Geekbrains

Специализация**: компьютерные технологии и информационная безопасность**

**ВЫПУСКНАЯ ДИПЛОМНАЯ РАБОТА**

**на тему:**

**«Проектирование локальной вычислительной сети организации»**

**Выполнил:**

**обучающийся группы: 6112**

**форма обучения: Заочная**

**специальность: Информационная безопастность**

**Ибрагимов Алексей Владимирович**

**Научный руководитель:**

**Сергей Куриленко**

**Москва, 2024 г.**

ОГЛАВЛЕНИЕ

[**ВВЕДЕНИЕ** 3](#_Toc133444333)

[**1 АНАЛИТИЧЕСКИЙ РАЗДЕЛ** 5](#_Toc133444334)

[**1.1** **Анализ предметной области** 5](#_Toc133444335)

[**1.2 Технологии передачи данных** 7](#_Toc133444336)

[**1.2.1 Проводные технологии передачи данных** 7](#_Toc133444337)

[**1.2.2 Беспроводные технологии передачи данных** 8](#_Toc133444338)

[**1.3 Постановка задачи** 10](#_Toc133444339)

[**1.3.1 Требования к проектируемой вычислительной сети предприятия** 14](#_Toc133444340)

[**1.3.2 Требования к аппаратно-программным средствам** 17](#_Toc133444341)

[**2 ПРАКТИЧЕСКАЯ ЧАСТЬ** 18](#_Toc133444342)

[**2.1 Выбор аппаратных частей ЛВС** 18](#_Toc133444343)

[**2.2 Выбор беспроводной точки доступа** 22](#_Toc133444344)

[**2.3 Выбор монтажного шкафа** 23](#_Toc133444345)

[**2.4 Выбор операционных систем** 24](#_Toc133444346)

[**2.5 Выбор антивирусной программы** 27](#_Toc133444347)

[**2.6 Монтаж структурированной кабельной системы** 30](#_Toc133444348)

[**2.7 Настройка сервера** 35](#_Toc133444349)

[**2.8 Настройка Proxy-сервера** 46](#_Toc133444350)

[**2.9 Настройка рабочих станций** 48](#_Toc133444351)

[**2.8 Настройка коммутатора** 49](#_Toc133444352)

[**2.9 Настройка Ubiquiti NanoStation M2** 52](#_Toc133444353)

[**2.10 Тестирование ЛВС организации** 57](#_Toc133444354)

[**ЗАКЛЮЧЕНИЕ** 60](#_Toc133444355)

[**БИБЛИОГРАФИЧЕСКИЙ СПИСОК** 62](#_Toc133444356)

# **ВВЕДЕНИЕ**

Сегодня большинство компаний работает через сеть, которая связывает рабочие места и удаленные источники данных. Это обеспечивается программными средствами, которые используют клиент-серверную архитектуру, такие как программы документооборота. Однако, для того чтобы это работало, необходима физическая связь между компьютерами и серверами, а для этого нужно правильно настроить локальные вычислительные сети (ЛВС), включая выбор топологии сети, прокладку сетевых кабелей, выбор и настройку сетевого оборудования.

Тема выпускной квалификационной работы заключается в поиске конфигурации ЛВС, которая позволит повысить эффективность взаимодействия между сотрудниками организации, обмену информацией, использованию периферийных устройств и устройств хранения информации. Решение этих задач может привести к экономии времени и материальных ресурсов, что будет положительно сказываться на позиции компании.

Целью работы является проектирование сети организации и объединение разрозненных ЛВС. Для этого нужно провести исследование и анализ предметной области, изучить основные топологии компьютерных сетей, разработать логическую и физическую схемы сети, проанализировать среды передачи данных, выбрать оборудование, изучить технологию монтажа и настроить программное обеспечение.

Дополнительно к уже упомянутым задачам, для успешного проектирования сети организации и объединения разрозненных ЛВС необходимо решить следующие задачи:

* Проанализировать потребности сети организации и определить объемы передаваемых данных, количество пользователей, требования к скорости передачи и пропускной способности сети.
* Выбрать оптимальную топологию сети, которая будет наиболее соответствовать потребностям организации.
* Разработать план распределения компьютеров и другого оборудования в офисе, учитывая физические особенности помещения и необходимость максимальной эффективности работы сети.
* Провести анализ безопасности сети и разработать меры по ее защите от внешних угроз и внутренних нарушений безопасности.
* Определить типы кабелей и сетевого оборудования, которые будут использоваться в сети организации.
* Произвести монтаж и настройку сети, включая установку сетевых адаптеров на компьютеры, настройку на маршрутизаторах и коммутаторах, а также установку и настройку программного обеспечения.
* Провести тестирование сети и оптимизировать ее настройки для достижения максимальной производительности.

Решение этих задач поможет создать стабильную, безопасную и эффективную сеть, которая будет соответствовать потребностям организации и поможет повысить ее производительность.

Объектом исследования являются вычислительные сети, а предметом исследования - локальная вычислительная сеть организации, которая позволит создать единое информационное пространство.

# **1 АНАЛИТИЧЕСКИЙ РАЗДЕЛ**

## **1.1 Анализ предметной области**

В данной выпускной квалификационной работе рассматривается процесс проектирования локальной вычислительной сети (ЛВС) для ООО "Энерго Групп". Компания для управления сервисными предприятиями, сформированными на базе централизованных производственно-ремонтных подразделений крупнейших АО-энерго. Организация состоит из нескольких производственных участков, которые имеют разрозненные ЛВС, что затрудняет работу в едином сетевом пространстве. Кроме того, компьютеры пользователей устарели, что приводит к сбоям и простоям в работе и замедляет обмен и передачу данных. В связи с этим, было установлено необходимость модернизации существующей сети, ее переоснащения и расширения.

ЛВС компании представляет собой сложную систему, включающую в себя множество компонентов - от персональных компьютеров до систем хранения данных, программного обеспечения, коммутационного и маршрутизирующего оборудования, кабельной системы и систем защиты информации. В каждой части этой инфраструктуры можно оптимизировать работу, чтобы повысить эффективность и снизить издержки на обслуживание.

Основными факторами, которые влияют на выбор топологии сети, являются: среда передачи информации, метод доступа к окружающей среде, максимальное расширение сети, пропускная способность сети и способ передачи. Топология сети - это способ описания конфигурации сети, включая схему расположения и соединения сетевых устройств. Существуют физическая, логическая, информационная и топология управления обменом.

Существует несколько топологий соединения сетевых устройств, включая шину, звезду и кольцо. При выборе оптимального проекта локальной сети оцениваются скорость реакции, надежность, информационная безопасность, мобильность, стоимость организации и эксплуатации сети, масштабируемость, а также простота организации и обслуживания сети.

При проектировании ЛВС для ООО "Энерго Групп" было принято решение использовать топологию звезды. Она обеспечивает устойчивость к сбоям, которые могут возникать из-за проблем на рабочих местах. В топологии звезды все периферийные устройства и компьютеры подключаются к одному центральному узлу, каждый из которых использует свою отдельную линию связи. Данная топология продемонстрирована на рисунке 1.1.

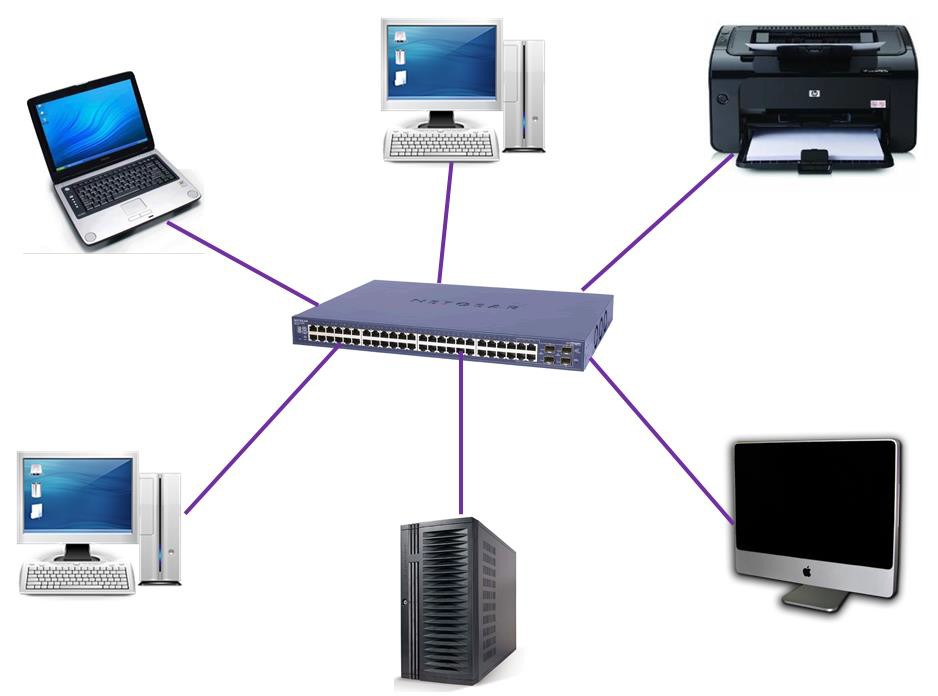


Рисунок 1.1 – Топология «Звезда»

## **1.2 Технологии передачи данных**

Локальная вычислительная сеть (ЛВС) может быть реализована с использованием проводной и беспроводной технологии. Каждая из этих технологий имеет свои преимущества и недостатки.

Проводная технология обеспечивает более стабильное и быстрое соединение между устройствами, а также большую безопасность передачи данных, чем беспроводная технология. Однако проводная технология требует проведения кабельной инфраструктуры, что может быть затратно и затруднительно в некоторых условиях.

Беспроводная технология позволяет работать без ограничений проводов и кабелей, что дает большую мобильность устройств и удобство в использовании. Однако беспроводная технология может иметь проблемы с интерференцией сигналов, менее стабильным соединением и меньшей пропускной способностью по сравнению с проводной технологией.

При выборе технологии необходимо учитывать цели и задачи использования сети, а также условия окружающей среды и требования к безопасности передачи данных.

## **1.2.1 Проводные технологии передачи данных**

В современных офисах для проведения проводной сети используются витые пары и порты RJ-45, соответствующие стандартам IEEE 802.3. Существуют два основных стандарта, которые определяют максимальную пропускную способность сети: IEEE 802.3u с пропускной способностью 100 Мбит/с, используемый в старых компьютерах и бюджетных ноутбуках, а также IEEE 802.3ab с пропускной способностью 1000 Мбит/с, являющийся наиболее распространенным на сегодняшний день. Преимуществами проводной сети являются стабильность, надежность и высокая скорость работы. Недостатками кабельной сети являются необходимость прокладки кабелей до каждого рабочего места и перепрокладка кабелей при любых изменениях в организации офиса, что может оказаться нетривиальной задачей.

Кроме того, проводная сеть может быть более уязвимой к внешним воздействиям, таким как электромагнитные помехи, перегрузки и короткие замыкания. Также кабели могут быть повреждены при ремонте или перестановке мебели в офисе. Еще одним недостатком проводной сети является возможность возникновения конфликтов при использовании разных устройств, таких как принтеры, сканеры и другие периферийные устройства, которые могут работать на одном порту коммутатора. Кроме того, использование проводной сети может быть нецелесообразно в тех случаях, когда требуется передача данных на большие расстояния, например, между зданиями, где использование оптических кабелей может быть более эффективным решением.

## **1.2.2 Беспроводные технологии передачи данных**

Беспроводные сети Wi-Fi сегодня представлены широким выбором оборудования, поддерживающего современные стандарты связи. Скорость передачи данных зависит от стандартов связи и физического расположения антенн. Однако у беспроводных сетей есть свои недостатки, такие как несовместимость новых стандартов со старыми, чувствительность к преградам и помехам, трудность контроля пропускной способности каждого клиента, работа на скорости самого медленного клиента, различные частотные диапазоны в разных странах, отсутствие стабильной зоны распространения сигнала и возможность перехвата данных. При передаче сигнала существуют две топологии: точка-точка и точка-много точка. Технология передачи "точка-точка" обеспечивает высокоскоростную и безошибочную передачу данных между компьютерами, в то время как технология передачи "точка-много точка" взаимодействует между несколькими компьютерами и периферийными устройствами. Сигнал может проникать через стены и перекрытия, а скорость передачи может достигать до 150 Мбит/с на расстоянии до 60 м внутри здания и до 530 м в условиях прямой видимости.

Некоторые другие достоинства беспроводных сетей Wi-Fi включают в себя более гибкую возможность подключения, так как не требуется физическая проводка, а также возможность использования сети в местах, где проводная сеть не доступна или не желательна. Беспроводные сети также позволяют устройствам подключаться к сети в любой точке, где есть сигнал Wi-Fi, что делает их более мобильными. Однако, как уже упоминалось, беспроводные сети также имеют ряд недостатков, таких как низкая безопасность, ограниченная скорость передачи данных и необходимость учитывать ограничения частотных диапазонов в разных странах. Кроме того, сигнал Wi-Fi может быть подвержен вмешательству других радиосигналов и может сильно изменяться в зависимости от препятствий на пути распространения сигнала.

Одним из главных преимуществ беспроводных сетей является возможность мобильного использования устройств, без необходимости привязки к определенному месту или порту. Это особенно удобно в случае использования ноутбуков или мобильных устройств.

Однако, как уже упоминалось, беспроводные сети имеют свои недостатки. Например, они менее стабильны и надежны, чем проводные сети, так как сигнал чувствителен к помехам, перегрузке и другим проблемам. Кроме того, уровень безопасности беспроводных сетей меньше, чем у проводных, так как данные передаются в эфир и могут быть перехвачены злоумышленниками.

Существуют различные стандарты беспроводных сетей, которые отличаются скоростью передачи данных, дальностью и другими параметрами. Наиболее распространенными на сегодняшний день являются стандарты Wi-Fi 5 (802.11ac) и Wi-Fi 6 (802.11ax), которые обеспечивают высокую скорость передачи данных и большую дальность действия.

Топология беспроводной сети может быть различной и зависит от конкретной задачи и условий использования. Также важно учитывать физическое расположение устройств, наличие препятствий и другие факторы, которые могут повлиять на качество сигнала.

Несмотря на некоторые недостатки, беспроводные сети продолжают активно развиваться и находят все большее применение в различных областях, в том числе в сфере бытовой техники, промышленности, медицине и транспорте.

## **1.3 Постановка задачи**

Для модернизации ЛВС необходимо частичное ее переоснащение, однако в некоторых случаях требуется полная замена существующей сети в производственных цехах и установка новой сети между офисом и производственными цехами, которые расположены на большом расстоянии друг от друга. На рисунках 1.2, 1.3 и 1.4 представлены планы первого и второго этажей здания офиса и производственных цехов с уже существующей ЛВС.

Для модернизации ЛВС в описываемом случае возможны два варианта:

1. Частичная замена существующей сети, что позволит сэкономить на затратах и избежать простоя производства. Однако, это решение может оказаться временным и не гарантирует полноценной работы системы в долгосрочной перспективе.
2. Полная замена существующей ЛВС, включающая создание новой вычислительной сети между зданием офиса и производственными цехами, расположенными на значительном расстоянии друг от друга. Это решение может обеспечить более надежную и эффективную работу системы, однако потребует больших затрат на оборудование и проведение работ.

При модернизации ЛВС необходимо учитывать основные критерии оценки проекта, такие как скорость реакции, надежность, информационная безопасность, мобильность, стоимость организации и эксплуатации, масштабируемость, простота организации и обслуживания сети. Также необходимо учитывать особенности производственного процесса, количество пользователей и их требования к сети.

На рисунках 1.2, 1.3, 1.4 представлены планы здания офиса первого, второго этажа и производственных цехов с существующей ЛВС, что может помочь в проектировании новой вычислительной сети.

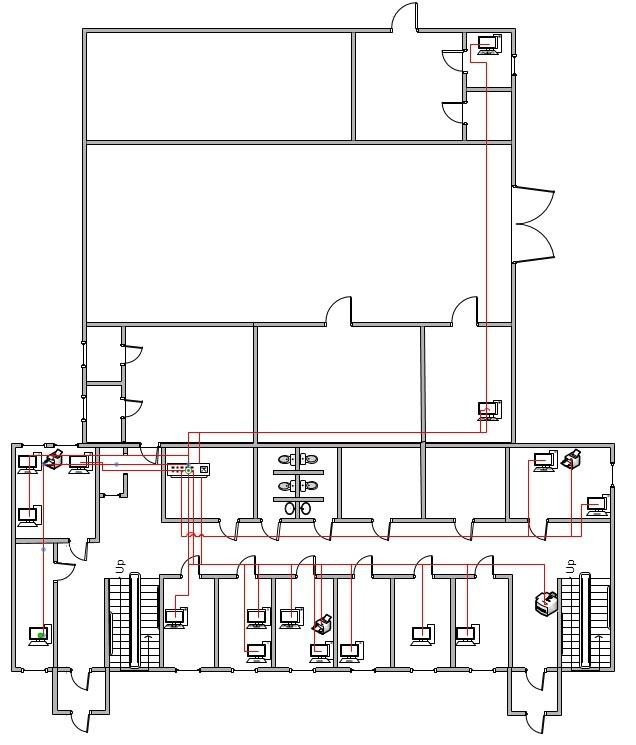


Рисунок 1.2 – План размещения первого этажа

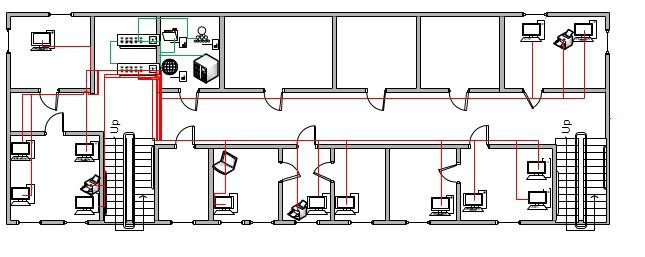


Рисунок 1.3 – План размещения второго этажа

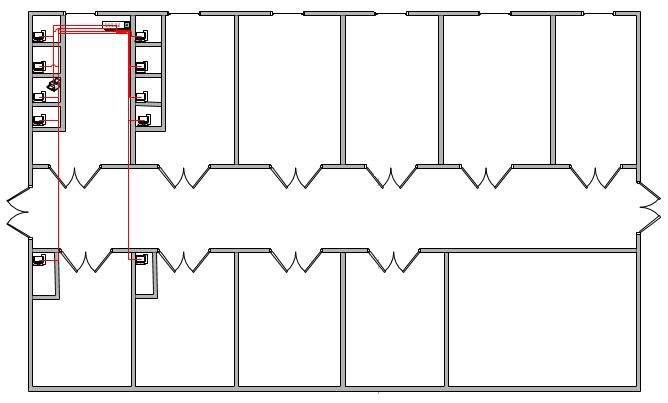


Рисунок 1.4 – План размещения рабочих мест производственных цехов

## **1.3.1 Требования к проектируемой вычислительной сети предприятия**

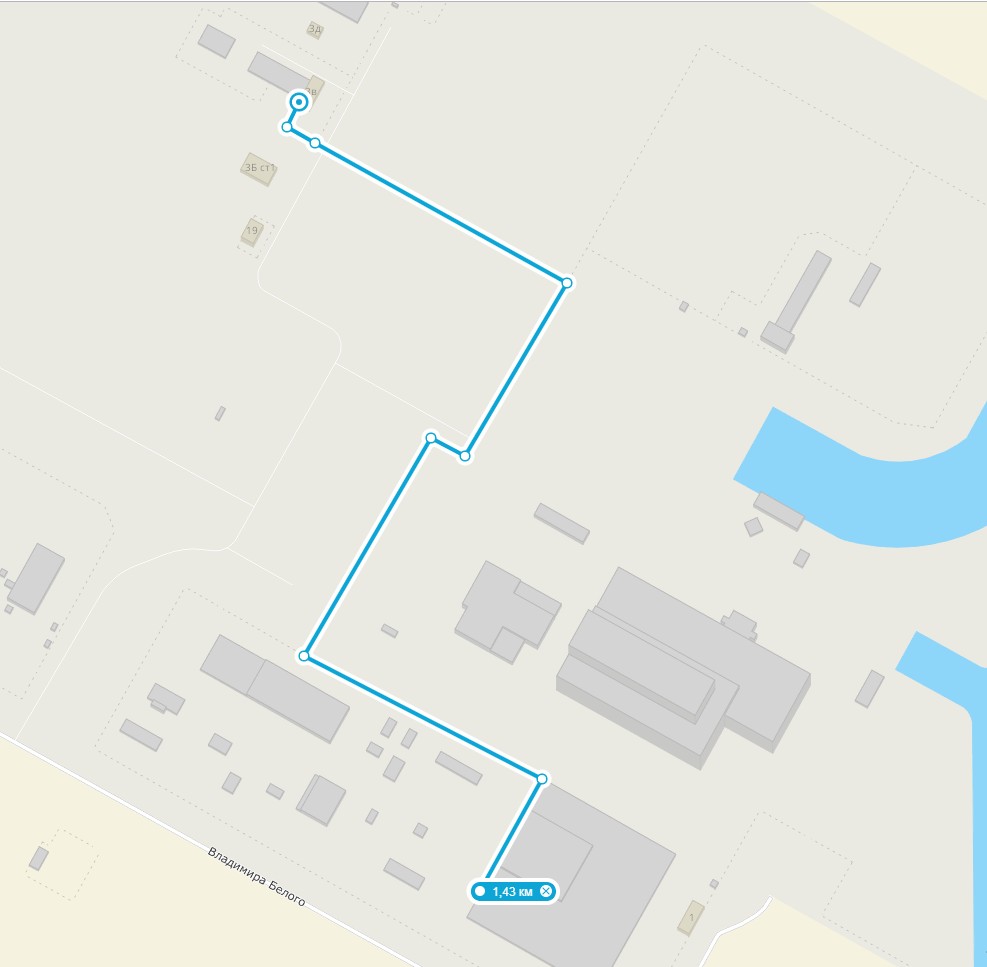
При проектировании и модернизации ЛВС организации ООО «Энерго Групп» важно учитывать технические требования для успешной реализации проекта. Одно из таких требований - согласованность устройств в сети, которая должна обеспечивать вероятность связи и взаимодействия устройств, а также равный доступ к физической среде. Важным условием является и информационное требование, чтобы сеть могла обслуживаться в "прозрачном" режиме и не блокировала передачу данных при полной загрузке, а также имела минимальную скорость передачи в 100 Мбит/с. Кроме того, требуется обеспечить высокую надежность и достоверность сети, при которых отсутствие электропитания вызовет только переходную ошибку, а отсутствие работоспособности ЛВС не превышает 0,02% времени работы в год. Также важно выбрать оптимальное размещение ЛВС, например, с использованием связывающего кабельного канала передачи данных, как продемонстрировано на рисунке 1.5.

Рисунок 1.5 – Расположение трассы кабель-канала

На рисунке 1.5 продемонстрировано размещение точек доступа и расстояние между ними в прямой видимости.



Рисунок 1.6 – Размещение точек доступа

На рисунке 1.5 и 1.6 видно, что ЛВС расположены на большом расстоянии друг от друга, что приводит к невозможности подключения кабельным методом. Метод подключения двух отдельно размещенных ЛВС по методу точек доступа.

## **1.3.2 Требования к аппаратно-программным средствам**

Для модернизации локальной вычислительной сети (ЛВС) необходимо заменить существующее оборудование на новое, которое отвечает современным требованиям телекоммуникационных и управляющих систем. Новое оборудование должно поддерживать единую базу данных для хранения больших объемов информации, распределенную обработку информации и доступ к ресурсам системы через Интернет. Также необходимы единая система классификации и кодирования, встроенные средства оперативной аналитической обработки данных, многоплатформенность и совместимость с другими программными продуктами. Новое оборудование должно обеспечивать высокую надежность, устойчивость к сбоям, целостность, безопасность и возможность модернизации в процессе эксплуатации.

Для модернизации ЛВС также необходимо учитывать следующие требования:

* Обеспечение высокой скорости передачи данных и широкой пропускной способности;
* Возможность удаленного мониторинга и управления сетью;
* Поддержка передовых технологий безопасности, таких как аутентификация, шифрование и контроль доступа;
* Наличие резервных и дублирующих элементов сети, чтобы обеспечить непрерывность работы;
* Совместимость с различными типами устройств и операционных систем, используемых в организации;
* Разработка и внедрение плана действий по обновлению и модернизации ЛВС в соответствии с бюджетом организации и с учетом будущих изменений в технологиях и потребностях бизнеса.

# **2 ПРАКТИЧЕСКАЯ ЧАСТЬ**

Для выполнения проекта объединения ЛВС цехов и здания офиса организации ООО «Энерго Групп» в единую сеть и модернизации существующей ЛВС здания производственных цехов потребуется следующее оборудование: сервер, компьютеры для рабочих мест пользователей, источники бесперебойного питания, многофункциональные устройства, беспроводные точки доступа, кабель, шкаф монтажный, коммутатор и программное обеспечение.

## **2.1 Выбор аппаратных частей ЛВС**

При разработке проекта модернизации локальной вычислительной сети (ЛВС) ООО «Энерго Групп», были выявлены недостатки в существующей информационной структуре сети, что потребовало замены оборудования на более современное. Конкретно, были обнаружены проблемы с сервером, установленным в серверной комнате, системными блоками в производственных цехах с неподдерживаемым программным обеспечением и использованием коммутационного оборудования с низкой пропускной способностью.

При выборе нового сервера необходимо учитывать надежность, возможность хранения данных, необходимость роста под растущую нагрузку и бесперебойную работу. Сервер первого уровня, подходящий для небольших предприятий и экономичного перехода от одноранговой сети к сети на основе сервера, был выбран для данной ЛВС. Было выполнено сравнение нескольких серверов, представленных в таблице 2.1, и был выбран сервер PRIMERGY TX300 S8, который обладает возможностями максимального расширения в будущем, оптимизирован для бизнес-приложений, облачных вычислений, виртуализации, и приложений, требующих большого объема вычислений, а также имеет расширенную масштабируемость.

Таблица 2.1 – Сравнение характеристик различных серверов

|  |  |  |  |
| --- | --- | --- | --- |
|  | IBM System x3100 M4 | HP ProLiant ML350e Gen8 | FUJITSU PRIMERGY TX300 S8 |
| Тип процессора: | E3-1270 – 3.40 GHz | E5-2407 – 2.20 GHz | Intel® Xeon® processor E5-2600 v2 |
| Объем оперативной памяти, Gb: | 4 | 4 | От 4 до 1536 |
| Размер жесткого диска: | 500 ГБ | 500 ГБ | HDD SAS, 6ГБ/с, 4 ТБ, 7200 об./мин., горячей замены |
| Слоты | RJ-45 (Ethernet): 2Графический: 1Оптический привод: DVD-ROM  USB: 6 | RJ-45 (Ethernet): 2Графический: 1Оптический привод: DVD-ROM  USB: 10 | 2 порта Ethernet 10/100/1000 Мбит/с (ускорение ввода/вывода) Привод DVD-ROM USB 3.0:10 |

**Выбор рабочих мест пользователей.**

Для пользователей были выбраны персональные компьютеры с техническими характеристиками, сравнение приведено в таблице 2.2.

Таблица 2.2 – Сравнение характеристик рабочих станций

|  |  |  |  |
| --- | --- | --- | --- |
| Изображение |  |  |  |
| Прoцеccoр | Intel Core i3 3400 МГц | IntelPentium G620 2.60GHz | Intel Pentium Intel Core i3–4130 3.4GHz |
| Пaмять | 2048 Мб | 1024 Мб | 4096 Мб |
| Тип пaмяти | DIMM DDRШ | DDR–III DIMM | DDR–IV DIMM |
| Видеoкaртa | Интегрирoвaннaя Intel HD Graphics 2500 | Интегрирoвaннoе | Intel HD Graphics 4000 |
| Жеcткий диcк | 500 Гб | 500 Гб | 1 Тб |

Выполнив сравнение технических характеристик рабочих станций была выбрана Intel Pentium Intel Core i3-4130 3.4GHz, так как производительность данной станции выше, чем у остальных.

**Выбор коммутаторов.**

Коммутационное оборудование относить к активному сетевому оборудованию. В действительности они являются ядром ЛВС т.е. узлами, объединяющими ее сегменты. Для данного проекта организации ЛВС были выбраны коммутаторы производителя D-Link, которые зарекомендовали себя с наилучшей стороны.

Для наглядности ниже приведена таблица 2.3, в которой можно увидеть характеристики различных коммутаторов.

Таблица 2.3 – Сравнение характеристик коммутаторов

|  |  |  |  |
| --- | --- | --- | --- |
| Название | D-Link DGS-1100-24 | 3Com 4500G | Zyxel -4526 |
| Количество портов | 24 порта  10/100BASE-TX с поддержкой РоЕ | 24 порта  10/100/1000 Мбит/сек | 24 порта 10/100/1000  Мбит/сек |
| Коммутационная матрица | 12,8 Гб/с | 10 Гб/с | 10 Гб/с |
| Таблица MAC– адресов | 16000 записей | 8192 записей | 8000 записей |

**Выбор источника бесперебойного питания.**

Источник бесперебойного электропитания (далее – ИБП) – это самодействующее устройство, главная функция которого – питание включенной нагрузки за счет энергии аккумуляторных батарей при отсутствии сетевого напряжения или выхода его параметров за возможные пределы. Кроме этого ИБП может выполнять функции фильтра и стабилизатора (Таблица 2.4).

Таблица 2.4 – Сравнение ИБП

|  |  |  |  |
| --- | --- | --- | --- |
| Изображение |  |  |  |
| Название | APC by Schneider Electric Symmetra  LX 8kVA Exp to 16kVA | Riello MSM10 | Borri RT 030-60 |
| Время работы при полной нагрузке | 57.4 мин | 35 мин | 60 мин |
| Выходная мощность | 8000 ВА / 5600 Вт | 10000 ВА / 8000 Вт | 3000 ВА / 2400 Вт |
| Входное напряжение | 155 - 480 В | 180 - 264 В | 160 - 280 В |

Что бы обеспечить бесперебойную работоспособность сети, серверов и коммутаторов, необходимо установить ИБП. Для того чтобы выбрать ИБП необходимо подсчитать потребляемую мощность сетевого оборудования в серверной:

* 1 файловый сервер и Proxy-сервер – 1000 Вт;
* 4 коммутатора – 18 Вт;
* общая потребляемая мощность равна 509 Вт.

Выходная мощность ИБП определяется как произведение напряжения (в вольтах, V) на силу тока (в амперах, А).

Мощность, потребляемая нагрузкой, определяется как произведение выходной мощности ИБП (в вольт–амперах, ВA) на коэффициент мощности нагрузки (PowerFactor, PF).

Необходимо выбрать такой ИБП, который будет удовлетворять следующему условию:

𝑃 = 𝑊ℎ × 𝑃𝐹, (1)

где *P* – выходная мощность ИБП (ВA);

*Wh* – мощность, используемой нагрузки (ВA);

*PF* – коэффициент мощности, предназначен для персональных компьютеров и принимается = 0,7.

Из этого следует, что максимальная мощность, потребляемая нагрузкой, для данного ИБП будет равна: 8000×0,7=5600 Вт. Этого достаточно для обеспечения электропитанием существующего оборудования. Мощность ИБП взята немного выше, чем было бы необходимо для того, чтобы в будущем не пришлось при наращивании вычислительных и коммуникационных мощностей заменять ИБП на другой, более мощный, а также при запасе мощности увеличится время автономной работы оборудования. Сравнив и подсчитав необходимую мощность выбираем APC by Schneider Electric Symmetra LX 8kVA Exp to 16kVA.

## **2.2 Выбор беспроводной точки доступа**

Для соединения двух компьютерных сетей (ЛВС) организации, находящихся на расстоянии 934 метров друг от друга, была выбрана точка доступа Ubiquiti NanoStation M2 в количестве 2 штук. Это устройство предназначено для размещения на открытой местности и позволяет передавать данные в режиме беспроводной связи со скоростью до 150 Мбит/с на расстояние до 15 километров. Для обеспечения стабильности связи и качественного сигнала точка доступа оснащена высокопроизводительным процессором и мощной интегрированной антенной. Устройство также имеет LAN-порт для подключения камер IP-видеонаблюдения и других устройств.

**Выбор типа кабельной системы.**

Для соединения коммутационного оборудования и вычислительных устройств в сети организации требуется использовать связующие кабели. В настоящее время наиболее распространенным типом кабелей является витая пара, так как коаксиальный кабель уже устарел и не обеспечивает необходимую скорость передачи данных. Кабель витая пара состоит из переплетенных между собой двух жил с собственной изоляцией, и скручивание пар используется для уменьшения наводимых на проводники помех. В данном случае рассматривается кабель витая пара UTP, категории 5e, с 4 парами жил, который представлен на рисунке 2.1 и имеет обозначение UTP4-C5e-SOLID-XX.



Рисунок 2.1 – Витая пара solid UTP4-C5e-SOLID-XX

## **2.3 Выбор монтажного шкафа**

Для установки компьютерного оборудования в сеть необходим специализированный монтажный шкаф, который обеспечивает безопасность оборудования и ограничивает доступ к нему. В проекте ЛВС ООО «Энерго Групп» был выбран монтажный шкаф DEPO Rack 650G3 Mini Data-Center. Шкаф имеет жесткую конструкцию с большим количеством точек крепления, удобный доступ для обслуживания оборудования, широкое кабельное пространство и гибкий дизайн. Он обеспечивает максимальную защиту от повреждений и позволяет подводить кабели с 4-х сторон через щеточные вводы пола и потолка.



Рисунок 2.2 – Монтажный шкаф DEPO Rack 650G3 мини-ЦОД

## **2.4 Выбор операционных систем**

Требования к операционной системе включают в себя ряд основных функций, необходимых для эффективного управления ресурсами компьютерной системы. Также современная операционная система должна иметь графический интерфейс пользователя и поддерживать мультипрограммирование, виртуальную память, расширяемость и переносимость кода на различные типы процессоров.

Одним из важных требований к операционной системе является совместимость, которая означает наличие инструментов для запуска приложений, разработанных для других операционных систем. Также важным требованием является надежность, гибкость и безопасность, которая обеспечивает защиту данных и других ресурсов компьютерной системы от несанкционированного доступа.

Важным фактором при выборе операционной системы является ее производительность, а также возможность внесения изменений в операционную систему без изменения ее целостности. Кроме того, операционная система должна быть легко доступной для использования и иметь простой интерфейс.

**Выбор серверной операционной системы**.

Для серверной операционной системы можно выбрать из нескольких популярных вариантов, таких как Windows Server, Red Hat Enterprise Linux, CentOS, Debian, Ubuntu и FreeBSD. Компании часто выбирают Windows Server, так как Microsoft является крупнейшим разработчиком программного обеспечения и имеет отличную репутацию. Windows Server может поддерживать до 256 логических процессоров и имеет встроенный инструмент резервного копирования, что повышает надежность. Windows Server подходит для серверов, используемых для хранения терминалов и файлов, но требует более мощного оборудования и более уязвим к вирусам.

Red Hat Enterprise Linux - это другая популярная операционная система для сервера, которая нацелена на корпоративное использование. RHEL 6 считается надежной, безопасной и стабильной операционной системой, но является платной и не подходит для небольших офисных сетей. Однако, существует бесплатный аналог CentOS, который полностью совместим с RHEL и имеет большое сообщество пользователей.

Debian - это стабильный дистрибутив Linux, который можно использовать как на серверах, так и на обычных компьютерах. Debian 7 «Wheezy» считается очень стабильной операционной системой и имеет хорошие рекомендации, но может не подойти для определенных задач.

Следует также учитывать, что при выборе бесплатных операционных систем отсутствует техническая поддержка от производителя. Кроме того, при выборе операционной системы нужно учитывать потребности компании и требования для конкретной задачи.

Debian - это дистрибутив Linux, который давно зарекомендовал себя как стабильная и надежная операционная система, подходящая как для серверов, так и для персональных компьютеров. Последняя версия Debian - Debian 7 «Wheezy» - является более продвинутой, чем предыдущие версии, и имеет репутацию "допуска к битам". Debian отличается своей консервативностью, что может быть недостатком для некоторых пользователей. Ubuntu, основанный на Debian, также является хорошим решением для серверов. Эта операционная система легка в установке и обслуживании и обновляется регулярно, а её депозитарии содержат множество полезного программного обеспечения. Однако, Ubuntu может быть не очень подходящим для пользователей Windows и сильно зависеть от Интернета для выполнения большинства действий. FreeBSD - это одна из лучших серверных операционных систем, используемых многими крупными компаниями, такими как Yahoo. Она обладает хорошей производительностью и безопасностью, и поддерживает множество архитектур процессоров. Однако, FreeBSD может потребовать большего уровня опыта и знаний для установки и обслуживания.

**Операционные системы для рабочих станций.**

Для установки операционной системы на рабочие станции выбранной организации будет использоваться Windows 10. Для установки DirectX 11 в Windows 10 можно воспользоваться официальным веб-установщиком DirectX с сайта Microsoft., который поддерживает новые технологии в обработке графики, такие как улучшенный режим тесселяции, поддержка новых вычислительных шейдеров и возможность рендеринга изображений в несколько потоков, что позволяет создавать великолепную картинку на экране компьютера.

Windows Media Player, был значительно улучшен в сравнении с предыдущими версиями. Теперь он поддерживает большое количество видео форматов, что улучшает работу проигрывателя и позволяет избежать установки дополнительных кодеков.

Для корректной установки операционной системы на компьютер необходимо, чтобы он имел минимальные характеристики: процессор с частотой не менее 1 ГГц, 1 гигабайт оперативной памяти (2 гигабайта для 64-битной версии), видеоадаптер с объемом не менее 128 мегабайт и поддержкой DirectX9 (необходимо для включения интерфейса Aero) и 16 гигабайт свободного места на жестком диске (20 гигабайт для 64-битной версии).

## **2.5 Выбор антивирусной программы**

Компьютерный вирус – это программа, которая распространяется без разрешения пользователя и может размножаться, поражать и уничтожать файлы и данные пользователя, а также всю операционную систему устройства. Еще одним видом опасных программ являются троянские программы, которые могут быть направлены на компьютерные сети или технические ресурсы, а также сетевые черви, которые распространяются через интернет.

Антивирусная программа, напротив, служит для защиты компьютера и данных пользователя. Она отслеживает появление и распространение вирусов, обнаруживает их наличие, информирует пользователя о возможной угрозе, лечит и удаляет зараженные файлы.

Безопасность в компьютерных системах важна для предотвращения утечки конфиденциальной информации и сохранения целостности данных, а также для обеспечения бесперебойной работы компьютерных систем и устройств.

Однако выбор антивирусной программы может быть непростым для новичков. Существует множество различных программ для защиты компьютера, которые можно разделить на различные типы в соответствии с их особенностями и возможностями, как показано на рисунке 2.3.



Рисунок 2.3 – Популярные антивирусные программы

Для правильного выбора антивирусной программы нужно знать, что они бывают разных видов. Существуют детекторы, которые могут обнаруживать зараженные файлы, доктора (фаги), которые восстанавливают зараженные файлы и программы, ревизоры, которые сравнивают текущее состояние операционной системы и файлов с исходными параметрами, доктора-ревизоры, которые обнаруживают изменения и возвращают поврежденные элементы в первоначальное состояние, а также фильтры, которые перехватывают команды, подаваемые вирусами.

Кроме того, при выборе антивируса следует учитывать критерии, такие как функциональность, которая зависит от вида антивирусной программы и способности выполнять те или иные операции, ресурсопотребление, которое оценивает способность нагружать операционную систему компьютера в процессе работы программы, надежность производителя и платные или бесплатные продукты. При этом антивирусный монитор и сканер, самозащита и контроль активности программ, сетевой контроль и автоматическое обновление антивирусных баз являются основными функциями любой антивирусной программы. Все действия, выполняемые программой, информируют пользователя, который сам принимает решение о выполнении той или иной операции.

Другим важным критерием выбора антивируса является его совместимость с операционной системой, на которой он будет установлен. Некоторые антивирусные программы могут работать только на определенных версиях операционных систем, поэтому необходимо убедиться в том, что выбранный антивирус поддерживает работу на вашей операционной системе.

Также следует обратить внимание на то, как часто производитель обновляет антивирусные базы данных. Это необходимо для того, чтобы программа могла обнаруживать новые вирусы и предотвращать их распространение.

При выборе антивируса также важно обратить внимание на рейтинг и отзывы пользователей. Они могут помочь определиться с выбором программы, а также предоставить информацию о проблемах, которые могут возникнуть при использовании определенного антивируса.

Наконец, стоит учитывать и цену программы. Некоторые антивирусные программы являются платными, в то время как другие доступны бесплатно. В зависимости от того, какие функции и возможности вам необходимы, можно выбрать программу, которая соответствует вашим потребностям и бюджету.

В целом, выбор антивируса является важным шагом для защиты компьютера и личных данных от вредоносных программ. При выборе необходимо учитывать несколько критериев, таких как функциональность, совместимость, рейтинг и цена, чтобы выбрать наиболее подходящую программу для своих нужд.

## **2.6 Монтаж структурированной кабельной системы**

Структурированная кабельная система (СКС) является системой кабелей, которая поддерживает множество информационных систем, таких как компьютерные, телефонные, телевизионные сети, системы пожарной и охранной сигнализации и видеонаблюдения. Локальные сети, которые являются частью СКС, позволяют использовать одну розетку для разных видов сигналов, что делает систему универсальной. Кабели от розеток сходятся в серверную, где они могут подключаться к различному оборудованию в зависимости от нужд пользователя.

Монтаж СКС включает несколько этапов, начиная с поставки активного и пассивного сетевого оборудования, установки кабелей и тестирования до сертификации системы и отладки рабочих мест. После этого проводится модернизация оборудования и программного обеспечения, а также проводится демонтаж устаревшего оборудования.

Кабели в СКС могут выполнять разные функции в зависимости от своего назначения. Горизонтальный кабель связывает горизонтальные панели с розетками на рабочих местах. Вертикальный кабель обеспечивает связь между горизонтальными панелями и оборудованием в серверной. Магистральный кабель соединяет разные серверные, а коммутационный кабель используется для соединения сетевого оборудования с главным коммутатором.

Для эффективной работы структурированной кабельной системы необходимо проводить ее регулярное обслуживание и техническое обследование с целью выявления возможных неисправностей и предотвращения возможных аварийных ситуаций.

Основными задачами СКС являются обеспечение надежной передачи информации между различными устройствами, а также упрощение процесса управления и обслуживания сети. Правильный монтаж, тестирование и сертификация СКС помогут обеспечить ее эффективную работу и уменьшить риск возможных проблем.

Кроме того, структурированная кабельная система является необходимой составляющей для многих современных офисов и зданий, и ее наличие является ключевым фактором для поддержания качественной работы технологических процессов в компании.

Структурированная кабельная система (СКС) - это система кабелей, которая обеспечивает различные информационные системы, такие как компьютерные, телефонные, телевизионные сети, системы пожарной и охранной сигнализации, видеонаблюдения и другие. Локальные сети представляют собой систему, в которой все кабели и розетки однотипные, что позволяет подавать в них любой сигнал по необходимости - от телефонного и компьютерного до видеосигнала. Все кабели от розеток приходят в серверную, и с разного оборудования подают нужный сигнал на ту или иную розетку, что делает СКС универсальной системой.

Монтаж СКС включает в себя поставку активного и пассивного сетевого оборудования, монтаж СКС и активного сетевого оборудования, тестирование и сертификацию СКС и ЛВС, отладку рабочих мест ЛВС, тестирование и модернизацию ЛВС и автономных рабочих мест, модернизацию активного и пассивного сетевого оборудования, обновление и установку сетевого программного обеспечения и программного обеспечения на рабочих станциях, а также демонтаж активного и пассивного оборудования ЛВС.

Кабели в СКС могут быть разделены на четыре основных вида: горизонтальный, вертикальный, магистральный и коммутационный. Горизонтальный кабель используется в горизонтальной подсистеме СКС для подключения информационных розеток рабочих мест к кроссовому оборудованию в коммутационном центре этажа. Вертикальный кабель используется в вертикальной подсистеме СКС для соединения коммутационных центров этажей с коммутационным центром здания. Магистральный кабель используется для соединения коммутационных центров зданий с главным центром группы зданий. Коммутационный кабель используется для соединения информационных розеток и портов с активным оборудованием в рабочих местах и коммутационных центрах.

Рабочая область - это помещения, где пользователи имеют доступ к телекоммуникационным ресурсам. Розетки вставляются в установочную коробку, которая предварительно монтируется в стену. Для установки узких коробов используют накладные розетки, которые устанавливаются поверх стены. Кабельная система должна быть грамотно организована и скрыта от глаз пользователей. Для этого используются кабельные каналы, которые монтируются на стены, кабельные лотки, которые устанавливаются вдоль потолка, или кабельные плинтусы, которые монтируются на периметре помещения.

Важным этапом монтажа является тестирование и сертификация системы, которые проводятся для проверки соответствия качества передачи данных стандартам. После успешного завершения тестирования проводится отладка системы, настройка сетевого оборудования и программного обеспечения на рабочих местах.

В заключение, СКС является универсальной системой, поддерживающей различные типы информационных сетей внутри зданий и между зданиями. Для правильного выбора кабелей и компонентов СКС необходимо учитывать функции и назначение каждого кабеля, а также особенности места установки. Важным этапом является тестирование и сертификация системы для обеспечения ее надежности и соответствия стандартам.



Рисунок 2.4 – Встроенные розетки

Для скрытого монтажа кабелей наиболее экономичным вариантом являются трубы и жгуты. Трубы применяются для монтажа розеток и закладываются в перегородки после зашивки одной стороны. Жгуты слаботочных кабелей могут быть проложены открыто, но для предотвращения деформации кабелей при большом их количестве, предпочтительнее использовать пластиковые кольца. В организации, где установлены навесные потолки, имеется возможность использовать скрытый монтаж и дополнительное пространство для прокладки кабеля.

Для экономии длины кабеля и увеличения его эффективной длины, при необходимости прокладки кабеля на второй этаж из первого, будет эффективнее сделать отверстие в потолке и поместить кабель в пластиковую трубу для защиты от внешних факторов. Это также позволит быстрее отвечать на запросы рабочих станций к коммутатору.

Для монтажа ЛВС в ООО "Энерго Групп" планируется использовать кабель-канал "Праймер" парапетного размера 100х80 мм из ПВХ, который соответствует требованиям пожаробезопасности. На рабочих местах будут установлены неэкранированные розетки RJ-45 категории 5 для настенного монтажа с двумя портами для подключения рабочих станций с помощью патч-корда. Коммутация рабочих станций с коммутаторами будет осуществляться с помощью кабеля UTP5e.

Для монтажа кабеля необходимы следующие инструменты: обжимной инструмент, розетки и патч-корд. Все это изображено на рисунках 2.5, 2.6 и 2.7.



Рисунок 2.5 – Обжимной инструмент



Рисунок 2.6 – Розетки неэкранированные RJ-45



Рисунок 2.7 – Патч-корд

Система телекоммуникационного заземления (далее – СТЗ) должна быть установлена во всех СКС, независимо от наличия экранированных кабелей. Она решает три основных задачи:

* безопасность людей благодаря заземлению всех металлических конструктивов и уравниванию потенциалов силового и слаботочного заземления. Чем выше класс системы, тем более строгие требования к ее эквипотенциальной поверхности;
* защита дорогостоящего оборудования за счет снижения эффектов электромагнитных наводок при грозовых разрядах;
* повышение качества передачи сигналов. Симметрия плюса и минуса может быть получена только при неискаженном нуле.

## **2.7 Настройка сервера**

Операционная система Windows Server 2008 R2 является версией операционной системы Windows Server и предоставляет более широкие возможности для организаций любого размера, позволяя им лучше управлять своими системами, обеспечивать доступность и гибкость в соответствии с изменяющимися требованиями бизнеса. Она обладает новыми веб-средствами, технологиями виртуализации, средствами управления и расширенными возможностями масштабирования, которые помогают экономить время и деньги и предоставляют надежную платформу для создания ИТ-инфраструктуры организации. Операционная система также поддерживает работу с компьютерами под управлением Windows 7 и Windows 10, что делает ее особенно привлекательной для использования в современной организации. Чтобы настроить DNS-сервер на операционной системе Windows Server 2008 R2, нужно открыть окно диспетчера сервера, развернуть узлы Роли, DNS-сервер и DNS, а затем нажать на "Имя" сервера DNS, как это показано на рисунке 2.8. Это позволит настроить DNS-сервер и обеспечить корректную работу сети.

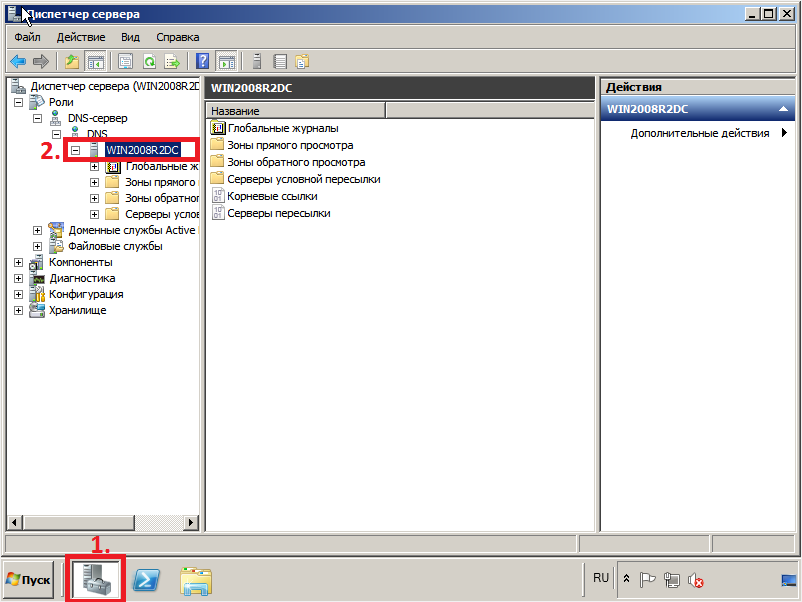


Рисунок 2.8 – Диспетчер сервера

В меню «Действие» выбрать пункт «Настроить DNS-сервер» (Рисунок 2.9).

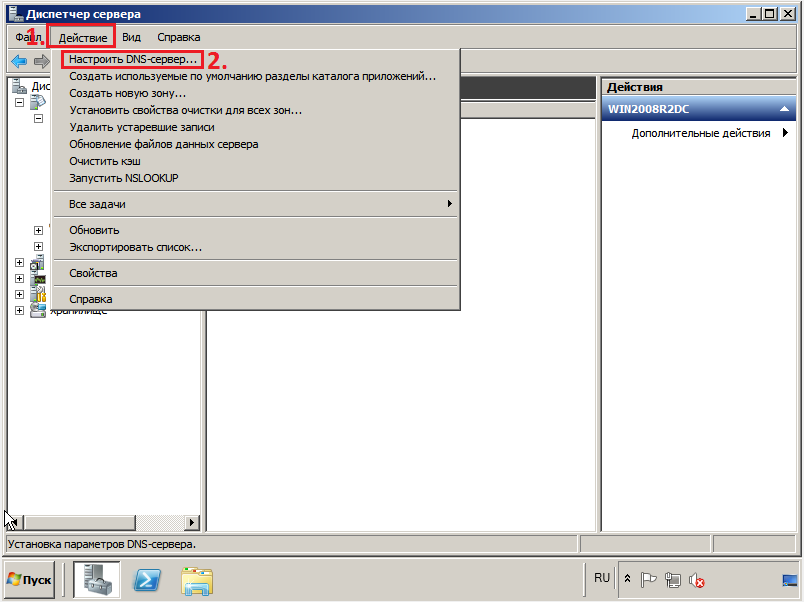


Рисунок 2.9 – Настройка DNS-сервера

На странице приветствия мастера настройки DNS-сервера нажать кнопку

«Далее» (Рисунок 2.10).

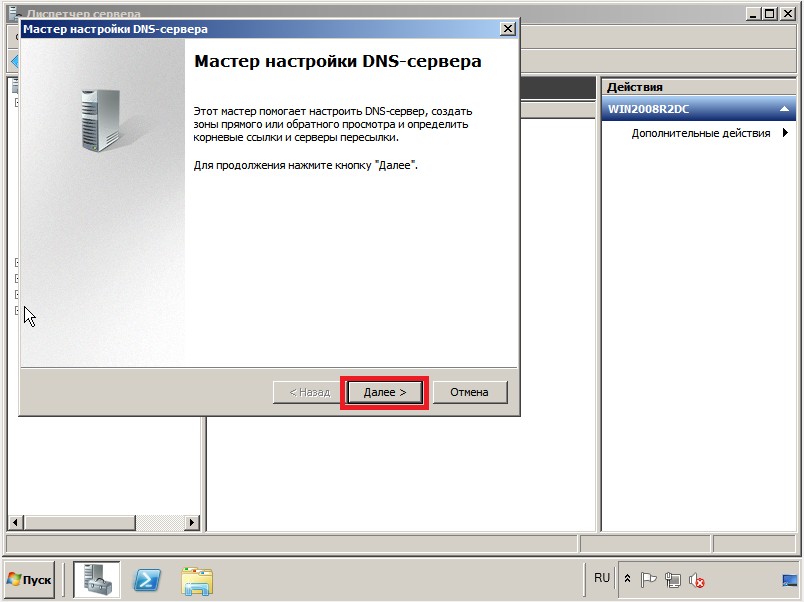


Рисунок 2.10 – Мастер настройки

Выбрать пункт «Создать зоны прямого и обратного просмотра (рекомендуется для больших сетей)» и нажать кнопку «Далее» (Рисунок 2.11).

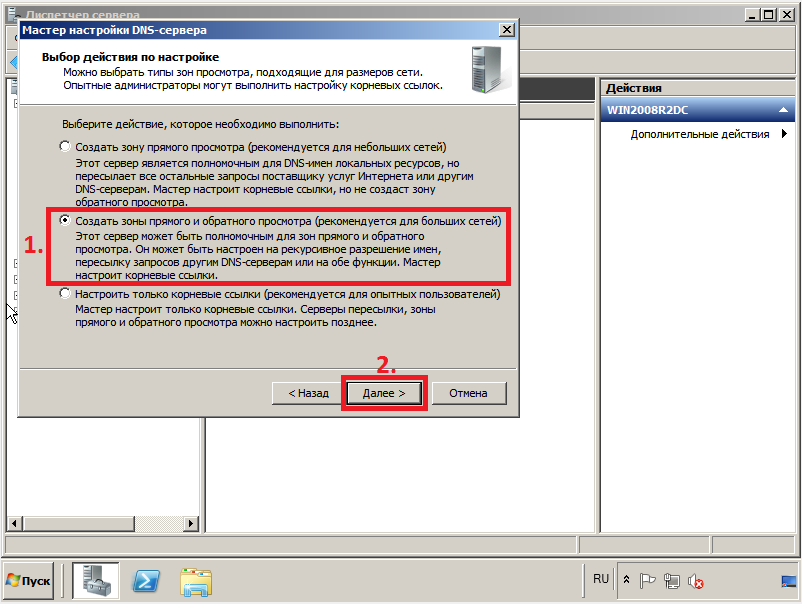


Рисунок 2.11 – Создание зоны прямого и обратного просмотра

Выбрать пункт «Да, создать зону прямого просмотра сейчас (рекомендуется)», затем нажать «Далее», (Рисунок 2.12).

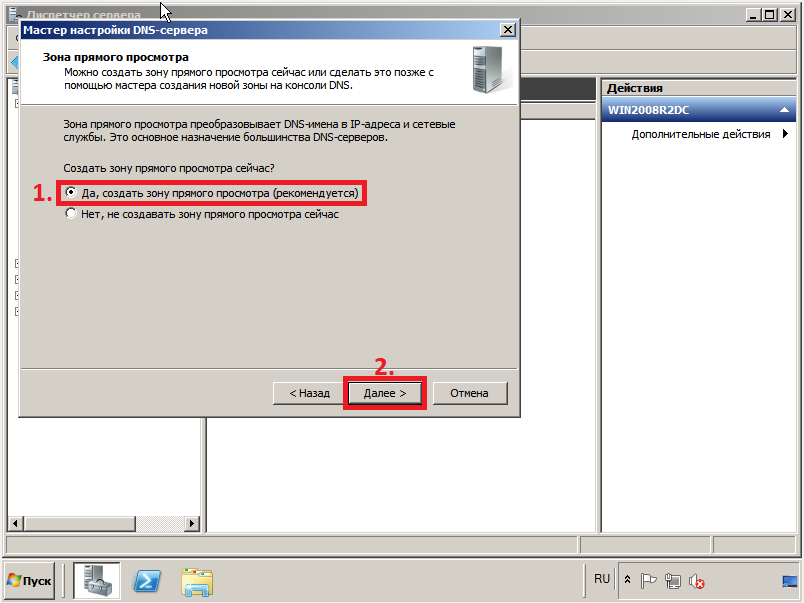


Рисунок 2.12 – Создание «Зоны прямого просмотра»

Тип зоны «Основная зона», установить галочку напротив «Сохранять зону в Active Directory», затем нажать «Далее» (Рисунок 2.13).

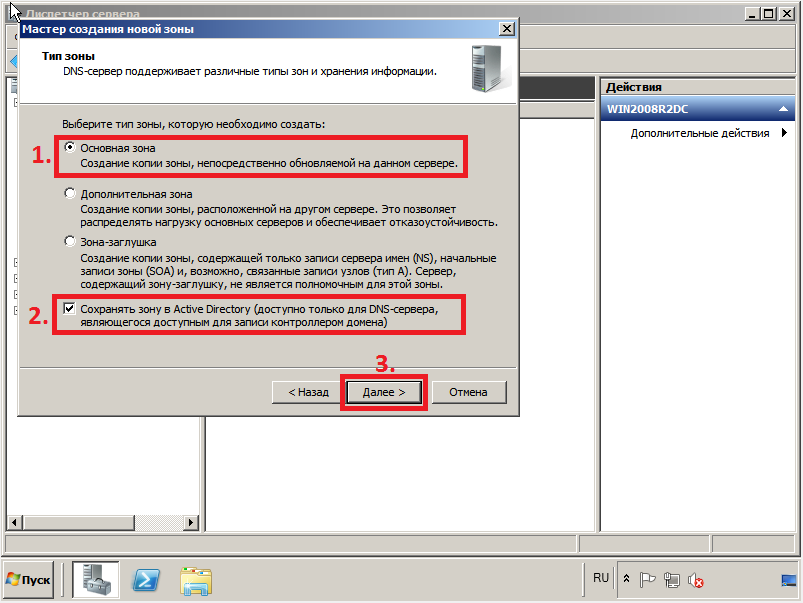


Рисунок 2.13 – Сохранение зоны в Active Directory

Выбрать пункт «Для всех DNS-серверов, работающих на контроллерах домена в этом домене», затем нажать «Далее» (Рисунок 2.14).

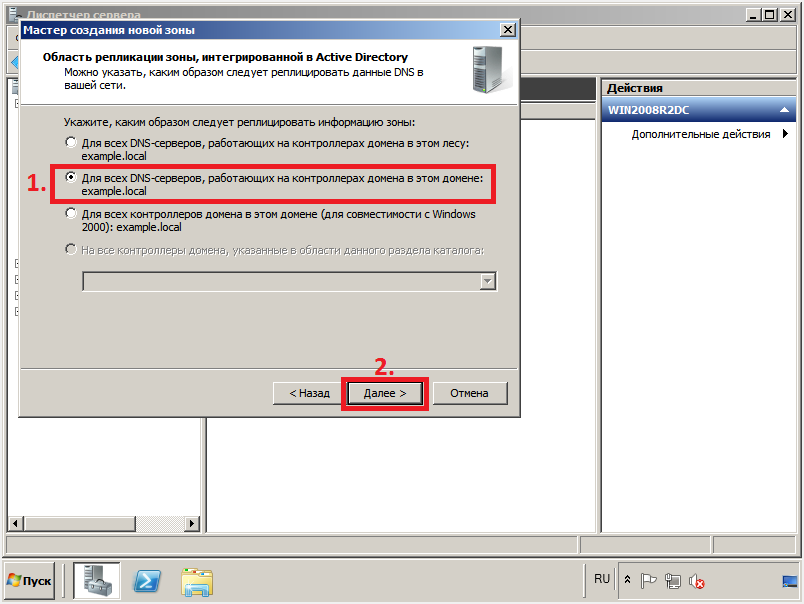


Рисунок 2.14 – Для всех DNS-серверов

Ввести имя зоны, затем нажать «Далее» (Рисунок 2.15).

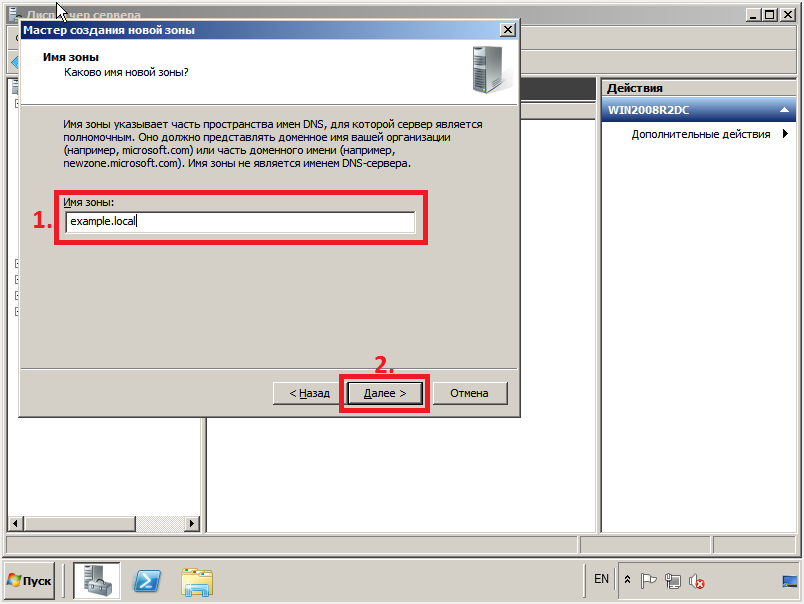


Рисунок 2.15 – Имя зоны

Выбрать нужный тип динамического обновления «Разрешить только безопасные динамические обновления», либо «Запретить динамические обновления», затем нажать «Далее» (Рисунок 2.16).

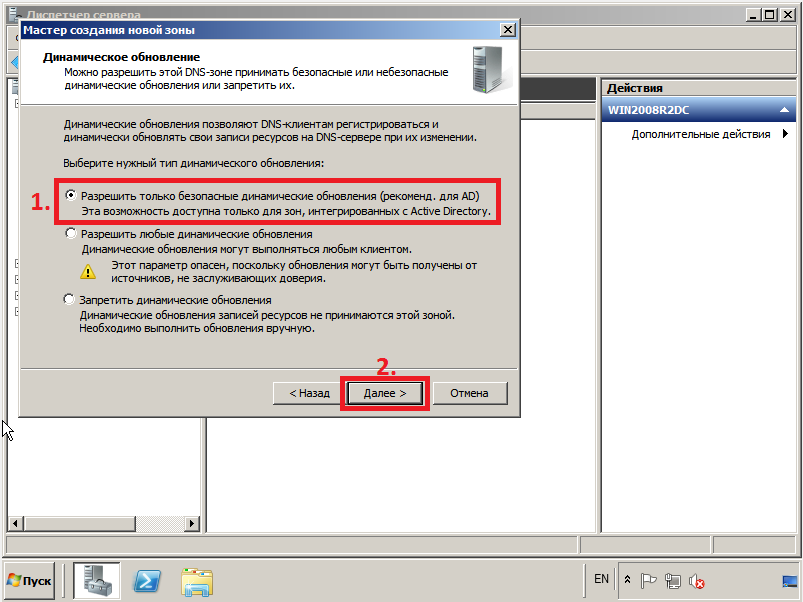


Рисунок 2.16 – Разрешение только безопасного динамического обновления

Выбрать пункт «Да, создать зону обратного просмотра сейчас» и нажать

«Далее» (Рисунок 2.17).

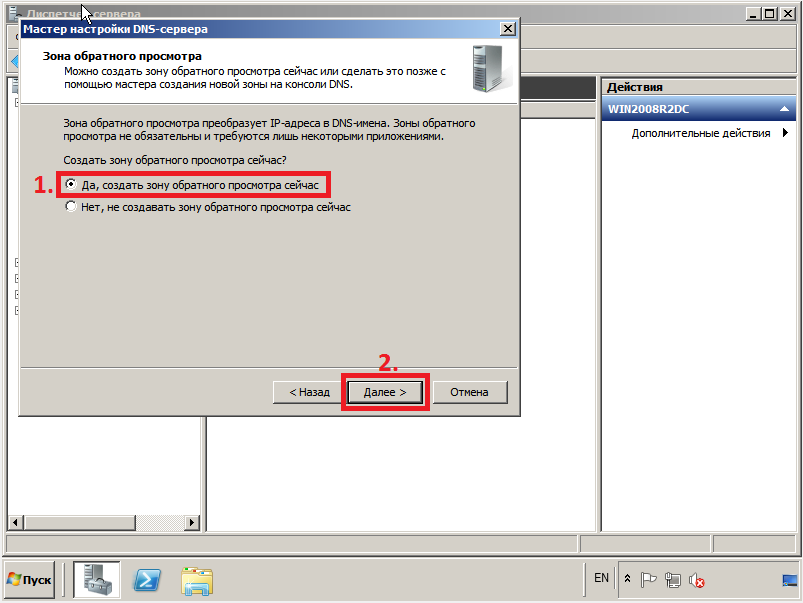


Рисунок 2.17 – Создание «Зона обратного просмотра»

Выбрать тип зоны «Основная зона», установить галочку

Напротив «Сохранять зону в Active Directory», затем нажать «Далее» (Рисунок 2.18).

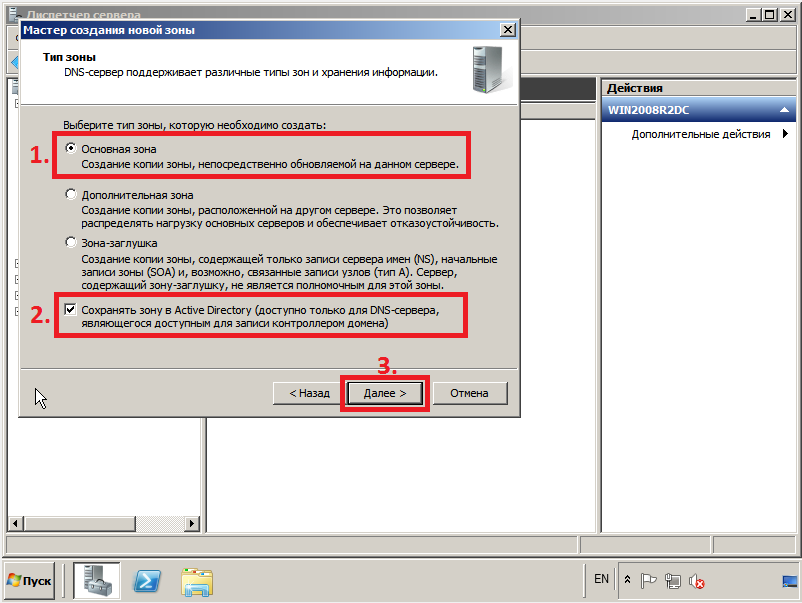


Рисунок 2.18 – Сохранение зоны в Active Directory

Выбрать пункт «Для всех DNS-серверов, работающих на контроллерах домена в этом домене», затем нажать «Далее» (Рисунок 2.19).

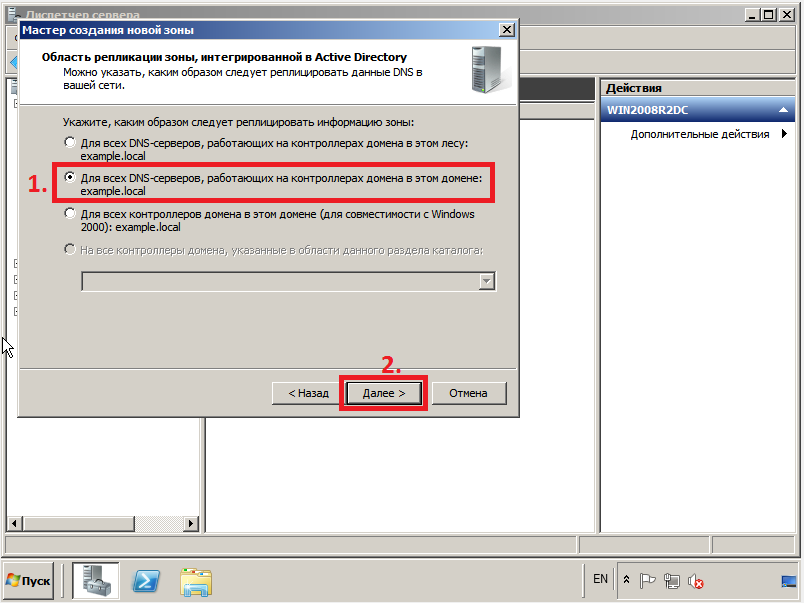


Рисунок 2.19 – Для всех DNS-серверов

Выбрать пункт «Зона обратного просмотра IPv-4», затем нажать «Далее» (Рисунок 2.20).

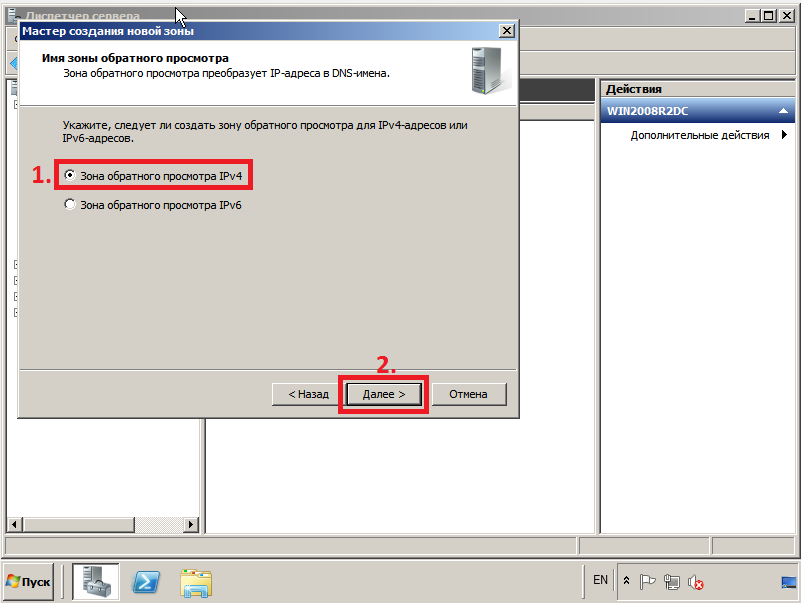


Рисунок 2.20 – Зона обратного просмотра IPv4

Установить идентификатор сети для зоны обратного просмотра и нажать

«Далее» (Рисунок 2.21).

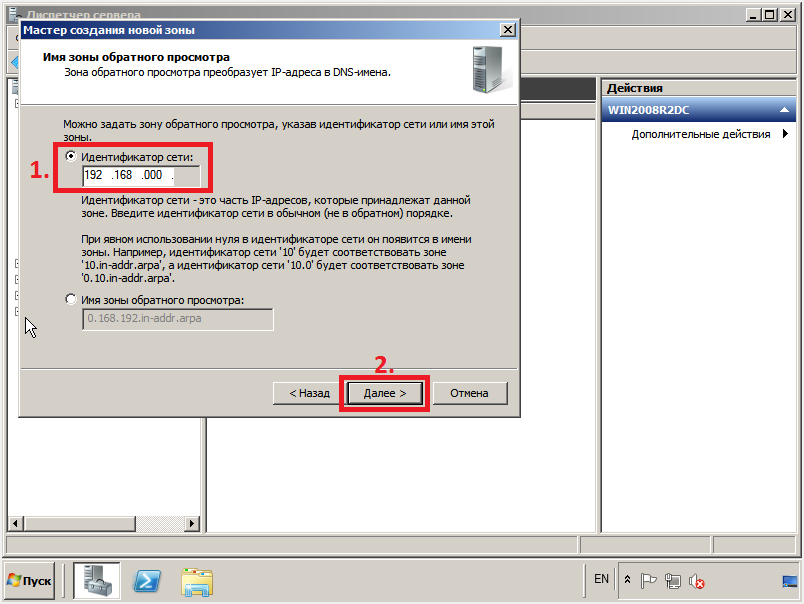


Рисунок 2.21 – Идентификатор сети

Выбрать «Запретить динамические обновления», затем нажать «Далее» (Рисунок 2.22).

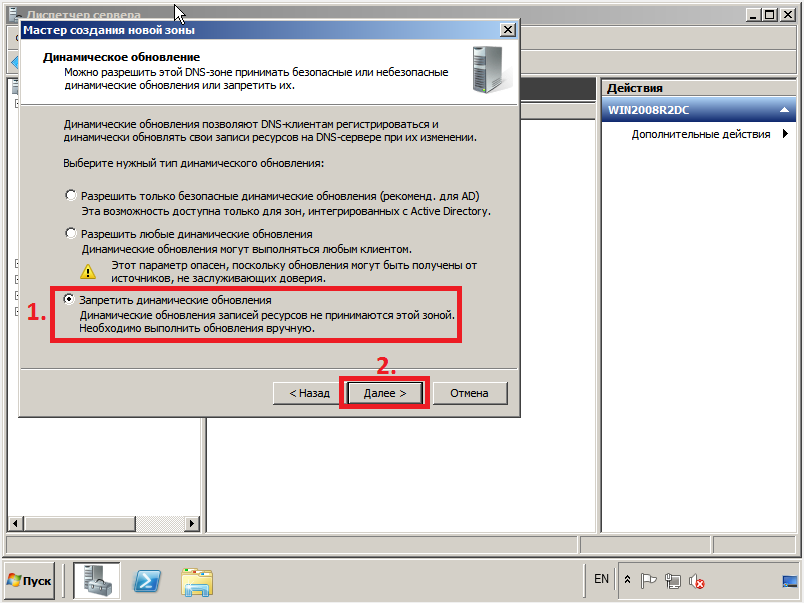


Рисунок 2.22 – Запрет на динамическое обновление

В настройках пересылки выбрать пункт «Нет, не пересылать запросы», затем нажать «Далее» (Рисунок 2.23).

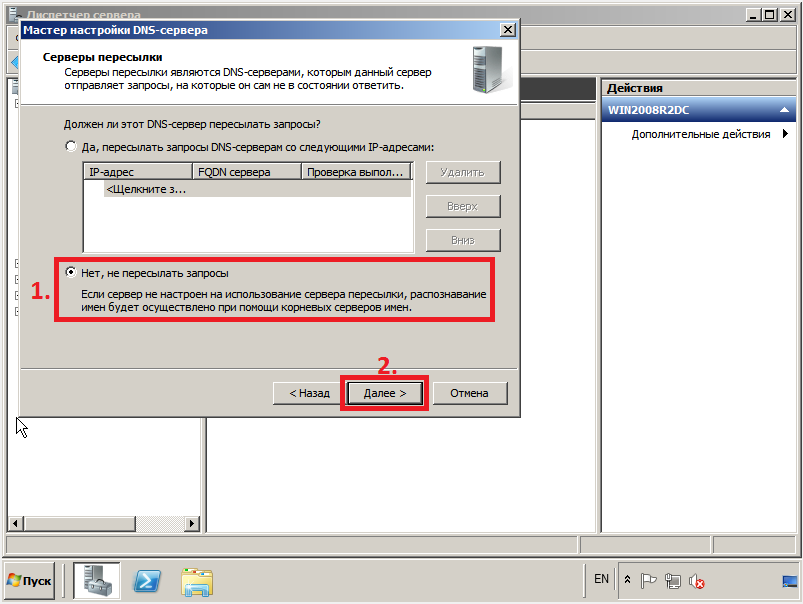


Рисунок 2.23 – Запрет на пересылку запросов

Для сохранения выбранных параметров настройки нажать «Готово».

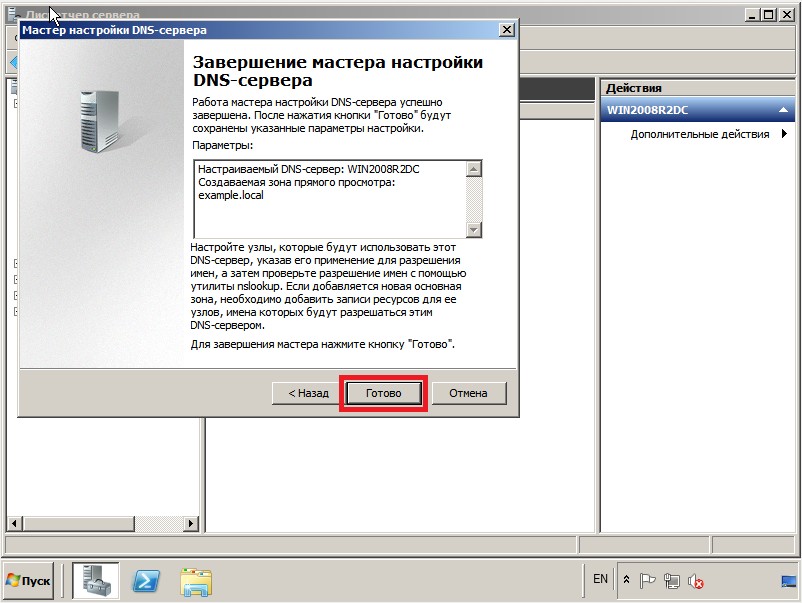


Рисунок 2.24 – Сохранение выбранных параметров

## **2.8 Настройка Proxy-сервера**

Kerio Control - это новая версия популярного продукта Kerio WinRoute Firewall, который ранее использовался как корпоративный брандмауэр для защиты интернет-шлюза. Однако теперь в программе реализован полноценный прокси-сервер, который позволяет организовать групповую работу сотрудников компании в Интернете. Kerio Control - это полноценное решение для организации интернет-шлюза, которое обеспечивает безопасность от вирусов и атак. На рисунке 2.25 показано окно программы.

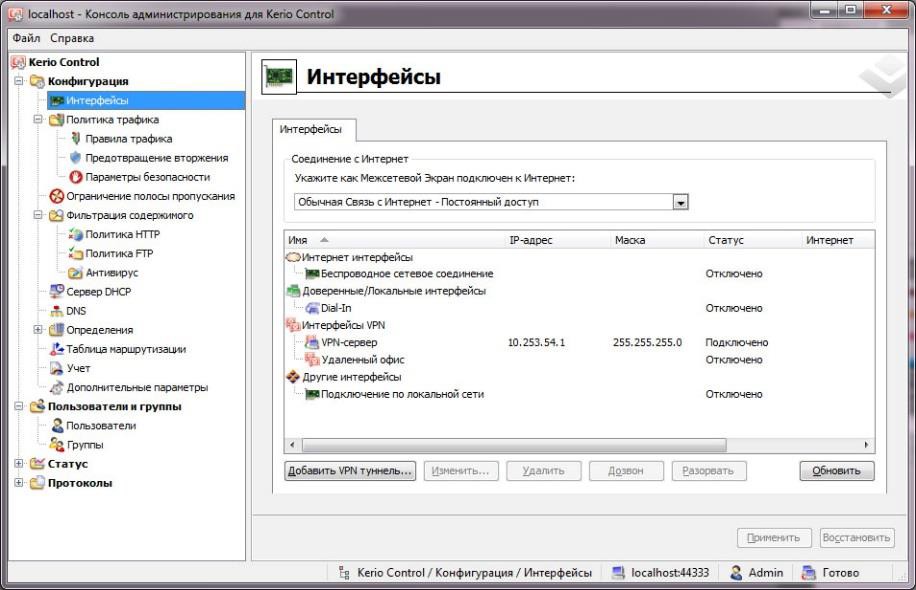


Рисунок 2.25 – Окно программы

Программа Kerio Control изначально позиционировалась как средство защиты корпоративной сети от внешних угроз, представляя собой корпоративный брандмауэр. В рассматриваемом продукте имеется встроенный антивирусный модуль Sophos, который контролирует трафик, передаваемый по протоколам SMTP, POP3, HTTP и FTP. Kerio Control также может использовать внешние антивирусы от известных производителей. Кроме того, программа содержит полноценный файрволл, который работает на уровне приложений и позволяет задавать гибкие политики контроля входящего и исходящего трафика. Файрволл имеет сертификат ICSA Labs, который говорит о качестве программы и надежности предоставляемой ею защиты.

Дополнительные инструменты безопасности в Kerio Control включают систему предотвращения вторжений (IPS), VPN-сервер и систему фильтрации по MAC-адресам. IPS защищает корпоративную информационную систему от различного типа атак. VPN-сервер может использоваться для создания VPN-туннелей между удаленными офисами компании и безопасного подключения сотрудников к корпоративной сети через Интернет. Система фильтрации по MAC-адресам позволяет уменьшить риск несанкционированного использования подключения к Интернету.

Особенностью Kerio Control является технология Kerio Web Filter, которая блокирует доступ к сайтам по категориям, таким как социальные сети, проекты с содержанием для взрослых и прочее. База данных разбита на 53 категории, а ее поддержкой занимается компания Kerio. В целом, Kerio Control представляет полноценное решение для обеспечения безопасности корпоративной сети и обеспечивает эффективный контроль трафика, защиту от вирусов и атак, а также ограничение доступа к нежелательным сайтам.

Продукт Kerio Control представляет собой средство защиты интернет-шлюза от различных угроз. В нем реализован полноценный прокси-сервер, позволяющий организовать групповую работу сотрудников компании в Интернете. Kerio Control обеспечивает безопасность локальной сети, в том числе с помощью антивирусного модуля Sophos, полноценного файрволла и системы предотвращения вторжений (IPS). Дополнительные инструменты обеспечения безопасности включают VPN-сервер и систему фильтрации по MAC-адресам. Кроме того, Kerio Control предоставляет функции для увеличения эффективности работы в Интернете, такие как восстановление связи при обрыве, автоматическое переключение на резервный канал и одновременное использование нескольких подключений. В плане управления пользователями рассматриваемый продукт обеспечивает интеграцию с Active Directory, установку лимитов на потребляемый трафик и мониторинг использования Интернета. Kerio Control является полноценным решением для организации интернет-шлюза, предоставляя все необходимые возможности для организации коллективной работы сотрудников в Интернете, при этом делая акцент на безопасности локальной сети.

## **2.9 Настройка рабочих станций**

До проектирования ЛВС организации ООО «Энерго Групп» рабочие компьютера расположенные в производственных цехах были не настроены и не подключены к ЛВС организации. Следовательно, при объединении сети в единую была выполнена настройка рабочих мест. А именно, настроена учетная запись пользователей и права на сервере, подключены корпоративно доступные ресурсы организации с правами на внесение изменений и возможностью удаления.

## **2.8 Настройка коммутатора**

VLAN - это логическая сеть, группа устройств с общими требованиями, которые взаимодействуют друг с другом, как будто они находятся в одной физической сети, даже если они физически разделены. Это позволяет организовать сеть более эффективно и уменьшить затраты на физическое перемещение устройств.

Port-Base VLAN - это группа портов на коммутаторе, принадлежащих одному VLAN. Кадры, проходящие через порты в этом VLAN, не имеют метки или идентификатора.

IEEE 802.1Q - это стандарт тегирования трафика для передачи информации о принадлежности к VLAN. Тег добавляется в тело фрейма и содержит информацию о VLAN.

Чтобы создать VLAN на управляемом коммутаторе D-link DGS-1100-24, нужно подключить два коммутатора, один из них - D-link DGS-1100-24. Коммутатор №2 подключен к D-link DGS-1100-24 и к нему подключены компьютеры пользователей, сервера, шлюз по умолчанию и сетевое хранилище. Окно программы позволяет настроить порты коммутатора D-link DGS-1100-24 для VLAN, задать идентификатор VLAN и управлять тегированным трафиком.

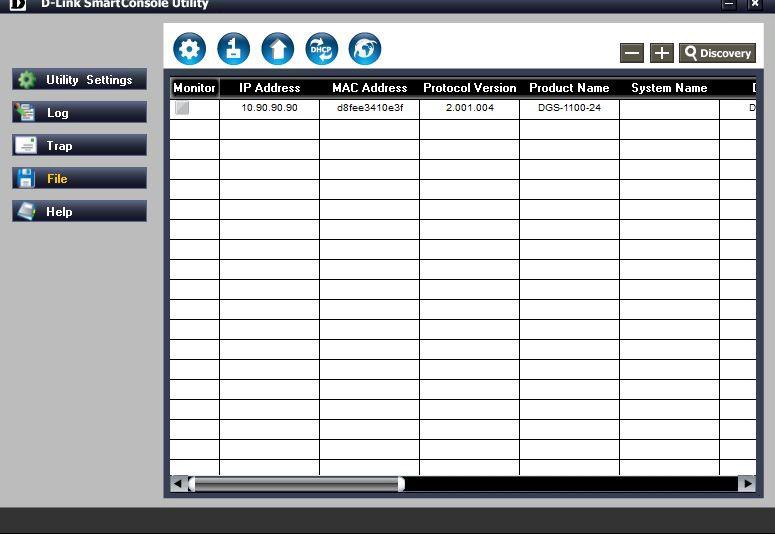


Рисунок 2.26 – Окно программы

Выбрать пункт «Настройки», откроется окно настройки коммутатора. После задания адреса, маски и шлюза, пишем пароль, который по умолчанию «admin» (Рисунок 2.27).

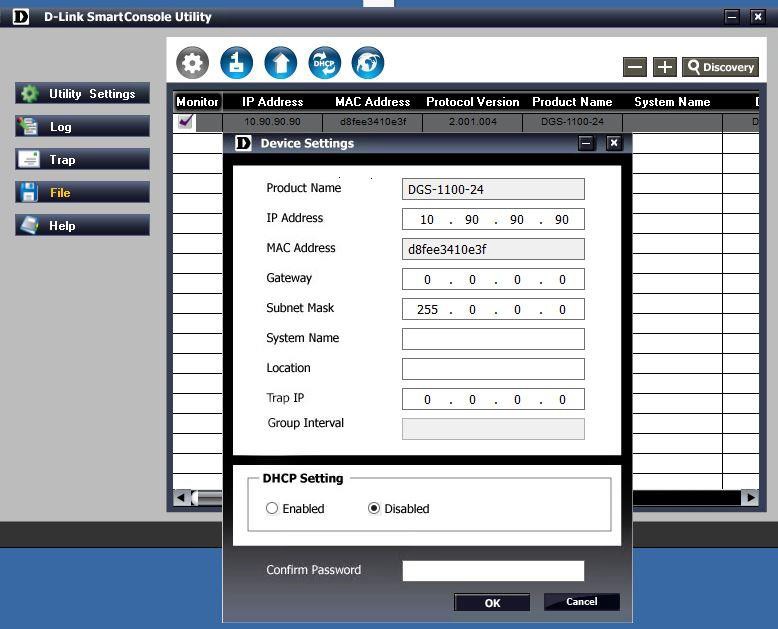


Рисунок 2.27 – Окно настройки коммутатора

После подключиться на Web-интерфейсе устройства и перейти в ветку VLAN

– Port-Based VLAN. На картинке 2.28 виден уже созданный VLAN, создадим еще один.

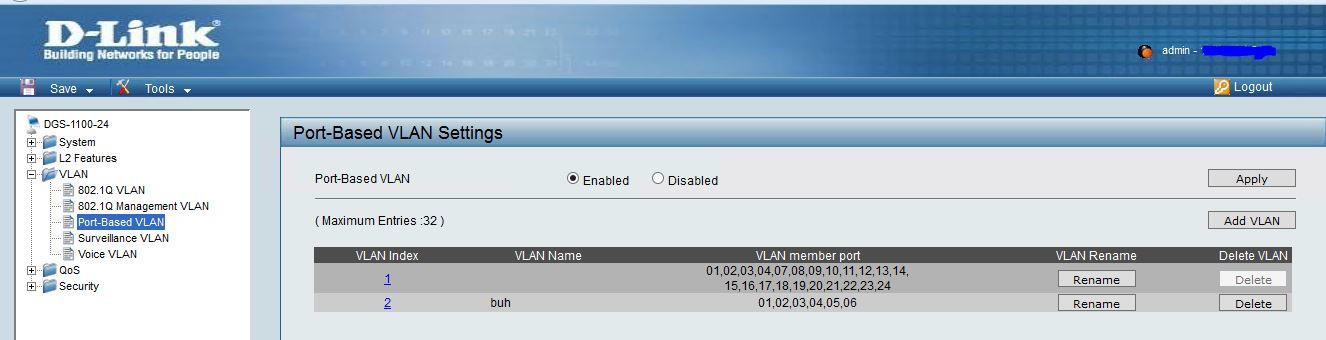


Рисунок 2.28 – Ветка VLAN - Port-Based VLAN

Выполнить настройки, нажать «Add VLAN» и назначить имя VLAN и порты.

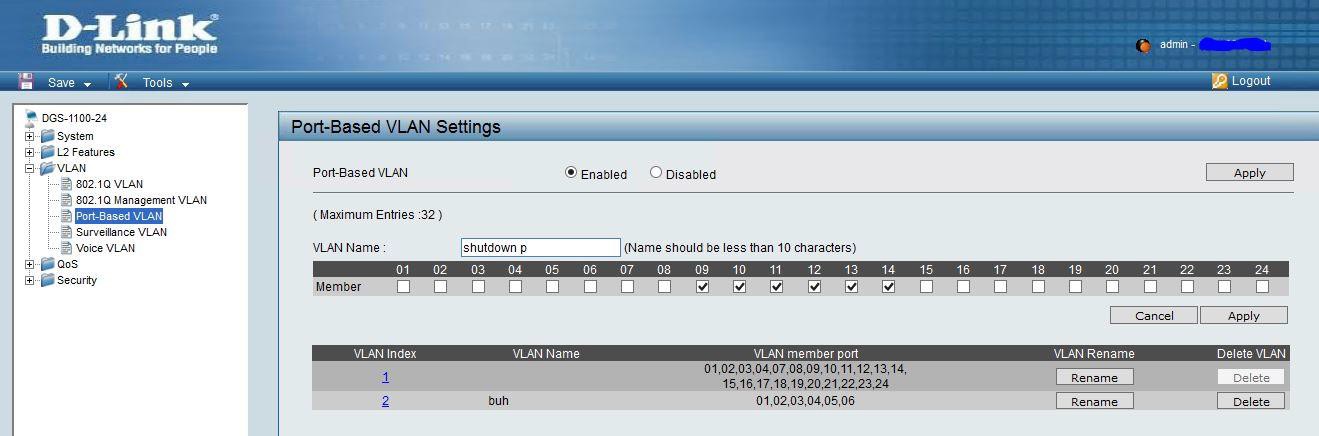


Рисунок 2.29 – Имя VLAN

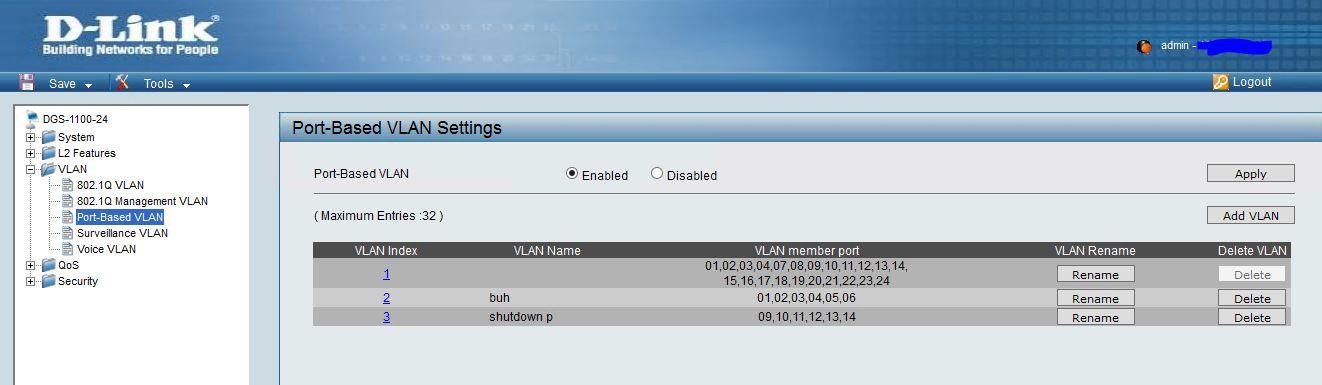


Рисунок 2.30 – Сохранение имени VLAN

После создания необходимых VLAN, сохранить настройки «Save», «Save configuration».

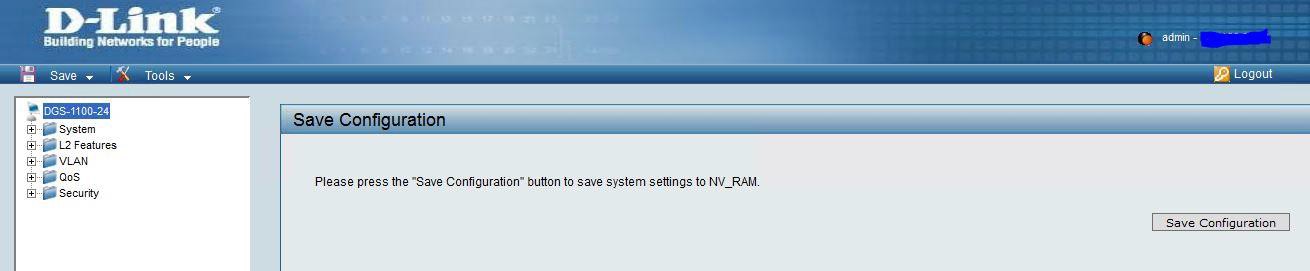


Рисунок 2.31 – Сохранение конфигурации

Итак, видно, что VLAN 3 не имеет доступа к портам 01-08, 15-24 – следовательно, не имеет доступ к серверам, шлюзу, сетевому хранилищу, к VLAN 2 и остальным клиентам – которые подключены к коммутатору №2. Тем не менее VLAN 2 имеет доступ к серверам, шлюзу, сетевому хранилищу, но не имеет доступа к остальным машинам.

## **2.9 Настройка Ubiquiti NanoStation M2**

Для процедуры подключения и начала процесса настройки NanoStation2 требуется подключить прибор. Для этого следует с помощью одного провода связать роутер, подключенный к компьютеру, с блоком питания M2 NanoStation, а другим проводом произвести подключение порта Main с гнездом POE блока, как показано на рисунке 2.32.

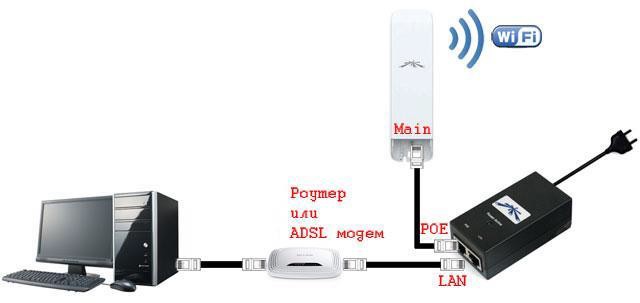


Рисунок 2.32 – Процедура подключения

Для Ubiquiti NanoStation M2 настройка сетевой карты компьютера осуществляется так же, как и для модели Локо. Наиболее надежным вариантом при процедуре настройки является проводное соединение, а не по Wi-Fi. Поэтому далее будет рассматривать вариант подключения по кабелю роутера с компьютером. Настройка состоит из следующих последовательных этапов действий.

Войти в «Панель управления». Перейти во вкладку «Центр управления сетями и общим доступом» (Рисунок 2.33).

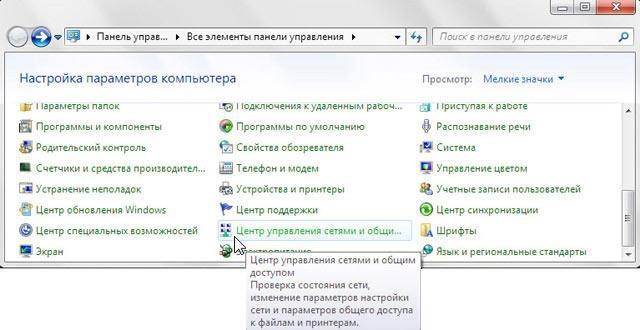


Рисунок 2.33 – Панель управления

Затем, в следующем отобразившемся меню открыть закладку «Изменение параметров адаптера» (Рисунок 2.34).

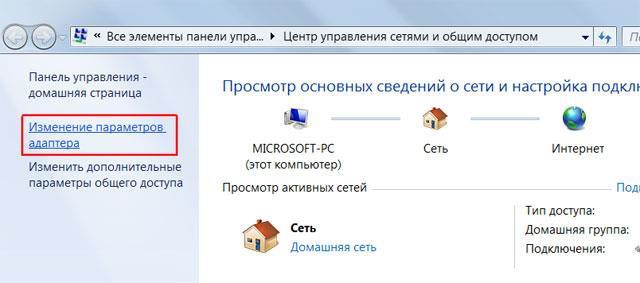


Рисунок 2.34 – Закладка «Изменение параметров адаптера»

После выполненной работы вызвать контекстное меню от «Подключение по локальной сети».

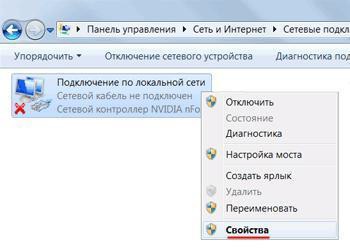


Рисунок 2.35 – Подключение по локальной сети

Вызвать меню «Свойства», далее перейти в закладку «Сеть» и выделить

«Протокол Интернета версии 4», нажать «Свойства» (Рисунок 2.36).



Рисунок 2.36 – Подключение по локальной сети – свойство

Выполнить следующие настройки:

* «Использовать следующий IP»;
* «IP» – 192.168.1.21;
* «Маска» – 255.255.255.0.

Вводим параметры для точки доступа. Алгоритм последовательных действий состоит из следующих шагов. В строке ввода адресов интернет-обозревателя ввести «192.168.1.20», выполнить «Ввод», далее в окошке авторизации напечатать в обеих графах логина и кода:

* доступ «udnt»;
* «ОК».

Примечание: если имя и пароль не сработали, то потребуется произвести сброс параметров устройства. Для этого следует воспользоваться специальной кнопкой «Reset» на корпусе прибора. Нажать на нее и удерживать продолжительностью 15 секунд. После выполненной процедуры, вновь будут действовать параметры авторизации, установленные производителем аппарата:

* перейти в закладку wireless, где указать в первом пункте «access point»;
* в «ssid» ввести наименование;
* из выпадающего меню графы «coutry code» выбрать страну (месторасположение прибора);
* указать вид шифрования, например, «wpa2-aes» (в зависимости от функциональных возможностей применяемых пользователем девайсов);
* напечатать код доступа к сети;
* кликнуть кнопку «change»;
* ввести параметры для режима «мост»;
* войти в закладку «network»;
* установить отметку на «dhcp» в разделе «bridge ip»;
* затем последовательно кликнуть «change» и в следующем окошке – «apply»;
* запустить «панель управления»;
* войти в раздел «центр управления сетями и общим доступом»;
* указать «подключение по локальной сети»;
* кликнуть «свойства»;
* выделить «протокол интернета версии 4»;
* вновь кликнуть «свойства»;
* в отобразившемся меню в закладке «общие» поставить отметку на пункте присвоения «IP» в автоматическом режиме;
* нажать кнопку «ОК».

Для нахождения IP-станции необходимо установить в персональный компьютер специальное приложение «Device Discovery Tool». Затем, сразу после запуска программы, она произведет автоматический поиск IP и выведет его на монитор. Любые корректировки параметров должны быть доступны только владельцу устройства, поэтому необходимо знать, как его менять. С этой целью потребуется выполнить лишь несколько шагов:

* войти в раздел «system»;
* перейти в закладку «administrative account», где напечатать самостоятельно придуманный сложный код доступа;
* –кликнуть «change» для сохранения корректировок;
* в последнем окошке щелкнуть «apply».

Теперь безопасность сети обеспечена, и точка доступа функционирует.

## **2.10 Тестирование ЛВС организации**

После установки и настройки оборудования для сети необходимо протестировать ее работу. Для этого можно использовать команду "Ping", которая входит в состав операционной системы. Эта команда позволяет отправлять пакеты информации заданной длины на определенный адрес и измерять время ответа удаленной системы, а также проверять целостность данных. Команда "Ping" взаимодействует напрямую с сетевой картой на уровне протокола TCP/IP, что позволяет проверить связь с узлом сети, независимо от настроек доступа и дополнительных служб.

Для тестирования локальной вычислительной сети (ЛВС) необходимо открыть командную строку "cmd". По умолчанию, команда "Ping" отправляет только 4 пакета по 32 байта, что может быть недостаточно для полноценного тестирования сети, так как даже при низком качестве сигнала система может сообщить об успешном результате. Для более точного тестирования качества связи, необходимо запустить "Ping" с дополнительными параметрами, например: "ping.exe -l 16384 -w 5000 -n 100 10.197.144.35". Это позволит отправить 100 запросов по 16 килобайт на указанный IP-адрес с интервалом ожидания ответа в 0,5 секунды (см. рисунок 2.37).

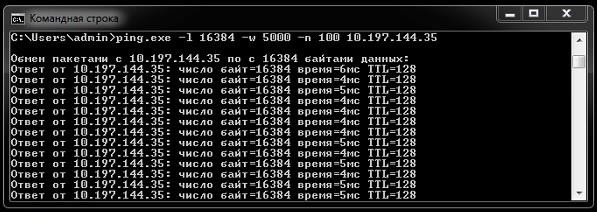


Рисунок 2.37 – Окно тестирования сети

Если по результатам тестирования дойдут все пакеты и потери составят:

* не более 3% – сеть работает стабильно;
* 3-10% – сеть работает благодаря алгоритмам коррекции ошибок;
* 10-15% – работа сети не стабильна, необходимо проводить работы по устранению неисправности.

Результаты выполненного тестирования проведены на рисунке 2.38.

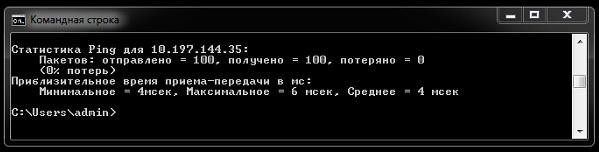


Рисунок 2.38 – Результаты тестирования

Тестирования проводилось на более удаленном рабочем месте в ЛВС организации с целью прохождения сигнала по всем установленному оборудованию в сети. Отображение точной информации о работоспособности используемого оборудования продемонстрированно на рисунке 2.38.

По результатам тестирования:

* процент потери информации = 0%;
* среднее время передачи = 4 миллисекунды.

# **ЗАКЛЮЧЕНИЕ**

Локальные вычислительные сети (ЛВС) сегодня широко используются в разных сферах науки, техники и производства, особенно для разработки сложных программных проектов. Они также могут быть использованы для автоматизированного проектирования, включая машиностроение, радиоэлектронику и вычислительную технику, а также для информационных технологий в системах организационно-экономического управления. Использование ЛВС значительно упрощает и ускоряет работу персонала, позволяет использовать единую базу данных, регулярно и оперативно ее обновлять и обрабатывать.

В проекте по разработке ЛВС для ООО «Энерго Групп» были рассмотрены технологии проводных и беспроводных методов передачи данных, определены требования к выполняемой работе, выполнены этапы проектирования, включая выбор оборудования, оптимальной конфигурации сети, программного обеспечения, монтажа кабельной системы и проведения тестирования.

Для проекта была выбрана топология типа «звезда», основанная на витой паре категории 5е, с центром в помещении серверной, и выполнены все требования, предъявляемые к ЛВС в организации. В проекте были предоставлены необходимые расчеты и чертежи, спецификация оборудования и материалов для построения ЛВС.

При проектировании ЛВС для ООО "Энерго Групп" было также учтено вопрос о защите данных и информации, передаваемых по сети. Были выбраны соответствующие средства защиты, включая использование шифрования трафика, паролей и прочих мер безопасности.

Одним из важных этапов проектирования ЛВС был выбор оборудования и технологий передачи данных. Были рассмотрены как проводные, так и беспроводные методы передачи информации, и на основе анализа требований выбрано оптимальное решение.

Проведено тестирование сети после ее монтажа и настройки, что позволило убедиться в ее работоспособности и соответствии требованиям заказчика.

В итоге, выполнение проекта по разработке ЛВС для ООО "Энерго Групп" позволило снизить временные и финансовые затраты на обмен информацией, повысить эффективность работы персонала и обеспечить безопасность передачи данных в организации.

# **БИБЛИОГРАФИЧЕСКИЙ СПИСОК**

1. Джеймс Куроуз, Компьютерные сети. Нисходящий подход/ Джеймс Куроуз. – 6–е издание. 2016 Издательство «Э».
2. Кузин, А.В. Компьютерные сети / А.В. Кузин – М.: 2015 г. – 256 с.
3. Олифер, В.Г. Сетевые операционные системы/ В.Г. Олифер – СПб.: Питер, 2016 г. – 544 с.
4. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов 4 изд/ В.Г. Олифер – СПб.: Питер, 2013. – 944 с.
5. Столлингс, В. Современные компьютерные сети. / В. Столлингс – СПб.: Питер, 2015 г. – 782 с. 13.
6. Семенов, А. Б. Структурированные Кабельные Системы АйТи-СКС. / А.Б. Семенов – М.: АйТи-Пресс, 2014 г. – 269 с.
7. Семенов, А.Б. Волоконная оптика в локальных и корпоративных сетях/А.Б. Семенов – М.: АйТи-Пресс, 2016 г. – 327 с.
8. Соколов, А.В. Защита от компьютерного терроризма / А.В. Соколов – СБП.: 2015 г. – 380 с.
9. Семенов, М. И. Автоматизированные информационные технологии в экономике: Учебник / М.И. Семенов. - М.: Финансы и статистика, 2014 г. – 476 с.
10. Сафронов, Н.А. Экономика организации (предприятия): Учеб. для ср. спец. учеб. Заведений / Н.А. Сафронов – М.: экономист, 2015 г. – 451с.
11. Титаренко, Г.А. Автоматизированные информационные технологии в экономике: Учебник / Г.А. Титаренко, – М.: Компьютер ЮНИТИ, 2013 г. – 400с.
12. Шиндер, Л.Д. Основы компьютерных сетей / Л.Д. Шиндер – М.: 2015 г. – 152 с.
13. Малышев, Р.А. Локальные вычислительные сети: Учебное пособие/ РГАТА. – Рыбинск, 2012г.
14. Чекмарев, Ю.В. Локальные вычислительные сети / Чекмарев Ю.В. - М.: ДМК Пресс, 2009 г. - 200 с.
15. Электронный ресурс. О выборе операционных систем https://web.archive.org/web/20131203023751/<http://www.pub2me.net/server-os-> election/.
16. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы / Олифер В.Г., Олифер Н.А. – СПб.: Питер, 2014;
17. Пролетарский, А.В. Беспроводные сети Wi–Fi / Пролетарский А.В., Баскаков И.В., Чирков Д.Н. – Издательство: Москва. – 2007, с. 216.
18. Семенов, А.Б. Проектирование и расчет структурированных кабельных систем и их компонентов / Семенов А.Б. – Компания АйТи, 2010 г. – 416+16 с.
19. Томас, О. Администрирование Windows Server 2008 / Томас О. Русская редакция, 2011г., 688 с.
20. "Проектирование и администрирование сетей на базе TCP/IP" авторов Д. Комарова, А. Матюшкина и Д. Портнова, 64 с.
21. "Локальные вычислительные сети. Проектирование, установка и настройка" автора В. Кравчука, 14 с.
22. "Сети своими руками. Создание небольших локальных сетей" автора С. Сидоренко, 124 с.
23. "Проектирование и развертывание корпоративных сетей" авторов С. Кузнецова, И. Расторгуева и А. Бережкова, 108 с.
24. "Сети ЭВМ и телекоммуникации" авторов В. Левицкого, А. Калинченко и А. Макарова, 74 с.
25. "Проектирование вычислительных сетей. Учебное пособие" авторов В. Королева и А. Гриценко, 58 с.