Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный университет телекоммуникаций и информатики» (СибГУТИ)

Колледж телекоммуникаций и информатики

Допустить к защите

Председатель ЦК

«Безопасности и управления в телекоммуникациях» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/Н.С.Матвеева/

«\_\_» \_\_\_\_\_\_\_\_\_\_\_20\_\_ г.

**Дипломная работа**

Проектирование и настройка беспроводной сети

для ОАО «Завод Электросигнал»

Студент:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/Е.Ю. Бухгольц/

Группа: СА-12

Специальность: 09.02.06 Сетевое и системное администрирование

Руководитель: \_\_\_\_\_\_\_\_\_\_/С.Н. Огольцов/

Новосибирск 2025

**СОДЕРЖАНИЕ**

[ВВЕДЕНИЕ 3](#_Toc200456117)

[1 Исследование объекта проектирования беспроводной сети 5](#_Toc200456118)

[2 Проект беспроводной сети 8](#_Toc200456119)

[2.1 Планирование беспроводной сети 8](#_Toc200456120)

[2.2 Рекомендации к подбору оборудования 16](#_Toc200456121)

[3 Администрирование проекта беспроводной сети предприятия 20](#_Toc200456122)

[3.1 Расчет IP-адресации 20](#_Toc200456123)

[3.2 Построение беспроводной сети 22](#_Toc200456124)

[4. Техника безопасности 36](#_Toc200456125)

[ЗАКЛЮЧЕНИЕ 41](#_Toc200456126)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 42](#_Toc200456127)

[ПРИЛОЖЕНИЕ А 44](#_Toc200456128)

# ВВЕДЕНИЕ

Современное общество невозможно представить без информационных технологий, которые проникают во все сферы жизни. Одним из ключевых элементов этой технологической революции стали беспроводные сети, обеспечивающие мобильность и доступ к информации в любое время и в любом месте.

Целью дипломной работы является разработка беспроводной сети для второго корпуса ОАО «Завод Электросигнал», расположенной по адресу г. Новосибирск, ул. Гурьевская, д. 38.

Для достижения цели необходимо выполнить следующие задачи:

* Рассмотреть объект проектирования беспроводной сети, выявить потребности для будущей сети;
* Провести анализ и выбрать стандарты, используемые для проектирования сети.
* Спроектировать сеть.
* Смоделировать сеть в среде Cisco Packet Tracer;
* Рассмотреть вопросы техники безопасности;

Объектом исследования выпускной квалификационной работы является предприятие.

Предметом исследования является разработка проекта беспроводной сети предприятия.

Дипломная работа состоит из следующих структурных элементов:

* титульный лист;
* задание на ВКР;
* рецензия;
* отзыв;
* содержание;
* введение;
* основная часть;
* заключение;
* список использованных источников;
* приложение.

Введение раскрывает актуальность, определяет цель, задачи, объект, предмет и структуру исследования.

В первой главе описывается краткая характеристика объекта проектирования, анализируется текущий метод реализации сети, его недостатки и поиски решения.

Во второй главе выполняется разработка проекта беспроводной сети. Определяется порядок проектирования беспроводной сети, отображение плана сети, расчет покрытия сигнала. Описаны рекомендации по оборудованию для реализации беспроводной сети.

В третьей главе выполняется администрирование проекта беспроводной с применением протокола TCP/IP. В данной главе рассчитываются IP- адреса, сеть разделяется на подсети, разрабатывается схема беспроводной сети в симуляторе Cisco Packet Tracer.

В четвёртой главе курсовой работы изучены вопросы о технике безопасности.

В заключении подводятся итоги выпускной квалификационной работы, формируется вывод по цели и задачам.

Источники литературы, использованные при работе, являются актуальными.

Приложение содержит в себе электронные версии ВКР, презентации, сопровождающих документов, схемы Visio и проект Cisco Packet Tracer.

# 1 Исследование объекта проектирования беспроводной сети

Электросигнал - новосибирский завод, осуществляющий разработку и производство различной радиоэлектронной продукции для ряда промышленных отраслей, а также для военных организаций и силовых структур, такие как радиоаппаратура для авиации, для железной дороги и метрополитена, для силовых структур, для промышленности Радиоаппаратура для ВМФ. Помимо производства радиоэлектронной аппаратуры, предприятие задействовано в некоторых других отраслях и выпускает средства вычислительной техники (серверы и компьютеры), инструментальные изделия и т. д .

Предприятие принадлежит корпорации «Новосибирский завод Электросигнал» [15]. Расположен в [Октябрьском районе](https://ru.wikipedia.org/wiki/%D0%9E%D0%BA%D1%82%D1%8F%D0%B1%D1%80%D1%8C%D1%81%D0%BA%D0%B8%D0%B9_%D1%80%D0%B0%D0%B9%D0%BE%D0%BD_(%D0%9D%D0%BE%D0%B2%D0%BE%D1%81%D0%B8%D0%B1%D0%B8%D1%80%D1%81%D0%BA)) города Новосибирск (рисунок 1.1). Электросигнал стоит из множества корпусов, чье количество достигает четырнадцати.

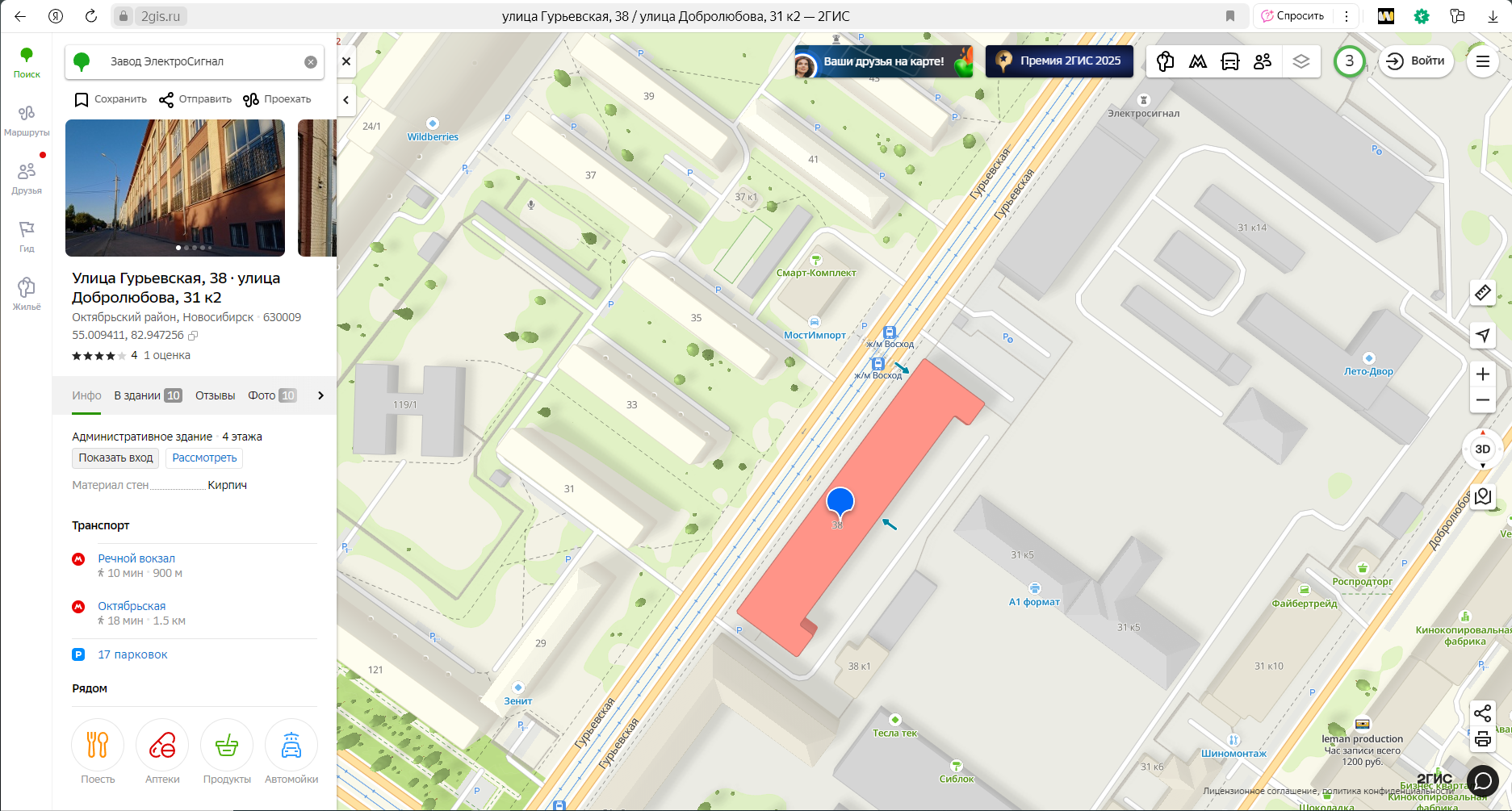


Рисунок 1.1 – Местоположение 2 корпуса завода «Электросигнал»

Источник: Взято с сайта 2gis.ru

Однако в корпусах предприятия также работают другие организации, например, такие как фотостудия, ателье. На время прохождения практики был предоставлен доступ ко второму корпусу.

На данный момент на предприятии развернута проводная сеть, однако во многих отделах существует проблема с организацией кабеля (рисунок 1.2).



Рисунок 1.2 – Прокладка кабеля до рабочего места

Источник: Собственная фотография

Подобное решение не соответствует требованиям к безопасности организации сети, о чем может свидетельствовать рисунок. Подобная «прокладка» кабеля зачастую становится проблемой для новых рабочих мест, а поскольку таких достаточно, то проблема серьезного масштаба и вынуждает найти решение.

Проводная сеть действительно может вызывать множество неудобств: от ограниченной мобильности сотрудников до сложности в установке и обслуживании. В связи с этим, одним из наиболее перспективных решений является переход на беспроводную сеть.

Беспроводные сети предлагают ряд значительных преимуществ. Во-первых, они обеспечивают мобильность, позволяя сотрудникам перемещаться по офису без необходимости быть привязанными к проводам. Это создает более динамичную и продуктивную рабочую среду. Во-вторых, установка беспроводной сети значительно проще и быстрее, что позволяет сократить затраты на оборудование и время на развертывание.

Кроме того, беспроводные сети обеспечивают большую гибкость: добавление новых устройств в сеть осуществляется легко и без лишних хлопот. Эстетически такая сеть выглядит более привлекательно, так как отсутствие проводов делает пространство более аккуратным и организованным. И, наконец, беспроводные сети предоставляют доступ к интернету в местах, где прокладка кабелей невозможна или затруднительна. Поэтому переход на беспроводную сеть может стать отличным решением для нашего предприятия [6].

Проект беспроводной локальной сети будет выполнен непосредственно для второго корпуса. Он построен из кирпича, имеет довольно толстые стены, что необходимо учитывать в будущем В основном здесь находятся офисы, внутри которых планировка выполнена планировка раздела помещения при помощи гипсокартона. Рабочих мест в корпусе более 150, поэтому рассчитываем сеть на количество 200 устройств.

Также необходимо определить требования к беспроводной сети, поэтому стоит рассмотреть, что находится на каждом этаже и выделить зоны:

Первый этаж полностью сдается под аренду, он не связан с информационными ресурсами ОАО «Электросигнал», однако по договору наличие сети обеспечивает предприятие, поэтому на этот этаж будет создана отдельная сеть Wi-Fi, которая не будет иметь возможности подключиться к серверам завода.

Рабочие места на втором, третьем и четвертом этажах уже имеют непосредственное отношение к предприятию и должны быть в сети завода.

Таким образом, была изучена характеристика предприятия.

# 2 Проект беспроводной сети

# 2.1 Планирование беспроводной сети

Беспроводная Wi-Fi серии стандартов IEEE 80211 сеть состоит из одной или нескольких точек доступа и не менее одного клиента. Точка доступа передает свой идентификатор сети (SSID) с помощью сигнальных пакетов, которые передаются каждый 100мс на скорости 0,1 Мбит/с. Соответственно наименьшая скорость беспроводной сети Wi-Fi 0,1 Мбит/с. Для подключения к беспроводной сети клиенту необходимо знать SSID нужной ему сети. При попаданий приемника в зону действия двух точек доступа с одинаковыми SSID приемник выбирает между точками доступа основываясь на уровне сигнала. Одно из преимуществ технологи Wi-Fi заключается в том, что клиенту дается полная свобода выбора критериев соединения и роуминга [11].

По способу объединения точек доступа в единую систему различают следующие варианты:

- автономные точки доступа (называются также самостоятельные, децентрализованные, умные);

- точки доступа, работающие под управлением контроллера (называются также «легковесные», централизованные);

- бесконтроллерные, но не автономные (управляемые без контроллера).

По способу организации и управления радиоканалами можно выделить беспроводные локальные сети следующих типов:

- со статическими настройками радиоканалов;

- с динамическими (адаптивными) настройками радиоканалов;

- со «слоистой» или многослойной структурой радиоканалов;

В зависимости от зоны покрытия беспроводные сети делятся на три вида

- WLAN (Wireless Local Area Network) – в основном используется для домашних Wi-Fi сетей;

- WPAN (Wireless Personal Area Network) – используется для персональных беспроводных сетей. Использует стандарт 802.15;

- WWAN (Wireless Wide Area Network) – беспроводные сети городского масштаба [12].

С развитием технологий беспроводной связи стандарты Wi-Fi претерпели значительные изменения, обеспечивая пользователей все более высокими скоростями передачи данных и улучшенной производительностью. Рассмотрим основные стандарты Wi-Fi, их преимущества и недостатки, актуальность и сферы применения, основные характеристики стандартов представлены в таблице 2.1 [17].

Таблица 2.1

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Стандарт Wi-FI | Наименование | Максимальная скорость передачи данных | Рабочие частоты | Максимальный диапазон работы |
| 802.11n | Wi-Fi 4 | 600 Мбит/с | 2.4 ГГц и 5 ГГц | 250 м |
| 802.11ac | Wi-Fi 5 | 3.5 Гбит/с | 5 ГГц | 100 м |
| 802.11ax | Wi-Fi 6 | 9.6 Гбит/с | 2.4 ГГц и 5 ГГц | 200 м |
| 802.11be | Wi-Fi 7 | 30 Гбит/с | 2.4 ГГц, 5 ГГц и 6 ГГц | => 200 м |

Стандарт 802.11n, также известный как Wi-Fi 4, поддерживает максимальную скорость передачи данных до 600 Мбит/с и работает на частотах 2.4 GHz и 5 GHz. Он использует технологию MIMO (Multiple Input Multiple Output), что позволяет увеличить пропускную способность за счет одновременной передачи данных через несколько антенн. Однако его скорость передачи ограничена по сравнению с более современными стандартами, что может быть недостатком для пользователей с высокими требованиями. Тем не менее, 802.11n все еще используется в некоторых устройствах, особенно в офисах и домашних условиях, где не требуется высокая скорость передачи данных.

Стандарт 802.11ac, или Wi-Fi 5, значительно увеличивает скорость передачи данных до 3.5 Гбит/с и работает исключительно на частоте 5 GHz. Он поддерживает MU-MIMO (Multi-User MIMO), что позволяет одновременно передавать данные нескольким устройствам, тем самым повышая общую производительность сети. Однако ограниченная поддержка только на частоте 5 GHz может уменьшить диапазон действия в помещениях с препятствиями. Несмотря на это, 802.11ac остается актуальным для большинства домашних и коммерческих сетей благодаря своей высокой скорости и эффективности.

Стандарт 802.11ax, известный как Wi-Fi 6, предлагает максимальную скорость передачи до 9.6 Гбит/с и работает на частотах 2.4 GHz и 5 GHz. Он значительно улучшает эффективность в условиях высокой плотности пользователей благодаря технологии OFDMA (Orthogonal Frequency Division Multiple Access), что позволяет более эффективно использовать доступные каналы. Поддержка MU-MIMO для большего количества пользователей одновременно улучшает производительность в многопользовательских сценариях, а функция энергосбережения для подключенных устройств (Target Wake Time) способствует более длительной работе мобильных устройств. Wi-Fi 6 активно внедряется и становится стандартом для новых устройств и сетей, отвечая требованиям современных пользователей.

Наконец, стандарт 802.11be, или Wi-Fi 7, ожидается как следующий шаг в эволюции беспроводных технологий с максимальной теоретической скоростью передачи до 30 Гбит/с. Он будет поддерживать более широкие каналы (до 320 МГц) и совершенствование технологий MU-MIMO и OFDMA, что значительно увеличит пропускную способность сети. Ожидается, что Wi-Fi 7 улучшит работу в условиях высокой плотности пользователей, что будет особенно актуально для современных приложений. Однако спецификация еще не завершена, и для полноценного использования потребуются новые устройства [20].

Основываясь на вышесказанной информации, можно выделить стандарт 802.11ax, поскольку он удовлетворяет требования к разрабатываемому проекту беспроводной сети. Стандарт является актуальным решением для многопользовательских сетей и уже активно вводится в реальные решения, а также поддерживает работу на частоте 2.4, что обеспечивает более широкий радиус действия сигнала.

Для дальнейшего проектирования беспроводной сети следует сначала поработать с планом предприятия, поэтому сначала нужно его создать. Для этого будет использована программа Visio.

Microsoft Visio – это уникальное приложение, которое позволяет оперативно и с минимальными усилиями сделать сложную схему, диаграмму или таблицу. Дополнительно оно включает инструменты для создания блок-схем, планов зданий, схем технических процессов, трехмерных карт или моделей бизнес-процессов. Поскольку программа создана Microsoft, то она является дополнением Office [13].

И так при помощи стандартного набора элементов был спроектирован план ОАО «Элестросигнал», отображенный на рисунке 2.1.

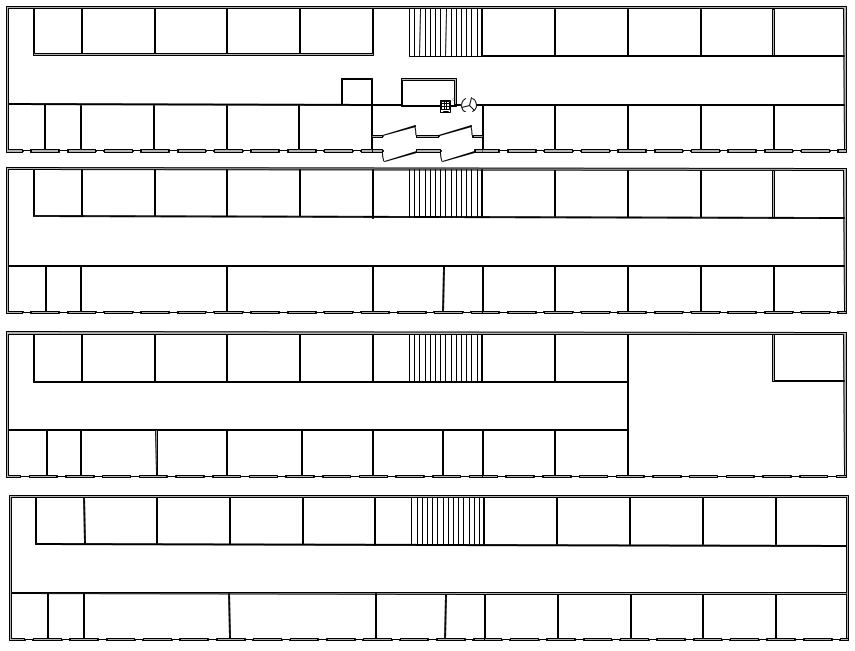


Рисунок 2.1 – План 2 корпуса ОАО «Электросигнал»

Источник: собственная разработка

Следующим этапом необходимо расположить точки доступа. Выше уже был выбран стандарт 802.11ax, следовательно, работать нужно будет по нему. Размеры предприятия примерно составляют 240 метров в длину и 40 метров в ширину [16].

Используя данные из таблицы можно было бы предположить, что будет достаточно одной точки доступа, однако максимальный диапазон работы возможен лишь при идеальных условиях, например – распространение сигнала на открытой местности, на предприятии же таких очевидно не добиться. Также нельзя забывать, что сеть являются многопользовательской, из-за чего мощности одной точки доступа будет не хватать.

Таким образом необходимо провести расчет, при каком расстоянии сохранится эффективность распространения сигнала, учитывая препятствия в виде кирпичной стены и гипсокартона. Расчеты проводились вручную, ход представлен на рисунке 2.2

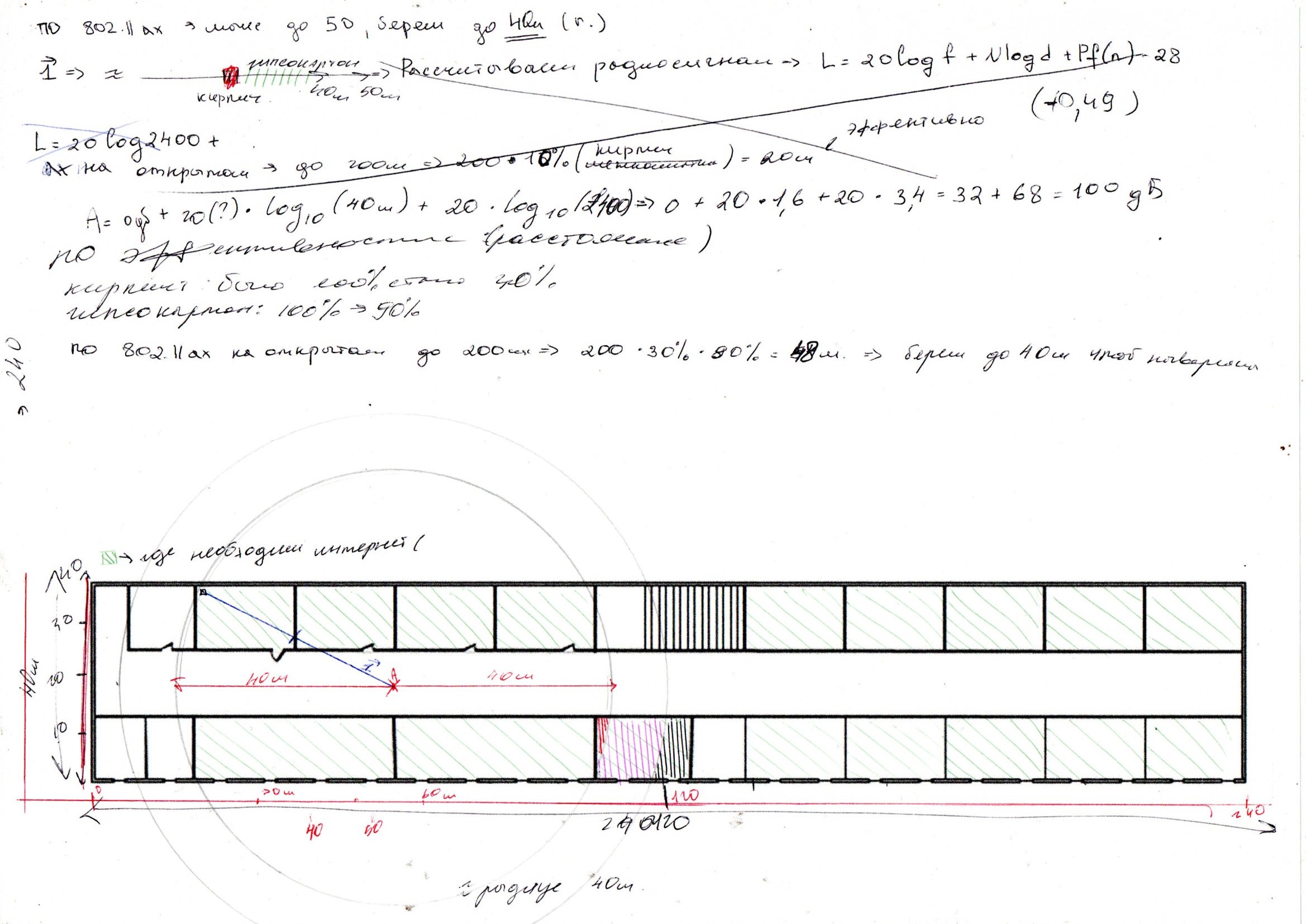


Рисунок 2.2 – Расчет эффективности сигнала с учётом препятствий

Источник: собственная разработка

Данный расчет основывается на средних значениях эффективного расстояния через прохождение препятствия.

Эффективное расстояние - означает насколько уменьшится радиус действия сигнала Wi-Fi после прохождения соответствующего препятствия по сравнению с открытым пространством.

Для расчета используем следующую формулу [9].

H = Smax × P; (1)

где H – эффективное расстояние, м;

Smax – максимальный диапазон сигнала, м;

P – процент прохождения сигнала через препятствие, %.

В случае данного расчета, точка доступа установлена в коридоре. Это означает, что для прохождения сигнала от точки доступа то конечного устройства потребуется пройти через кирпичную и гипсокартонную стены. В среднем, значения P составляет 30% и 80% соответственно. Проводим расчет при помощи формулы 1:

H = 200 × 30% × 80% = 48 м

Для надежности принято решение округлить до десятка в меньшую сторону, таким образом получен радиус эффективного прохождения сигнала, а, следовательно, качественной работы в 40 м.

Исходя из выше рассчитанного значения размещаем точки доступа на предприятии, по этажам. На схемах их местоположение обозначается красным крестом, а также выделен радиус сигнала.

На первом этаже располагаются офисы, поэтому необходимо обеспечить равномерное покрытие, исходя из этого точки доступа будут расположены по всему этажу в количестве четырех (рисунок 2.3)

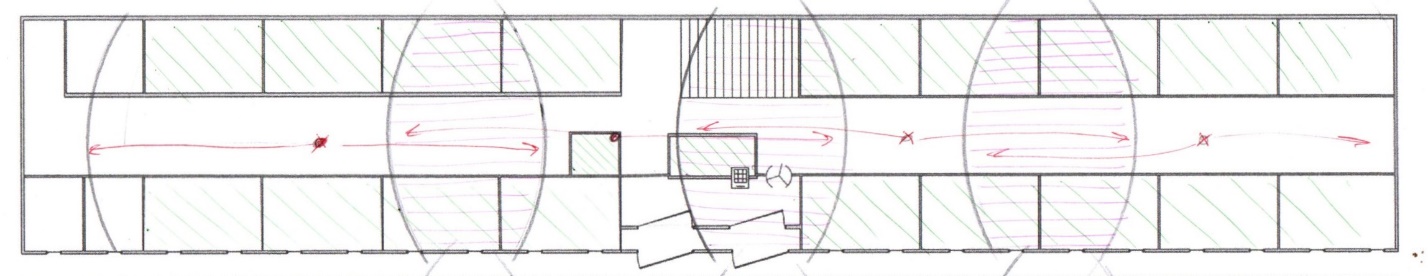


Рисунок 2.3 – Расположение точек доступа на 1-ом этаже

Источник: собственная разработка

Следующим действием нужно расположить точки доступа на втором этаже. Требования аналогичны с первым этажем, поэтому размещение точек такое же (рисунок 2.4).

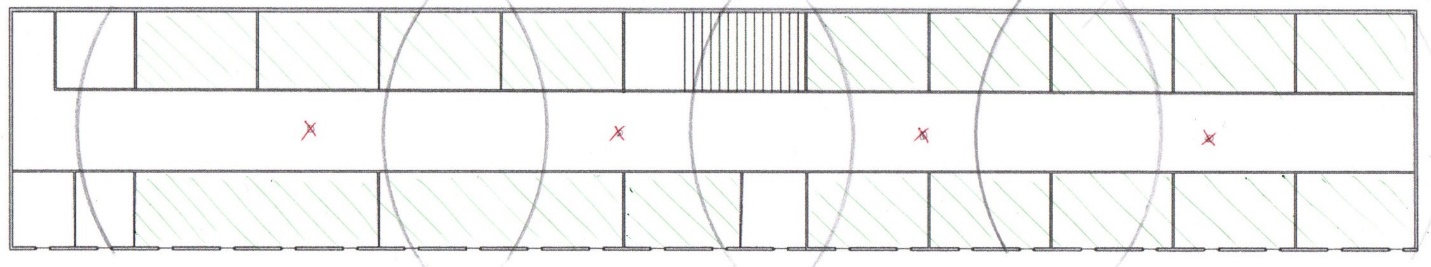


Рисунок 2.4 – Расположение точек доступа на 2-ом этаже

Источник: собственная разработка

На третьем этаже находится столовая, для которой наличие рабочего Wi-Fi не имеет необходимости, поэтому расчет осуществляется лишь на часть этажа и количество точек доступа сокращается до трёх (рисунок 2.5).



Рисунок 2.5 - Расположение точек доступа на 3-ем этаже

Источник: собственная разработка

На четвертом этаже есть помещение занимающее весомую территорию, однако его расположение не позволяет изолировать его из покрытия сигнала, поэтому расположение точек доступа аналогично с первым и вторым этажами (рисунок 2.6).

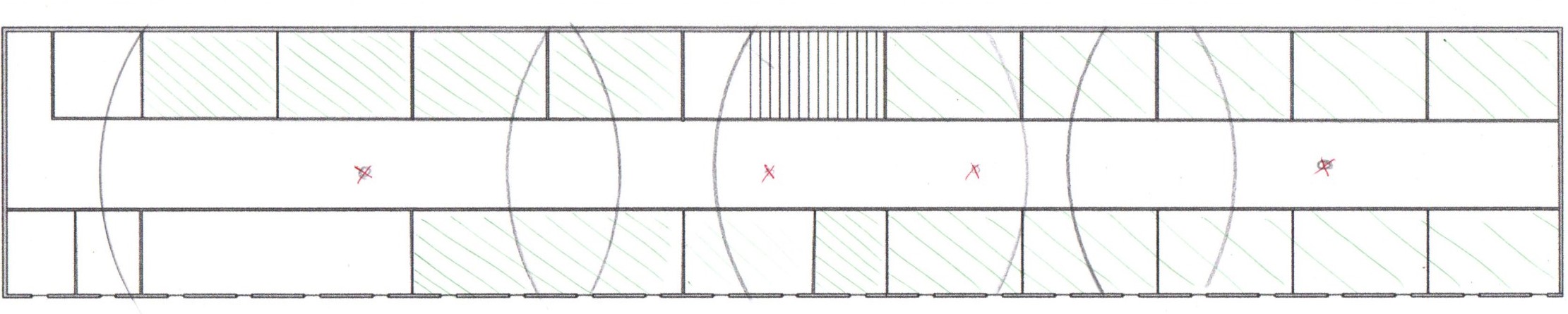


Рисунок 2.6 - Расположение точек доступа на 4-ом этаже

Источник: собственная разработка

Таким образом для осуществления работы беспроводной сети понадобится 15 точек доступа.

Однако, как можно заметить по рисункам, существуют зоны пересечения, более демонстративно они отображены на изображении первого этажа прямыми параллельными фиолетового цвета. Из этого вытекает следующие проблемы: к какой точке доступа подключаться пользователю в этой сети? В целом, в обычном представлении, точка доступа равняется одной сети Wi-Fi, но такое решение является неудобным, следовательно, нужно найти другое. Таким является технология Mesh Wi-Fi.

Mesh Wi-Fi — это система беспроводной сети, состоящая из нескольких узлов (маршрутизаторов и точек доступа), которые работают вместе, создавая единую сеть с одним SSID и паролем. В отличие от традиционных роутеров, где сигнал распространяется только от одного устройства, Mesh-система использует несколько точек доступа, взаимодействующих между собой для обеспечения стабильного и быстрого интернет-соединения на любой площади дома [14].

Схема адресации осуществляется системным администратором.  В данной локальной системе будет использоваться статистическая маршрутизация.

Настройка сети, установка ПО и последующая откладка осуществляется непосредственно самим системным администратором.

В заключительном этапе системный администратор должен будет обучить пользователей основам компьютерной грамотности.

# 2.2 Рекомендации к подбору оборудования

Требования к оборудованию беспроводной сети на основе стандарта 802.11ax, также известного как Wi-Fi 6, включают несколько ключевых аспектов, обеспечивающих высокую производительность и стабильность соединения. Во-первых, точки доступа должны полностью поддерживать стандарт 802.11ax для эффективного использования спектра частот и улучшения работы в условиях высокой плотности пользователей. Оборудование должно функционировать в диапазоне 2.4 ГГц, что обеспечивает большую дальность действия и лучшее проникновение сигнала через преграды, а также требует оптимизации для снижения помех от других беспроводных устройств.

Для достижения целевой пропускной способности интернета около 10 Гбит/с точки доступа должны поддерживать технологии MU-MIMO (Multi-User Multiple Input Multiple Output) и OFDMA (Orthogonal Frequency Division Multiple Access), позволяющие одновременно обслуживать несколько клиентов и увеличивать общую эффективность сети. Учитывая расчет на 14 пользователей на одну точку доступа, оборудование должно иметь достаточный объем оперативной памяти и процессорной мощности для обработки одновременных запросов. Также необходимо обеспечить высокие скорости передачи данных, соответствующие требованиям стандарта 802.11ax, включая использование технологий 1024-QAM (Quadrature Amplitude Modulation) для увеличения скорости передачи информации [3].

Внедрение механизмов качества обслуживания (QoS) позволит приоритизировать трафик и обеспечивать надежную работу приложений в реальном времени, таких как видеоконференции и VoIP. Дополнительно, оборудование должно поддерживать технологию Mesh Wi-Fi, что позволит создавать бесшовные сети с несколькими точками доступа, обеспечивающими стабильное покрытие на больших площадях и в сложных условиях. Mesh-системы автоматически оптимизируют маршрутизацию данных между узлами, что повышает надежность соединения и минимизирует мертвые зоны.

Кроме того, оборудование должно поддерживать современные протоколы безопасности, такие как WPA3, для защиты данных пользователей и предотвращения несанкционированного доступа к сети. Рекомендуется также использование централизованных систем управления точками доступа для эффективного мониторинга состояния сети, управления ресурсами и диагностики в случае возникновения проблем. Соблюдение этих требований позволит создать надежную и высокопроизводительную беспроводную сеть, способную удовлетворить потребности современных пользователей.

Поскольку беспроводные технологии внедряются в существующие сеть нужно позаботиться об успешном подключении оконечных устройств к точкам доступа, при условии, что эти устройства старые и не поддерживают беспроводное подключение. Для этого рекомендуется приобрести Wi-Fi адаптер, например как Wi-Fi адаптер Tenda W311MI (рисунок 2.7) [19].

Как можно увидеть на рисунке, такой адаптер соответствует характеристикам проектируемой сети и является подходящим решением.

Для установки точек доступа Wi-Fi под потолок необходимо приобрести специальные крепления, которые обеспечат надежное и удобное размещение оборудования. Такие крепления помогают оптимизировать покрытие сети, минимизируя помехи и обеспечивая стабильное соединение.

Примеры креплений для точек доступа:

* крепление для потолка с крепежом - позволяет установить точку доступа на потолок с использованием стандартных крепежных элементов;
* крепление с поворотным механизмом - дает возможность; регулировать угол наклона точки доступа для достижения оптимального покрытия;
* крепление с защитной оболочкой - защищает оборудование от внешних факторов, что особенно важно в общественных местах.

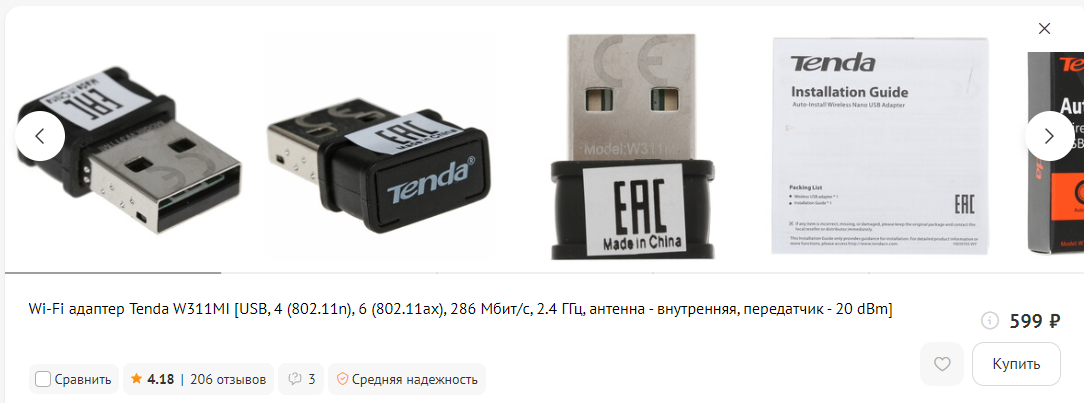


Рисунок 2.1 – Wi-Fi адаптер

Источник: взято с сайта www.dns-shop.ru

Конкретных примеров приведено не будет, так как покупку крепления следует оформлять после покупки сетевого оборудования и выбирать его в соответствии с ним, учитывая требования этого оборудования к монтажу.

Таким образом, в данной главе был расписан порядок проектирования беспроводной сети: определено на каком стандарте будет работать сеть, какая эффективная зона действия сигнала в условиях предприятия ОАО «Завод Электросигнал», размещены на плане предприятия и подсчитаны точки доступа Wi-Fi, приведены рекомендации к сетевому беспроводному и дополнительному оборудованию. На этом проектирование предварительное проектирование сети можно считать законченным.

# 3 Администрирование проекта беспроводной сети предприятия

# 3.1 Расчет IP-адресации

IP-aдpeca (IP address) представляют собой основной тип адресов, на основании которых сетевой уровень передает сообщения, называемые IP-пакетами. Маршрутизатор по определению входит сразу в несколько сетей. Поэтому каждый порт маршрутизатора имеет собственный IP-адрес. Конечный узел также может входить в несколько ІР-сетей. В этом случае компьютер должен иметь несколько IP-адресов - по числу сетевых адаптеров. Таким образом, IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение.

Так как проектируемая беспроводная сеть обладает подсетями, необходимо рассчитать эти подсети. Это применяется для повышения пропускной способности: логические адреса способны более эффективно решать задачи маршрутизации [2].

Рассчитать подсети можно как вручную, так и при помощи внешних средств. В данном проекты расчеты выполнены при помощи сайта ipmeter.ru [18]. Результат сайт выдает в виде таблицы (рисунок 3.1).

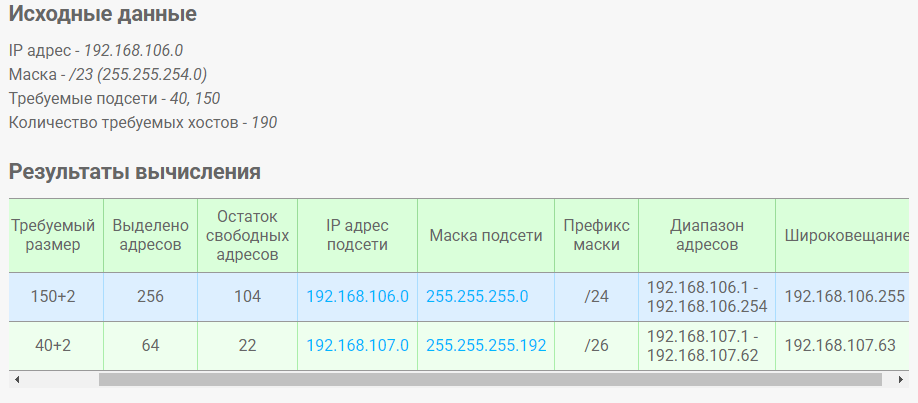


Рисунок 3.1 – Расчет адресов

Источник: скриншот с сайта ipmeter.ru

Для сети офисов на первом этаже берем отдельную сеть 192.168.166.0 с маской 24 (255.255.255.0).

Теперь необходимо схематично отобразить будущую сеть при помощи раннее используемой программы Microsoft Visio (рисунок 3.2).

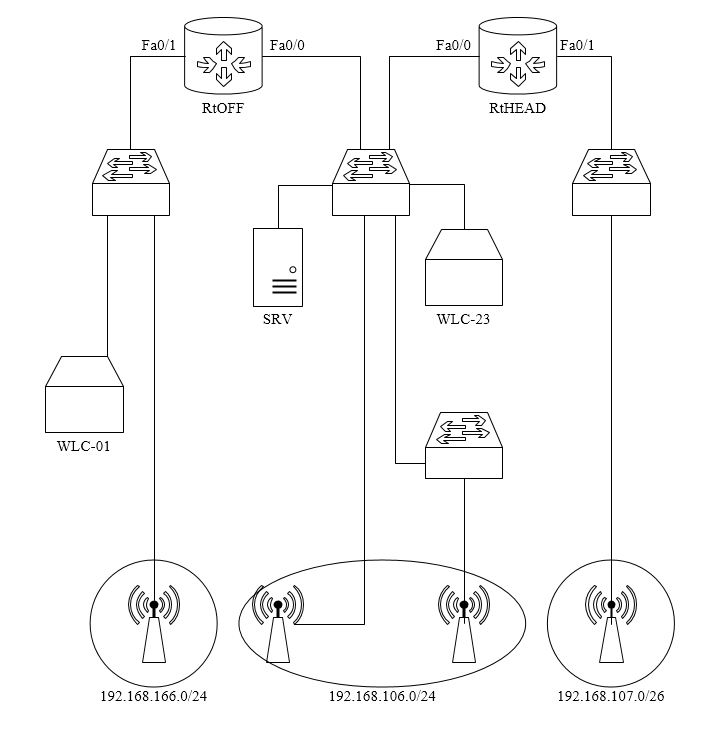


Рисунок 3.2 – Схема сети

Источник: собственная разработка на основе исходных данных

Также для дальнейшего удобства нужно поместить основную информацию в таблицу 3.1 с сетевым оборудованием.

Таблица 3.1 – IP-адресация

|  |  |  |  |
| --- | --- | --- | --- |
| Имя устройства | Интерфейс | Адрес/Маска | Шлюз |
| SRV | Fa0/0 | 192.168.106.250 |  |
| WLC-01 | Management | 192.168.166.253 | 192.168.166.254 |
| WLC-23 | Management | 192.168.106.254/24 | 192.168.106.250 |
| RtOFF | Fa0/0 | 192.168.106.25/24 |  |
| Fa0/1 | 192.168.166.254/24 |  |
| RtHEAD | Fa0/0 | 192.168.106.251/24 |  |
| Fa0/1 | 192.168.107.62/25 |  |

Теперь, когда предварительная работа выполнена и зафиксирована в удобном формате, можно приступить к построению сети.

# 3.2 Построение беспроводной сети

Packet Tracer – отличная замена для всех, кто нуждается в нескольких реальных устройствах: вы можете разработать сложную топологию из десятков (если не сотен) устройств Cisco и следить как за тем, как пакеты передвигаются между ними. И все это возможно в пределах вашего ноутбука вне зависимости от вашего местонахождения [4].

Первым делом необходимо создать схему. Планировать ее было решено в виде этажей, соблюдая реальное место нахождения сервера и т.д. для наглядности. С таким подходом была разработана схема, отображающая предыдущую, но уже в эмуляторе (рисунок 3.3).

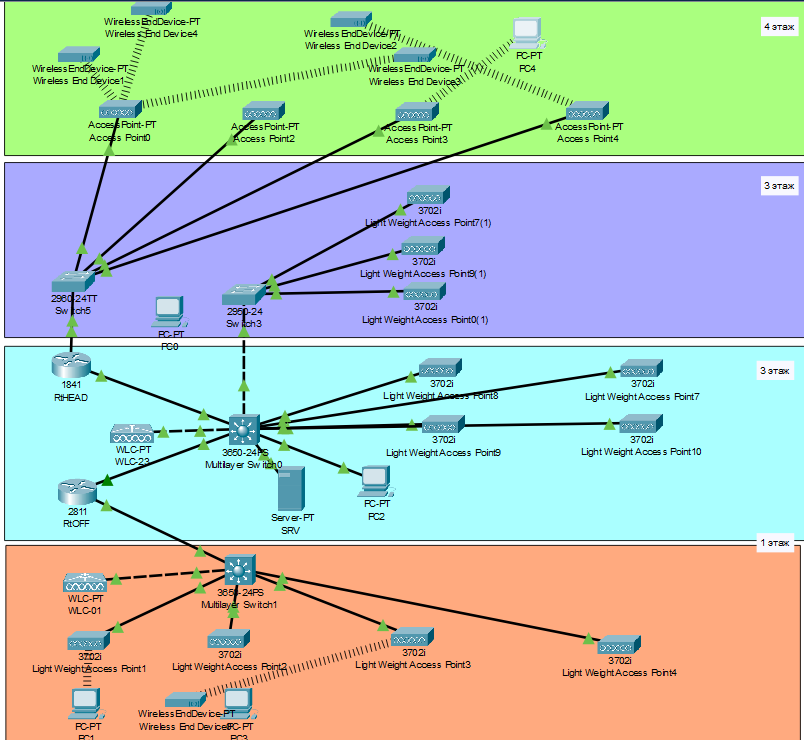


Рисунок 3.3 – Схема локальной сети в Cisco Packet Tracer

Источник: собственная разработка на основе исходных данных

В данной схеме присутствуют три вида устройств, организующих беспроводную связь:

1. Light Weight Access Point (LWAP) — это тип беспроводной точки доступа, который работает в связке с контроллером беспроводной локальной сети (WLC). LWAP не имеет полной функциональности маршрутизатора и вместо этого полагается на WLC для управления и настройки. Он обеспечивает:

* Централизованное управление настройками и политиками безопасности.
* Поддержку масштабируемости, позволяя легко добавлять новые точки доступа в сеть.
* Упрощение управления сетью благодаря автоматическому обнаружению WLC.

1. Wireless LAN Controller (WLC) — это устройство, которое управляет несколькими LWAP в беспроводной сети. WLC выполняет следующие функции:
   * Централизованное управление точками доступа, включая настройки, обновления прошивки и мониторинг производительности.
   * Поддержка различных функций безопасности, таких как аутентификация пользователей и шифрование трафика.
   * Оптимизация радиочастотного спектра и управление нагрузкой для обеспечения стабильного соединения.
   * Упрощение развертывания и администрирования беспроводной сети
2. Access Point PT (или просто точка доступа) — это устройство, которое предоставляет беспроводное соединение для клиентов (например, ноутбуков, смартфонов и других устройств). В отличие от LWAP, обычные точки доступа могут работать независимо и не требуют контроллера для функционирования. Они обеспечивают:
   * Подключение пользователей к проводной сети через беспроводные технологии.
   * Возможность работы в различных режимах (например, точка-точка или точка-многоточка).
   * Простоту установки и настройки, что делает их популярными для малых и средних сетей.

Эти устройства работают вместе для создания надежной и масштабируемой беспроводной сети, обеспечивая пользователей стабильным доступом к ресурсам сети.

Для работы Wi-Fi на этажах с первого по третий будет использоваться связка в виде WLC и LWAP, на четвертом этаже будут использоваться самостоятельны точки доступа.

Однако для начала нужно совершить базовую конфигурацию и настроить IP-адресацию, делаем это при помощи DHCP-службы на сервере второго этажа (рисунки 3.3 - 3.4).



Рисунок 3.4 - Назначение адреса на сервере

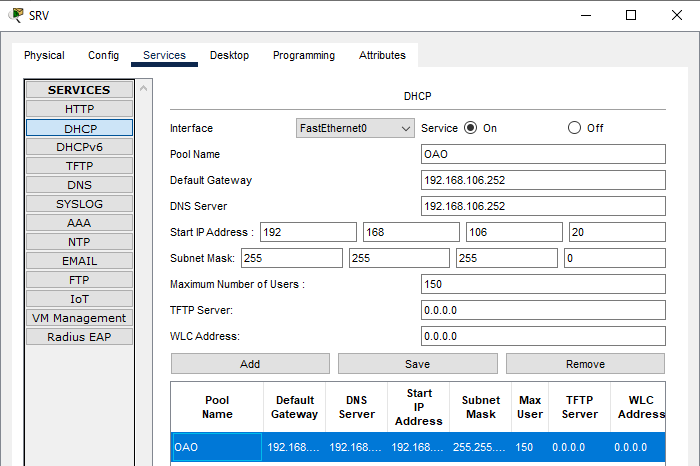


Рисунок 3.5 – Создание пула адресов DHCP

Таким простым способом настраиваем DHCP, согласно таблице 3.1, эта сеть будет распространяться на точки доступа Wi-FI и оконечные устройства в пределах второго, третьего этажей.

Для проверки работы службы берем компьютер из указанной области действия и переключаем способ получения адреса (рисунок 3.6).



Рисунок 3.6 – Проверка работы DHCP на сервере

Как можно заметить он получил свой адрес из того пула, который был указан раннее.

Далее нужно организовать адресацию для других сетей, для них уже будут использоваться роутеры RtOFF и RtHEAD соотвественно.

В начале настраиваем RtOFF, связан он между основной сетью и сетью первого этажа. Сначала нужно назначить адреса из сетей на соответствующие интерфейсы согласно созданной ранее таблице адресации (рисунок 3.7).

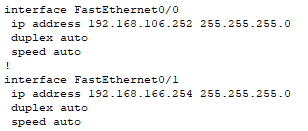


Рисунок 3.7 – Назначение адресов на RtOFF

Затем необходимо поднять службу DHCP (рисунок 3.8)

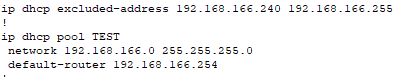


Рисунок 3.8 – Настройка DHCP на RtOFF

Также в настройке службы были указаны адреса, которые исключатся из пула адресов, раздаваемых службой. Этот диапазон будет занят выше ранговым оборудованием, находящийся на статике.

Далее нужно настроить маршрутизацию, для этой цели был выбран протокол OSPF.

OSPF (Open Shortest Path First) — это протокол маршрутизации с состоянием канала, который используется для передачи данных в IP-сетях. Он обеспечивает быструю конвергенцию и поддерживает иерархическую структуру через области (areas), что упрощает управление в крупных сетях. OSPF использует алгоритм Дейкстры для вычисления кратчайших путей и способен работать с различными типами сетевых подключений. Протокол также поддерживает аутентификацию для повышения безопасности. OSPF является масштабируемым и эффективным решением для корпоративных и провайдерских сетей [5].

Для его настройки необходимо на роутере ввести следующие настройки (рисунок 3.9):



Рисунок 3.9 – Настройка OSPF на RtOFF

Теперь необходимо проверить связь между этими двумя сетями, для этого отправляем пакет из оконечных устройств данных сетей (рисунок 3.10).

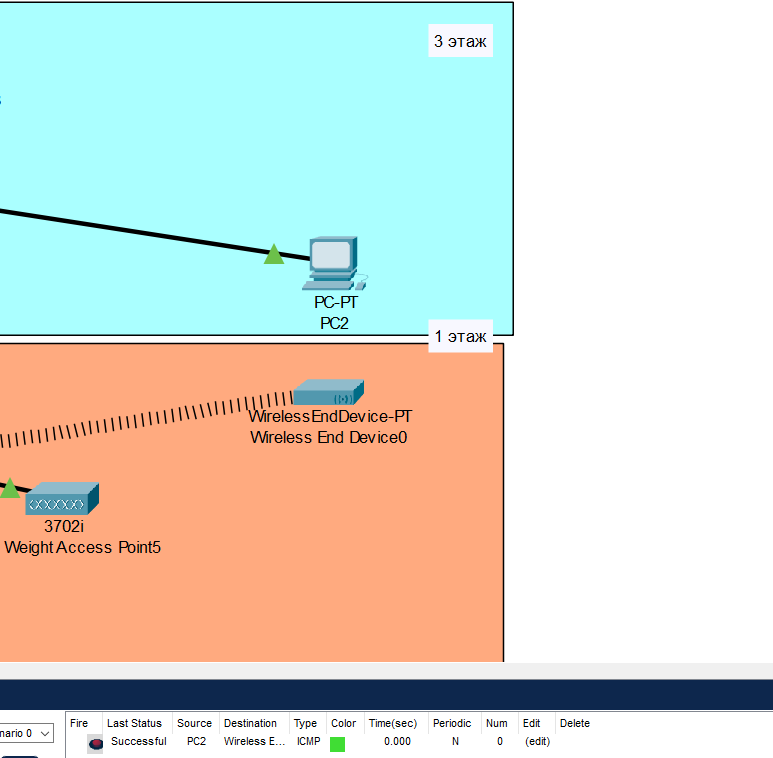


Рисунок 3.10 – Проверка связности между подсетями

Как можно заметить связь успешно настроена. Теперь такие же настройки выполняем на роутере RtHEAD (рисунки 3.11 – 3.13)

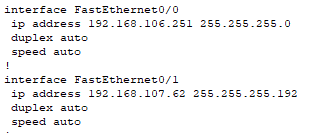


Рисунок 3.11 – Назначение адресов на RtHEAD

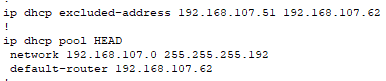


Рисунок 3.12 – Настройка DHCP на RtHEAD

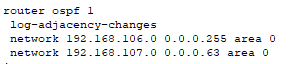


Рисунок 3.13 – Настройка OSPF на RtHEAD

Теперь следует приступить к настройке самого оборудования беспроводной сети. Однако сначала нудно выбрать какой метод аутентификации будет использоваться для подключения.

WPA, WEP и WPA2 — это протоколы шифрования, предназначенные для защиты беспроводных сетей. Каждый из них имеет свои особенности, преимущества и недостатки.

WEP (Wired Equivalent Privacy) был одним из первых протоколов безопасности, введенных в 1997 году. Его основная цель заключалась в том, чтобы обеспечить уровень безопасности, сопоставимый с проводными сетями. Однако WEP использует статический ключ шифрования, что делает его уязвимым для атак. На сегодняшний день этот протокол считается небезопасным и не рекомендуется к использованию из-за уязвимостей в алгоритме RC4 и коротких ключей, которые позволяют злоумышленникам легко перехватывать и расшифровывать трафик.

В ответ на недостатки WEP был разработан WPA (Wi-Fi Protected Access), который появился в 2003 году. WPA значительно улучшил безопасность благодаря использованию TKIP (Temporal Key Integrity Protocol), который динамически генерирует ключи шифрования. Это сделало WPA более защищенным, чем WEP, но все же не лишенным уязвимостей, особенно в реализации.

Наиболее продвинутым из этих протоколов является WPA2, принятый в 2004 году. WPA2 использует AES (Advanced Encryption Standard) для шифрования данных, что обеспечивает высокий уровень безопасности. Он поддерживает как личный режим аутентификации (PSK), так и корпоративный (802.1X). Несмотря на свою надежность, WPA2 также подвержен некоторым уязвимостям, таким как KRACK (Key Reinstallation Attack), однако эти проблемы касаются скорее реализации протокола, чем его самой структуры.

В современных условиях рекомендуется использовать WPA2 или WPA3 (новейший стандарт, предлагающий еще более высокий уровень безопасности) для защиты беспроводных сетей. WEP следует избегать, так как он больше не соответствует современным требованиям безопасности. Эти протоколы играют важную роль в обеспечении защиты данных пользователей и безопасности беспроводных сетей в целом [7].

Исходя из вышесказанного, в работе будет использоваться аутентификация WPA2

Теперь переходим к настройке WLC-23. Сперва следует настроить адресацию (рисунок 3.14).

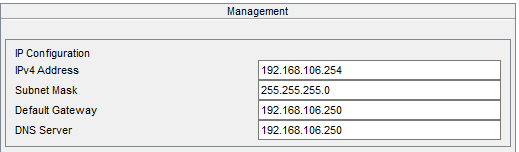


Рисунок 3.14 – Назначение адресов на WLC-23

Далее переходим к настройке самой беспроводной сети (рисунок 3.15).

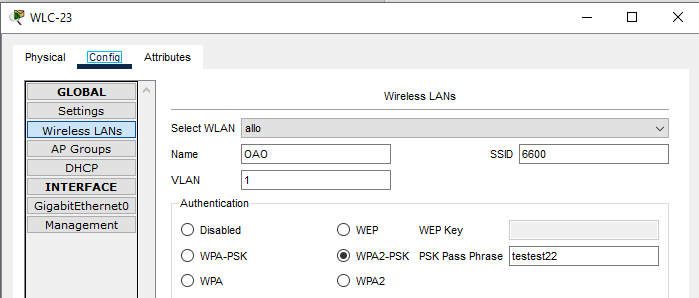


Рисунок 3.15 – Настройка WLAN на WLC-23

Следующим этапом будет настойка LWAP (рисунок 3.16).

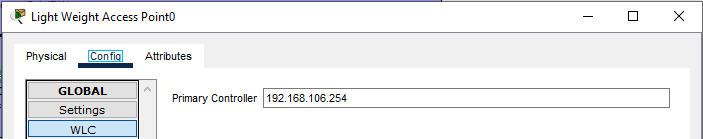


Рисунок 3.16 – Назначение главного контроллера на LWAP

Таким образом мы указываем адрес главного контроллера, т.е. WLC-23.

Точка доступа также теперь и имеет шлюз, указанный в DHCP, что подтверждает бесперебойную работу (рисунок 3.17).

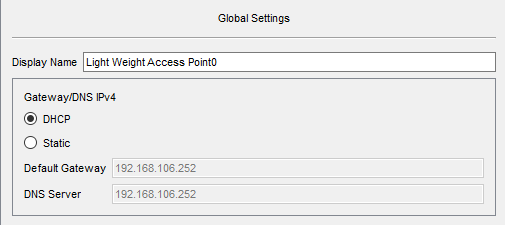


Рисунок 3.17 – Демонстрация работы DHCР на LWAP

Далее нужно осуществить подключение конечного устройства, для этого выбираем либо оконечное устройство беспроводной сети или компьютер. Следующая настройка будет показана на компьютере, поскольку таким образом можно приблизиться к действующей реальности. По стандарту программы Cisco Packet Tracer на ПК стоит адаптер проводной сети, интерфейс Ethernet, с таким Wi-Fi разумеется не будем работать, поэтому нужно сменить адаптер (рисунок 3.18).

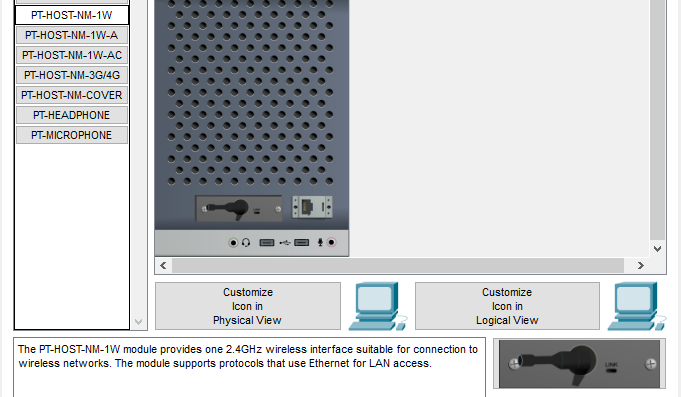


Рисунок 3.18 – Переключение адаптера на ПК

Далее переходим в конфигурацию компьютера, раздел беспроводной сети (рисунок 3.19).

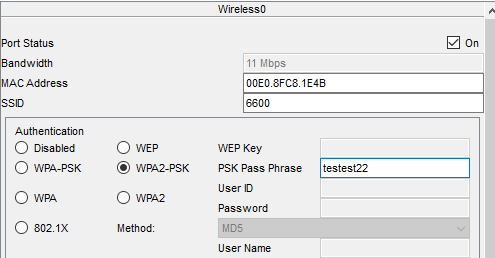


Рисунок 3.20 – Подключение к сети Wi-Fi

Выбираем необходимые параметры, вводим соответствующий SSID и кодовую фразу. Далее можно увидеть успешное подключение (рисунок 3.20).

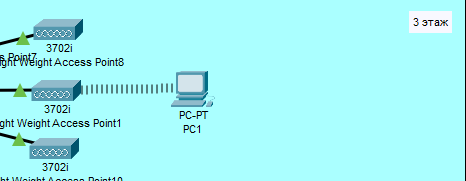


Рисунок 3.20 – Демонстрация успешного подключения

Настройка самостоятельных точек доступа выглядит аналогично, только конечные устройства уже подключаются напрямую к нему (рисунок 3.21).

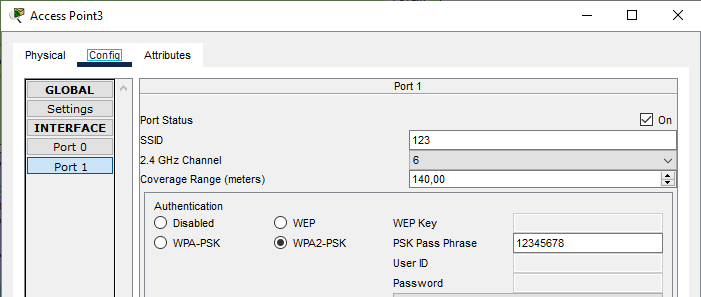


Рисунок 3.21 – Настройка Access Point

Далее следует провести такую же настройку, как раньше, на компьютере и проверить работу (рисунок 3.22).

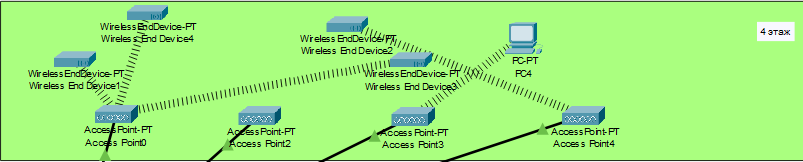


Рисунок 3.22 – Демонстрация работы Wi-F с AP

Для дополнительного показателя связности сети отправим пакет с компьютера начальства на компьютер офиса с первого этажа (рисунок 3.23).

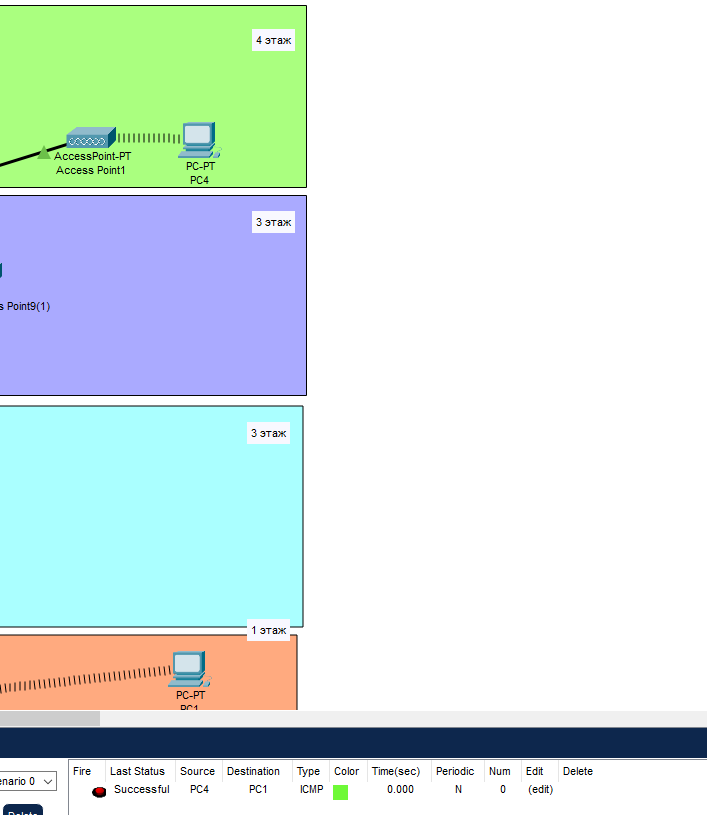


Рисунок 3.23 – Демонстрация работоспособности беспроводной сети

Можно увидеть, что сеть работает.

Таким образом, в Cisco Packet Tracer была разработана эмуляция проекта, что обеспечило возможность визуализировать и протестировать предложенные решения в защищенной среде.

# Техника безопасности

Все проблемы, возникающие при работе ВДТ и ПЭВМ, можно разделить на три группы:

* параметры рабочего места и рабочей зоны;
* визуальные факторы (яркость, контрастность, мерцание изображения, блики);
* излучения (рентгеновское, электромагнитное излучение вч и свч диапазона, гамма-излучение, электростатические поля).

Условия труда работающих с ЭВМ характеризуются возможностью воздействия на них следующих производственных факторов: шума, тепловыделений, вредных веществ, статического электричества, ионизирующих и неионизирующих излучений, недостаточной освещенности, параметров технологического оборудования и рабочего места.

ПЭВМ являются источниками широкополостных электромагнитных излучений:

* мягкого рентгеновского;
* ультрафиолетового 200-400 нм;
* видимого 400-750 нм;
* ближнего ИК 750-2000 нм;
* радиочастотного диапазона 3кГц;
* электростатических полей.

Существенным недостатком Wi-Fi постоянное СВЧ-излучение, в котором находятся жители крупных городов. В 2011 году Международное Агентство по Исследованиям в области рака классифицировало радиоизлучение как “возможно канцерогенное для людей”. Классификация IARC радиоизлучения 65 отражает факт, что некоторые ограниченные доказательства существуют, что излучение радиоволн гипотетически может быть фактором риска для рака.

Однако достоверного подтверждения этим гипотезам до настоящего времени нет. Так же не было выявлено связи между воздействием радио и раковыми заболеваниями.

При этом нельзя утверждать, что Wi-Fi абсолютно безвреден для человека. В настоящее время данный вопрос требует более глубоких исследований. Всемирная организация здравоохранения и IARC намерены гарантированно провести дополнительные исследования в этой области.

Приведем несколько цифр доступных всем: максимальная мощность сотового сигнала достигает 8 Вт, сигнала обычного бытового Wi-Fi передатчика – 100 мВт. Допустимая плотность потока энергии (по СаНПиН 2.1.8/2.2.4) – 0,1 Вт/м2. А плотность потока энергии - физическая величина, численно равная потоку энергии через единичную площадку, перпендикулярную направлению.

Из чего следует что, излучение беспроводного интернета никак не превышает установленные нормы. Лучшая защита от нежелательного облучения - это расстояние. Причем достаточно 1м, но ученые перестраховываются и рекомендуют 3м. Большую опасность представляют 3Gмодемы, так как работают по сигналам сотовой связи.

Дополнительную безопасность от Wi-Fi излучений можно получить, придерживаясь этих правил:

* точки доступа должны быть расположены подальше от мест сна и постоянных рабочих мест;
* по возможности отключать Wi-Fi роутер, если интернет не используется; - держать устройства, принимающие Wi-Fi подальше от себя, например, на столе;
* максимально оградить маленьких детей от Wi-Fi роутеров, с целью избежание перенапряжение растущего организма дополнительным излучением.

Научные исследования демонстрируют, что сигналы Wi-Fi намного ниже допустимых международных норм и не требуют ограничений в использовании и дополнительных мер безопасности. Так что нет никаких видимых причин для отказа от тех огромных преимуществ, которые обеспечивает технология Wi-Fi [8].

Излучение радиочастоты от оборудования Wi-Fi во всех местах, доступных для широкой публики, должно быть не выше уровня, установленного официальными медицинскими инструкциями по технике безопасности. Пределы, определенные в нормативных инструкциях, намного ниже «порога вредности» и основаны на данных тысяч изданных научных исследований по воздействию излучения радиоволн. Единые нормы определены для взрослых и детей. При этом допускается продолжительное воздействие в режиме 24 часа, 7 дней в неделю.

Далее, так как работа технического персонала непосредственно связана с компьютером, следовательно, он подвержен дополнительным воздействиям целой группы факторов, что неоспоримо снижает производительность их труда.

К таким факторам относятся:

* пониженный уровень освещенности;
* нарушение микроклимата;
* наличие напряжения.

Работа людей в помещение относится к выполнению работ категории (1а), т.к. управление оборудованием происходит дистанционно с помощью компьютеров. Для создания нормальных условий для работников предприятий связи установлены нормы производственного микроклимата. В помещениях при работе с персональным компьютером должны соблюдаться следующие климатические условия.

Холодное время года:

* оптимальная температура 22-24 С˚;
* допустимая температура 18-26 С˚;
* относительная влажность 40-60 %;
* скорость движение воздуха относительная и допустимая 0,1 м/с.

Тёплое время года:

* оптимальная температура 23-25 С˚;
* относительная влажность 40-60 %;
* допустимая влажность 55%;
* скорость движение воздуха относительная 0,1 м/с и допустимая 0,1-0,2 м/с [1].

Также для разворачивания беспроводной сети необходимо будет установить крепление оборудования, соблюдая некоторые правила, чтобы избежать несчастных случаев и обеспечить надежность установки.

Первым шагом является оценка рабочего места: необходимо проверить наличие препятствий, таких как провода, трубы и вентиляционные каналы, которые могут помешать установке. Также убедиться, что место установки не подвергается воздействию влаги или высоких температур.

Не забывать о средствах индивидуальной защиты (СИЗ). Рекомендуется носить защитные очки для защиты глаз от пыли и обломков, а также использовать перчатки для защиты рук от острых краев и загрязнений.

При работе на высоте использовать устойчивую лестницу или подъемник, чтобы избежать падений. Убедиться, что лестница стоит на ровной поверхности и надежно закреплена. Также важно соблюдать электробезопасность: нужно отключить электрическое питание в зоне установки, если работа ведется рядом с электропроводкой, и использовать инструменты с изолированными ручками.

Правильное использование инструментов также имеет значение. Использовать их нужно лишь в соответствии с назначением и инструкциями производителя, а также следить за тем, чтобы они были в хорошем состоянии и исправны.

При монтаже крепления нужно следовать инструкциям производителя как крепления, так и точки доступа. Необходимо использовать соответствующие крепежные элементы и проверяйте их на прочность. После установки обязательно проверить, что точка доступа надежно закреплена и не колеблется, а кабели не натянуты и не могут быть повреждены.

Также следует убедиться, что точка доступа легко доступна для обслуживания и проверки.

Дополнительной мерой безопасности является регулярная проверка оборудования точек доступа и других элементов беспроводной сети, необходимой для обеспечения её стабильной работы. Такие проверки помогают выявить потенциальные неисправности и предотвратить сбои, что в свою очередь поддерживает оптимальную производительность и улучшает качество сигнала. Кроме того, регулярное обслуживание способствует повышению безопасности сети, позволяя своевременно обновлять программное обеспечение и защищать от возможных уязвимостей. Это также увеличивает срок службы оборудования и снижает затраты на его замену, что делает регулярные проверки неотъемлемой частью эффективного управления беспроводной сетью [10].

Таким образом была рассмотрена техника безопасности.

# ЗАКЛЮЧЕНИЕ

В ходе выполнения выпускной квалификационной работы были рассмотрены: технология Wi-Fi, её стандарты, методы проектирования беспроводных сетей и их виды. Был исследован объект проектирования, выявлены его потребности, проведены нужные расчеты и составлен проект, необходимый для реализации поставленной цели.

Чтобы спроектировать беспроводную сеть в «CiscoPacketTracer», были выполнены предварительные расчёты и освежены в памяти команды, изученные в процессе обучения.

Далее были рассмотрена техника безопасности.

В заключение следует подчеркнуть, что развитие и внедрение беспроводных сетей играют ключевую роль в современном информационном обществе. С каждым годом требования пользователей к скорости, стабильности и доступности интернет-соединения растут, а технологии продолжают эволюционировать, предлагая новые решения и возможности. Актуальность этой темы будет только возрастать, учитывая стремительный рост числа подключенных устройств и потребность в эффективных коммуникационных решениях в различных сферах, от бытового использования до бизнеса и образования.

В соответствие с целью курсовой работы была спроектирована беспроводная сеть для ОАО «Завод Электросигнал».

Для достижения поставленной цели были решены следующие задачи:

* разработка проекта WLAN,
* план помещений, расположение оборудования,
* рекомендации к выбору оборудования,
* проверка работоспособности сети в программе «CiscoPacketTracer».

Цель курсовой работы достигнута.

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. СП 2.2.3670-20. Санитарные правила Санитарно-эпидемиологические требования к условиям труда / Минздрав России, 2020.
2. Ломовцева Н.В. IP-адресация: учебное пособие / Н. В. Ломовцева, Л. В. Волкова. 2-е изд., пересмотр, и доп. Екатеринбург, 2022. 60 с.
3. Мелихов, С. В. Технологии цифровой радиосвязи: OFDM, COFDM, OFDMA, SC-FDMA, MIMO. Томск: Томск. гос. ун-т систем упр. и радиоэлектроники, 2021. 46 c.
4. Минин В.Е Cisco Packet Tracer: учебно-методическое пособие / В.Е. Минин, К.Ф. Измайлов. Гомель, 2023. 104 с.
5. Сергеев А.Н. Основы локальных компьютерных сетей: учебное пособие / А. Н. Сергеев. СПб.: Издательство «Лань», 2021. 184 с.
6. Ушаков Ю.А Построение и настройка беспроводных сетей: методические указания / Ю. А. Ушаков, М. В. Ушакова, П. Н. Полежаев, А. Л. Коннов; Оренбургский гос. ун-т. – Оренбург : ОГУ, 2017. 41 с.
7. Фаткиева Р.Р. Основы построения защищенных компьютерных сетей. Санкт-Петербург: СПбГЭТУ «ЛЭТИ», 2021. 31 c.
8. Вредит ли Wi-Fi живым организмам? // Сайт habr.com URL: https://habr.com/ru/companies/nag/articles/373459/ (дата обращения: 30.05.2025).
9. Коэффициенты затухания сигнала Wi-Fi при прохождении через различные среды // Сайт help.keenetic.com URL: https://help.keenetic.com/hc/ru/articles/213968869-Коэффициенты-затухания-сигнала-Wi-Fi-при-прохождении-через-различные-среды (дата обращения: 28.05.2025).
10. Общие требования к прокладке проводов и кабелей // Сайт inkabel.ru URL: https://inkabel.ru/obshhie-trebovaniya-k-prokladke-provodov-i-kabelej/ (дата обращения: 30.05.2025).
11. Преимущества и недостатки Wi-Fi // Сайт rslink.ru URL: http://rslink.ru/preimushhestva-i-nedostatki-wi-fi/ (дата обращения: 30.05.2025).
12. Промышленный Wi-Fi: рациональные решения для организации сетей передачи данных // Сайт zolteh.ru URL: https://zolteh.ru/technic/promyshlennyj-wi-fi-ratsionalnye-resheniya-dlya-organizatsii-setej-peredachi-dannyh/ (дата обращения: 30.05.2025).
13. Уникальный векторный редактор – Microsoft Visio // Сайт junior3d.ru URL: https://junior3d.ru/article/microsoft-visio.html (дата обращения: 10.05.2025).
14. Что такое Mesh Wi-Fi и как подобрать устройства с поддержкой этой технологии // Сайт tp-link.ru URL: https://tp-link.ru/support/mesh-wifi/chto-takoe-mesh-wi-fi-i-kak-podobrat-ustroystva-s-podderzhkoy-etoy-tekhnologii/ (дата обращения: 28.05.2025).
15. Электросигнал // Сайт web.archive.org URL: https://web.archive.org/web/20240201152720/https:/ru.wikipedia.org/wiki/Электросигнал\_%28завод,\_Новосибирск%29 (дата обращения: 03.04.2025).
16. Электросигнал // Сайт 2gis.ru URL: https://2gis.ru/novosibirsk/search/Электросигнал/ (дата обращения: 28.05.2025).
17. IEEE Standarts // Сайт standards.ieee.org URL: https://standards.ieee.org/about/standards-in-action/ (дата обращения: 28.05.2025).
18. IP Калькулятор сети онлайн // Сайт ipmeter.ru URL: https://ipmeter.ru/ (дата обращения: 08.05.2025).
19. Wi-Fi адаптеры // Сайт www.<dns-shop.ru> URL: [https://www.dns-shop.ru/catalog/recipe/622ae55407ce0ef6/wi-fi-6-80211ax/](https://www.dns-shop.ru/catalog/recipe/622ae55407ce0ef6/wi-fi-6-80211ax/?ysclid=mbovw1kql6410197719&utm_medium=organic&utm_source=yandex&utm_referrer=https%3A%2F%2Fyandex.ru%2F) (дата обращения: 28.05.2025).
20. Wi-Fi Alliance® applauds UK Ofcom’s proposal to expand 6 GHz Wi-Fi® access // Сайт wi-fi.org URL: https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-applauds-uk-ofcoms-proposal-expand-6-ghz-wi-fi-access (дата обращения: 28.05.2025).

# ПРИЛОЖЕНИЕ А