Министерство науки и высшего образования Российской федерации
Севастопольский государственный университет

АДМИНИСТРИРОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ

Методические указания
к лабораторным работам
по дисциплине
«Администрирование информационных систем»
для студентов дневной и заочной форм обучения
направления 09.03.02 «Информационные системы и технологии»

Севастополь
2020

СОДЕРЖАНИЕ

1 ЦЕЛЬ РАБОТЫ

Исследование возможностей, предоставляемых windows active directory.

2 КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

2.1СлужбакаталоговActiveDirectory - WindowsServer

ActiveDirectory – служба каталогов от корпорации Microsoftдля операционных систем семейства Windows Server. Служба позволяет администраторам использовать групповые политики для обеспечения единообразия настройки пользовательской рабочей среды, разворачивать программное обеспечение на множестве компьютеров через групповые политики или посредством System Center Configuration Manager, устанавливать обновления операционной системы, прикладного и серверного программного обеспечения на всех компьютерах в сети, используя службу обновления Windows Server. AD хранит данные о ресурсах (компьютерах, пользователях, серверах, сетевых и периферийных устройствах и т.д.) и настройки среды в централизованной базе данных.

Для реализации данного решения, необходим специальный сервер – **контроллер домена**. Именно он будет выполнять функции аутентификации пользователей и устройств в сети, а также выступать в качестве хранилища базы данных. При попытке использовать любой из объектов (ПК, сервер, принтер) сети, выполняется обращение к контроллеру домена, который либо разрешает это действие (есть необходимые права), либо блокирует его.

Основные возможности Windows AD:

– единая база регистрации пользователей, которая хранится централизованно на одном либо нескольких серверах; таким образом, при появлении нового сотрудника в офисе вам нужно будет всего лишь завести ему

учетную запись на сервере и указать, на какие рабочие станции он сможет получать доступ;

– поскольку все ресурсы домена индексируются, это дает возможность простого и быстрого поиска для пользователей; например, если нужно найти цветной принтер в отделе;

– совокупность применения разрешений NTFS, групповых политик и делегирования управления позволит вам тонко настроить и распределить права между участниками домена;

– перемещаемые профили пользователей дают возможность хранить важную информацию и настройки конфигурации на сервере; фактически, если пользователь, обладающий перемещаемым профилем в домене, сядет работать за другой компьютер и введет свои имя пользователя и пароль, он увидит свой рабочий стол с привычными ему настройками;

– с помощью групповых политик вы можете изменять настройки операционных систем пользователей, от разрешения пользователю устанавливать обои на рабочем столе до настроек безопасности, а также распространять по сети программное обеспечение, например, Volume Shadow Copy client и т. п.;

– многие программы (прокси-серверы, серверы баз данныхи др.) не только производства Microsoft на сегодняшний день научились использовать доменную аутентификацию, таким образом, вам не придется создавать еще одну базу данных пользователей, а можно будет использовать уже существующую;

– использование Remote Installation Services облегчает установку систем на рабочие места, но, в свою очередь, работает только при внедренной службе каталогов.

2.2Рабочие группы и домены

Рабочая группа – это логическая группировка компьютеров, объединенных общим именем для облегчения навигации в пределах сети, при этом принципиально важно, что каждый в рабочей группе равноправен (т. е. сеть получается одноранговой) и поддерживает собственную локальную базу данных учетных записей пользователей (Security Accounts Manager, SAM).

Отсюда вытекает основная проблема, которая не позволяет использовать рабочие группы в крупных корпоративных сетях.

Действительно, вход в защищенную систему является обязательным, а непосредственный и сетевой входы принципиально различаются (непосредственный контролируется локальным компьютером, а сетевой — удаленным), то, например, пользователю, вошедшему на компьютер Comp1 под локальной учетной записью User1, будет отказано в доступе к принтеру, установленному на компьютере Comp2, поскольку в его локальной базе нет пользователя с именем User1.

Таким образом, для обеспечения «прозрачного» взаимодействия в рабочей группе нужно создавать одинаковые учетные записи с одинаковыми паролями на всех компьютерах, где работают пользователи и расположены ресурсы. В ОС Windows для рабочих групп предусмотрен специальный режим: «Использовать простой общий доступ к файлам», позволяющий обойти указанную проблему (данный режим включен по умолчанию). Понятно, что управлять учетными записями и ресурсами в рабочей группе можно только при небольшом количестве компьютеров и пользователей, однако увеличении их числа начинают возникать трудности, поэтому в крупных сетях следует применять домены.

Домены–это основная логическая единица построения. В сравнении с рабочими группами домены AD – это группы безопасности, имеющие единую базу регистрации, тогда как рабочие группы – это всего лишь логическое объединение машин. AD использует для именования и службы поиска DNS (Domain Name Server – сервер имен домена), а не WINS (Windows Internet Name

Service – сервис имен Internet), как это было в ранних версиях NT. Таким образом, имена компьютеров в домене имеют вид, например, buh.work.com, где buh – имя компьютера в домене work.com.

Группы пользователей и компьютеров –используются для административных целей и имеют такой же смысл, как и при использовании на локальных машинах в сети. В отличие от OU, к группам нельзя применять групповые политики, но для них можно делегировать управление. В рамках схемы Active Directory выделяют два вида групп: группы безопасности (применяются для разграничения прав доступа к объектам сети) и группы распространения (применяются в основном для рассылки почтовых сообщений, например, в сервере Microsoft Exchange Server).

Они подразделяются по области действия:

– универсальные группы могут включать в себя пользователей в рамках леса, а также другие универсальные группы или глобальные группы любого домена в лесу;

– глобальные группы домена могут включать в себя пользователей домена и другие глобальные группы этого же домена;

– локальные группы домена используются для разграничения прав доступа, могут включать в себя пользователей домена, а также универсальные группы и глобальные группы любого домена в лесу;

– локальные группы компьютеров – группы, которые содержит SAM (security account manager) локальной машины. Область их распространения ограничивается только данной машиной, но они могут включать в себя локальные группы домена, в котором находится компьютер, а также универсальные и глобальные группы своего домена или другого, которому они доверяют. Например, вы можете включить пользователя из доменной локальной группы Users в группу Administrators локальной машины, тем самым дав ему права администратора, но только для этого компьютера.

2.3 Лес ActiveDirectory

Лес Active Directory – определяет набор одного или нескольких доменов, использующих одни и те же схему, конфигурацию и глобальный каталог. Кроме этого, все домены участвуют в двусторонних транзитивных отношениях доверия. Обратим внимание на термины, которые используются в определении леса:

Схема– схема Active Directory используется совместно всеми доменами в пределах леса. Схема — это конфигурационная информация, которая управляет структурой и содержимым каталога.

Конфигурация– конфигурация определяет логическую структуру леса, например, число и конфигурацию сайтов в пределах леса.

Глобальный каталог– глобальный каталог можно воспринимать в виде справочника для леса. Глобальный каталог содержит информацию о всех объектах леса включая информацию о расположении объектов.

Доверие – доверие предоставляет различным доменам возможность работать вместе. Без доверия домены работают как отдельные сущности, то есть пользователи из домена A не смогут получать доступ к ресурсам в домене B. Если отношение доверия устанавливается между доменами таким образом, что домен B доверяет домену A, то пользователи домена A смогут получать доступ к ресурсам домена B, если у них есть соответствующие разрешения.

Существует три основных типа отношений доверия:

Транзитивные – транзитивные отношения доверия создаются автоматически между доменами одного леса. Они позволяют пользователям любого домена потенциально получать доступ к ресурсам любого другого домена этого леса, если у пользователей есть соответствующие права доступа.

Shortcut – это отношение доверия между доменами одного леса, которые уже имеют транзитивное отношение доверия. Такое отношение доверия

предоставляет более быструю аутентификацию и проверку доступа к ресурсам между несоседними доменами леса.

Внешние – внешние отношения доверия позволяют доменам из различных лесов совместно использовать ресурсы. Такие отношения доверия не являются транзитивными, то есть они относятся только к тем доменам, для которых они создавались.

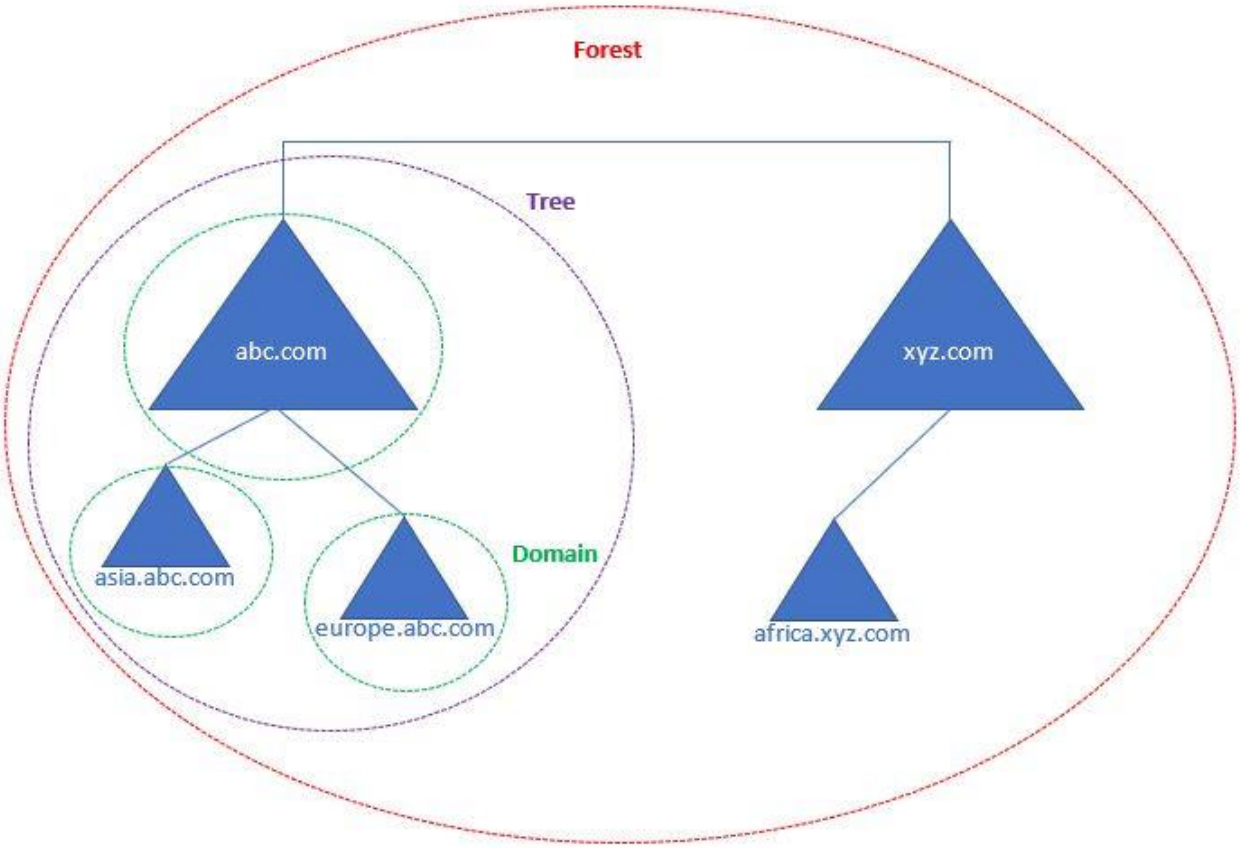

Рисунок 2.3.1 – Структура леса AD

2.4 Ресурсная запись и ее элементы

Ресурсная запись (RR – Resource Record) – единица хранения и передачи информации в DNS, включающая в себя следующие элементы (поля):

– Имя (Name) – имя домена, к которому относится запись;

– TTL (Time To Live) – допустимое время хранения записи неответственным сервером;

– Тип (Type) – параметр, определяющий назначение и формат записи в поле данных (Rdata);

– Класс (Class)– тип сети передачи данных (подразумевается возможность DNS работать с типами сетей, отличных от TCP/IP);

– Длина поля данных (Rdlen);

– Поле данных (Rdata) – содержание и формат поля зависят от типа записи.

Ниже представлены типы ресурсных записей (зоны), используемые чаще всего:

– A (IPv4 Address Record – адресная запись) – связывает доменное имя с IPv4-адресом хоста;

– AAAA (IPv6 Address Record) – связывает доменное имя с IPv6-адресом хоста (аналогично A-записи);

– CNAME (Canonical Name Record – каноническая запись имени) – используется для перенаправления на другое доменное имя;

– MX (Mail Exchange – почтовый обменник) – ссылается на почтовый сервер, обслуживающий домен;

– NS (NameServer– сервер имен) – ссылается на DNS-сервер, ответственный за домен;

– TXT – текстовое описание домена. Зачастую требуется для выполнения специфических задач (например, подтверждения права собственности на домен при привязке его к почтовому сервису);

– PTR (Point to Reverse – запись указателя) – связывает IP-адрес машины с доменом, используется преимущественно для проверки сторонними почтовыми сервисами отправляемых через эту машину электронных писем на отношение к домену, указанному в параметрах почтового сервера. При несоответствии этих параметров письмо проверяется более тщательно по другим критериям.

2.5Обратный просмотр DNS

Обратный просмотр DNS (англ. *reverseDNSlookup*)–обращение к особой доменной зоне для определения имени узла по его IP-адресу с помощью PTR-записи.

Для выполнения запроса адрес узла переводится в обратную нотацию:

IPv4-адрес *192.168.0.1* превращается в *1.0.168.192.in-addr.arpa*.

Благодаря иерархической модели управления именами появляется возможность делегировать управление зоной владельцу диапазона IP-адресов. Для этого в записях авторитетного DNS-сервера указывают, что за зону CCC.BBB.AAA.in-addr.arpa (то есть за сеть AAA.BBB.CCC.000/24) отвечает отдельный сервер.

Количество PTR-записей, описывающих разные имена, на один адрес не ограничивается спецификациями, но может ограничиваться размером UDP-пакета, так как DNS-сервер инкапсулирует свой ответ в UDP. В большинстве случаев для одного IP-адреса создаётся только одна PTR-запись, но бывает и так, что их создаётся множество – например, когда IP-адрес используется для нескольких виртуальных серверов с разными именами.

3 ПРИМЕР ВЫПОЛНЕНИЯ РАБОТЫ

Установка и настройка DNS-сервера и Active Directory в Windows Server 2019 практически не отличается от предыдущих выпусков серверов компании Microsoft, таких как Windows Server 2012, 2008. В несколько шагов устанавливается роль DNS и Доменные службы Active Directory, также для сервера имён потребуется небольшая настройка.

До установки ролей сервера, требуется задать имя будущему серверу, а также статический IP-адрес.

Требуется нажать правой клавишей мыши на "Этот компьютер" и выбрать "Свойства". В открывшемся окне –"Изменить параметры" – "Изменить". Необходимо задать имя компьютера и нажать "ОК". Для того, чтобы изменения вступили в силу, требуется перезагрузить компьютер.

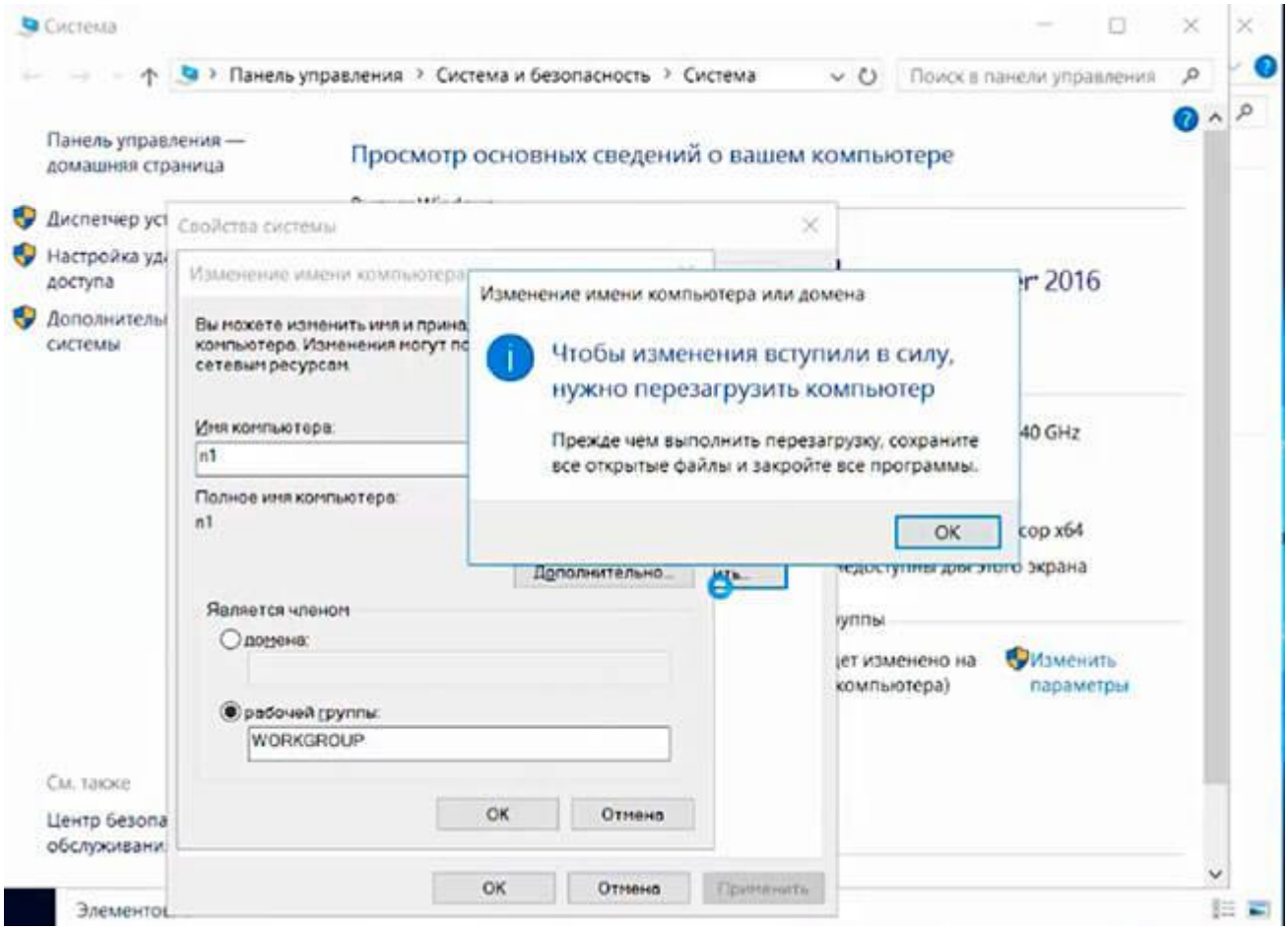

Рисунок 3.1– Установка имени компьютера

Для того, чтобы открыть сетевые соединения, в поле "Поиск" вводится команда**ncpa.cpl**, далеевыполняется выбор нужного сетевого интерфейса: правой клавишей мыши –"Свойства". В версии IP (TCP/IPv4) устанавливается IP-адрес. Пример:

IP-адрес: адрес сервера (например, 10.32.94.11)

Маска подсети: маска сети (например, 255.255.255.0)

Основной шлюз: шлюз, если имеется (например, 10.32.94.1)

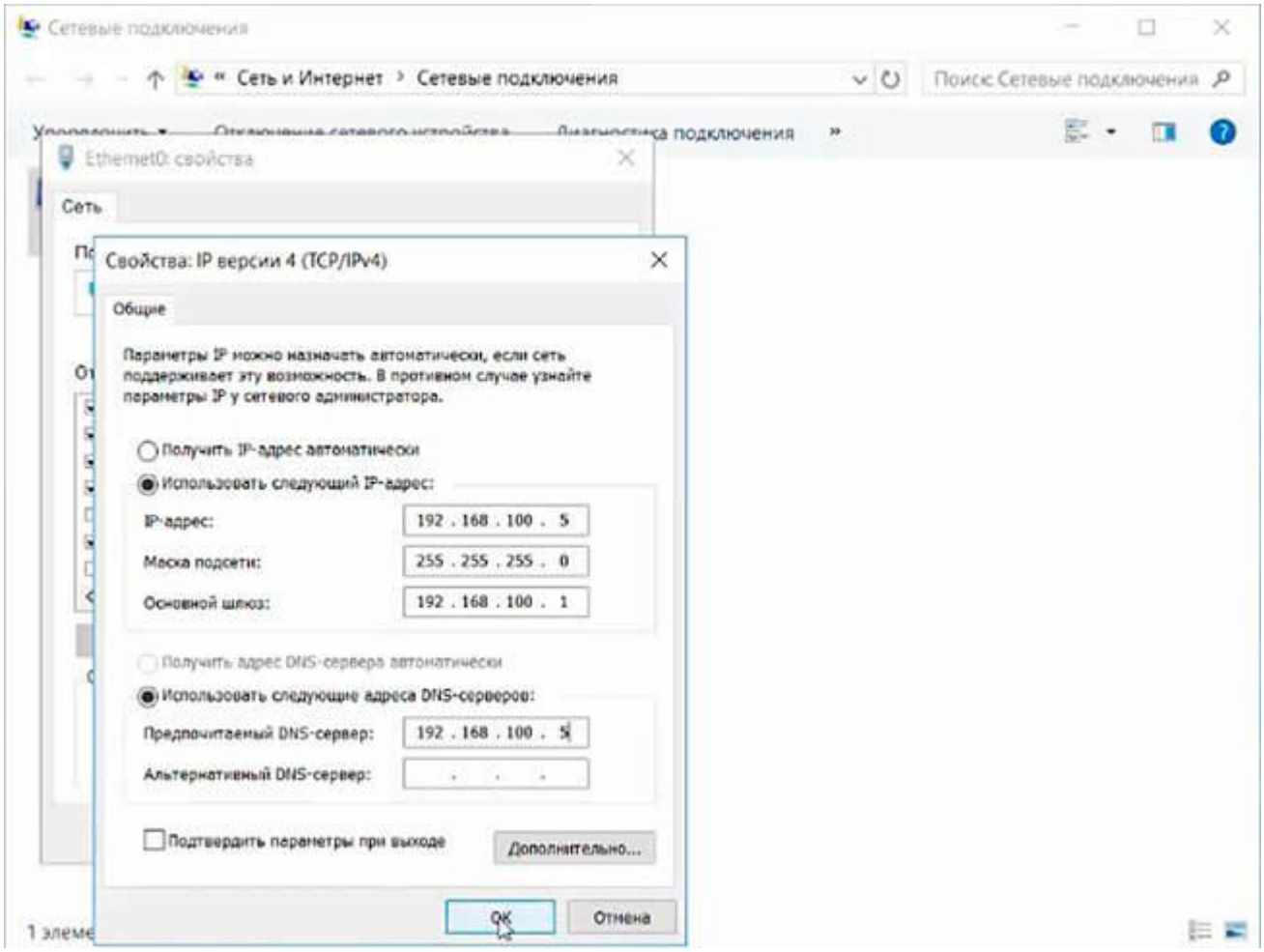

Рисунок 3.2– Установка IP-адреса компьютера

Далее можно начать установку ролей сервера. Для этого необходимо выбрать "Диспетчер серверов".

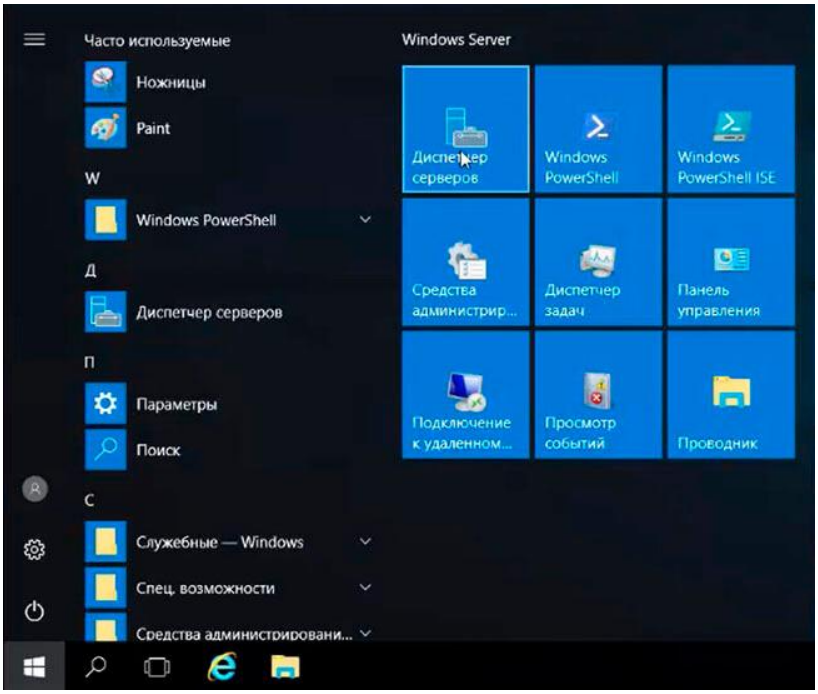

Рисунок 3.3– Выбор Диспетчера серверов в «Пуск»

В следующем окне выбрать пункт "Добавить роли и компоненты".

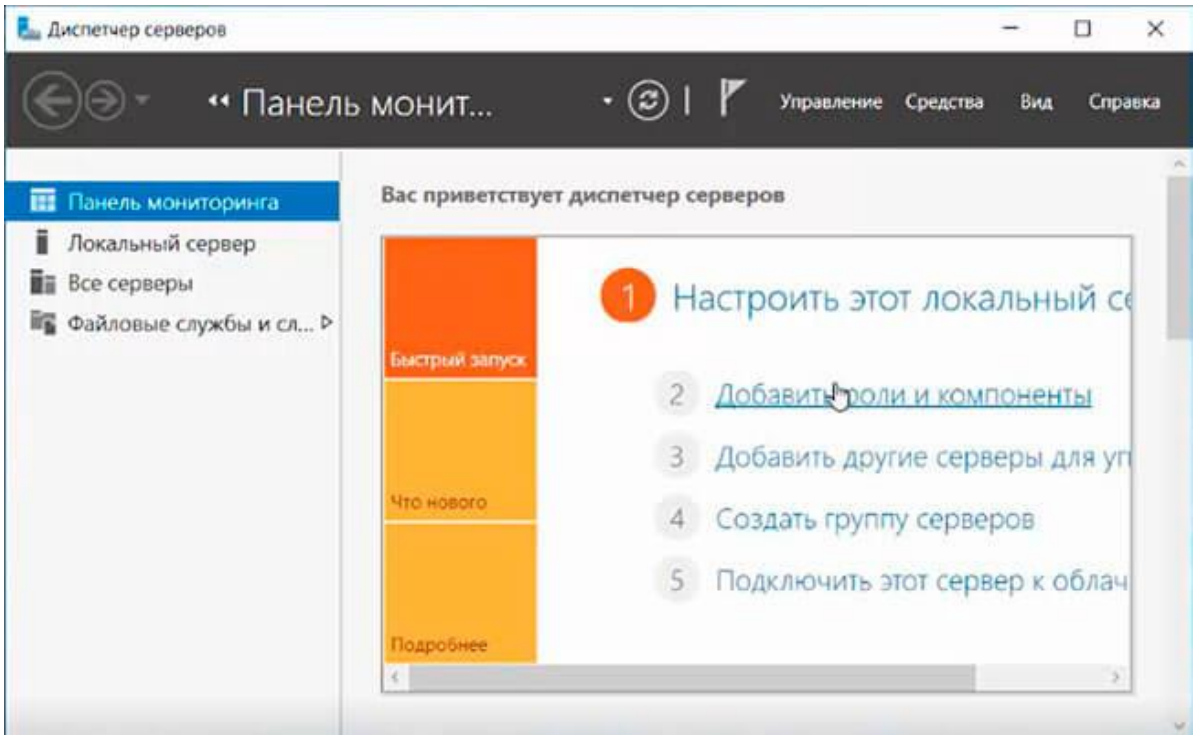

Рисунок 3.4– Окно Диспетчера серверов

Требуется прочитать инструкцию "Перед началом работы" и нажать "Далее". Затем оставить по умолчанию чекбокс "Установка ролей или компонентов" и снова нажать на "Далее". В следующем окне выбирать сервер, на который будут установлены роли и "Далее".

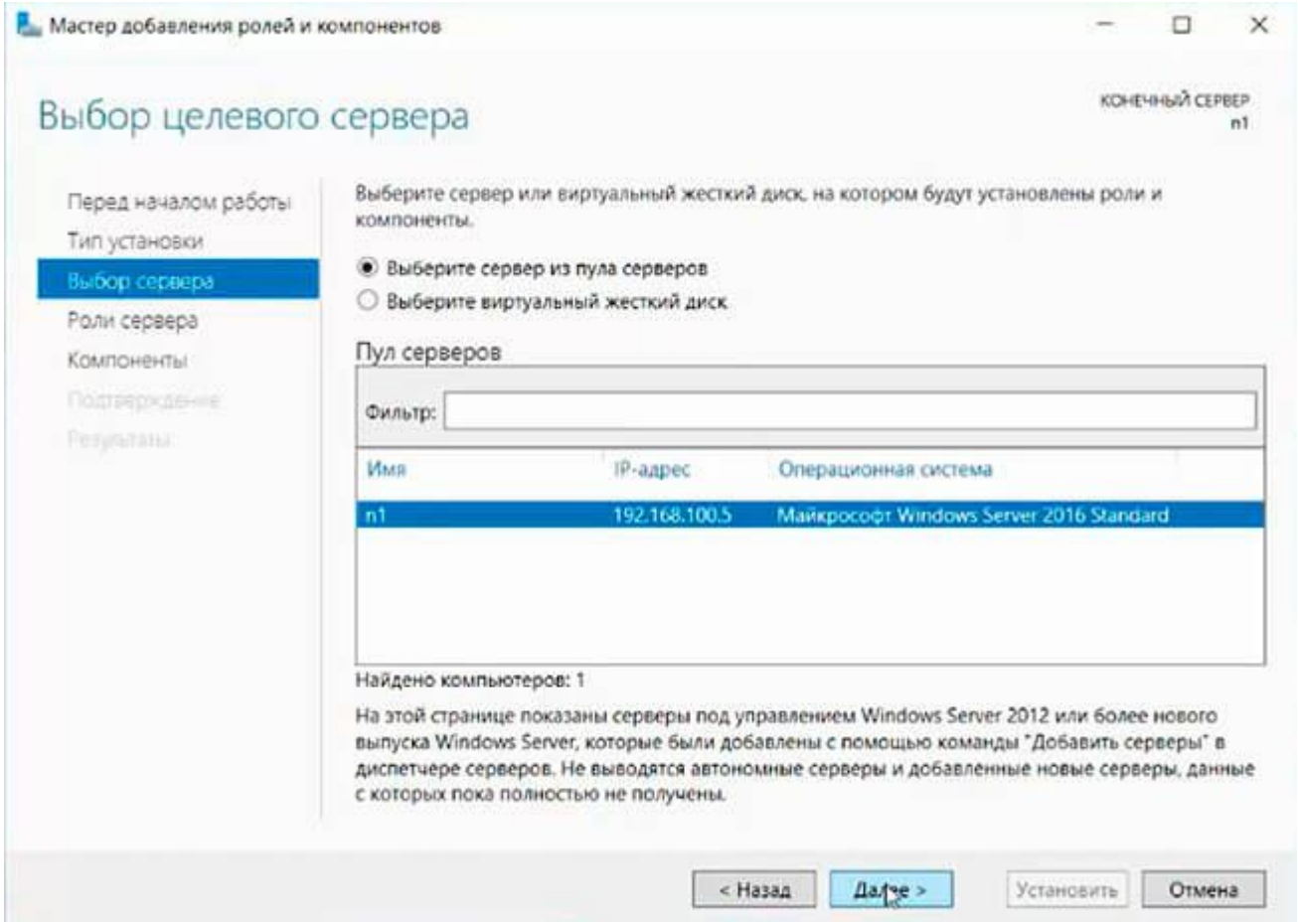

Рисунок 3.5– Выбор целевого сервера

Для выбора ролей сервера необходимо установить галочки напротив "DNS-сервера" и "Доменные службы Active Directory". При появлении запроса о добавлении компонентов – "Добавить компоненты". Затем нажать "Далее".

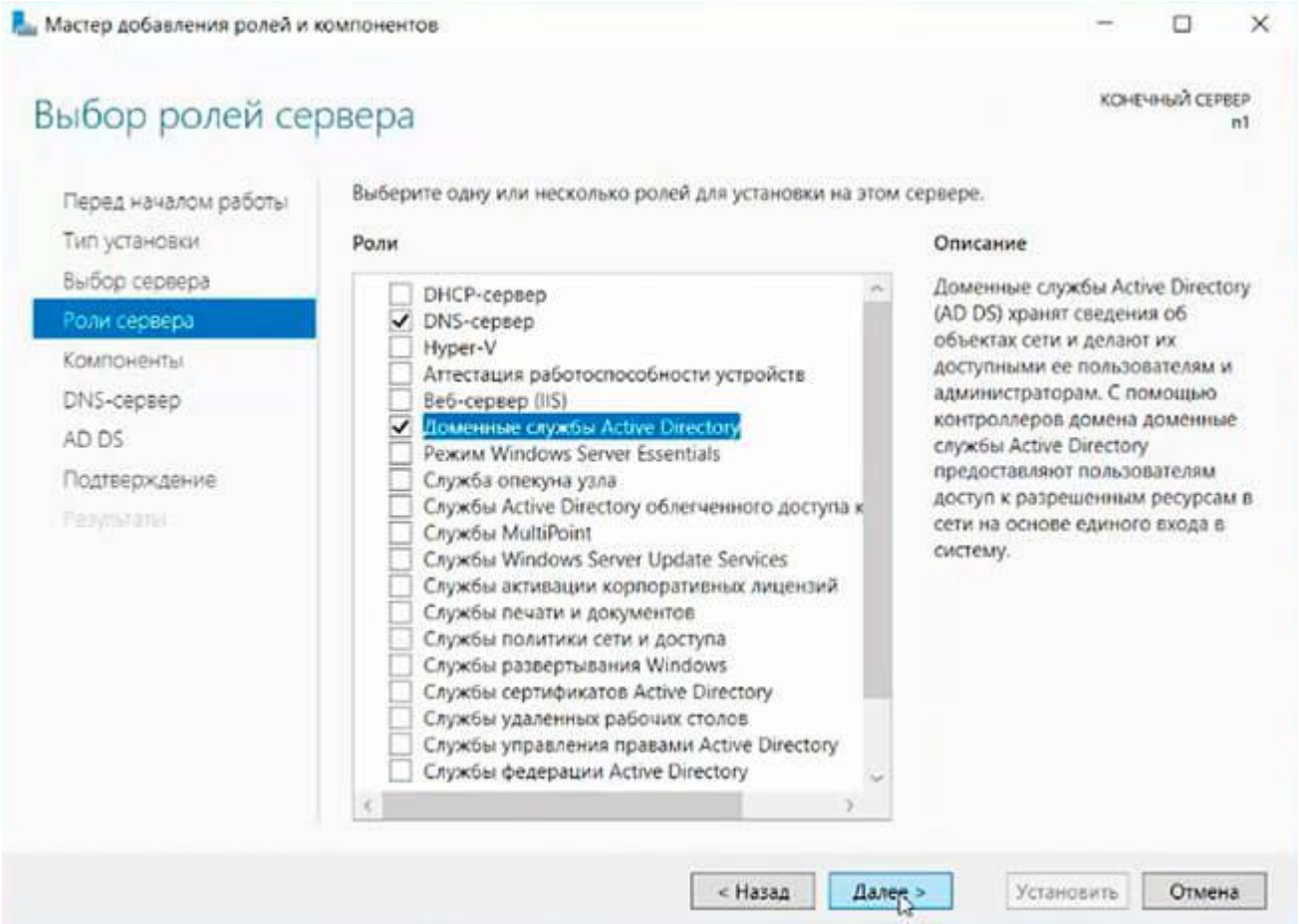

Рисунок 3.6– Выбор ролей сервера

В следующих окнах требуется нажать "Далее", а в окне "Подтверждение установки компонентов" выбрать "Установить". Этот мастер можно закрыть, по окончании установки появится предупреждение в диспетчере серверов.

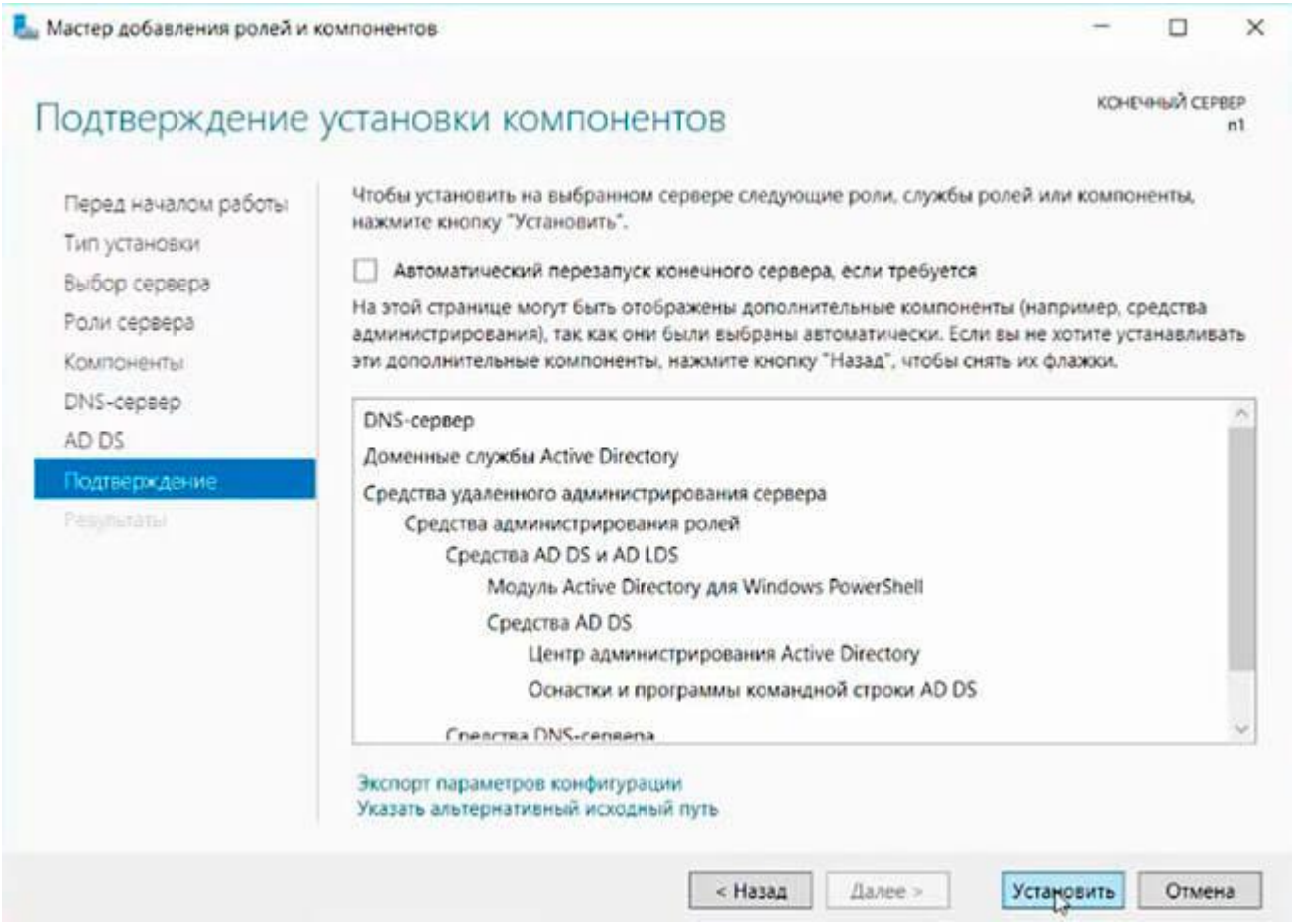

Рисунок 3.7– Подтверждение установки компонентов

После окончания установки выбранных ролей сервера, необходимо нажать на значок предупреждения в "Диспетчере серверов" и выбрать "Повысить роль этого сервера до уровня контроллера домена".

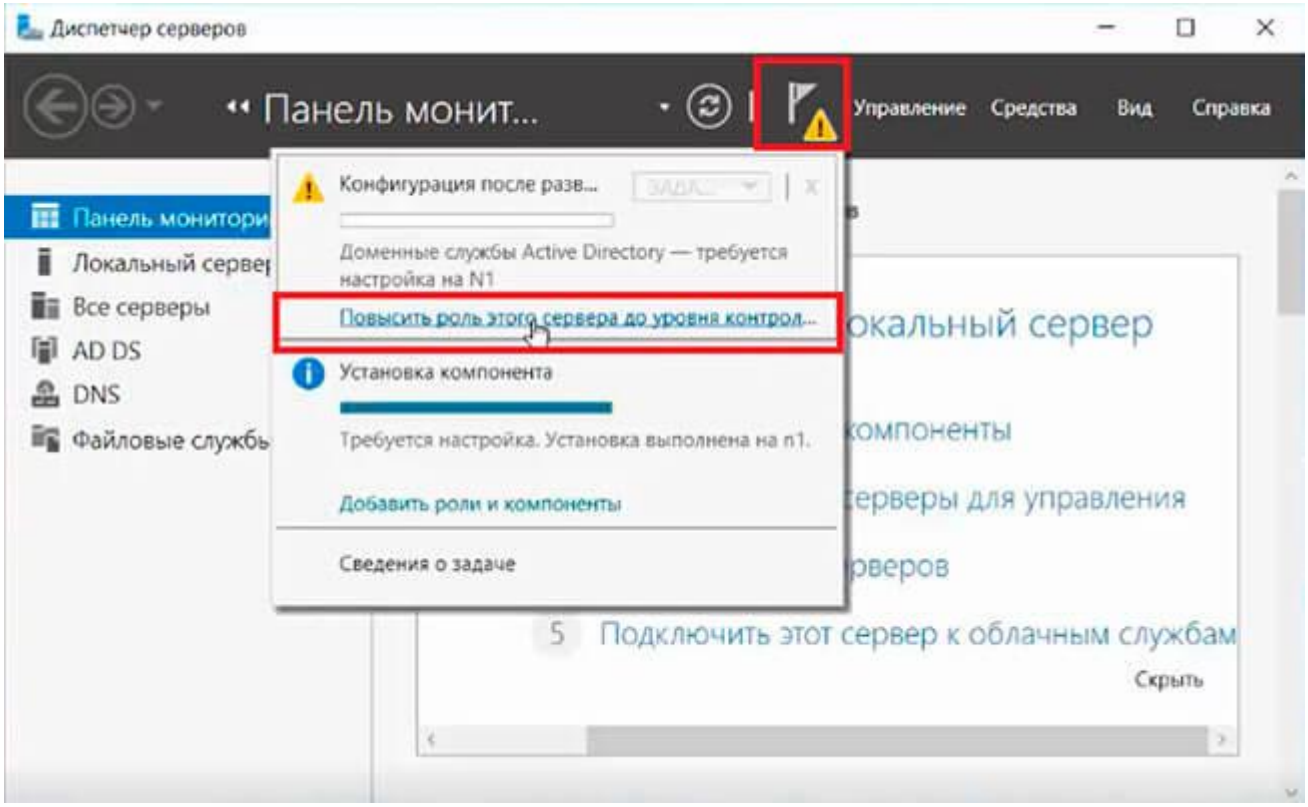

Рисунок 3.8– Повышение роли сервера

В следующем окне необходимо выбрать "Добавить новый лес". Имя корневого домена – уникальное имя вашего домена.

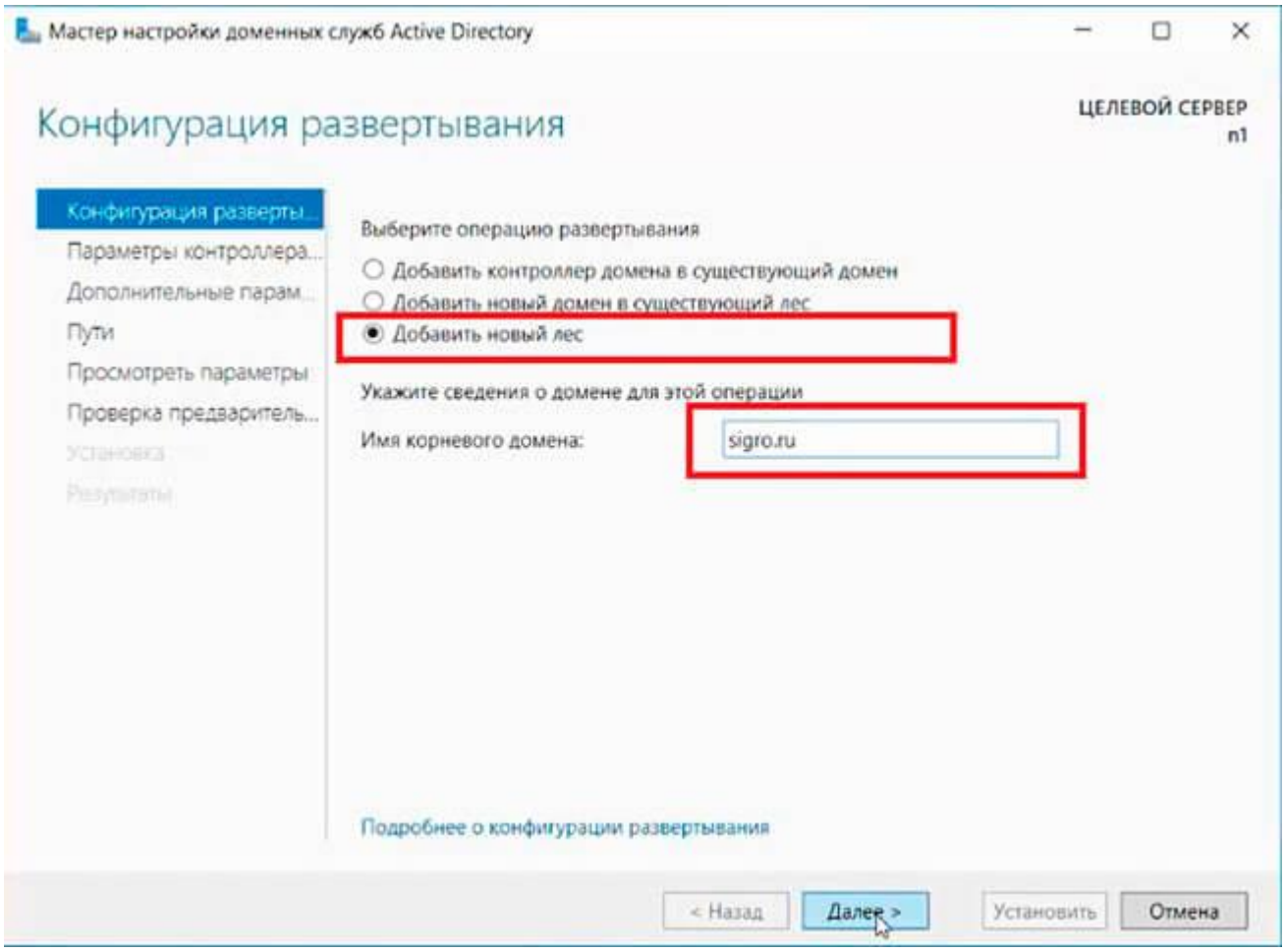

Рисунок 3.9– Установка имени корневого домена

В"Параметрах контроллера домена" необходимо оставить по умолчанию режим работы леса и домена – "Windows Server 2016". Требуется ввести пароль для режима восстановления служб каталогов (DSRM).Этот пароль может пригодиться, его обязательно необходимо запомнить или записать в надежное место.

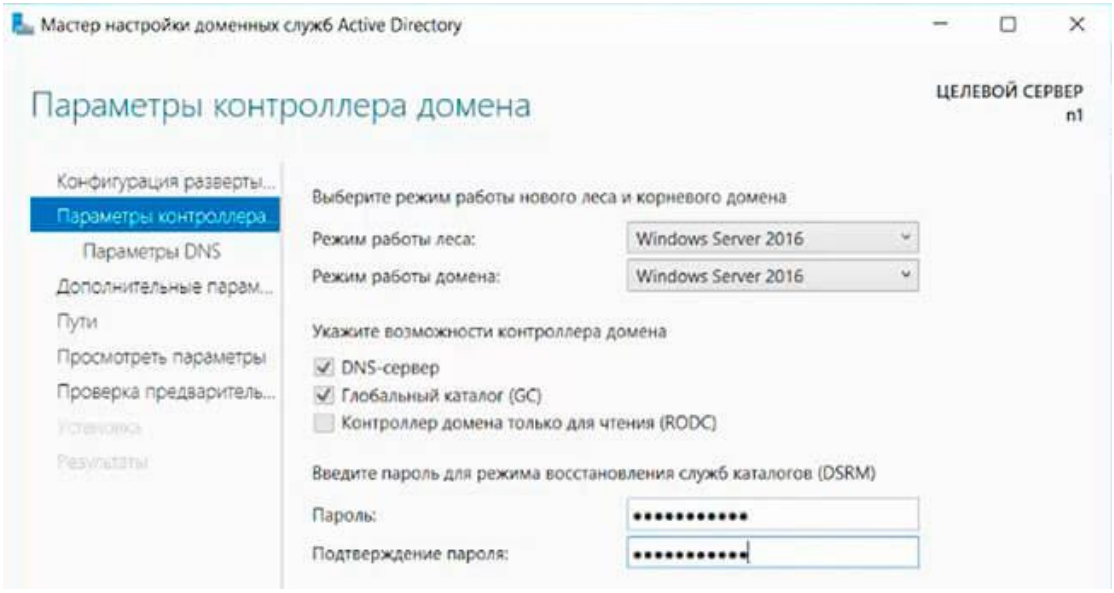

Рисунок 3.10– Установка параметров контроллера домена

В окне "Параметры DNS" – необходимо нажать на кнопку "Далее".

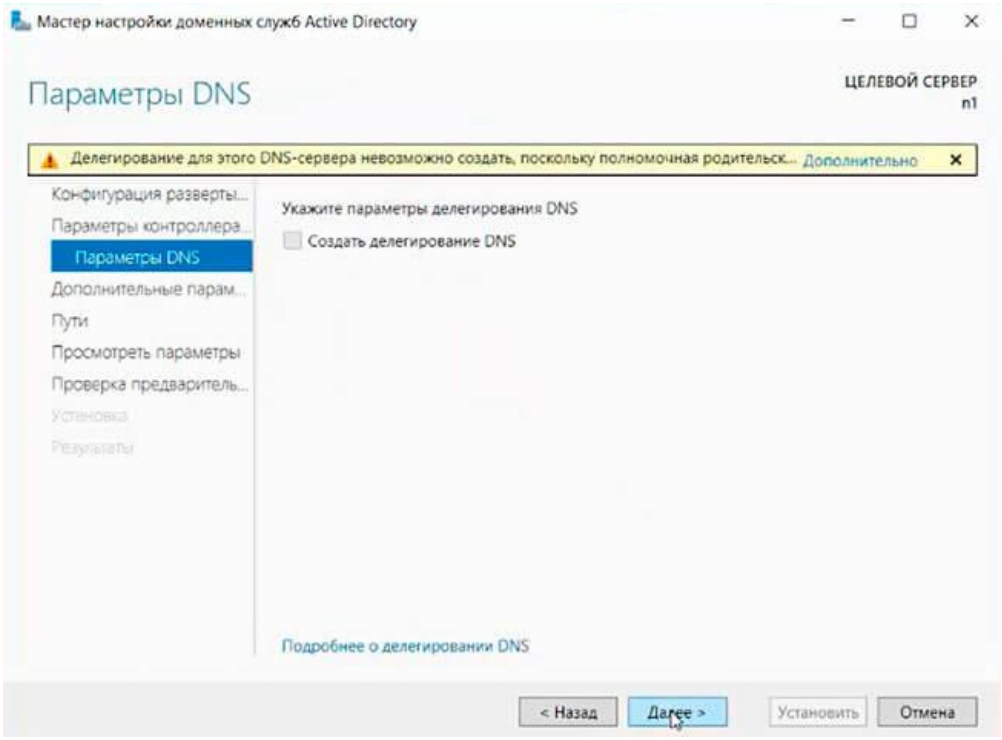

Рисунок 3.11– Подтверждение изменений параметров DNS

В окне "Дополнительные параметры" – нажать на "Далее".

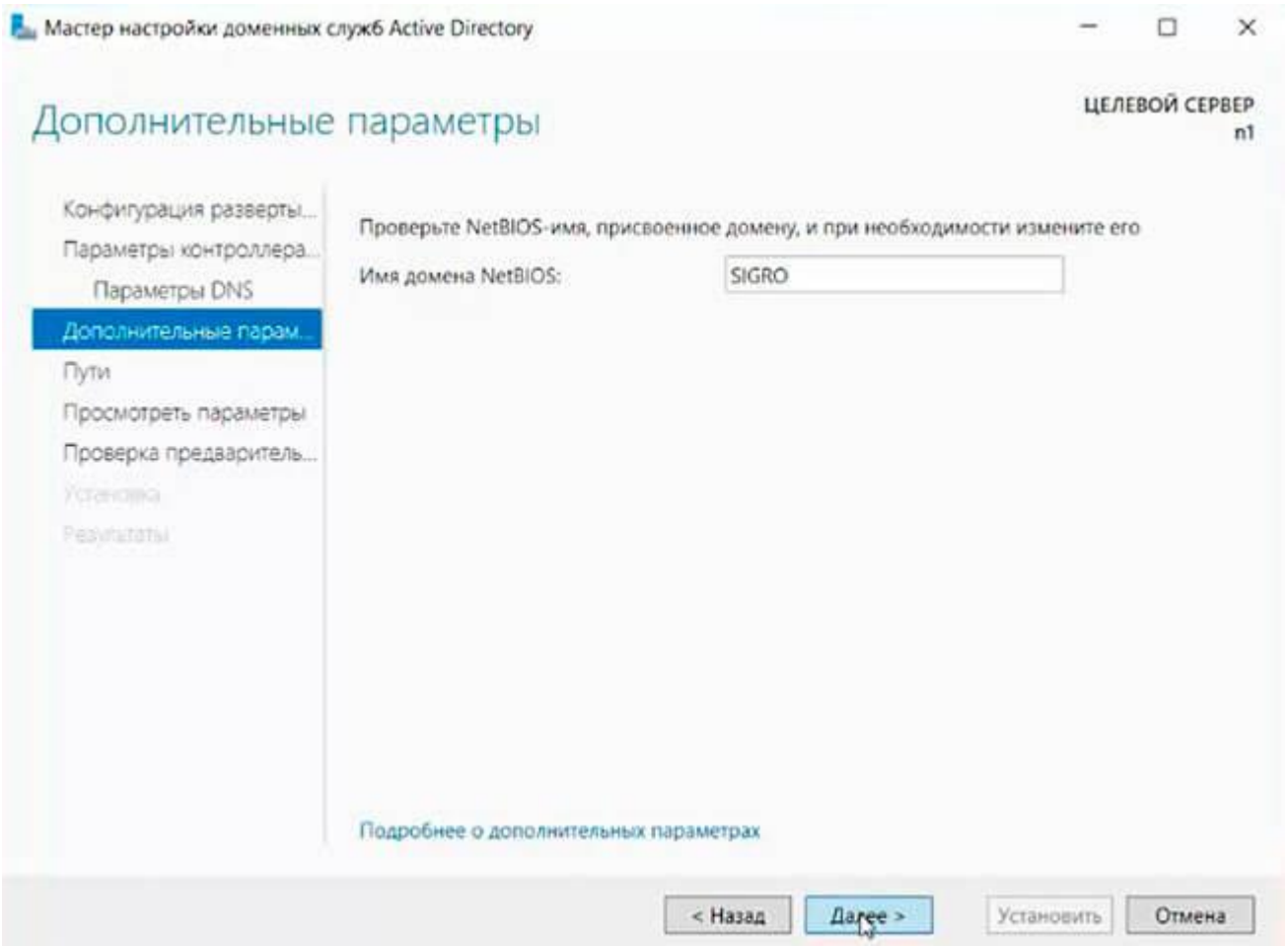

Рисунок 3.12– Окно дополнительные параметры

В открывшемся окне необходимо оставить по умолчанию расположение базы данных AD DS, файлов журналов и попок SYSVOL, а после требуетсянажать на "Далее".

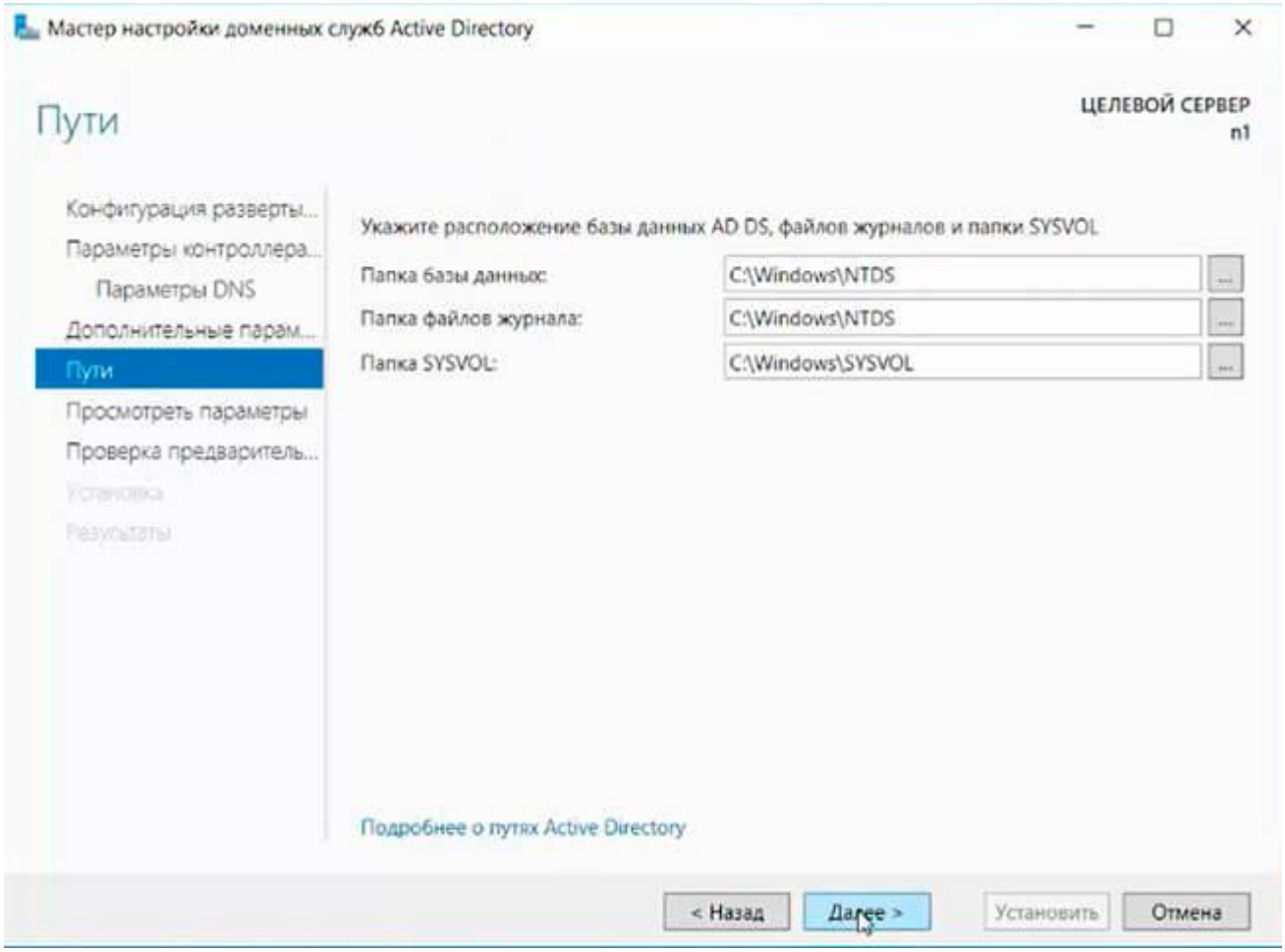

Рисунок 3.13– Окно установки путей

В окне просмотра параметров необходимо проверить корректность выбранных ранее параметров, а затем нажать "Далее".

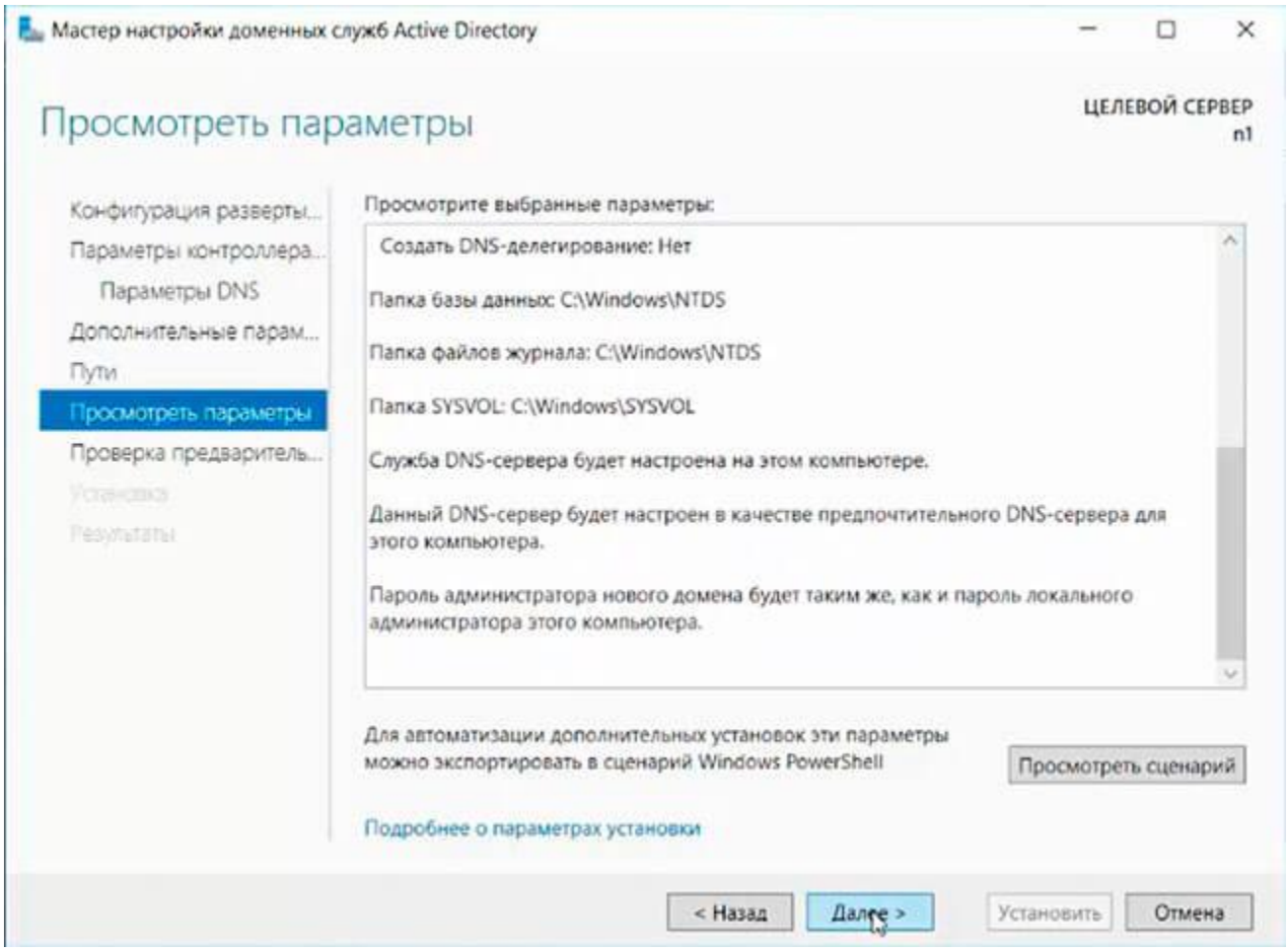

Рисунок 3.14– Окно просмотра параметров

После того, как сервер проверит соответствие предварительных требований, необходимо нажать на кнопку "Установить".

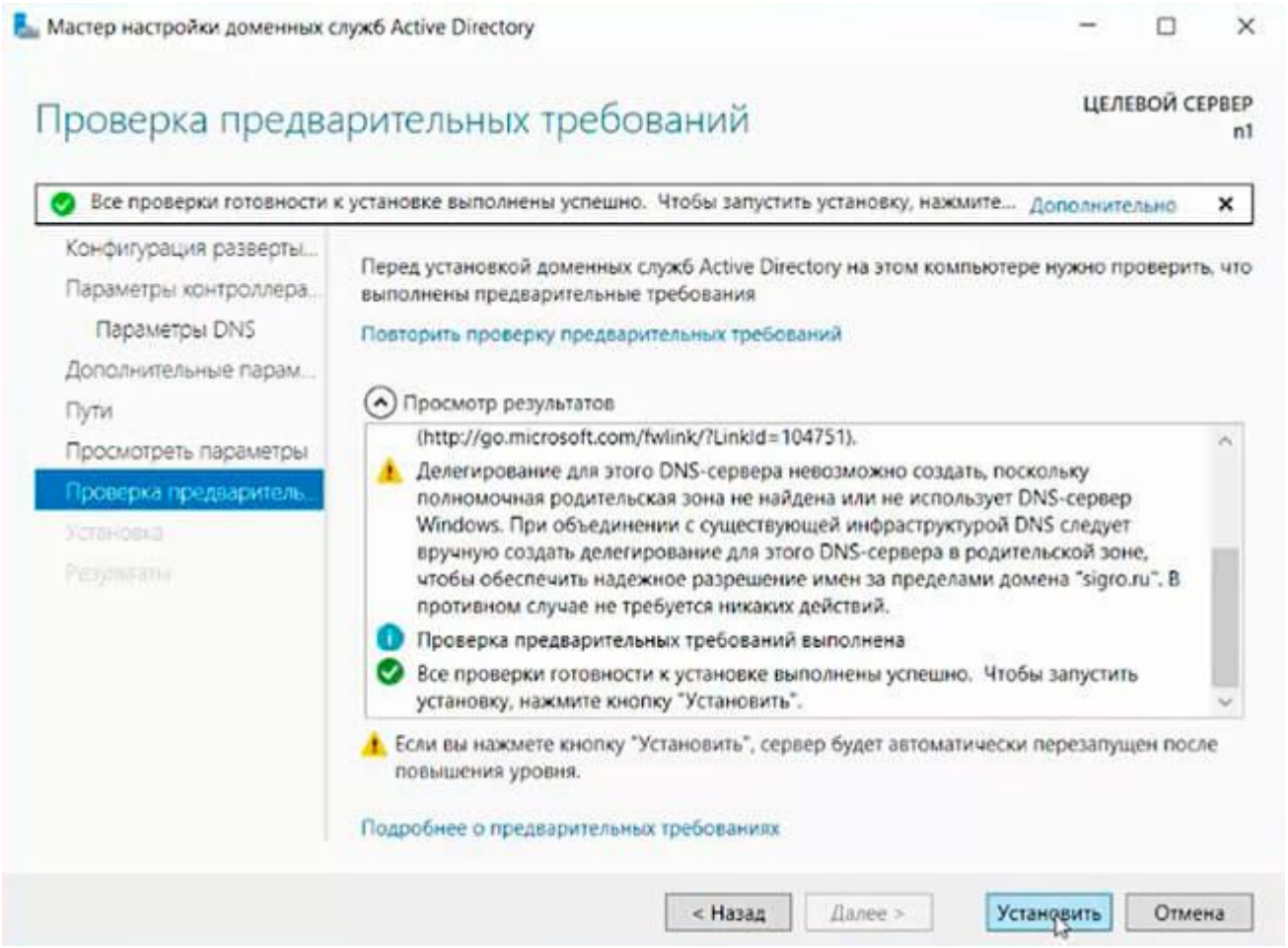

Рисунок 3.15– Окно проверки предварительных параметров

После настройки контроллера домена, можно перейти к настройке обратной зоны DNS-сервера. Для этого в "Диспетчер серверов" требуется выбрать "Средства", а далее "DNS".

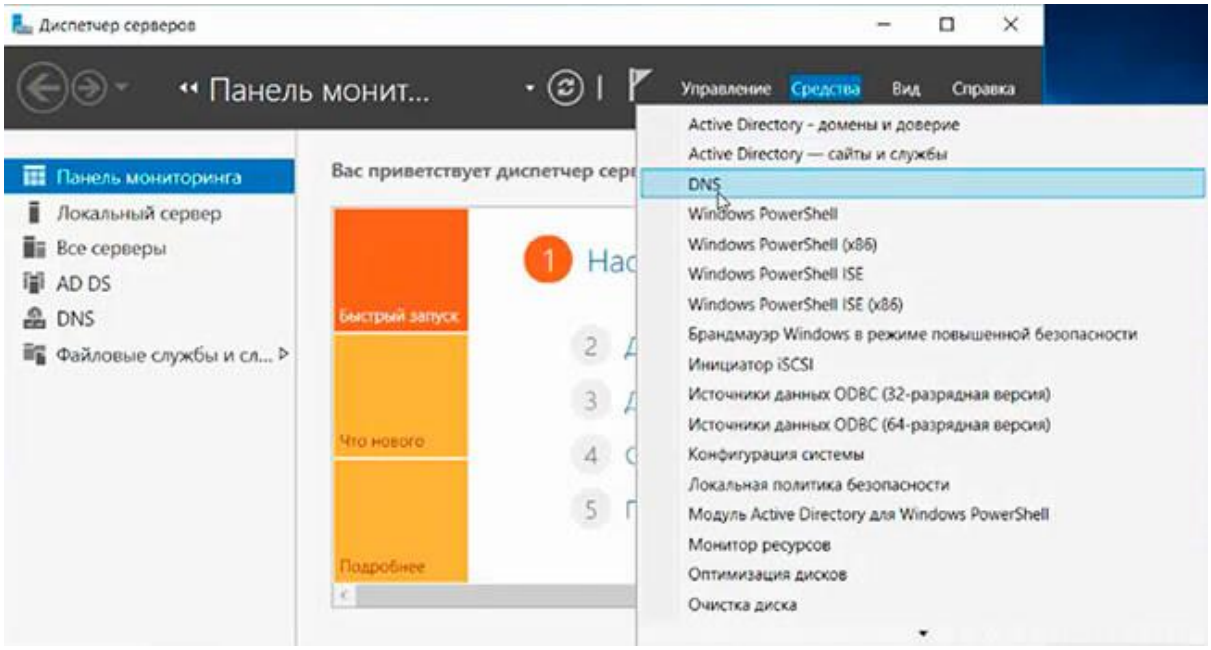

Рисунок 3.16– Окно выбора обратной зоны DNS

В открывшемся окненеобходимо выбрать созданный ранее сервер, затем "Зона обратного просмотра". Правой клавишей мыши - "Создать новую зону...".

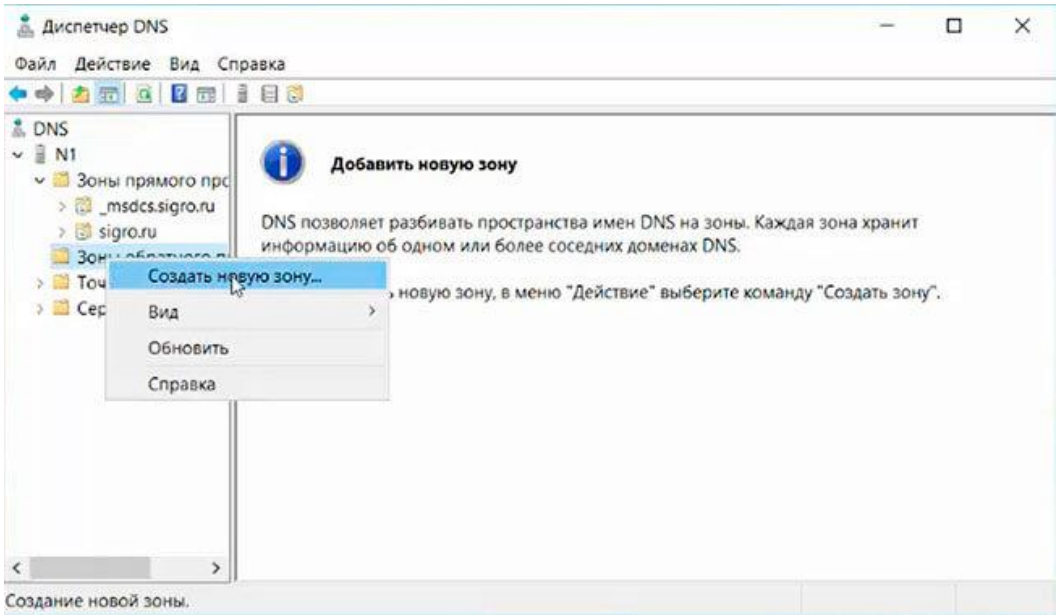

Рисунок 3.17– Создание новой зоны

В мастере создания новой зоны необходимо оставить тип зоны - "Основная зона", затем нажать на "Далее".

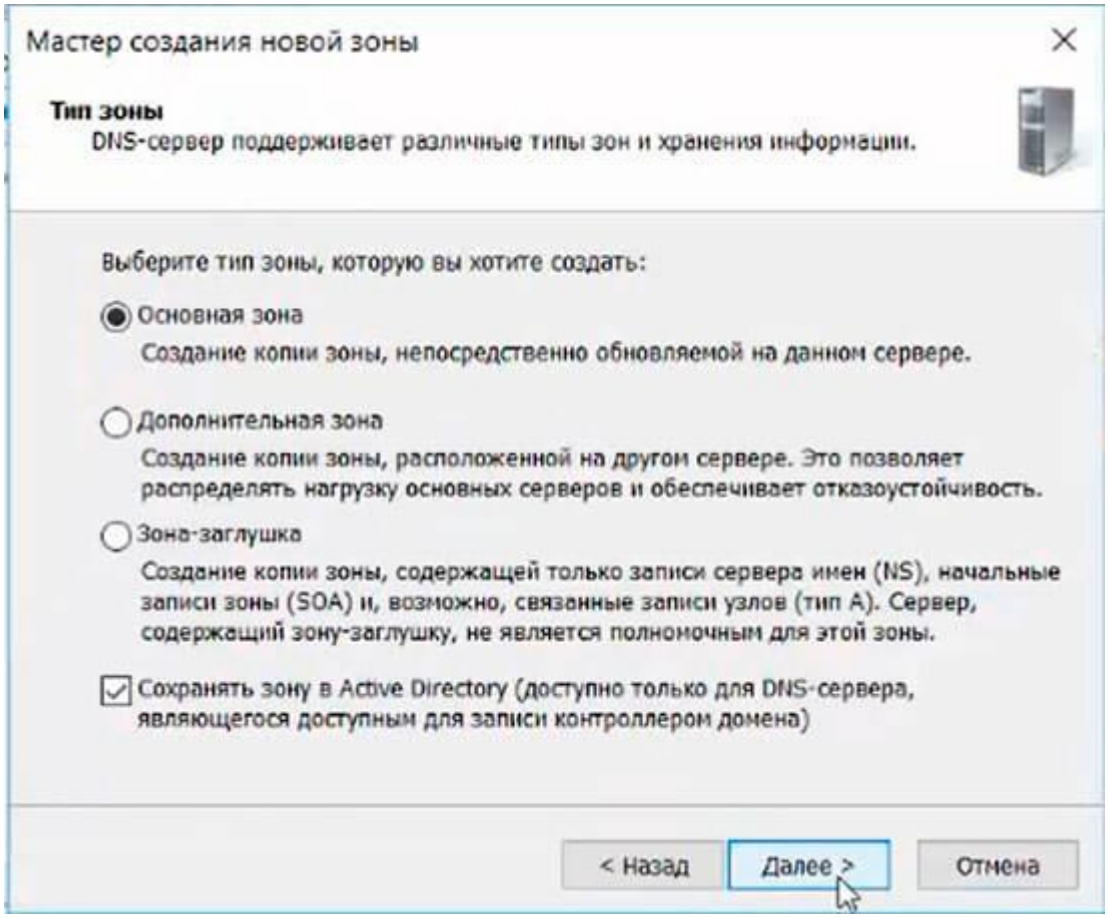

Рисунок 3.18– Окно выбора типа создаваемой зоны

Необходимо оставить по умолчанию чекбокс на пункте "Для всех DNS-серверов, работающих на контроллерах домена в этом домене, а после этого снова нажать на "Далее".

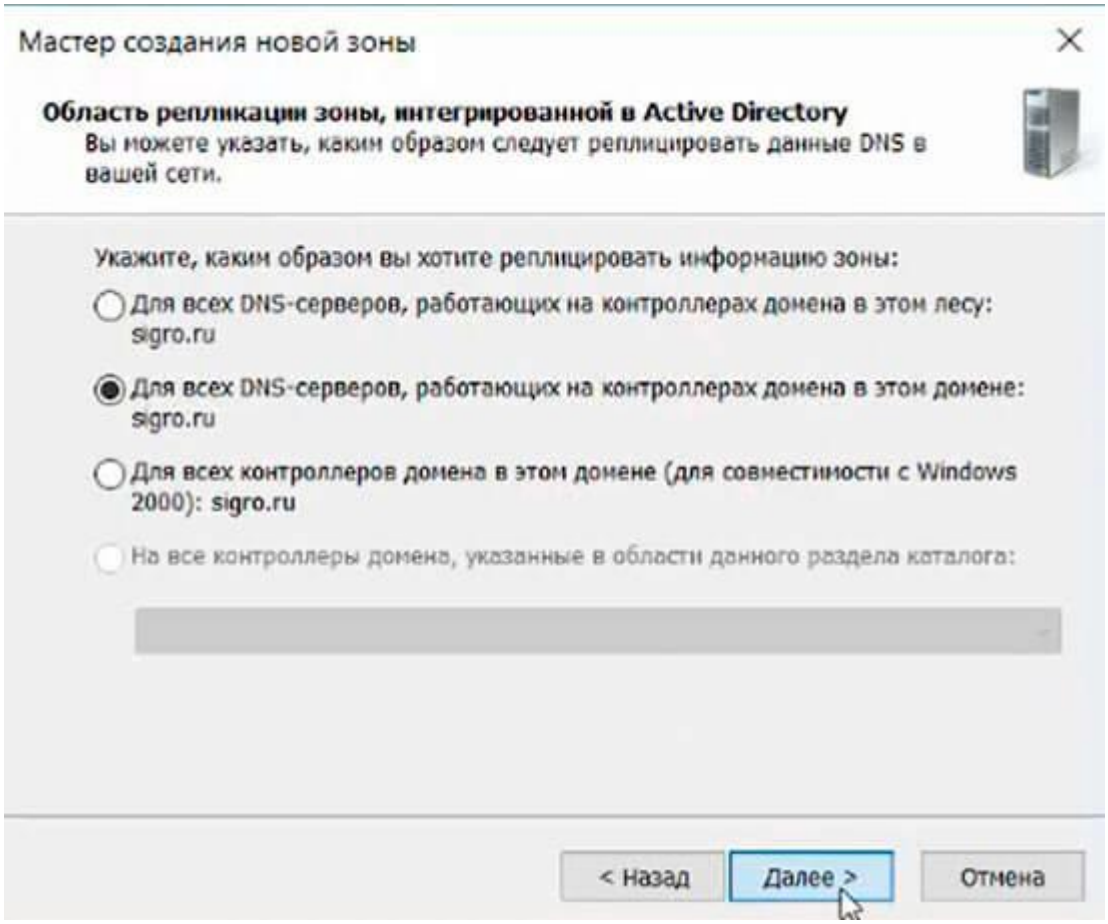

Рисунок 3.19– Окно установки репликации зоны

В открывшемся окне необходимо выбрать пункт "Зона обратного просмотра IPv4", а затем нажать на "Далее".

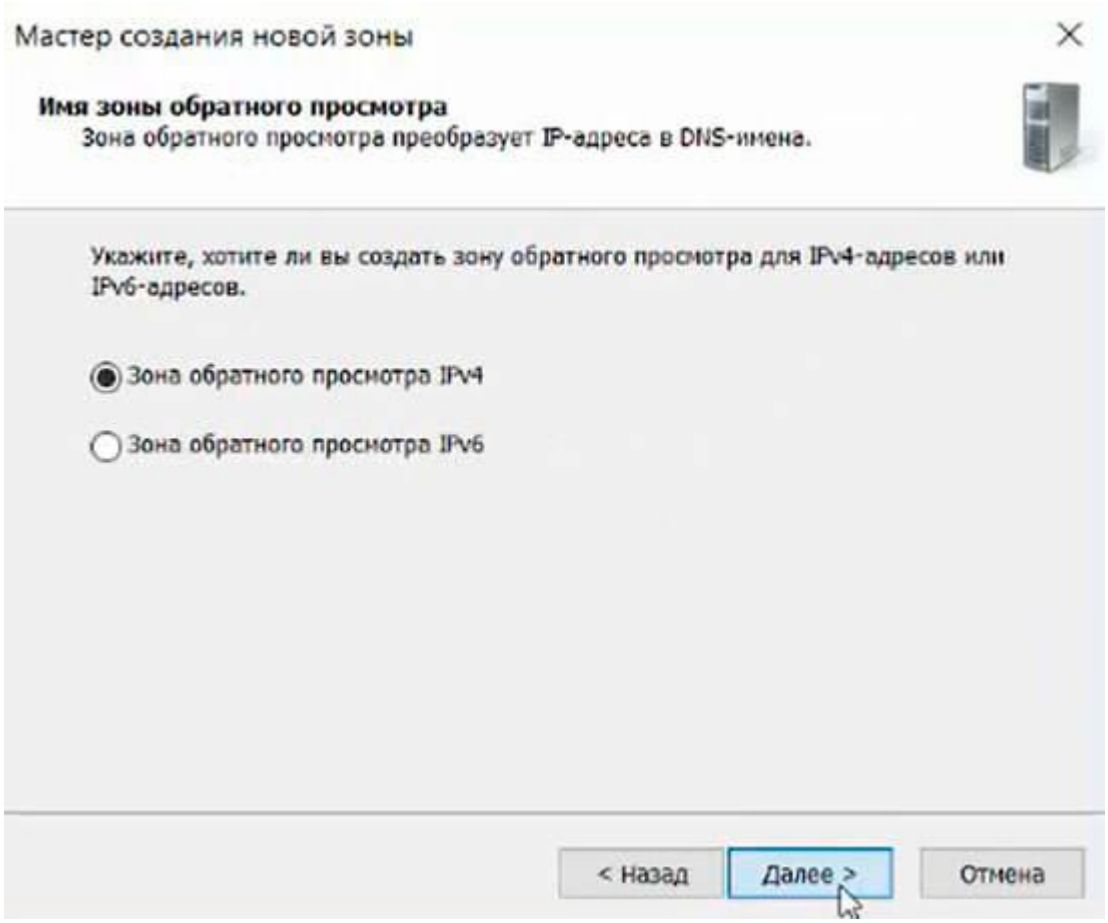

Рисунок 3.20– Окно установки зоны обратного просмотра

Для настройки зоны обратного просмотра требуется задать "Идентификатор сети", например: 192.168.100. После этого появится автоматически зона обратного просмотра. Далее необходимо нажать на кнопку "Далее".

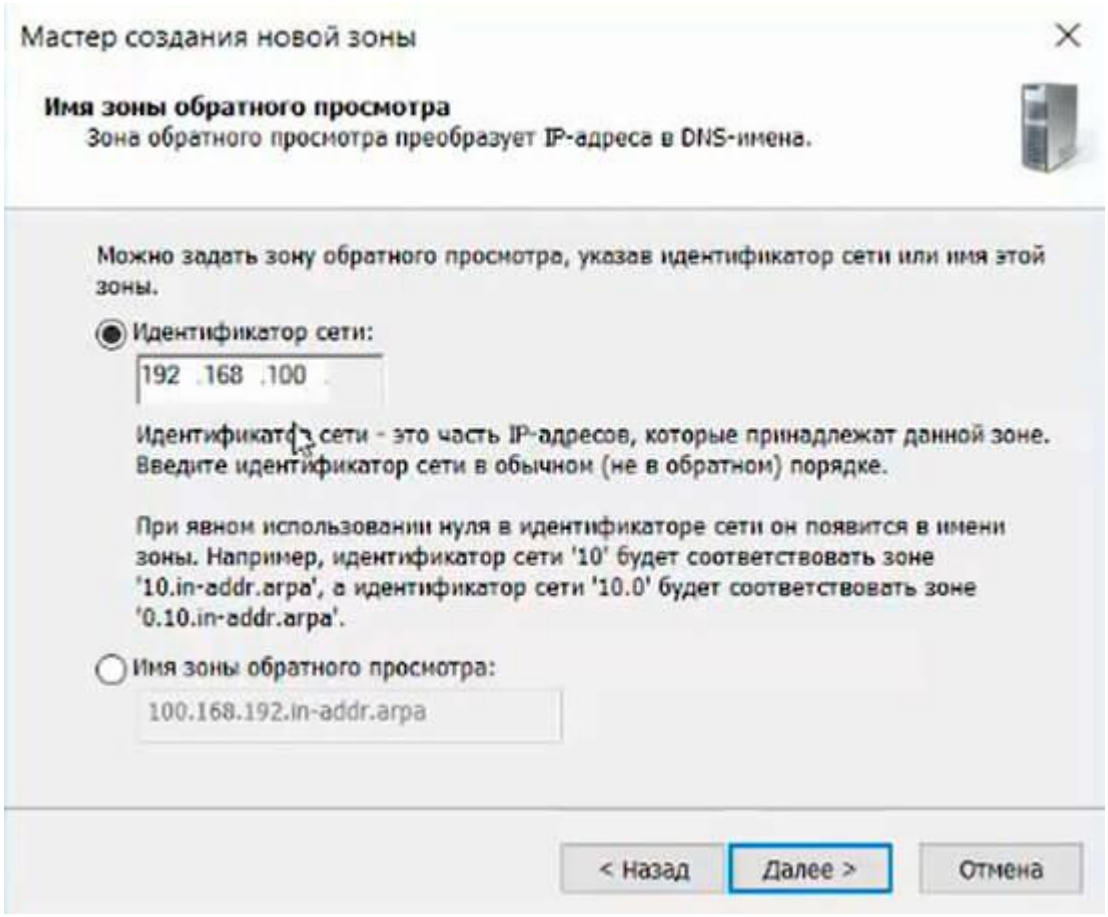

Рисунок 3.21– Установка идентификатора сети

В следующем окне необходимо оставить по умолчанию «Разрешить только безопасные динамические обновления», а затем нажать на"Далее".

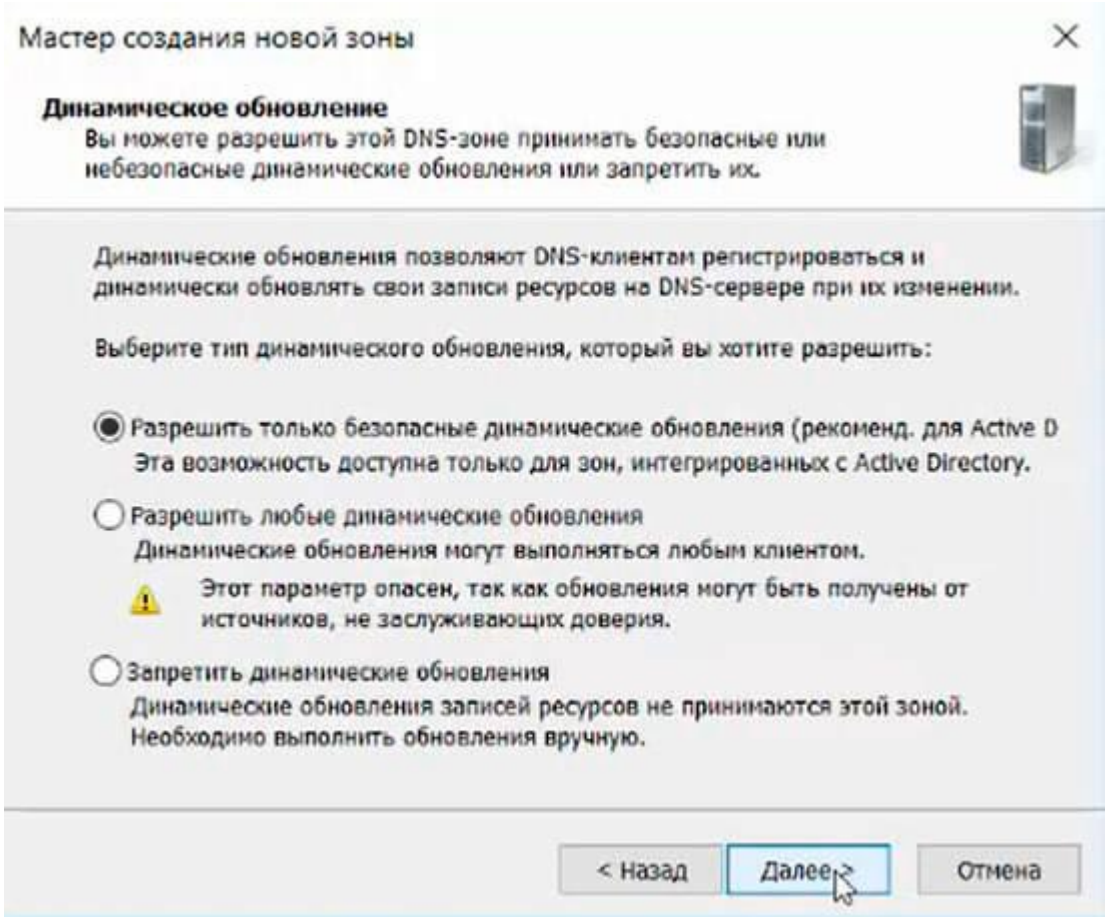

Рисунок 3.22– Окно выбора типа динамического обновления

Для завершения настройки создания новой зоны требуется проверить настройки и нажать на кнопку "Готово".

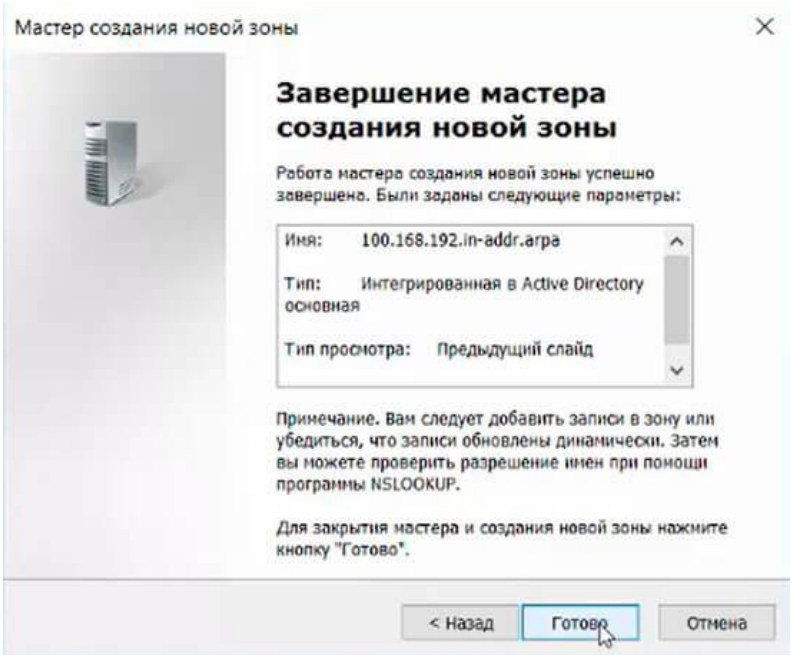

Рисунок 3.23– Окно завершения создания новой зоны

После появится зона обратного просмотра для домена.

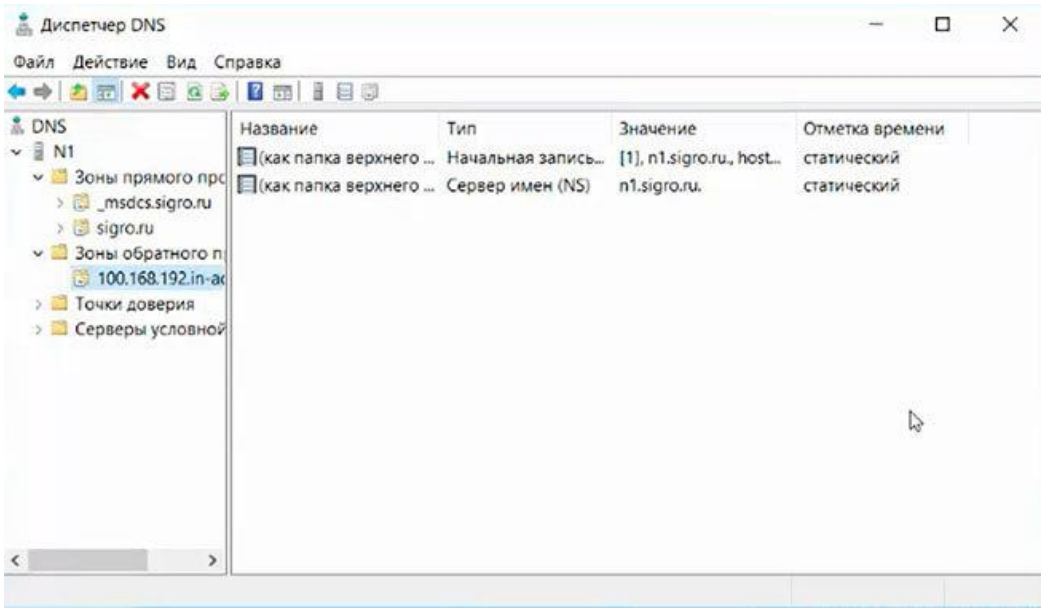

Рисунок 3.24– Окно завершения создания новой зоны

В "Диспетчере серверов" необходимо выбрать "Пользователи и компьютеры Active Directory" и проверить работу Active Directory.

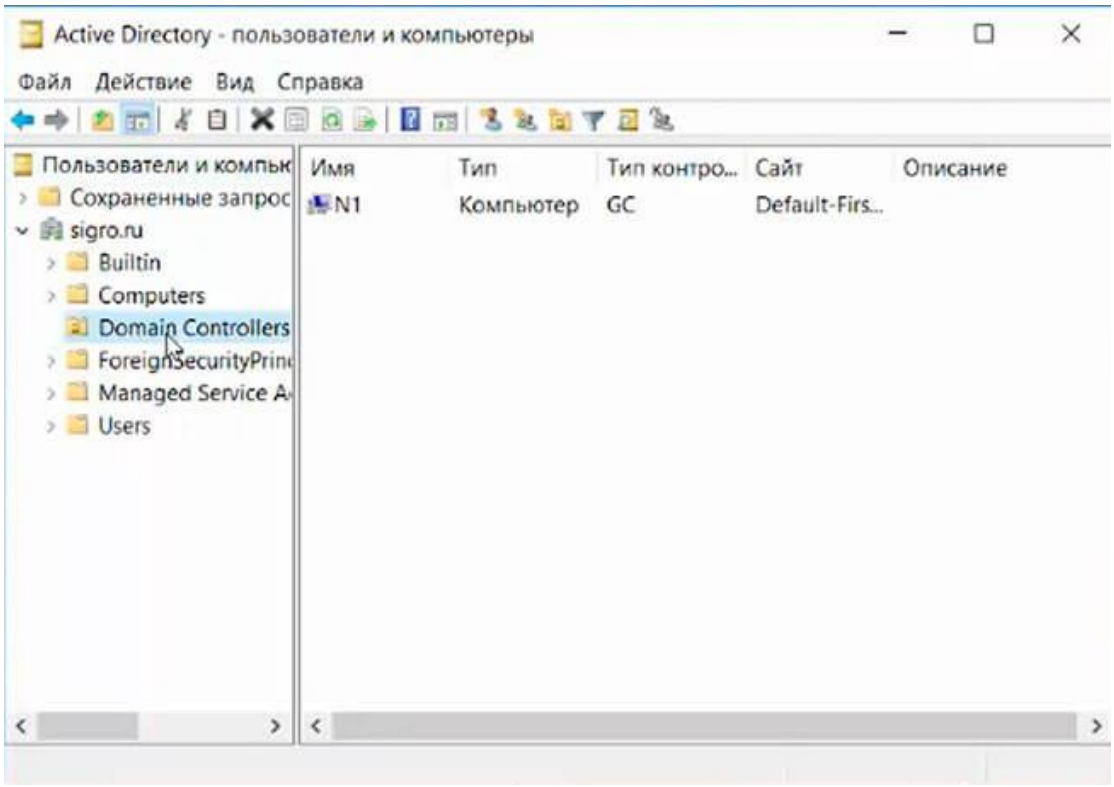

Рисунок 3.25– Проверка работы ActiveDirectory

На этом установка и настройка выбранных ролей сервера заканчивается.

4 СОДЕРЖАНИЕ ОТЧЕТА

Титульный лист, цель работы, описание выполненной работы с иллюстрациями (скриншоты выполненных действий) и выводы по проделанной работе.

5 ЗАДАНИЕ НА РАБОТУ

Необходимо установить и настроить работу службы AD, а также распределить роли пользователей. Задание для выполнения уточняется преподавателем в ходе проведения лабораторного занятия.

6КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что такое ActiveDirectory и каковы её основные возможности?
2. Для чего необходим контроллер домена, какие функции он выполняет?
3. Что такое «рабочие группы» и чем вызваны сложности эксплуатации их в крупных сетях?
4. Какие группы выделяют в рамках схемы AD и как они подразделяются по области действия?
5. Что такое лес AD и какую структуру он имеет?
6. Объясните понятие «доверие» и назовите основные виды отношения доверия.
7. Что такое «транзитивное» отношение доверия и назовите доверие, которое не является транзитивным.
8. Что такое глобальный каталог леса Active Directory?
9. Что такое ресурсная запись и какие элементы она включает?
10. Какие типы ресурсных записей бывают?
11. Что такое обратный просмотр DNS и для чего он используется?
12. Чем ограничивается количество PTR-записей, описывающих разные имена, на один адрес и почему?

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Немнюгин С.А. Параллельное программирование для многопроцессорных вычислительных систем/ С.А. Немнюгин, О.А. Стесик - СПБ.: Издательство ” BHV”,2002.-400 с.

1. Эндрюс Г.Р. Основы многопоточного параллельного и распределенного