**Республика Казахстан**

**Некоммерческое акционерное общество**

**«АЛМАТИНСКИЙ ИНСТИТУТ ЭНЕРГЕТИКИ И СВЯЗИ»**

**Кафедра Компьютерных технологий**

**Допущен к защите**

Зав. кафедрой:

к.ф.-м.н., профессор З.К.Куралбаев

**«\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_2010г.**

**ДИПЛОМНЫЙ ПРОЕКТ**

на тему: «Проектирование беспроводной сети Wi-Fi на основе стандарта 802.11n в общежитии № 2 Алматинского Института Энергетики и Связи»

**по специальности**

«Вычислительная техника и программное обеспечение»

**Выполнил:**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Д.А. Антонов

**Руководитель:**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_д.т.н., профессор М.А. Ташимов

**Алматы 2010**

**Республика Казахстан**

**Некоммерческое акционерное общество**

**«АЛМАТИНСКИЙ ИНСТИТУТ ЭНЕРГЕТИКИ И СВЯЗИ»**

Антонов Дмитрий Александрович

**ДИПЛОМНЫЙ ПРОЕКТ**

на тему: «Проектирование беспроводной сети Wi-Fi на основе стандарта 802.11n в общежитии № 2 Алматинского Института Энергетики и Связи»

**по специальности**

«Вычислительная техника и программное обеспечение»

**Алматы 2010**

**Республика Казахстан**

**Некоммерческое акционерное общество**

**«АЛМАТИНСКИЙ ИНСТИТУТ ЭНЕРГЕТИКИ И СВЯЗИ»**

|  |  |
| --- | --- |
| **Консультанты:**  по экономической части:  ст. преп. З.Д.Еркешева  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_ 2010 г.  по безопасности жизнедеятельности:  ассистент С.Е. Мананбаева  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_ 2010 г.  по применению  вычислительной техники:  профессор М.А.Ташимов  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_ 2010 г.  по делопроизводству на казахском  и русском языках:  преп. К.С.Телгожаева  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_ 2010 г.  Алматы 2010 | **Нормоконтролер:**  ст. преп. А.А.Ержан  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_ 2010 г.  **Рецензент:**  к.т.н., зам. ген. Директора ТОО «Системотехника» Т.Р. Амирбаев  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_ 2010 г.  **Руководитель:**  д.т.н., профессор М.А.Ташимов  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_ 2010 г.  **Студент:**  Д.А.Антонов  **Группа**: Бвт-06-5  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_ 2010 г. |

РЕСПУБЛИКА КАЗАХСТАН

НЕКОММЕРЧЕСКОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО

**«**АЛМАТИНСКИЙ ИНСТИТУТ ЭНЕРГЕТИКИ И СВЯЗИ»

Факультет: Радиотехника и Связь

Специальность: Вычислительная техника и программное обеспечение

Кафедра: Компьютерные Технологии

ЗАДАНИЕ

на выполнение дипломного проекта

Студента: Дмитрия Александровича Антонова

Тема проекта:

«Проектирование беспроводной сети Wi-Fi на основе стандарта 802.11n в общежитии № 2 Алматинского Института Энергетики и Связи»,

утверждена приказом ректора № 80 от «25» сентября 2010 года.

Срок сдачи законченного проекта (работы): «\_\_»\_\_\_\_\_\_\_\_\_2010 года.

Исходные данные к проекту (требуемые параметры результатов проектирования (исследования) и исходные данные объекта): на основе компании ОАО «Казахтелеком» спроектировать сеть беспроводного доступа Wi-Fi стандарт 802.11n в общежитии № 2 Алматинского Института Энергетики и Связи. Для предоставления современных услуг связи: высокоскоростной доступ в Интернет, компьютерная сеть. Перечень подлежащих разработке в дипломном проекте вопросов или краткое содержание дипломного проекта:

1. Общие понятия беспроводного доступа Wi-Fi (характеристики, стандарты).
2. Выбор оборудования системы беспроводного доступа.
3. Расчет зоны покрытия точек доступа
4. Охрана безопасности и жизнедеятельности
5. Экономическая эффективность проекта

Перечень графического материала (с точным указанием обязательных  
чертежей):

1. Топология сети беспроводного доступа в общежитии № 2 Алматинского Института Энергетики и Связи.
2. Зона покрытия беспроводной сети Wi-Fi в общежитии № 2 Алматинского Института Энергетики и Связи.

Рекомендуемая основная литература:

1. Феер К. Беспроводная цифровая связь. Методы модуляции и расширения спектра М.: Радио и связь, под редакцией В. И. Журавлева 2000 г.;
2. Варакин Л. Е.Системы связи с шумоподобными сигналами. М: Радио и связь, 1985;
3. Серопегин В.И., Радиотехнологии в сфере WLL, Технологии и Средства Cвязи № 4, 2000.
4. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. Учебник. – Санкт-Петербург, Питер, 2001

Консультации по проекту (работе) с указанием относящихся к ним разделов проекта (работы):

|  |  |  |  |
| --- | --- | --- | --- |
| Раздел | Консультант | Сроки | Подпись |
| Основная часть | М.А.Ташимов |  |  |
| БЖД | С.Е Мананбаева. |  |  |
| Экономика | З.Д.Еркешева |  |  |
| Делопроизводство на казахском и русском языках | К.С.Телгожаева |  |  |
| Применение вычислительной техники | М.А.Ташимов |  |  |
| Нормоконтролер | А.А.Ержан |  |  |

ГРАФИК

подготовки дипломного проекта

|  |  |  |
| --- | --- | --- |
| Наименование разделов, перечень разрабатываемых вопросов | Сроки представления | Примечание |
| Анализ и описание системы беспроводного доступа |  |  |
| Выбор оборудования |  |  |
| Проектирование сети |  |  |
| Безопасность жизнедеятельности |  |  |
| Бизнес-план |  |  |

Дата выдачи задания

Заведующий кафедрой З. К. Куралбаев

(подпись)

Руководитель М. А. Ташимов

(подпись)

Задание принял к исполнению

студент Д. А. Антонов

(подпись)

**АНДАТПА**

Берілген дипломдық жұмысында Алматы Энергетика және Байланыс Институтының №2 жатақханасында Wi-Fi (IEEE-802.11n) стандартының негізінде сымсыз кеңжолақты байланыс желісін құру жоспары мен негіздемесі қарастырылған.

Жобада стандарттың сипаттамалары, оның басқа стандарттардан ерекшеліктері, желіні құру сұлбасы және жабдықтардың құрамы ұсынылған.

Жобада, сондай-ақ, жабдықтарды пайдалану кезіндегі өміртіршілік қауіпсіздігі мәселелері қарастырылған.

Осы жобаны енгізудің техник-экономикалық негіздемесі жасалды.

**АННОТАЦИЯ**

В данной дипломной работе рассмотрен план и обоснование построения сети беспроводной связи на основе стандарта Wi-Fi (IEEE-802.11n) в общежитии № 2 Алматинского Института Энергетики и Связи.

В дипломе так же представлены характеристики стандарта, отличие его от других стандартов, схема построения сети и состав оборудования.

В проекте также описаны меры безопасности жизнедеятельности.

Разработано технико-экономическое обоснование внедрения данного проекта.

# СОДЕРЖАНИЕ

ВВЕДЕНИЕ

1 ОБЗОР ТЕХНОЛОГИИ БЕСПРВОДНОГО ДОСТУПА Wi-FI

1.1 Особенности развития технологий беспроводного доступа

1.2 История развития

1.3 Основные стандарты

1.4 Факторы более высокой скорости передачи данных стандарта 802.11n

1.5 Топологии беспроводных сетей Wi-Fi

1.6 Беспроводное оборудование, применяемое в Wi-Fi сетях

2 РЕАЛИЗАЦИЯ СЕТИ БЕСПРВОДНОГО ДОСТУПА

2.1 Место реализации проекта

2.3 Описание и характеристика выбранного оборудования

2.4. Разработка структурной схемы организации сети

2.5 Программирование

3 РАСЧЕТНАЯ ЧАСТЬ

3.1 Расчет эффективной изотропной излучаемой мощности

3.2 Расчет зоны действия сигнала

4 ЗАЩИТА БЕСПРОВОДНЫХ СЕТЕЙ

4.1 Защита информации

4.2 WEP и его последователи

4.3 Программное обеспечение

4.4 Инвентаризация беспроводной сети

4.5 Анализ защищенности беспроводных устройств

4.6 Обнаружение атак на беспроводные сети

5 БИЗНЕС ПЛАН

5.1 Общая информация о проекте

5.2 Обоснование выбора и состава оборудования

5.3 Финансовый план

6 БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ

6.1 Анализ условий труда обслуживающего персонала при эксплуатации технического оборудования

6.2 Расчет системы искусственного освещения помещения

6.3 Анализ пожарной безопасности

ЗАКЛЮЧЕНИЕ

СПИСОК ЛИТЕРАТУРЫ

ПРИЛОЖЕНИЕ А

ПРИЛОЖЕНИЕ Б

ПРИЛОЖЕНИЕ E

**ВВЕДЕНИЕ**

Во всем мире стремительно растет потребность в беспроводных соединениях, особенно в сфере бизнеса и IT технологий. Пользователи с беспроводным доступом к информации всегда и везде могут работать гораздо более производительно и эффективно, чем их коллеги, привязанные к проводным телефонным и компьютерным сетям, так как существует привязанность к определенной инфраструктуре коммуникаций.

На современном этапе развития сетевых технологий, технология беспроводных сетей Wi-Fi является наиболее удобной в условиях требующих мобильность, простоту установки и использования. Wi-Fi (от англ. wireless fidelity - беспроводная связь) - стандарт широкополосной беспроводной связи семейства 802.11 разработанный в 1997г. Как правило, технология Wi-Fi используется для организации беспроводных локальных компьютерных сетей, а также создания так называемых горячих точек высокоскоростного доступа в Интернет.

Беспроводные сети обладают, по сравнению с традиционными проводными сетями, немалыми преимуществами, главным из которых, конечно же, является:

- Простота развёртывания;

- Гибкость архитектуры сети, когда обеспечивается возможность динамического изменения топологии сети при подключении, передвижении и отключении мобильных пользователей без значительных потерь времени;

- Быстрота проектирования и реализации, что критично при жестких требованиях к времени построения сети;

- Так же, беспроводная сеть не нуждается в прокладке кабелей (часто требующей дробления стен).

В то же время беспроводные сети на современном этапе их развития не лишены серьёзных недостатков. Прежде всего, это зависимость скорости соединения и радиуса действия от наличия преград и от расстояния между приёмником и передатчиком. Один из способов увеличения радиуса действия беспроводной сети заключается в создании распределённой сети на основе нескольких точек беспроводного доступа. При создании таких сетей появляется возможность превратить здание в единую беспроводную зону и увеличить скорость соединения вне зависимости от количества стен (преград). Аналогично решается и проблема масштабируемости сети, а использование внешних направленных антенн позволяет эффективно решать проблему препятствий, ограничивающих сигнал.

Целью данной работы является проектирование сети беспроводного доступа в общежитии № 2 Алматинского Института Энергетики и Связи, с целью повышения уровня информатизации, предоставления современных услуг связи: высокоскоростной доступ в Интернет, компьютерная сеть, на базе технологии Wi-Fi.

**1 ОБЗОР ТЕХНОЛОГИИ БЕСПРВОДНОГО ДОСТУПА Wi-FI**

## 

## 1.1 Особенности развития технологий беспроводного доступа

На заре развития радиотехники термин "беспроводный" (wireless) использовался для обозначения радиосвязи в широком смысле этого слова, т. е. буквально во всех случаях, когда передача информации осуществлялась без проводов. Позже это толкование практически вышло из обращения, и "беспроводный" стало употребляться как эквивалент термину "радио" (radio) или "радиочастота" (RF - radio frequency). Сейчас оба понятия считаются взаимозаменяемыми в том случае, если речь идет о диапазоне частот от 3 кГц до 300 ГГц. Тем не менее термин "радио" чаще используется для описания уже давно существующих технологий (радиовещание, спутниковая связь, радиолокация, радиотелефонная связь и т. д.). А термин "беспроводный" в наши дни принято относить к новым технологиям радиосвязи, таким, как микросотовая и сотовая телефония, пейджинг, абонентский доступ и т. п.

Различают три типа беспроводных сетей (рис. 1.1): WWAN (Wireless Wide Area Network), WLAN (Wireless Local Area Network) и WPAN (Wireless Personal Area Network)

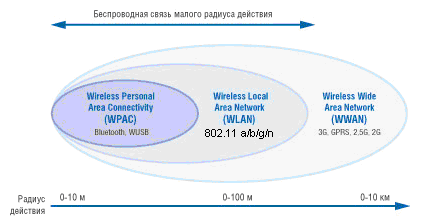


Рисунок 1.1 - Радиус действия персональных, локальных и глобальных беспроводных сетей

При построении сетей WLAN и WPAN, а также систем широкополосного беспроводного доступа (BWA - Broadband Wireless Access) применяются сходные технологии. Ключевое различие между ними (рис. 1.2) - диапазон рабочих частот и характеристики радиоинтерфейса. Сети WLAN и WPAN работают в нелицензионных диапазонах частот 2,4 и 5 ГГц, т. е. при их развертывании не требуется частотного планирования и координации с другими радиосетями, работающими в том же диапазоне. Сети BWA (Broadband Wireless Access) используют как лицензионные, так и нелицензионные диапазоны (от 2 до 66 ГГц).

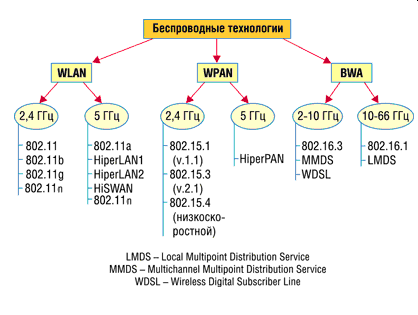


Рисунок 1.2 - Классификация беспроводных технологий

Беспроводные локальные сети WLAN.

Основные назначение беспроводных локальных сетей (WLAN) – организация доступа к информационным ресурсам внутри здания. Вторая по значимости сфера применения – это организация общественных коммерческих точек доступа (hot spots) в людных местах – гостиницах, аэропортах, кафе, а также организация временных сетей на период проведения мероприятий (выставок, семинаров).

Беспроводные локальные сети создаются на основе семейства стандартов IEEE 802.11. Эти сети известны также как Wi-Fi (Wireless Fidelity), и хотя сам термин Wi-Fi, в стандартах явным образом не прописан, бренд Wi-Fi получил в мире самое широкое распространение.

## 1.2 История развития

В 1990 г. Комитет по стандартам IEEE 802 (Institute of Electrical and Electronic Engineers). сформировал рабочую группу по стандартам для беспроводных локальных сетей 802.11. Это группа занялась разработкой всеобщего стандарта для радиооборудования и сетей, работающих на частоте 2.4 ГГц со скоростями 1 и 2 Мбит/с. Работа по созданию стандарта были завершены через семь лет, и в июне 1997 г. была ратифицирована первая спецификация 802.11.

Стандарт IEEE 802.11 стал первым стандартом для продуктов WLAN от независимой международной организации. Однако к моменту выхода стандарта в свет первоначально заложенная в нем скорость передачи данных оказалась недостаточной. Это послужило причиной последующих доработок, поэтому сегодня можно говорить о группе стандартов.

## 

## 1.3 Основные стандарты

В настоящее время широко используется преимущественно три стандарта группы IEEE 802.11 (представлены в таблице 1.1)

Таблица 1.1 - Основные характеристики стандартов группы IEEE 802.11

|  |  |  |  |
| --- | --- | --- | --- |
| Стандарт | 802.11g | 802.11a | 802.11n |
| Частотный диапазон, ГГц | 2,4-2,483 | 5,15-5,25 | 2,4 или 5,0 |
| Метод передачи | DSSS,OFDM | DSSS,OFDM | MIMO |
| Скорость, Мбит/с | 1-54 | 6-54 | 6-300 |
| Совместимость | 802.11 b/n | 802.11 n | 802.11 a/b/g |
| Метод модуляции | BPSK, QPSK  OFDM | BPSK, QPSK OFDM | BPSK, 64-QAM |
| Дальность связи в помещении, м | 20-50 | 10-20 | 50-100 |
| Дальность связи вне помещения, м | 250 | 150 | 500 |

**1.3.1 Стандарт IEEE 802.11g**

Стандарт IEEE 802.11g, принятый в 2003 году, является логическим развитием стандарта 802.11b и предполагает передачу данных в том же частотном диапазоне, но с более высокими скоростями. Кроме того, стандарт 802.11g полностью совместим с 802.11b, то есть любое устройство 802.11g должно поддерживать работу с устройствами 802.11b. Максимальная скорость передачи данных в стандарте 802.11g составляет 54 Мбит/с.При разработке стандарта 802.11g рассматривались две конкурирующие технологии: метод ортогонального частотного разделения OFDM, заимствованный из стандарта 802.11a и предложенный к рассмотрению компанией Intersil, и метод двоичного пакетного сверточного кодирования PBCC, предложенный компанией Texas Instruments. В результате стандарт 802.11g содержит компромиссное решение: в качестве базовых применяются технологии OFDM и CCK, а опционально предусмотрено использование технологии PBCC.

Идея сверточного кодирования (Packet Binary Convolutional Coding, PBCC) заключается в следующем. Входящая последовательность информационных бит преобразуется в сверточном кодере таким образом, чтобы каждому входному биту соответствовало более одного выходного. То есть сверточный кодер добавляет определенную избыточную информацию к исходной последовательности. Если, к примеру, каждому входному биту соответствуют два выходных, то говорят о сверточном кодировании со скоростью равной 1/2. Если же каждым двум входным битам соответствуют три выходных, то скорость сверточного кодирования будет составлять уже 2/3.

Любой сверточный кодер строится на основе нескольких последовательно связанных запоминающих ячеек и логических элементов XOR. Количество запоминающих ячеек определяет количество возможных состояний кодера. Если, к примеру, в сверточном кодере используется шесть запоминающих ячеек, то в кодере хранится информация о шести предыдущих состояниях сигнала, а с учетом значения входящего бита получим, что в таком кодере применяется семь бит входной последовательности. Такой сверточный кодер называется кодером на семь состояний.

Выходные биты, формируемые в сверточном кодере, определяются операциями XOR между значениями входного бита и битами, хранимыми в запоминающих ячейках, то есть значение каждого формируемого выходного бита зависит не только от входящего информационного бита, но и от нескольких предыдущих битов.

Главным достоинством сверточных кодеров является помехоустойчивость формируемой ими последовательности. Дело в том, что при избыточности кодирования даже в случае возникновения ошибок приема исходная последовательность бит может быть безошибочно восстановлена. Для восстановления исходной последовательности бит на стороне приемника применяется декодер Витерби.

Дибит, формируемый в сверточном кодере, используется в дальнейшем в качестве передаваемого символа, но предварительно он подвергается фазовой модуляции. Причем в зависимости от скорости передачи возможна двоичная, квадратурная или даже восьмипозиционная фазовая модуляция.

В отличие от технологий DSSS (коды Баркера, ССК-последовательности), в технологии сверточного кодирования не применяется технология уширения спектра за счет использования шумоподобных последовательностей, однако уширение спектра до стандартных 22 МГц предусмотрено и в данном случае. Для этого применяют вариации возможных сигнальных созвездий QPSK и BPSK.

Рассмотренный метод PBCC-кодирования опционально используется в протоколе 802.11b на скоростях 5,5 и 11 Мбит/с. Аналогично в протоколе 802.11g для скоростей передачи 5,5 и 11 Мбит/с этот способ тоже применяется опционально. Вообще, вследствие совместимости протоколов 802.11b и 802.11g технологии кодирования и скорости, предусмотренные протоколом 802.11b, поддерживаются и в протоколе 802.11g. В этом плане до скорости 11 Мбит/с протоколы 802.11b и 802.11g совпадают друг с другом, за исключением того, что в протоколе 802.11g предусмотрены такие скорости, которых нет в протоколе 802.11b.

Опционально в протоколе 802.11g технология PBCC может использоваться при скоростях передачи 22 и 33 Мбит/с.

Для скорости 22 Мбит/с по сравнению с уже рассмотренной нами схемой PBCC передача данных имеет две особенности. Прежде всего, применяется 8-позиционная фазовая модуляция (8-PSK), то есть фаза сигнала может принимать восемь различных значений, что позволяет в одном символе кодировать уже три бита. Кроме того, в схему, за исключением сверточного кодера, добавлен пунктурный кодер (Puncture). Смысл такого решения довольно прост: избыточность сверточного кодера, равная 2 (на каждый входной бит приходится два выходных), достаточно высока и при определенных условиях помеховой обстановки является излишней, поэтому можно уменьшить избыточность, чтобы, к примеру, каждым двум входным битам соответствовали три выходных. Для этого можно, конечно, разработать соответствующий сверточный кодер, но лучше добавить в схему специальный пунктурный кодер, который будет просто уничтожать лишние биты. Допустим, пунктурный кодер удаляет один бит из каждых четырех входных бит. Тогда каждым четырем входящим бит будут соответствовать три выходящих. Скорость такого кодера составляет 4/3. Если же такой кодер используется в паре со сверточным кодером со скоростью 1/2, то общая скорость кодирования составит уже 2/3, то есть каждым двум входным битам будут соответствовать три выходных.

Технология PBCC является опциональной в стандарте IEEE 802.11g, а технология OFDM — обязательной. Для того чтобы понять суть технологии OFDM, рассмотрим более подробно многолучевую интерференцию, возникающую при распространении сигналов в открытой среде.

Эффект многолучевой интерференции сигналов заключается в том, что в результате многократных отражений от естественных преград один и тот же сигнал может попадать в приемник различными путями. Но разные пути распространения отличаются друг от друга по длине, а потому ослабление сигнала будет для них неодинаковым. Следовательно, в точке приема результирующий сигнал представляет собой интерференцию многих сигналов, имеющих различные амплитуды и смещенных друг относительно друга по времени, что эквивалентно сложению сигналов с разными фазами.

Следствием многолучевой интерференции является искажение принимаемого сигнала. Многолучевая интерференция присуща любому типу сигналов, но особенно негативно она сказывается на широкополосных сигналах, поскольку при использовании широкополосного сигнала в результате интерференции определенные частоты складываются синфазно, что приводит к увеличению сигнала, а некоторые, наоборот, противофазно, вызывая ослабление сигнала на данной частоте.

Говоря о многолучевой интерференции, возникающей при передаче сигналов, отмечают два крайних случая. В первом из них максимальная задержка между сигналами не превышает длительности одного символа и интерференция возникает в пределах одного передаваемого символа. Во втором — максимальная задержка между сигналами больше длительности одного символа, поэтому в результате интерференции складываются сигналы, представляющие разные символы, и возникает так называемая межсимвольная интерференция (Inter Symbol Interference, ISI).

Наиболее отрицательно на искажение сигнала влияет именно межсимвольная интерференция. Поскольку символ — это дискретное состояние сигнала, характеризующееся значениями частоты несущей, амплитуды и фазы, для разных символов меняются амплитуда и фаза сигнала, а следовательно, восстановить исходный сигнал крайне сложно.

По этой причине при высоких скоростях передачи применяется метод кодирования данных, называемый ортогональным частотным разделением каналов с мультиплексированием (Orthogonal Frequency Division Multiplexing, OFDM). Суть его заключается в том, что поток передаваемых данных распределяется по множеству частотных подканалов и передача ведется параллельно на всех таких подканалах. При этом высокая скорость передачи достигается именно за счет одновременной передачи данных по всем каналам, тогда как скорость передачи в отдельном подканале может быть и невысокой.

Благодаря тому что в каждом из частотных подканалов скорость передачи данных можно сделать не слишком высокой, создаются предпосылки для эффективного подавления межсимвольной интерференции.

При частотном разделении каналов необходимо, чтобы отдельный канал был достаточно узким для минимизации искажения сигнала, но в то же время — достаточно широким для обеспечения требуемой скорости передачи. Кроме того, для экономного использования всей полосы канала, разделяемого на подканалы, желательно расположить частотные подканалы как можно ближе друг к другу, но при этом избежать межканальной интерференции, чтобы обеспечить их полную независимость. Частотные каналы, удовлетворяющие вышеперечисленным требованиям, называются ортогональными. Несущие сигналы всех частотных подканалов ортогональны друг другу. Важно, что ортогональность несущих сигналов гарантирует частотную независимость каналов друг от друга, а следовательно, и отсутствие межканальной интерференции.

Рассмотренный способ деления широкополосного канала на ортогональные частотные подканалы называется ортогональным частотным разделением с мультиплексированием (OFDM). Для его реализации в передающих устройствах используется обратное быстрое преобразование Фурье (IFFT), переводящее предварительно мультиплексированный на n-каналов сигнал из временного представления в частотное.

Одним из ключевых преимуществ метода OFDM является сочетание высокой скорости передачи с эффективным противостоянием многолучевому распространению. Конечно, сама по себе технология OFDM не исключает многолучевого распространения, но создает предпосылки для устранения эффекта межсимвольной интерференции. Дело в том, что неотъемлемой частью технологии OFDM является охранный интервал (Guard Interval, GI) — циклическое повторение окончания символа, пристраиваемое в начале символа.

Охранный интервал создает паузы между отдельными символами, и если его длительность превышает максимальное время задержки сигнала в результате многолучевого распространения, то межсимвольной интерференции не возникает.

При использовании технологии OFDM длительность охранного интервала составляет одну четвертую длительности самого символа. При этом символ имеет длительность 3,2 мкс, а охранный интервал — 0,8 мкс. Таким образом, длительность символа вместе с охранным интервалом составляет 4 мкс.

В протоколе 802.11g на низких скоростях передачи применяется двоичная и квадратурная фазовые модуляции BPSK и QPSK. При использовании BPSK-модуляции в одном символе кодируется только один информационный бит, а при QPSK-модуляции — два информационных бита. Модуляция BPSK применяется для передачи данных на скоростях 6 и 9 Мбит/с, а модуляция QPSK — на скоростях 12 и 18 Мбит/с.

Для передачи на более высоких скоростях используется квадратурная амплитудная модуляция QAM (Quadrature Amplitude Modulation), при которой информация кодируется за счет изменения фазы и амплитуды сигнала. В протоколе 802.11g применяется модуляция 16-QAM и 64-QAM. Первая модуляция предполагает 16 различных состояний сигнала, что позволяет закодировать 4 бита в одном символе; вторая — 64 возможных состояния сигнала, что дает возможность закодировать последовательность 6 бит в одном символе. Модуляция 16-QAM используется на скоростях 24 и 36 Мбит/с, а модуляция 64-QAM — на скоростях 48 и 54 Мбит/с.

1.3.2 Стандарт IEEE 802.11а

Стандарт IEEE 802.11а предусматривает скорость передачи данных до 54 Мбит/с. В отличие от базового стандарта спецификациями 802.11а предусмотрена работа в новом частотном диапазоне 5ГГц. В качестве метода модуляции сигнала выбрано ортогонально частотное мультиплексирование (OFDM), обеспечивающее высокую устойчивость связи в условиях многолучевого распространения сигнала.

В соответствии с правилами FCC частотный диапазон UNII разбит на три 100-мегагерцевых поддиапазона, различающихся ограничениями по максимальной мощности излучения. Низший диапазон (от 5,15 до 5,25 ГГц) предусматривает мощность всего 50 мВт, средний (от 5,25 до 5,35 ГГц) — 250 мВт, а верхний (от 5,725 до 5,825 ГГц) — 1 Вт. Использование трех частотных поддиапазонов с общей шириной 300 МГц делает стандарт IEEE 802.11а самым широкополосным из семейства стандартов 802.11 и позволяет разбить весь частотный диапазон на 12 каналов, каждый из которых имеет ширину 20 МГц, причем восемь из них лежат в 200-мегагерцевом диапазоне от 5,15 до 5,35 ГГц, а остальные четыре канала — в 100-мегагерцевом диапазоне от 5,725 до 5,825 ГГц (рисунок 1.3). При этом четыре верхних частотных канала, предусматривающие наибольшую мощность передачи, используются преимущественно для передачи сигналов вне помещений.

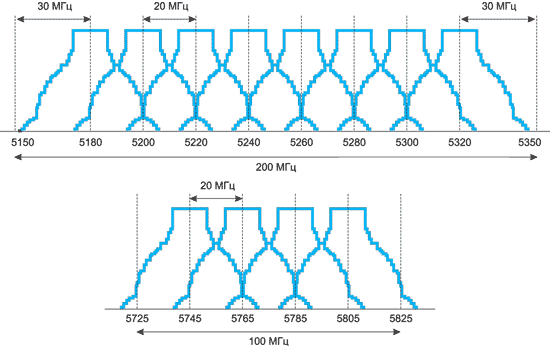


Рисунок 1.3 - Разделение диапазона UNII на 12 частотных поддиапазонов

Стандарт IEEE 802.11a основан на технике частотного ортогонального разделения каналов с мультиплексированием (OFDM). Для разделения каналов применяется обратное преобразование Фурье с окном в 64 частотных подканала. Поскольку ширина каждого из 12 каналов, определяемых в стандарте 802.11а, имеет значение 20 МГц, получается, что каждый ортогональный частотный подканал (поднесущая) имеет ширину 312,5 кГц. Однако из 64 ортогональных подканалов задействуется только 52, причем 48 из них применяются для передачи данных (Data Tones), а остальные — для передачи служебной информации (Pilot Тones).

По технике модуляции протокол 802.11a мало чем отличается от 802.11g. На низких скоростях передачи для модуляции поднесущих частот используется двоичная и квадратурная фазовые модуляции BPSK и QPSK. При применении BPSK-модуляции в одном символе кодируется только один информационный бит. Соответственно при использовании QPSK-модуляции, то есть когда фаза сигнала может принимать четыре различных значения, в одном символе кодируются два информационных бита. Модуляция BPSK используется для передачи данных на скоростях 6 и 9 Мбит/с, а модуляция QPSK — на скоростях 12 и 18 Мбит/с.

Для передачи на более высоких скоростях в стандарте IEEE 802.11а используется квадратурная амплитудная модуляция 16-QAM и 64-QAM. В первом случае имеется 16 различных состояний сигнала, что позволяет закодировать 4 бита в одном символе, а во втором — уже 64 возможных состояния сигнала, что позволяет закодировать последовательность из 6 битов в одном символе. Модуляция 16-QAM применяется на скоростях 24 и 36 Мбит/с, а модуляция 64-QAM — на скоростях 48 и 54 Мбит/с.

Информационная емкость OFDM-символа определяется типом модуляции и числом поднесущих. Поскольку для передачи данных применяются 48 поднесущих, емкость OFDM-символа составляет 48 x Nb, где Nb — двоичный логарифм от числа позиций модуляции, или, проще говоря, количество бит, которые кодируются в одном символе в одном подканале. Соответственно емкость OFDM-символа составляет от 48 до 288 бит.

Последовательность обработки входных данных (битов) в стандарте IEEE 802.11а выглядит следующим образом. Первоначально входной поток данных подвергается стандартной операции скрэмблирования. После этого поток данных поступает на сверточный кодер. Скорость сверточного кодирования (в сочетании с пунктурным кодированием) может составлять 1/2, 2/3 или 3/4. Поскольку скорость сверточного кодирования может быть разной, то при использовании одного и того же типа модуляции скорость передачи данных оказывается различной. Рассмотрим, к примеру, модуляцию BPSK, при которой скорость передачи данных составляет 6 или 9 Мбит/с. Длительность одного символа вместе с охранным интервалом равна 4 мкс, а значит, частота следования импульсов составит 250 кГц. Учитывая, что в каждом подканале кодируется по одному биту, а всего таких подканалов 48, получаем, что общая скорость передачи данных составит 250 кГц x 48 каналов = 12 МГц. Если при этом скорость сверточного кодирования равна 1/2 (на каждый информационный бит добавляется один служебный), информационная скорость окажется вдвое меньше полной скорости, то есть 6 Мбит/с. При скорости сверточного кодирования 3/4 на каждые три информационных бита добавляется один служебный, поэтому в данном случае полезная (информационная) скорость составляет 3/4 от полной скорости, то есть 9 Мбит/с. Аналогичным образом каждому типу модуляции соответствуют две различные скорости передачи (таблица 1.2).

Таблица 1.2 - Соотношение между скоростями передачи и типом модуляции в стандарте 802.11a

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Скорость передачи, Мбит/с | Тип модуляции | Скорость сверточного кодирования | Количество бит в одном символе в одном подканале | Общее количество бит в символе (48 подканало) | Количество информационных бит в символе |
| 6 | BPSK | 1/2 | 1 | 48 | 24 |
| 9 | BPSK | 3/4 | 1 | 48 | 36 |
| 12 | QPSK | 1/2 | 2 | 96 | 48 |
| 18 | QPSK | 3/4 | 2 | 96 | 72 |
| 24 | 16-QAM | 1/2 | 4 | 192 | 96 |
| 36 | 16-QAM | 3/4 | 4 | 192 | 144 |
| 48 | 64-QAM | 2/3 | 6 | 288 | 192 |
| 54 | 64-QAM | 3/4 | 6 | 288 | 216 |

После сверточного кодирования поток бит подвергается операции перемежения, или интерливинга. Суть ее заключается в изменении порядка следования бит в пределах одного OFDM-символа. Для этого последовательность входных бит разбивается на блоки, длина которых равна числу бит в OFDM-символе (NCBPS). Далее по определенному алгоритму производится двухэтапная перестановка бит в каждом блоке. На первом этапе биты переставляются таким образом, чтобы смежные биты при передаче OFDM-символа передавались на несмежных поднесущих. Алгоритм перестановки бит на этом этапе эквивалентен следующей процедуре. Первоначально блок бит длиной NCBPS построчно (строка за строкой) записывается в матрицу, содержащую 16 строк и NCBPS/16 рядов. Далее биты считываются из этой матрицы, но уже по рядам (или так же, как записывались, но из транспонированной матрицы). В результате такой операции первоначально соседние биты будут передаваться на несмежных поднесущих.

Затем следует этап второй перестановки битов, цель которого заключается в том, чтобы соседние биты не оказались одновременно в младших разрядах групп, определяющих модуляционный символ в сигнальном созвездии. То есть после второго этапа перестановки соседние биты оказываются попеременно в старших и младших разрядах групп. Делается это с целью улучшения помехоустойчивости передаваемого сигнала.

После перемежения последовательность бит разбивается на группы по числу позиций выбранного типа модуляции и формируются OFDM-символы.

Сформированные OFDM-символы подвергаются быстрому преобразованию Фурье, в результате чего формируются выходные синфазный и квадратурный сигналы, которые затем подвергаются стандартной обработке — модуляции.

1.3.3 Стандарт IEEE 802.11n

Этот стандарт был утверждён 11 сентября 2009. 802.11n по скорости передачи сравнима с проводными стандартами. Максимальная скорость передачи стандарта 802.11n примерно в 5 раз превышает производительность классического Wi-Fi.

Можно отметить следующие основные преимущества стандарта 802.11n:

– большая скорость передачи данных (около 300 Мбит/с);

– равномерное, устойчивое, надежное и качественное покрытие зоны действия станции, отсутствие непокрытых участков;

– совместимость с предыдущими версиями стандарта Wi-Fi.

Недостатки:

– большая мощность потребления;

– два рабочих диапазона (возможная замена оборудования);

– усложненная и более габаритная аппаратура.

Увеличение скорости передачи в стандарте IEEE 802.11n достигается, во-первых, благодаря удвоению ширины канала с 20 до 40 МГц, а во-вторых, за счет реализации технологии MIMO.

Технология MIMO (Multiple Input Multiple Output) предполагает применение нескольких передающих и принимающих антенн. По аналогии традиционные системы, то есть системы с одной передающей и одной принимающей антенной, называются SISO (Single Input Single Output).

Стандарт IEEE 802.11n основан на технологии OFDM-MIMO. Очень многие реализованные в нем технические детали позаимствованы из стандарта 802.11a, однако в стандарте IEEE 802.11n предусматривается использование как частотного диапазона, принятого для стандарта IEEE 802.11a, так и частотного диапазона, принятого для стандартов IEEE 802.11b/g. То есть устройства, поддерживающие стандарт IEEE 802.11n, могут работать в частотном диапазоне либо 5, либо 2,4 ГГц.

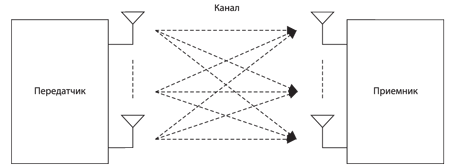


Рисунок 1.4 - Принцип реализации технологии MIMO

Передаваемая последовательность делится на параллельные потоки, из которых на приемном конце восстанавливается исходный сигнал. Здесь возникает некоторая сложность — каждая антенна принимает суперпозицию сигналов, которые необходимо отделять друг от друга. Для этого на приемном конце применяется специально разработанный алгоритм пространственного обнаружения сигнала. Этот алгоритм основан на выделении поднесущей и оказывается тем сложнее, чем больше их число. Единственным недостатком использования MIMO является сложность и громоздкость системы и, как следствие, более высокое потребление энергии.Для обеспечения совместимости MIMO-станций и традиционных станций предусмотрено три режима работы:

- Унаследованный режим (legacy mode).

- Смешанный режим (mixed mode).

- Режим зеленого поля (green field mode).

Каждому режиму работы соответствует своя структура преамбулы — служебного поля пакета, которое указывает на начало передачи и служит для синхронизации приемника и передатчика. В преамбуле содержится информация о длине пакета и его типе, включая вид модуляции, выбранный метод кодирования, а также все параметры кодирования. Для исключения конфликтов в работе станций MIMO и обычных (с одной антенной) во время обмена между станциями MIMO пакет сопровождается особой преамбулой и заголовком. Получив такую информацию, станции, работающие в унаследованном режиме, откладывают передачу до окончания сеанса между станциями MIMO. Кроме того, структура преамбулы определяет некоторые первичные задачи приемника, такие как оценка мощности принимаемого сигнала для системы автоматической регулировки усиления, обнаружение начала пакета, смещение по времени и частоте.

Режимы работы станций MIMO.

Унаследованный режим. Этот режим предусмотрен для обеспечения обмена между двумя станциями с одной антенной. Передача информации осуществляется по протоколам 802.11а. Если передатчиком является станция MIMO, а приемником — обычная станция, то в передающей системе используется только одна антенна и процесс передачи идет так же, как и в предыдущих версиях стандарта Wi-Fi. Если передача идет в обратном направлении — от обычной станции в многоантенную, то станция MIMO использует много приемных антенн, однако в этом случае скорость передачи не максимальная. Структура преамбулы в этом режиме такая же, как в версии 802.11а.

Смешанный режим. В этом режиме обмен осуществляется как между системами MIMO, так и между обычными станциями. В связи с этим системы MIMO генерируют два типа пакетов, в зависимости от типа приемника. С обычными станциями работа идет медленно, поскольку они не поддерживают работу на высоких скоростях, а между MIMO — значительно быстрее, однако скорость передачи ниже, чем в режиме зеленого поля. Преамбула в пакете от обычной станции такая же, что и в стандарте 802.11а, а в пакете MIMO она немного изменена. Если передатчиком выступает система MIMO, то каждая антенна передает не целую преамбулу, а циклически смещенную. За счет этого снижается мощность потребления станции, а канал используется более эффективно. Однако не все унаследованные станции могут работать в этом режиме. Дело в том, что если алгоритм синхронизации устройства основан на взаимной корреляции, то произойдет потеря синхронизации.

Режим зеленого поля. В этом режиме полностью используются преимущества систем MIMO. Передача возможна только между многоантенными станциями при наличии унаследованных приемников. Когда идет передача MIMO-системой, обычные станции ждут освобождения канала, чтобы избежать конфликтов. В режиме зеленого поля прием сигнала от систем, работающих по первым двум схемам, возможен, а передача им — нет. Это сделано для того, чтобы исключить из обмена одноантенные станции и тем самым повысить скорость работы. Пакеты сопровождаются преамбулами, которые поддерживаются только станциями MIMO. Все эти меры позволяют максимально использовать возможности систем MIMO-OFDM. Во всех режимах работы должна быть предусмотрена защита от влияния работы соседней станции, чтобы предотвратить искажения сигналов. На физическом уровне модели OSI для этого используются специальные поля в структуре преамбулы, которые оповещают станцию о том, что идет передача и необходимо определенное время ожидания. Некоторые методы защиты принимаются и на канальном уровне. В зависимости от используемой полосы пропускания режимы работы классифицируются следующим образом:

1. Наследуемый режим. Этот режим нужен для согласования с предыдущими версиями Wi-Fi. Он очень похож на 802.11a/g как по оборудованию, так и по полосе пропускания, которая составляет 20 МГц.

2. Двойной наследуемый режим. Устройства используют полосу 40 МГц, при этом одни и те же данные посылаются по верхнему и нижнему каналу (каждый шириной 20 МГц), но со смещением фазы на 90°. Структура пакета ориентирована на то, что приемником является обычная станция. Дублирование сигнала позволяет уменьшить искажения, повышая тем самым скорость передачи.

3. Режим с высокой пропускной способностью. Устройства поддерживают обе полосы частот — 20 и 40 МГц. В этом режиме станции обмениваются только пакетами MIMO. Скорость работы сети максимальна.

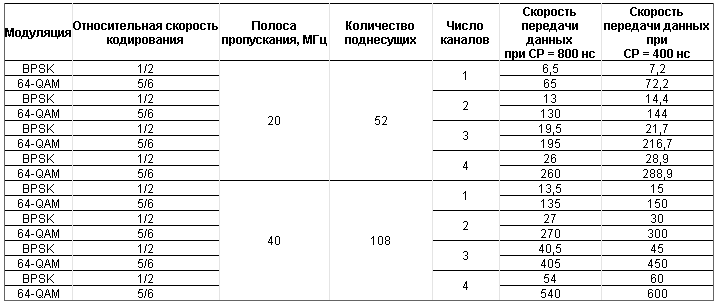
4. Режим верхнего канала. В этом режиме используется только верхняя половина диапазона 40 МГц. Станции могут обмениваться любыми пакетами.

5. Режим нижнего канала. В этом режиме используется только нижняя половина диапазона 40 МГц. Станции также могут обмениваться любыми пакетами.

Методы повышения быстродействия.

Скорость передачи данных зависит от многих факторов (таблица 1.3) и, прежде всего, от полосы пропускания. Чем она шире, тем выше скорость обмена. Второй фактор — количество параллельных потоков. В стандарте 802.11n максимальное число каналов равно 4. Также большое значение имеют тип модуляции и метод кодирования. Помехоустойчивые коды, которые обычно применяются в сетях, предполагают внесение некоторой избыточности. Если защитных битов будет слишком много, то скорость передачи полезной информации снизится. В стандарте 802.11n максимальная относительная скорость кодирования составляет до 5/6, то есть на 5 битов данных приходится один избыточный. В таблице 3 приведены скорости обмена при квадратурной модуляции QAM и BPSK. Видно, что при прочих одинаковых параметрах модуляция QAM обеспечивает гораздо большую скорость работы.

Таблица 1.3 - Скорость передачи данных при различных типах модуляции



Передатчики и приемники 802.11n

В стандарте IEEE 802.11n допускается использование до четырех антенн у точки доступа и беспроводного адаптера. Обязательный режим подразумевает поддержку двух антенн у точки доступа и одной антенны и беспроводного адаптера. В стандарте IEEE 802.11n предусмотрены как стандартные каналы связи шириной 20 МГц, так и каналы с удвоенной шириной. Общая структурная схема передатчика изображена на рисунке 1.5. Передаваемые данные проходят через скремблер, который вставляет в код дополнительные нули или единицы (так называемое маскирование псевдослучайным шумом), чтобы избежать длинных последовательностей одинаковых символов. Затем данные разделяются на N потоков и поступают на кодер с прямой коррекцией ошибок (FEC). Для систем с одной или двумя антеннами N = 1, а если используются три или четыре передающих канала, то N = 2.

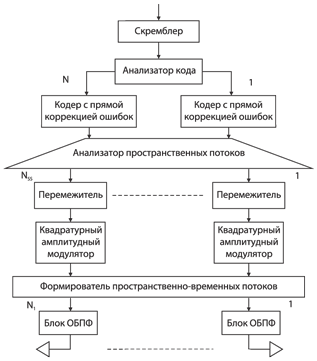


Рисунок 1.5 - Общая структура передатчика MIMO-OFDM

Кодированная последовательность разделяется на отдельные пространственные потоки. Биты в каждом потоке перемеживаются (для устранения блочных ошибок), а затем модулируются. Далее происходит формирование пространственно-временных потоков, которые проходят через блок обратного быстрого преобразования Фурье и поступают на антенны. Количество пространственно-временных потоков равно количеству антенн. Структура приемника аналогична структуре передатчика изображена на рисунке 1.6, но все действия выполняются в обратном порядке.

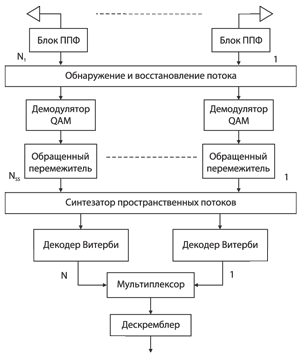


Рисунок 1.6 - Общая структура приемника MIMO-OFD

## 

## 1.4 Факторы более высокой скорости передачи данных стандарта 802.11n

Cтандарт 802.11n применяет три основных механизма для увеличения скорости передачи данных:

- применение нескольких приемопередатчиков и специальных алгоритмов передачи и приема радиосигнала, известный по аббревиатуре MIMO;

- увеличение полосы частот сигнала с 20 до 40 МГц;

- оптимизация протокола уровня доступа к сети.

Рассмотрим каждый из этих механизмов немного подробнее.

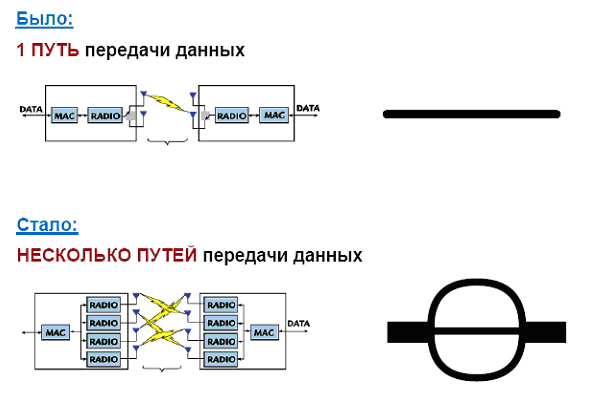


Рисунок 1.7 - Первый фактор увеличения скорости передачи данных

Первый фактор. С применением MIMO появляется возможность одновременно передавать несколько потоков данных в одном и том же канале, а затем при помощи сложных алгоритмов обработки восстанавливать их на приеме. Проводя аналогию с автодорогами, можно сказать, что ранее существовал только 1 путь, соединяющий точки А и Б. Теперь таких путей несколько и общая пропускная способность системы увеличилась.

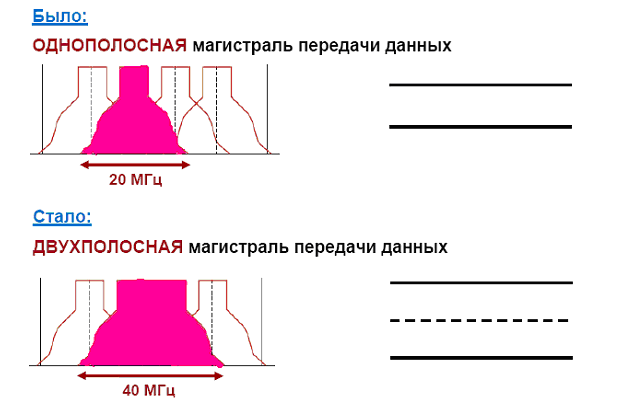


Рисунок 1.8 - Второй фактор увеличения скорости передачи данных

Второй фактор – увеличение доступной ширины полосы частот. Теоретически достижимая пропускная способность канала связи напрямую зависит от ширины занимаемой им полосы частот. В новом стандарте появилась возможность объединять соседние каналы по 20 МГц и таким образом увеличивать пропускную способность практически в 2 раза. По аналогии с автомагистралями можно считать, что вдвое увеличивается количество доступных для движения полос.

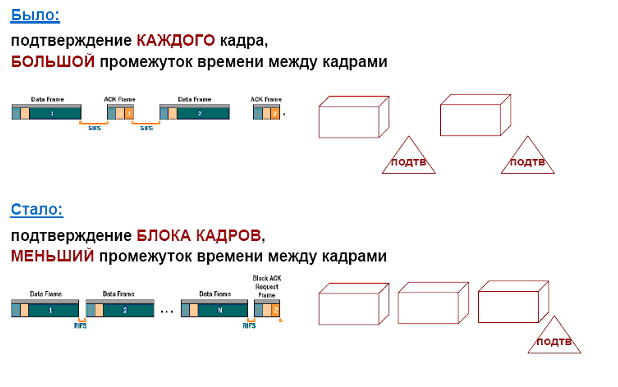


Рисунок 1.9 - Третий фактор увеличения скорости передачи данных

Первые два фактора относились к физическому каналу. Третий важный фактор увеличения производительности – оптимизация протокола передачи данных на уровне доступа к среде. В предыдущих версиях прием каждого переданного кадра (порции данных) должен был подтверждаться приемной стороной. В новой версии введена возможность блокового подтверждения. Приемник информации передает одно подтверждение сразу на несколько успешно принятых кадров, что уменьшает загрузку общей пропускной способности канала служебными сообщениями. Кроме того, уменьшен временной промежуток между кадрами, что также позволило повысить полезную пропускную способность. Проводя аналогии с повседневной жизнью, можно сравнить кадры с контейнерами для перевозок грузов. Новые правила 802.11 n позволили уменьшить дистанцию между контейнерами и позволили диспетчеру подтверждать не каждый груз в отдельности, а сразу партию грузов.

## 1.5 Топологии беспроводных сетей Wi-Fi

Сети стандарта 802.11 могут строиться по любой из следующих топологий:

* Независимые базовые зоны обслуживания (Independent Basic Service Sets, IBSSs);
* Базовые зоны обслуживания (Basic Service Sets, BSSs);
* Расширенные зоны обслуживания (Extended Service Sets, ESSs).

Независимые базовые зоны обслуживания (IBSS)

IBSS представляет собой группу работающих в соответствии со стандартом 802.11 станций, связывающихся непосредственно одна с другой. На рисунке 1.10 показано, как станции, оборудованные беспроводными сетевыми интерфейсными картами (network interface card, NIC) стандарта 802.11, могут формировать IBSS и напрямую связываться одна с другой.



Рисунок 1.10 - Ad-Hoc сеть (IBSS)

Специальная сеть, или независимая базовая зона обслуживания (IBSS), возникает, когда отдельные устройства-клиенты формируют самоподдерживающуюся сеть без использования отдельной точки доступа (AP – Access Point). При создании таких сетей не разрабатывают какие-либо карты места их развертывания и предварительные планы, поэтому они обычно невелики и имеют ограниченную протяженность, достаточную для передачи совместно используемых данных при возникновении такой необходимости.

Поскольку в IBSS отсутствует точка доступа, распределение времени (timing) осуществляется нецентрализованно. Клиент, начинающий передачу в IBSS, задает сигнальный (маячковый) интервал (beacon interval) для создания набора моментов времени передачи маячкового сигнала (set of target beacon transmission time, TBTT). Когда завершается ТВТТ, каждый клиент IBSS выполняет следующее:

* Приостанавливает все несработавшие таймеры задержки (backoff timer) из предыдущего ТВТТ;
* Определяет новую случайную задержку;

Базовые зоны обслуживания (BSS)

BSS - это группа работающих по стандарту 802.11 станций, связывающихся одна с другой. Технология BSS предполагает наличие особой станции, которая называется точка доступа AP (Access Point). Точка доступа - это центральный пункт связи для всех станций BSS. Клиентские станции не связываются непосредственно одна с другой. Вместо этого они связываются с точкой доступа, а уже она направляет кадры к станции-адресату. Точка доступа может иметь порт восходящего канала (uplink port), через который BSS подключается к проводной сети (например, восходящий канал Ethernet). Поэтому BSS иногда называют инфраструктурой BSS. На рисунке 1.11 представлена типичная инфраструктура BSS.



Рисунок 1.11 - Инфраструктура локальной беспроводной сети BSS

Расширенные зоны обслуживания (ESS)

Несколько инфраструктур BSS могут быть соединены через их интерфейсы восходящего канала. Там, где действует стандарт 802.11, интерфейс восходящего канала соединяет BBS с распределительной системой (Distribution System, DS). Несколько BBS, соединённых между собой через распределительную систему, образуют расширенную зону обслуживания (ESS). Восходящий канал к распределительной системе не обязательно должен использовать проводное соединение. На рисунке 1.12 представлен пример практического воплощения ESS. Спецификация стандарта 802.11 оставляет возможность реализации этого канала в виде беспроводного. Но чаще восходящие каналы к распределительной системе представляют собой каналы проводной технологии Ethernet.



Рисунок 1.12 - Расширенная зона обслуживания ESS беспроводной сети

**1.6** **Беспроводное оборудование, применяемое в Wi-Fi сетях**

Сегодня беспроводные сети позволяют предоставить подключение пользователей там, где затруднено кабельное подключение или необходима полная мобильность. При этом беспроводные сети без проблем взаимодействуют с проводными сетями.

1.6.1 Точки доступа Wi-Fi.

Все точки доступа можно разделить по способу подключения: через USB порт и порт подключения Ethernet - RJ45. Последние пользуются наибольшим успехом, так как наиболее просты в настройке и управлении, а также обладают большей скоростью передачи в локальную сеть. Точки доступа могут быть комнатного (in door) и всепогодного (out door) исполнения.Для создания беспроводной сети внутри помещений используют комнатный вариант прибора. Он обладает меньшей стоимостью и, как правило, большим эстетическим видом. Работают такие точки доступа в пределах одной или нескольких комнат. На открытых участках местности (прямая видимость) возможна работа на расстоянии до 300 метров с использованием стандартных всенаправленных антенн. Точки доступа всепогодного исполнения предназначены для создания радиосети между зданиями. В зависимости от типов антенн такие устройства способны организовывать каналы связи на расстоянии порядка 3-5 км. Максимальная дальность беспроводного канала связи заметно увеличивается при использовании усилителей. В этом случае длина радиоканала достигает 8-10 км. Устройства типа точка доступа представлены на рисунке 1.13.

Комбинированные устройства.

Большой интерес вызывают беспроводные точки доступа, объединяющие в себе функции других устройств, например, высокоскоростного беспроводного широкополосного маршрутизатора со встроенным коммутатором Fast Ethernet. Маршрутизатор позволяет быстро и легко настроить общий доступ к Интернет для проводной или беспроводной сети или организовать совместное использование широкополосного канала связи и кабельного/DSL модема дома или в офисе.

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| а | б | в | г |
| Рисунок 1.13 - Виды точек доступа: а, б – внутренние; в, г – внешние | | | |

1.6.2 Wi-Fi адаптеры.

Для подключения к беспроводной сети Wi-Fi достаточно обладать ноутбуком или карманным персональным компьютером (КПК) с подключенным Wi-Fi адаптером.

Любой беспроводной Wi-Fi адаптер должен соответствовать нескольким требованиям:

1. необходима совместимость со стандартами;
2. работа в диапазоне частот 2,4 ГГц - 2,435 ГГц (или 5 ГГц);
3. поддерживать протоколы WEP и желательно WPA;
4. поддерживать два типа соединения "точка-точка", и "компьютер сервер";
5. поддерживать функцию роуминга.

Существует три основных разновидности Wi-Fi адаптеров, различаемых по типу подключения:

Подключаемые к USB порту компьютера. Такие адаптеры компактны, их легко настраивать, а USB интерфейс обеспечивает функцию "горячего подключения";

Подключаемые через PCMCIA слот (CardBus) компьютера. Такие устройства располагаются внутри компьютера (ноутбука) и поддерживают любые стандарты, позволяющие передавать информацию со скоростью до 108 Мбит/с;

Устройства, интегрированные непосредственно в материнскую плату компьютера. Самый перспективный вариант. Такие адаптеры устанавливаются на ноутбуки серии Intel Centrino. И, в настоящее время используются на подавляющем большинстве мобильных компьютеров. Все виды беспроводных адаптеров представлены на рисунке 1.14.

|  |  |  |
| --- | --- | --- |
|  |  |  |
| а | б | в |
| Рисунок 1.14 - Беспроводные адаптеры:  а – с USB портом, б – формата PCMCIA, в – встроенный в материнскую плату | | |

**2 РЕАЛИЗАЦИЯ СЕТИ БЕСПРВОДНОГО ДОСТУПА**

## 2.1 Место реализации проекта

Предприятием на основе которого будет внедряется этот проект выбрано ОАО «Казахтелеком», так как на сегодняшний день ОАО «Казахтелеком» является лидером телекоммуникационных услуг на территории всей республики. Место реализации беспроводного доступа общежитие №2 Алматинского Института Энергетики и Связи.

Основными видами деятельности ОАО «Казахтелеком» являются:

* Предоставление услуг местной телефонной связи;
* Предоставление услуг междугородной и международной связи;
* Предоставление доступа к сетям передачи данных;
* Реализация таксофонных карт;
* Услуги интеллектуальной сети;

В настоящее время развитие традиционных коммутационных систем практически прекращено. В основном идет процесс адаптации к сетям нового поколения. Для максимального захвата рынка и значительного увеличения доходов от услуг телекоммуникаций требуется не только модернизация телекоммуникационной сети, но и внедрение новых технологий, необходимое для предоставления всего спектра современных услуг для всех абонентов.

Необходимость и актуальность организации сети беспроводного доступа, на базе технологии Wi-Fi, в общежитии АИЭС, обусловлена растущей потребностью студентов к повышению уровня информатизации. Уровень информатизации можно повысить с помощью современных услуг связи: высокоскоростной доступ в Интернет, компьютерная сеть.

Для удовлетворения потребности будет использоваться оборудование на базе стандарта 802.11n (Wi-Fi).

Задачи проекта:

* Развертывание сети беспроводного доступа Wi-Fi в общежитии №2 Алматинского Института Энергетики и Связи
* Удовлетворение существующего и прогнозируемого спроса на услуги телекоммуникаций.
* Закрепление положительного имиджа АО «Казахтелеком», как оператора, предоставляющего различные виды услуги телекоммуникаций в нужное время и в нужном месте;
* Удержание и захват высокодоходных рыночных сегментов;
* Повышение уровня информатизации студентов.

Область применения технологий беспроводного доступа Wi-Fi:

* Экономическая нецелесообразность подключения по проводной линии;
* Быстрый захват потенциальных абонентов.
* Обеспечение высокой скорости передачи данных.

**2.2 Техническое решение проекта**

Проект «Беспрводной доступ Wi-Fi в общежитии АИЭС» базируется на оборудовании c поддержкой стандарта 802.11n, получившим сертификат Wi-Fi. Wi-Fi покрывает всю территорию общежития и обьединяет всех пользователей в единую сеть с доступом в интернет. Сеть осуществляется установленными по всей территории общежития беспроводными унифицированными точками доступа, управляемыми беспроводным коммутатором.

## 2.3 Описание и характеристика выбранного оборудования

Точка доступа

D-Link DWL-8600AP - унифицированная беспроводная точка доступа следующего поколения, соответствующая стандарту IEEE 802.11n. Гибкая в управлении и мощная, данная точка доступа предназначена для развертывания сетей в режиме автономной беспроводной точки доступа или в режиме управляемой точки доступа, управление которой осуществляется при подключении к беспроводному коммутатору. Предприятия могут начать работу с организации сети с помощью одной интеллектуальной точки доступа DWL-8600AP, предоставляющей ряд расширенных функций LAN, а затем в любое время перейти к централизованной системе управления после подключения аналогичной точки доступа DWL-8600AP к унифицированному проводному/беспроводному коммутатору D-Link.

Стандарт 802.11n увеличивает пропускную способность в 6 раз больше по сравнению с сетями стандарта 802.11a/g. Точка доступа DWL-8600AP является обратно совместимой с устройствами стандарта 802.1a/b/g и позволяет настройку 2x2:2\* в обоих направлениях Tx/Rx. Технология Multiple In Multiple Out (MIMO) и каналы с увеличенной пропускной способностью увеличивают физическую скорость передачи данных при использовании стандарта 802.11n. MIMO обеспечивает одновременную передачу нескольких сигналов с помощью нескольких антенн вместо одной. Использование DWL-8600AP на предприятии подготавливает платформу для будущего поколения беспроводных устройств и мобильных приложений.

DWL-8600AP поддерживает функцию APSD (Автоматический переход в режим сохранения энергии) по расписанию и вне расписания. Выполняемая вне расписания функция APSD (U-APSD) является более эффективным методом управления питанием по сравнению с функцией Power Save Polling 802.11. Основным преимуществом функции U-APSD является возможность синхронизации передачи и получения голосовых фреймов с точкой доступа, таким образом, устройство может переходить в режим сохранения энергии в случае, когда не выполняется отправка или прием пакетов. DWL-8600AP является полностью совместимой с устройствами стандарта 802.3af даже в режиме максимально потребляемой мощности. В отличие от точки доступа стандарта 802.11n других производителей, которым требуется PoE или 802.3at при работе обеих частот, DWL-8600AP обеспечивает непрерывную поддержку энергосберегающей технологии D-Link Green. Вид DWL-8600AP представлен на рисунке 20.



Рисунок 2.1 – беспроводная точка доступа DWL-8600AP

Коммутаторы DWS-4026 автоматически настраивают каждую подключенную точку доступа DWL-8600AP, таким образом, во время установки не требуется настройка. При замене DWL-8600AP выполняется автоматическая настройка точки доступа с теми же параметрами, что и у предыдущего устройства, что значительно упрощает процесс замены.

DWL-8600AP поддерживает набор встроенных функций, позволяющий администраторам организовать защищенную сеть и подключиться к любому коммутатору и маршрутизатору, совместимому с устройствами Ethernet. Расширенные функции беспроводной сети, поддерживаемые точкой доступа, включают: WEP-шифрование данных, безопасность WPA/WPA2, фильтрация MAC-адресов, балансировка нагрузки между точками доступа, QoS/WMM (Wireless Media) и обнаружение несанкционированных точек доступа. DWL-8600AP поддерживает возможность локального хранения настроек безопасности. Можно расширить беспроводные подключения путем добавления нескольких точек доступа DWL-8600AP к другим точкам доступа с поддержкой стандарта 802.11a/g/n. Благодаря функции AP Clustering можно объединить до 8 точек доступа для удобства управления и настройки всех точек доступа. Предприятия, не требующие сложной сетевой инфраструктуры, могут использовать DWL-8600AP для установки беспроводной сети без дополнительного аппаратного обеспечения.

В качестве альтернативного варианта DWL-8600AP может работать совместно с унифицированным проводным/беспроводным коммутатором. В данном режиме несколько точек доступа DWL-8600AP могут быть подключены непосредственно или опосредованно к одному из данных коммутаторов для обеспечения высокого уровня безопасности и беспроводной мобильности. При подключении к этим коммутаторам каждая точка доступа DWL-8600AP автоматически настраивается на оптимальный радиочастотный канал и выходную мощность передатчика, обеспечивая беспроводных клиентов сигналом наилучшего качества как в полосе 2,4ГГц, так и в полосе 5ГГц, предоставляя непрерывное беспроводное соединение.

DWL-8600AP обеспечивает максимальную скорость беспроводного соединения для каждого из частотных диапазонов. При одновременной работе в двух диапазонах частот можно создать две сети, использующие полную полосу пропускания беспроводного канала, что позволит повысить общую производительность беспроводной сети. Кроме того, DWL-8600AP остается полностью обратно совместимой с оборудованием стандарта 802.11b, работающим на частоте 2,4ГГц.

Большинство из существующих контролеров сети LAN осуществляет централизованную обработку трафика, что иногда вызывает его неоправданную задержку. Точка доступа DWL-8600AP – при подключении к коммутатору DWS-4026 – предоставляет администраторам ряд дополнительных функций. В зависимости от беспроводного приложения, беспроводной трафик может направляться обратно к коммутатору в целях обеспечения общей безопасности или локально перенаправляться к точке доступа для оптимальной производительности. Точка доступа данной серии предоставляет администраторам максимальную гибкость управления, благодаря опциям перенаправления гостевого трафика к коммутатору для централизованного управления безопасностью и перенаправления VoIP-трафика непосредственно к точке доступа для оптимальной производительности. Более того, DWL-8600AP поддерживает функции AP Clustering и Wireless Distribution System (WDS). Функция WDS позволяет точке доступа работать в режиме беспроводного моста, объединяя две различные сети без необходимости подключения кабеля.

DWL-8600AP непрерывно сканирует оба диапазона частот и связанные с ними каналы для обнаружения несанкционированных подключений, обеспечивая при этом соединение для мобильных клиентов. Если обнаружено несанкционированное подключение, точка доступа отправляет отчет коммутатору DWS-4026, который ей управляет. Используя управляющую консоль, администратор может определить несанкционированную точку доступа и предпринять соответствующие действия. DWL-8600AP поддерживает такие функции как 64/128/152-битное WEP-шифрование данных, WPA/WPA2 и Multiple SSID для каждого радиочастотного канала. При подключении к коммутатору DWS-4026 эти функции наряду с фильтрацией MAC-адресов и запретом широковещания SSID могут использоваться для настройки параметров безопасности и ограничения доступа во внутреннюю сеть извне. DWL-8600AP поддерживает 802.1Q VLAN Tagging и WMM (Wi-Fi Multimedia) для передачи данных таких приложений как VoIP и потоковое аудио/видео с заданным приоритетом. Общие характеристики представлены в таблице 2.1.

Таблица 2.1 – общие характеристики оборудования DWL-8600AP

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Модель | | DWL-8600AP | | | | | | | | |
| Производитель | | D-Link | | | | | | | | |
| Стандарты | | • IEEE 802.11a, 802.11b, 802.11g, 802.11n Wireless LAN  • IEEE 802.3, 802.3u Ethernet  • IEEE 802.11d Regulatory Domain Selection  • IEEE 802.11h  • Управление потоком IEEE 802.3x  • IEEE 802.3af Power over Ethernet (PoE) | | | | | | | | |
| Скорость передачи данных | | • Для 802.11a/g: 54, 48, 36, 24, 18, 12, 9 и 6 Мбит/с  • Для 802.11b: 11, 5.5, 2 и 1 Мбит/с  • Для 802.11n:   |  |  |  |  |  | | --- | --- | --- | --- | --- | | GI3=800нс | | | GI=400нс | | | Индекс MCS2 | 20МГц (Мбит/с) | 40МГц (Мбит/с) | 20МГц (Мбит/с) | 40МГц (Мбит/с) | | 0  1  2  3  4  5  6  7  8  9  10  11  12  13  14  15 | 6,5  13  19,5  26  39  52  58,5  65  13  26  39  52  78  104  117  130 | 13,5  27  40,5  54  81  108  121,5  135  27  54  81  108  162  216  243  270 | 7,2  14,4  21,7  28,9  43,3  57,8  65  72,2  14,4  28,9  43,3  57,8  86,7  115,6  130  144,4 | 15  30  45  60  90  120  135  150  30  60  90  120  180  240  270  300 | | | | | | | | | |
|  | |  | | | | | | | | |
| *Продолжение таблицы 2.1* | | | | | | | | | | |
| Диапазон частот | | • 802.11a: от 5,15 ГГц до 5,35 ГГц и от 5,725 ГГц до 5,825 ГГц  • 802.11b/g: от 2,4 ГГц до 2,4835 ГГц  • 802.11n: от 2,4 ГГц до 2,497 ГГц и от 4,9 ГГц до 5,85 ГГц | | | | | | | | |
| Технологии модуляции | | • Для 802.11b (DSSS): DBPSK @ 1 Мбит/с, DQPSK @ 2 Мбит/с, CCK @ 5,5 and 11 Мбит/с  • Для 802.11a/g (OFDM): BPSK @ 6 и 9 Мбит/с, QPSK @ 12 и 18 Мбит/с, 16QAM @ 24 и 36 Мбит/с, 64QAM @ 48, 54 Мбит/с  • Для 802.11a/g (DSSS): DBPSK @ 1 Мбит/с, DQPSK @ 2 Мбит/с, CCK @ 5,5 и 11 Мбит/с  • Для 802.11n: PSK/CCK, DQPSK, DBPSK, OFDM | | | | | | | | |
| Радиочастотные каналы | | • 5ГГц: 12 неперекрывающихся каналов для США и Канады, 8 неперекрывающихся каналов для Японии, 19 неперекрывающихся каналов для стран Европейского союза, 5 неперекрывающихся каналов для Китая  • 2,4ГГц: 11каналов для США, 13 каналов для стран Европейского союза, 13 каналов для Японии | | | | | | | | |
| Выходная мощность передатчика4 (Типичная для каждой скорости соединения) | | • 802.11a:  17dBm при 6/9/12/18 Мбит/с  15dBm при 24/36 Мбит/с  14dBm при 48 Мбит/с  13dBm при 54 Мбит/с  • 802.11b:  17dBm при 1/2/5.5/11 Мбит/с  • 802.11g:  17dBm при 6/9/12/18 Мбит/с  16dBm при 24/36 Мбит/с  15dBm при 48 Мбит/с  14dBm при 54 Мбит/с  • 802.11n: | | | | | | | | |
| 5GHz Band/HT-20  17dBm при MCS0/8  17 dBm при MCS1/9  17 dBm при MCS2/10  15 dBm при MCS3/11  15 dBm при MCS4/12  14 dBm при MCS5/13  13 dBm при MCS6/14  12 dBm при MCS7/15 | | 5GHz Band/HT-40  16 dBm при MCS0/8  16 dBm при MCS1/9  16 dBm при MCS2/10  14 dBm при MCS3/11  14 dBm при MCS4/12  13 dBm при MCS5/13  12 dBm при MCS6/14  11 dBm при MCS7/15 | | | 2.4GHz Band/HT-20  17 dBm при MCS0/8  17 dBm при MCS1/9  17 dBm при MCS2/10  16 dBm при MCS3/11  16 dBm при MCS4/12  15 dBm при MCS5/13  14 dBm при MCS6/14  13 dBm при MCS7/15 | | 2.4GHz Band/HT-40  16 dBm при MCS0/8  16 dBm при MCS1/9  16 dBm при MCS2/10  15 dBm при MCS3/11  15 dBm при MCS4/12  14 dBm при MCS5/13  13 dBm при MCS6/14  12 dBm при MCS7/15 | |
|  | |  | | | | | | | | |
| *Продолжение таблицы 2.1* | | | | | | | | | | |
| Чувствительность приемника | • 802.11a:  -87dBm при 6 Мбит/с  -86dBm при 9 Мбит/с  -84dBm при 12 Мбит/с  -81dBm при 18 Мбит/с  -77dBm при 24 Мбит/с  -75dBm при 36 Мбит/с  -68dBm при 48 Мбит/с  -67dBm при 54 Мбит/с  • 802.11b:  -92dBm при 1 Мбит/с  -90dBm при 2 Мбит/с  -88dBm при 5.5 Мбит/с  -84dBm при 11 Мбит/с  • 802.11g:  -87dBm при 6 Мбит/с  -87dBm при 9 Мбит/с  -85dBm при 12 Мбит/с  -82dBm при 18 Мбит/с  -79dBm при 24 Мбит/с  -76dBm при 36 Мбит/с  -71dBm при 48 Мбит/с  -70dBm при 64 Мбит/с  802.11n: | | | | | | | | | |
| 5GHz Band/HT-20 | | 5GHz Band/HT-40 | | | 2.4GHz Band/HT-20 | | | | 2.4GHz Band/HT-40 |
| –82dBm при MCS0/8  –79 dBm at MCS1/9  –77 dBm при MCS2/10  –74 dBm при MCS3/11  –70 dBm при MCS4/12  –66 dBm при MCS5/13  –65 dBm при MCS6/14  –64 dBm | | –79 dBm при MCS0/8  –76 dBm at MCS1/9  –74 dBm at MCS2/10  –71 dBm at MCS3/11  –67 dBm at MCS4/12  –63 dBm at MCS5/13  –62 dBm at MCS6/14  –61 dBm | | | -85 dBm при MCS0/8  -82 dBm при MCS1/9  -80 dBm при MCS2/10  -77 dBm при MCS3/11  -74 dBm при MCS4/12  -69 dBm при MCS5/13  -68 dBm при MCS6/14  -67 dBm | | | | -82 dBm при MCS0/8  -79 dBm при MCS1/9  -77 dBm при MCS2/10  -74 dBm при MCS3/11  -71 dBm при MCS4/12  -66 dBm при MCS5/13  -65 dBm при MCS6/14  -63 dBm |
| Антенны | • 4 дипольных съемных всенаправленных антенны с реверсным разъемом SMA  • Коэффициент усиления: 6dBi для частоты 5ГГц, 4dBi для частоты 2,4 ГГц | | | | | | | | | |
| Интерфейс Ethernet | Порт 10/100/1000BASE-T с 802.3af PoE | | | | | | | | | |
| Настраиваемый режим работы | • Только «Точка доступа»  • «Точка доступа» с Wireless Distribution System (WDS)  • Wireless Distribution System (WDS) | | | | | | | | | |
|  | | | | | | | | | | |
| *Продолжение таблицы 2.1* | | | | | | | | | | |
| Безопасность | | • 64/128/152-битное WEP-шифрование данных  • Фильтрация MAC-адресов: через RADIUS или локальную базу данных  • WPA/WPA2 EAP  • TKIP/AES  •802.11i/WPA2: Поддержка предварительной аутентификации и кэширования ключей для WPA2 Enterprise  • Включение/запрещение широковещания 802.1Q SSID  • 16 SSID для каждого частотного диапазона  • RADIUS (RFC 2865, 3580): Поддержка аутентификации c сервером RADIUS, до 4 внешних серверов RADIUS  •Изолированная безопасность для каждого SSID (различные параметры безопасности для каждого SSID)  • Изоляция станции | | | | | | | | |
| Поддерживаемые протоколы/методы управления | | •Используются протоколы, поддерживаемые унифицированными коммутаторами DWS-4026  • HTTP/HTTPS  • SSH  • SNMP  • Системный журнал  • Telnet | | | | | | | | |
| Возможности | | | Автономный режим | | | Управляемый режим (DWS-4026) | | |
| Централизованное управление | | | - | | | + | | |
| Централизованное распределение программного обеспечения | | | - | | | + | | |
| Визуальные инструменты управления точкой доступа | | | - | | | + | | |
| Автоматическая настройка мощности | | | - | | | + | | |
| Динамический выбор канала | | | - | | | + | | |
| Быстрый роуминг L2 | | | - | | | + | | |
| Быстрый роуминг L3 | | | - | | | + | | |
| Адаптивный портал | | | - | | | + | | |
| Протоколы безопасности WEP/WPA/WPA2 | | | + | | | + | | |
| Обнаружение несанкционированнх точек доступа | | | + | | | + | | |
|  | |  | | |  | | |  | | |
| *Продолжение таблицы 2.1* | | | | | | | | | | |
|  | | Минимизация несанкционированных точек доступа | | | - | | | + | | |
| WIDS | | | - | | | + | | |
| Изоляция станции | | | + | | | + | | |
| Фильтрация MAC-адресов | | | + | | | + | | |
| Балансировка нагрузки между точками доступа | | | + | | | + | | |
| WDS | | | + | | | - | | |
| Функция AP Clustering | | | + | | | - | | |
| QoS/WMM | | | + | | | + | | |
| Локальное хранение конфигурационного файла | | | + | | | - | | |
| Индикаторы диагностики | | • Power  • LAN  • 2.4GHz  • 5.0GHz | | | | | | | | |
| Питание | | • Рабочее напряжение: 48В постоянного тока  •/- 10% для PoE  • Источник питания: через внешний адаптер питания 48В постоянного тока, 0,4А  • Потребляемая мощность: Макс.11 Вт без Poe, Макс. 12 Вт с PoE | | | | | | | | |
| Размеры | | 190,5 х 198,8 х 36,8 мм | | | | | | | | |
| Вес | | 1,02кг | | | | | | | | |
| Рабочая температура | | От 0° до 40°С | | | | | | | | |
| Температура при хранении | | От -20° до 65°С | | | | | | | | |
| Рабочая влажность | | От 10% до 90% (без образования конденсата) | | | | | | | | |
| Влажность при хранении | | От 5% до 95% (без образования конденсата) | | | | | | | | |
| MTBF | | 523,721 час | | | | | | | | |
| Сертификаты | | • FCC Class B  • CE  • C-Tick  • VCCI  • TELEC  • Wi-Fi  • ICES-003  • EN60601-1-2  • NCC  • CSA International | | | | | | | | |

Беспроводной коммутатор

Серия коммутаторов DWS-4026 включает в себя унифицированные проводные/беспроводные коммутаторы Gigabit Ethernet следующего поколения, поддерживающие ряд расширенных функций и стандарт 802.11n. Благодаря возможности управления до 64 беспроводных точек доступа DWL-8600AP и до 256 точек доступа DWL-8600AP в кластере коммутаторов, DWS-4026 является полнофункциональным и экономичным решением для среднего и крупного бизнеса и провайдеров услуг. Коммутатор DWS-4026 поддерживает гибкие функции управления и, в зависимости от требований клиента, используется в качестве беспроводного контроллера в базовой/беспроводной сети или гигабитного коммутатора уровня 2+ с поддержкой PoE для конечных пользователей. С помощью настройки централизованного управления WLAN и функций управления, DWS-4026 позволяет сетевым администраторам поддерживать управление, безопасность, резервирование и отказоустойчивость, необходимые для простого и эффективного масштабирования и управления сетями. Вид DWS-4026 представлен на рисунке 2.3.



Рисунок 2.3 – беспроводной коммутатор DWS-4026

Большинство из существующих контроллеров сети LAN осуществляет централизованную обработку трафика, что иногда вызывает его неоправданную задержку. Коммутаторы DWS-4026 предоставляют пользователям дополнительные функции. В зависимости от беспроводного приложения, беспроводной трафик может направляться обратно к коммутатору в целях обеспечения большей безопасности или локально перенаправляться к точке доступа для оптимальной производительности. Коммутаторы данной серии предоставляют администраторам максимальную гибкость благодаря опциям туннелирования трафика клиента к коммутатору для централизованного управления безопасностью и перенаправления трафика непосредственно от точки доступа для оптимальной производительности. DWS-4026 поддерживает новейшую функцию Wireless Intrusion Detection System (WIDS), предназначенную для обнаружения несанкционированных точек доступа и несанкционированных клиентов, а также различных угроз безопасности беспроводной сети. С помощью функции WIDS администраторы могут обнаружить различные угрозы и использовать сканирование радиочастотных каналов для обзора беспроводной сети в целях предотвращения любых потенциальных угроз безопасности. Другими функциями безопасности являются WPA/WPA2 Enterprise, 802.11i, адаптивный портал и аутентификация на основе MAC-адресов. Для проводных клиентов DWS-4026 использует функцию Dynamic ARP Inspection (DAI) и DHCP Snooping для обеспечения максимальной безопасности. Совместное использование функций Dynamic ARP Inspection (DAI) и DHCP Snooping предотвращает угрозы самого высокого уровня, например, “man-in-the-middle” и ARP poisoning. Благодаря поддержке остальных расширенных функций безопасности, таких как управление доступом 802.1X, предотвращение атак DoS, управление широковещательным штормом и защищенный порт, DWS-4026 обеспечивает надежную и централизованную безопасность, предоставляя максимальную отказоустойчивость сети.

Беспроводные клиенты могут воспользоваться преимуществами гибкого и непрерывного роуминга между точками доступа, управляемыми коммутатором DWS-4026 даже в том случае, если они не находятся в одной подсети. Так как DWS-4026 использует различные механизмы, такие как предварительная аутентификация и кэширование ключей, беспроводные клиенты могут свободно перемещаться в зоне действия сети без необходимости повторной аутентификации. Быстрый роуминг осуществляется без разрыва соединения, обеспечивая надежную работу соединения для таких мобильных приложений, как беспроводная IP-телефония и беспроводное подключение КПК. Более того, DWS-4026 поддерживает функцию туннелирования между точками доступа, которая используется для поддержки роуминга уровня 3 для беспроводных клиентов без перенаправления каких-либо данных трафика к унифицированному коммутатору. Это поможет значительно оптимизировать сетевой трафик и сохранить полосу пропускания.

DWS-4026 разработан и оптимизирован для трафика Voice over Wireless, благодаря таким функциями, как Auto-VoIP и Voice VLAN. Функция Auto-VoIP согласовывает потоки VoIP и предоставляет им обслуживание более высокого класса, чем для обычного трафика. Оборудование VoIP использует популярные протоколы управления вызовом, такие как SIP, H.323 и SCCP. Функция Voice VLAN позволяет портам коммутатора передавать голосовой трафик с определенным приоритетом, уровень приоритета обеспечивает разделение речевого трафика и трафика данных с высоким приоритетом, приходящих на порт. Voice QoS позволяет администраторам назначать приоритет трафику, чувствительному к задержкам, и сохранять его целостность.

Помимо этого, DWS-4026 поддерживает функцию формирования трафика, которая помогает упорядочить пакеты трафика с течением времени, таким образом, скорость передаваемого трафика ограничена. Другими расширенными функциями QoS являются: управление полосой пропускания на основе потока, минимальная гарантия по полосе пропускания и CoS 802.1p. Все эти функции помогают сохранить сетевой трафик соответствующим образом.

DWS-4026 поддерживает функцию «самовосстановления» сети, увеличивающей отказоустойчивость беспроводной сети. Чтобы восполнить недостаточную зону покрытия в результате выхода из строя точки доступа (например, из-за сбоя питания), коммутатор автоматически увеличивает выходную мощность передатчика соседних точек доступа, чтобы увеличить их зону покрытия. Для обеспечения непрерывного подключения существующих клиентов, коммутатор выполняет балансировку нагрузки между точками доступа, когда сетевой трафик достигает определенного порогового значения. В то же время коммутатор отклоняет подключение новых клиентов к точке доступа для того, чтобы избежать перегрузки полосы пропускания. Благодаря функции «самовосстановления» сети и балансировке нагрузки между точками доступа, коммутатор DWS-4026 может эффективно управлять полосой пропускания, оптимизировать трафик WLAN и обеспечить зону максимального покрытия.

Помимо функционирования в качестве управляющего устройства в беспроводной коммутации, DWS-4026 может также использоваться как стандартный проводной коммутатор уровня 2+ с расширенным функционалом, включая поддержку динамической маршрутизации пакетов (RIPv1/v2), функции безопасности ACL, многоуровневого качества обслуживания (QoS), VLAN, IGMP/MLD Snooping. Помимо этого, коммутаторы поддерживают оптические порты 10-Gigabit. Всё это позволяет предприятию объединять беспроводную сеть с проводной сетевой инфраструктурой. При замене существующей инфраструктуры 10/100 Мбит/с для подключения настольных компьютеров на гигабитное подключение можно использовать коммутатор DWS-4026 в качестве устройства управления беспроводной сетью, коммутатора LAN или универсального устройства, выполняющего функции проводного коммутатора и контроллера беспроводной сети.

Несколько коммутаторов DWS-4026 могут объединяться в кластер, позволяя администраторам настройку и управление всех коммутаторов с помощью одного коммутатора «Мастера». Помимо этого, в кластере можно управлять информацией обо всех точках доступа, а также клиентах, связанных с ними. Это значительно упрощает управление и позволяет снизить усилия, затрачиваемые на обслуживание при масштабировании сети.

Общие характеристики представлены в таблице 2.2.

Таблица 2.2 – общие характеристики оборудования DWS-4026

|  |  |
| --- | --- |
| Функции управления WLAN | +До 64 точек доступа, подключенных к коммутатору  + До 256 точек доступа в кластере  + До 2048 беспроводных клиентов (1024 пользователей при использовании туннелирования, 2048 пользователей, если туннелирование не используется) |
| Роуминг | + Быстрый роуминг  + Роуминг между коммутаторами и точками доступа, подключенными к одному коммутатору  + Внутри – и Меж- сетевой роуминг  + Туннелирование между точками доступа |
| Управление доступом и полосой пропускания | + До 32 SSID на точку доступа (16 SSID на радиочастотный диапазон)  + Балансировка загрузки между точками доступа на основе количества пользователей или использования точки доступа |
| Управляемые точки доступа | DWL-8600AP |
| Управление точками доступа | + Автоматическое обнаружение точек доступа  + Удаленная перезагрузка точек доступа  + Мониторинг точек доступа: список управляемых точек доступа, несанкционированных и не прошедших аутентификацию точек доступа  + Мониторинг клиентов: список клиентов ассоциированных с каждой управляемой точкой доступа  + Мониторинг клиентов Ad-hoc  + Аутентификация точек доступа с помощью локальной базы данных или внешнего сервера RADIUS  + Централизованное управление каналами/политиками безопасности  + Визуальные инструменты управления точками доступа (Поддержка до 16 jpg-файлов)  + Поддержка унифицированной точки доступа (DWL-8600AP): Управляемый/Автономный режим |
| Функции безопасности WLAN | + Wireless Intrusion Detection & Prevention System (WIDS)  + Минимизация несанкционированных точек доступа  + Классификация несанкционированных и действительных точек доступа на основе МАС-адреса  + WPA Personal/Enterprise  + WPA2 Personal/Enterprise  + 64/128/152-битное WEP-шифрование данных  + Классификация беспроводных станций и точек доступа на основе канала, MAC-адреса, SSID, времени  + Поддержка типа шифрования: WEP, WPA, Dynamic WEP, TKIP, AES-CCMP, EAP-FAST, EAP-TLS, EAP-TTLS, EAP- MD5, PEAP-GTC, PEAP-MS-CHAPv2, PEAP-TLS  + Аутентификация на основе МАС-адресов  + Изоляция станции |
|  | + Размер таблицы MAC-адресов: 8K записей  + IGMP Snooping: 1K многоадресных групп |
|  |  |
| *Продолжение Таблицы 2.2* | |
| Функции уровня 2 | + 8021.D Spanning Tree  + 802.1w Rapid Spanning Tree  + 802.1s Multiple Spanning Tree  + Link Aggregation 802.3ad: до 32 групп, до 8 портов в группе  + 802.1ab LLDP  + LLDP-MED  + One-to-One Port Mirroring  + Many-to-One Port Mirroring  + Размер Jumbo-фреймов: до 9Кб  VLAN  + 802.1Q VLAN Tagging  + 802.1V  + Группы VLAN: до 3965 записей  + VLAN на основе подсетей  + VLAN на основе MAC-адреса  + GVRP  + Double VLAN  + Voice VLAN |
| Функции уровня 3 | + Статическая маршрутизатизация IPv4  + Размер таблицы маршрутизации: до 128 статических маршрутов  + Плавающие статические маршруты  + VRRP  + Proxy ARP  + RIPv1/v2 |
| Quality of Service (Качество обслуживания) | + Очереди приоритетов 802.1p (до 8 очередей на порт)  + CoS на основе: порта коммутатора, VLAN, DSCP, порта TCP/UDP, TOS, MAC-адреса источника, IP-адреса источника  + Auto-VoIP  + Минимальная гарантия по полосе пропускания на очередь  + Формирование трафика на порт  + Управление полосой пропускания на основе потока |
| ACL (Список управления доступом) | ACL на основе: порта коммутатора, MAC-адреса, очередей приоритетов 802.1p, VLAN, Ethertype, DSCP, IP-адреса, типа протокола, номера порта TCP/UDP |
| Функции безопасности LAN | + Аутентификация RADIUS при административном доступе  + Аутентификация TACACS+ при административном доступе  + Функция Port Security: 20 MAC-адресов на порт, уведомление в случае срабатывания функции  + Фильтрация MAC-адресов  + Управление доступом 802.1x на основе портов и Guest  + Защита от атак DoS |
|  |  |
| *Продолжение Таблицы 2.2* | |
|  | + Dynamic ARP Inspection (DAI)  + DHCP Snooping  + Управление широковещательным штормом: шаг 1 % от скорости канала  + Защищенный порт  + DHCP-фильтрация |
| Методы управления | + Web-интерфейс  + Кластеризация коммутаторов  + Учетная запись RADIUS  + CLI  + Сервер Telnet: до 5 сессий  + Клиент Telnet  + Клиент TFTP  + SNMP v1, v2c, v3  + sFlow  + Несколько файлов конфигурации  + Поддержка двух копий ПО (Dual Images)  + RMON v1: 4 группы (Statistics (Статистика), History (История), Alarms (Уведомления), Events(События))  + Клиент BOOTP/DHCP  + Сервер DHCP  + DHCP Relay  + SYSLOG  + Описание портов |
| Интерфейсы устройства | + 24 порта 10/100/1000BASE-T с поддержкой PoE 802.3af  + 4 комбо-порта SFP  + Консольный порт RS-232  + 2 открытых слота для установки дополнительных модулей с портами 10 Gigabit |
| Резервный источник питания | Коннектор для подключения источника питания DPS-600 |
| Power over Ethernet | + Стандарт: 802.3af  + Выходная мощность на каждом порту: 15,4Вт  + Общая выходная мощность: 370 Вт  + Автоотключение порта при значении тока выше 350мА |
| Производительность | + Коммутационная матрица: 88 Гбит/с  + Макс. скорость передачи пакетов: 65,47 Mpps  + Метод коммутации: Store and Forward  + Размер буфера пакетов: 750 КБ |
| Управление потоком | + Управление потоком 802.3x в режиме полного дуплекса  + Метод «обратного давления» в полудуплексном режиме  + Предотвращение блокировок HOL |
| Дополнительные uplink-модули с портами 10GE | + DEM-410X Модуль с 1 слотом 10GE XFP (Для подключения к оптоволоконной магистрали сети)  + DEM-410CX Модуль с 1 портом 10GE CX4 (Для стекирования коммутаторов) |
|  |  |
| *Продолжение Таблицы 2.2* | |
| Дополнительные трансиверы XFP 10GE | + DEM-421XT Трансивер XFP 10GBASE-SR, MMF, макс.  расстояние до 300 м, 3,3/5В  + DEM-422XT Трансивер XFP 10GBASE-LR, SMF, макс. расстояние до10 км, 3,3/5В  + DEM-423XT Трансивер XFP 10GBASE-ER, SMF, макс. расстояние до 40 км, 3,3/5В |
| Индикаторы диагностики | + На устройство: Power, Console, RPS  + Для порта 10/100/1000BASE-T: Link/Activity/Speed, PoE  + Для слота SFP: Link/Activity  + Для слота 10 Gigabit: Link/Activity |
| Питание | + Питание: внутренний универсальный источник питания от 100 до 240 В переменного тока, 50/60 Гц  + Потребляемая мощность: 525 Вт (макс., при функционировании всех портов PoE) |
| MTBF | 185,540 часов |
| Размеры | + 440 (Ш) x 389 (Г) x 44 (В) мм  + Установка в 19” стойку, высота 1U |
| Вес | 6кг |
| Температура | + Рабочая температура: от 0° до 40° C  + Температура хранения: от -10° до 70° C |
| Влажность | + Рабочая влажность: от 10% до 90% без образования конденсата  + Влажность хранения: от 5% до 90% без образования конденсата |
| Электромагнитная совместимость | FCC Class A, ICES-003, VCCI, CE, C-Tick, EN 60601-1-2 |
| Безопасность | UL/cUL, CB |

## 2.4 Разработка структурной схемы организации сети

Беспроводная сеть, которую планируется реализовать, будет основана на новом стандарте IEEE 802.11n.

Сеть будет управляться сервером с помощью беспроводного коммутатора. Так как беспроводной коммутатор и точки доступа распространяют сигнал сферически, планируется установить по три точки доступа на втором и четвёртом этажах по всей площади общежития, а беспроводной коммутатор - на третьем этаже, в центре, для охвата каждой точки доступа. Схема беспроводной сети представлена на рисунке 2.4

Организация сети доступа

* Организовать сеть беспроводного доступа, для чего приобрести и установить 6 точек доступа DWL-8600AP по 3 точки на втором и четвертом этажах.
* Беспроводной коммутатор DWS-4026 разместить в рабочем помещении на третьем этаже.
* Настроить беспроводной коммутатор, определить точки доступа. Обеспечить мониторинг и защиту сети.
* Организация подключения к сети Internet. Доступ к сети Internet организовать через широкополосный /DSL модем.



Рисунок 2.4 – Схема беспроводной сети

## 

## 2.5 Программирование

При проектировании беспроводной сети Wi-Fi была разработана программа расчёта эффективной изотропной излучаемой мощности для удобства проведения расчетов. Приложение разработано на языке Delphi 7

Вид программы расчёта эффективной изотропной излучаемой мощности представлен на рисунке 2.5. Код показан в приложении E.

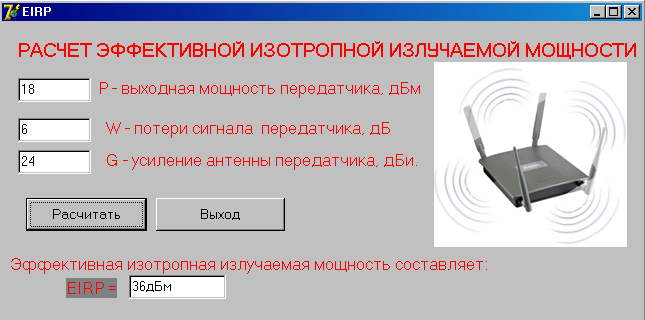


Рисунок 2.5 – Вид программы

**3 РАСЧЕТНАЯ ЧАСТЬ**

## 3.1 Расчет эффективной изотропной излучаемой мощности

Эффективная изотропная излучаемая мощность определяется по формуле:

EIRP = РПРД - WАФТпрд + GПРД, (3.1)

где РПРД - выходная мощность передатчика, дБм;

WАФТпрд - потери сигнала в АФТ передатчика, дБ;

GПРД - усиление антенны передатчика, дБи.

Расчет эффективной изотропной излучаемой мощности одной точки доступа (данные представлены в таблице 3.1)

Таблица 3.1 – Параметры данных

|  |  |  |  |
| --- | --- | --- | --- |
| Обозначение | Наименование | Ед. изм. | Значение |
| РПРД | выходная мощность передатчика | дБм | 18 |
| GПРД | коэффициент усиления антенны | дБи | 24 |
| WАФТпрд | потери сигнала передатчика | дБ | 6 |

По формуле (3.1) эффективная изотропная излучаемая мощность составляет:

EIRP = 18 – 6 + 24 = 36 дБм

## 

## 3.2 Расчет зоны действия сигнала

Эта методика позволяет определить теоретическую дальность работы беспроводного канала связи, построенного на оборудовании D-LINK. Следует сразу отметить, что расстояние между антеннами, получаемое по формуле – максимально достижимое теоретически, а так как на беспроводную связи влияет множество факторов, получить такую дальность работы, особенно в черте города, увы, практически невозможно.

Для определения дальности связи необходимо рассчитать суммарное усиление тракта и по графику определить соответствующую этому значению дальность. Усиление тракта в дБ определяется по формуле:

(3.2)



где

– мощность передатчика;



– коэффициент усиления передающей антенны;



– коэффициент усиления приемной антенны;



– реальная чувствительность приемника;



По графику, приведённому на рисунке 3.1, находим необходимую дальность работы беспроводного канала связи.

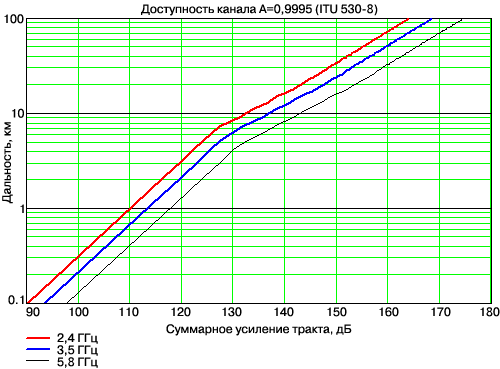


Рисунок 3.1 – График для определения дальности работы беспроводного канала связи

По графику (кривая для 2.4 GHz) определяем соответствующую этому значению дальность. Получаем дальность равную ~300 метрам.

Без вывода приведём формулу для расчёта дальности. Она берётся из инженерной формулы расчёта потерь в свободном пространстве:

(3.3)



где

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:

Суммарное усиление = Мощность передатчика (дБмВт) + | Чувствительность приёмника (–дБмВт)(по модулю) | + Коэф. Уисления антенны передатчика + Коэф усиления антенны приёмника – затухание в антенно-фидерном тракте передатчика – затухание в антенно-фидерном тракте приёмника – SOM

Для каждой скорости приёмник имеет определённую чувствительность. Для небольших скоростей (например, 1-2 мегабита) чувствительность наивысшая: от –90 дБмВт до –94 дБмВт. Для высоких скоростей, чувствительность намного меньше.

В зависимости от марки радио-модулей максимальная чувствительность может немного варьироваться. Ясно, что для разных скоростей максимальная дальность будет разной.

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 погодные аномалии: туман, снег, дождь;
* рассогласование антенны, приёмника, передатчика с антенно-фидерным трактом.

Параметр SOM берётся равным 15 дБ. Считается, что 15-ти децибельный запас по усилению достаточен для инженерного расчета.

В итоге получим формулу дальность связи:

.



D=0.25km = 250м

**4 ЗАЩИТА БЕСПРОВОДНЫХ СЕТЕЙ**

## 

## 4.1 Защита информации

По мере увеличения количества поставщиков и производителей, отдающих предпочтение беспроводным технологиям, последние все чаще преподносятся как средство, способное спасти современный компьютерный мир от опутывающих его проводов.

Разработчики беспроводного доступа не заметили подводных рифов в собственных водах, в результате чего первые робкие попытки беспроводных технологий завоевать мир провалились. Препятствием для широкого распространения беспроводных технологий, то есть тем самым «рифом», стал недостаточно высокий уровень безопасности.

## 

## 4.2 WEP и его последователи

Поскольку система беспроводной связи, построенная на базе статически распределяемых среди всех абонентов ключей шифрования WEP и аутентификации по MAC-адресам, не обеспечивает надлежащей защиты, многие производители сами начали улучшать методы защиты. Первой попыткой стало увеличение длины ключа шифрования — с 40 до 128 и даже до 256 бит. По такому пути пошли компании D-Link, U.S. Robotics и ряд других. Однако применение такого расширения, получившего название WEP2, приводило к несовместимости с уже имеющимся оборудованием других производителей. К тому же использование ключей большой длины только увеличивало объем работы, осуществляемой злоумышленниками, и не более того.

Понимая, что низкая безопасность будет препятствовать активному использованию беспроводных технологий, производители обратили внимание на спецификацию 802.1x, предназначенную для предоставления единого для всех сетевых технологий в рамках группы стандартов 802 сетевого механизма контроля доступа. Этот стандарт, называемый также динамическим WEP, применим и к беспроводным технологиям, что достигается благодаря использованию протокола EAP (Extensible Authentication Protocol). Данный протокол позволяет устранить угрозу создания ложных точек доступа, повысить криптографическую стойкость трафика к взлому и облегчить распределение аутентификационной информации по абонентам сети беспроводного доступа. Со временем протокол EAP видоизменялся, и сейчас существует несколько его разновидностей:

• Cisco Wireless EAP (LEAP);

• Protected EAP (PEAP);

• EAP-Transport Layer Security (EAP-TLS);

• EAP-Tunneled (EAP-TTLS);

• EAP-Subscriber Identity Module (EAP-SIM).

Надо заметить, что компания одной из первых реализовала проект этого стандарта в своем оборудовании Aironet. Клиент 802.1x уже встроен в операционную систему Windows XP; для других клиентов необходимо дополнительно устанавливать соответствующее программное обеспечение.

Новизна стандарта 802.1x вызывает при его применении ряд сложностей, первой по значимости из которых является возможная нестыковка между собой оборудования различных производителей, а второй — отсутствие клиентов 802.1x для некоторых типов устройств доступа. Но эти проблемы постепенно решаются, и в ближайшее время стандарт будет признан и станет повсеместно применяться для аутентификации беспроводного доступа. Остается, правда, человеческий фактор, который также мешает повышению защищенности любой технологии, и не только беспроводной. Например, по данным исследования TNS Intersearch, проводившегося по заказу Microsoft, из всех компаний, развернувших беспроводные точки доступа у себя в сети, только 42% задействовали механизмы аутентификации — никакие технические решения в такой ситуации не помогут.

Однако слабость базовых механизмов защиты не ограничивается одной лишь аутентификацией. Остаются открытыми вопросы дешифрования трафика, управления ключами, подмены сообщений и т.п., которые также активно решаются мировым сообществом. Например, последняя из названных проблем устраняется протоколом MIC (Message Integrity Check), позволяющим защитить передаваемые пакеты от изменения.

Слабая криптография WEP постепенно заменяется другими алгоритмами. Некоторые производители предлагают использовать DES или TripleDES в качестве альтернативы RC4. Интересное решение представила компания Fortress, которая разработала протокол канального уровня wLLS (wireless Link Layer Security), базирующийся:

• на алгоритме обмена ключами Диффи—Хеллмана;

• 128-разрядном шифровании IDEA (опционально могут использоваться также DES и 3DES);

• динамической смене ключей через каждые два часа;

• использовании двух пар ключей (для шифрования сетевого трафика и шифрования при обмене ключами).

Применение одного и того же ключа шифрования WEP приводило к накапливанию злоумышленником объема данных, достаточного для взлома используемой криптографии. Решением проблемы стала динамическая смена ключей, которую одной из первых реализовала компания Fortress в своем протоколе wLLS. Сменяемые через каждые два часа ключи усложняли работу криптоаналитика.

Второй подход, предложенный в протоколе TKIP (Temporal Key Integrity Protocol), заключается в смене ключей через каждые 10 Кбайт переданных данных. Этот протокол, заменив статический ключ шифрования динамически изменяющимися и распределяемыми по клиентам, позволил увеличить их длину — с 40 до 128 бит. При этом RC4 по-прежнему оставался алгоритмом шифрования.

Многие производители делают ставку на более сложный алгоритм AES (длина ключей шифрования 128, 192 или 256 бит), ставший национальным стандартом шифрования США. Однако его внедрение потребует реализации новых микросхем в оборудовании, что, в свою очередь, скажется на его цене и на стоимости перехода на новую версию.

Новые алгоритмы и протоколы значительно повышали защищенность беспроводных технологий и способствовали их более широкому распространению, однако они плохо интегрировались друг с другом, а оборудование, их использующее, стыковалось только после приложения серьезных усилий. Устранить все эти недостатки позволяет стандарт WPA (Wi-Fi Protected Access), анонсированный альянсом Wi-Fi (бывший WECA) 31 октября 2002 года. Данный стандарт призван унифицировать все технологии безопасности для беспроводных сетей 802.11. В настоящее время в этот стандарт входят:

• аутентификация пользователей при помощи 802.1x и EAP;

• шифрование при помощи TKIP;

• динамическое распределение ключей при помощи 802.1x;

• контроль целостности при помощи MIC (он же Michael).

В этом году стандарт WPA должен преобразоваться в более новую и расширенную спецификацию 802.11i (или WPA2). Именно в WAP2 алгоритм шифрования WEP будет заменен на AES.

## 

## 4.3 Программное обеспечение

Решения предлагаются различными производителями для защиты беспроводных сетей. Программное обеспечение позволяет достичь трех целей:

Найти чужих, то есть провести инвентаризацию беспроводной сети с целью обнаружить любые несанкционированные точки доступа и беспроводных клиентов, которые могут прослушивать трафик и вклиниваться во взаимодействие абонентов;

Проверить своих, то есть проконтролировать качество настройки и порекомендовать способы устранения дыр в санкционировано установленных беспроводных устройствах;

Защитить своих, то есть предотвратить несанкционированный доступ и атаки на узлы беспроводного сегмента сети (рисунок 4.1).

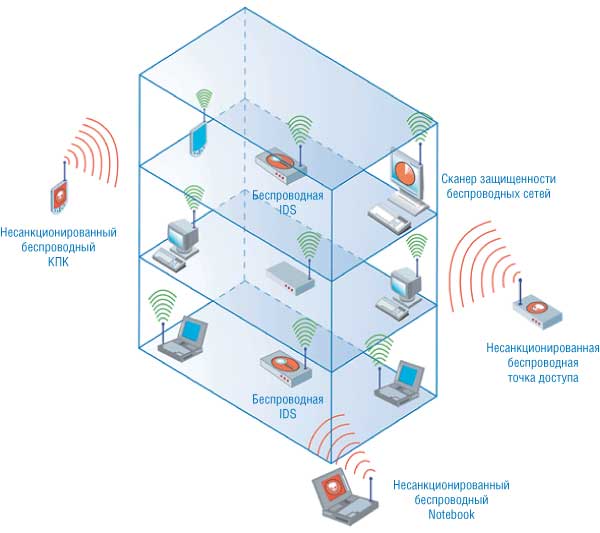


Рисунок 4.1 – Беспроводная сеть

## 

## 4.4 Инвентаризация беспроводной сети

Первую, и самую распространенную, задачу можно решить с помощью достаточно большого количества инструментов — NetStumbler, Wellenreiter, WifiScanner и др., а также с помощью сканеров безопасности беспроводных сетей и ряд систем обнаружения атак.

Пионером среди средств инвентаризации беспроводных устройств является NetStumbler, который запускается под Windows 9x/2000/XP и позволяет не только очень быстро находить все незащищенные беспроводные точки доступа, но и проникать в сети, якобы защищенные с помощью WEP. Аналогичные задачи решают WifiScanner, PrismStumbler и множество других свободно распространяемых продуктов. В этом плане интересна система Wellenreiter, которая также ищет беспроводных клиентов и точки доступа. Однако если подключить к ней GPS-приемник, система приобретает поистине безграничные возможности: вы сможете не только определить все несанкционированно установленные беспроводные устройства, но и узнать их местонахождение с точностью до метра. Еще одной отличительной особенностью этой системы является ее способность работать под управлением карманного компьютера.

В наглядном виде представляет результаты своей работы система Red-Vision от компании red-M, которая не только обнаруживает все точки доступа, но и визуально размещает их на схеме помещения вашей компании. В рекламных проспектах red-M пользователям обещают: «Мы откроем вам глаза на беспроводные технологии!»

## 4.5 Анализ защищенности беспроводных устройств

Поиск дыр в беспроводных устройствах осуществляют многие утилиты и инструменты, но, как правило, поиск дыр ограничивается попыткой взлома ключей шифрования WEP, и не более того. По такому принципу, например, действуют AirSnort и WEPCrack.

Более интересен специализированный инструментарий, обеспечивающий всесторонний аудит беспроводных устройств. Таких продуктов сегодня немного. Если быть точным, то только один — Wireless Scanner от компании Internet Security Systems, вид интерфейса системы Wireless Scanner представлен на рисунке 4.2



Рисунок 4.2 – Интерфейс системы Wireless Scanner

Эта система, базирующаяся на широко известном и самом первом в мире сетевом сканере безопасности Internet Scanner, проводит инвентаризацию сети и обнаруживает все санкционировано и несанкционированно установленные беспроводные точки доступа и клиенты. После этого проводится всесторонний анализ каждого устройства с целью определения любых слабых мест в системе защиты — недостатков в настройке или ошибок программирования. В базу сигнатур уязвимостей Wireless Scanner входит большое число записей о дырах в решениях ведущих игроков этого рынка — Cisco, Avaya, 3Com, Lucent, Cabletron и т.д. В гораздо меньшем объеме проверку проводит Wireless Security Auditor (WSA) — программный продукт от компании IBM. Пока это только прототип, и трудно сказать, каков будет окончательный результат усилий разработчиков. Как и вышеназванные системы, WSA проводит инвентаризацию сети и анализирует конфигурацию обнаруженных устройств в плане безопасности.

## 4.6 Обнаружение атак на беспроводные сети

После обнаружения чужих устройств и устранения дыр в своих перед пользователями встает задача обеспечения непрерывной защиты беспроводной сети и своевременного обнаружения атак на ее узлы. Эту задачу решают системы обнаружения вторжений, коих тоже существует достаточно, чтобы задуматься над выбором.. Применительно к беспроводным сетям очень трудно провести грань между сканером, инвентаризирующим сеть, и системой обнаружения атак, так как под обнаружением большинство производителей понимают идентификацию несанкционированных точек доступа. Отличие между ними заключается только в том, что сканеры выполняют эту задачу по команде или через заданные интервалы времени, а системы обнаружения контролируют сеть постоянно.

Система Airsnare от компании Digital Matrix. Она отслеживает MAC-адреса всех пакетов, передаваемых в беспроводном сегменте, и в случае обнаружения чужих адресов сигнализирует об этом, а также позволяет определить IP-адрес несанкционированно подключенного узла. В комплект поставки входит интересный модуль AirHorn, который позволяет послать злоумышленнику сообщение о том, что он вторгся в чужие владения и стоит поскорее их покинуть, если ему не нужны лишние проблемы.

Лидером рынка беспроводной безопасности можно назвать систему Airdefense одноименной компании, которая позволяет:

• автоматически обнаруживать все подключенные к сети беспроводные устройства;

• строить карту сети с указанием точек расположения беспроводных устройств;

• отслеживать изменения (отключено, украдено, выведено из строя и т.д.) в составе беспроводных устройств;

• контролировать сетевой трафик, передаваемый в беспроводном сегменте, и обнаруживать в нем различные аномалии;

• собирать информацию для проведения расследований, связанных с несанкционированной активностью;

• обнаруживать различные атаки и попытки сканирования;

• отслеживать отклонения в политике безопасности и настройках беспроводных устройств.

**5 БИЗНЕС ПЛАН**

## 5.1 Общая информация о проекте

Главной целью данного проекта является организация сети беспроводного доступа в Общежитии № 2 Алматинского Института Энергетики и Связи, с целью предоставления современных услуг связи: высокоскоростной доступ в Интернет, компьютерная сеть, на базе технологии Wi-Fi. Данный проект построен для компании ОАО «Казахтелеком», которая является оператором связи на телекоммуникационном рынке Казахстана.

Основой экономической эффективности технологии беспроводной передачи данных является низкая стоимость, быстрота развертывания, широкие функциональные возможности по передаче трафика данных, IP-телефонии, видео, – все это делает беспроводную технологию одним из самых быстрорастущих телекоммуникационных направлений.

Основными целями, которые ставит перед собой руководство компании, являются:

а) создать удобства и преимущества, связанные с локальной мобильностью;

б) получение прибыли.

## 5.2 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 D-Link. D-Link - в своём классе предлагает лучшие решения для беспроводных ЛВС:

1. Безопасность;

2. Расширяемость;

3. Управление;

4. Продвинутые возможности;

5. Высочайшая скорость;

6. Масштабируемость.

Решение D-Link создает отдельные полностью беспроводные сети, обеспечивая мобильность пользователей и увеличивая их продуктивность быстро и экономически эффективно. Решение основано на беспроводных продуктах стандартов IEEE 802.11n, предназначенных для организации связи в пределах здания. Эти продукты включают в себя точки радиодоступа, антенны и аксессуары, а также средства управления сетью.

Проект будет финансироваться из собственных средств компании. Установкой и обслуживанием будут заниматься местные специалисты, работающие в данной компании.

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

## 5.3 Финансовый план

5.3.1 Расчет капитальных вложений

Затраты по капитальным вложениям на реализацию проекта включают в себя затраты на приобретение основного оборудования, монтаж оборудования, транспортные расходы и проектирование, и рассчитывается по формуле:

(5.1)



где: КО – капитальные вложения на приобретение основного оборудования;

КМ. – расходы по монтажу оборудования;

КТР – транспортные расходы;

КПР – затраты на проектирование

Общий перечень необходимого основного оборудования и его стоимость приведены в таблице 5.1

Таблица 5.1 - Смета затрат на приобретение основного оборудования для реализации проекта.

|  |  |  |  |
| --- | --- | --- | --- |
| Наименование | Количество, шт. | Цена за ед., тенге | Сумма, тенге  (без НДС) |
| Беспроводная точка доступа DWL-8600AP | 6шт | 110 000 | 660 000 |
| ADSL D-Link 2500U | 2шт | 10 000 | 20 000 |
| Беспроводной коммутатор  DWS-4026 | 1шт | 200 000 | 150 000 |
| Fujitsu-Siemens PRIMERGY TX200 S3 | 2шт | 400 000 | 800 000 |
| Кабельная продукция  UTP 5e | 200 м | 35 | 7 000 |
| Прочие материалы |  |  | 100 000 |
| ИТОГО: |  |  | 1 737 000 |

Транспортные расходы, составляют 3% от стоимости всего оборудования и рассчитываются по формуле:

тенге



Монтаж оборудования, пуско-наладка производится инженерами-монтажниками, расходы составляют 1% от стоимости всего оборудования и рассчитываются по формуле:

тенге



Расходы по проектированию и разработке проекта составляют 0,5% от стоимости всего оборудования и рассчитываются по формуле:

тенге



Общая сумма капитальных вложений по реализации проекта составляет:

тенге



5.3.2 Эксплуатационные расходы

Текущие затраты на эксплуатацию данной системы связи определяются по формуле:

(5.2)



где ФОТ – фонд оплаты труда;

ОС – отчисления на соц. нужды;

ОАО – амортизационные отчисления;

Э – электроэнергия для производственных нужд;

Н – накладные затраты;

Фонд оплаты труда

В штате данного проекта состоят 2 инженера-техника. Месячная зарплата у инженера-техника составляет 70 000 тенге. Заработная плата сотрудников приведена в таблице 5.2

Таблица 5.2 – Заработная плата сотрудников

|  |  |  |  |
| --- | --- | --- | --- |
| Должность | Количество | Месячная заработная плата, тенге | Годовая заработная плата, тенге |
| Инженер-техник | 2 | 70 000 | 1 680 000 |

Затраты по оплате труда состоят из основной и дополнительной заработных плат и рассчитываются по формуле:

(5.3)



где:

Зосн - основная заработная плата,

Здоп - дополнительная заработная плата.

Основная заработная плата в год состовляет:

Зосн =1 680 000 тенге

Дополнительная заработная плата составляет 10% от основной заработной платы и рассчитывается по формуле:

(5.4)



тенге



Общий фонд оплаты труда за год составит:

ФОТ=1 680 000 + 168 000 =1 848 000 тенге

Расчет затрат по социальному налогу

В соответствии со статьей 385 Налогового кодекса РК социальный налог составляет 11% от начисленных доходов и рассчитывается по формуле:

(5.5)



где ПО – отчисления в пенсионный фонд.

ФОТ – фонд оплаты труда

0,11 – ставка на социальные нужды

Отчисления в пенсионный фонд составляют 10% от ФОТ, социальным налогом не облагаются и рассчитываются по формуле:

(5.6)



тенге



Тогда социальный налог будет равен

тенге



Расчет затрат на амортизацию

Амортизационные отчисления берутся исходя из того, что норма амортизации на оборудование связи составляет 25% и вычисляются по следующей формуле:

(5.7)



Где НА- норма амортизации;

∑К – стоимость оборудования;

Тогда амортизационные отчисления составляют:

тенге



Расчет затрат на электроэнергию

Затраты на электроэнергию для производственных нужд в течение года, включают в себя расходы электроэнергии на оборудование и дополнительные нужды и рассчитываются по формуле:

, (5.8)



Где: ЗЭЛ.ОБОР. – затраты на электроэнергию для оборудования;

ЗДОП.НУЖ. – затраты на дополнительные нужды;

Затраты электроэнергии на оборудование рассчитывается по формуле

, (5.9)



где: W – потребляемая мощность, W=16,8кВт;

Т – время работы;

S – тариф, равный 1 кВтч=12тг

24 – количество рабочих дней в месяце;

12 – количество месяцев в году.

тенге



Затраты на дополнительные нужды составляют 5% от затрат на электроэнергию оборудования и рассчитываются по формуле:

(5.10)



Где ЗЭЛ.ОБОР - затраты на электроэнергию для оборудования;

Затраты на электроэнергию для дополнительных нужд:

тенге



Тогда суммарные затраты на электроэнергию будут равны:

тенге



Расчет накладных затрат

Накладные расходы составляют 75 % от всех затрат и рассчитываются по формуле:

(5.11)



Где ФОТ – фонд оплаты труда;

Тогда накладные затраты составят:

тенге



Результаты расчета годовых эксплуатационных расходов проекта по построению сети Wi-Fi, представлены в таблице 5.3

Таблица 5.3 – Годовые эксплуатационные расходы

|  |  |
| --- | --- |
| **Показатель** | **Сумма тенге** |
| ФОТ | 1 848 000 |
| Отчисления на социальные нужды (Ос) | 182 952 |
| Амортизационные отчисления (А0 ) | 453 791,25 |
| Затраты на электроэнергию (Э) | 60 964 |
| Накладные расходы (Н) | 1 909 280 |
| **ИТОГО** | **4 454 987** |

5.3.3 Расчет доходов

Рассчитаем условный доход, полученный от внедрения сети.

Услуга Megaline Wi-Fi предоставляет возможность пользователям ноутбуков, карманных персональных компьютеров и смартфонов, имеющих порт Wi-Fi, получить беспроводный доступ в сеть Интернет. Оплата услуги Megaline Wi-Fi производиться посредством предоплаченной карты Tarlan + по тарифам (представлены в таблице 5.4) услуги “Зона Интернет”. Карты Tarlan продаются в размере 500, 1000, 2000 и 5000 тенге.

Таблица 5.4 – Тарифы услуги «Зона интернет Wi-Fi»

|  |  |
| --- | --- |
| Время | Размер платы за каждую полную или  неполную минуту, в тенге |
| рабочие дни: | |
| с 08.00 до 18.00; | 1,34 |
| с 18.00 до 23.00; | 1,68 |
| с 23.00 до 08.00. | 0,65 |
| выходные и праздничные дни: | |
| с 08.00 до 23.00; | 1,24 |
| с 23.00 до 08.00. | 0,59 |

По статистическим данным каждый пользователь Сети в среднем за месяц использует Tarlan карту на сумму 1000 тенге.

Доход от реализации услуг рассчитывается по формуле

, (5.12)



где – месячная абонентская плата клиентов;



N – количество клиентов, По статистическим данным в среднем в общежитии насчитывается 500 клиентов (всего проживает 700 человек);

n – число месяцев;

тенге



Оценки эффективности от реализации проекта производится на основе следующих показателей:

1. Чистый доход;
2. Чистый приведенный доход;
3. Срок окупаемости без дисконтирования;
4. Срок окупаемости с учетом дисконтирования.

Для расчета срока окупаемости необходимо определить чистый доход и доход предприятия после налогообложения.

Прибыль от реализации услуг определяется по формуле:

(5.13)



Где П - прибыль от реализации услуг, КПН – корпоративный подоходный налог с юридических лиц. Сумма налога в бюджет составляет 20% от чистого дохода предприятия. Чистый доход предприятия после налогообложения рассчитывается по формуле:

(5.14)



Прибыль от реализации услуг рассчитывается по формуле:

(5.15)



Где Д - реальный доход от внедрения услуг в год, ∑Э – эксплуатационные расходы

КПН в соответствии с формулой (4.14) составил



Прибыль от реализации услуг в соответствии с формулой (5.16) составила

тенге



Тогда чистая прибыль после налогообложения в соответствии с формулой (4.13) составит:



Таблица 5.5 - Показатели доходов без учёта дисконтирования

|  |  |  |
| --- | --- | --- |
| Наименование показателя | 1 год | 2 год |
| Доходы от реализации услуг, тенге | 6 000 000 | 6 000 000 |
| Эксплуатационные расходы, тенге | 4 454 987 | 4 454 987 |
| Прибыль, тенге | 1 545 013 | 1 545 013 |
| Чистая прибыль, тенге | 1 236 010 | 1 236 010 |
| Амортизационные отчисления А0 , тенге | 453 791 | 453 791 |
| Чистый денежный поток, тенге | 1 689 801 | 3 379 602 |
| Капитальные вложения, тенге | 1 815 165 | 0 |
| Чистые поступления, тенге | -125 364 | 3 254 238 |

По графику на рисунке 5.1 графически определяется срок окупаемости средств, вложенных в проект. Без дисконтирования срок окупаемости равен 13 месяцев. График построен по данным таблицы 5.5

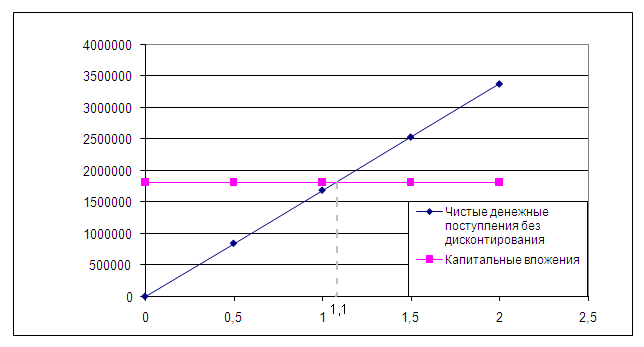


Рис 5.1 - График определения срока окупаемости проекта без учета дисконтирования

Для приведения разновременных затрат к единому моменту времени необходимо произвести оценку эффективности проекта на основе показателей чистого приведенного дохода и срока окупаемости с учетом дисконтирования.

Приведенный чистый доход рассчитывается по формуле:

(5.17)



Где ЧД– чистый доход от внедрения проекта.

Кпр – коэффициент дисконтирования, который рассчитывается по формуле:

(5.18)



Где t- год после внедрения проекта;

r – ставка дисконта составляет 0,20

Коэффициент дисконтирования для двух лет:



Тогда приведенный чистый доход для первых двух лет будет равен:

тенге



тенге



Результаты расчета показателей дохода с дисконтированием представленны в таблице 5.6

Таблица 5.6 - Показатели доходов с учётом дисконтирования от реализации проекта

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование показателя | | 1 | | 2 | |
| Доходы от реализации услуг, тенге | | 6 000 000 | | 6 000 000 | |
| Эксплуатационные расходы, тенге | | 4 454 987 | | 4 454 987 | |
| Прибыль, тенге | | 1 545 013 | | 1 545 013 | |
| Чистая прибыль, тенге | | 1 236 010 | | 1 236 010 | |
| Амортизационные отчисления А0 , тенге | | 453 791 | | 453 791 | |
| Чистый денежный поток, тенге | 1 689 801 | | 3 379 602 | |
| Коэффициент привидения | 0,83 | | 0,69 | |
| Приведенный чистый доход с учетом дисконтирования, тенге | 1 402 534 | | 2 331 925 | |
| Капитальные вложения, тенге | 1 815 165 | | 0 | |
| Чистые поступления, тенге | -412 631 | | 1 919 294 | |

По графику на рисунке 5.2 графически определяется срок окупаемости капиталовложений с учётом дисконтирования, который составил 1,3 года. График построен на основании данных таблицы 5.6

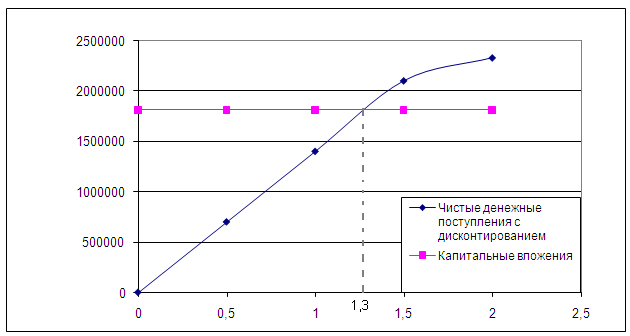


Рис 5.2 - График определения срока окупаемости проекта с учетом дисконтирования

Коэффициент экономической эффективности проекта рассчитывается по формуле:

Eр = (5.19)



И составил:



при нормативном значении Eн = 0,5, при нормативном значении срока окупаемости Тн = 5 лет

Таким образом, коэффициент экономической эффективности от реализации проекта составил 0.85 при нормативном значении 0.2, а срок окупаемости проекта составил 1,3 года при нормативном значении 5 лет, то есть выполняется неравенства Тр < Тн и Ер > Ен, что свидетельствует о целесообразности внедрения проекта.

**Выводы по разделу «Бизнес план»**

В данной части выпускной работы был представлен бизнес-план в котором рассматривается вопрос о внедрении сети беспроводного доступа в общежитие №2 Алматинского Института Энергетики и Связи.

В финансовой части бизнес плана был рассчитан объём капитальных вложений, который составил 1 815 165 тенге, эксплуатационные расходы, на реализацию проекта составили 4 454 987 тенге, из них большую часть составили накладные расходы, равные 1 909 280 тенге.

Расчетный срок окупаемости проекта составил 1,3 года при нормативном значении 5 лет, коэффициент экономической эффективности 0.85 при нормативном значении 0.2, то есть выполняется неравенства Тр < Тн и Ер>Ен, что свидетельствует целесообразности его внедрения.

**6 БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ**

## 6.1 Анализ условий труда обслуживающего персонала при эксплуатации технического оборудования

Главной целью данного проекта является организация сети беспроводного доступа в общежитии № 2 АИЭС (Алматинский Институт Энергетики и Связи), с целью предоставления современных услуг связи: высокоскоростной доступ в Интернет, компьютерная сеть, на базе технологии Wi-Fi.

Технический персонал состоит из двух сотрудников: главный технический специалист и диспетчер поддержки и мониторинга беспроводной сети. Диспетчера поддержки и мониторинга беспроводной сети меняются каждый день согласно расписанию.

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.

Согласно ГОСТ 12.1.005-88 ССБТ «Оптимальные и допустимые нормы микроклимата, в зависимости от категории работ», работа людей в помещение относится к работе лёгкой тяжести(1а), так как управление оборудованием осуществляется дистанционно с помощью компьютеров

С целью создания нормальных условий для работников предприятий Связи установлены нормы производственного микроклимата. В помещениях при работе с ЭВМ должны соблюдаться следующие климатические условия:

Холодный период года

● оптимальная температура 22-24 С˚, допустимая температура 18-26 С˚;

● относительная влажность 40-60 %, допустимая влажность 75%;

● скорость движение воздуха относительная и допустимая 0,1 м/с;

Тёплый период года

● оптимальная температура 23-25 С˚, допустимая температура 20-30 С˚;

● относительная влажность 40-60 %, допустимая влажность 55%;

● скорость движение воздуха относительная 0,1 м/с и допустимая 0,1-0,2 м/с.

Помещение имеет размеры: длина (L) = 6,5 метров, ширина (B) = 4,5 метра, высота (H) = 4 метра. Помещение находится в здании на 3-м этаже, рассчитано на 2 рабочих места.

План помещения выбранного для размещения оборудования и технического персонала изображен на рисунке 6.1.



Рисунок 6.1 – План рабочего помещения

Рабочее место состоит из следующих компонентов:

- два стола;

- два эргономических стула;

- два персональных компьютера, один из которых является сервером

1) Сервер Fujitsu-Siemens PRIMERGYT X200 S3(2x Intel Xeon 5050 (3.0 GHz)

2) Intel Core i7 965XE (3.0 GHz, 2 GB ОЗУ)

- беспроводной коммутатор DWS-4026

## 6.2 Расчет системы искусственного освещения помещения

Помещение зала имеет естественное освещение через одно боковое окно, и искусственное освещение, которое позволяет вести работы в темное время суток и днем в местах, где показатель КЕО не соответствует нормативам.

Поэтому рассчитаем общее освещение помещения аппаратного зала длиной А = 6,5 м., шириной В = 4,5 м., высотой Н = 4 м. С побеленным потолком, светлыми стенами и не завешенными окнами. Разряд зрительной работы – III высокой точности. Нормируемая освещенность – 300 лк. [1]. Для помещения используем люминесцентную лампу ЛБ (белого цвета), мощностью 40 Вт., световым потоком 3120 лм., диаметром 40 мм. и длиной со штырьками 1213,6 мм. [1].

Высота светильника h= 4-r, где r- высота лампочки



h= 4- 3,2 = 0,8 м



Высота рабочей поверхности = 1,2 м.



Определим необходимое расстояние между светильниками [1]:

м., (6.1)



где [1]



Высота светильника над освещаемой поверхностью:

м., (6.2)



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

м., (6.3)



Определим индекс помещения I [1]:

, (6.4)



Определим коэффициент использования η по таблице 2.5 [1] .



В качестве светильника возьмем ЛСП02 рассчитанный на две лампы мощностью 40 Вт, диаметром 40 мм и длиной со штырьками 1213,6 мм. Длина светильника 1234 мм, ширина 276 мм. Световой поток лампы ЛБ 40 Фл составляет 3120 лм., световой поток, излучаемый светильником Фсв равен:

лм. (6.5)



Определим число светильников:

, (6.6)



где S – площадь помещения, S=29,25 м.;



КЗ – коэффициент запаса, КЗ=1,5[1];

Е – заданная минимальная освещенность, Е=400 лк.; [1]

Z – коэффициент неравномерности освещения, Z=1,2; [1]

n – количество ламп в светильнике, n=2;

Фл – световой поток выбранной лампы, Фл=3120 лм.;

η – коэффициент использования, η=0,61[1].

светильников (Расположение светильников показано на рисунке 6.2 )

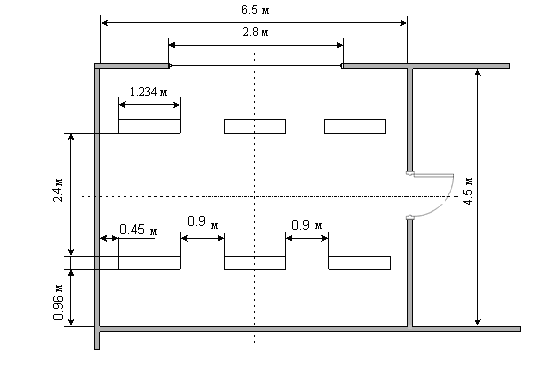


Рисунок 6.2 – Расположение светильников в помещении

Итого, для создания нормированной освещенности нам понадобится 12 ламп в 6-ти светильниках располагающихся в два ряда, в каждом ряду по три светильника, в каждом светильнике по две лампы.

## 

## 6.3 Анализ пожарной безопасности

Согласно СНиП 2.04.09-84 здание по степени опасности развития пожара, от функционального назначения и пожарной нагрузки горючих материалов, относится к 1-ой группе категории D.

Причинами возникновения пожара могут быть:

* Возгорание элементов аппаратуры;
* Возгорание отделочных материалов от неисправных выключателей, розеток.
* Несоблюдение режимов эксплуатации оборудования, неправильное действие персонала.

При возникновении пожара может пострадать не только помещение, но и дорогостоящая аппаратура, привести к человеческим жертвам. Поэтому необходимо чтобы были приняты меры по раннему выявлению и ликвидированию пожаров. Источниками зажигания могут оказаться электронные схемы ЭВМ, приборы, применяемые для технического обслуживания, устройства электропитания, кондиционеры воздуха, где в результате различных нарушений образуются перегретые элементы, и др.[4]

В соответствии с требованиями правил пожарной безопасности помещение оборудованы углекислотными огнетушителями ОУ-5 с учетом – один огнетушитель на 100 м2. Общая площадь помещения управления составляет 29,25 м2 таким образом устанавливаются 1 огнетушитель. В качестве огнетушащего вещества применяется комбинированный углекислотно-хладоновый состав. Расчетная масса комбинированного углекислотно-хладонового состава md ,кг, для объемного пожаротушения определяется по формуле:

(6.7)



где k = l,2- коэффициент компенсации не учитываемых потерь углекислотно-хладонового состава[4],

gn = 0,04 – нормативная массовая концентрация углекислотно-хладонового состава, [4]

V – объем помещения,

(6.8)



Где: А = 6,5 м – длина помещения,

В = 4,5 м – ширина помещения,

Н = 4 м – высота помещения.

Тогда:



Следовательно:



Расчетное число баллонов ξ определяется из расчета вместимости в 20-литровый баллон 12 кг углекислотно-хладонового состава.

Внутренний диаметр магистрального трубопровода di, мм, определяется по формуле:

[4] (6.9)



Эквивалентная длинна магистрального трубопровода l2. м, определяется по формуле:

(6.10)



где k1=1,2-коэффициент увеличения длины трубопровода для компенсации не учитывающих местных потерь, [4]

l=3м – длина трубопровода по проекту тогда, [4]

м.



Расход углекислотно-хладонового состава Q, кг/с, в зависимости от эквивалентной длины и диаметра трубопровода равна 1,4 кг/с

Расчетное время подачи углекислотно-хладонового состава t. мин, определяется по формуле:

(6.11)



Масса основного запаса углекислотно-хладонового состава m, кг, определяется по формуле:



(6.12)

где К2=0,2 – коэффициент учитывающий остаток углекислотно-хладонового состава в баллонах и трубопроводах



Таким образом из полученных результатов можно сделать вывод, что для обеспечения нормального функционирования системы автоматического пожаротушения потребуется 1 баллон углекислотно-хладонового состава вместимостью 20 литров, с массой смеси 7 кг. Автоматические установки газового пожаротушения имеют устройства для автоматического пуска в соответствии с ГОСТ 12,4.009-83

**Выводы по разделу «Безопасность жизнедеятельности»**

В данном разделе был произведён анализ условий труда в рабочем помещении. Уровень условий труда признан допустимым, и данные, полученные из расчетов полностью удовлетворяют требованиям стандартов безопасности жизнедеятельности.

Естественно, что одно окно не соответствуют нормативам естественного освещения рабочего помещения. Поэтому для создания нормированной освещенности рассчитал что понадобится 12 ламп мощностью 40 Вт., световым потоком 3120 лм., диаметром 40 мм. и длиной со штырьками 1213,6 мм. в 6-ти светильниках, располагающихся в два ряда, в каждом ряду по три светильника, в каждом светильнике по две лампы.

Электротехническое оборудование в помещения является потенциальным источником возникновения и пожароопасности.

Из расчетов получили, что для обеспечения нормального функционирования системы автоматического пожаротушения потребуется 1 баллон углекислотно-хладонового состава вместимостью 20 литров, с массой смеси 7 кг.

**ЗАКЛЮЧЕНИЕ**

В своем дипломном проекте я произвел обоснование проекта «Проектирование беспроводной сети Wi-Fi на основе стандарта 802.11n в общежитии № 2 Алматинского Института Энергетики и Связи». В работе был сделан анализ сети беспроводного доступа Wi-Fi.В качестве выбора оборудования для реализации проекта было отдано предпочтение в пользу фирмы D-Link. Обоснование выбора оборудования производилось с учетом: технических характеристик, возможностии применения, стоимостии и так далее. В технической части проекта рассмотрен вариант построения сети беспроводного доступа с установлением шести точек доступа. Выбор обусловлен условиями технических параметров оборудования. В расчетной части дипломного проекта произведены расчеты эффективной изотропной излучаемой мощности и зона покрытия сети.

В разделе безопасности и жизнедеятельности был проведены: анализ условий труда, расчет системы искусственного освещения и пожарной безопасности.

В экономической части дипломного проекта был произведен анализ рынка связи и представлен бизнес-план проектируемой системы с указанием срока окупаемости проекта.

**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 Сайт компании Aperto Networks.: http://www.Aperto Networks..com

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

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

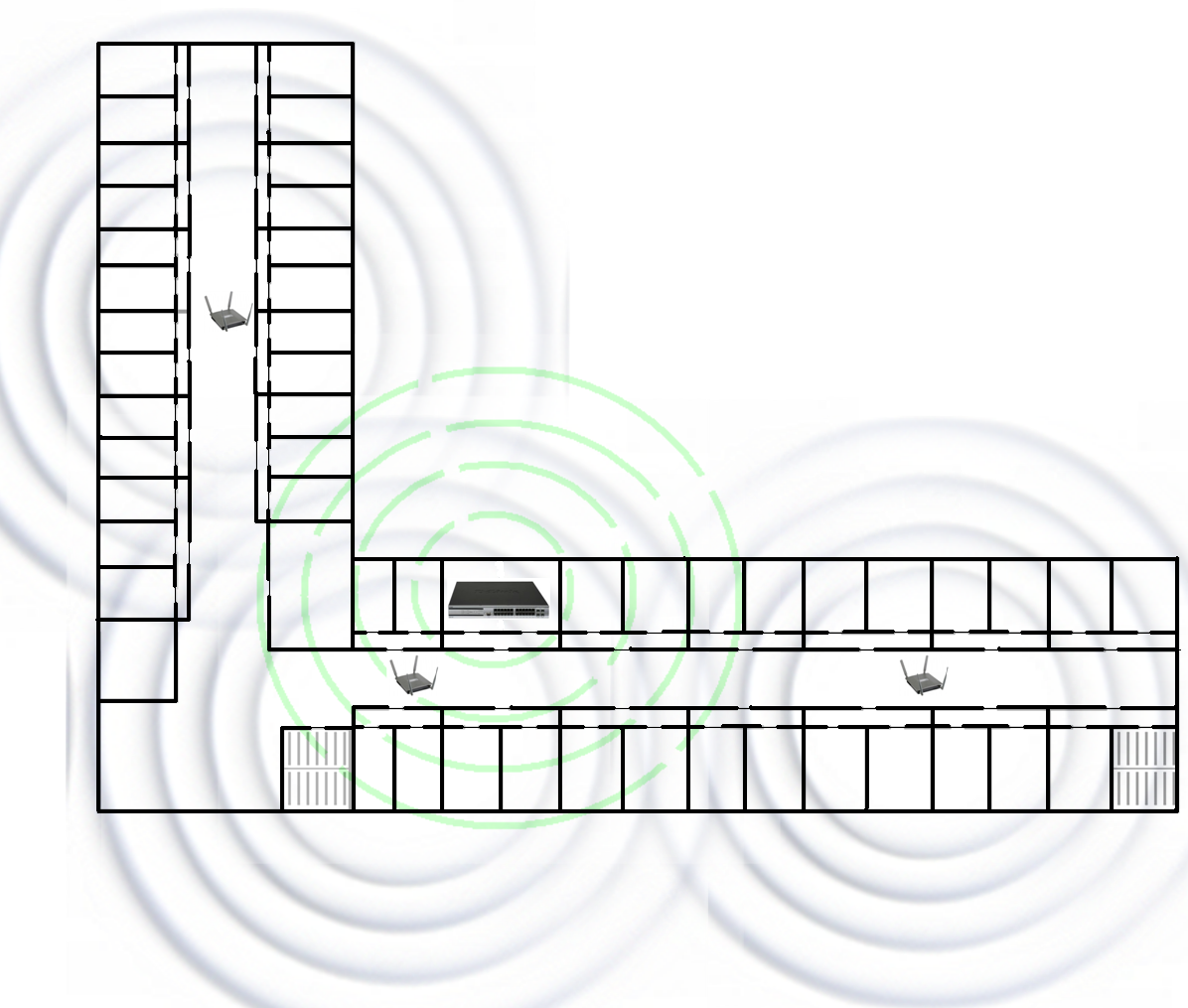
15 Баклашов Н.И., Китаева Н.Ж., Терехов Б.Д. Охрана труда на предприятиях связи и охрана окружающей среды: Учебник. – М.: Радио и связь, 1989.

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

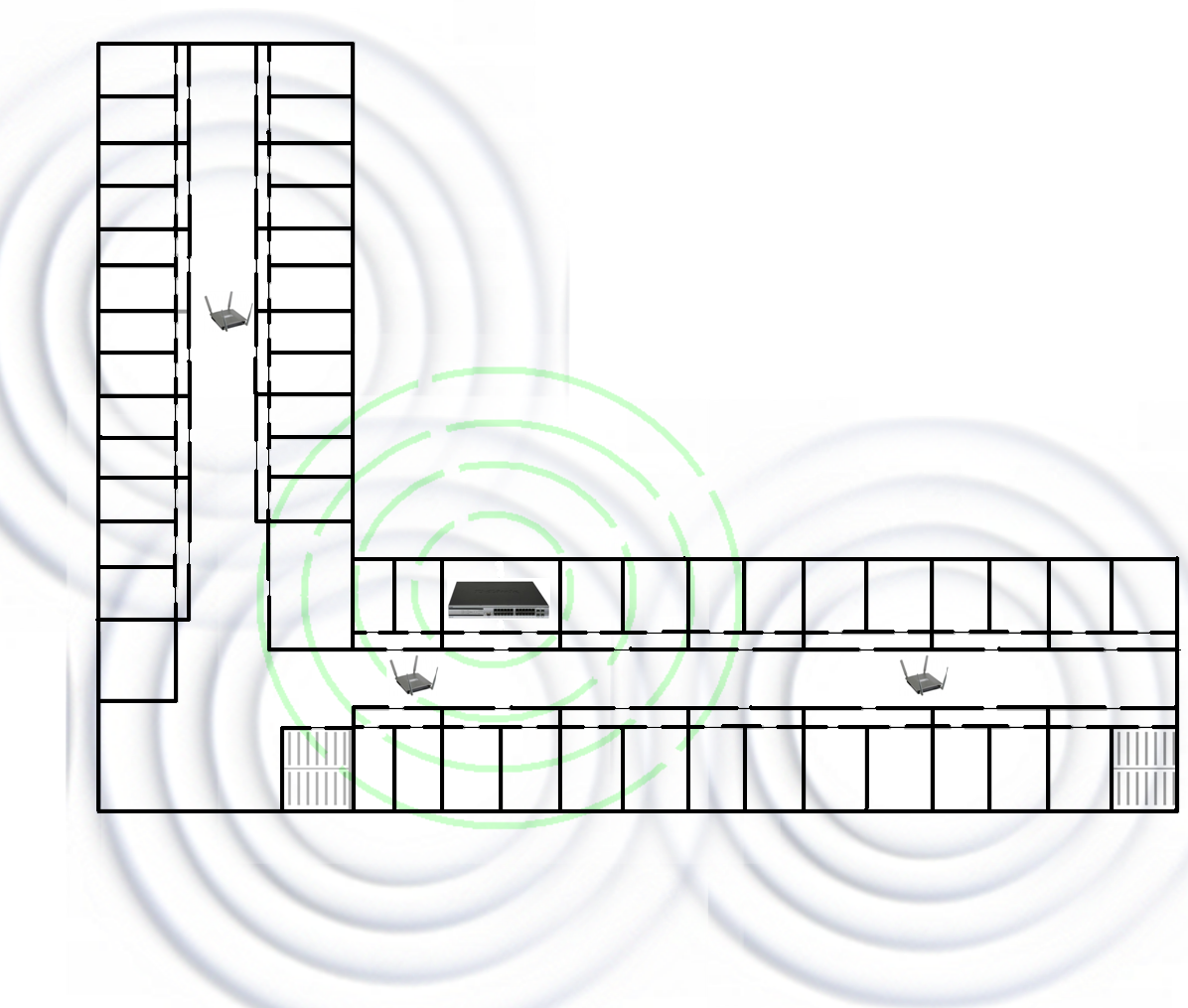
17 Долин П.А. Основы техники безопасности в электроустановках. – М.: Энергоатомиздат, 1984.

18 Сайт ОАО «Казахтелеком»: www.telecom.kz

19 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.



ПРИЛОЖЕНИЕ А – Размещение точек доступа на втором этаже и беспроводного коммутатора на третьем



ПРИЛОЖЕНИЕ Б – Размещение точек доступа на четвёртом этаже и беспроводного коммутатора на третьем

ПРИЛОЖЕНИЕ E - Код программы «Расчёт эффективной изотропной излучаемой мощности»

unit Unit1;

interface

uses

Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls, Forms,

Dialogs, StdCtrls, ExtCtrls, XPMan;

type

TForm1 = class(TForm)

Edit1: TEdit;

Edit2: TEdit;

Edit3: TEdit;

Button1: TButton;

Label1: TLabel;

Label2: TLabel;

Label3: TLabel;

Edit4: TEdit;

Button2: TButton;

Label4: TLabel;

Label5: TLabel;

Label6: TLabel;

XPManifest1: TXPManifest;

Image1: TImage;

procedure Button2Click(Sender: TObject);

procedure Button1Click(Sender: TObject);

private

{ Private declarations }

public

{ Public declarations }

end;

var

Form1: TForm1;

implementation

{$R \*.dfm}

procedure TForm1.Button2Click(Sender: TObject);

begin

close;

end;

procedure TForm1.Button1Click(Sender: TObject);

begin

Edit4.Text:=FloatToStr(StrToFloat(trim(Edit1.Text)) StrToFloat(trim(Edit2.Text)) +

StrToFloat(trim(Edit3.Text))) + 'дБм';

end;end.

Республика Казахстан

Некоммерческое акционерное общество

«Алматинский институт энергетики и связи»

**Отзыв руководителя**

О работе студента: Антонова Дмитрия Александровича

Группа: БВТ-06-5

Специальность: 050704 «Вычислительная техника и программное обеспечение»

Тема дипломного проекта: «Проектирование беспроводной сети Wi-Fi на основе стандарта 802.11n в общежитии № 2 Алматинского Института Энергетики и Связи».

В дипломном проекте поставлены и решены следующие задачи: обзор существующей технологии беспроводного доступа Wi-Fi, выбор оборудования для реализации проекта на основе стандарта 802.11n, расчет зоны покрытия сети, экономическая эффективность и охрана труда.

Актуальность темы вызвана тем, что услуги по предоставлению беспроводного доступа Wi-Fi представляют весьма высокодоходный сегмент рынка телекоммуникационных услуг.

Теоретическая и практическая ценность проекта: расчет параметров теоретически правилен и имеет практическую ценность.

Достоинства и недостатки дипломного проекта: работа выполнена в соответствии с заданием и отвечает требованиям, предъявляемым к дипломному проекту.

Оценка дипломного проекта: дипломный проект заслуживает оценки “отлично”, а ее автор присвоения академической степени бакалавра по специальности 050704 «Вычислительная техника и программное обеспечение».

**Руководитель** д.т.н., профессор Ташимов М.А.

# Рецензия

# НА ДИПЛОМНЫЙ ПРОЕКТ

Студенту: Антонову Дмитрию Александровичу

Специальности: 050704 «Вычислительная техника и программное обеспечение»

Тема дипломного проекта: «Проектирование беспроводной сети Wi-Fi на основе стандарта 802.11n в общежитии № 2 Алматинского Института Энергетики и Связи».

Дипломный проект посвящен проектированию сети Wi-Fi в общежитии № 2 Алматинского Института Энергетики и Связи.

В первой главе, описываются обзор технологии, определение, стандарты, принципы работы.

Во второй главе, описывается реализация проекта на территории общежития, приведена схема построения сети.

В третьей главе, приведены расчеты максимальной дальности сигнала, эффективной изотропной излучаемой мощности.

В дипломном проекте представлен бизнес-план по реализации проекта, а также описание безопасности жизнедеятельности.

Хотелось также отметить актуальность разрабатываемого проекта тем, что услуги по предоставлению беспроводного доступа Wi-Fi представляют весьма высокодоходный сегмент рынка телекоммуникационных услуг. Разработка целесообразна и соответствует требованиям научно-исследовательских комплексов. Работа выполнена на высоком техническом уровне, очень аккуратно.

Дипломный проект включает: более 70 страниц текста, большое количество рисунков, имеющих информативное значение и подтверждающих результаты проведенного исследования, введение, аннотацию и заключение.

Дипломный проект заслуживает оценки “отлично”, а ее автор присвоения академической степени бакалавра по специальности 050704 «Вычислительная техника и программное обеспечение»

**Рецензент** к.т.н., зам. ген. Директора ТОО

«Системотехника» Т.Р Амирбаев

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

«\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_ 2010 г.