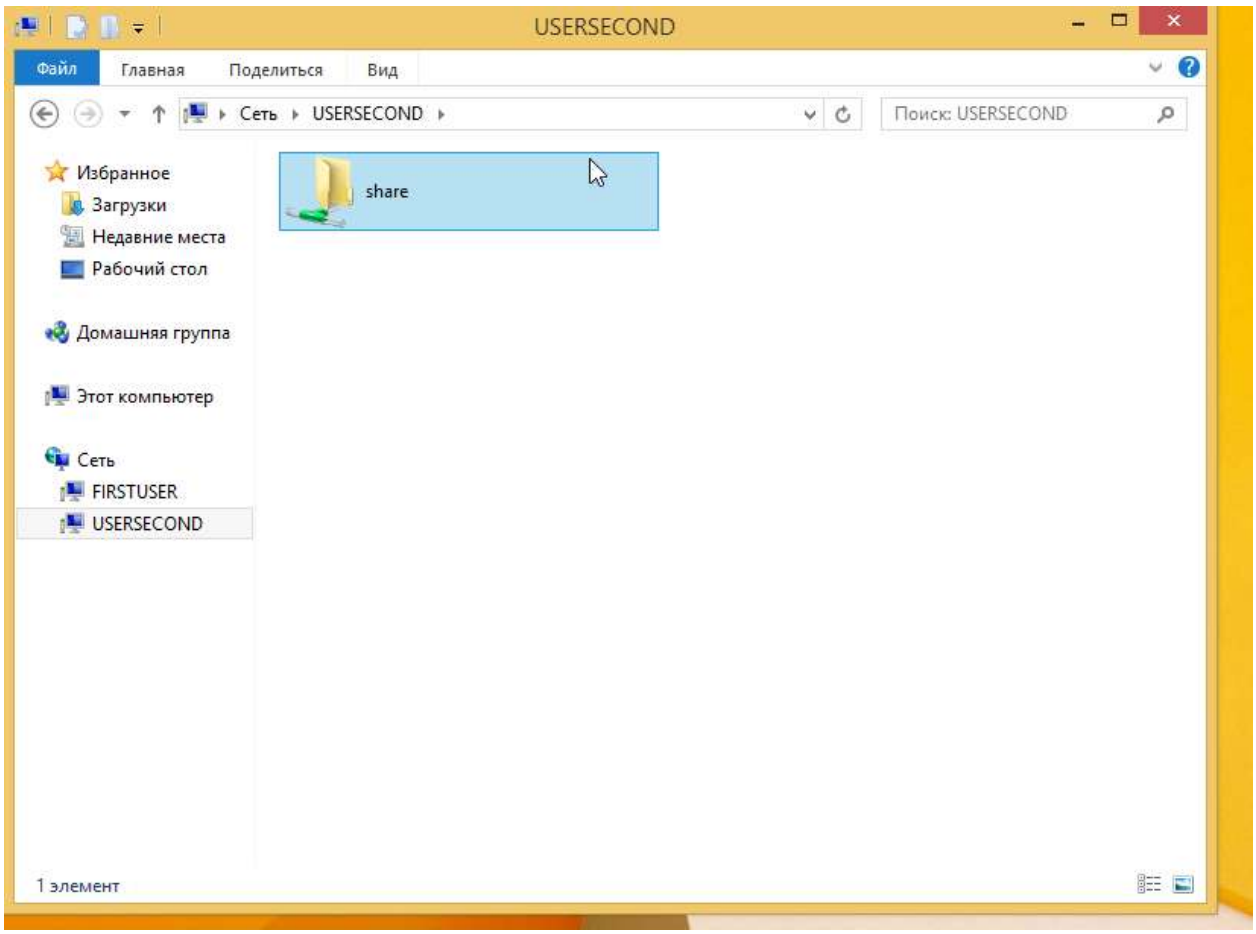
У нас открывается окно, в котором отображены папки для открытого доступа. На картинке ниже таких папок нет.

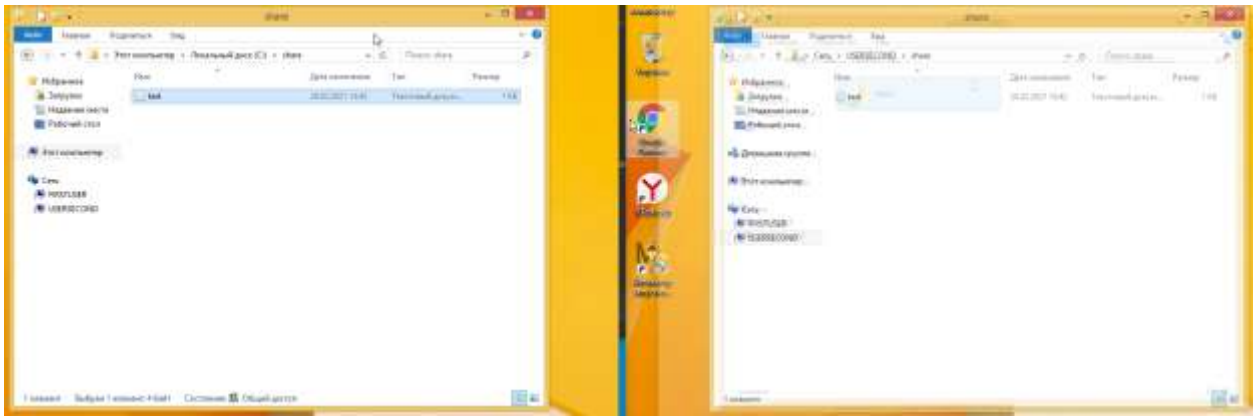


Далее создадим папку. Переходим в ее свойства, на вкладку **Доступ** и далее **Расширенная настройка**. Нажимаем на галочку **Открыть общий доступ к этой папке.**



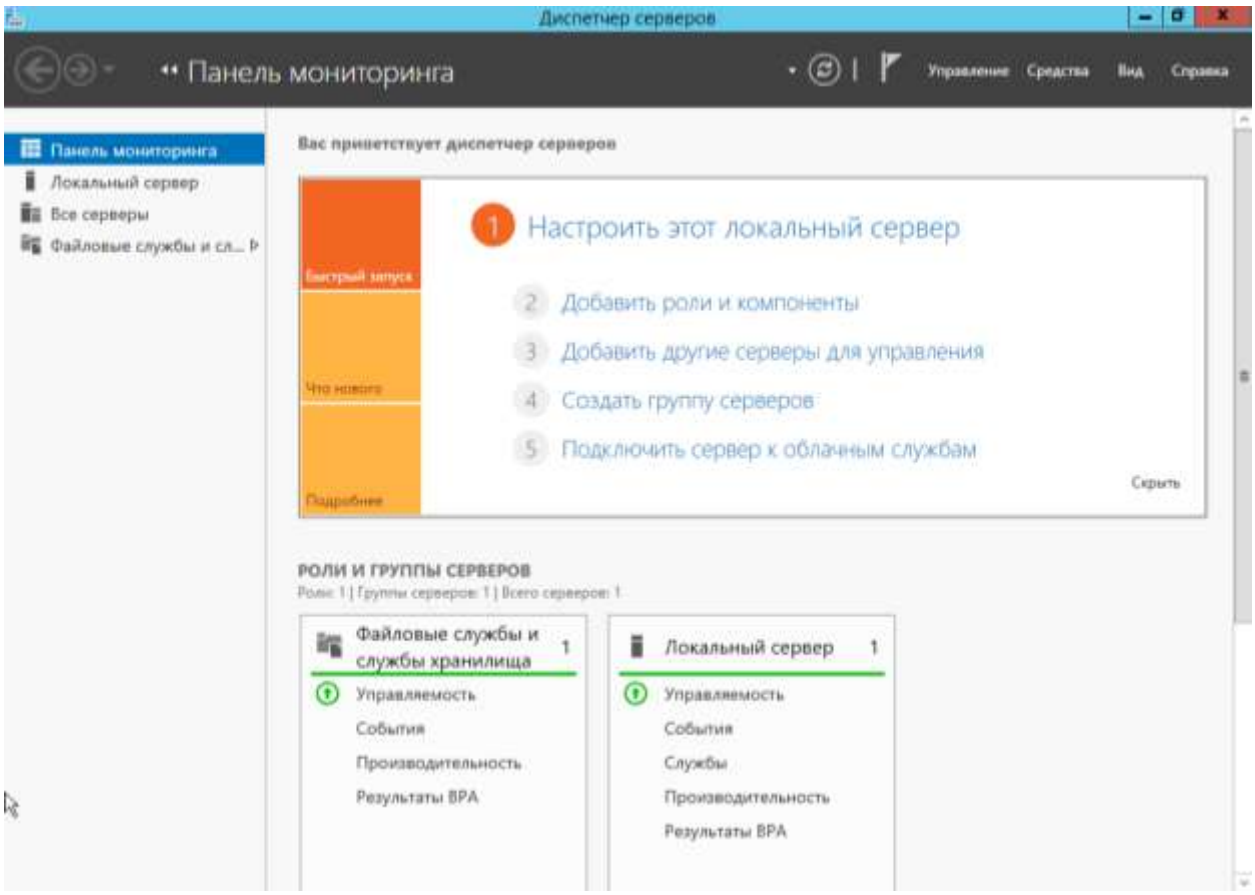
Переходим обратно на другого пользователя, обновляем папку и появляется созданная папка.

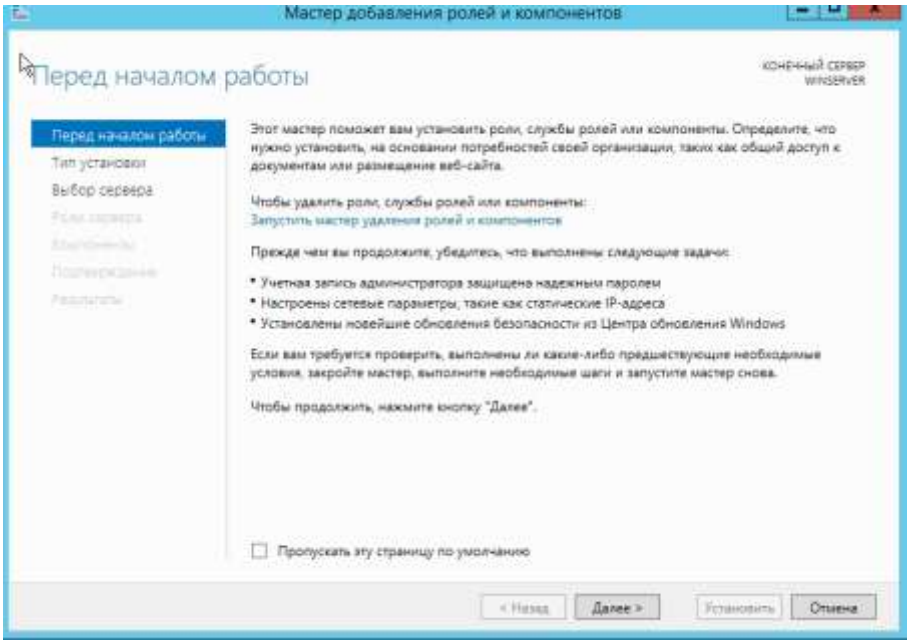




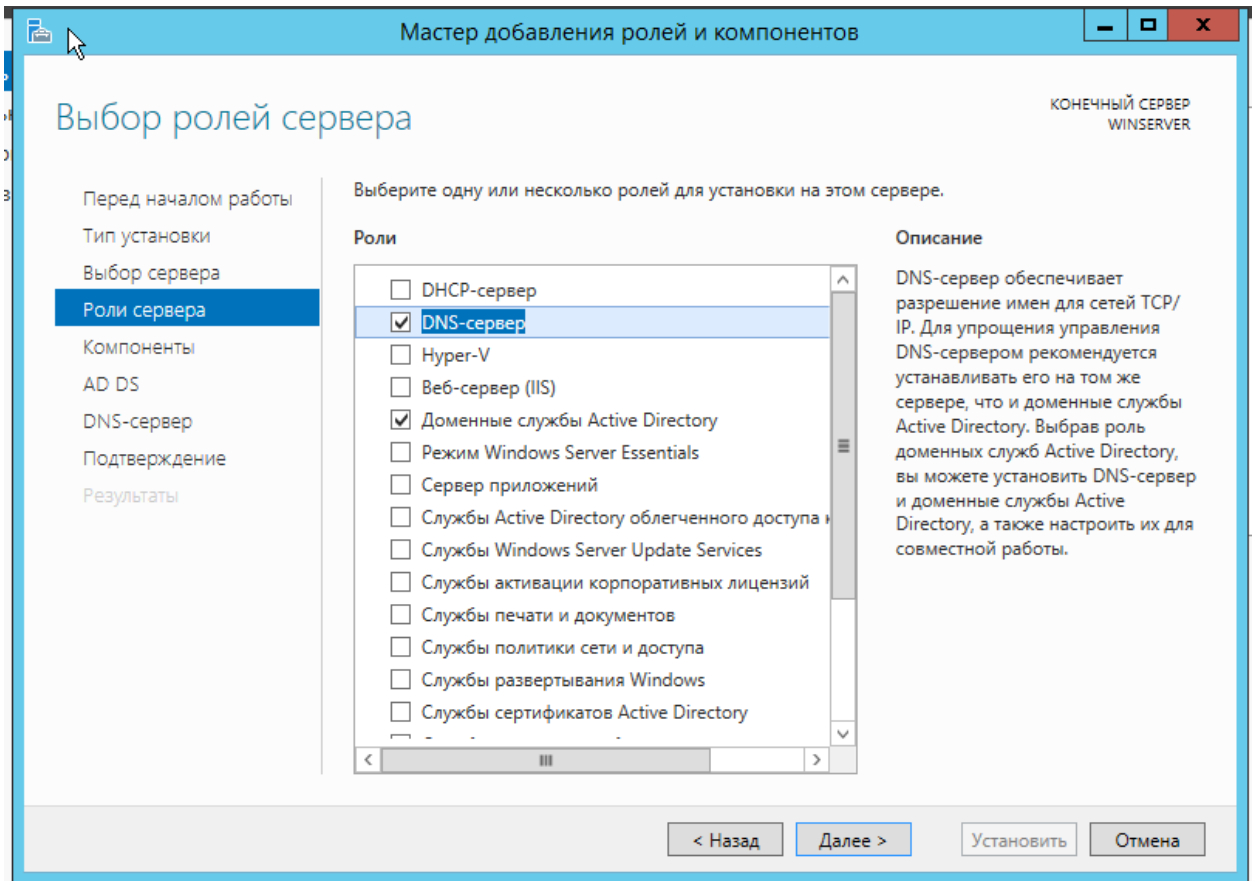
Далее настроим и установим DNS и домен.

Для установки и настройки DNS и домена, переходим в диспетчер серверов и выбираем **Добавить роли и компоненты.**

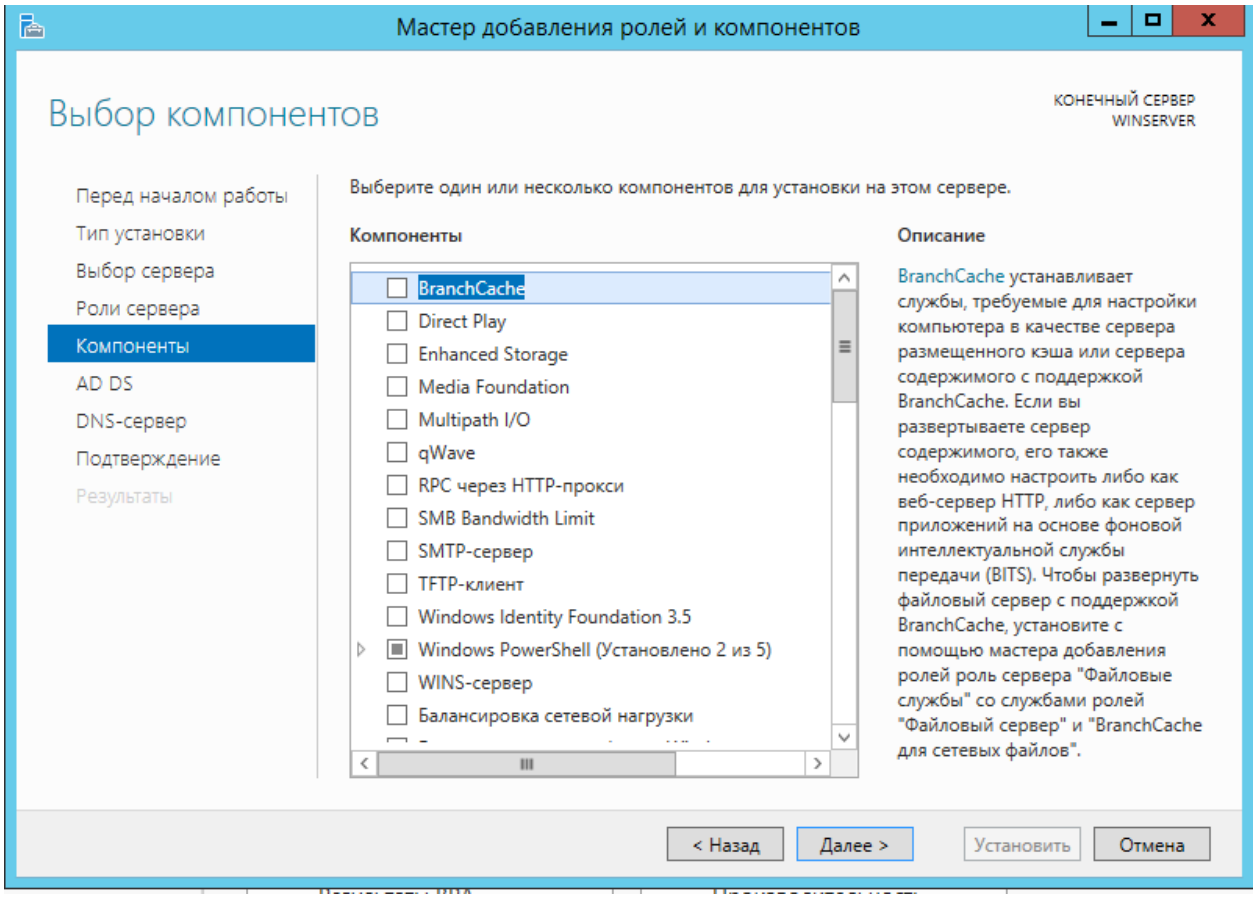




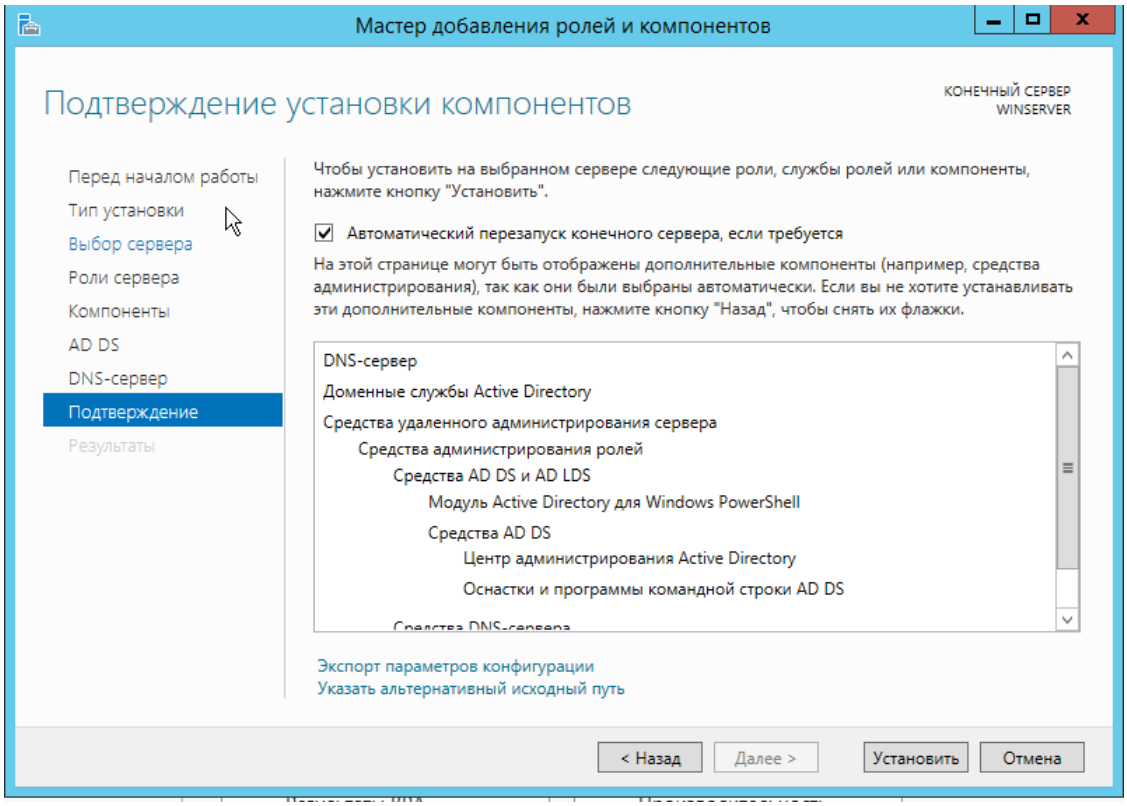
Далее нажимаем **Далее** до **Роли сервера** и выбираем **DNS** и **Доменные службы Active Directory**.

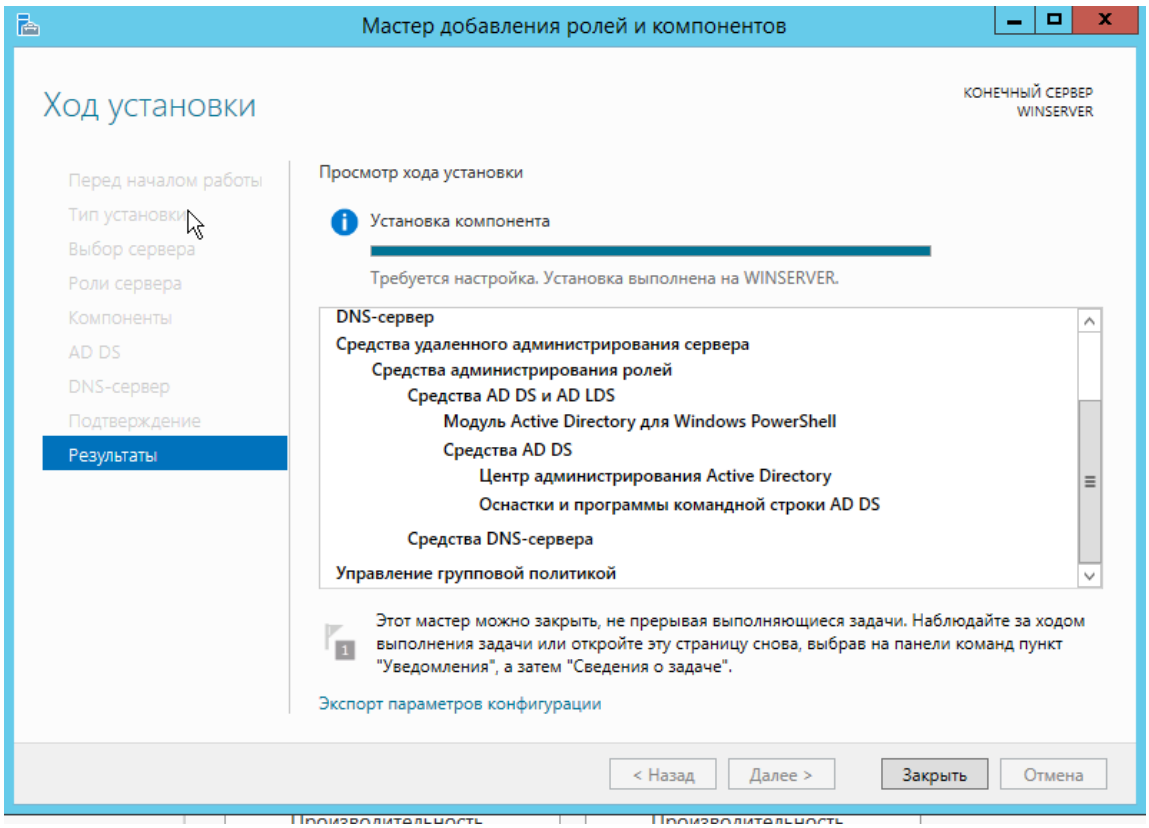


Компоненты нам не нужны, пропускаем до пункта **Подтверждение**.



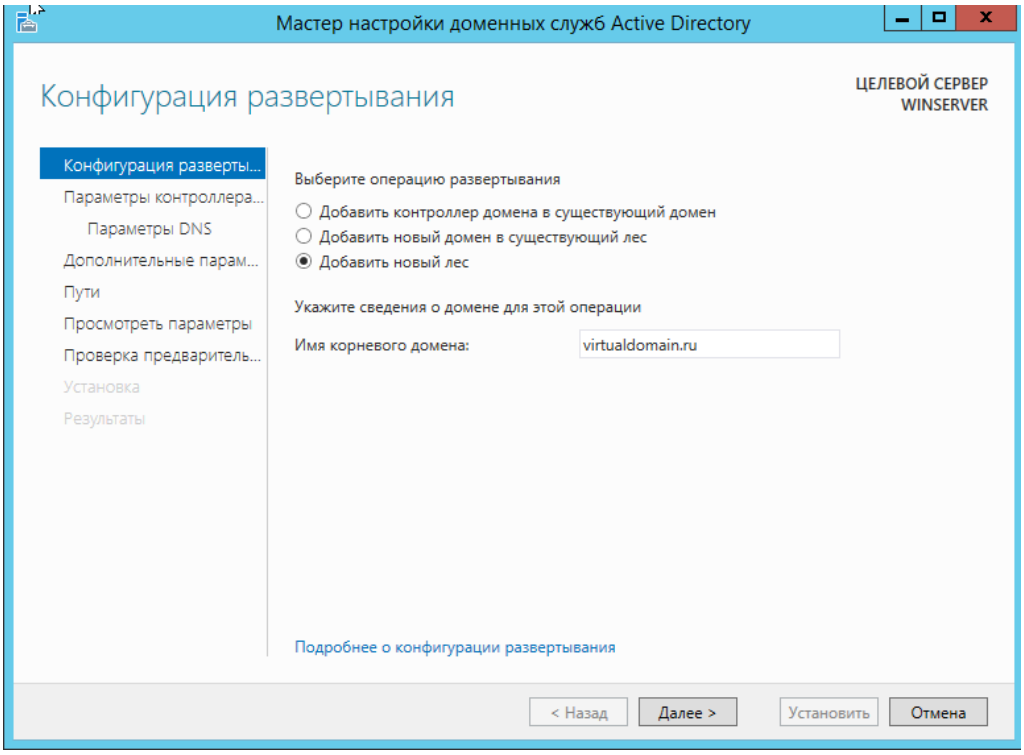
Нажимаем на **Установить.** После окончания установки, сервер перезапустится.



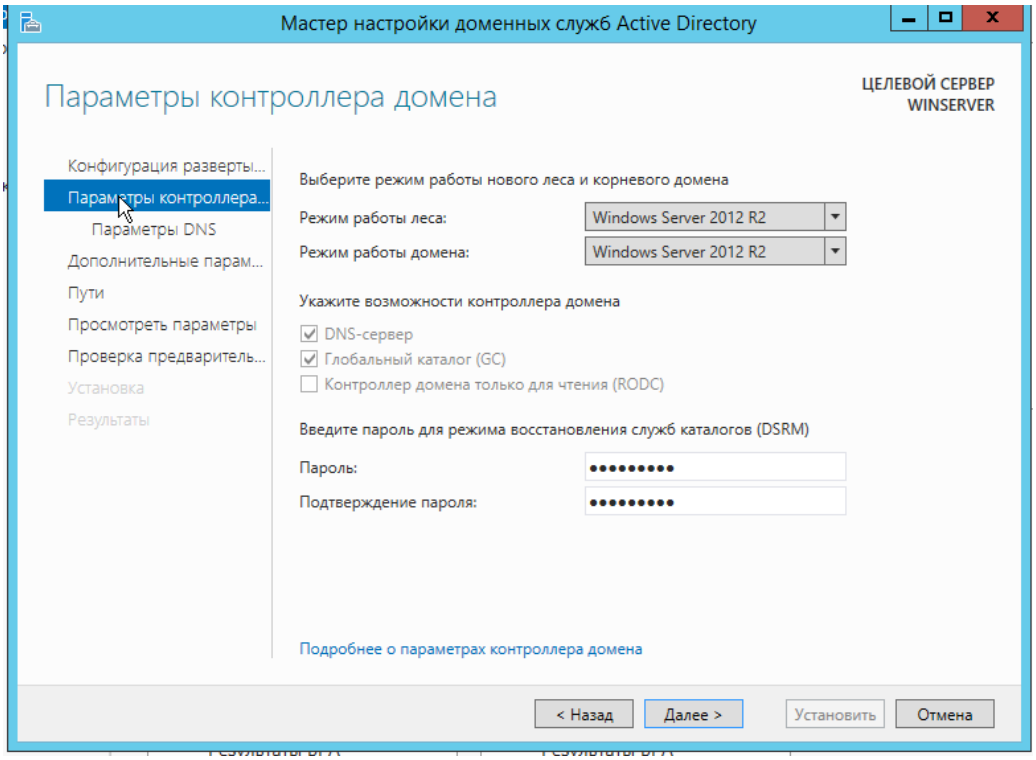


Для настройки Домена переходим в **Мастер настройки доменных служб Active Directory**.

Выбираем операцию развертывания **Добавить новый лес**. И указываем **Имя корневого домена**

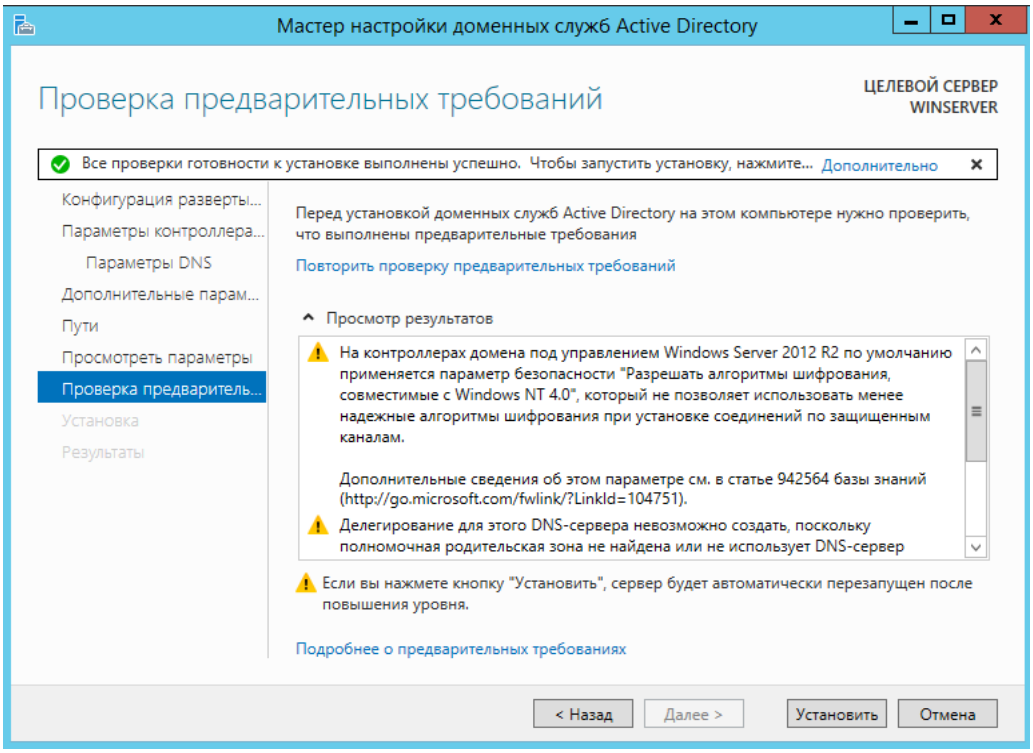


На следующей вкладке необходимо ввести пароль для режима восстановления служб каталогов DSRM

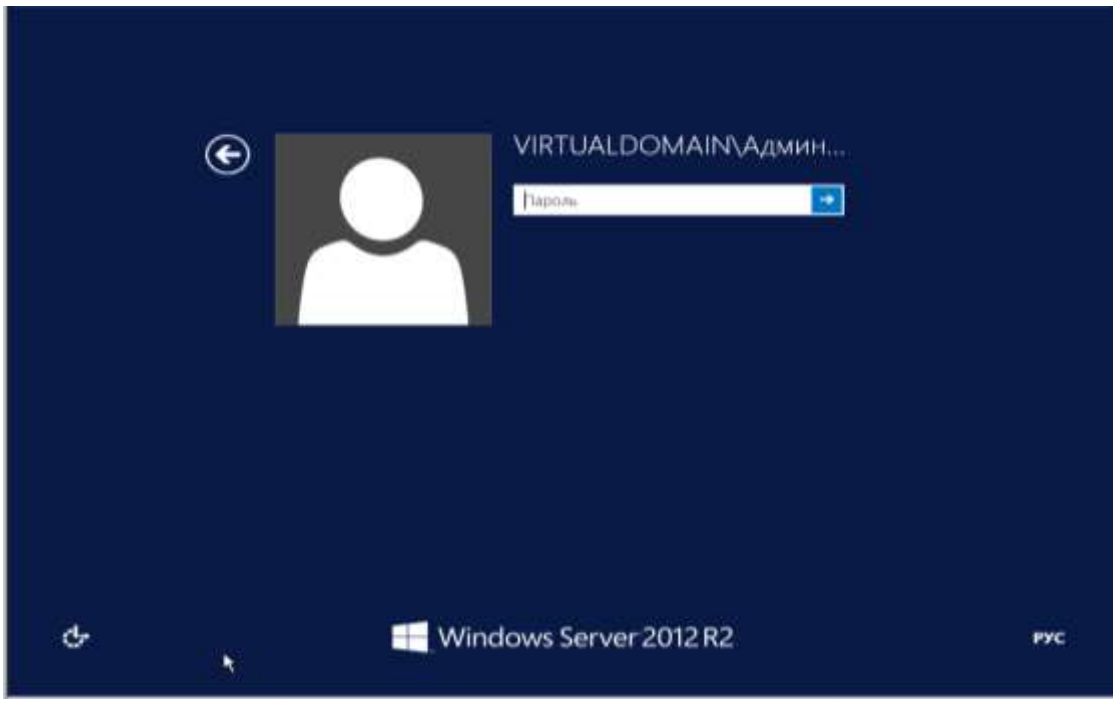


Далее нажимаем Далее до момента проверка предварительных требований. Проверяем что “Все проверки готовности к установке

выполнены успешно”. И нажимаем установить, после установки сервер перезапустится.



После перезапуска, сервер автоматически перейдет в домен. И при авторизации будем видеть наш домен\имя администратора.



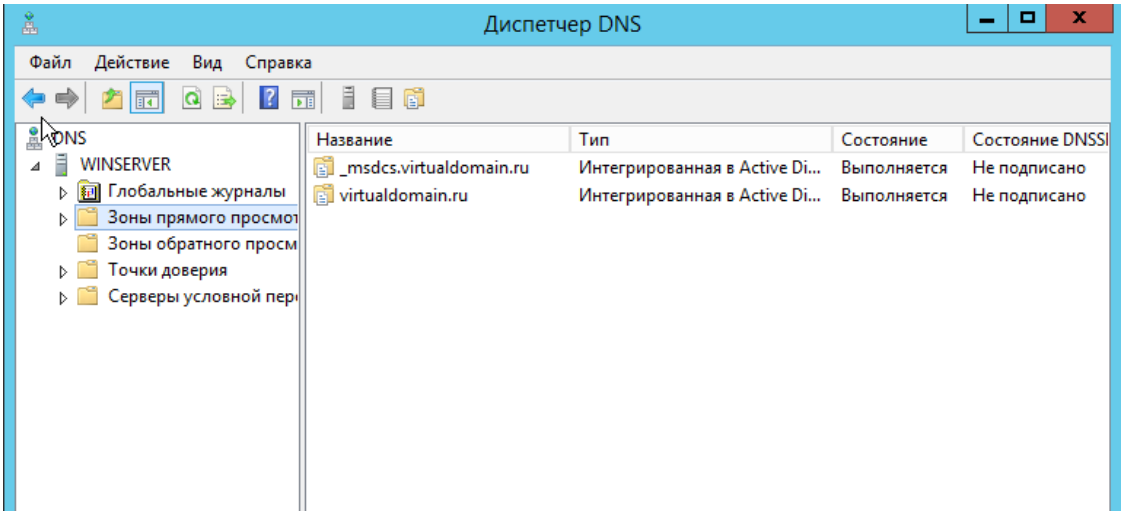
Далее настроим Зону обратного просмотра для DNS.

Доменная зона — совокупность доменных имён в пределах конкретного домена.

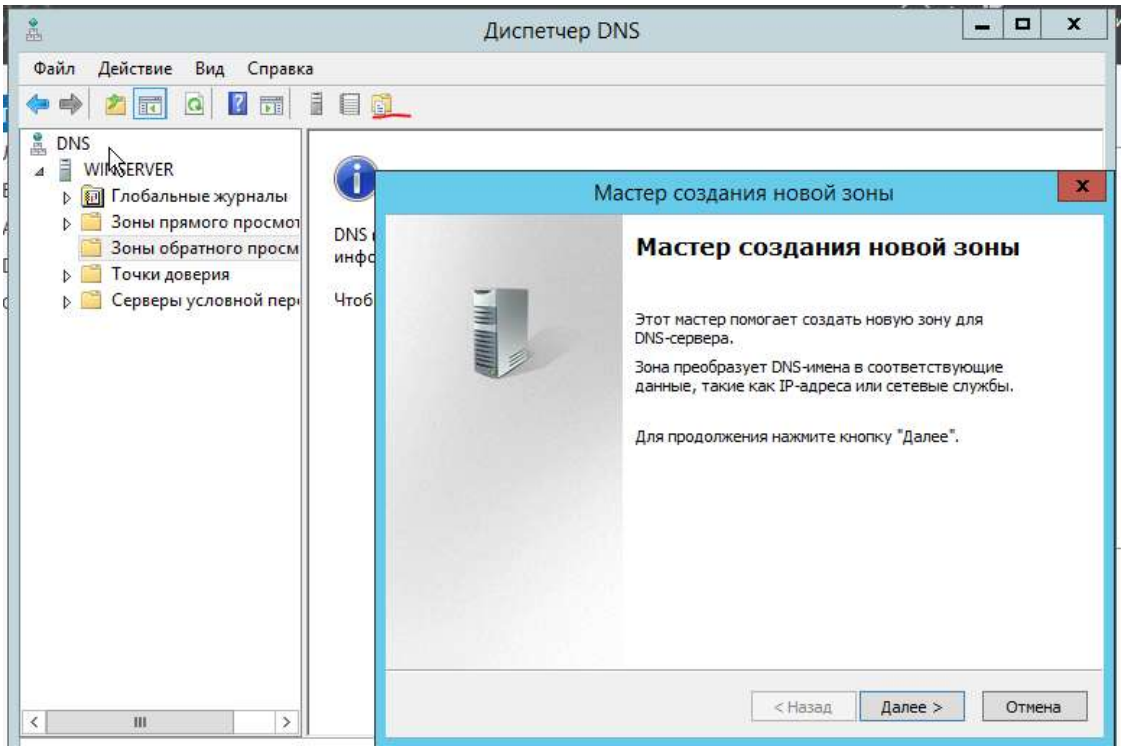
Зоны прямого просмотра предназначены для сопоставления доменного имени с IP-адресом.

Зоны обратного просмотра работают в противоположную сторону и сопоставляют IP-адрес с доменным именем.

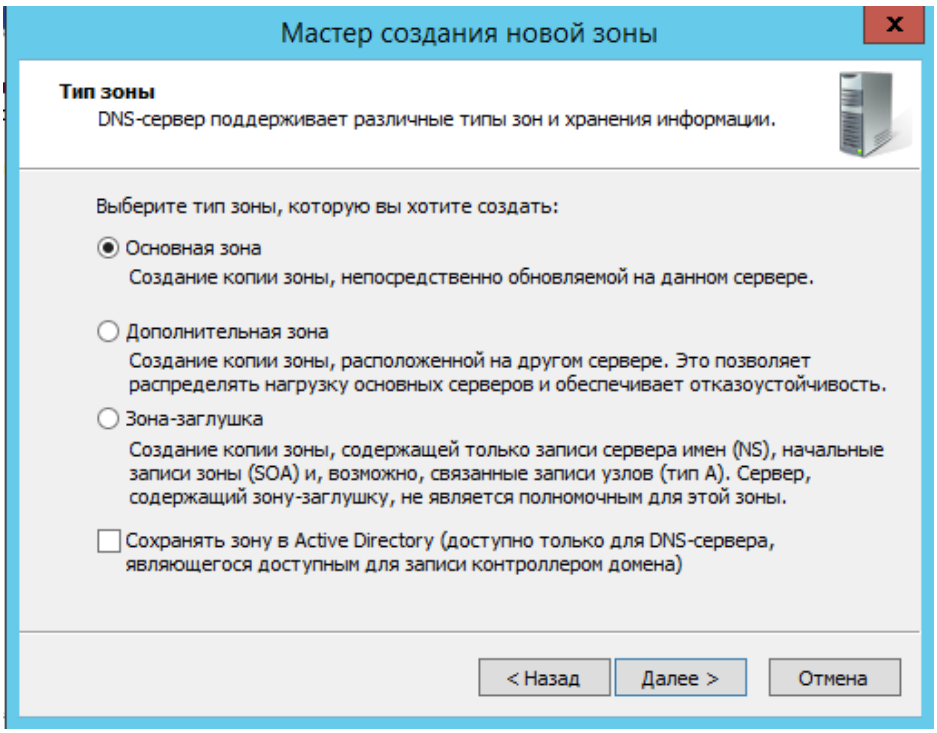
Создание зон и управление ими осуществляется при помощи **Диспетчера DNS**. Переходим на вкладку Зоны прямого просмотра и проверяем что есть файл с нашем доменом.



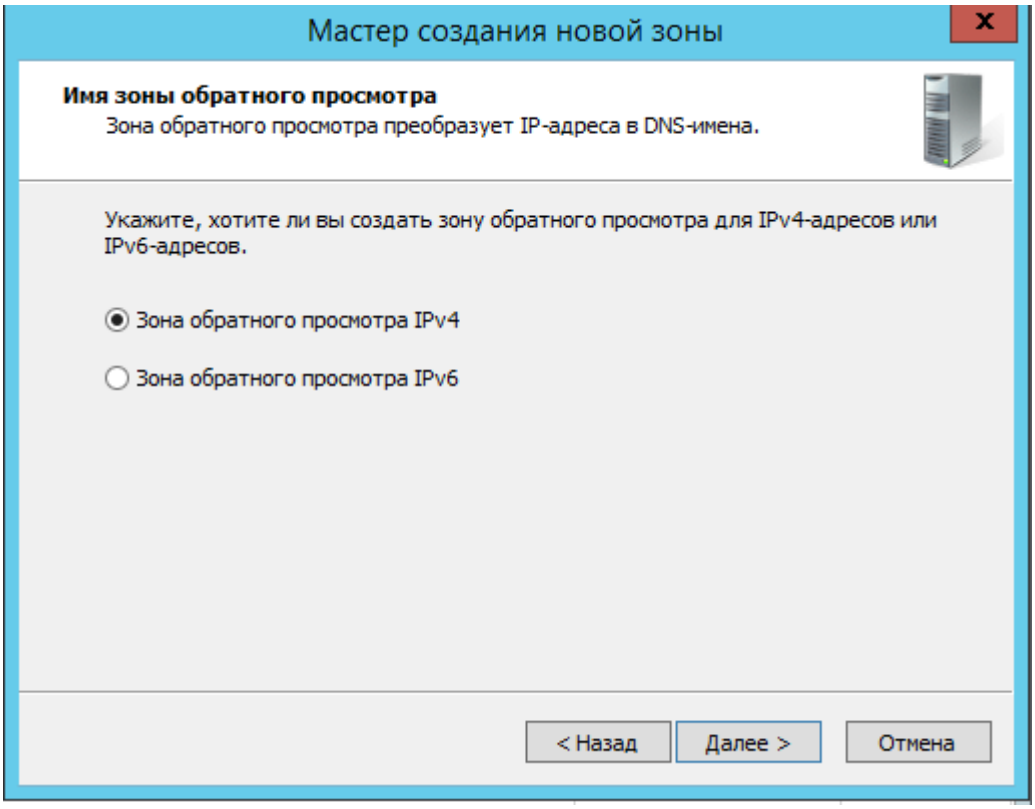
Далее переходим в зону обратного просмотра, и нажимаем на **Мастер создания новой зоны.**



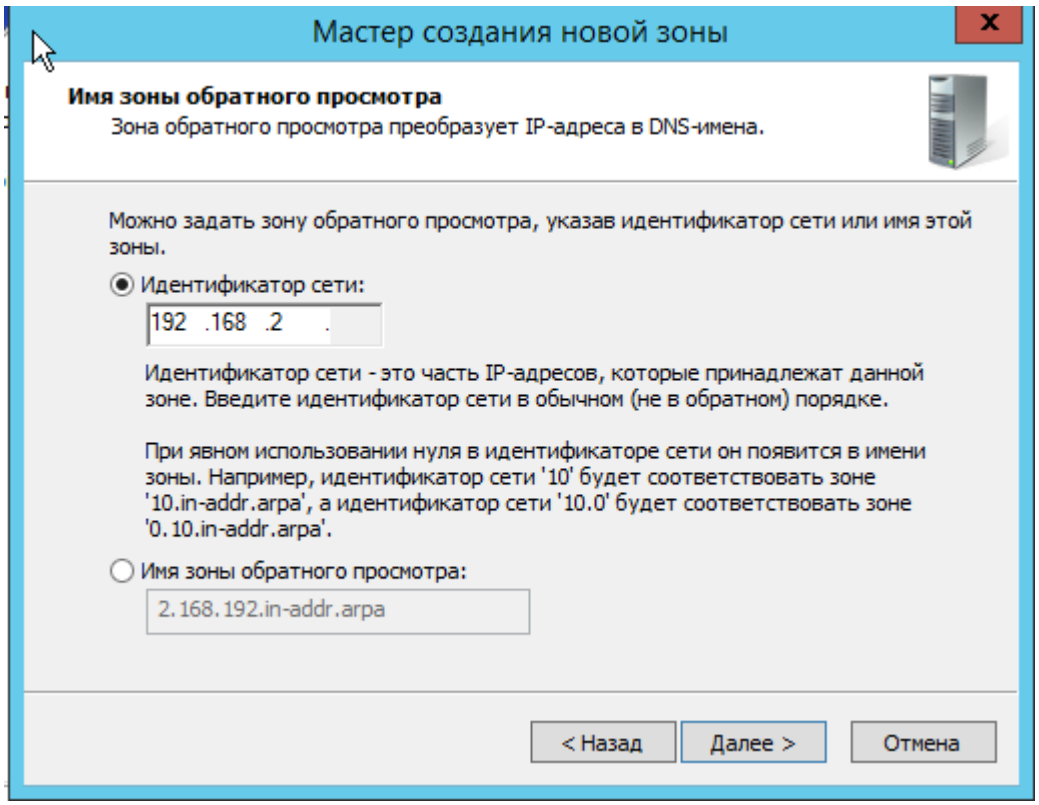
Далее необходимо выбрать **Основная зона.** И **Далее**



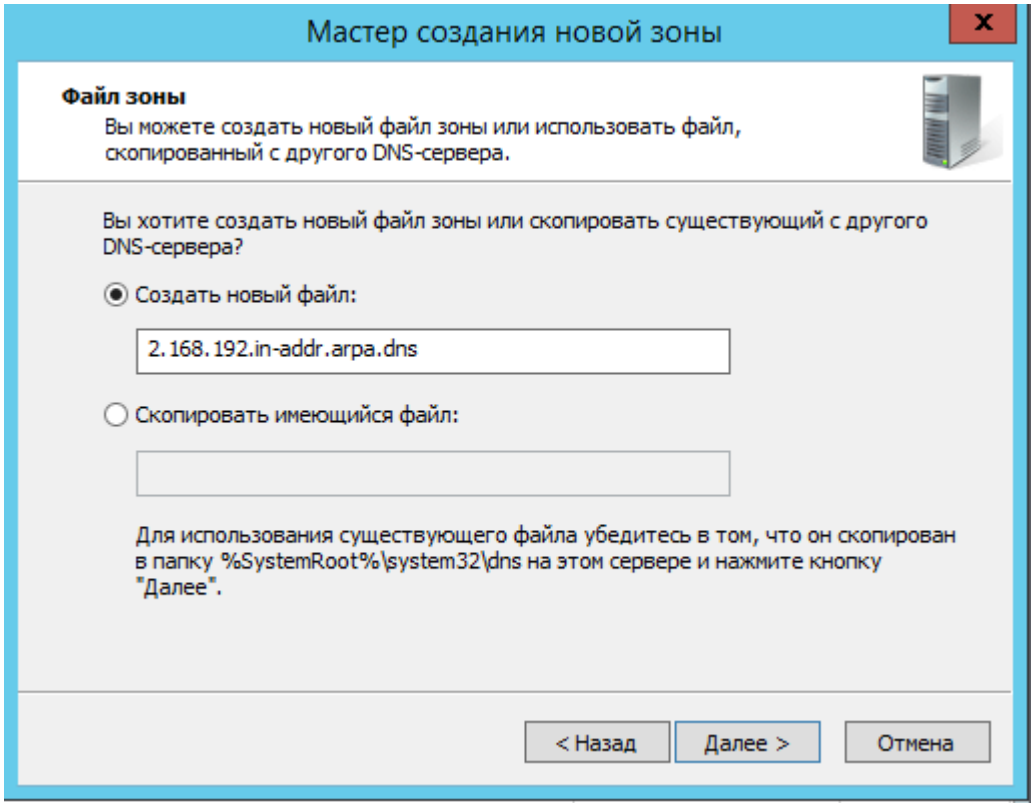
На следующей вкладке необходимо указать зону обратного просмотра для IPv4 или IPv6 адресов. Указываем **IPv4** и **Далее.**



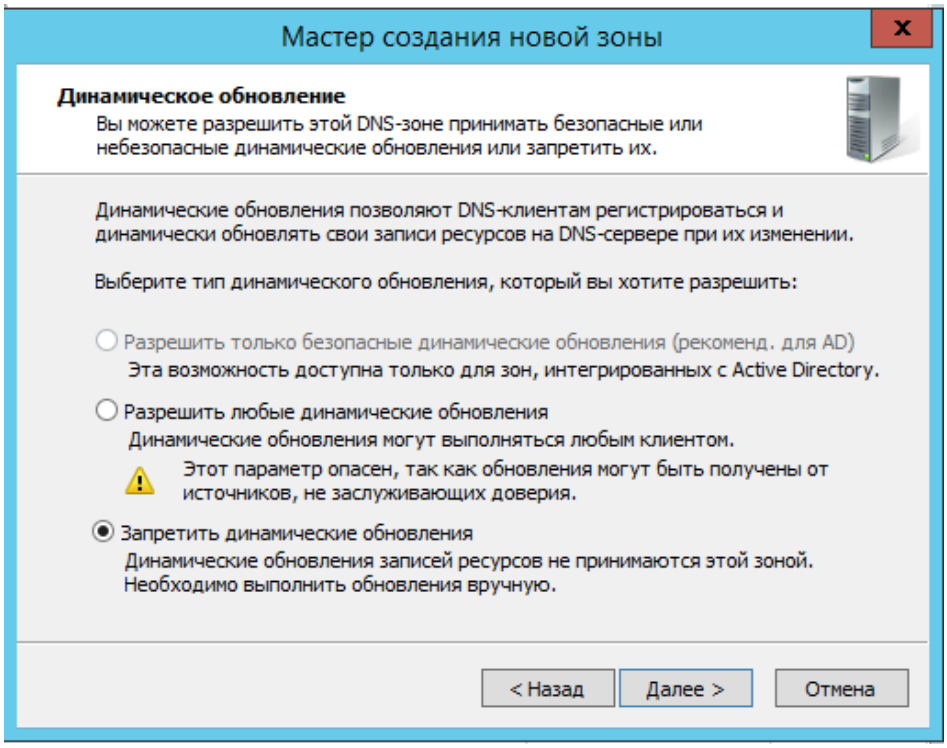
Далее необходимо указать идентификатор сети. Указывается первые три октета сетевого адреса и **Далее.**



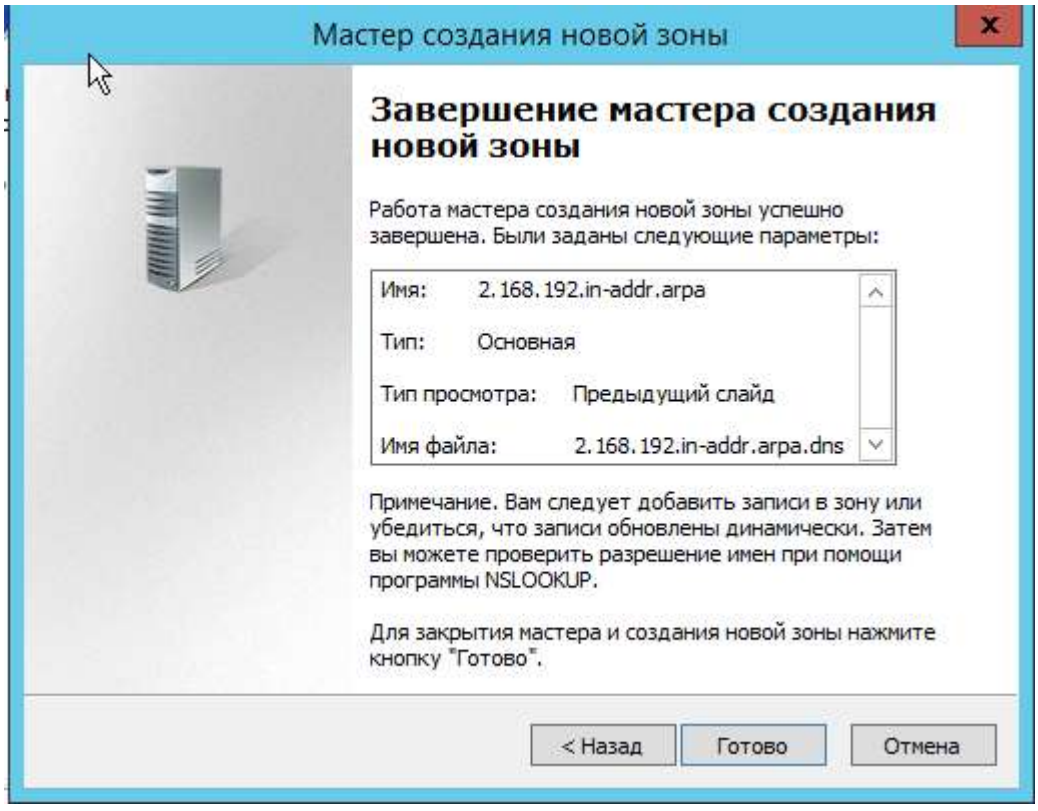
При необходимости поменяйте название будущего файла зоны и перейдите **Далее**



Выбираем **Запретить динамическое обновления.** Разрешать не рекомендуется в силу значимой уязвимости.



Проверьте правильность конфигурации и завершите настройку, нажав на кнопку Готово



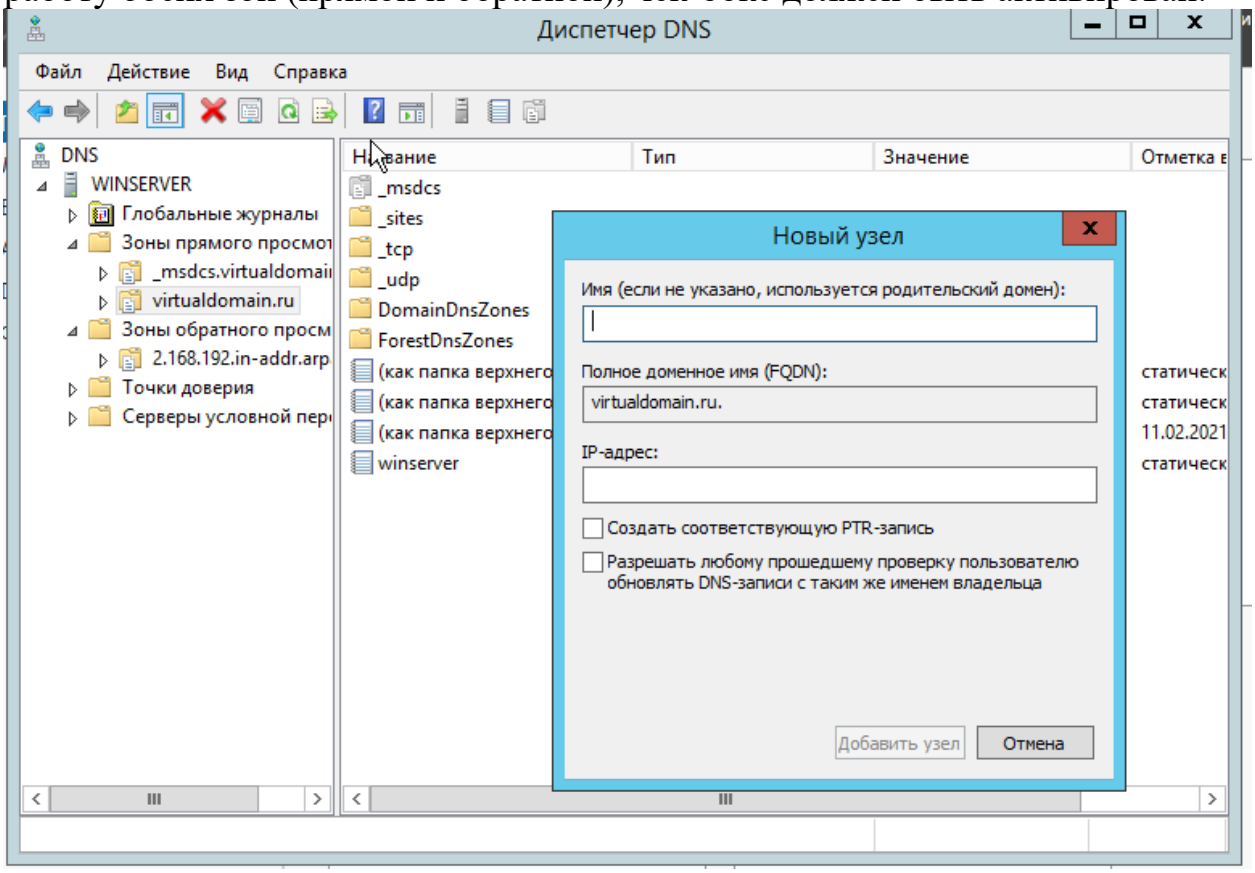
Ресурсная запись — единица хранения и передачи информации в DNS, заключает в себе сведения о соответствии какого-либо имени с определенными служебными данными.

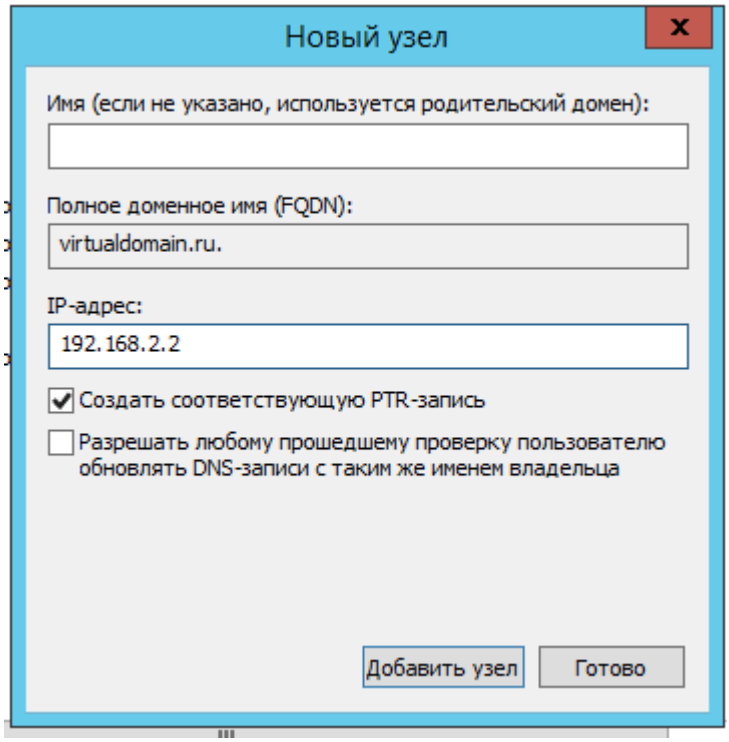
Запись A — запись, позволяющая по доменному имени узнать IP-адрес.

Запись PTR — запись, обратная A записи.

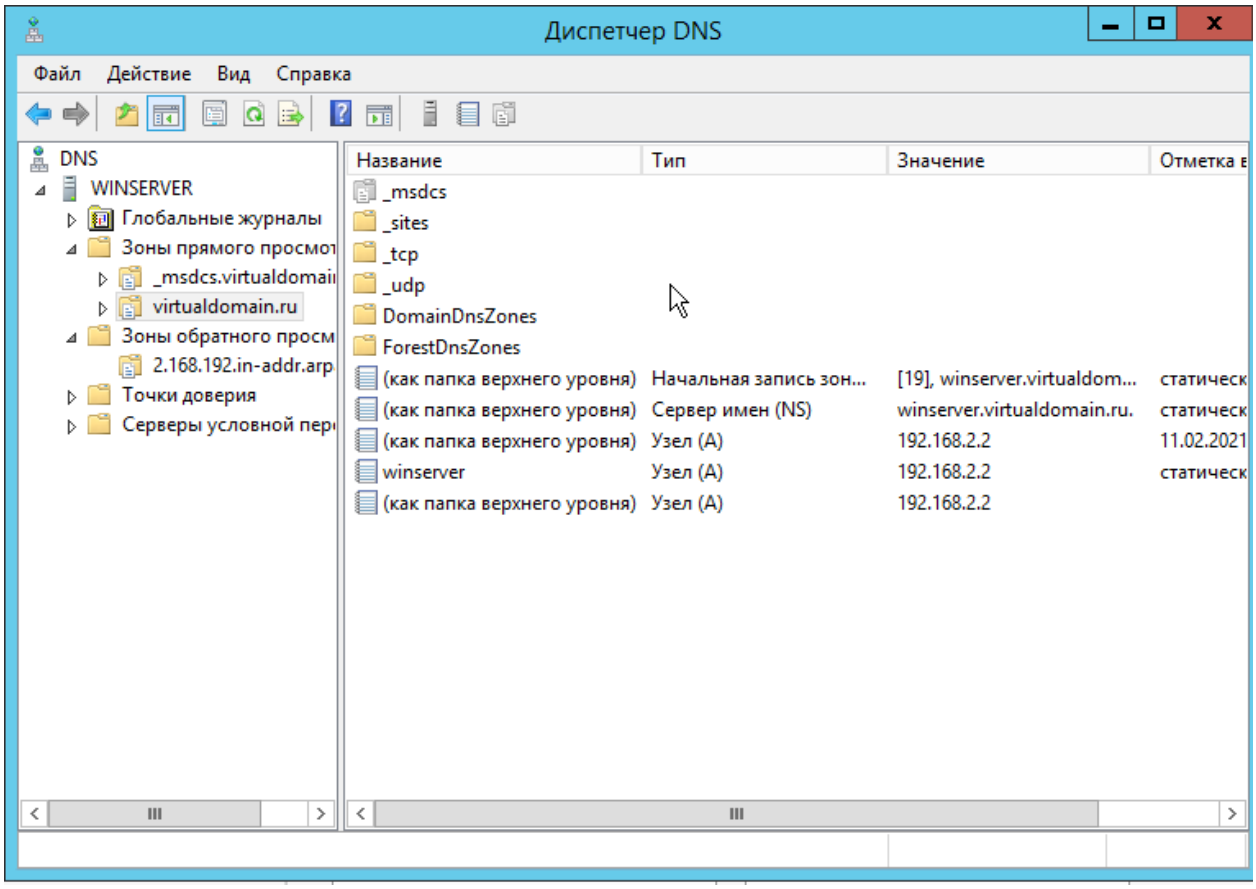
В Диспетчере DNS выберите каталог созданной ранее зоны внутри **каталога Зон Прямого Просмотра**. В правой части Диспетчера, где отображается содержимое каталогов, правой кнопки мыши вызовите выпадающее меню и запустите команду «**Создать узел (A или AAAA)…**»:

Откроется окно создания Нового Узла, где понадобится вписать в соответствующие поля имя узла (без доменной части, в качестве доменной части используется название настраиваемой зоны) и IP-адрес. Здесь же имеется чек-бокс Создать соответствующую PTR-запись — чтобы проверить работу обеих зон (прямой и обратной), чек-бокс должен быть активирован:





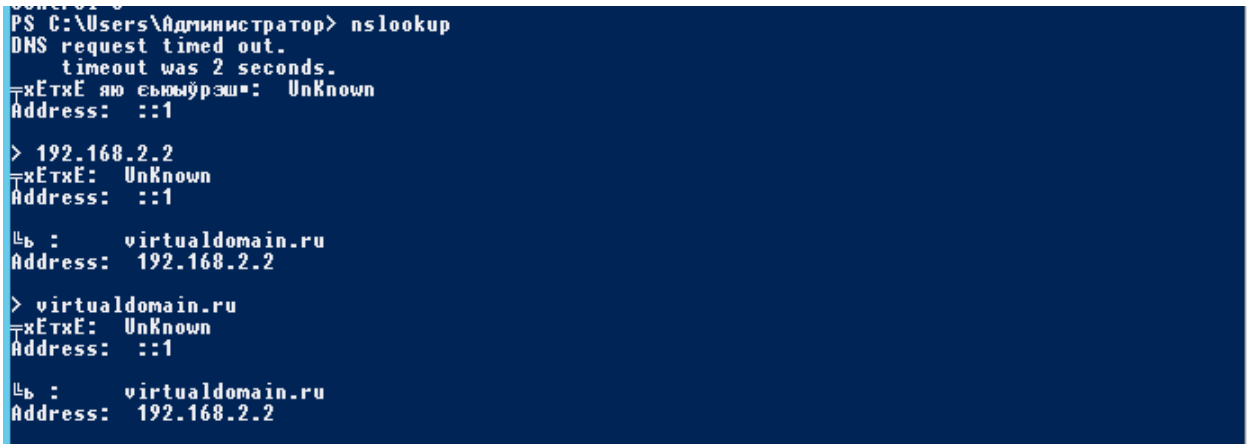
Проверьте изменения в каталогах обеих зон (на примере ниже в обеих зонах появилось по 2 новых записи):



- Откройте командную строку (cmd) или PowerShell и запустите команду nslookup:

Чтобы убедиться, что прямая и обратная зоны работают как положено, можно отправить два запроса:

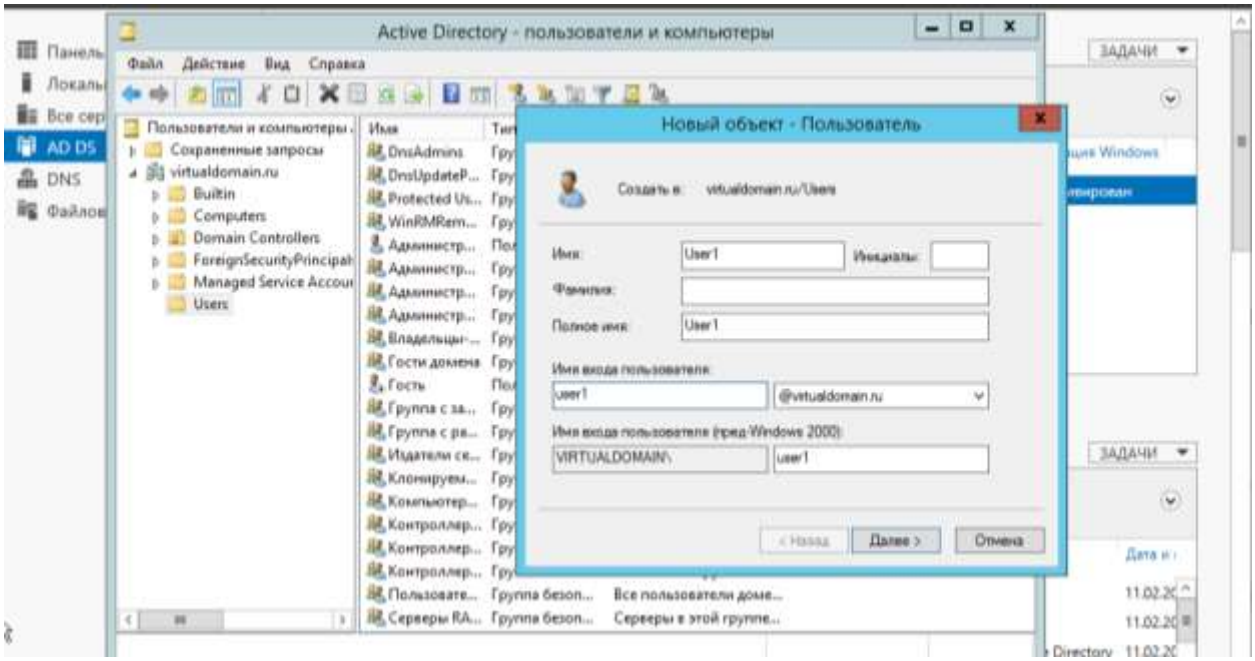
- Запрос по домену;
- Запрос по IP-адресу:



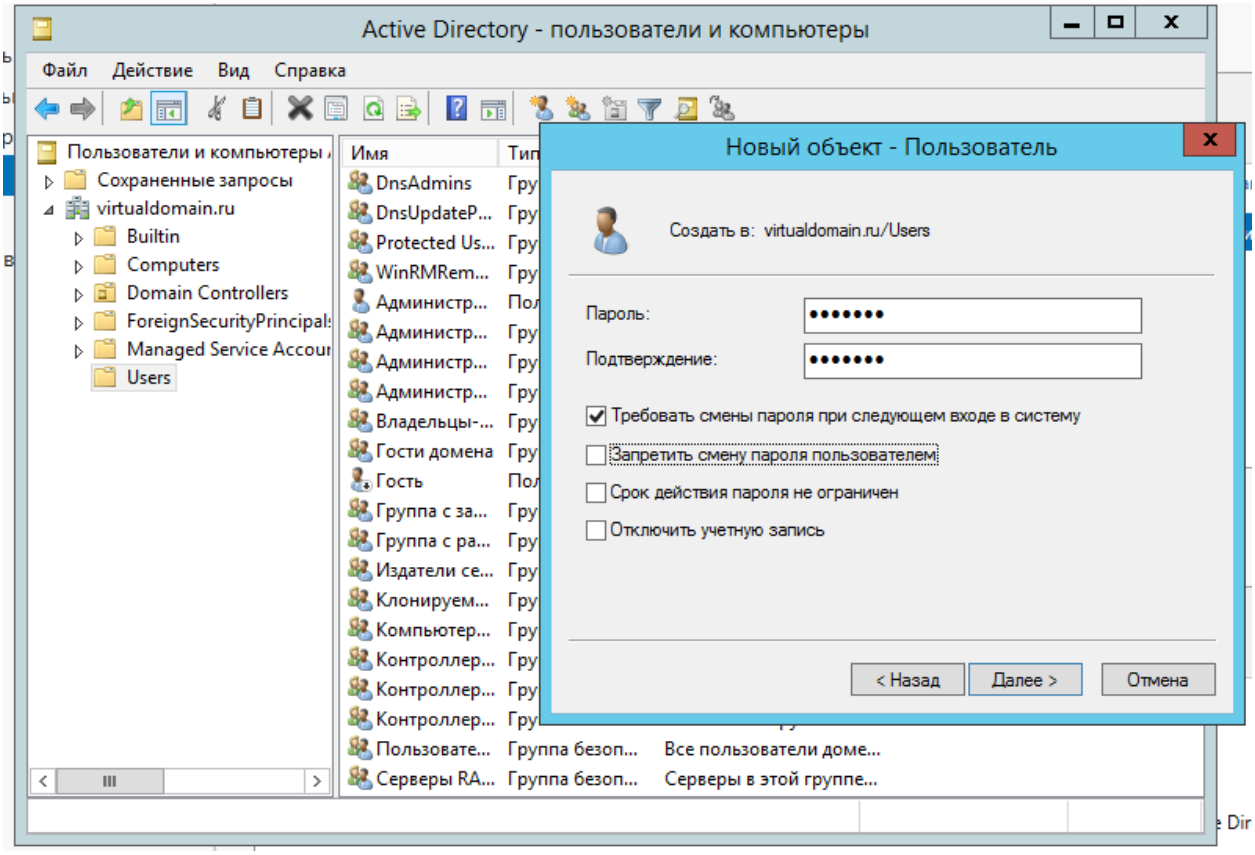
Создадим пользователя.

Переходим в Active Directory – пользователи и компьютеры, выбираем папку **Users,** создаем новый объект Пользователь.

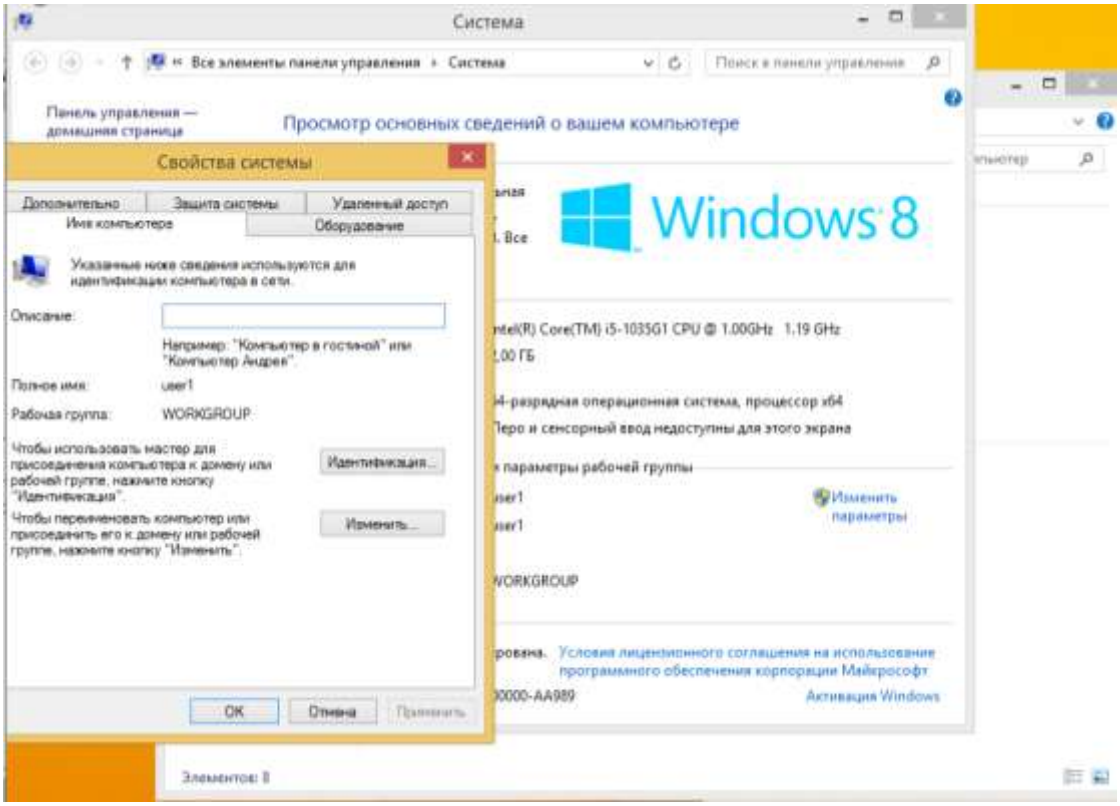
Указываем **Имя**, **Фамилию**, **Имя входа пользователя** и нажимаем **Далее**



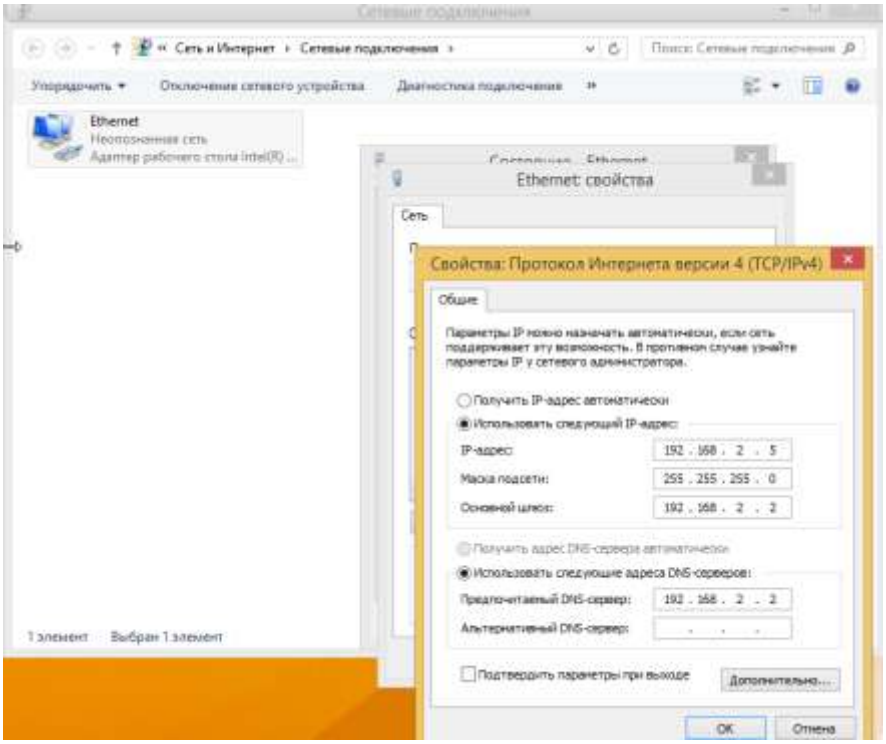
Указывает **Пароль** и повторяем его, **Далее.**



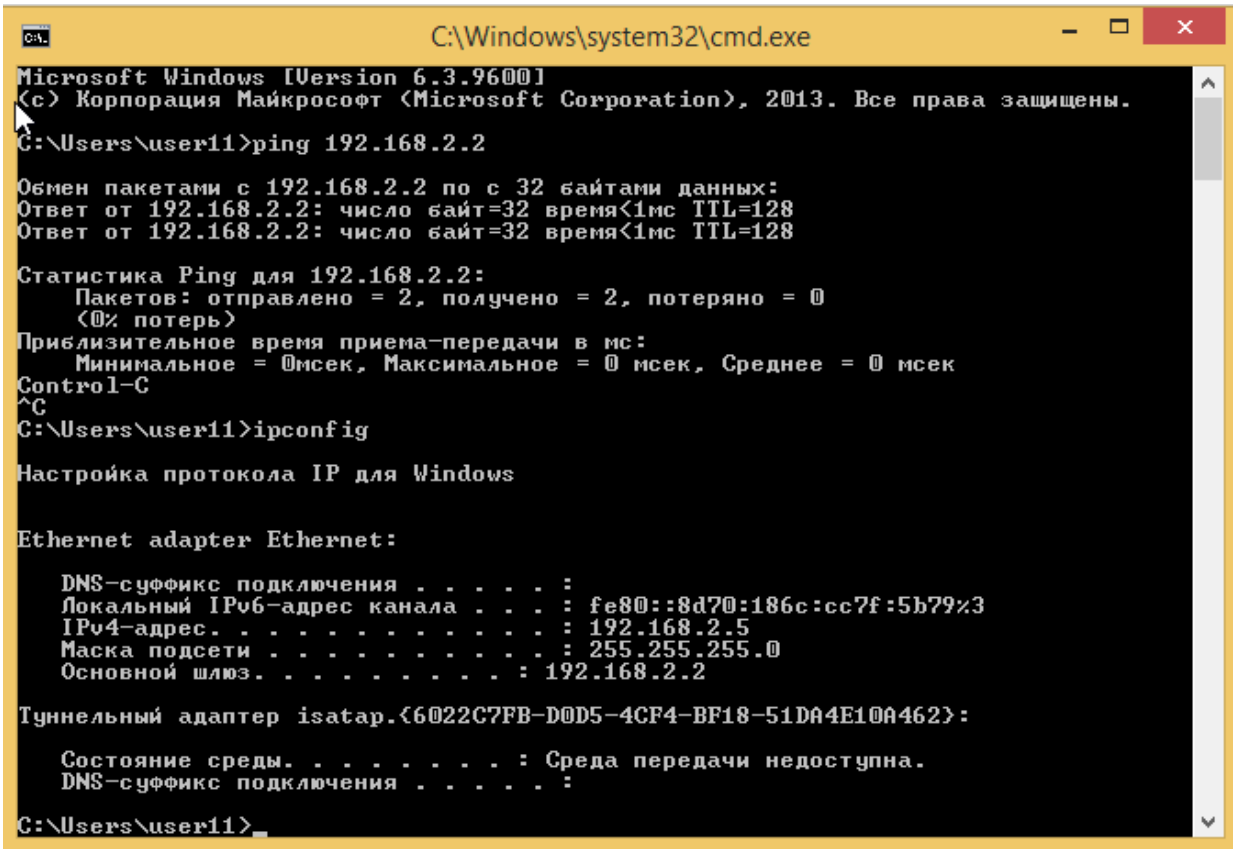
Переходи на машину пользователя. Переход в систему, видим, что у ПК рабочая группа WORKGROUP.



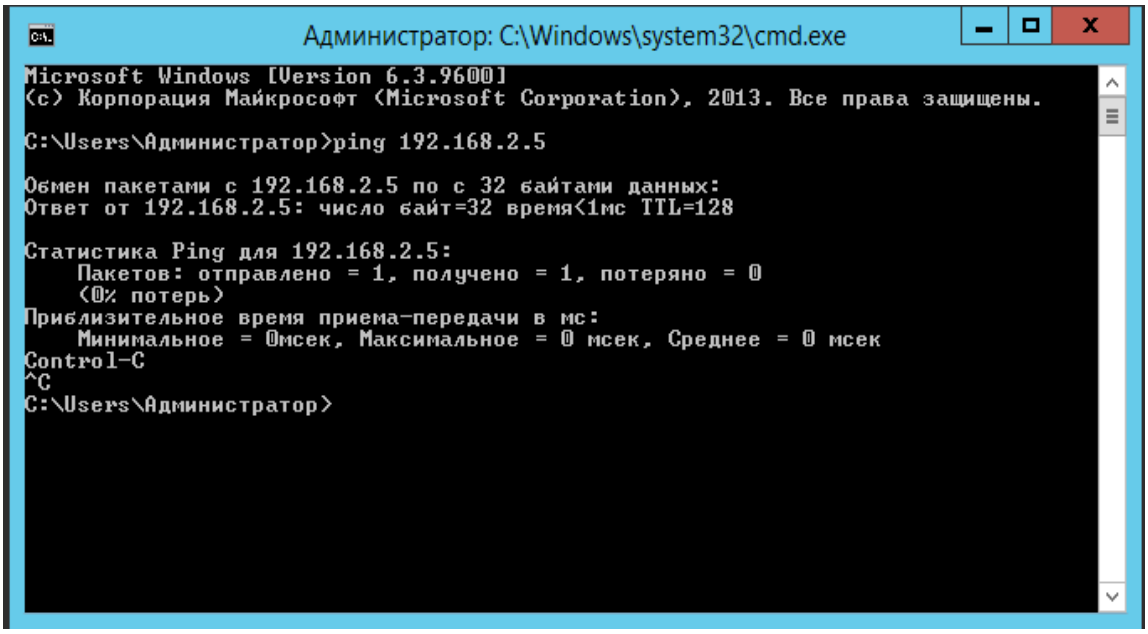
Далее, переходим в **Сетевые подключения**, открывает Свойства Адптера, IPv4 и далее указываем статический IP. В Предпочтениях DNS-сервера указываем IP адрес нашего сервера.



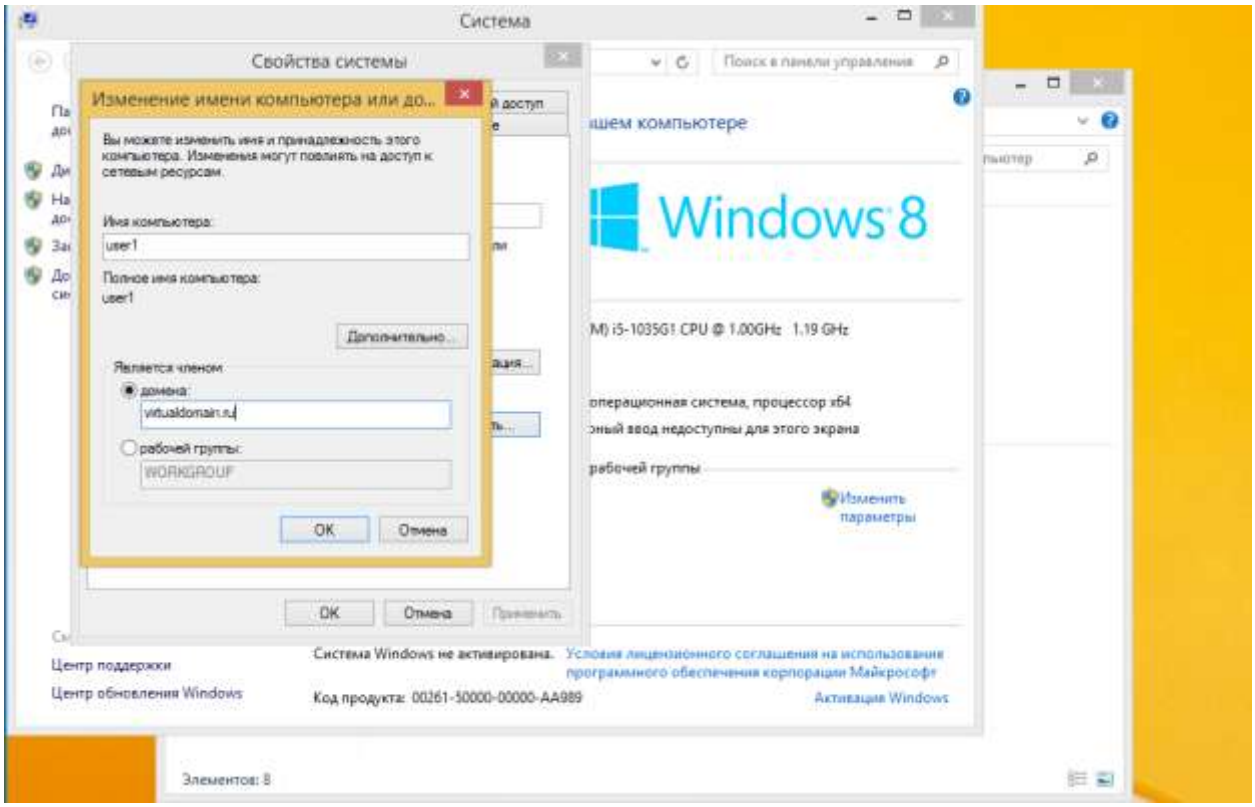
Проверяем применились ли сетевые настройки. Запускаем CMD и прописываем ping и IP адрес win сервера.



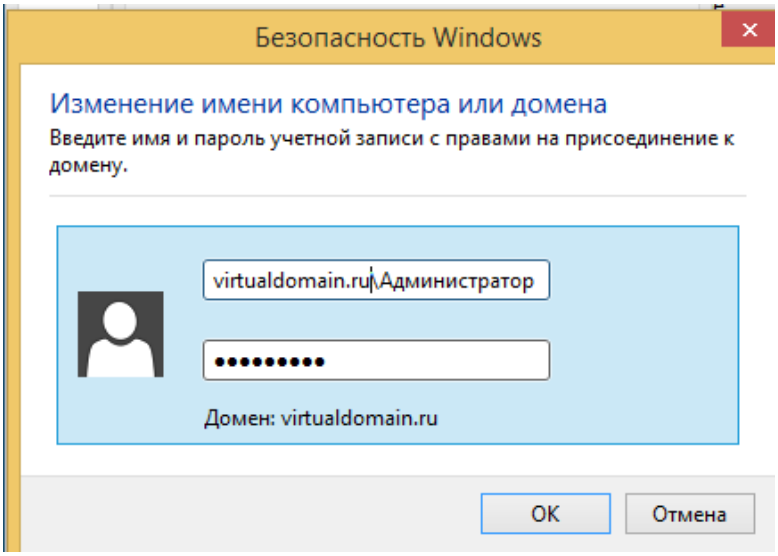
На машине Сервера, так же можно проверить подключение к машине пользователя.

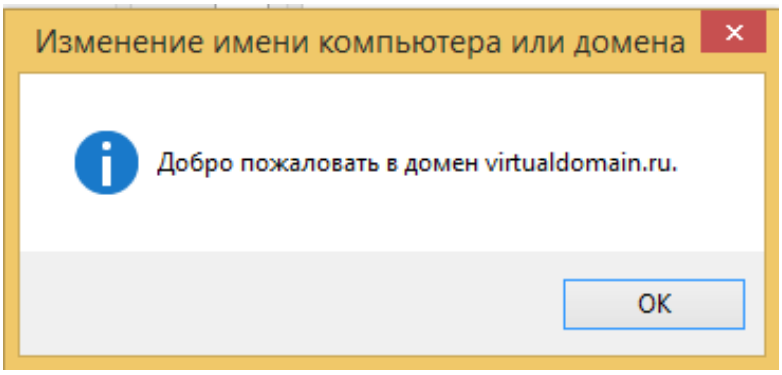


Подключаем машину пользователя к домену. **Система**, **Изменить Параметры**, **Изменение имени компьютера или домена** и вводим в Является членом домена: выбранный домен. Далее **ОК**

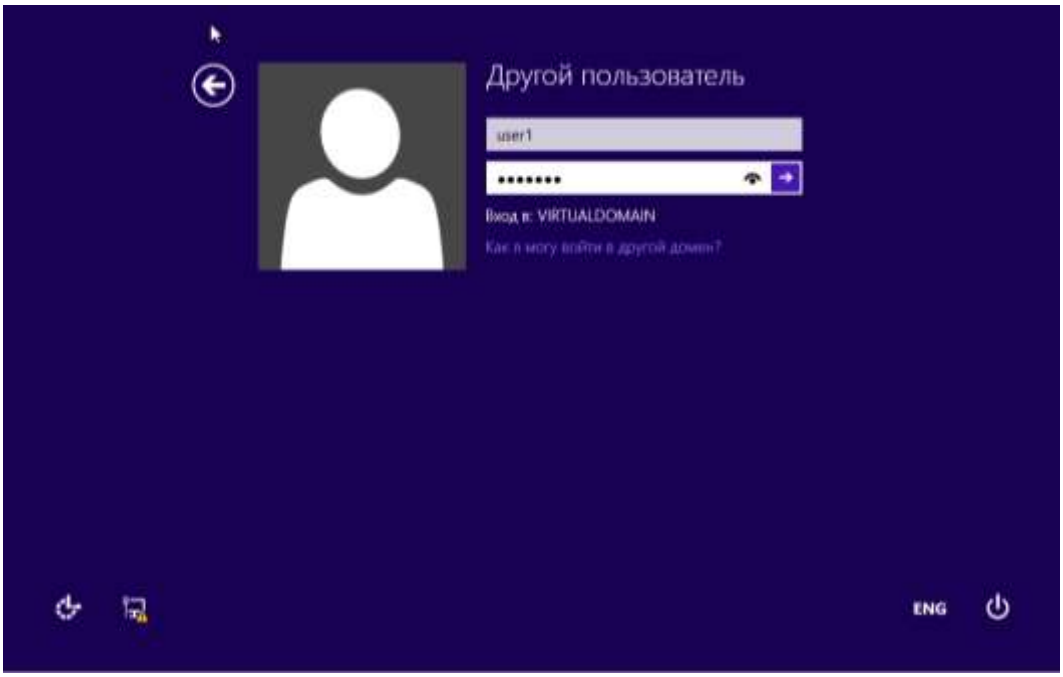


Далее появляется окно **Безопасность Windows**, в нем указывается Пользователь в виде: domain\администратор сервера и пароль администратора сервера.

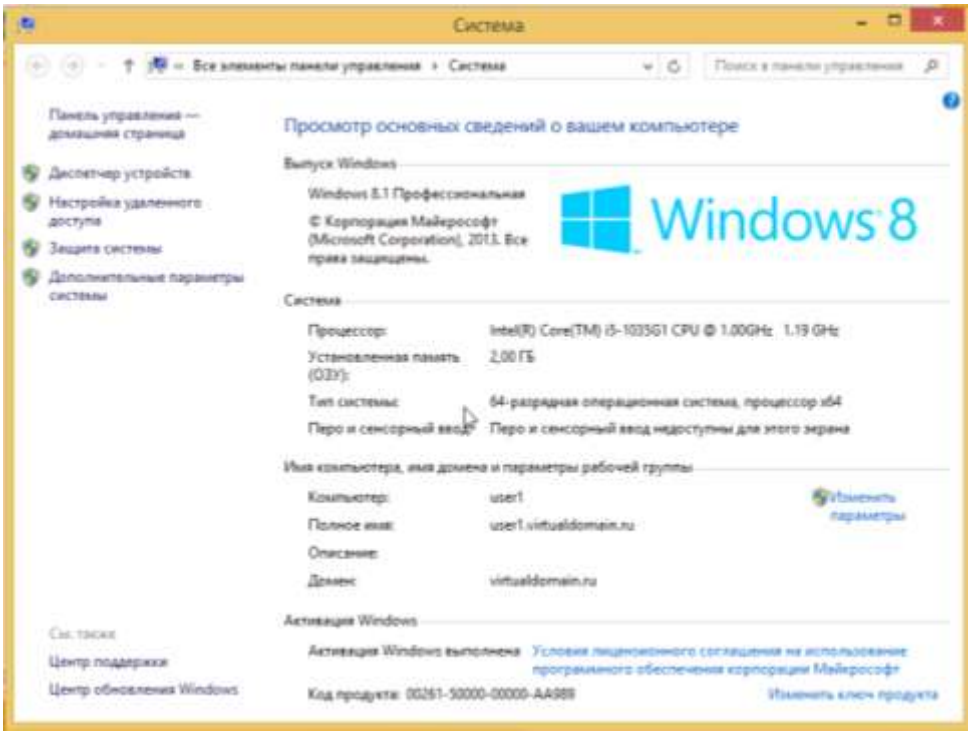




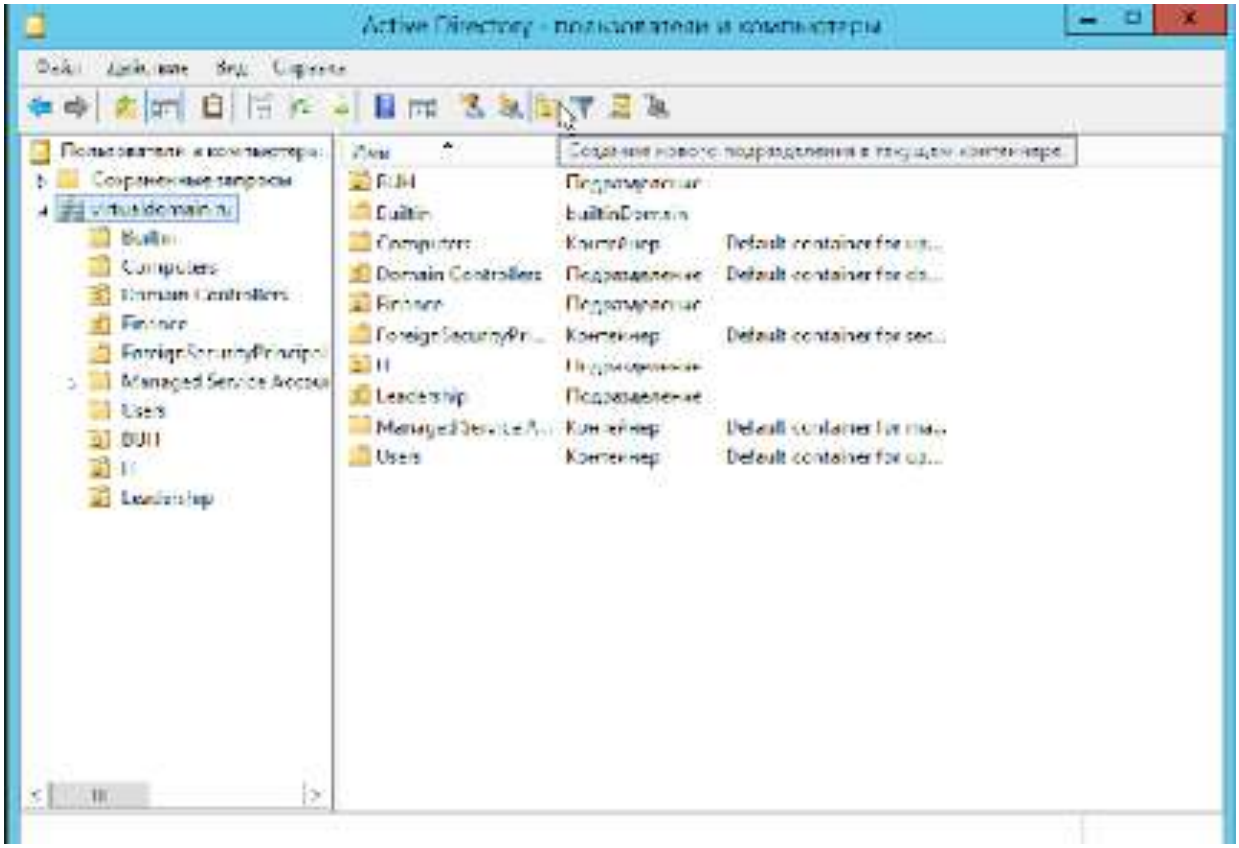
Далее необходимо перезапустить компьютер. При авторизации выбрать **Другой Пользователь**, и указываем логин и пароль пользователя. Чуть ниже можно увидеть, что мы в ходим в домен.



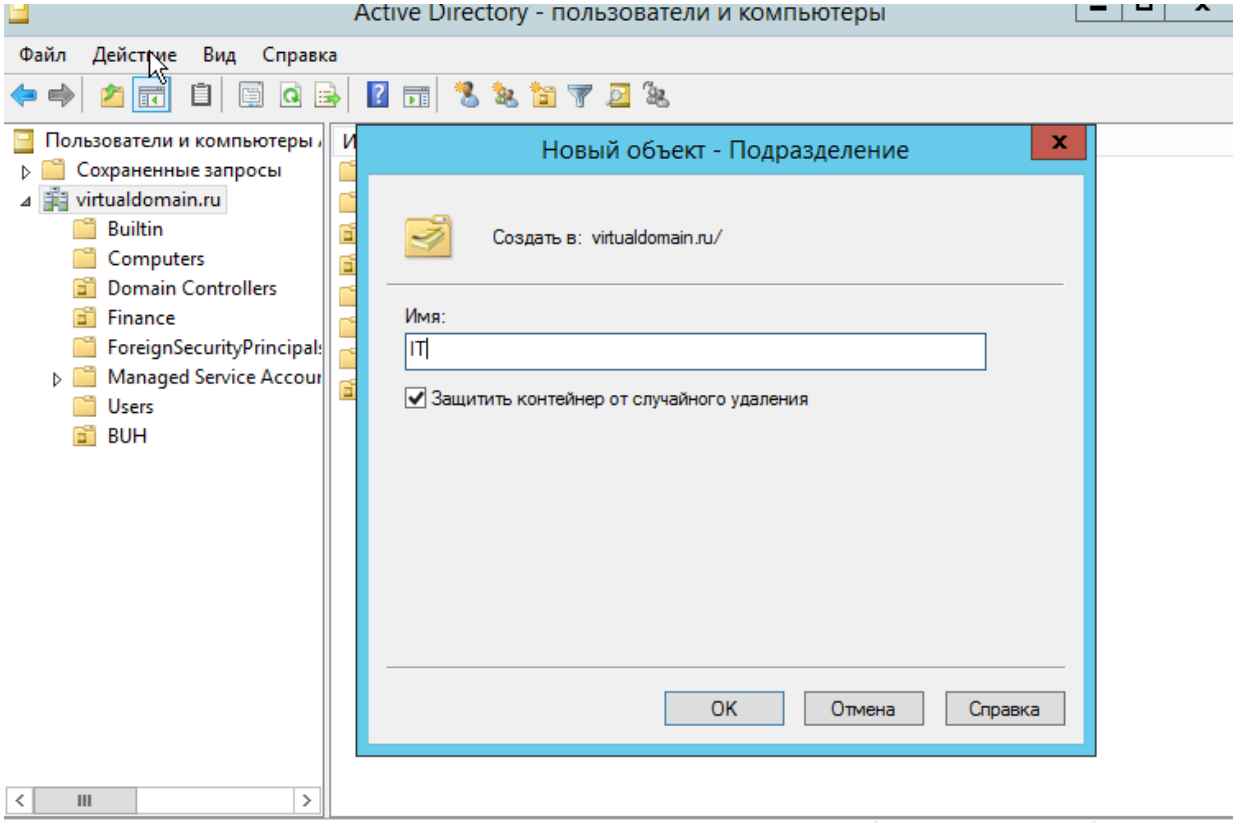
Далее заходим в **Система** и убеждаемся что компьютер в домене.

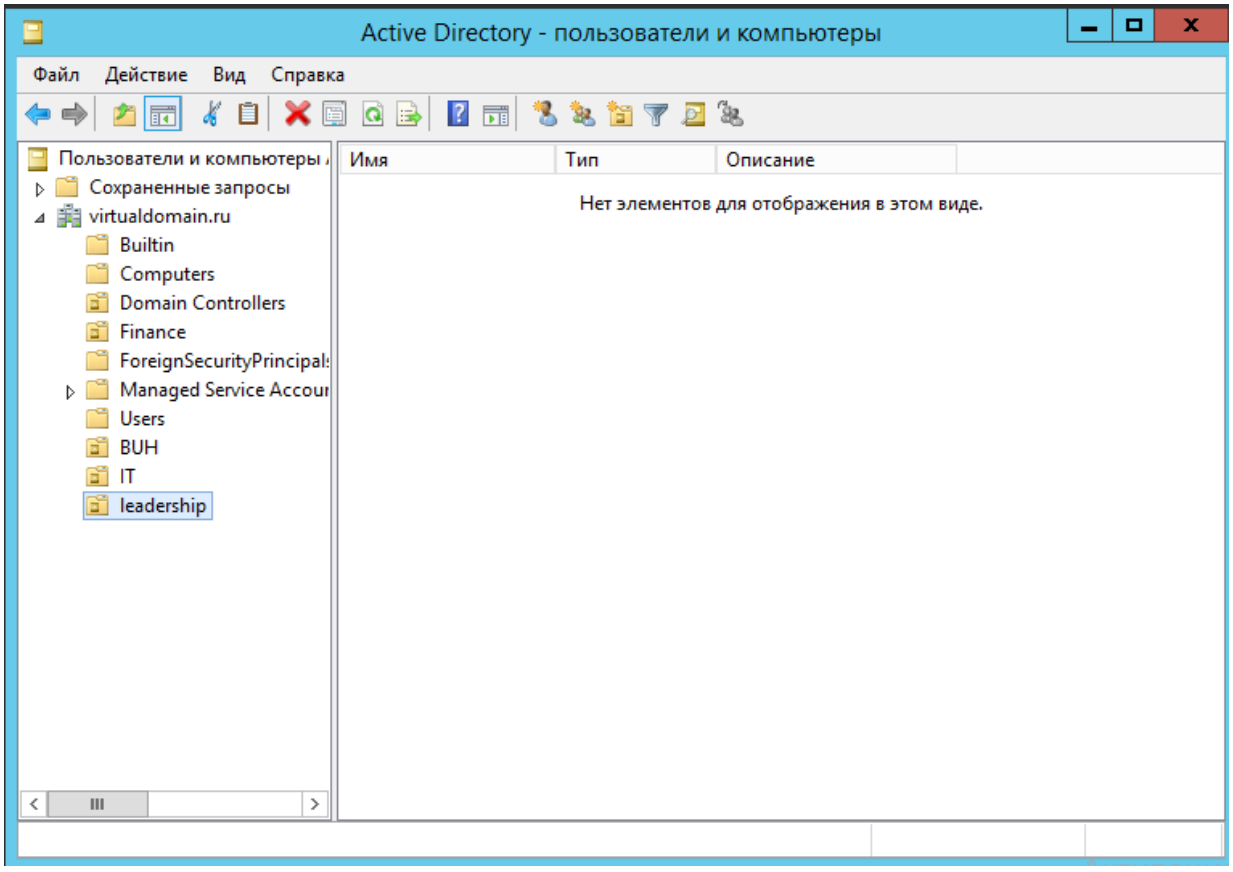


Необходимо выбрать **Создание нового подразделения в текущем контейнере**, выбрав сервер.

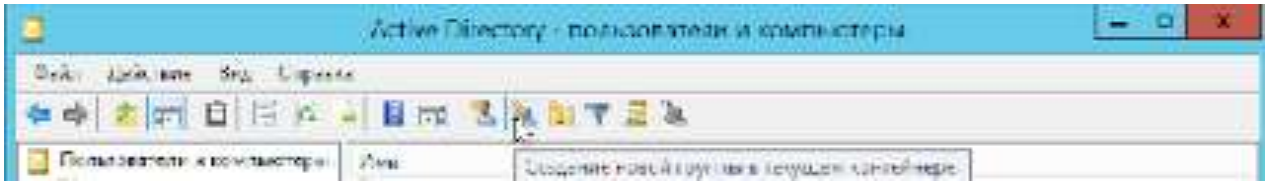


Выбираем Имя для группы, нажимаем **ОК**. Далее необходимо создать остальные подразделения, аналогичным способом.

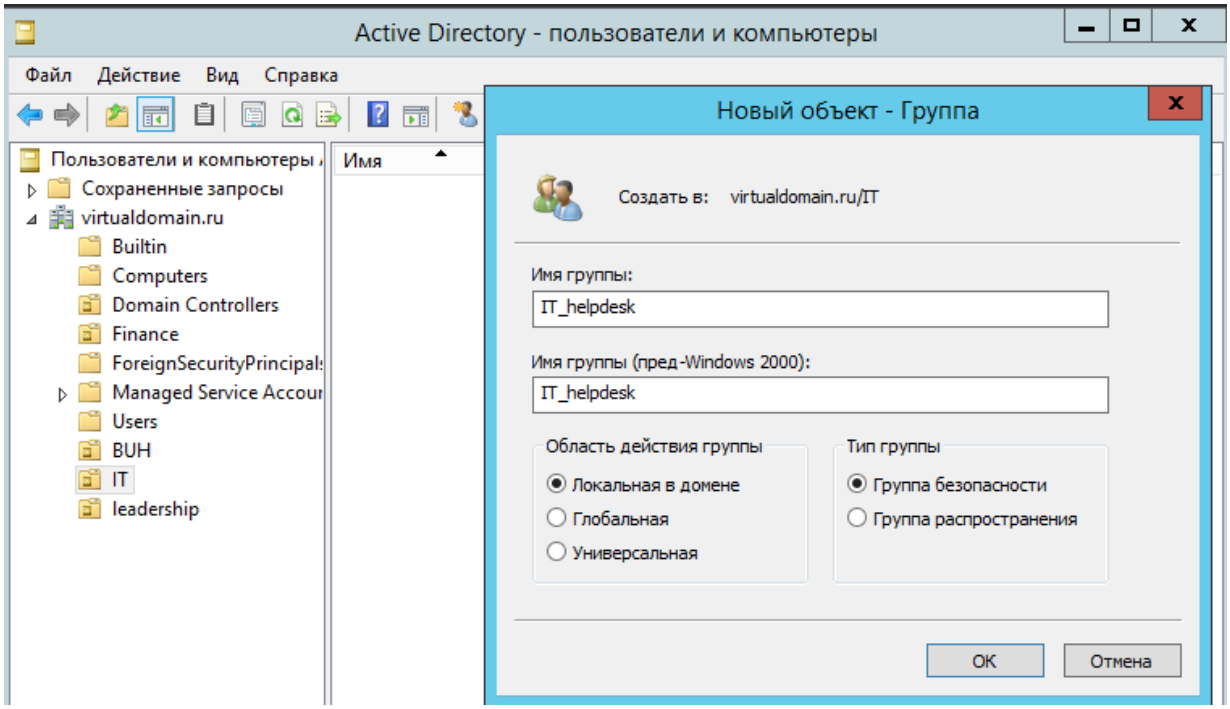


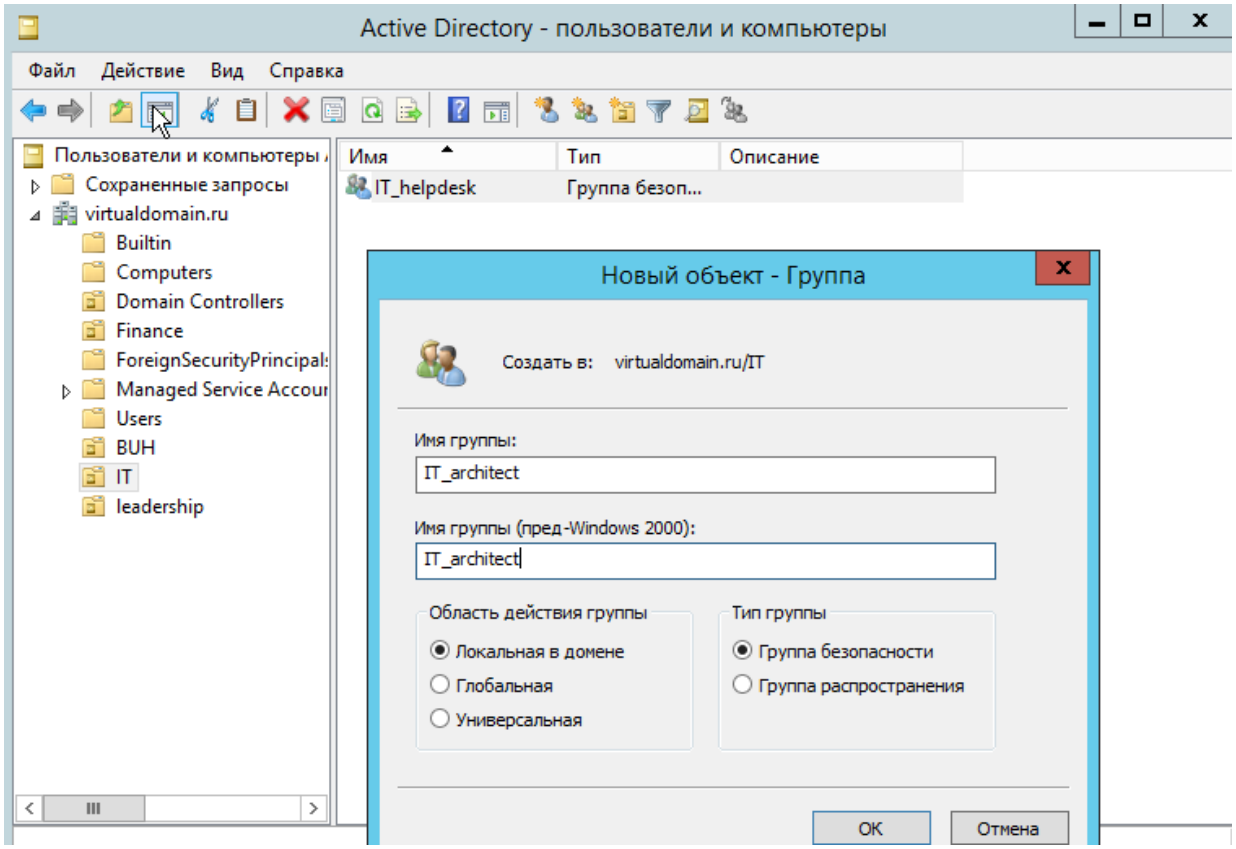


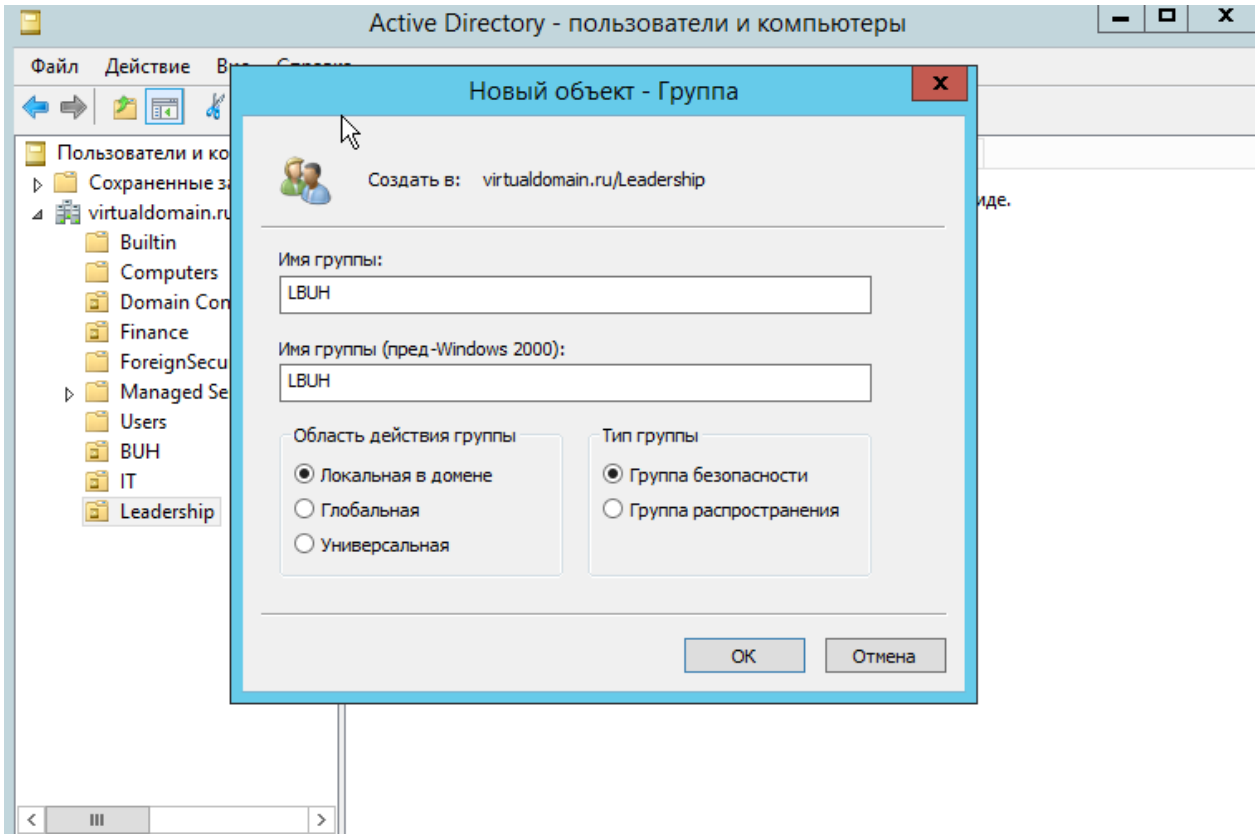
Далее необходимо создать группы в каждом из ранее созданных подразделений. Необходимо выбрать подразделение, нажать ПКМ и выбрать **Создать -> Группа** или на панели выбрать **Создание новой группы в текущем контейнере**.



Указываем Имя группы и выбираем Область действия группы. Далее нажимаем **ОК.** Аналогичным способом создаем группы в оставшихся подразделениях.

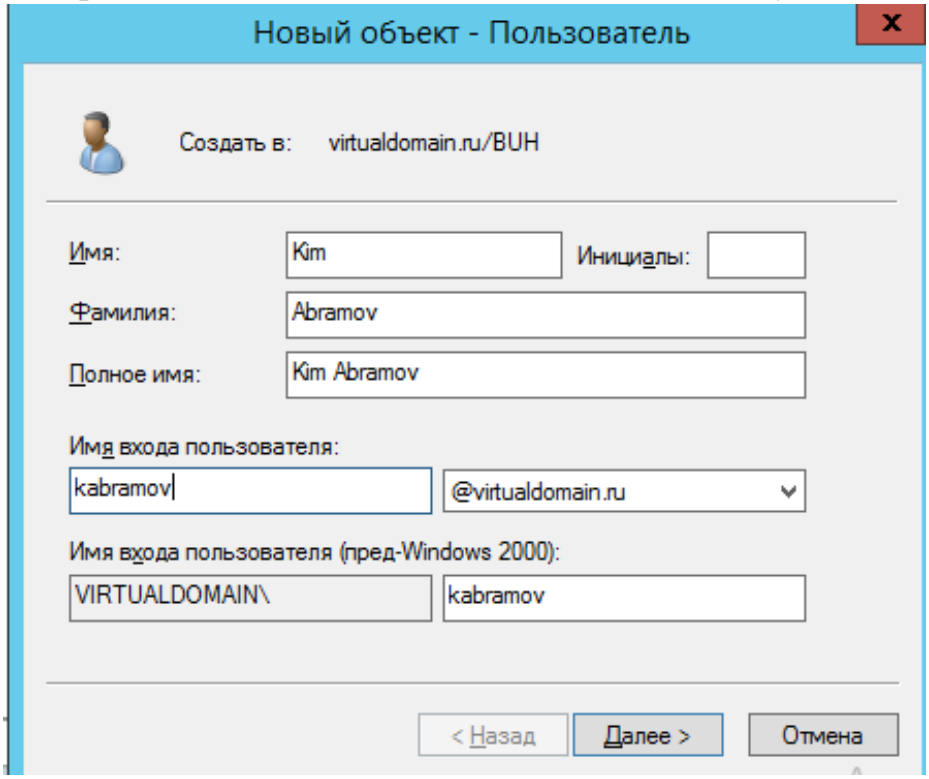




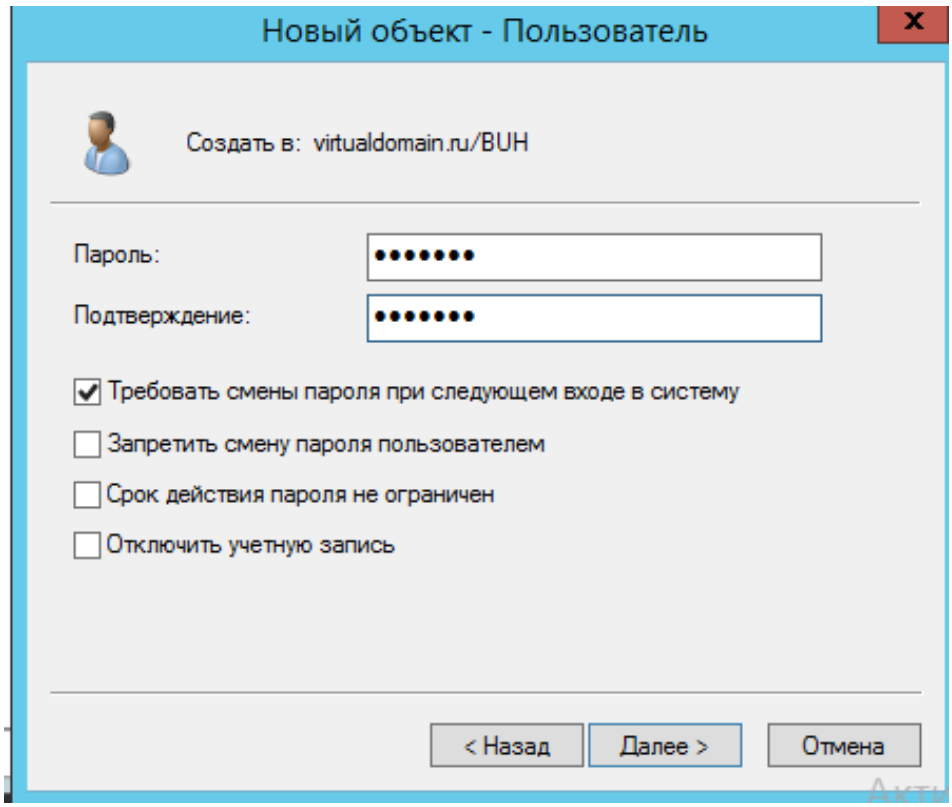


После создания Групп, необходимо создать пользователей. Выбираем подразделение, нажимаем ПКМ и выбираем **Создать -> Пользователь** или

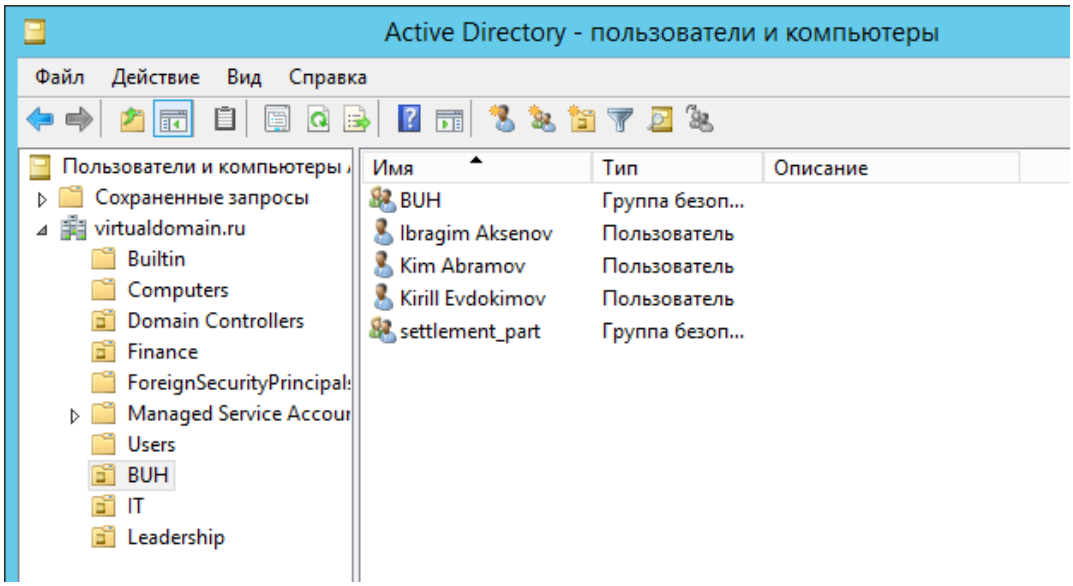
на панели выбрать **Создание нового пользователя в текущем контейнере**.

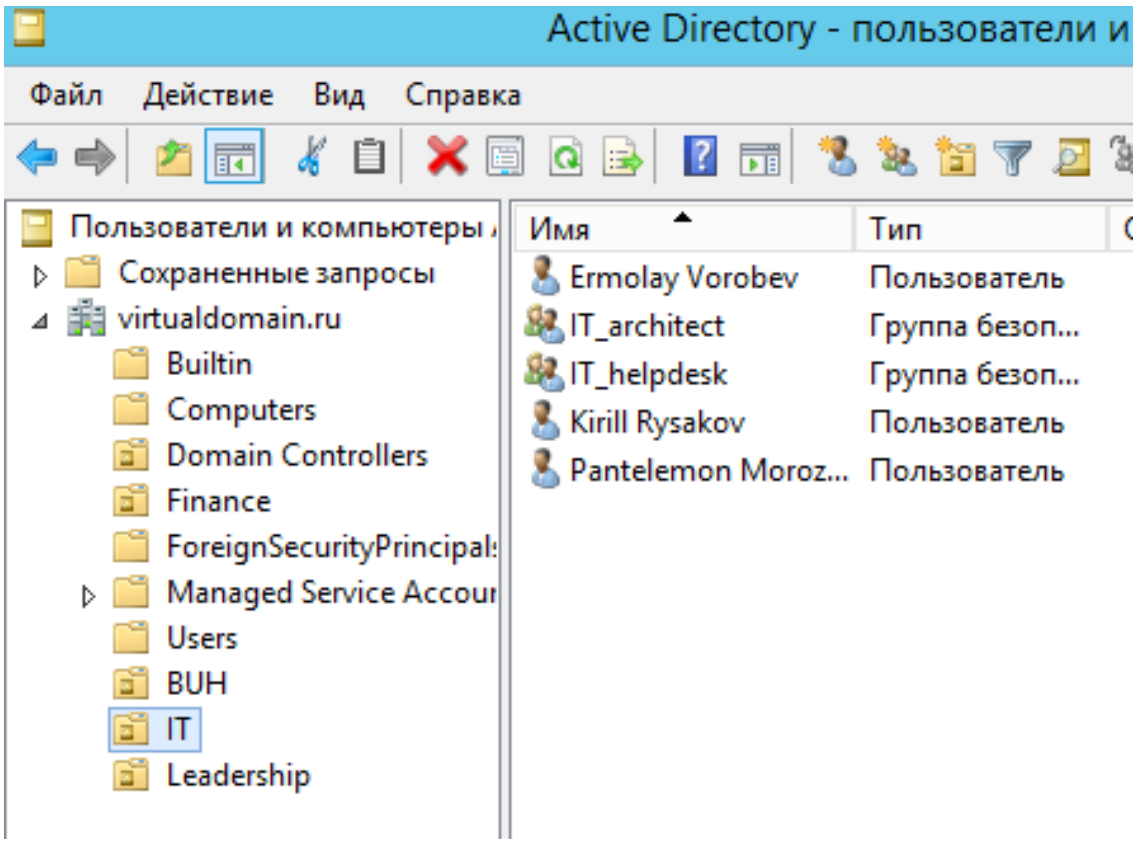


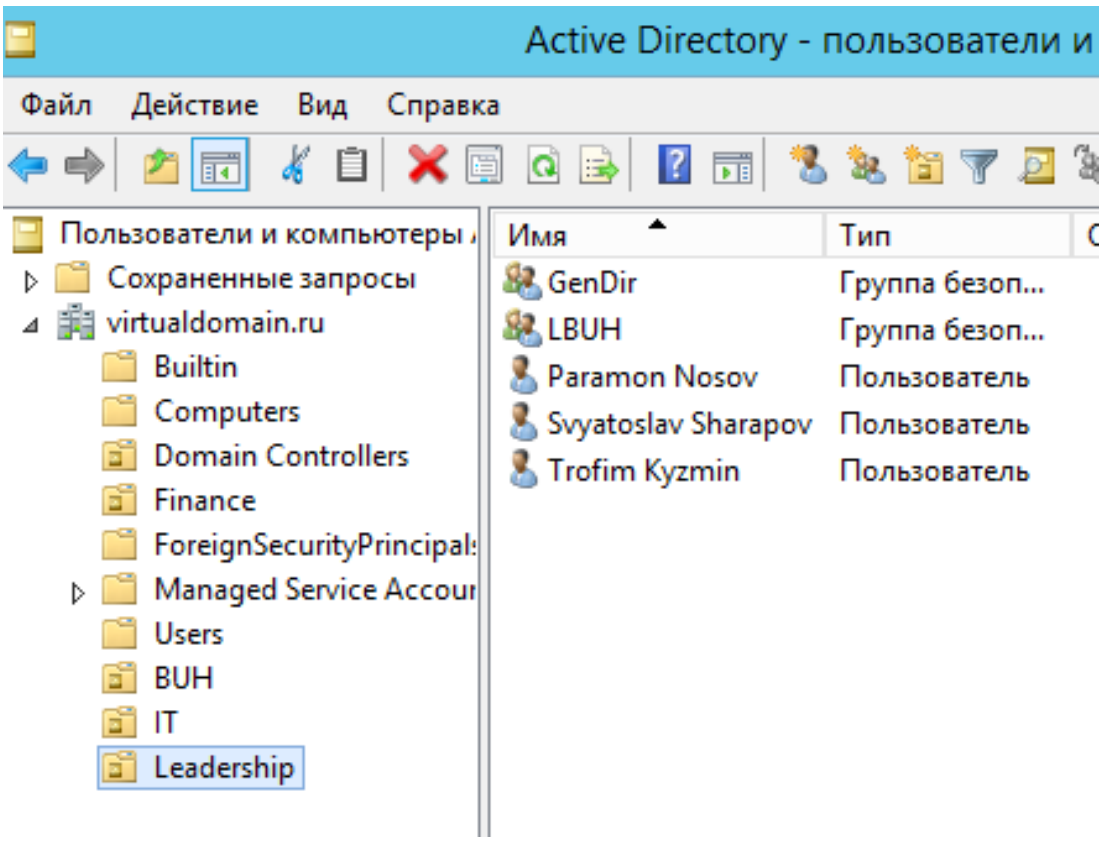
Указываем **Имя, Фамилию** при необходимости **Инициалы**. При это автоматически заполняется Полное имя. Далее необходимо указать **Имя входа пользователей**. Данное имя будет использовать далее при в ходе на ПК. Нажимаем **Далее**. Далее необходимо ввести пароль для пользователя. И указать дополнительный функции.



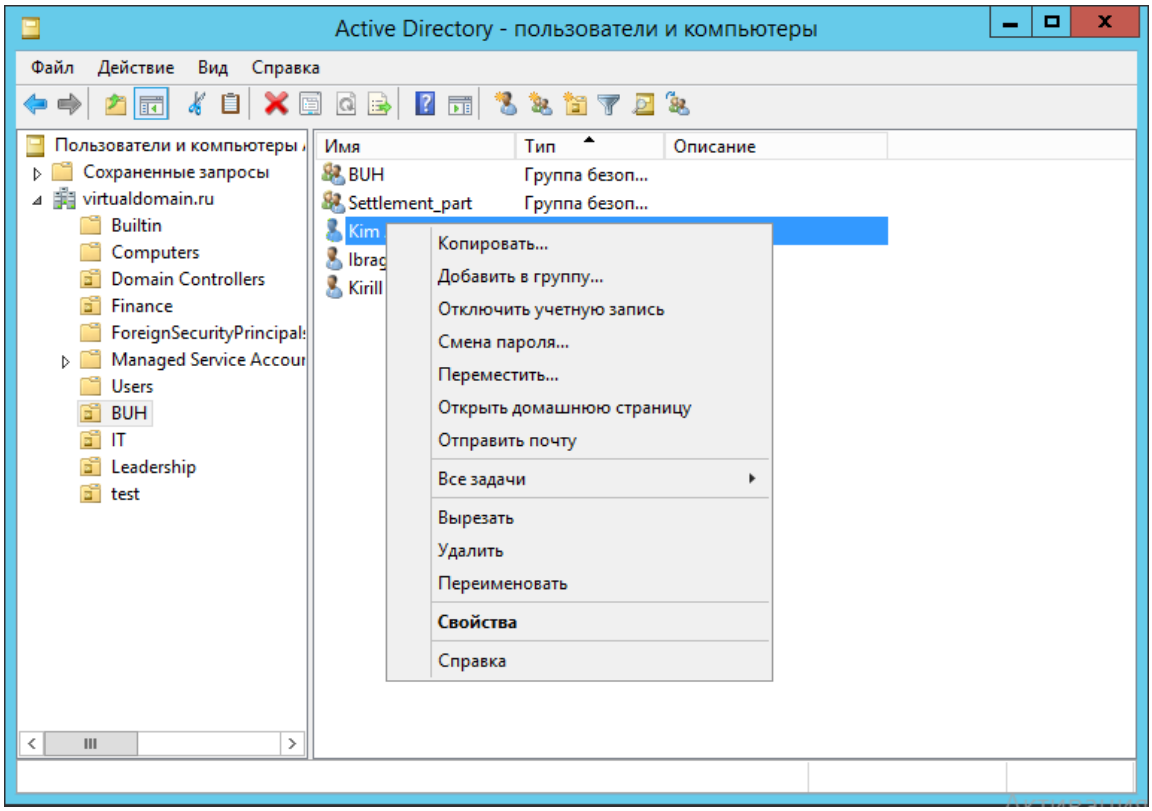
Далее необходимо аналогичным способом создать оставшихся пользователей в контейнеры.



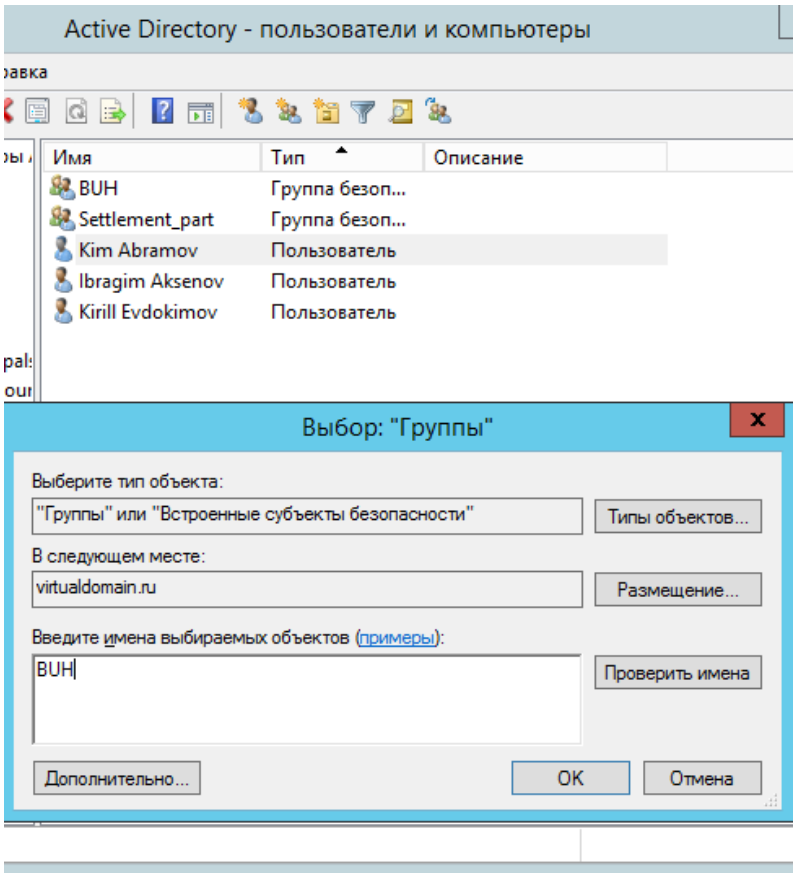




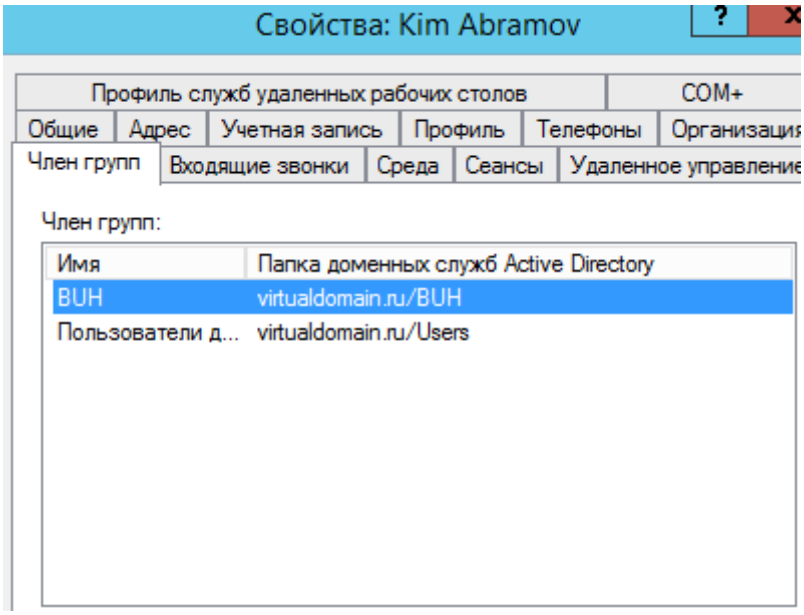
Далее необходимо созданных пользователей добавить в группы. Выбираем пользователя, нажимаем ПКМ и выбираем **Добавить в группу….**



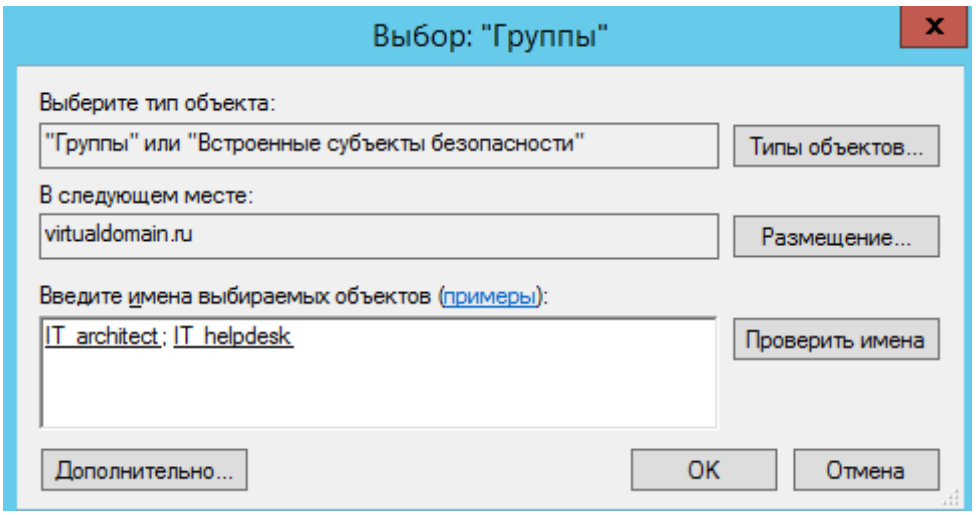
Далее в поле Введите имена выбираемых объектов, необходимо вписать Имя Группы, к которой они принадлежат. И нажать на **ОК.**



Что бы убедиться, что пользователь в группе, необходимо открыть его свойства. И перейти на вкладку член группы.

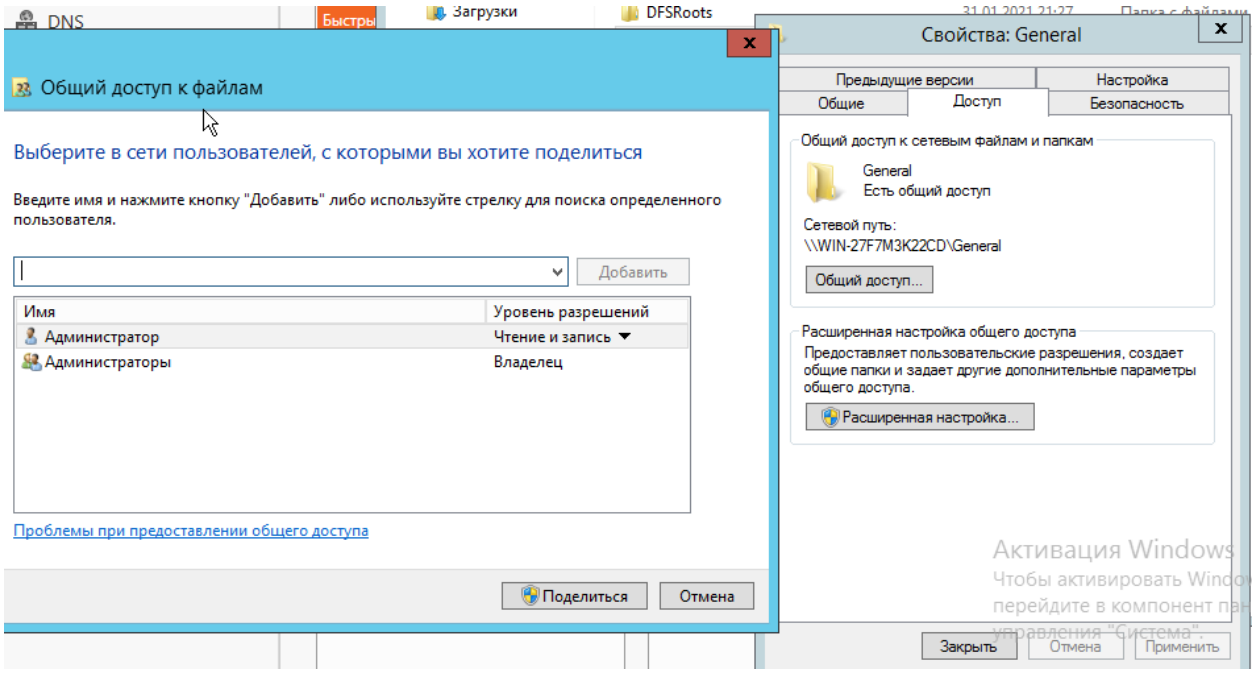


Так же, Группа, может находится в другой Группе. Например, LIT группа находится выше, чем IT_architect и IT_helpdesk.

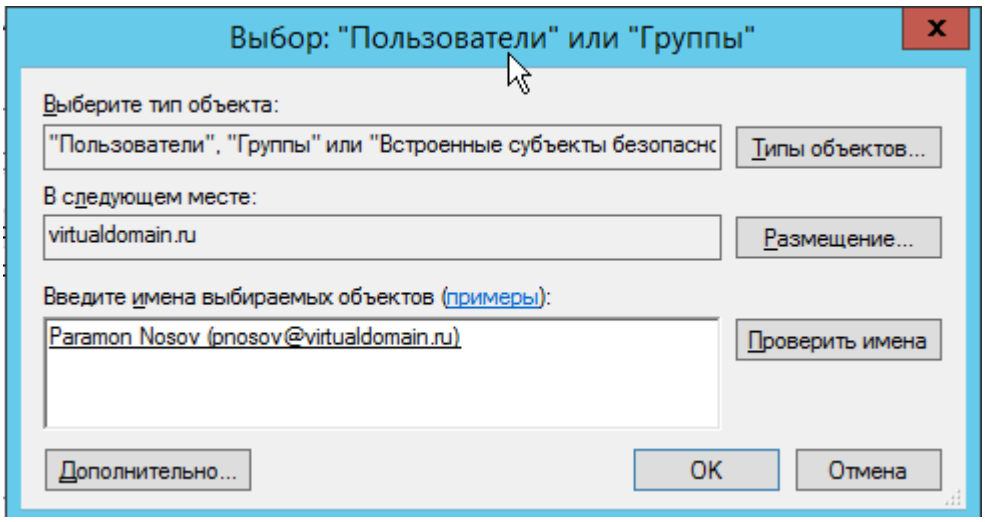


Далее необходимо создать папки, для которых чуть позже будем настраивать доступ.

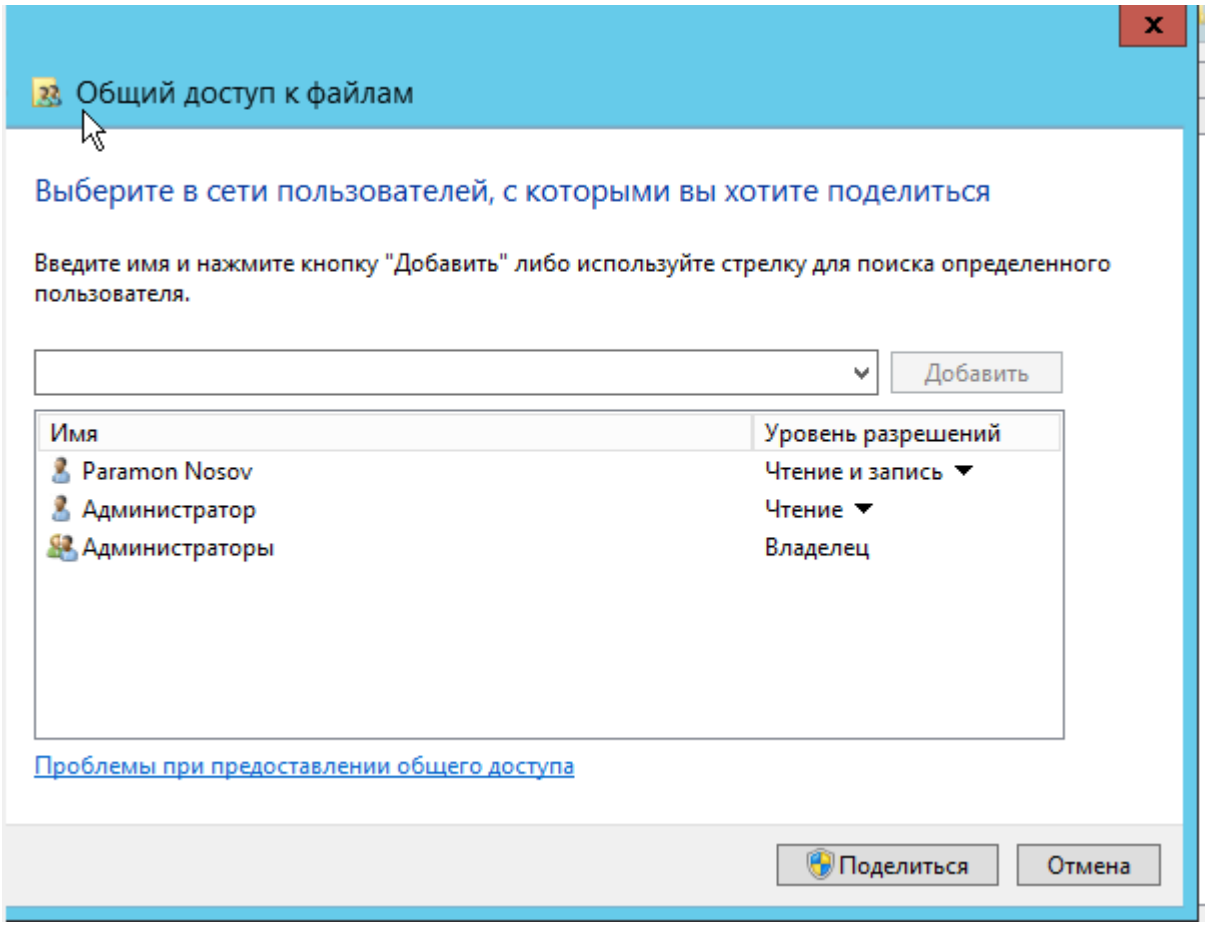
Открываем свойства папки. Переходим на вкладку доступ и нажимаем **Общий доступ**.



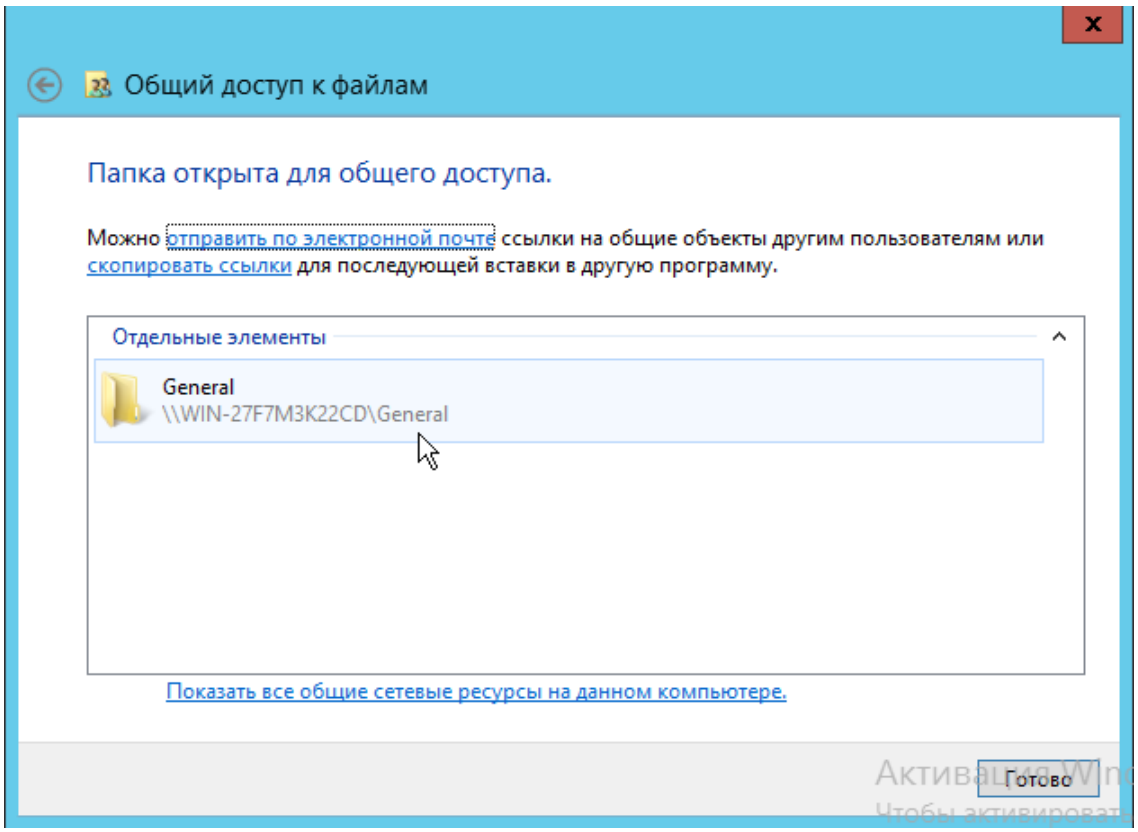
Далее необходимо добавить пользователя к которому есть допуск к выбранной папке и нажимаем **ОК**.



Наш первый пользователь виден в списке. Устанавливаем ему уровень разрешений. В данном случае **Чтение и запись.**



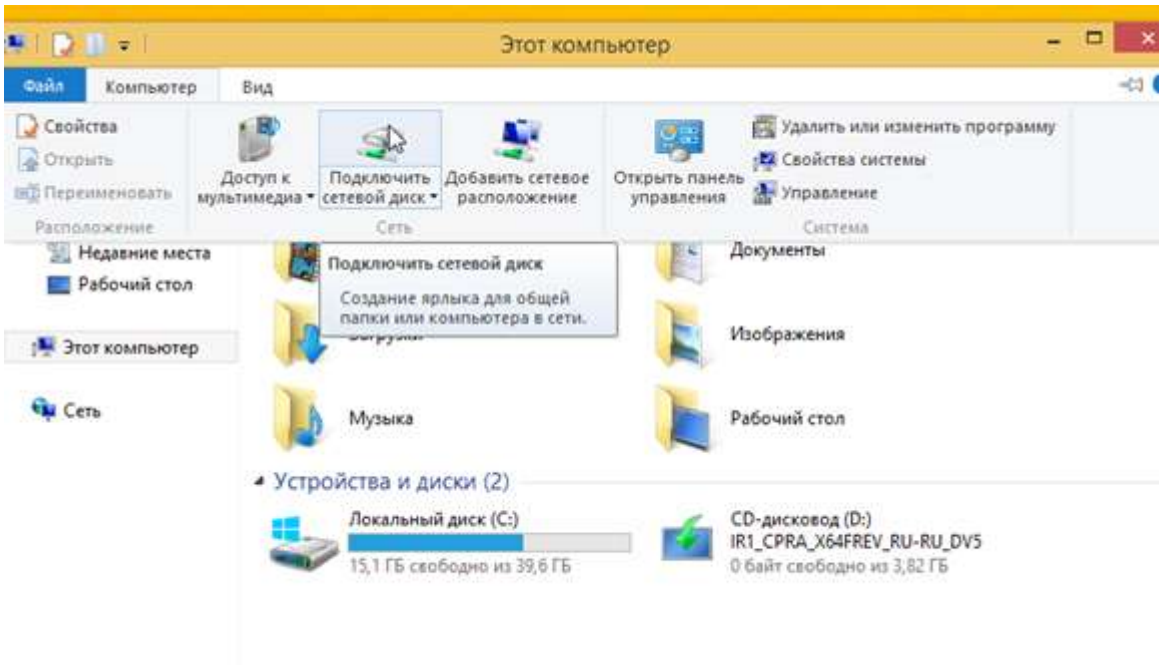
Далее добавляем оставшихся пользователей и нажимаем **Поделится.**



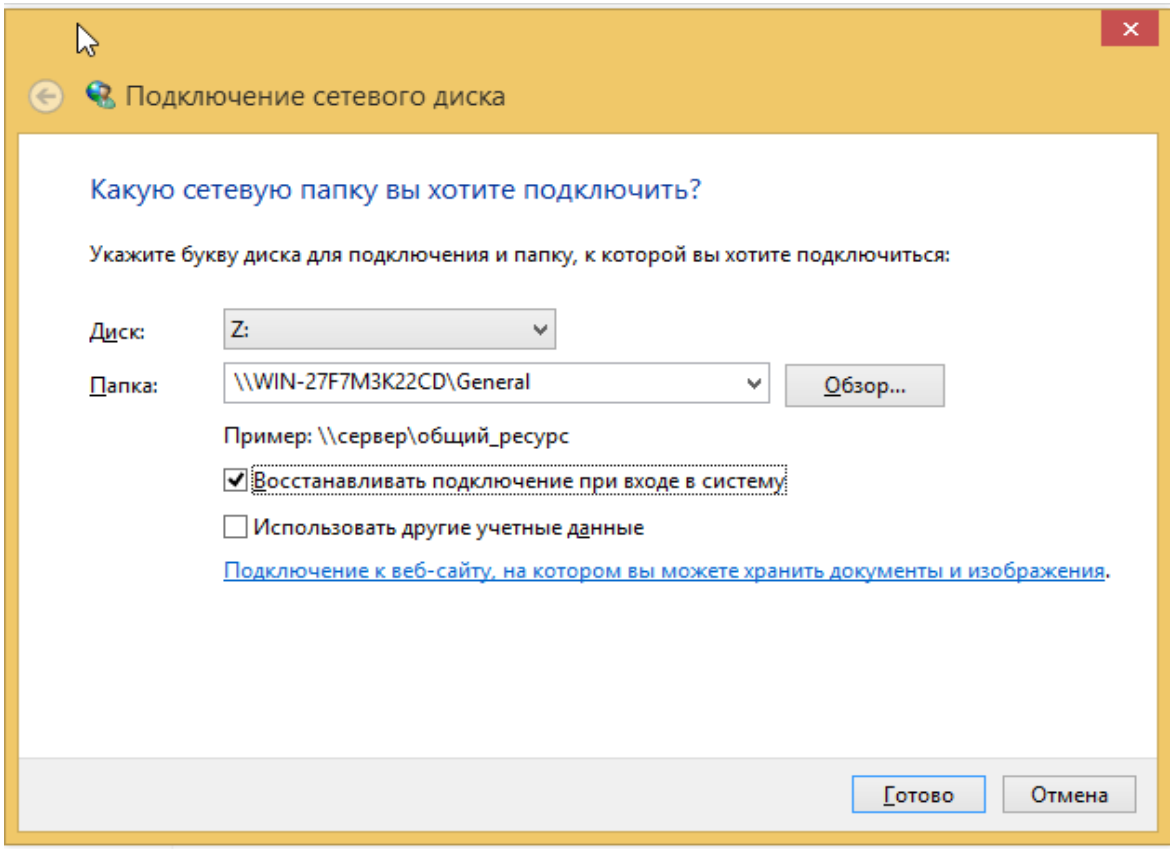
Аналогичным способом добавляем уровень разрешений для пользователей и папкам.

Далее необходимо каждому пользователю добавить общие папки.

Переходим на машину пользователя, заходит в нее под учетной записью созданного ранее пользователя. Далее переходим в Этот Компьютер. И нажимаем подключить сетевой диск.

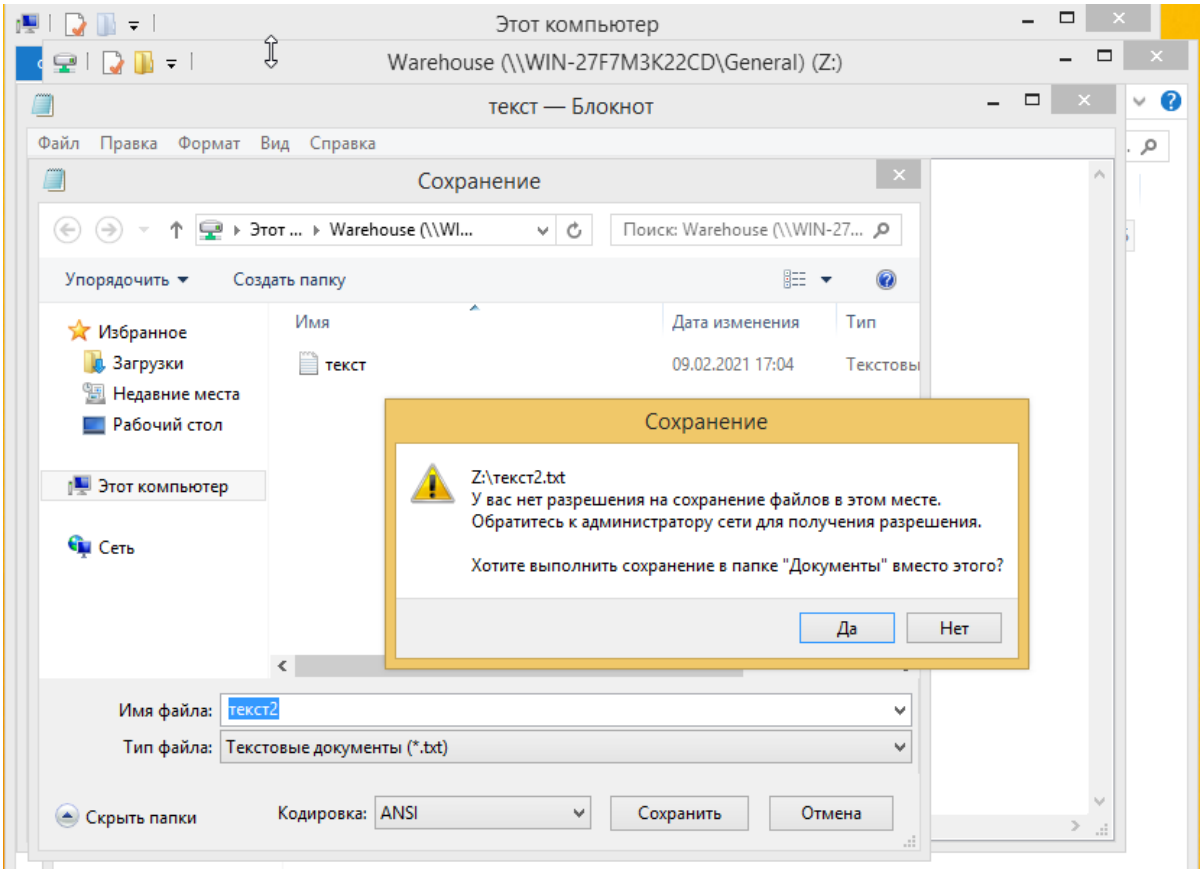


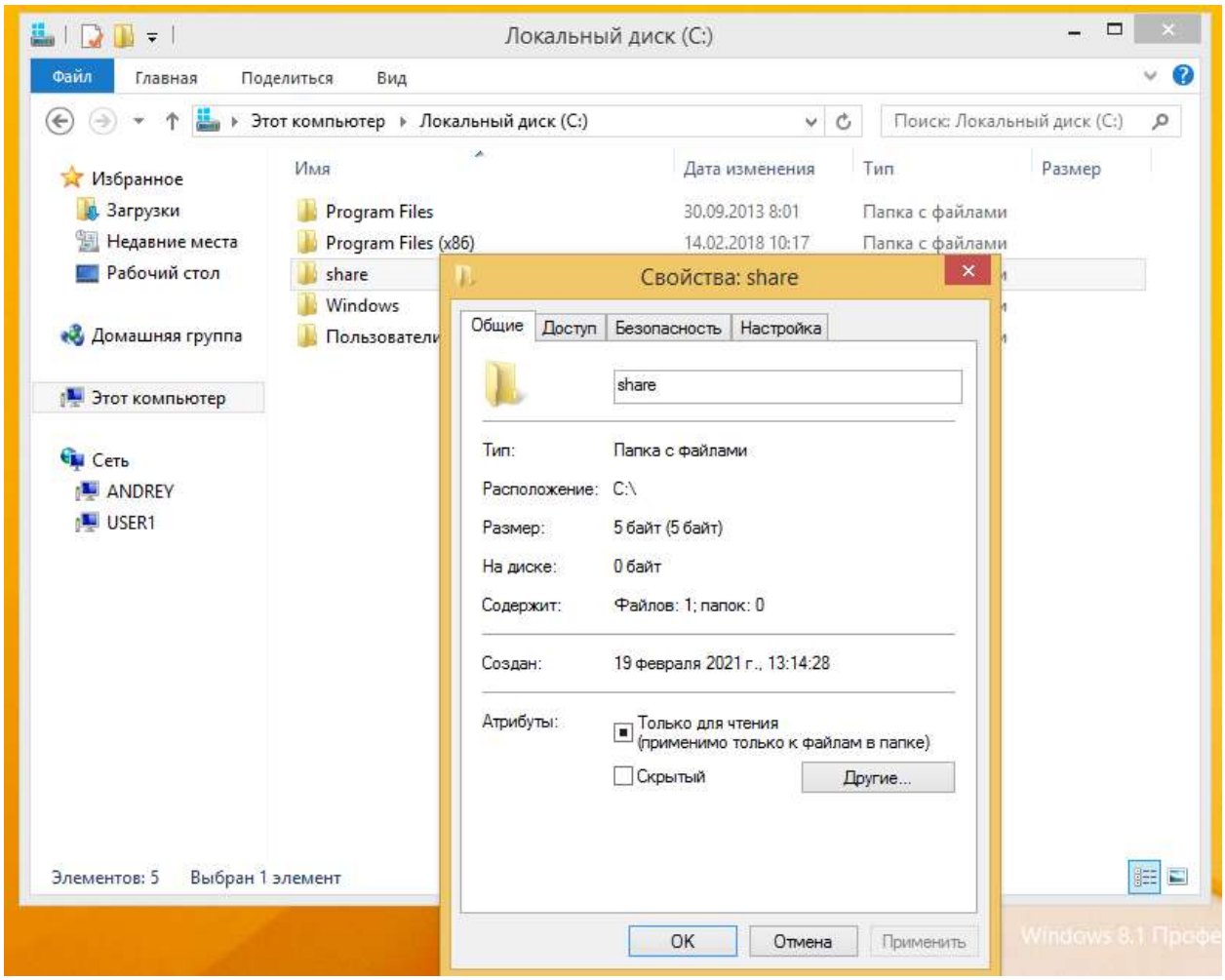
Указываем путь к папке и нажимаем готово



Автоматически у нас появляется сетевой диск в “Этот Компьютер”.

Пример демонстрации файла с правами **Чтение**




Локальный диск (C:)
Файл
Главная
Поделиться
Вид
Этот компьютер ▸ Локальный диск (C:)
Поиск: Локальный диск (C:)
Избранное
Загрузки
Недавние места
Рабочий стол
Домашняя группа
Этот компьютер
Сеть
ANDREY
USER1
Имя
Дата изменения
Тип
Размер
Program Files
30.09.2013 8:01
Папка с файлами
Program Files (x86)
14.02.2018 10:17
Папка с файлами
share
Windows
Пользовател
Элементов: 5
Выбран 1 элемент
Свойства: share
Общие
Доступ
Безопасность
Настройка
share
Тип:
Папка с файлами
Расположение:
C:\
Размер:
5 байт (5 байт)
На диске:
0 байт
Содержит:
Файлов: 1; папок: 0
Создан:
19 февраля 2021 г., 13:14:28
Атрибуты:
Только для чтения
(применимо только к файлам в папке)
Скрытый
Другие...
OK
Отмена
Применить