**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ**
**РЕСПУБЛИКИ КАЗАХСТАН**

**Некоммерческое акционерное общество**
**АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ**

**кафедра** Телекоммуникационных систем

**«Допущен к защите»**
**Заведующий кафедрой** _____
_____
(Ф.И.О., ученая степень, звание)
_____ «_____»_____**20__ г.**
(подпись)

# ДИПЛОМНЫЙ ПРОЕКТ

**На тему:** „Разработка альтернативного способа организации беспроводной локальной сети

**Специальность** 5В0719 Радиотехника, Электроника и Телекоммуникации

**Выполнил (а)** Дуванцев Н. С. МТС-10-07
(Фамилия и инициалы) группа

**Научный руководитель** Зайцев Е. О.
(Фамилия и инициалы, ученая степень, звание)

**Консультанты:**
**по экономической части:**
Бекишева А. И., к. э. н., доцент
(Фамилия и инициалы, ученая степень, звание)
_____ «19» мая 2014 г.
(подпись)

**по безопасности жизнедеятельности:**
Дюсебаев М. К., д. т. н., профессор
(Фамилия и инициалы, ученая степень, звание)
_____ «05» июня 2014 г.
(подпись)

**по применению вычислительной техники:**
Артюкин А. В., старший преподаватель
(Фамилия и инициалы, ученая степень, звание)
_____ «05» июня 2014 г.
(подпись)

**Нормоконтролер:** Кондратович А. П., старший преподаватель
(Фамилия и инициалы, ученая степень, звание)
_____ «6» 06 2014 г.
(подпись)

**Рецензент:** _____
(Фамилия и инициалы, ученая степень, звание)
_____ «_____»_____20___г.
(подпись)

**Алматы 2014 г.**

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ**
**РЕСПУБЛИКИ КАЗАХСТАН**

**Некоммерческое акционерное общество**
**АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ**

Факультет Радиотехники и связи
Специальность 5В0719 - Радиотехника, электроника и телекоммуникации
Кафедра Телекоммуникационных систем

# ЗАДАНИЕ
на выполнение дипломного проекта

Студент Дукпищев Никита Сергеевич
(фамилия, имя, отчество)

Тема проекта „Разработка альтернативного способа организации беспроводной локальной сети"

утверждена приказом ректора № ___ от «___» сентября 20___ г.
Срок сдачи законченной работы «___» _____ 20___ г.
Исходные данные к проекту требуемые параметры результатов проектирования (исследования) и исходные данные объекта
Персональный компьютер HP D1V57EA (процессор Intel Pentium Dual Core G2030-3000; 4GB SDRAM 1600 MHz; HDD SATA 500 GB; HP WLAN 802.11 a/n Wi-Fi); Маршрутизатор Linksys Smart Wi-Fi Router EA2700 (802.11n 2,4/5 HHz; 4xLAN; WEP; WPA; WPA2); Беспроводная точка доступа Linksys WAP300N (802.11n 2,4/5 HHz; WEP; WPA; WPA2)

Перечень подлежащих разработке дипломного проекта вопросов или краткое содержание дипломного проекта:
Рассмотрение существующих методов построения и принципов работы беспроводных локальных сетей; Описание используемых методов защиты сетей и выявление их недостатков и уязвимостей; Предложение альтернативного способа организации беспроводных локальных сетей; Данный дипломный проект заключается в том, что беспроводные технологии очень распространены на сегодняшний день, особенно построение беспроводной сети на основе Wi-Fi. Но защищенность Wi-Fi сети на сегодняшний день очень слаба, поэтому развитие Li-Fi сможет поднять защищенность локальных беспроводных сетей на новый уровень

Перечень графического материала (с точным указанием обязательных чертежей)

Рисунки – различные топологии построения беспроводной локальной сети; Иллюстрации использования технологии Li-Fi в повседневной жизни; Зоны покрытия беспроводной сети Wi-Fi и Li-Fi.

Рекомендуемая основная литература

„Основы построения беспроводных локальных сетей стандарта 802.11. Практическое руководство по изучению, разработке и использованию беспроводных ЛВС стандарта 802.11"/ Гедман Роман, Джонатан Лизри. – М.: Cisco Press Перевод с английского Издательский дом „Вильямс", 2004; „Секреты беспроводных технологий"/ Джек Монкалау. – М.: "НТ-Пресс, 2005; Сети и системы радиодоступа / Григорьев В.А., Лагутенко О.И., Распаев Ю.А – М.: Эко-Трендз, 2005

Консультанты по проекту с указанием относящихся к ним разделов

| Раздел | Консультант | Сроки | Подпись |
|---|---|---|---|
| Техническая часть | Зайцев Е.О. | | |
| Экономическая часть | Бекишева А.И. | | |
| Безопасность жизнедеятельности | Дюсебаев М.К. | 17.03 – 03.06.14 | |
| ВТ | Артюкин А.В. | 12.05 – 5.06.14 | |
| | | | |

# ГРАФИК
подготовки дипломного проекта

| Наименование разделов, перечень разрабатываемых вопросов | Сроки представления руководителю | Примечание |
|---|---|---|
| Выявление проблем современных беспроводных сетей | 22.02.14 | |
| Сравнение различных технологий беспроводной передачи данных | 22.02.14 | |
| Анализ сети Li-Fi и возможность развертывания сети | 24.02.14 | |
| Сравнение беспроводных сетей Li-Fi и Wi-Fi на примере офиса | 28.02.14 | |
| Выбор оборудования для развертывания Wi-Fi сети в помещении | 07.03.14 | |
| Анализ различных моделей распространения сигнала | 16.03.14 | |
| Расчет оборудования | 01.04.14 | |
| Анализ освещенности помощения | 14.04.14 | |
| Расчет зоны покрытия Wi-Fi | 17.04.14 | |
| Расчет зоны покрытия Li-Fi | 18.04.14 | |
| Расчет потерь Wi-Fi сигнала в программе Mathcad | 22.04.14 | |
| Анализ построенной сети | 03.05.14 | |

Дата выдачи задания «02» февраля 2014 г.

Заведующий кафедрой _____ Шомахметов Д.Р.
(подпись) (Фамилия и инициалы)

Руководитель _____ Зайцев Е.О.
(подпись) (Фамилия и инициалы)

Задание принял к исполнению
студент _____ Дуплищев Н.С.
(подпись) (Фамилия и инициалы)

**Аңдатпа**

Айтылмыш дипломдық жобада менімен қара сымсыз жергілікті аудың құрылысының түрлі технологиялары болды, оның плюсі және минустар қара.

Жоғарылату мақсатпен аудың қауіпсіздігінің, ал олай ғой босатып ал, нешінші в айтылмыш кезді өте тие радиоэфирді, мен деректердің берілісінің нұрдың қиюын үшін Li-Fi сымсыз ау құрылыс үшін пайдалану ұсын.

Тарауда тіршілік әрекетімнің қауіпсіздігінің, кел персоналдың және жабдықтың анализы Wi-Fi сымсыз ауының құрылысы үшін болды. Бағала помеще жұмысшысының жарықталғандығы санитарлық шамаларға деген айдала бол.

**Аннотация**

В данном дипломном проекте мной были рассмотрены различные технологии построения беспроводной локальной сети, рассмотрены их плюсы и минусы.

С целью повысить безопасность сети, а так же освободить радиоэфир, который в данный момент очень загружен, я предлагаю использовать световой способ передачи данных для построения беспроводной сети Li-Fi.

В разделе безопасность жизнедеятельности, был составлен анализ персонала и оборудования для построения беспроводной сети Wi-Fi. Ссылаясь на санитарные нормы была оценена освещенность рабочего помещения, проведены расчеты естественного и искусственного освещений, в результате которых были предоставлены соответствующие рекомендации.

**Annotation**

In this thesis project me covered various technology to build a wireless local area network, considered the pros and cons.

In order to increase network security, as well as the release of the airwaves, which is currently very busy, I suggest using a light way to transfer data to build a wireless network Li-Fi.

In the safety of  life, an analysis was made of staff and equipment to build a wireless network Wi-Fi. Referring to the sanitary norms was estimated illumination workroom, the calculations of natural and artificial lighting, which resulted in the provided recommendations.

## Содержание

## Введение

Вне всяких сомнений, на сегодняшний день беспроводные средства связи активно развивающаяся отрасль связи. Ежедневно беспроводные технологии вытесняют устаревшие проводные системы. Например, все чаще локальные сети строят или дополняют беспроводными системами: домашние сети, сети предприятий. Множество продуктов работаю на беспроводных технологиях: датчики, производственные линии, бытовые приборы. Но несмотря на такой активный рост беспроводных средств связи, существуют и нерешенные проблемы. Одной из таких проблем является информационная безопасность связи.

Количество беспроводных технологий с каждым годом растет и постоянно ищутся способы их улучшения. Одни технологии будут хороши в одних сферах, но буду иметь серьезные недостатки в других. Например: ZigBee в решении “умный дом”, за счет низкого энергопотребления и небольших размерах устройств. WiMAX в высокоскоростном доступе к сети Internet в пределах города, за счет больших зон покрытия. Wi-Fi в пределах территории компании\офиса\дома для мобильных и стационарных устройств.

Но основной недостаток этих технологий – помехи. В жилой многоэтажке Wi-Fi устройства в разных квартирах влияют друг на друга. В производственном помещении оборудование так же может повлиять на сигнал, немаловажная составляющая хорошей беспроводной сети – оценка распространения сигнала с учетом стен, перекрытий, а так же тип и толщина материала.

Новая технология Li-Fi не использует радиочастоты, поэтому какое либо оборудование не может повлиять на него, а так же, за счет того, что обычно свет ограничивается в пределах комнаты, это помогает создать более защищенную сеть, чем с использованием технологии Wi-Fi.

Актуальность данного проекта заключается в том, что беспроводные технологии очень распространены на сегодняшний день, особенно построение локальной беспроводной сети на основе Wi-Fi. Но защищенность Wi-Fi сети сейчас очень слаба, потому развитие Li-Fi сможет поднять защищенность локальных беспроводных сетей на новый уровень.

Объектом исследования является локальные сети.

Предметом исследования является использование нового беспроводного доступа к локальной сети.

Для достижения указанной цели необходимо решить ряд задач:

- Исследование и анализ влияния беспроводных сетях связи друг на друга.
- Рассмотрение существующих методов построения и принципов работы беспроводных локальных сетей.
- Описание используемых методов защиты сетей и выявление их недостатков и уязвимостей.

- Предложение альтернативного способа организации беспроводных локальных сетей.

# 1 Теоретическая часть

## 1.1 Стандарт 802.11 (Wi-Fi)

Беспроводная сеть - это система передачи данных, в которой в качестве носителя используются радиоволны. Беспроводная сеть позволяет предоставить пользователям доступ к информационным ресурсам там, где развертывание кабельной системы невозможно или экономически нецелесообразно. Wi-Fi (англ. *Wireless Fidelity* - «беспроводная точность») - стандарт на оборудование Wireless LAN. Разработан консорциумом Wi-Fi Alliance на базе стандартов IEEE 802.11, «Wi-Fi» - торговая марка «Wi-Fi Alliance». Подключение нового пользователя к сети выполняется очень быстро, т. к. не требует прокладки проводов и установки информационных розеток. Средства безопасности на базе протоколов WEP, WPA и 802.1x обеспечивают надежное шифрование данных при передаче по радиоканалу и предоставляют функции аутентификации пользователей. Для дополнительной безопасности сеть может быть настроена на использование VPN.

Беспроводные сети имеют ряд существенных преимуществ перед обычными кабельными сетями:

- в отличие от обычной проводной LAN-сети, WLAN-сеть можно очень быстро развернуть, что очень удобно при проведении презентаций или в условиях работы вне офиса;
- пользователи мобильных устройств при подключении к локальным беспроводным сетям могут легко перемещаться в рамках действующих зон сети;
- скорости современных сетей довольно высоки (до 54 Мб/с), что позволяет их использовать для очень широкого спектра задач;
- с помощью дополнительного оборудования беспроводная сеть может быть успешно соединена с кабельными сетями;
- WLAN-сеть может оказаться единственным выходом, если не возможна или не желательна прокладка кабеля внутри здания, которая влечет за собой неизбежное сверление стен и прокладку кабельных каналов.

Но кроме описанных достоинств беспроводных сетей, есть и недостатки, а именно:

- чувствительность к радиопомехам;
- в некоторых случаях, в условиях крайне тяжелой радиочастотной обстановки, нормальная работа сети практически невозможна;
- скорость соединения плавает, соединение может прерываться;
- происходит сильное поглощение радиоволн железобетоном и некоторыми другими материалами, что приводит к ослаблению сигнала, а в итоге к снижению скорости передачи данных.[4]

Стандарт Radio Ethernet IEEE 802.11 - это стандарт организации беспроводных коммуникаций на ограниченной территории в режиме локальной сети, т. е. когда несколько абонентов имеют равноправный доступ к общему каналу передач. 802.11 - первый промышленный стандарт для беспроводных локальных сетей (Wireless Local Area Networks), или WLAN. Стандарт был разработан Institute of Electrical and Electronics Engineers (IEEE), 802.11 может быть сравнен со стандартом 802.3 для обычных проводных Ethernet-сетей.

Стандарт Radio Ethernet IEEE 802.11 определяет порядок организации беспроводных сетей на уровне управления доступом к среде (MAC-уровне) и физическом (PHY) уровне. В стандарте определен один вариант MAC (Medium Access Control)-уровня и три типа физических каналов.

Подобно проводному Ethernet, IEEE 802.11 определяет протокол использования единой среды передачи, получивший название carrier sense multiple access collision avoidance (CSMA/CA). Вероятность коллизий беспроводных узлов минимизируется путем предварительной посылки короткого сообщения, называемого ready to send (RTS). Оно информирует другие узлы о продолжительности предстоящей передачи и адресате. Это позволяет другим узлам задержать передачу на время, равное объявленной длительности сообщения. Приемная станция должна ответить на RTS посылкой clear to send (CTS). Передающий узел узнает, свободна ли среда и готов ли приемный узел к приему. После получения пакета данных приемный узел должен передать подтверждение (ACK) факта безошибочного приема. Если ACK не получено, попытка передачи пакета данных будет повторена.

В стандарте предусмотрено обеспечение безопасности данных, которое включает аутентификацию для проверки того, что узел, входящий в сеть, авторизован в ней, а также шифрование для защиты от подслушивания.

На физическом уровне стандарт предусматривает два типа радиоканалов и один инфракрасного диапазона.

В основу стандарта 802.11 положена сотовая архитектура. Сеть может состоять из одной или нескольких ячеек (сот). Каждая сота управляется базовой станцией, называемой точкой доступа (Access Point, AP). Точка доступа и находящиеся в пределах радиуса ее действия рабочие станции образуют базовую зону обслуживания (Basic Service Set, BSS). Точки доступа многосотовой сети взаимодействуют между собой через распределительную систему (Distribution System, DS), представляющую собой эквивалент магистрального сегмента кабельных ЛС. Вся инфраструктура, включающая точки доступа и распределительную систему, образует расширенную зону обслуживания (Extended Service Set). Стандартом предусмотрен также односотовый вариант беспроводной сети, который может быть реализован и без точки доступа, при этом часть ее функций выполняется непосредственно рабочими станциями. В настоящее время существует множество стандартов семейств IEEE 802.11:

- 802.11 первоначальный основополагающий стандарт. Поддерживает передачу данных по радиоканалу со скоростями 1 и 2 (опционально) Мбит/с;

- 802.11a высокоскоростной стандарт WLAN. Поддерживает передачу данных со скоростями до 54 Мбит/с по радиоканалу в диапазоне около 5 ГГц;

- 802.11b самый распространенный стандарт. Поддерживает передачу данных со скоростями до 11 Мбит/с по радиоканалу в диапазоне около 2,4 ГГц;

- 802.11c стандарт, регламентирующий работу беспроводных мостов. Данная спецификация используется производителями беспроводных устройств при разработке точек доступа;

- 802.11d определял требования к физическим параметрам каналов (мощность излучения и диапазоны частот) и устройств беспроводных сетей с целью обеспечения их соответствия законодательным нормам различных стран;

- 802.11e создание данного стандарта связано с использованием средств мультимедиа. Он определяет механизм назначения приоритетов разным видам трафика, таким как аудио- и видео приложения. Требование качества запроса, необходимое для всех радио интерфейсовIEEEWLAN;

- 802.11f стандарт, связанный с аутентификацией, определяет механизм взаимодействия точек связи между собой при перемещении клиента между сегментами сети. Другое название стандарта – Inter Access Point Protocol. Стандарт, описывающий порядок связи между равнозначными точками доступа;

- 802.11g устанавливает дополнительную технику модуляции для частоты 2,4 ГГц. Предназначен для обеспечения скоростей передачи данных до 54 Мбит/с по радиоканалу в диапазоне около 2,4 ГГц;

- 802.11h разработка данного стандарта связана с проблемами при использовании 802.11a в Европе, где в диапазоне 5 ГГц работают некоторые системы спутниковой связи. Для предотвращения взаимных помех стандарт 802.11h имеет механизм «квазиинтеллектуального» управления мощностью излучения и выбором несущей частоты передачи. Стандарт, описывающий управление спектром частоты 5 ГГц для использования в Европе и Азии;

- 802.11i (WPA2) целью создания данной спецификации является повышение уровня безопасности беспроводных сетей. В ней реализован набор защитных функций при обмене информацией через беспроводные сети, в частности технология AES (Advanced Encryption Standard) - алгоритм шифрования, поддерживающий ключи длиной 128, 192 и 256 бит. Предусматривается совместимость всех используемых в данное время устройств, в частности Intel Centrino с 802.1H-сетями. Затрагивает протоколы 802.1X, TKIP и AES;

- 802.11j предназначена для Японии и расширяет стандарт 802.11a добавочным каналом 4,9 ГГц;

- 802.11n позволяет поднять пропускную способность сетей до 100 Мбит/с;

- 802.11r предусматривает создание универсальной и совместимой системы роуминга для возможности перехода пользователя из зоны действия одной сети в зону действия другой;

Из всех существующих стандартов беспроводной передачи данных IEEE 802.11 на практике наиболее часто используются всего три, определенных Инженерным институтом электротехники и радиоэлектроники (IEEE), - 802.11b, 802.11g и 802.11a.

***Стандарт 802.11b***

- Частотный диапазон - 2,4 ГГц.
- Количество используемых радиоканалов - 3 не перекрывающихся.
- Макс. скорость передачи данных - 11 Мб/с.
- Примерная дальность действия - 30 м при 11 Мб/с.

***Стандарт 802.11g***

- Частотный диапазон - 2,4 ГГц.
- Количество используемых радиоканалов - 3 не перекрывающихся.
- Макс. скорость передачи данных - 54 Мб/с.
- Примерная дальность действия - 100 м при 1 Мб/с, 15 м при 54 Мб/с.

***Стандарт 802.11a***

- Частотный диапазон - 5 ГГц.
- Количество используемых радиоканалов - 8 не перекрывающихся.
- Макс. скорость передачи данных 54 Мб/с.
- Примерная дальность действия - 50 м при 11 Мб/с, 12 м при 54 Мб/с, 100 м при 6 Мб/с.[3]

В окончательной редакции широко распространенный стандарт 802.11b был принят в 1999 г. и благодаря ориентации на свободный от лицензирования диапазон 2,4 ГГц завоевал наибольшую популярность у производителей оборудования. Пропускная способность (теоретическая - 11 Мбит/с, реальная - от 1 до 6 Мбит/с) отвечает требованиям большинства приложений. Поскольку оборудование 802.11b, работающее на максимальной скорости 11 Мбит/с, имеет меньший радиус действия, чем на более низких скоростях, то стандартом 802.11b предусмотрено автоматическое понижение скорости при ухудшении качества сигнала. К началу 2004 года в эксплуатации находилось около 15 млн радиоустройств 802.11b.

В конце 2001 г. появился стандарт беспроводных локальных сетей 802.11a, функционирующих в частотном диапазоне 5 ГГц (диапазон ISM). Беспроводные ЛВС стандарта IEEE 802.11a обеспечивают скорость передачи данных до 54 Мбит/с, т. е. примерно в пять раз быстрее сетей 802.11b, и позволяют передавать большие объемы данных, чем сети IEEE 802.11b.

К недостаткам 802.11a относятся большая потребляемая мощность радиопередатчиков для частот 5 ГГц, а также меньший радиус действия (оборудование для 2,4 ГГц может работать на расстоянии до 300 м, а для 5 ГГц - около 100 м). Кроме того, устройства для 802.11a дороже, но со временем ценовой разрыв между продуктами 802.11b и 802.11a будет уменьшаться.

802.11g является новым стандартом, регламентирующим метод построения WLAN, функционирующих в нелицензируемом частотном диапазоне 2,4 ГГц. Максимальная скорость передачи данных в беспроводных сетях IEEE 802.11g составляет 54 Мбит/с. Стандарт 802.11g представляет собой развитие 802.11b и обратно совместим с 802.11b. Соответственно ноутбук с картой 802.11g сможет подключаться и к уже действующим точкам доступа 802.11b, и ко вновь создаваемым 802.11g. Теоретически 802.11g обладает достоинствами двух своих предшественников. В числе преимуществ 802.11g надо отметить низкую потребляемую мощность, большую дальность действия и высокую проникающую способность сигнала.

Стандарт 802.11n утверждён в сентябре 2009 г. Ключевой компонент стандарта под названием MIMO (Multiple Input, Multiple Output - много входов, много выходов) предусматривает применение пространственного мультиплексирования с целью одновременной передачи нескольких информационных потоков по одному каналу, а также многолучевое отражение, которое обеспечивает доставку каждого бита информации соответствующему получателю с небольшой вероятностью влияния помех и потерь данных. Именно возможность одновременной передачи и приема данных определяет высокую пропускную способность устройств 802.11n. Беспроводные адаптеры и точки доступа, реализованные в данном стандарте, передают и получают данные по схеме 4 x 4, то есть используют 4 разделенных потока для доставки голосовой информации, видео и данных по любому из двух каналов - 5-ГГц или 2,4-ГГц. Устройства будут иметь несколько антенн.[3]

Стандартом Wi-Fi предусмотрено несколько вариантов топологии беспроводной сети.

Простейшей структурой является локальная сеть «каждый с каждым» **Ad-hoc или по-другому называемый** Independent Basic Service Set (IBSS - независимый основной набор услуг), которую можно считать беспроводным аналогом одноранговой сети Ethernet, при которой узлы сети связываются напрямую друг с другом. Такая структура удобна для быстрого развертывания сетей. Для ее организации требуется минимум оборудования - каждое устройство просто должно быть снабжено адаптером WLAN. Пример данной сети приведен на рисунке 1.1.[6]

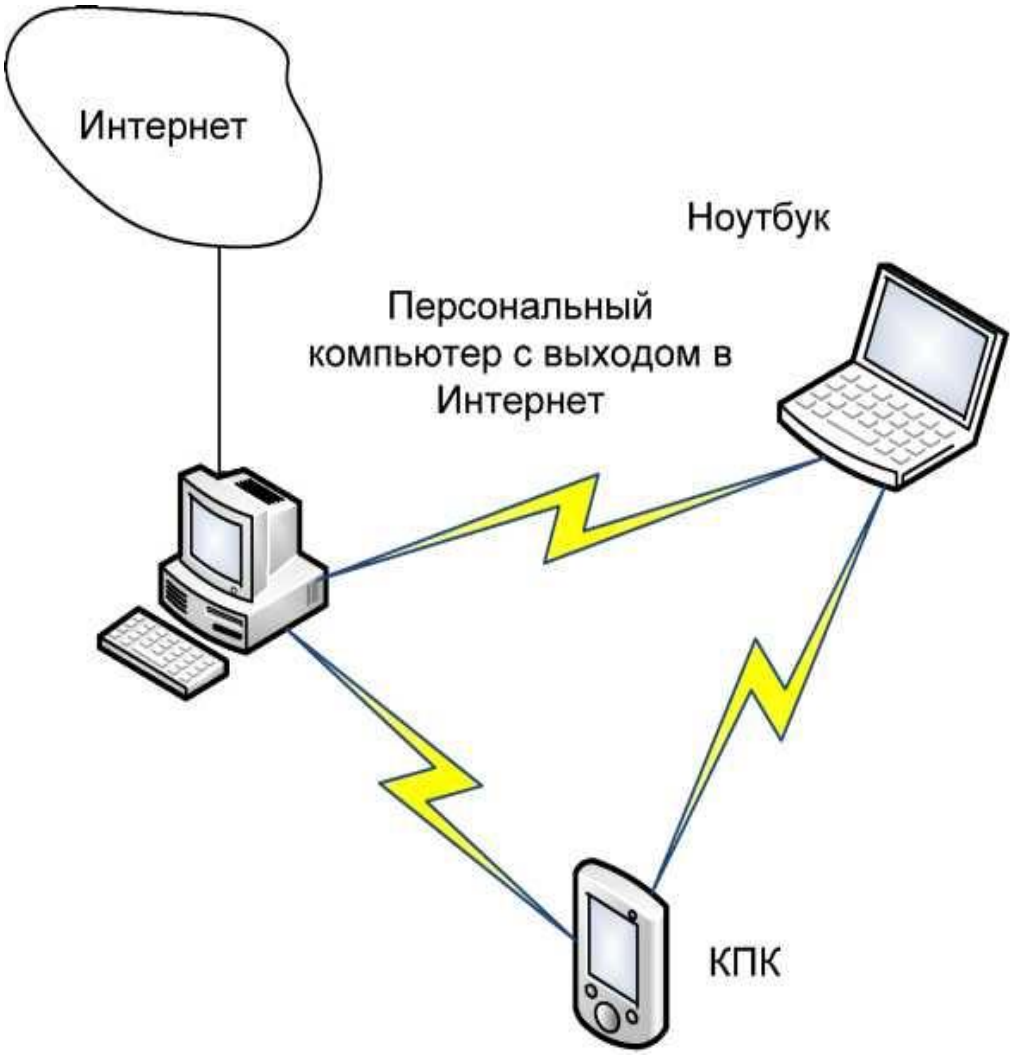


Рисунок 1.1 - Фрагмент одноранговой беспроводной сети

Данная топология предназначена для развертывания временных сетей на выставках, проведения различных семинаров и совещаний, а также для использования дома или в офисах малых компаний. Этот способ позволит соединить до восьми устройств в одноранговую сеть, где каждое устройство будет связано с другим. Но на самом деле его стоит использовать для соединения в сеть двух или трех устройств. Большее количество узлов объединять по этой схеме непрактично и неудобно. К примеру, чтобы КПК получил доступ к глобальной сети, потребуется постоянно держать компьютер включенным, с выходом в Интернет. Чаще используется другой вид организации беспроводных сетей, получивший название Infrastructure Mode - инфраструктурный режим (рисунок 1.2). В этом режиме узлы сети связаны друг с другом не напрямую, а через точку доступа – Access Point. Различают два режима взаимодействия с точками доступа - BSS (Basic Service Set - базовый набор услуг) и ESS (Extended Service Set - расширенный набор услуг).

В базовом режиме BSS все узлы связаны между собой через одну точку доступа, которая может также играть роль моста для соединения с Интернетом и внешней кабельной сетью.[6]

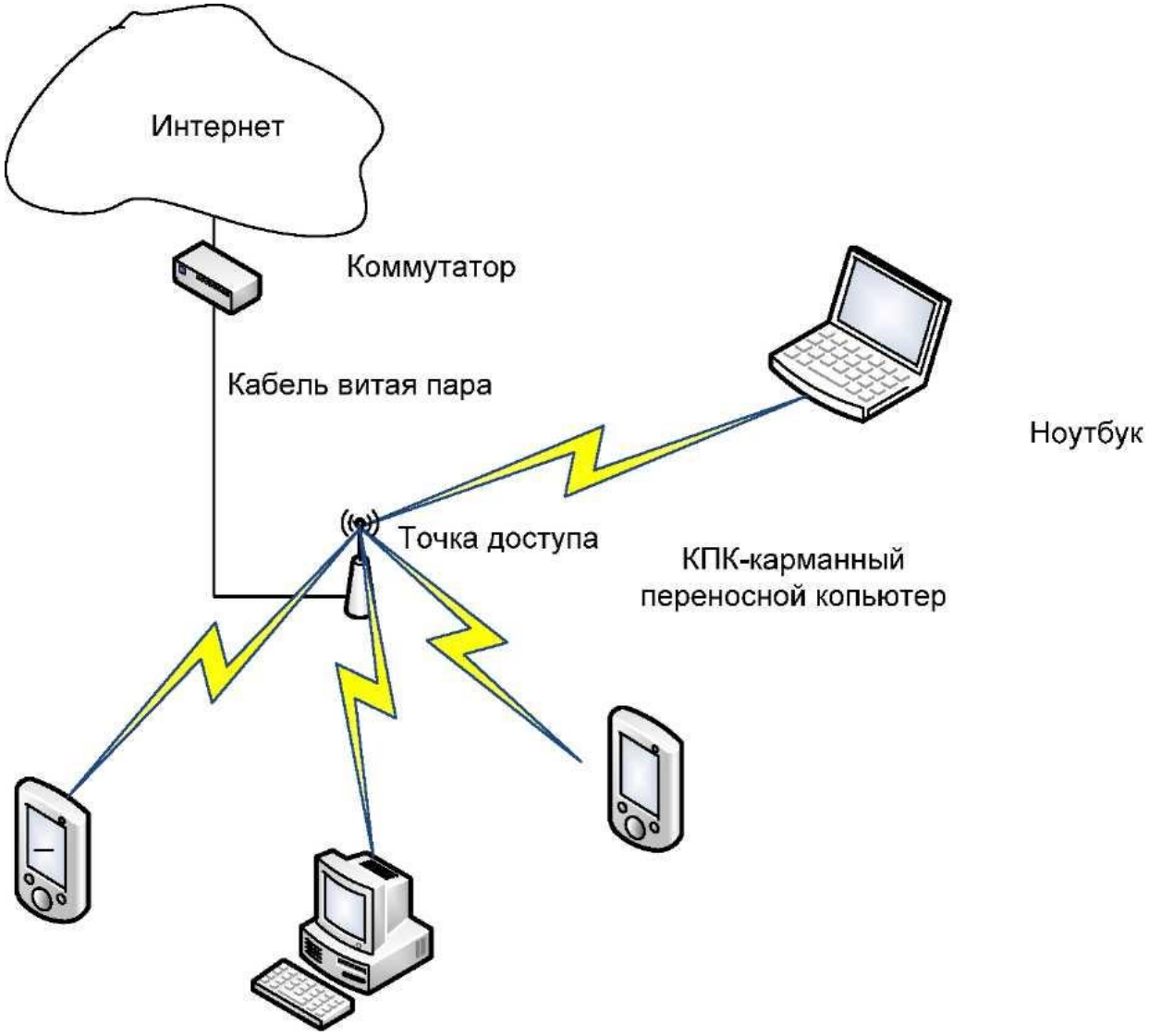


Рисунок 1.2 - Базовый режим связи через одну точку доступа

Расширенный режим ESS представляет собой объединение нескольких точек доступа, т. е. нескольких сетей BSS. В этом случае точки доступа могут взаимодействовать и друг с другом, а пользователь может переходить от одной точки доступа к другой. Расширенный режим удобно использовать тогда, когда необходимо объединить в одну сеть достаточно удаленных друг от друга пользователей или подключить несколько проводных сетей. Точки доступа соединяются между собой либо по радиоканалу, либо проводами (Ethernet-соединение) при отсутствии радиовидимости, например при наличии разделяющих помещение бетонных стен или межэтажных перекрытий.[6]

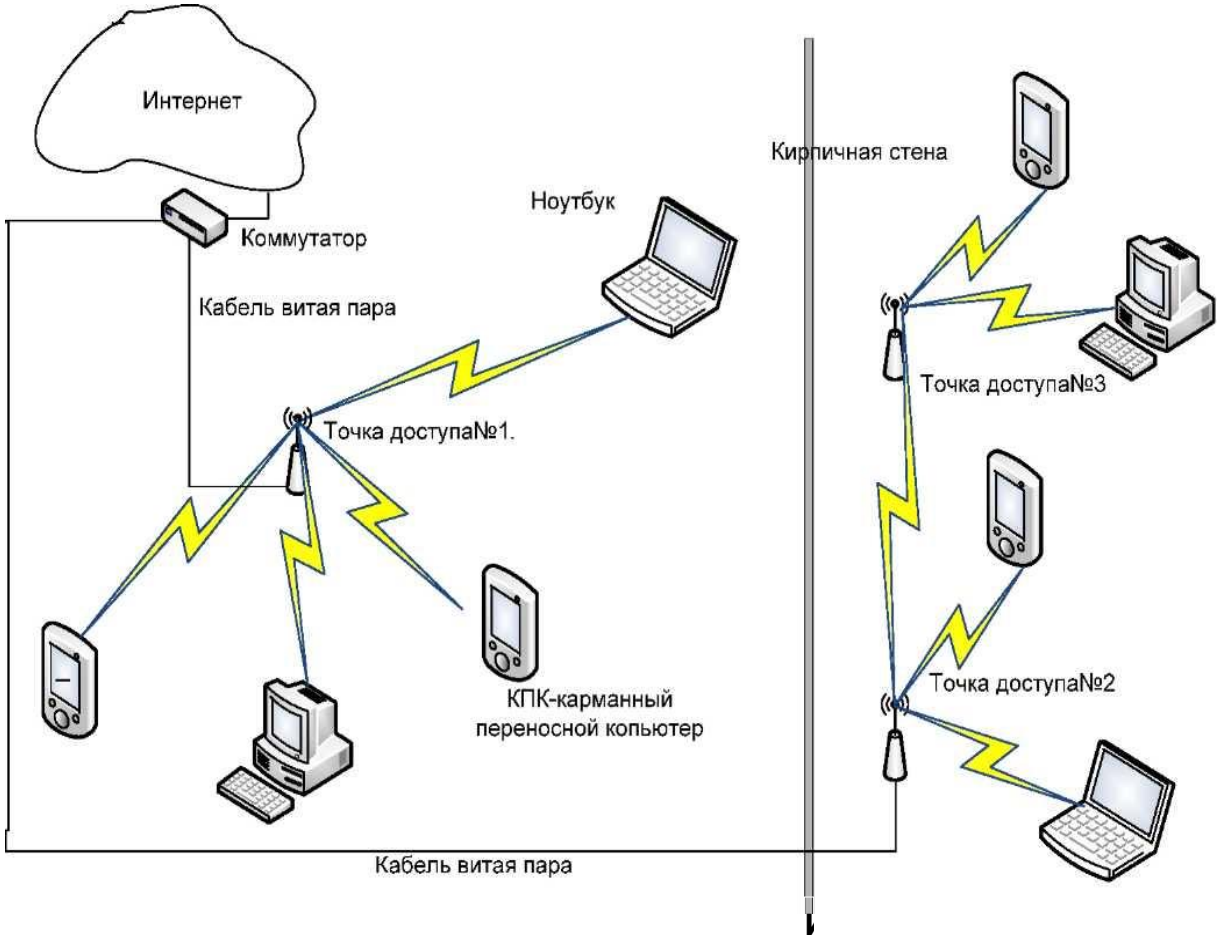


Рисунок 1.3 - Расширенный режим связи через несколько точек доступа

Рано или поздно перед каждым активным пользователем Интернета встает проблема построения домашней сети.

Подключение при помощи витой пары подразумевает прокладку кабеля - а это короба, дрель, пыль, грязь и все прочие радости, связанные со сверлением стен. Да и не всегда ясно, где будет любимое рабочее место и где устанавливать розетки. Есть простой выхода из этой ситуации - организовать беспроводную сеть Wi-Fi, позволяющую получать доступ к Интернету из любой комнаты в квартире и соединение между компьютерами и мобильными устройствами. Оптимальная схема сети, к примеру, может выглядеть так, как показано на рисунке 1.4.[6]

Устанавливаем в прихожей, около телефонной розетки, одно небольшое устройство, которое одновременно является ADSL-модемом и точкой доступа Wi-Fi, например ZyXEL P-660HTWEE. Снабжаем настольный компьютер адаптером Wi-Fi, ноутбуки и КПК обычно имеют встроенные Wi-Fi-адаптеры, настраиваем все оборудование - сеть готова. Если уже есть домашний компьютер, подсоединенный к Интернет, и появилось новое мобильное устройство, с которого также нужно выходить в мировую сеть, то очевидным решением будет установка точки доступа Wi-

Fi, которую надо подсоединить к компьютеру через Ethernet-порт. Тут могут быть два разных варианта. Первый: точка доступа соединяется напрямую со встроенным в компьютер Ethernet-портом. В этом случае для того, чтобы все пользователи Wi-Fi-сети могли выходить в Интернет, необходимо, чтобы компьютер был включен, что не всегда удобно (рисунок 1.5).[6]

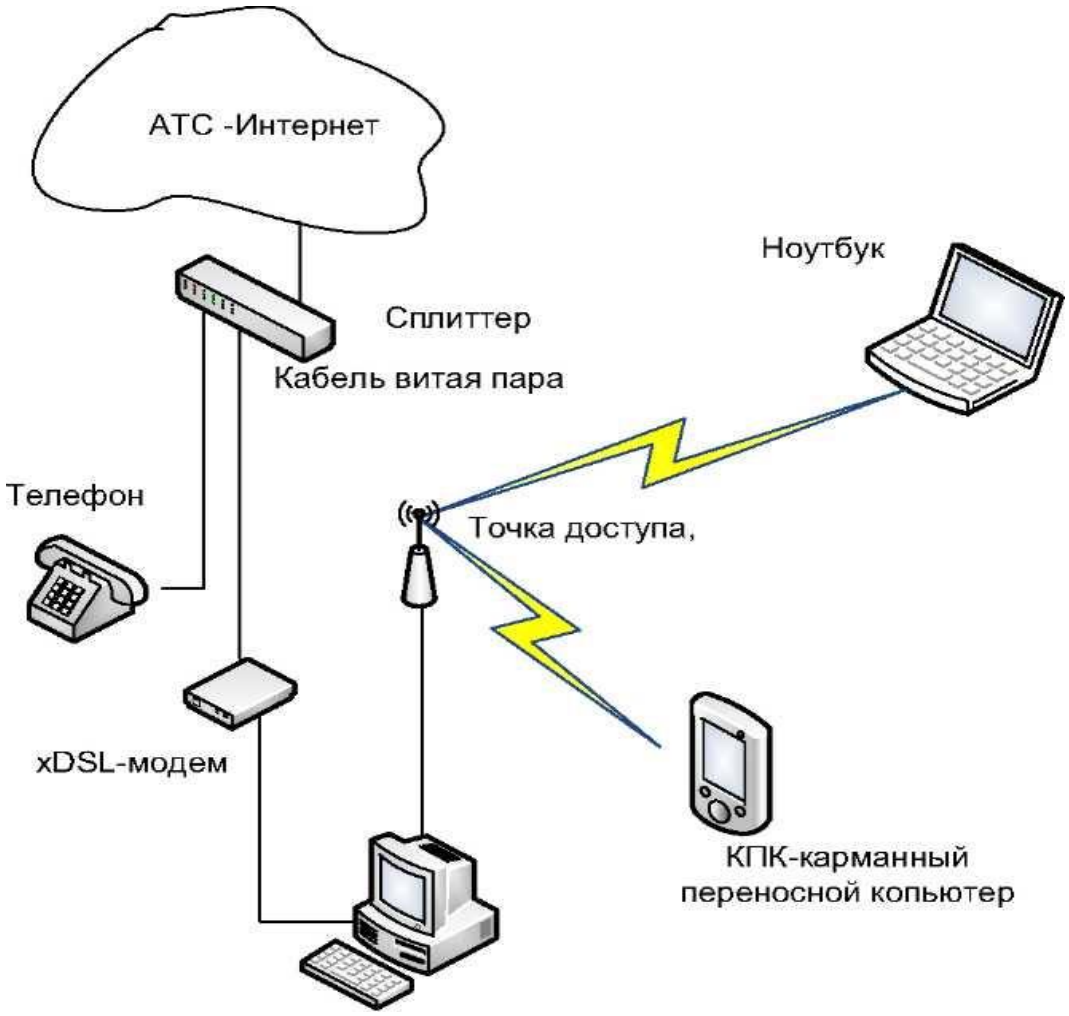


Рисунок 1.5 - Подключение беспроводной сети через компьютер

Если же модем имеет Ethernet-порт, то более технологичным будет второй способ подключения. Точка доступа Wi-Fi подсоединяется не к компьютеру, а к небольшому Ethernet-коммутатору, к которому, в свою очередь, подключены также компьютер и модем. В этом случае все устройства могут работать с сетью независимо друг от друга (рисунок 1.6).[6]

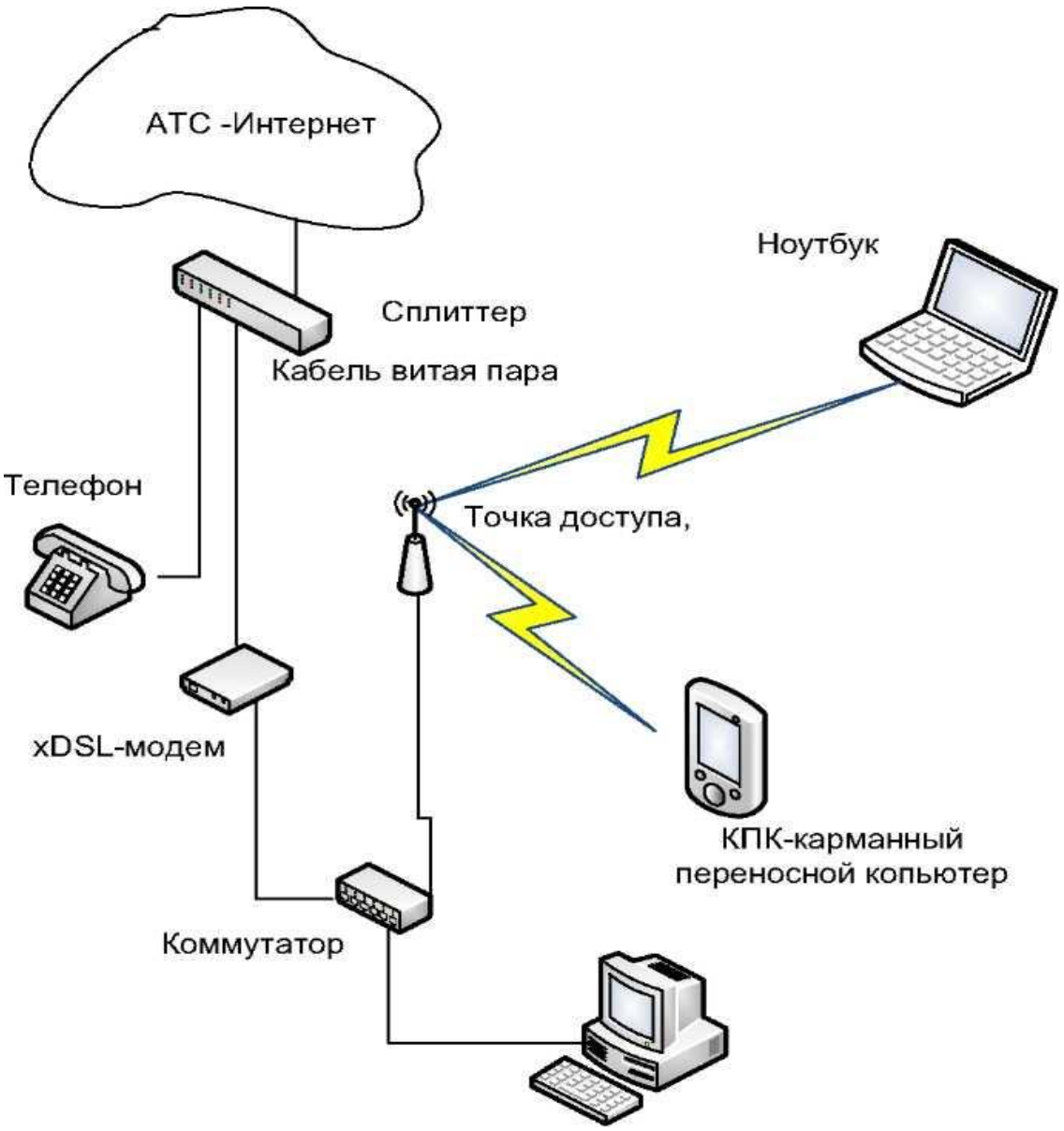


Рисунок1.6 - Подключение беспроводной сети через коммутатор

Если речь идет о создании беспроводной сети в пределах небольшой квартиры, то одной точки доступа будет вполне достаточно. Если же требуется реализовать задачу создания беспроводной сети в большом помещении, состоящем из комнат, разделенных бетонными стенами с арматурой, то одной точки доступа может оказаться явно недостаточно.

Для того чтобы расширить радиус действия беспроводной сети, проще всего развернуть распределенную беспроводную сеть на базе двух или более точек доступа. В худшем случае все же придется воспользоваться дрелью, чтобы соединить между собой точки доступа Ethernet-кабелем.[6]

Перед развертыванием беспроводной сети рекомендуется определить степень поглощения радиоволн во всех возможных местах размещения

клиентских устройств. Для этого потребуется беспроводная точка доступа и ноутбук или КПК, снабженные беспроводными адаптерами.

Методика планирования сети примерно следующая: устанавливаем точку доступа в месте предполагаемого размещения и включаем электропитание (ни в какой Интернет не включаем, никакие параметры беспроводной сети не настраиваем). Берем мобильное устройство и запускаем мастер установки беспроводной сети или просто включаем беспроводный адаптер, где сразу же начнется процедура поиска локальных беспроводных сетей, которые находятся в радиусе действия беспроводного адаптера. Большинство производителей устанавливают идентификатор сети SSID в значение «default», поэтому среди всех найденных сетей нас интересует именно эта.

Может получиться так, что вы обнаружите несколько Wi-Fi сетей без защиты и даже со стандартным названием сети «default». Скорее всего соседи по неопытности или невнимательности не защитили свою беспроводную сеть, таким образом, любой проходящий мимо человек с мобильным устройством может подключиться к соседям и даже больше – вполне вероятно получит доступ к сети Интернет за чужой счет. Но если это не так критично для домашней беспроводной сети, то для офисной сети это может стать большими неприятностями. Если не защитить офисную сеть, это вполне может стать утечкой информации.

Необходимо походить с ноутбуком по помещениям, в которых предполагается работать через Wi-Fi, и понаблюдать за уровнем сигнала и информацией об изменении скорости работы сети. Анализ картины на местности поможет выбрать необходимую схему сети и оптимальные места расположения точек доступа.[9]

## 1.2 Виды атак и методы защиты в сетях Wi-Fi

С точки зрения безопасности, следует учитывать не только угрозы, свойственные проводным сетям, но также и среду передачи сигнала. В беспроводных сетях получить доступ к передаваемой информации намного проще, чем в проводных сетях, равно как и повлиять на канал передачи данных. Достаточно поместить соответствующее устройство в зоне действия сети.

Радиоканал передачи данных, используемый в Wi-Fi потенциально подвержен вмешательству с целью нарушения конфиденциальности, целостности и доступности информации.

Большинство атак начинаются с разведки, в ходе которой производится сканирование сети (Net Stumbler, Wellenreiter), сбор и анализ пакетов - многие служебные пакеты в сети Wi-Fi передаются в открытом виде. При этом крайне проблематично выяснить, кто легальный пользователь, пытающийся подключиться к сети, а кто собирает

информацию. После разведки принимаются решения о дальнейших шагах атаки.

Защита сети с помощью отключения ответа на широковещательный запрос ESSID и скрытия название сети в служебных пакетах Beacon frame является недостаточной, так как сеть всё равно видна на определённом радиоканале и атакующий просто ждёт авторизованного подключения к сети, так как при этом в незашифрованном виде передаётся ESSID. На этом защитная мера теряет смысл. Хуже того, некоторые системы (например WinXp Sp2) непрерывно рассылают имея сети в эфир, пытаясь подключиться. Это также является интересной атакой, так как в таком случае можно пересадить пользователя на свою точку доступа и получать всю информацию, что он передаёт по сети.

Можно уменьшить подверженность разведке, разместив точку доступа так, чтобы она обеспечивала необходимое покрытие, и это покрытие минимально выходило за контролируемую территорию. Нужно регулировать мощность точки доступа и использовать специальные инструменты для контроля распространения сигнала. Также можно полностью экранировать помещение с точкой доступа для полной невидимости сети извне.

В случае анализа небольшой территории подойдёт встроенный Wi-Fi адаптер ноутбука, но на большее не хватит. Нужен более мощный адаптер с разъёмом для внешней антенны. Многие используют такие, как Alfa networks AWUS036H, Ubiquiti SRC, Linksys WUSB54GC.

В Linux-подобных системах настроить работу адаптера на приём всех пакетов, а не только тех, которые предназначены именно ему проще, чем на Windows. В некоторых драйверах такой режим поддерживается изначально, другие нужно изменять.

Наиболее распространённые программы для сбора информации — это Kismet и Aircrack-ng suite.

Kismet может не только перехватывать пакеты и обнаруживать скрытые сети, это также и инструмент для мониторинга и отладки сети, причём не только Wi-Fi, программа может работать с телефонными и Bluetooth сетями.

Aircrack-NG представляет собой набор инструментов для аудита беспроводных сетей. А ещё в эта программа реализует стандартную атаку FMS наряду с некоторыми оптимизациями KoreK'a, также новую PTW-атаку, которая ещё сильнее уменьшает время на взлом WEP.

Другие программы: Dwepcrack (улучшенная FMS атака), AirSnot (FMS), WepLab (улучшенная FMS атака, атака Koreka).

В Wi-Fi предусмотрены как аутентификация, так и шифрование, но эти элементы защиты имеют свои изъяны.

Шифрование значительно снижает скорость передачи данных, и, зачастую, оно осознанно отключается администратором для оптимизации трафика. Первоначальный стандарт шифрования WEP (Wired Equivalent

Privacy) был дискредитирован за счёт уязвимостей в алгоритме распределения ключей RC4. Это несколько притормозило развитие Wi-Fi рынка и вызвало создание институтом IEEE рабочей группы 802.11i для разработки нового стандарта, учитывающего уязвимости WEP, обеспечивающего 128-битное AES шифрование и аутентификацию для защиты данных. Wi-Fi Alliance в 2003 представил свой собственный промежуточный вариант этого стандарта - WPA (Wi-Fi Protected Access). WPA использует протокол целостности временных ключей TKIP (Temporal Key Integrity Protocol). Также в нём используется метод контрольной суммы MIC (Message Integrity Code), которая позволяет проверять целостность пакетов . В 2004 Wi-Fi Alliance выпустили стандарт WPA2, который представляет собой улучшенный WPA. Основное различие между WPA и WPA2 заключается в технологии шифрования: TKIP и AES. WPA2 обеспечивает более высокий уровень защиты сети, так как TKIP позволяет создавать ключи длиной до 128 бит, а AES - до 256 бит.

Угроза блокирования информации в канале Wi-Fi практически оставлена без внимания при разработке технологии. Само по себе блокирование канала не является опасным, так как обычно Wi-Fi сети являются вспомогательными, однако блокирование может представлять собой лишь подготовительный этап для атаки "человек посередине", когда между клиентом и точкой доступа появляется третье устройство, которое перенаправляет трафик между ними через себя. Такое вмешательство позволяет удалять, искажать или навязывать ложную информацию.

Угрозы информационной безопасности, возникающие при использовании Wi-Fi сетей, можно условно разделить на два класса:

- прямые - угрозы информационной безопасности, возникающие при передаче информации по беспроводному интерфейсу IEEE 802.11;
- косвенные — угрозы, связанные с наличием на объекте и рядом с объектом большого количества Wi-Fi-сетей.

Для информационной безопасности в Wi-Fi сетях используются следующие методы шифрования:

- WEP-шифрование (Wired Equivalent Privacy). Аналог шифрования трафика в проводных сетях. Используется симметричный потоковый шифр RC4 (англ. Rivest Cipher 4), который достаточно быстро функционирует. На сегодняшний день WEP и RC4 не считаются криптостойкими. Есть два основных протокола WEP:40-битный WEP (длина ключа 64 бита, 24 из которых – это вектор инициализации, который передается открытым текстом);104-битный WEP (длина ключа 128 бит, 24 из которых – это тоже вектор инициализации); Вектор инициализации используется алгоритмом RC4. Увеличение длины ключа не приводит к увеличению надежности алгоритма.

Основными недостатками являются:использование для шифрования непосредственно пароля, введенного пользователем;недостаточная длина ключа шифрования;использование функции CRC32 для контроля

целостности пакетов;повторное использование векторов инициализации и др.[8]

- TKIP-шифрование (англ. Temporal Key Integrity Protocol). Используется тот же симметричный потоковый шифр RC4, но является более криптостойким. Вектор инициализации составляет 48 бит. Учтены основные атаки на WEP. Используется протокол Message Integrity Check для проверки целостности сообщений, который блокирует станцию на 60 секунд, если были посланы в течение 60 секунд два сообщения не прошедших проверку целостности. С учетом всех доработок и усовершенствований TKIP все равно не считается криптостойким.

- CKIP-шифрование (англ. Cisco Key Integrity Protocol). Имеет сходства с протоколом TKIP. Создан компанией Cisco. Используется протокол CMIC (англ. Cisco Message Integrity Check) для проверки целостности сообщений.

- WPA-шифрование. Вместо уязвимого RC4, используется криптостойкий алгоритм шифрования AES (англ. Advanced Encryption Standard). Возможно использование EAP (англ. Extensible Authentication Protocol, расширяемый протокол аутентификации). Есть два режима:Pre-Shared Key (WPA-PSK) - каждый узел вводит пароль для доступа к сети;Enterprise - проверка осуществляется серверами RADIUS.

- WPA2-шифрование (IEEE 802.11i). Принят в 2004 году, с 2006 года WPA2 должно поддерживать все выпускаемое Wi-Fi оборудование. В данном протоколе применяется RSN (англ. Robust Security Network, сеть с повышенной безопасностью). Изначально в WPA2 используется протокол CCMP (англ. Counter Mode with Cipher Block Chaining Message Authentication Code Protocol, протокол блочного шифрования с кодом аутентичности сообщения и режимом сцепления блоков и счетчика). Основой является алгоритм AES. Для совместимости со старым оборудованием имеется поддержка TKIP и EAP (англ. Extensible Authentication Protocol) с некоторыми его дополнениями. Как и в WPA есть два режима работы: Pre-Shared Key и Enterprise.

WPA и WPA2 имеют следующие преимущества:ключи шифрования генерируются во время соединения, а не распределяются статически; для контроля целостности передаваемых сообщений используется алгоритм Michael; используется вектор инициализации существенно большей длины.[8]

### 1.3 Стандарт 802.16 (WiMax)

В ближайшие годы развитие локальных беспроводных сетей пойдет по направлению массового внедрения так называемой технологии WiMAX(сокращенно от Worldwide Interoperability for Microwave Access). Сети WiMAX (стандарт IEEE 802.16a) предполагают использование частотного диапазона от 2 до 11 ГГц и обеспечивают скорость передачи данных до 70 Мбит/с на расстояние до 50 км. Пропускной способности

одной базовой станции вполне хватит для обеспечения десятков бизнес-пользователей и сотен домашних подключений.

Разработанный Институтом инженеров по электротехнике и электронике (IEEE) **Стандарт 802.16** представляет собой рассчитанную на внедрение в городских беспроводных сетях технологию, задачей которой является обеспечение сетевого уровня между локальными (IEEE 802.11) и региональными сетями (WAN), где планируется применение разрабатываемого стандарта IEEE 802.20. Эти стандарты совместно со стандартом IEEE 802.15 (PAN –Personal Area Network - Bluetooth) и 802.17 (мосты уровня MAC) образуют взаимосогласованную иерархию протоколов беспроводной связи.

*Краткие характеристики стандарта 802.16:*

- Пропускная способность до 135 Мбит/с.
- МодуляцияOFDM - 64-QAM.
- Доступ к среде адаптивный, динамический.
- Управление сетью централизованное.
- Стандарт 802.16е предназначен для мобильных систем. Безопасность в сети обеспечивается на уровне протокола 3-DES.

Таблица 1.1 – Стандарт 802.16

| Название стандарта | 802.16 | 802.16а | 802.16е |
|---|---|---|---|
| Дата принятия | Декабрь 2001 | Январь 2003 | Январь 2004 |
| Частотный диапазон | 10..66 ГГц | 2..11 ГГц | 2..6 ГГц |
| Быстродействие | 32..135 Мбит/с для 28 МГц – канала | До 75 Мбит/с для 28 МГц – канала | До 15 МбитЭс для 5 МГц – канала |
| Модуляция | 64QAM, 16QAM, QPSK | 64QAM, 16QAM, QPSK, OFDM | 64QAM, 16QAM, QPSK, OFDM |
| Ширина канала | 20, 25 и 28 МГц | Регулируемая 1,5..20 МГц | Регулируемая 1,5..20 МГц |
| Радиус действия | 2..5 км | 7..10 км макс. Радиус 50 км. | 2..5 км |
| Условия работы | Прямая видимость | Работа на отражениях | Работа на отражениях |

*Характеристики стандарта 802.16а*

- Дальность действия - до 50 км.
- Покрытие: расширенные возможности работы вне прямой видимости позволяют улучшить качество покрытия обслуживаемой зоны.
- Частота - от 2 до 11 ГГц.
- Спектральная эффективность - до 5 бит/сек/Гц.

- Максимальная скорость передачи данных на сектор одной базовой станции - до70 Мбит/с. Типовая базовая станция имеет до 6 секторов.

Структурная схема организации сети на основе стандарта 802.16представлена на рисунке 1.7.

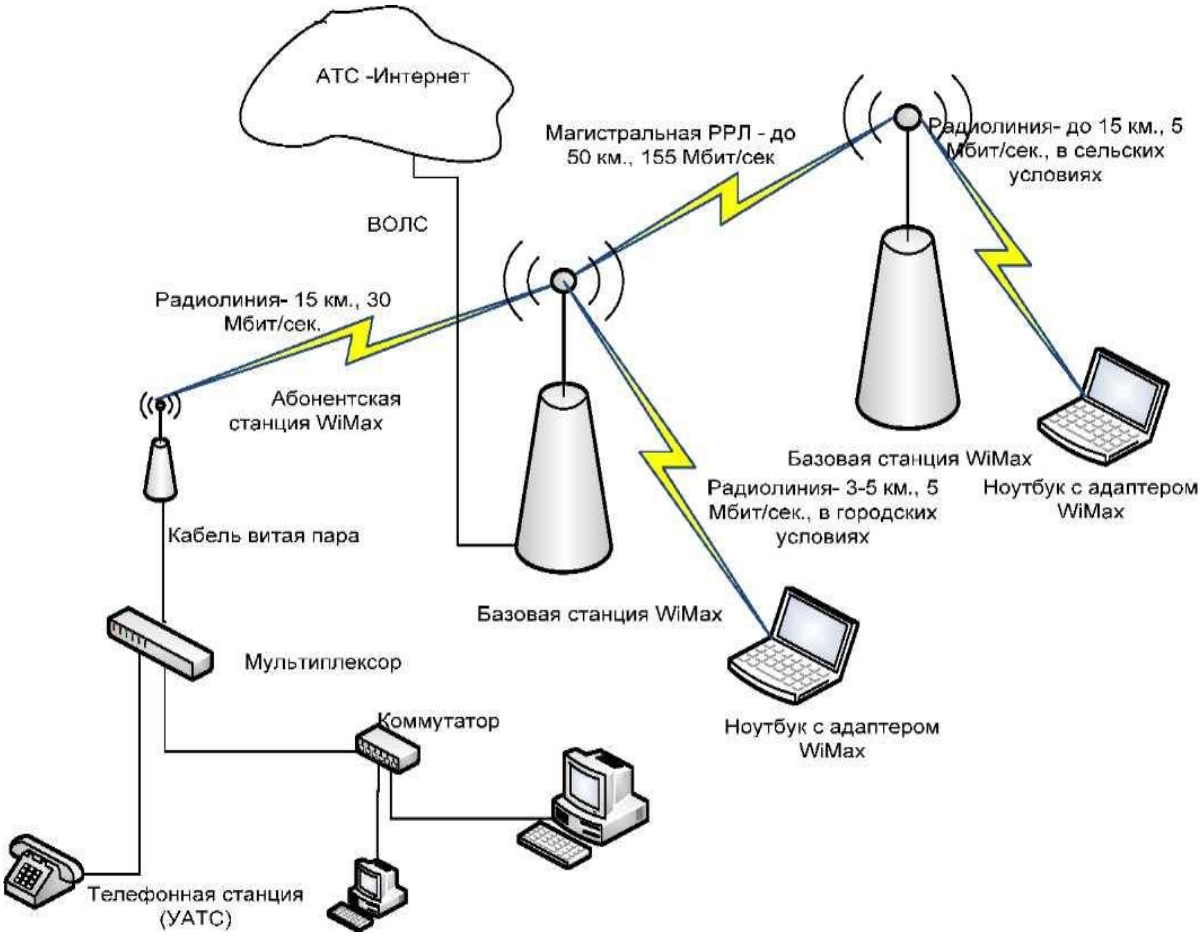


Рисунок 1.7 - Корпоративная сеть с фрагментами WiMax

Качество обслуживания контролируется на уровне управления доступом к среде, что позволяет использовать дифференцированные уровни обслуживания. Это дает возможность предоставлять коммерческим предприятиям обслуживание типа T1, а домашним пользователям - типа DSL, а также осуществлять передачу голоса и видео. Важной особенностью 802.16а является работа с отраженными радиосигналами в условиях отсутствия прямой видимости. Это достигается благодаря применению технологии OFDM для расшифровки сильно искаженного отраженного сигнала. Суть OFDM заключается в использовании большого количества узкополосных сигналов - поднесущих. Каждый из них отвечает за свой отдельный бит, а все вместе они определяют кодовое слово, в котором используются методы восстановления информации - коды Рида-Соломона вместе со сверхточным кодированием. Стандарт также допускает более гибкое по сравнению с 802.11 распределение полосы частот, используемых для передач данных. Причем это можно сделать как за счет уменьшения количества поднесущих, так и с по-

мощью их сужения. Минимальная ширина сигнала, предусмотренная стандартом, составляет 1,25 МГц, а максимальная - 20 МГц. Естественно, что с уменьшением частотного ресурса скорость передачи уменьшается, но сама эта возможность позволяет использовать частотный спектр отдельными фрагментами, а не целиком, как это было в 802.11.

Существенным отличием 802.16 от 802.11 является возможность использования протокола с разрешением конфликтов. Устройства 802.11 работают по принципам Ethernet, все они имеют равные права на доступ к радиотракту, а попытавшись одновременно установить связь, разрешают конфликты, повторяя попытки захвата среды через случайное время. В 802.16 имеется выделенное устройство - базовая станция оператора, которая раздает своим подчиненным права доступа к радиосреде. В результате протокол нового стандарта позволяет более эффективно использовать радиочастотный ресурс и обеспечить эффективную передачу данных. Причем в самом стандарте предусматриваются несколько режимов передачи - так называемых профилей. Один предназначен для пакетных данных, другой - для псевдосинхронных каналов, третий - для широковещательных передач.[5]

### 1.4 Стандарт 802.15.1 (Bluetooth)

Так называется технология обеспечения радиосвязи между мобильными и стационарными PC, мобильными телефонами, принтерами и прочими периферийными устройствами. В настоящее время технология Bluetooth является твердо устоявшимся коммуникационным стандартом для беспроводной связи на малых расстояниях. Она заменяет целую кучу отдельных кабелей, присоединяющих одно устройство к другому посредством одной универсальной радиолинии с малым радиусом действия. Например, радио технология Bluetooth, встроенная и в сотовый телефон, и в ноутбук, заменяет кабель, используемый в настоящее время для присоединения ноутбука к сотовому телефону. Принтеры, персональные компьютеры, факсы, клавиатуры, джойстики и практически любые другие цифровые устройства могут быть частью системы Bluetooth. Радио технология Bluetooth также обеспечивает универсальный мост к существующим сетям передачи данных, интерфейсу периферийных устройств, а также обеспечивает механизм для формирования небольших частных специальных групп соединяемых устройств вне инфраструктуры фиксированной сети. Серьезной соперницей Bluetooth является технология инфракрасной связи IrDA, но она не предназначена для построения беспроводных локальных сетей и работает только по принципу точка-точка в зоне прямой видимости. При разработке спецификации во главу угла ставились экономичность (как в плане стоимости, так и в плане энергосбережения), сохранение маленького форм-фактора и предельная простота эксплуатации. Для конечного пользователя это означает быстрое и легкое подключение пери-

ферии или соединение компьютеров без каких бы то ни было кабелей. К тому же технология дает возможность связать больше двух устройств, используя единое радио соединение. Общее число проданных во всем мире Bluetooth-совместимых устройств уже превысило 1 миллиард экземпляров. Спецификация стандарта Bluetooth приведена в таблице 1.2.

Таблица 1.2 - Спецификация стандарта Bluetooth и IrDA

| **Параметры** | **Bluetooth** | **IrDA** |
|---|---|---|
| Тип модуляции | метод частотных скачков | Амплитудная |
| Частотный диапазон | 2,4 ГГц | излучение в оптическом диапазоне 850...900 нм |
| Число скачков в секунду | 1600 | |
| Мощность передатчика, мВт | 100 | 20…80 |
| Скорость передачи данных, Мбит/с | 24 | 4 |
| Способ модуляции | двухуровневая частотная | двухуровневая импульсная |
| Количество устройств в сети | Не ограничено | 2 |
| Защита информации | 40- и 64- битное шифрование | Нет |
| Радиус действия, м | 10…100 | 1 |

Проект являлся конкурентом стандарта IEEE 802.11 (оба стандарта используют один и тот же частотный диапазон, одни и те же 79 каналов). Главной его целью являлось удаление любых кабелей из телефонии, а если получится - и из локальных сетей. Технология Bluetooth использует нелицензируемый (практически везде кроме России) частотный диапазон 2,4...2,4835 ГГц. При этом используются широкие защитные полосы: нижняя граница частотного диапазона составляет 2 ГГц, а верхняя -3,5 ГГц. Точность заданий частоты (положение центра спектра) устанавливается с точностью ± 75 кГц. Дрейф частоты в этот интервал не входит. Кодирование сигнала осуществляется по двухуровневой схеме **GFSK**(Gaussian Frequency Shift Keying). Логическому 0 и 1 соответствуют две разные частоты. В оговоренной частотной полосе выделяется 79 радиоканалов по 1 МГц каждый. В некоторых странах используется меньшее число каналов (например, во Франции - 23). Каждый из каналов структурируется с помощью выделения временных слотов (доменов) длительностью 625 мкс (разделение по времени). По мощности передатчики делятся на три класса: 100 мВт (для связи до 100 м; 20 дБм); 2 мВт (до 10 м; 4 дБм) и 1 мВт (~10 см; 0 дБм). Коэффициент модуляции при этом лежит в диапазоне (0,28...0,35). Чувствительность приемника должна быть не хуже 70 дБм.

BER (Bit Error Rate) для приемника должна находиться на уровне <0,1 %. Желательно, чтобы приемник имел индикатор мощности входного сигнала (требование является опционным). Для первого класса предусмотрено регулирование мощности, которое осуществляется на основе анализа числа ошибок. Протокол использует коммутацию каналов и пакетов. Передача данных выполняется с использованием алгоритма доступа **Time-Division Duplex Multiple Access.** Каждый пакет передается с использованием иного частотного канала по отношению к предыдущему. Производится 1600 переключений частоты в секунду. Последовательность переключения частот определяется BD_ADDR мастера. Скачкообразное переключение частоты отводит на переходные процессы 250.. .260 мкс. Длительность тика часов мастера равна 312,5 мкс, что определяет частоту часов - 3,2 кГц. Допускается временная неопределенность при приеме, равная ±20 мкс. Структура протоколов Bluetooth не следует моделям OSI, TCP/IP и даже 802 (ведутся работы по адаптации Bluetooth к модели IEEE 802). Физический уровень протокола соответствует базовым принципам моделей OSI и 802. Разработчики потратили много усилий, чтобы сделать протокол как можно дешевле для реализации. В среднем временная привязка мастерных пакетов не должна дрейфовать больше чем на 20 $10^{-6}$ относительно идеальной временной привязки слота в 625 мкс. Временной разброс при этом не должен превышать 1 мкс. В спецификации определено 5 уровней: физический, базовый (baseband), управления каналом **LMP**(Link Management Protocol) и **L2CAP**(Logical Link Control and Adaptation Protocol), сетевой и уровень приложений. На базовом уровне протокола определено 13 типов пакетов. Пакеты ID, NULL, POLL, FHS , DM1 ориентированы на каналы SCO и ACL. Пакеты DH1, AUX1, DM3, DH3, DM5 и DH5 предназначены только для каналов ACL. Кодирование данных в пакетах DM1, DM2 и DM3 осуществляется с привлечением битов четности по алгоритму FEC 2/3 (5 бит управления на 10 бит данных). Форматы пакетов HV1, HV2, HV3 и DV определены только для каналов SCO. Максимальный размер поля данных (341 байт) имеют пакеты DH5. Уровень протокола baseband специфицирует пять логических каналов: **LC**(Control Channel) и **LM**(Link Manager) используются на канальном уровне, а **UA**(User Asynchronous), **UI**(User Isosynchronous) и **US**(User Synchronous) служат для асинхронной, изосинхронной и синхронной транспортировки пользовательских данных. Предусмотрено семь субсостояний, которые используются для добавления клиента или подключения к пикосети: **page, pagescan, inquiry, inquiry scan, master response, slave response** и **inquiry response.**Состояние Standby по умолчанию является режимом с пониженным энергопотреблением, при этом работает только внутренний задающий генератор. В состоянии соединения главный узел (master) и клиент (slave) могут обмениваться пакетами, используя код доступа к каналу.[5]

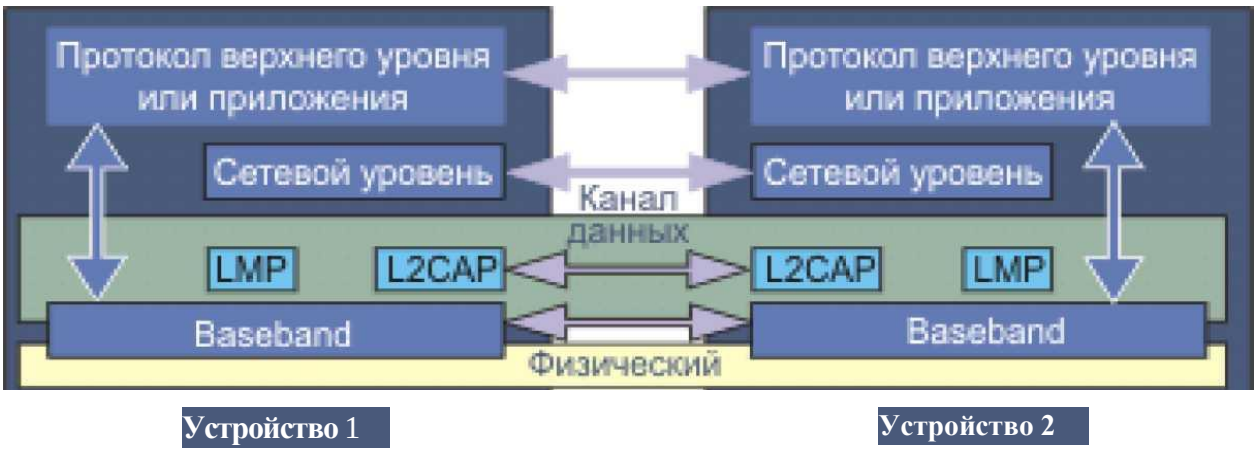


Рисунок 1.8 - Взаимодействие сетевых субуровней в протоколе

В протоколе baseband предусмотрено три типа схем коррекции ошибок: 1/3 FEC, 2/3 FEC и ARQ. В 1/3 FEC каждый бит повторяется три раза.
В 2/3 FEC используется полиномиальный генератор для получения 15-битовых кодов для исходных 10 бит.

В схеме ARQ пакеты DM, DH и поле данных пакета DV передаются повторно до тех пор, пока не будет получено подтверждение или не произойдет тайм-аут. При тайм-ауте возможно продолжение со следующего пакета.

Протоколом baseband рекомендуется использование буферов типа FIFO. Если данные не могут быть приняты, контроллер приема (Link Controller) вставляет в заголовок отклика индикатор **stop.**Когда передатчик получает индикатор stop, он блокирует очереди в FIFO. Получатель может возобновить процесс передачи, послав отправителю индикатор **go.**Взаимодействие протоколов в рамках Bluetooth показано на рисунке 1.8.[10]

### 1.5 Стандарт 802.15.4 (ZigBee)

ZigBee — стандарт для набора высокоуровневых протоколов связи, использующих небольшие, маломощные цифровые трансиверы, основанный на стандарте IEEE 802.15.4-2006 для беспроводных персональных сетей, таких как, например, беспроводные наушники, соединённые с мобильными телефонами посредством радиоволн коротковолнового диапазона. Технология определяется спецификацией ZigBee, разработанной с намерением быть проще и дешевле, чем остальные персональные сети, такие как Bluetooth. ZigBee предназначен для радиочастотных устройств, где необходима длительная работа от батареек и безопасность передачи данных по сети.

Альянс ZigBee является органом, обеспечивающим и публикующим стандарты ZigBee, он также публикует профили приложений, что позволяет

производителям изначальной комплектации создавать совместимые продукты. Текущий список профилей приложений, опубликованных, или уже находящихся в работе:

- Домашняя автоматизация
- Рациональное использование энергии (ZigBee Smart Energy 1.0/2.0)
- Автоматизация коммерческого строительства
- Телекоммуникационные приложения
- Персональный, домашний и больничный уход
- Игрушки

Сотрудничество между IEEE 802.15.4 и ZigBee подобно тому, что было между IEEE 802.11 и альянсом Wi-Fi. Спецификация ZigBee 1.0 была ратифицирована 14 декабря 2004 и доступна для членов альянса ZigBee. Сравнительно недавно, 30 октября 2007 г., была размещена спецификация ZigBee 2007. О первом профиле приложения — «Домашняя автоматизация» ZigBee, было объявлено 2 ноября 2007. ZigBee работает в промышленных, научных и медицинских (ISM-диапазон) радиодиапазонах: 868 МГц в Европе, 915 МГц в США и в Австралии, и 2.4 ГГц в большинстве стран в мире (под большинством юрисдикций стран мира). Как правило, в продаже имеются чипы ZigBee, являющиеся объединёнными радио- и микроконтроллерами с размером Flash-памяти от 60К до 128К таких производителей, как Jennic JN5148, Freescale MC13213, Ember EM250, Texas Instruments CC2430, Samsung Electro-Mechanics ZBS240 и Atmel ATmega128RFA1. Радиомодуль также можно использовать отдельно с любым процессором и микроконтроллером. Как правило, производители радиомодулей предлагают также стек программного обеспечения ZigBee, хотя доступны и другие независимые стеки.

Так как ZigBee может активироваться (то есть переходить от спящего режима к активному) за 15 миллисекунд или меньше, задержка отклика устройства может быть очень низкой, особенно по сравнению с Bluetooth, для которого задержка, образующаяся при переходе от спящего режима к активному, обычно достигает трёх секунд. Так как ZigBee большую часть времени находится в спящем режиме, уровень потребления энергии может быть очень низким, благодаря чему достигается длительная работа от батарей.

Первый выпуск стека сейчас известен под названием ZigBee 2004. Второй выпуск стека называется ZigBee 2006, и, в основном, заменяет структуру MSG/KVP, использующуюся в ZigBee 2004 вместе с «библиотекой кластеров». Стек 2004 года сейчас более или менее вышел из употребления. Реализация ZigBee 2007 в настоящее время является текущей, она содержит два профиля стека, профиль стека № 1 (который называют просто ZigBee) для домашнего и мелкого коммерческого использования, и профиль стека № 2 (который называют ZigBee Pro). ZigBee Pro предлагает больше функций, таких как широковещание, маршрутизацию вида «многие-к-одному» и высокую безопасность с использованием симметричного ключа

(SKKE), в то время как ZigBee (профиль стека № 1) занимает меньше места в оперативной и Flash-памяти. Оба профиля позволяют развернуть полномасштабную сеть с ячеистой топологией и работают со всеми профилями приложений ZigBee.

ZigBee 2007 полностью совместим с устройствами ZigBee 2006. Устройство ZigBee 2007 может подключаться и работать с сетью ZigBee 2006, и наоборот. В связи с наличием различий в опциях маршрутизации, устройства ZigBee Pro могут быть только конечными устройствами (ZEDs) сетей ZigBee 2006, и наоборот, устройства ZigBee 2006 и ZigBee 2007 могут быть только конечными устройствами в сети ZigBee Pro. При этом приложения, которые запускаются на устройствах, работают одинаково, независимо от реализации профиля стека.

Основными областями применения технологии ZigBee являются беспроводные сенсорные сети, автоматизация жилья («Умный дом» и «Интеллектуальное здание»), медицинское оборудование, системы промышленного мониторинга и управления, а также бытовая электроника и «периферия» персональных компьютеров.

Способность к самоорганизации и самовосстановлению, ячеистая (mesh-) топология, защищённость, высокая помехоустойчивость, низкое энергопотребление и отсутствие необходимости получения частотного разрешения делают ZigBee-сеть подходящей основой для беспроводной инфраструктуры систем позиционирования в режиме реального времени (RTLS).

Протоколы ZigBee разработаны для использования во встроенных приложениях, требующих низкую скорость передачи данных и низкое энергопотребление. Цель ZigBee — это создание недорогой, самоорганизующейся сети с ячеистой топологией предназначенной для решения широкого круга задач. Сеть может использоваться в промышленном контроле, встроенных датчиках, сборе медицинских данных, оповещении о вторжении или задымлении, строительной и домашней автоматизации и т. д. Созданная в итоге сеть потребляет очень мало энергии — индивидуальные устройства согласно данным сертификации ZigBee позволяют энергобатареям работать два года.[10]

Типовые области приложения:

- Домашние развлечения и контроль — рациональное освещение, продвинутый температурный контроль, охрана и безопасность, фильмы и музыка.

- Домашнее оповещение — датчики воды и энергии, мониторинг энергии, датчики задымления и пожара, рациональные датчики доступа и переговоров.

- Мобильные службы — мобильные оплата, мониторинг и контроль, охрана и контроль доступа, охрана здоровья и телепомощь.

- Коммерческое строительство — мониторинг энергии, HVAC, света, контроль доступа.

- Промышленное оборудование — контроль процессов, промышленных устройств, управление энергией и имуществом.

Существуют три различных типа устройств ZigBee:

- Координатор ZigBee (ZC) — наиболее ответственное устройство, формирует пути древа сети и может связываться с другими сетями. В каждой сети есть один координатор ZigBee. Он и запускает сеть от начала. Он может хранить информацию о сети, включая хранилище секретных паролей производства компании Trust Centre.

- Маршрутизатор ZigBee (ZR) — Маршрутизатор может выступать в качестве промежуточного маршрутизатора, передавая данные с других устройств. Он также может запускать функцию приложения.

- Конечное устройство ZigBee (ZED) — его функциональная нагруженность позволяет ему обмениваться информацией с материнским узлом (или координатором, или с маршрутизатором), он не может передавать данные с других устройств. Такое отношение позволяет узлу львиную часть времени пребывать в спящем состоянии, что позволяет экономить энергоресурс батарей. ZED требует минимальное количество памяти, и поэтому может быть дешевле в производстве, чем ZR или ZC.[5]

### 1.6“Световая точность” Li–Fi

"Li-Fi" - это новая технология (аббревиатура в названии составлена, по аналогии с широко известными Hi-fi и Wi-Fi, из английских слов "light" - "свет" и "fidelity" - "точность"), обещающая надежный и дешевый способ подключения к интернету практически из любого места с помощью специальных светодиодов.[18]

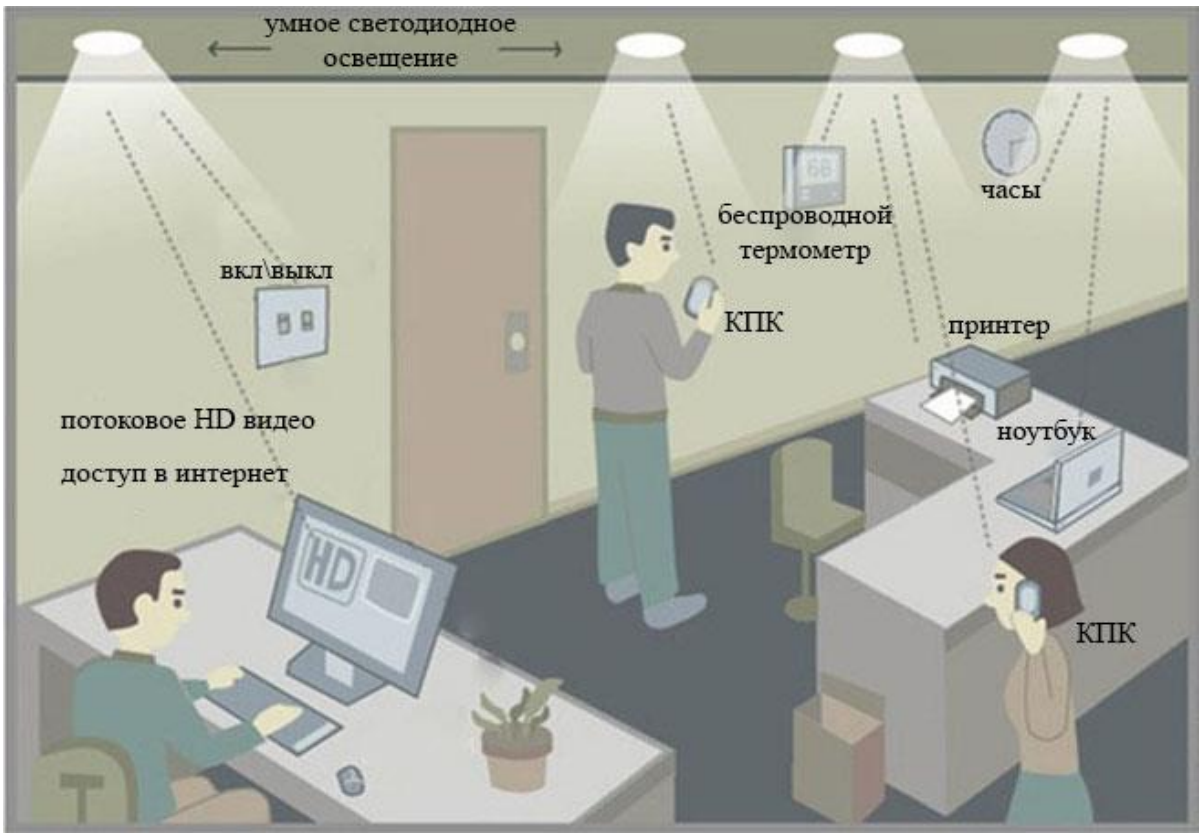


Рисунок 1.9 - Пример Li-Fi сети в офисе

Проект изучения передачи данных с помощью так называемого ультрапараллельного видимого света был инициирован университетами Эдинбурга, Оксфорда и Кэмбриджа и финансируется британским Советом по исследованиям в области инженерных и физических наук.

Крошечные микросветодиоды, разработанные в Университете Стратклайд в Глазго, испускают параллельные потоки света, умножая таким образом количество данных, которое может быть передано за единицу времени.

"Представьте себе головку душа, которая направляет воду строго параллельными струями, - а мы таким же образом заставили вести себя свет", - объясняет профессор Харальд Хаас, специалист по оптической беспроводной передаче данных университета Эдинбурга и один из инициаторов проекта.

Профессор Харальд Хаас занимается разработкой новой технологии уже десять лет.Метод цифровой модуляции, называемый ортогональным частотным разделением каналов (OFDM), позволил ученым использовать микросветодиоды для передачи миллионов пучков света разной интенсивности в секунду. Говоря проще, лампы включаются и выключаются - но с бешеной скоростью.

Из этих включений-выключений складываются огромные массивы бинарных данных, цепочки единиц и нулей, передаваемые с высокой скоростью.

Ранее в этом году немецкие ученые из Фраунгоферовского института Генриха Герца заявляли, что в лабораторных условиях способны достичь скорости передачи данных с помощью светодиодов в 1 Гбит в секунду.

В октябре китайские исследователи сообщили, что построили светодиод на микрочипе со скоростью в 150 Мбит в секунду, обеспечивающий подключение к интернету сразу четырем компьютерам.[18]


Рисунок 1.10 -ПреимуществаLi-Fi

Профессор Харальд Хаас занимается разработкой "Li-Fi" уже десять лет. Научным языком эта технология называется "передачей данных видимым светом", или сокращенно VLC ("visual light communication").

В 2011 году Хаас продемонстрировал, что светодиодная лампа, оснащенная технологией обработки сигнала, может передавать на компьютер видеоизображение высокой четкости ("high-definition").Он же и придумал

более звучное название для технологии VLC - "light fidelity" или просто "Li-Fi".[19]

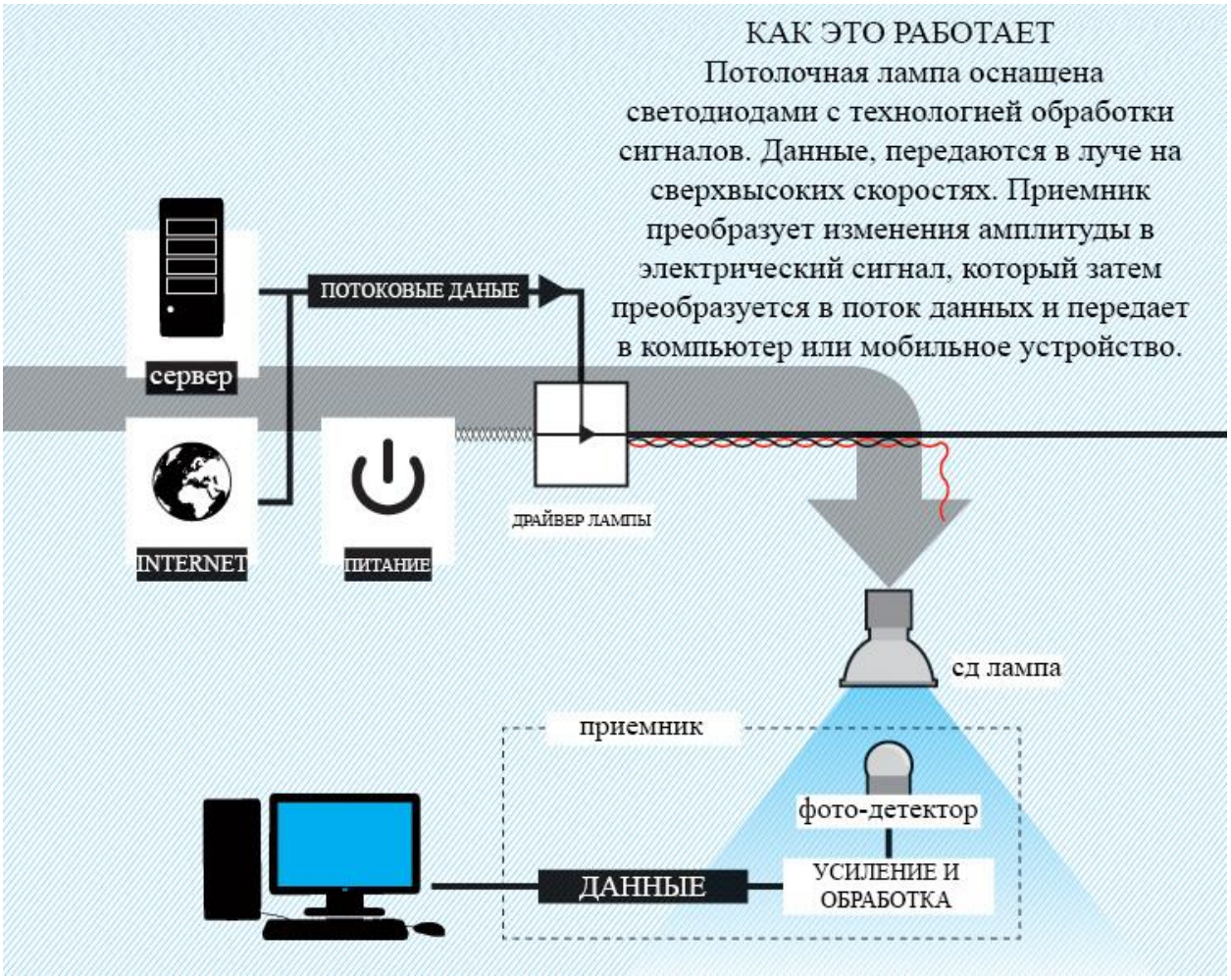


Рисунок 1.11–Как работает Li-Fi

"Li-Fi" обещает стать более дешевым и энергоэффективным методом передачи данных, чем существующие беспроводные радиосистемы, учитывая доступность и повсеместное распространение светодиодов.

Видимый свет - часть электромагнитного спектра, в 10 тысяч раз более широкая, чем спектр радиоизлучения. Потенциально свет может обеспечить практически неограниченную широту канала передачи данных.

По мнению профессора Хааса, еще одно преимущество новой технологии заключается в том, что при равномерном распределении светодиодных передатчиков можно достичь гораздо более точного и стабильного подключения к интернету внутри зданий.

Недостатком традиционных Wi-Fi-роутеров всегда было то, что сигнал слабеет по мере удаления от передатчика, и в домах и офисах появляются зоны, где связь слабая настолько, что подсоединение к интернету становится нестабильным или вовсе прерывается.

Кроме того, видимый свет не проходит сквозь стены, поэтому технология VLC потенциально более надежна, чем традиционный Wi-Fi, с

точки зренияохранения конфиденциальности передачи данных, подчеркивает профессор Хаас.[20]

Т а б л и ц а 1 . 3 – Сравнение технологий Wi-Fiи Li-Fi

| Параметры | Li-Fi | Wi-Fi |
|---|---|---|
| Скорость | * * * | * * * |
| Зона покрытия | * | * * |
| Плотность потока данных | * * * | * |
| Безопасность | * * * | * * |
| Надежность | * * | * * |
| Доступная мощность | * * * | * |
| Мощность на прием/передачу | * * * | * * |
| Воздействие на экологию | * | * * |
| Взаимодействие между устройствами | * * * | * * * |
| Влияние препятствий | * * * | * |
| Спецификация | * * * | * * |
| Рыночная готовность | * | * * * |
| * низкое * * среднее * * * высокое | | |

## 2 Расчетная часть

### 2.1 Модели распространения сигнала

Существуют эмпирические и теоретические (расчетные) модели распространения сигнала. Среди эмпирических моделей можно выделить 2 группы:

- Статистические моделитребуют только общего описания типа здания.

- Одно или многолучевые моделиоценивают уровень принимаемого сигнала и основаны на учете потерь на всех препятствиях на пути прохождения сигнала.

Модели, выражают величину потери мощности сигнала в произвольной точке. Для этого необходимо определить потерю мощности при идеальных условиях- отсутствии препятствий, отражений, и без учета наличия нескольких возможных траекторий передачи сигнала, описывается по формуле Фрииса:

$$\frac{Pr}{Pt} = Gt * Gr\left(\frac{\lambda}{4\pi d}\right)^2 > \quad (2.1)$$

$$d = \frac{\sqrt{Pt*Gt*Gr*\lambda^2}}{Pr*16\pi^2} \quad (2.2)$$

гдеd- расстояние в метрах между передающей и принимающей антенной.

Pt- мощность передающей антенны нарасстояние d;

Pr- мощность принимаемая антенной;

Gt- КУ передающей антенны;

Gr- КУ принимаемая антенн;

**λ**– длинна волны.

Формула 2.1выраженная в децибелах, прикоэффициентах усиления, равных единице:

$$L = 10\log(\frac{Pr}{Pt}) \quad (2.3)$$

Из формулы 2.2 вычислим потерю мощности сигнала в свободном пространстве:

$$L_{FS} = 32.45 + 20\log(d) + 20\log(f) \quad (2.4)$$

При условии измерении расстояния в километрах, а частоты в мегагерцах.

Расчет выполнен в программе Mathcad, смотрите Приложение ГРасчет

потерь Wi-Fiсигнала.

Статистическая модель OneSlopeописывает зависимость увеличения потери мощности сигнала с расстоянием, с усредненным учетом препятствий:

$$L(d) = L_{FS} + 10n\log(d/d_0) \quad (2.5)$$

где $d_0$=1 м.

$L_{FS}$- потери в свободном пространстве на расстояние $d_0$.

n- коэффициент, зависящий от типа помещений, количества препятствий и их материала.

Статистическая модель DualSlope учитывает отличия потери мощности сигнала на дальних и ближних расстояниях. В ней появилось разделение между приемником и передатчиком на 2 зоны точки разрыва $d_{BR}$- ближнюю и дальнюю:

$$L_1(d) = 10n_1\log(\mathrm{d}/d_{BR}) + L_{BR}\mathrm{d}<d_{BR} \quad (2.6)$$

$$L_2(d) = 10n_2\log(\mathrm{d}/d_{BR}) + L_{BR}\mathrm{d}>d_{BR} \quad (2.7)$$

где n1и 2- коэффициенты уменьшения мощности на промежутке до и после $d_{BR}$. Как правило принимают равным 2 и 6 соответственно.

$L_{BR}$- значение потери мощности сигнала в точке разрыва.

Статистическая модель Log-distance аналогична модели OneSlope,но добавляет к потере мощности сигнала случайную величину X:

$$L(d) = L_{FS} + 10n\log(d/d_0)+\mathrm{X} \quad (2.8)$$

FSL (Free Space Loss) - потери в свободном пространстве (дБ); F- центральная частота канала, на котором работает система связи (МГц); D - расстояние между двумя точками (км).

FSL определяется суммарным усилением системы. Оно считается следующим образом:

$$Y_{\text{дБ}} = P_{t,\text{дБмВт}} + G_{t,\text{дБ}u} + G_{\text{т,дБ}u} - P_{min,\text{дБмВт}} - L_{t,\text{дБ}} - L_{\text{т,дБ}}\ , \quad (2.9)$$

где$P_{t,\text{дБмВт}}$ - мощность передатчика;

$G_{t,\text{дБ}u}$ - коэффициент усиления передающей антенны;

$G_{\text{т,дБ}u}$ - коэффициент усиления приемной антенны;

$P_{min,\text{дБмВт}}$ - чувствительность приемника на данной скорости;

$L_{t,\text{дБ}}$- потери сигнала в коаксиальном кабеле передающего тракта;

$L_{т,дБ}$ - потери сигнала в коаксиальном кабеле приемного тракта.

Таблица 2.1 -Чувствительностьот скорости передачи

| Скорость | Чувствительность |
|---|---|
| 54 Мбит/с | -66 дБмВт |
| 48 Мбит/с | -71 дБмВт |
| 36 Мбит/с | -76 дБмВт |
| 24 Мбит/с | -80 дБмВт |
| 18 Мбит/с | -83 дБмВт |
| 12 Мбит/с | -85 дБмВт |
| 9 Мбит/с | -86 дБмВт |
| 6 Мбит/с | -87 дБмВт |

Для каждой скорости приемник имеет определенную чувствительность. Для небольших скоростей (например, 1-2 Мегабита) чувствительность наименьшая: от -90 дБмВт до -94 дБмВт. Для высоких скоростей чувствительность намного выше. В качестве примера в таблице выше приведены несколько характеристик обычных точек доступа 802.11a,b,g.

FSL вычисляется по формуле:

$$FSL = Y_{дБ} - SOM \qquad (2.10)$$

где SOM(System Operating Margin) - запас в энергетике радиосвязи (дБ). Учитывает возможные факторы, отрицательно влияющие на дальность связи, такие как:

- температурный дрейф чувствительности приемника и выходной мощности передатчика;
- всевозможные атмосферные явления: туман, снег, дождь;
- рассогласование антенны, приемника, передатчика с антенно-фидерным трактом.

Параметр SOM обычно берется равным 10 дБ. Считается, что 10-децибельный запас по усилению достаточен для инженерного расчета.

Центральная частота канала F берется из таблицы 2.2:

Т а б л и ц а 2 . 2 –Центральные частоты каналов

| Канал | Центральная частота (МГц) |
|---|---|
| 1 | 2412 |
| 2 | 2417 |
| 3 | 2422 |
| 4 | 2427 |
| 5 | 2432 |
| 6 | 2437 |
| 7 | 2442 |
| 8 | 2447 |
| 9 | 2452 |
| 10 | 2457 |
| 11 | 2462 |
| 12 | 2467 |
| 13 | 2472 |
| 14 | 2484 |

В итоге получим формулу дальности связи:

$$D = 10^{(\frac{FSL}{20} - \frac{33}{20} - lgF)} \quad (2.11)$$

Пользуясь всеми вышеперечисленными данными можно рассчитать дальность Wi-Fi сигнала.

## 3 Бизнес-план

### 3.1 Цель и задача проекта

Ежедневное развитие технологий в сфере телекоммуникаций вынуждает провайдеров и производителей оборудования искать новые способы организации и предоставления услуг, а так же повышать уровень сервиса уже существующих технологий на более высокий уровень с меньшими затратами.

В связи с этим активно растет популярность широкополосного доступа с помощью беспроводных технологий. Беспроводные технологии получают все большее распространение в нашей жизни и на то есть свои доводы.

Беспроводные технологии более экономичны по сравнению с проводными. Нет необходимости тянуть провода к каждому компьютеру или устройству. Беспроводная технология Wi-Fi позволяет покрыть малый офис или небольшой участок одной точкой доступа. Так же технология Wi-Fi позволяет просто и быстро развернуть компьютерную сеть, легко увеличить размерность сети добавив новые точки доступа. Все это позволяет с меньшими трудовыми и временными затратами развернуть сеть.

Внедрение технологии Wi-Fi позволит операторам уменьшить капитальные и операционные затраты, снизить совокупную стоимость владения сетью, расширить спектр услуг, связанных с передачей данных по высокоскоростным каналам. С абонентской точки зрения, резкое увеличение скорости передачи данных серьезно улучшит качество предоставляемых услуг, что, в свою очередь, будет способствовать распространению новых платных мультимедийных сервисов (многопользовательских игр, социальных сетей, видеоконференций, систем мониторинга, интерактивных онлайн-приложений и др.).

### 3.2 Обоснование выбора и состава оборудования

На сегодняшний день рынок оборудования беспроводного доступа представлен большим разнообразием производителей. Выбор того или иного производителя должен проводится с учетом множества факторов, основные из них это: годность оборудования для реализации данного проекта, используемая технология, совместимость с другим оборудованием, стоимость оборудования. При сравнении различных систем радио доступа большое преимущество имеет продукция фирмы Linksys. Linksys - в своём классе предлагает лучшие решения для беспроводных ЛВС:

- Безопасность;
- Расширяемость;
- Управление;
- Продвинутые возможности;
- Высочайшая скорость;

- Масштабируемость;

Решение Linksys создает отдельные полностью беспроводные сети, обеспечивая мобильность пользователей и увеличивая их продуктивность быстро и экономически эффективно. Решение основано на беспроводных продуктах стандартов IEEE 802.11b/g/n, предназначенных для организации связи в пределах здания.

Оборудование Linksysвыделяется своей устойчивой связью и стабильной пропускной способностью.

Для реализации данного проекта потребуется использовать различное оборудование. Перечень и краткое описание применения оборудования с соответствующими стоимостными показателями приведены ниже.

### 3.3 Расчет капитальных затрат беспроводной сети

Стоимость оборудования, необходимого для построения сети Wi-Fi, указана в таблице 3.1.

Т а б л и ц а 3.1 – Стоимость оборудования

| Наименование оборудования | Количество, шт | Цена за единицу, тенге | Общая цена, тенге |
|---|---|---|---|
| МаршрутизаторLinksys Smart Wi-Fi Router EA2700 | 2 | 21950 | 43 900 |
| ПКНР D1V57EA | 13 | 103 595 | 1346735 |
| Беспроводная точка доступа Linksys WAP300N | 4 | 16 700 | 66 800 |
| Прочие затраты | | | 90000 |
| Итого | | | 1547435 |

Капитальные затраты определим по формуле:

$$K = Ц + K_{мон} + K_{пер} \tag{3.1}$$

где Ц – цена системы (Ц =1547 435тг.)

$К_{мон}$ – стоимость монтажа на месте составляет 5% от цены системы:

$$К_{мон} = Ц \times 0{,}05 \tag{3.2}$$

$К_{мон}$ = 1547435×0,05 =77 372тг.;

$К_{пер}$– стоимость перевозки к месту эксплуатации составляет 2% от цены системы:

$$К_{пер} = Ц \times 0,02 \quad (3.3)$$

$К_{пер}$ = 1547435×0,02 =30949 тг.;
Тогда капитальные затраты составят:
К = 1547435 + 77372 + 30949 =1655 756тг.

Эксплуатационные расходы определяются по формуле:

$$Эр = ФОТ + Ос + Ао + М + Эл + З_{аренд} + М + Н \quad (3.4)$$

где ФОТ – фонд оплаты труда;
Ос – отчисления на социальные нужды (социальный налог);
Ао – амортизационные отчисления;
М – затраты на материалы и запасные части;
Эл – затраты на электроэнергию;
Ппр- прочие производственные и транспортные расходы;
Н – накладные расходы;

Для вычисления ФОТ приведем среднемесячную заработную плату работников, которую сведем в таблицу 3.2.

Т а б л и ц а 3.2 – Среднемесячные оклады работников обслуживания сети Wi-Fi

| Наименованиедолжностей | Месячная заработная плата, $ЗП_i$ (тг.) | Числоработников, n (чел.) | Итого месячная зар. плата,тыстг. |
|---|---|---|---|
| Ведущий инженер | 80000 | 1 | 80 |
| Инженер оператор | 75000 | 1 | 75 |
| Итого | | 2 | 155 |

Фонд оплаты труда состоит из основной ($ЗП_{осн}$и дополнительной ($ЗП_{доп}$) заработной платы персонала, обслуживающего прибор (устройство или систему) или объект связи, а также директора предприятия, менеджера по рекламе и юриста и премиальных выплат:

$$ФОТ = ЗП_{осн} + ЗП_{доп} + П, \quad (3.5)$$

Основная заработная плата за год рассчитывается по формуле:

$$ЗП_{осн.} = 12 \cdot \sum_{i=1}^{n} ЗП_i \quad (3.6)$$

где $ЗП_i$ – месячная заработная плата i-того работника;

n – число работников.

$ЗП_{осн}$ = 12×155000=1860 000 тг.

Дополнительная заработная плата (работа в праздничные дни, сверхурочные работы и т.п.) составляет 30% от основной заработной платы работников:

$$ЗП_{доп} = ЗП_{осн} \times 0,3 \quad (3.7)$$

$ЗП_{доп}$ = 1860 000× 0,3 = 558 000 тг.

Премиальные выплаты, входящие в ФОТ, составляют 15% от основной заработной платы:

$$П = ЗП_{осн.} \times 0,15 \quad (3.8)$$

П =155000×0,15 =23 500тг.

Таким образом, ФОТ составляет:

ФОТ =1860 000 + 558 000+ 23500= 2441 500тг.

Отчисления на социальные нужды составляют 11% от фонда оплаты труда, пенсионные отчисления составляют 10% от фонда оплаты труда, так как не облагаются социальным налогом:

$$Ос = 0,11 \times (ФОТ \times 0,9) \quad (3.9)$$

Ос =0,11 ×2441500×0,9 =241 708тг.

Амортизационные отчисления на предприятиях связи составляют 15-25% от основных производственных фондов. В данном случае амортизационные отчисления составляют 25% от стоимости оборудования:

$$Ао = Ц \times 0,25 \quad (3.10)$$

Ао = 1547435×0,25 = 386 859тг.

Затраты на электроэнергию можно рассчитать по следующей формуле:

$$Эл = W \times T \times S \quad (3.11)$$

где W – потребляемая мощность оборудования (W = 2 кВт);

T – количество часов работы оборудования (T = 8760 ч.);

S – стоимость киловатт-часа электроэнергии (S = 19,29тг/кВТ·ч);

Тогда

Эл = 2×8760×19,29 = 337961 тг.

Прочие производственные и транспортные расходы определяются укрупнено в размере 35% от фонда заработной платы

$$Ппр=Нпр*ФОТ, \quad (3.12)$$

где Нпр - норматив прочих произв. и трансп. расходов.
Ппр=0,35*2441500=854525 тг

М – материальные затраты, запасные части - 0.5% капитальных затрат

М=1547435×0.005=7737 тг.

Н – накладные расходы (косвенные расходы, куда входят неучтенные расходы) – это 50 % от себестоимости.

Н=(2441500+241708+ 386859+337961+854525+7737)*0,50=2135145 тг.

Исходя из выше рассчитанных данных, годовые эксплуатационные расходы составят:

Эр =2441500+241708+386 859+337961+854525+7737+2 135145= 6405435 тг.

Т а б л и ц а 3.3 - Годовые эксплуатационные расходы

| Наименование статей затрат | Расчетные данные |
|---|---|
| Эксплуатационные расходы, тг. | 6405435 |
| В том числе: | |
| Фонд оплаты труда, тг. | 2 441500 |
| Отчисления на социальные нужды, тг | 241708 |
| Амортизационные отчисления, тг. | 386859 |
| Затраты на электроэнергию, тг. | 337961 |
| Прочие производственные и транспортные расходы, тг. | 854525 |
| Материальные затраты, запасные части, тг. | 7737 |
| Накладные расходы, тг. | 2135145 |

### 3.4 Расчет капитальных затрат проводной сети

Стоимость оборудования, необходимого для построенияEthernet сети, указана в таблице 3.4.

Т а б л и ц а 3.4 – Стоимость оборудования

| Наименование оборудования | Количество, шт | Цена за единицу, тенге | Общая цена, тенге |
|---|---|---|---|
| Маршрутизатор LinkSys RVS4000-EU | 2 | 32 330 | 64 660 |
| ПКНР D1V57EA | 13 | 103 595 | 1346735 |
| Коммутатор LinkSys SD-208 | 2 | 6257 | 12514 |
| Прочие затраты | | | 200000 |
| Итого | | | 1 623 849 |

Капитальные затраты определим по формуле:

$$K = Ц + K_{мон} + K_{пер} \tag{3.13}$$

где Ц – цена системы (Ц =1 623 849тг.)

$К_{мон}$ – стоимость монтажа на месте составляет 10% от цены системы:

$$К_{мон} = Ц \times 0,1 \tag{3.14}$$

$К_{мон}$ = 1 623 849×0,1 =162 385тг.;

$К_{пер}$– стоимость перевозки к месту эксплуатации составляет 2% от цены системы:

$$К_{пер} = Ц \times 0,02 \tag{3.15}$$

$К_{пер}$ = 1 623 849×0,02 =32 477 тг.;

Тогда капитальные затраты составят:

К = 1 623 849 + 162 385 + 32 477 =1 818 711тг.

Эксплуатационные расходы определяются по формуле:

$$Эр = ФОТ + Ос + Ао + М + Эл + З_{аренд} + М + Н \tag{3.16}$$

где ФОТ – фонд оплаты труда;

Ос – отчисления на социальные нужды (социальный налог);

Ао – амортизационные отчисления;

М – затраты на материалы и запасные части;

Эл – затраты на электроэнергию;

Ппр- прочие производственные и транспортные расходы;
Н – накладные расходы

Для вычисления ФОТ приведем среднемесячную заработную плату работников, которую сведем в таблицу 3.5.

Т а б л и ц а 3.5 – Среднемесячные оклады работников обслуживания сети Wi-Fi

| Наименованиедолжностей | Месячная заработная плата, $ЗП_i$ (тг.) | Числоработников, n (чел.) | Итого месячная зар. плата,тыстг. |
|---|---|---|---|
| Ведущий инженер | 80000 | 1 | 80 |
| Инженер оператор | 75000 | 1 | 75 |
| Итого | | 2 | 155 |

Фонд оплаты труда состоит из основной ($ЗП_{осн}$и дополнительной ($ЗП_{доп}$) заработной платы персонала, обслуживающего прибор (устройство или систему) или объект связи, а также директора предприятия, менеджера по рекламе и юриста и премиальных выплат:

$$ФОТ = ЗП_{осн} + ЗП_{доп} + П, \quad (3.17)$$

Основная заработная плата за год рассчитывается по формуле:

$$ЗП_{осн.} = 12 \cdot \sum_{i=1}^{n} ЗП_i \quad (3.18)$$

где $ЗП_i$ – месячная заработная плата i-того работника;
n – число работников.
$ЗП_{осн}$ = 12×155000=1860 000 тг.
Дополнительная заработная плата (работа в праздничные дни, сверхурочные работы и т.п.) составляет 30% от основной заработной платы работников:

$$ЗП_{доп} = ЗП_{осн} \times 0,3 \quad (3.19)$$

$ЗП_{доп}$ = 1860 000× 0,3 = 558 000 тг.
Премиальные выплаты, входящие в ФОТ, составляют 15% от основной заработной платы:

$$П = ЗП_{осн.} \times 0,15 \quad (3.20)$$

П =155000×0,15 =23 500тг.

Таким образом, ФОТ составляет:

ФОТ =1860 000 + 558 000+ 23500= 2 441 500тг.

Отчисления на социальные нужды составляют 11% от фонда оплаты труда, пенсионные отчисления составляют 10% от фонда оплаты труда, так как не облагаются социальным налогом:

$$Ос = 0,11 \times (ФОТ \times 0,9) \quad (3.21)$$

Ос =0,11 ×2441500×0,9 =241 708тг.

Амортизационные отчисления на предприятиях связи составляют 15-25% от основных производственных фондов. В данном случае амортизационные отчисления составляют 25% от стоимости оборудования:

$$Ао = Ц \times 0,25 \quad (3.22)$$

Ао = 1 818711×0,25 = 454 678тг.

Затраты на электроэнергию можно рассчитать по следующей формуле:

$$Эл = W \times T \times S \quad (3.23)$$

где W – потребляемая мощность оборудования (W = 2 кВт);

T – количество часов работы оборудования (T = 8760 ч.);

S – стоимость киловатт-часа электроэнергии (S = 19,29тг/кВТ·ч);

Тогда

Эл = 2×8760×19,29 = 337961 тг.

Прочие производственные и транспортные расходы определяются укрупнено в размере 35% от фонда заработной платы

$$Ппр=Нпр*ФОТ, \quad (3.24)$$

где Нпр - норматив прочих произв. и трансп. расходов.

Ппр=0,35*2441500=854525 тг

М – материальные затраты, запасные части - 0.5% капитальных затрат

М=1 818711×0.005=9 094 тг.

Н – накладные расходы (косвенные расходы, куда входят неучтенные расходы) – это 50 % от себестоимости.

Н=(2441500+241708+ 454 678+337961+854525+9 094)*0,50=2169 733 тг.

Исходя из выше рассчитанных данных, годовые эксплуатационные расходы составят:

Эр =2 441500+241708+454 678+337961+854525+9 094+2 169 733= 6 509 199 тг.

Т а б л и ц а 3.6 - Годовые эксплуатационные расходы

| Наименование статей затрат | Расчетные данные |
|---|---|
| Эксплуатационные расходы, тг. | 6 509 199 |
| В том числе: | |
| Фонд оплаты труда, тг. | 2 441500 |
| Отчисления на социальные нужды, тг | 241708 |
| Амортизационные отчисления, тг. | 454 678 |
| Затраты на электроэнергию, тг. | 337961 |
| Прочие производственные и транспортные расходы, тг. | 854525 |
| Материальные затраты, запасные части, тг. | 9 094 |
| Накладные расходы, тг. | 2 169 733 |

Т а б л и ц а 3 . 7 - Общие годовые эксплуатационные расходы

| Наименование статей затрат | Беспроводная сетьWi-Fi | Проводная сеть Ethernet |
|---|---|---|
| Эксплуатационные расходы тг. | 6405435 | 6 509 199 |
| В том числе: | | |
| Фонд оплаты труда, тг. | 2 441500 | 2 441500 |
| Отчисления на социальные нужды, тг. | 241708 | 241708 |
| Амортизационные отчисления, тг. | 386859 | 454 678 |
| Затраты на электроэнергию, тг. | 337961 | 337961 |
| Прочие производственные и транспортные расходы, тг. | 854525 | 854525 |
| Материальные затраты, запасные части, тг. | 7737 | 9 094 |
| Накладные расходы, тг. | 2135145 | 2 169 733 |

Сравним стоимость оборудования, эксплуатационные затратыпо таблицам 3.1, 3.4, 3.7:

Общая стоимость оборудования для построения беспроводной сети - 1547 435 тенге. Стоимость оборудования для проводной сети - 1 623 849 тенге.

Затраты на оборудование проводной сети получились больше на 76414 тенге. Из таблицы 3.7 видно, что эксплуатационные расходы проводной сети незначительно больше (103 764 тенге). Но чем масштабнее локальная сеть, тем больше будут расходы. Так же развертывание проводной сети требует

больших временных затрат, проводная сеть не мобильна и беспроводную сеть проще расширять.

## 4 Безопасность жизнедеятельности

### 4.1 Анализ условий труда в помещениях

В помещениях используется различное оборудование: компьютеры, мобильные телефоны, КПК, Wi-Fi оборудование. Персонал использует оборудование для доступа к сети.

Работа сотрудников непосредственно связана с компьютером, а соответственно с вредным дополнительным воздействием целой группы факторов, что существенно снижает производительность их труда.

К таким факторам можно отнести:

1) неправильная освещенность;

2) нарушение микроклимата;

3) наличие напряжения.

Улучшение световых условий и контроль за микроклиматом в помещении оказывает благоприятное воздействие на работоспособность и активность человека. Гигиеническими приемлемыми являются яркость до 5000 нт. Поэтому применяют искусственное освещение для проведения работ в темное время суток, в местах без достаточного освещения и при различных погодных условиях (снег, дождь, туман).

Исходные данные:

Длина – L = 7,5м

Ширина – B = 12м

Высота – H = 5м

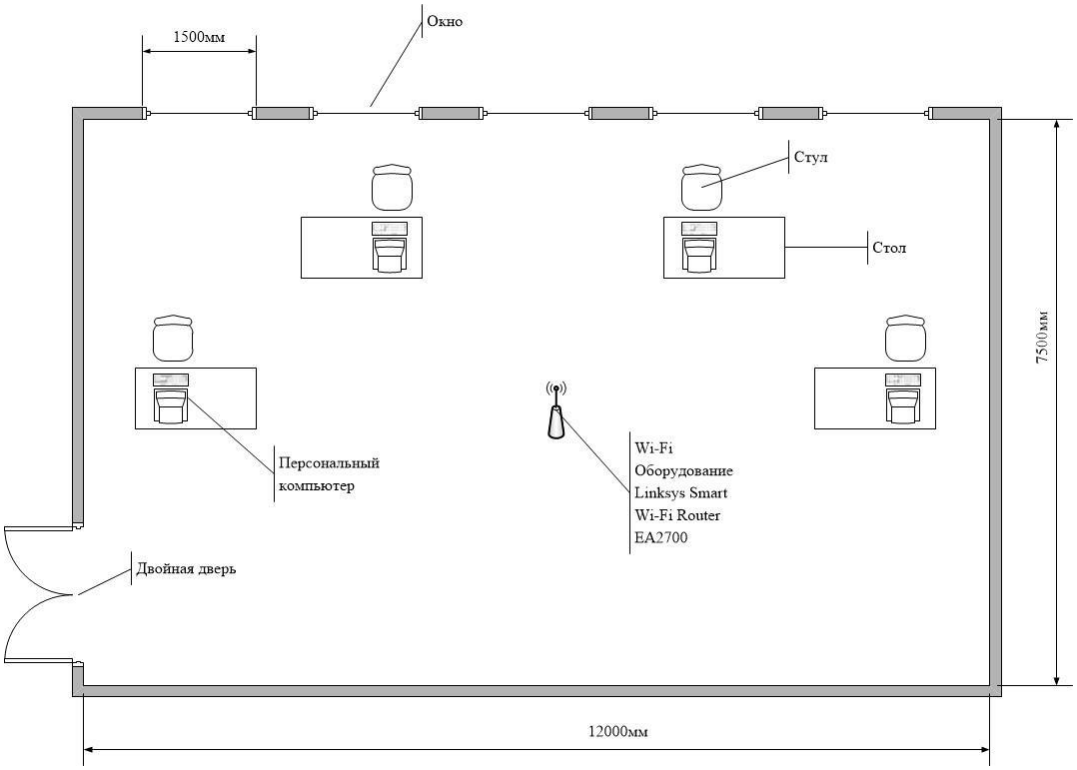


Рисунок 4.1 - План помещения

**4.2 Оборудование и персонал:**

1. МаршрутизаторLinksys Smart Wi-Fi Router EA2700

| | |
|---|---|
| Ширина | 173 мм |
| Высота/Толщина | 230 мм |
| Длина/Глубина | 189 мм |
| Вес | 0,32 кг |
| Напряжение | 220В |

Рисунок4.2 -Linksys Smart Wi-Fi Router EA2700

2. Персональный компьютер. Моноблок HP F6E38EA

| | |
|---|---|
| Ширина | 189 мм |
| Высота/Толщина | 31 мм |
| Длина/Глубина | 152 мм |
| Вес | 0,23 кг |
| Потребляемая мощность | 150 Вт |
| Напряжение | 220В |


Рисунок 4.3 -Моноблок HP F6E38EA

Корпусы устройств выполнены из пластика, тем самым не представляют опасности для человека. При взаимодействии с оборудованием персонал не касается металлических деталей или плат устройств.

В помещении трудятся 4 сотрудника: 2 человека занимаются мониторингом компьютерной сети и проверкой оборудования. Другие 2 человека занимаются деятельностью предприятия. Предприятие работает лишь в дневное время, сотрудники работают в 1-ну смену. Так как помещение, оборудование безопасно, то сотрудникам нет необходимости надевать спец. одежду. Легковоспламеняющихся веществ или предметов нет, таким образом, угрозы пожара нет. Влияние Wi-Fi сигнала на организм на человека не доказано, оборудование, установленное в помещении безопасно.

Необходимо рассчитать безопасное производственное освещение и так как в помещении 4 человека, при работе лампы выделяют тепло, то необходим кондиционер.

### 4.3 Расчет естественного освещения

Расчет естественного освещения заключается в определении площади световых проемов при боковом и верхнем освещении.

Общую площадь окон определяем по формуле (4.1) для бокового освещения:

$$S_0 = \frac{S_п \cdot e_н \cdot \eta_0 \cdot K_{зд} \cdot K_з}{100 \cdot \tau_0 \cdot r_1} \quad , \tag{4.1}$$

где $S_п$– площадь пола помещения, м$^2$:

$S_п = L \cdot B = 12 \cdot 7{,}5 = 90$ м$^2$

$e_н$ – нормированное значение КЕО для зданий располагаемых в различных районах, которое можно найти по формуле:

$$e_н = e_{КЕО} \cdot m \quad , \tag{4.2}$$

$e_{КЕО}$ - значение КЕО для зрительных работ: $e_н = 1{,}5\%$

$e_н = 1{,}5 \cdot 0{,}75 = 1{,}125$

$К_з$ – коэффициент запаса для лаборатории: $К_з = 1{,}2$;

$\tau_0$ - общий коэффициент светопропускания, определяемый по формуле:

$$\tau_0 = \tau_1 \cdot \tau_2 \cdot \tau_3 \cdot \tau_4 \cdot \tau_5 , \tag{4.3}$$

$\tau_1$ - коэффициент светопропускания материала: для стеклопакета $\tau_1 = 0{,}8$;

$\tau_2$ - коэффициент, учитывающий потери света в переплетах светопроёма для деревянных спаренных стеклопакетов: $\tau_2 = 0{,}7$;

$\tau_3$ - коэффициент, учитывающий потери света в несущих конструкциях, при боковом освещении равен 1;

$\tau_4$ - коэффициент, учитывающий потери света в солнцезащитных устройствах, для убирающихся регулируемых жалюзи: $\tau_4 = 1$;

$\tau_5$ - коэффициент, учитывающий потери света в защитной сетке, устанавливаемой под фонарями, принимают равным 0,9.

Тогда $\tau_0 = 0{,}8 \cdot 0{,}7 \cdot 1 \cdot 1 \cdot 0{,}9 = 0{,}504$

$\eta_0$ – световая характеристика окон:

Отношение длины помещения к его глубине: $\frac{L}{\frac{B}{2}} = \frac{7{,}5}{4{,}5} = 1{,}66$;

Тогда $\tau_0 = 0{,}8 \cdot 0{,}7 \cdot 1 \cdot 1 \cdot 0{,}9 = 0{,}504$

$\eta_0$ – световая характеристика окон:

Отношение длины помещения к его глубине: $\frac{L}{\frac{B}{2}} = \frac{7{,}5}{4{,}5} = 1{,}66$;

$h_1 = h_{ок} + h_{н.ок} - h_{пов} = 3 + 1 - 0{,}8 = 3{,}2$ м,

где $h_1$ – высота от уровня условной рабочей поверхности до верха окна;

уровень условной рабочей поверхности $h_{пов}$=0,8 м.

Отношение глубины помещения к его высоте от уровня условной рабочей поверхности до верха окна: $\frac{B}{h_1} = \frac{9}{3{,}2} = 2{,}8$

Учитывая эти отношения $\eta_0$ = 9.6

$r_1$ – коэффициент, учитывающий повышение КЕО при боковом освещение благодаря свету, отраженному от поверхностей помещения и подстилающего слоя, прилегающего к зданию:

Отношение расстояния расчетной точки от наружной стены к глубине помещения: $\frac{H}{B} = \frac{5}{9} = 0{,}55$;

Отношение длины помещения к его глубине: $\frac{L}{B} = \frac{7{,}5}{9} = 0{,}83$

$$\frac{\rho_{пот} + \rho_{ст} + \rho_{пол}}{3} = \frac{50 + 10 + 30}{3} = 30\,\%$$

Следовательно, средневзвешенный коэффициент отражения потолка, стен и пола равен 0.3.

Учитывая все эти коэффициенты, найдем $r_1$ = 1,1

$К_{зд}$ – коэффициент, учитывающий затенение окон противостоящими зданиями:

$$\frac{P}{H_{зд}} = \frac{12}{3} = 4;$$

$К_{зд} = 1$

Подставим все значения в расчетную формулу (4.1):

Получим: $S_0 = \frac{90 \cdot 9{,}6 \cdot 1{,}125 \cdot 1{,}2 \cdot 1}{100 \cdot 0{,}504 \cdot 1{,}1} \approx 22$ м$^2$.

Необходимая площадь светового проема для помещения - 22 м$^2$.

Необходимую площадь светового проема можно получить расположив 5 окон с размерами 3х1,5м.

Высота окна – 3м.

Ширина окна – 1,5м.

3·1,5 = 4,5м – площадь светового проема одного окна.

$\frac{22}{4{,}5} \approx 5$ окон.

Но в связи с тем, что погодные условия так же влияют на освещенность (снег, дождь, туман), то необходимо оборудовать помещение искусственным освещением.

### 4.4Расчет системы искусственного освещения помещения

Освещение в помещении смешанное (естественное и искусственное).Освещение на рабочих местах оказывает многоплановое воздействие на работника, в частности на его эмоциональное состояние, работоспособность, мотивацию, производительность и безопасность труда.

Поэтому рассчитаем общее освещение помещения аппаратного зала длиной А = 7,5 м., шириной В = 12 м., высотой Н = 5,5 м. С побеленным потолком, светлыми стенами и не завешенными окнами. Разряд зрительной работы – III высокой точности. Нормируемая освещенность – 300 лк.. Для помещения используем люминесцентную лампу ЛБ (белого цвета), мощностью 80 Вт., световым потоком – 4700лм длина лампы - 1514,2 мм, диаметр трубки - 32 мм.

Высота светильника $h_c$ = 5-r, где r- высота лампочки

$$h_c = 5 - 3{,}2 = 1{,}8 \text{ м}$$

Высота рабочей поверхности $h_P$ = 0,95 м.

Определим необходимое расстояние между светильниками:

$$L = \lambda \cdot h \text{ м.,} \qquad (4.4)$$

где $\lambda = 1.2 \div 1.4$

Высота светильника над освещаемой поверхностью:

$$h = H - h_p - h_c = 5 - 0{,}95 - 0{,}8 = 3{,}25м \quad (4.5)$$

По этим данным находим, что необходимое расстояние между светильниками равно:

$$L = \lambda \cdot h = 1{,}2 \cdot 3{,}25 = 3{,}9м \quad (4.6)$$

Определим индекс помещения I:

$$I = \frac{A \cdot B}{h \cdot (A+B)} = \frac{7{,}5 \cdot 12}{3{,}25 \cdot (7{,}5+12)} = 1{,}42 \quad (4.7)$$

Коэффициент использования η = 0,61.

В качестве светильника возьмем ЛСП 54 - 2Х80 рассчитанный на две лампы мощностью 80 Вт, диаметром 32 мм и длиной 1514,2 мм. Длина светильника 1525 мм, ширина 100 мм.

Рисунок 4.4 - Светильник ЛСП 54

Световой поток лампы ЛБ 80 составляет 4700 лм., световой поток, излучаемый светильником Фсв равен:

$$\Phi_{CB} = \Phi_Л \cdot 2 = 4700 \cdot 2 = 9400\, ЛМ \quad (4.8)$$

Определим число светильников:

$$N = \frac{E \cdot K_З \cdot S \cdot Z}{n \cdot \Phi_Л \cdot \eta}, \quad (4.9)$$

где S – площадь помещения, S=90 м$^2$.;
КЗ – коэффициент запаса, КЗ=1,5;
E – заданная минимальная освещенность, E=300 лк.;
Z – коэффициент неравномерности освещения, Z=1,2;
n – количество ламп в светильнике, n=2;
Фл – световой поток выбранной лампы, Фл=4700 лм.;
η – коэффициент использования, η=0,61.

$N = \frac{300 \cdot 1{,}5 \cdot 90 \cdot 1{,}2}{2 \cdot 4700 \cdot 0{,}61} = 8{,}47 \approx 9$ светильников (Расположение светильников показано на рисунке 11)

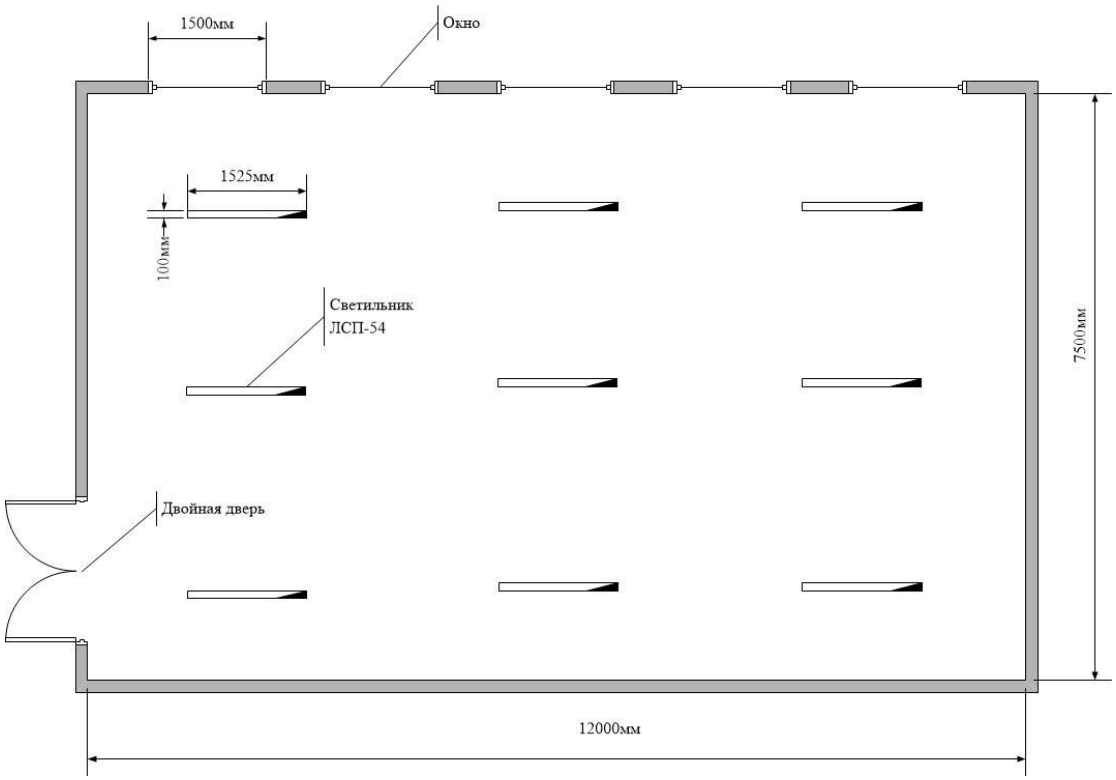


Рисунок 4.5 – Расположение светильников в помещении

Итого, для создания нормированной освещенности нам понадобится 18 ламп в 9-ти светильниках располагающихся в три ряда, в каждом ряду по три светильника, в каждом светильнике по две лампы.

### 4.5. Расчет воздухообмена в помещении

Так как в помещении работают 4 человека, оборудование, свет, то есть необходимость установки кондиционера. Кондиционер устанавливается для вентиляции помещения и поддержания комфортной температуры внутри помещения.

Выбираем кондиционер по площади помещения:

$S = L \cdot B = 12 \cdot 7{,}5 = 90\,\text{м}^2$

Кондиционер: колонная сплит-система Midea MFS2-48ARN1

Т а б л и ц а 4 . 1 - Технические характеристики кондиционера

| Общие характеристики | |
|---|---|
| Тип | колонная сплит-система |
| Максимальная длина коммуникаций | 25 м |
| Основные режимы | охлаждение / обогрев |
| Максимальный воздушный поток | 30 куб. м/мин |
| Мощность в режиме охлаждения | 12300 Вт |
| Мощность в режиме обогрева | 14100 Вт |
| Потребляемая мощность при обогреве | 5000 Вт |
| Потребляемая мощность при охлаждении | 5200 Вт |
| Режим приточной вентиляции | нет |
| Дополнительные режимы | режим вентиляции (без охлаждения и обогрева), автоматический режим, самодиагностика неисправностей |
| Режим осушения | есть |
| Обслуживаемая площадь | 102 кв. м |

## Заключение

В данном дипломном проекте были рассмотрены различные беспроводныесистемы связи. Построена беспроводная локальная сеть на основе технологии Wi-Fi, показана зона покрытия в офисе.

Как альтернатива предложена новая технология Li-Fi, описан принцип работы, описаны преимущества построения сети на данной беспроводной технологии. Проведено сравнение беспроводной сети офиса на технологиях Wi-Fi и Li-Fi. Описаны перспективы использования световой передачи данных.

## Список литературы


1 Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. Учебник. – Санкт-Петербург, Питер, 2001.

2 Щербо В.К. Стандарты вычислительных сетей. – М.: Кудиц – Образ, 2000

3 «Основы построения беспроводных локальных сетей стандарта 802.11. Практическое руководство по изучению, разработке и использованию беспроводных ЛВС стандарта 802.11» / Педжман Рошан, Джонатан Лиэри. – М.: Cisco Press Перевод с английского Издательский дом «Вильямс»,2004

4 «Современные технологии беспроводной связи» / Шахнович И. – М.: Техносфера, 2004

5 «Сети и системы радиодоступа» / Григорьев В.А., Лагутенко О.И., Распаев Ю.А. – М.: Эко-Трендз, 2005

6 «Анатомия беспроводных сетей» / Сергей Пахомов. – Компьютер-Пресс, №7, 2002

7 «WLAN: практическое руководство для администраторов и профессиональных пользователей» / Томас Мауфер. – М.: КУДИЦ-Образ, 2005

8 «Беспроводные сети. Первый шаг» / Джим Гейер. – М.: Издательство: Вильямс, 2005

9 «Секреты беспроводных технологий» / Джек Маккалоу. – М.: НТ-Пресс, 2005

10 «Современные технологии и стандарты подвижной связи» / Кузнецов М.А., Рыжков А.Е. – СПб.: Линк, 2006

11 «Базовые технологии локальных сетей» / В.Г. Олифер, Н.А. Олифер. – СПб.: Питер, 1999

12 Информация об оборудовании, сайт компании Linksys.: http://www.linksys.com

13 Шахнович С. Современные беспроводные технологии. - ПИТЕР, 2004

14 Голубицкая Е.А., Жигуляская Г.М. Экономика связи. – М.: Радио и связь, 1999.

15 Баклашов Н.И., Китаева Н.Ж., Терехов Б.Д. Охрана труда на предприятиях связи и охрана окружающей среды: Учебник. – М.: Радио и связь, 1989.

16 Верховский Е.И. Пожарная безопасность на предприятиях радиоэлектроники. – М.: Высшая школа, 1987

17 Базылов К.Б., Алибаева С.А., Бабич А.А. Методические указания для студентов всех форм обучения специальности 050719 –Радиотехника электроника и телекоммуникации. – Алматы: АИЭС, - 2008. - 20 с.

18 Информация о сети Li-Fi: http://www.lificonsortium.org/tech6.html

19 Общая информации о развитии, использовании и скоростях Li-Fi: http://habrahabr.ru/post/198874/

20 Сайт компании Oledcomm, продвигающая технологию Li-Fi: http://www.oledcomm.com/LiFi.html

## Приложение А

Использование Li-Fi

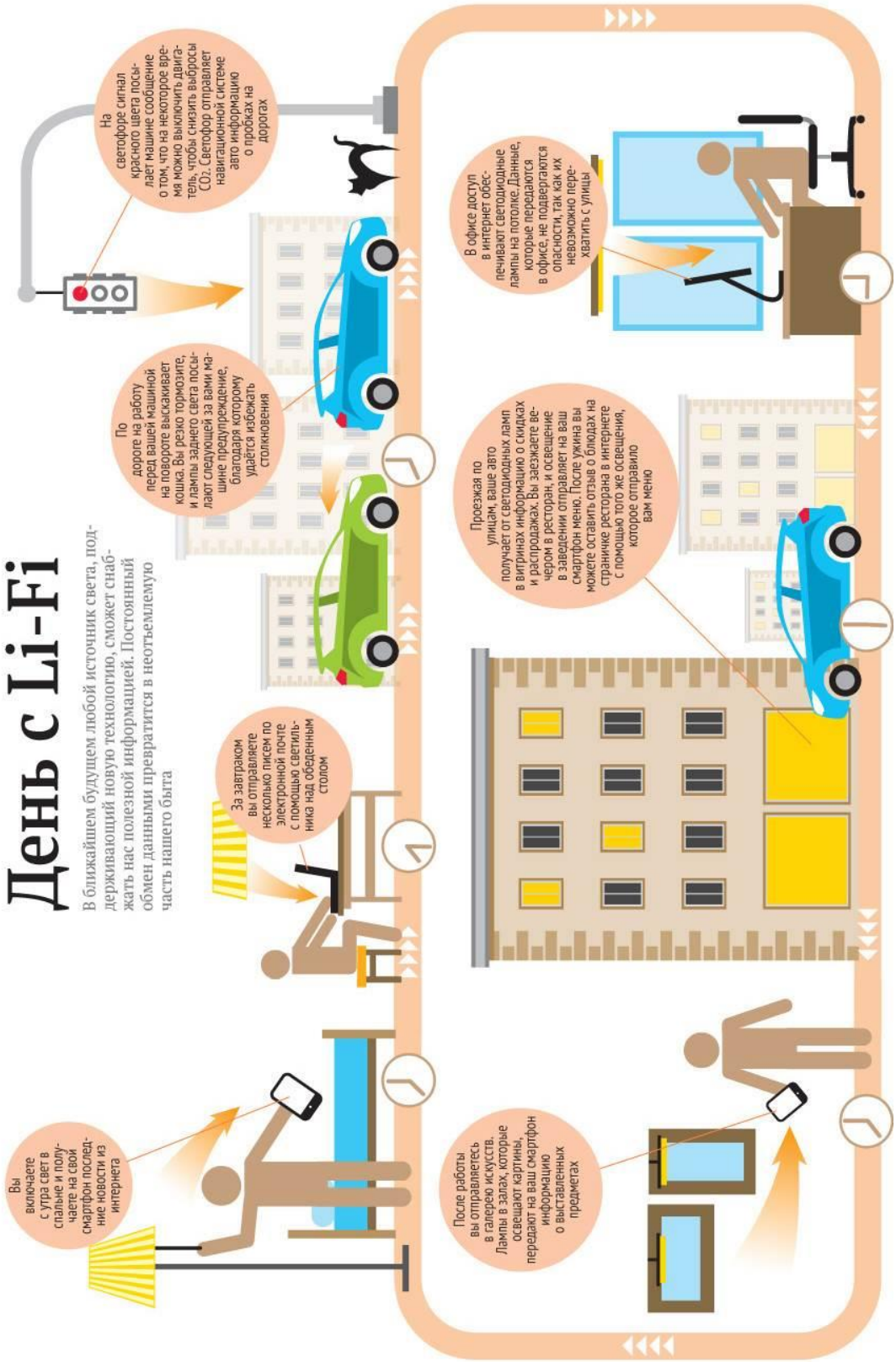


Рисунок А1 – Использование Li-Fi в повседневной жизни

**Приложение Б**

Зона покрытия Wi-Fi

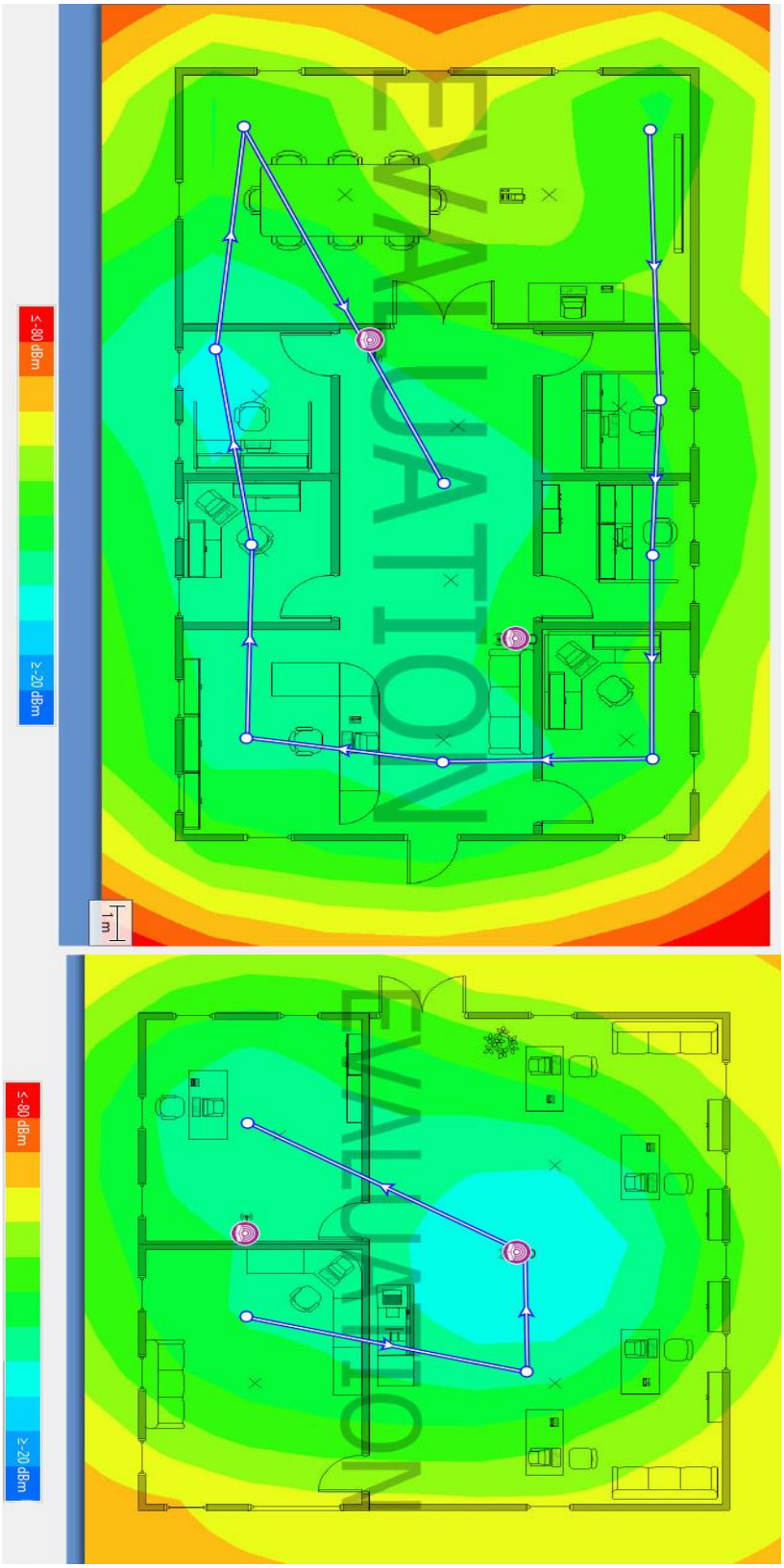


Рисунок Б2 – Зона покрытия Wi-Fi

## Приложение В

Зона покрытия Li-Fi

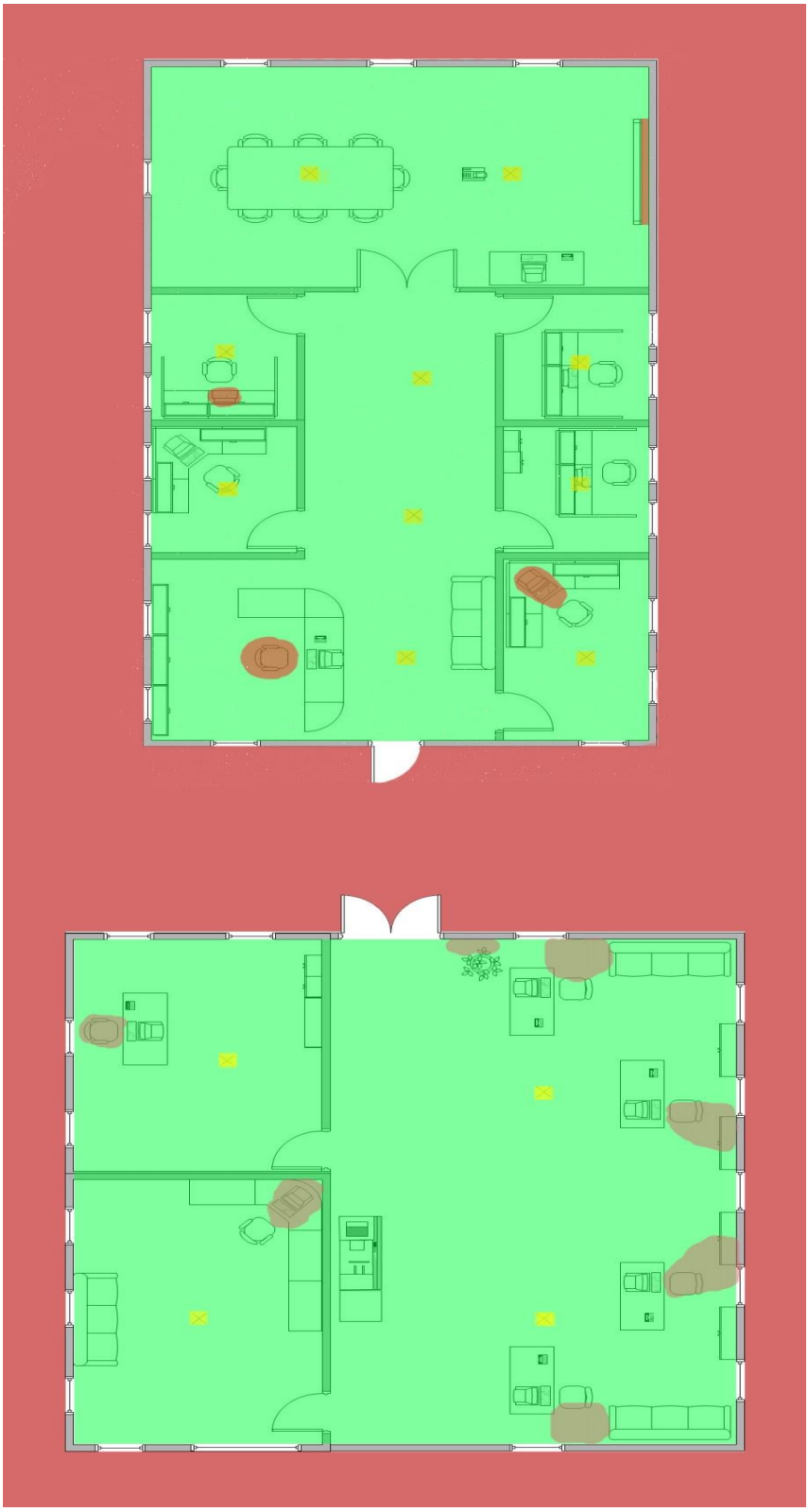

Рисунок В1 – Зона покрытия Li-Fi

## Приложение Г

Расчет потерь Wi-Fi сигнала

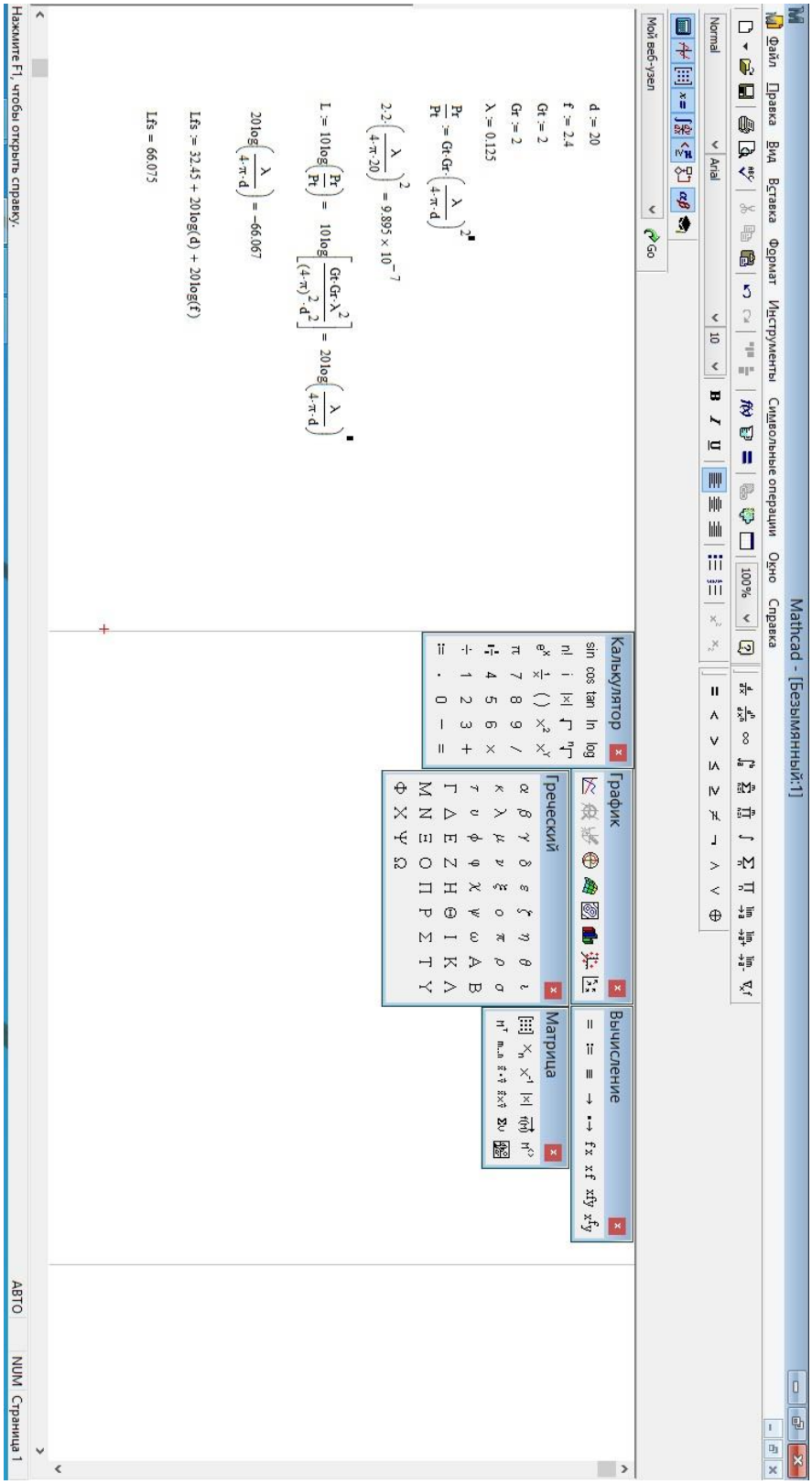


Рисунок Г1 – Расчет в программе Mathcad