**ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ (АССОЦИАЦИЯ)**

**«КИСЛОВОДСКИЙ ГУМАНИТАРНО-ТЕХНИЧЕСКИЙ ИНСТИТУТ»**

Факультет Инженерный

Кафедра Систем автоматического управления

Направление Управление в технических системах

К защите допустить:

Зав. кафедрой, д.т.н., профессор Гайдук А.Р.

«\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2017 г.

**ПОЯСНИТЕЛЬНАЯ ЗАПИСКА**к выпускной квалификационной работе

На тему:

# «Модернизация локальной вычислительной сети санатория имени Г.К. Орджоникидзе корпуса 2 »

Руководитель работы: д.т.н., доцент\_\_\_\_\_\_\_\_\_Шеболков В.В.

(должность, ученая степень и звание)

Консультанты:

по экономическому разделу \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_к.э.н. Курданов М.Д.

по безопасности и экологичности системы \_\_\_\_\_\_\_\_\_\_\_\_\_Сербулова Т.Н.

Студент: Каракулин Роберт Олегович гр.241

(фамилия, имя, отчество, группа)

Кисловодск 2017

**ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ ВЫСШЕГООБРАЗОВАНИЯ (АССОЦИАЦИЯ)**

**«КИСЛОВОДСКИЙ ГУМАНИТАРНО-ТЕХНИЧЕСКИЙ ИНСТИТУТ»**

Факультет Инженерный

Кафедра Систем автоматического управления

Направление Управление в технических системах

**ЗАДАНИЕ**

# на выпускную квалификационную работу

|  |
| --- |
| Каракулину Роберту Олеговичу |
| 1.Тема выпускной квалификационной работы:  «Модернизация локальной вычислительной сети санатория имени  Г.К. Орджоникидзе корпуса 2» | |

утверждена приказом по вузу № 9 от 15.01.2017 г.

|  |  |  |
| --- | --- | --- |
| 2. Срок сдачи студентом законченной работы | | 25.06.2017 г. |
| 3. Исходные данные к работе |  | |

3.1. Спроектировать локальную информационную сеть для корпуса 2 санатория Г .К. Орджоникидзе ,

|  |
| --- |
| 3.2. Сеть должна обеспечивать возможность доступа к сети интернет отдыхающих санатория по беспроводным технологиям . |
| 3.3. Выбрать вид беспроводной технологии и разместить точки доступа в здании корпуса 2 санатория . 3.4. Выполнить экспериментальную проверку уровней сигнала в помещениях санатория. |

4. Содержание пояснительной записки

|  |
| --- |
| 1.Введение. |
| 2. Реализация сети беспроводного доступа |
| 3. Расчет уровней сигнала в помещениях корпуса 2 |
| 4. Защита беспроводных сетей |
| 5.Экспериментальные исследования сети |
| 6. Экономическое обоснование разработки |
| 7. Безопасность и экологичность работы.  8 заключение |

5. Перечень графического материала (с точным указанием графического материала – слайдов)

|  |
| --- |
| 1. Анализ технического задания ……………………………….(1 слайд). |
| 2. Структурная схема спроектированной сети …………..……(1 слайд). |
| 3. Характеристика выбранного оборудования…………...…….(1 слайд). |
| 4. Размещение точек доступа в здании санатория……………...(1 слайд). |
| 5. Экспериментальная проверка уровней сигнала………….…..(1 слайд). |
| 6. Технико-экономическое обоснование разработки..…………(1 слайд). |
| 7. Безопасность и экологичность разработки…………………(1 слайд). |
| 6. Консультации по проекту (с указанием относящихся к ним разделов проекта)  Технико-экономическое обоснование к.э.н. /Курданов М.Д./  (подпись)  Безопасность и экологичность /Сербулова Т.Н./  (подпись) |

7. Дата выдачи задания 15 декабря 2016 г.

Руководитель \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ к.т.н., доцент/Шеболков В.В./

(подпись)

Задание принято к исполнению 15 декабря 2016 г.

Студент \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Каракулин Р.О.\_

(подпись)

УДК 65.011.56

Модернизация локальной вычислительной сети

санаторий имени Г.К. Орджоникидзе корпуса №2

Выпускная квалификационная работа

Каракулин Роберт Олегович

Кисловодск, КГТИ, 2017 г.

**РЕФЕРАТ**

Выпускная квалификационная работа (ВКР) содержит 87 страниц, 12 таблиц, 29 рисунка, список источников из 13 наименований.

Ключевые слова: автоматизированная система, беспроводная технология, WiFi оборудование, беспроводная сеть, локальная сеть, безопасность, экономическая эффективность.

В ВКР выполнено проектирование и модернизация локально вычислительной сети.

Рассмотрены вопросы безопасности, а также выполнено технико-экономическое обоснование системы.

**Оглавление**

[1 Анализ технического задания 9](#_Toc486327753)

[1.1 Особенности технологий беспроводного доступа 9](#_Toc486327754)

[1.2 История развития 10](#_Toc486327755)

[1.3 Основные стандарты 11](#_Toc486327756)

[1.4 Факторы более высокой скорости передачи данных стандарта 802.11n. ..26](#_Toc486327757)

[1.5 Топологии беспроводных сетей Wi-Fi. 28](#_Toc486327758)

[1.6 Беспроводное оборудование, применяемое в Wi-Fi сетях 30](#_Toc486327759)

[2 РЕАЛИЗАЦИЯ СЕТИ БЕСПРВОДНОГО ДОСТУПА 33](#_Toc486327760)

[2.1 Место реализации работы 33](#_Toc486327761)

[2.2 Техническое решение работы 33](#_Toc486327762)

[2.3 Описание и характеристика выбранного оборудования 34](#_Toc486327763)

[2.4 Разработка структурной схемы сети 37](#_Toc486327764)

[3 Расчет уровней сигнала в помещениях корпуса 2 40](#_Toc486327765)

[3.1 Расчет эффективной изотропной излучаемой мощности 40](#_Toc486327766)

[3.2 Расчет зоны действия сигнала. 40](#_Toc486327767)

[4 ЗАЩИТА БЕСПРОВОДНЫХ СЕТЕЙ 43](#_Toc486327768)

[4.1 Защита информации 43](#_Toc486327769)

[4.2 WEP и его последователи 43](#_Toc486327770)

[4.3 Программное обеспечение 46](#_Toc486327771)

[4.4 Инвентаризация беспроводной сети 46](#_Toc486327772)

[4.5 Анализ защищенности беспроводных устройств 47](#_Toc486327773)

[4.6 Обнаружение атак на беспроводные сети 48](#_Toc486327774)

[5 ЭКСПЕРЕМЕНТАЛЬНЫЕ ИССЛЕДОВАНИЯ СЕТИ. 50](#_Toc486327775)

[5.1 Измерение уровня сигнала. 50](#_Toc486327776)

[5.2 Установка и настройка беспроводной точки доступа D-Link DWL - 2100AP 53](#_Toc486327777)

[6 Экономическое обоснование разработки 56](#_Toc486327778)

[6.1 Общая информация о сети 56](#_Toc486327779)

[6.2 Обоснование выбора и состава оборудования 56](#_Toc486327780)

[6.3 Финансовый план 57](#_Toc486327781)

[7 Безопасность и экологичность работы. 65](#_Toc486327782)

[7.1 Параметры микроклимата в серверном кабинете . 65](#_Toc486327783)

[7.2 Электромагнитные поля и источники ионизирующих излучений помещения серверного кабинета. 66](#_Toc486327784)

[7.3 Пожароопасность и взрывоопасность. 67](#_Toc486327785)

[7.4 Описание рабочего места сетевого администратора. 67](#_Toc486327786)

[7.5 Охрана окружающей среды при использовании ЭВМ 69](#_Toc486327787)

[ЗАКЛЮЧЕНИЕ 72](#_Toc486327788)

[СПИСОК ЛИТЕРАТУРЫ 73](#_Toc486327789)

[ПРИЛОЖЕНИЕ А План здания с точками доступа 74](#_Toc486327790)

[ПРИЛОЖЕНИЕ Б- Код программы «Расчёт эффективной изотропной излучаемой мощности» 75](#_Toc486327791)

**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. wirelessfidelity - 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 во 2 корпусе Санатории имени им. Г. К. Орджоникидзе***с*** целью повышения уровня информатизации, предоставления современных услуг связи: высокоскоростной доступ в Интернет, компьютерная сеть, на базе технологии Wi-Fi.

# 1 Анализ технического задания

## **1.1 Особенности технологий беспроводного доступа**

В соответствии с техническим заданием мне необходимо было разработать беспроводную сеть для информационного обслуживания корпуса номер 2.

Разрабатываемая сеть предназначена для обеспечения беспроводного доступа к информационным ресурсам существующей локальной информационной сети и сети Internet.

Санаторийразмещен в четырехэтажном кирпичном здании Г-образной формы в плане, межэтажные перекрытия - бетонные плиты, План здания приведен в приложении.

Решение задачи проектирования начнем с рассмотрения технологий беспроводного доступа.

Различаюттритипабеспроводныхсетей (рис. 1.1): WWAN (Wireless Wide Area Network), WLAN (Wireless Local Area Network) и WPAN (Wireless Personal Area Network)

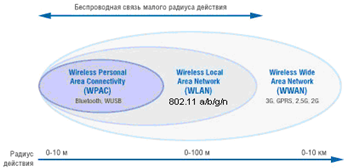


Рисунок 1.1 - Радиус действия персональных, локальных и глобальных беспроводных сетей

При построении сетей WLAN и WPAN, а также систем широкополосного беспроводного доступа (BWA - BroadbandWirelessAccess) 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 (BroadbandWirelessAccess) используют как лицензионные, так и нелицензионные диапазоны (от 2 до 66 ГГц).

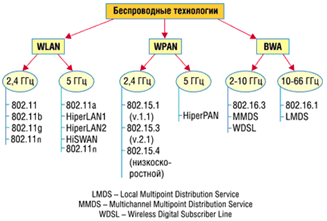


Рисунок 1.2 - Классификация беспроводных технологий

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 (hotspots) 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 (WirelessFidelity), 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 (InstituteofElectricalandElectronicEngineers). 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, (метр) | 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 TexasInstruments. 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 (PacketBinaryConvolutionalCoding, 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 (InterSymbolInterference, 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 (OrthogonalFrequencyDivisionMultiplexing, 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 (GuardInterval, 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 (QuadratureAmplitudeModulation), 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.

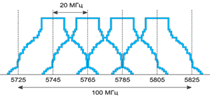
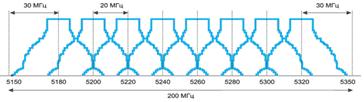


Рисунок 1.3 - Разделение диапазона UNII на 12 частотных поддиапазонов

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 (DataTones), а остальные — для передачи служебной информации (PilotТones).

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 подканале | 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 (MultipleInputMultipleOutput) предполагает применение нескольких передающих и принимающих антенн. По аналогии традиционные системы, то есть системы с одной передающей и одной принимающей антенной, называются SISO (SingleInputSingleOutput).

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.

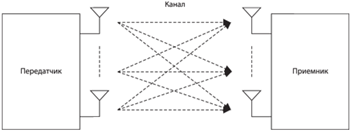


Рисунок 1.4 - Принцип реализации технологии MIMO

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 (legacymode).

- Смешанный режим (mixedmode).

- Режимзеленогополя (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:

- 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.

- 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.

-. 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.

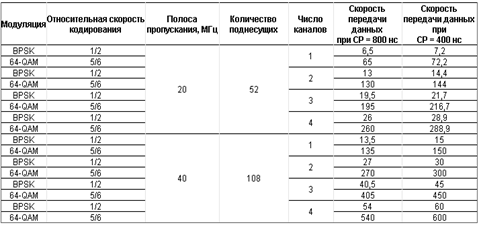
- Режим верхнего канала. В этом режиме используется только верхняя половина диапазона 40 МГц. Станции могут обмениваться любыми пакетами.

- 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 1.6. 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.

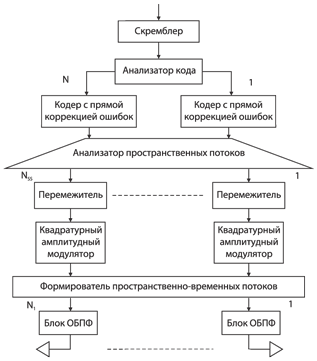


Рисунок 1.5 - Общая структура передатчика MIMO-OFDM

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.

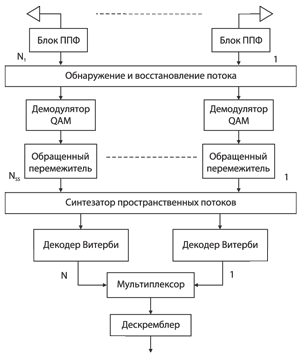


Рисунок 1.6 - Общая структура приемника MIMO-OFD

## **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.

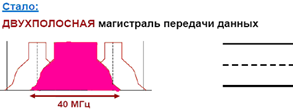
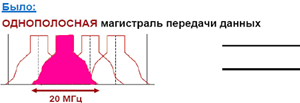


Рисунок 1.8 - Второй фактор увеличения скорости передачи данных

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 (IndependentBasicServiceSets, IBSSs);  
- Базовые зоны обслуживания (BasicServiceSets, BSSs);  
-Расширенные зоны обслуживания (ExtendedServiceSets, 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 (networkinterfacecard, NIC) стандарта 802.11, могут формировать IBSS и напрямую связываться одна с другой.

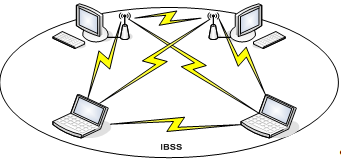


Рисунок 1.10 - Ad-Hoc сеть (IBSS)

Специальная сеть, или независимая базовая зона обслуживания (IBSS), возникает, когда отдельные устройства-клиенты формируют самоподдерживающуюся сеть без использования отдельной точки доступа (AP – AccessPoint). 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 (beaconinterval) для создания набора моментов времени передачи маячкового сигнала (setoftargetbeacontransmissiontime, TBTT). Когда завершается ТВТТ, каждый клиент IBSS выполняет следующее:Приостанавливает все несработавшие таймеры задержки (backofftimer) из предыдущего ТВТТ;Определяет новуюслучайную 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 (AccessPoint). 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 (uplinkport), 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.

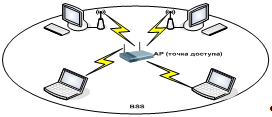


Рисунок 1.11 - Инфраструктура локальной беспроводной сети BSS

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 (DistributionSystem, 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.

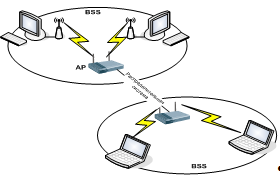


Рисунок 1.12 - Расширенная зона обслуживания ESS беспроводной сети

**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 - RJ46. 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 (indoor) и всепогодного (outdoor) 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 FastEthernet. 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:

-необходима совместимость со стандартами;

-работа в диапазоне частот 2,4 ГГц - 2,435 ГГц (или 5 ГГц);

-поддерживать протоколы WEP и желательно WPA;

-поддерживать два типа соединения "точка-точка", и "компьютер сервер";

-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 IntelCentrino. 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 работы**

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 технологииWi-Fi, обусловлена растущей потребностью пользователей современной техники и 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 работы:

- Развертывание сети беспроводного доступа Wi-Fi во 2 корпусе Санатории имени им. Г. К. Орджоникидзе

- Удовлетворение существующего и прогнозируемого спроса на услуги телекоммуникаций.

- Повышение уровня информатизации отдыхающих .

Область применения технологий беспроводного доступа Wi-Fi:

- Экономическая нецелесообразность подключения по проводной линии;

- Обеспечение высокой скорости передачи данных.

**2.2 Техническое решение работы**

ВКР по «Установке беспроводного доступа Wi-Fi в Санатории имени им. Г. К. Орджоникидзе, базируется на оборудовании c поддержкой стандарта 802.11n, получившим сертификат Wi-Fi. Wi-Fi покрывает всю территорию корпуса и обьединяет всех пользователей в единую сеть с доступом в интернет. Сеть осуществляется установленными по всей территории корпуса беспроводными унифицированными точками доступа, управляемыми беспроводным коммутатором.

## **2.3 Описание и характеристика выбранного оборудования**

В качестве оборудования беспроводного сегмента сети выбрано оборудование фирмы UbiquitiUniFi AP (UAP) — одного из ведущихпроизводителей телекоммуникационного оборудования. Это точка доступа с пропускной способностью канала до 150 Мб/с, мощным процессором привлекательными характеристиками по критерию эффективность-стоимость .  Система на базе UbiquitiUniFi AP поддерживает внутрисетевой роуминг — бесшовный переход клиентского устройства от одной «базовой станции» к другой. Это означает, во-первых полную свободу перемещений абонентов в пределах общей зоны покрытия всех устройств UbiquitiUniFi AP, а во-вторых — практически не ограниченную возможность масштабирования системы. Программный комплекс позволяет гибко настраивать сетевую модель системы, построенной из нескольких десятков и даже сотен точек UbiquitiUniFi AP. Для наглядного планирования зоны покрытия достаточно загрузить в программу план помещений и начать расставлять устройства и наблюдать уровень мощности сигнала в каждой конкретной точки. Такой подход позволяет оперативно выявлять проблемы и точно проектировать сеть, приобретая столько устройство, сколько действительно требуется для эффективной ее работы.

Интерфейс программы, позволяет без проблем получать статистику по каждой из UbiquitiUniFi AP используемой в системе, а также быстро изменять топологию сети

.

Рис.2.1 Беспроводная система UbiquitiUniFi AP 3-pack

Для работы UbiquitiUniFi AP требуется маршрутизатор. Если учесть, что питание точки доступа осуществляется по технологии PoE, то наилучшим решением для UniFi сети любого масштаба будет Ubiquiti TOUGH Switch -устройство объединяющее в себе функции производительного коммутатора и PoE-инжектора с возможностью контроля напряжения.

Система сама определят «узкие места» - источники чрезмерной нагрузки на сеть и показывает их администратору. Для авторизации пользователей возможно подключить отдельный Radius-сервер, а прошивки на всех UniFi AP, входящих в одну сеть могут обновляться одновременно.

UbiquitiUniFi AP LR обеспечивает пропускную способность канала —   
до 300 Мб/с. Отличной поддержкой такой сети станет  UbiquitiTOUGHSwitchPoE. Универсальный коммутатор с 5 или 8 гигабитными портами поддерживающими технологию PoweroverEthernet. Вам не придется тратить дополнительные средства на PoE-инжекторы.

Все необходимое для передачи данный и снабжение питание сетевых устройств через интернет-кабель уже имеется в [UbiquitiTOUGHSwitchPoE](http://www.ubnt.su/review/toughswitch.htm)**.**

Для того чтобы интегрировать UbiquitiUniFi AP LR в уже имеющуюся сеть достаточно просто подключить его к маршрутизатору. Система автоматически детектирует нового клиента и начнет процесс конфигурирования устройства.

Таблица 2.1 – Технические характеристки Ubiquiti UniFi LR (UAP LR)

|  |  |
| --- | --- |
| Размеры | 20 x 20 x 3.65 см |
| Вес | 430 гр |
| Сетевой интерфейс | 1 х 10/100 Ethernet |
| Кнопки | Reset |
| Антенна | встроенная 2х2 MIMO |
| Стандарт Wi-Fi | 802.11 b/g/n (2.4 ГГц) |
| Питание | Passive Power over Ethernet 12-24 В, 24V 0.5A |
| Максимальна потребляемая мощность |  |
| Максимальная мощность передатчика | 27 дБм |
| BSSID | до 4х независимых сетей на канал |
| Энергосбережение | поддерживается |
| Безопасность | WEP, WPA-PSK, WPA-TKIP, WPA2 AES, |
| Сертификаты | CE, FCC, IC |
| Монтаж | На стену/потолок (крепления в комплекте) |
| Рабочая температура | от -10 до +70 С |
| Влажность | от 5 до 95% (с конденсацией) |
| Расширенное управление трафиком |  |
| VLAN | 802.1Q |
| Расширенный QoS | ограничение ширины канала пользователя |
| Изоляция гостевого трафика | поддерживается |
| WMM | Voice, Video, Best Effort, and Background |
| Число одновременных клиентов | более 100 |
| Поддерживаемые скорости передачи данных |  |
| 802.11n | 6.5 Mbps .. 300 Mbps (MCS0 - MCS15, HT 20/40) |
| 802.11b | 1, 2, 5.5, 11 Mbps |
| 802.11g | 6, 9, 12, 18, 24, 36, 48, 54 Mbps |

Коммутатор UbiquitiTOUGHSwitchPoEPro — надежный и высокопроизводительный свич, не только коммутирует несколько устройств, но и параллельно снабжает их питанием по витой паре. Коммутатор Ubiquiti TOUGHSwitch отлично подойдет для создания различных систем видеонаблюдения, например - масштабируемых, а так же систем Wi-Fi доступа на основе оборудования серии [UniFi](http://www.ubnt.su/info/catalog-unifi.htm). Управление и настройка производятся через специальное ПО через [AirOS](http://www.ubnt.su/review/airos-7.htm).

Ubiquiti TOUGHSwitch PoE Pro предоставляет возможность выбора напряжения подаваемого на каждый из 8 гигабитных портов, что позволяет подключать к нему устройства с питанием как 24 так и 48В*.* Для поддержки энергоемких клиентов Ubiquiti TOUGHSwitch PoE Pro оснащен 150-ваттным блоком питания.

Идеальное решение для UniFi-сетей масштаба офиса или подключения высоко- производительной антенной матрицы на базе нескольких Rocket M.



Рисунок 2.2 - Коммутатор Ubiquiti TOUGHSwitch PoE Pro

Таблица 2.2 Технические характеристики UbiquitiTOUGHSwitchPoEPro

|  |  |
| --- | --- |
| Потребляемая мощность | 110-120VAC / 210-230VAC |
| Максимум потребляемой мощности | 150 W |
| PoE Out Диапазон напряжения | 45-48VDC / 22-24VDC |
| Max. PoE Wattage Per Data Port | 11.5 W (24 V), 23 W (48V) |
| ESD Рейтинг | 24 kV Air / 24 kV Contact |
| PoE Метод | Passive |
| Кнопка | Reset |
| USB-порт | 2.0 |
| Процессор | MIPS 24K, 400 MHz |
| Системная память | 64 MB |
| Code Storage | 8 MB |
| Рабочая температура | -25 to 55° C |
| Рабочая влажность | 90% без конденсации |
| Management Port | (1) 10/100 Ethernet Port |
| Data Ports | (8) 10/100/1000 Ethernet Ports |
| Рабочая температура | -25 to 55° C |
| Рабочая влажность | 90% без конденсации |
| Вес | 1.24 kg |
| Размеры | 210 x 185 x 41 mm |

## **2.4 Разработка структурной схемы сети**

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

Сеть будет управлятьсясервером с помощью беспроводных коммутаторов. Так как беспроводные коммутаторы и точки доступа распространяют сигнал сферически, планируется установить 2 точки доступа на 2 и 4 этажах, по 3 точки доступа на 1 и 3 этажах по всей площади корпуса , а беспроводной коммутатор - на втором и четвертом этаже, в центре, для охвата каждой точки доступа. Схема беспроводной сети представлена на рисунке 2.4

- Организация сети доступа требует выполнения следующих работ..

- Организовать сеть беспроводного доступа, для чего необходимо установить 10 точек доступа Ubiquiti UniFi по 3 точки на первом и третьем этажах и по 2 точки на втором и четвертых этажах.

- Разместить беспроводной коммутатор Ubiquiti TOUGHSwitchPoEPro в рабочем помещении на третьем этаже.

- Настроить беспроводной коммутатор, определить точки доступа. Обеспечить мониторинг и защиту сети.

- Организовать подключения к сети Internet. Доступ к сети Internet организовать через широкополосный /DSL модем.

Проектируемая сеть простроена по топологии ”звезда ” (рисунок 3.4), в которой роль центрального элемента выполняет беспроводной коммутатор Ubiquiti TOUGHSwitchPoEPro, а исполнительными компонентами являются тоски доступа Ubiquiti UniFi, размещенные на этажах санатория. Конфигурирование сети выполняется программным путем. М етса размещения точек определялись расчетным путем (см. раздел 4) и уточнялись экспериментально путем измерения уровнкей сигналов (см. раздел 5).



Рисунок 2.4 – Схема беспроводной сети

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 2.6. Код приведен в приложении Б.

# 3 РАСЧЕТ УРОВНЕЙ СИГНАЛА В ПОМЕЩЕНИЯХ КОРПУСА 2

## **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.

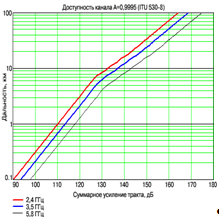


Рисунок 3.1 – График для определения дальности работы беспроводного канала связи

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 (freespaceloss) – 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 (SystemOperatingMargin) – 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 децебельный 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 – Размещение компонентов беспроводной сети

## **4.4 Инвентаризация беспроводной сети**

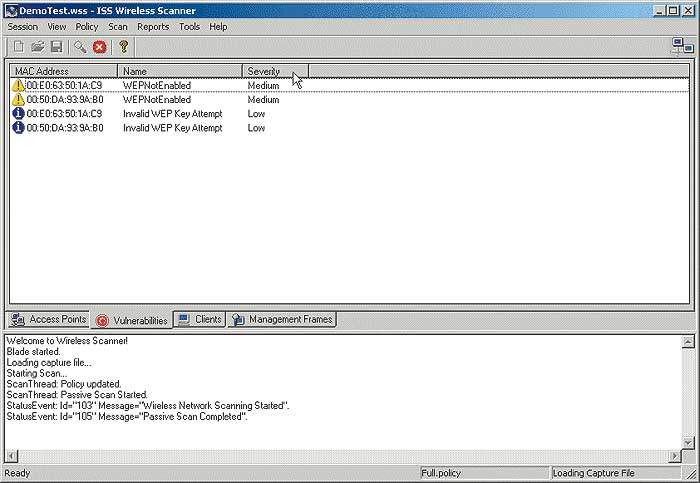
Первую, и самую распространенную, задачу можно решить с помощью достаточно большого количества инструментов — NetStumbler, Wellenreiter, WifiScanner и др., а также с помощью сканеров безопасности беспроводных сетей и ряд систем обнаружения атак.

Пионером среди средств инвентаризации беспроводных устройств является NetStumbler, который запускается под Windows 95/2000/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;

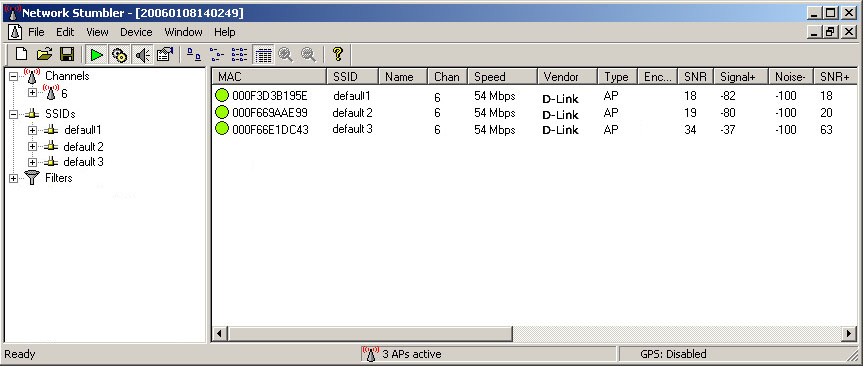
- обнаруживать различные атаки и попытки сканирования;

- отслеживать отклонения в политике безопасности и настройках беспроводных устройств.

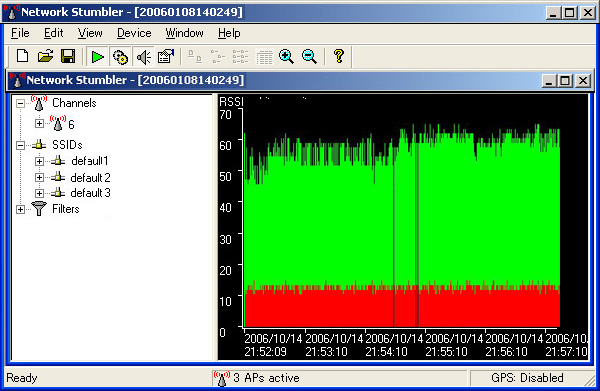
# 5 ЭКСПЕРЕМЕНТАЛЬНЫЕ ИССЛЕДОВАНИЯ СЕТИ

## **5.1 Измерение уровня сигнала**

Для обнаружения точек доступа, попадающих в зону действия беспроводной сети и определения каналов, на которых они работают, можно использовать программу Network Stumbler (<http://www.stumbler.net/>). Рис 2.1 С ее помощью можно также оценить соотношение сигнал/шум на выбранных каналах. Программа NetStumbler сканирует диапазон частот 2,4 ГГц и показывает все найденные в данном месте беспроводные точки доступа и адаптеры, работающие в режимеAd-Hoc. NetStumbler выдает информацию о MAC-адресах обнаруженных беспроводных устройств, значения SSID, имена устройств, каналы, сообщает о том, включено ли шифрование WEP и т. д.NetStumbler поможет определить правильно ли настроена ваша беспроводная сеть, найти места с недостаточным радиопокрытием, установить наличие и характеристики других сетей, которые могут мешать работе вашей сети.  
Суть работы программы состоит в рассылке широковещательных пакетов и анализе ответов на них. Испытания проводились с помощью ноутбука с беспроводным адаптером DWL-G132. Двойным щелчком мыши запускается программа, – и мы видим список работающих беспроводных сетей, организованных с помощью точек доступа (AP).

Рисунок 5.1 – Интерфейс программы NetStumbler

Слева расположена колонка с выбором опций – Channels (каналы, на которых работают устройства), SSID (название сети), и Filters – фильтрация по заданным критериям. Раскрывая опцию Channels, мы видим список используемых каналов:При выборе интересующего МАС-адреса в окне справа отображается качество связи с данным устройством.

  
Рисунок 5.2 Уровни отображения сигнала

По горизонтали откладывается дата и время измерения, по вертикали – уровень сигнала (зелёный) и уровень шума (красный) в dBm, соответственно, отношение сигнал/шум можно определить, вычитая из уровня сигнала уровень шума. (рисунок 6.2)

После испытания с помощью программы NetStumbler были определенны места для наилучшего расположения точек доступа (рисунок 5.3) Отображения уровня сигнала, чтобы во всех обслуживаемых помещениях был достаточный сигнал для подключения к сети.

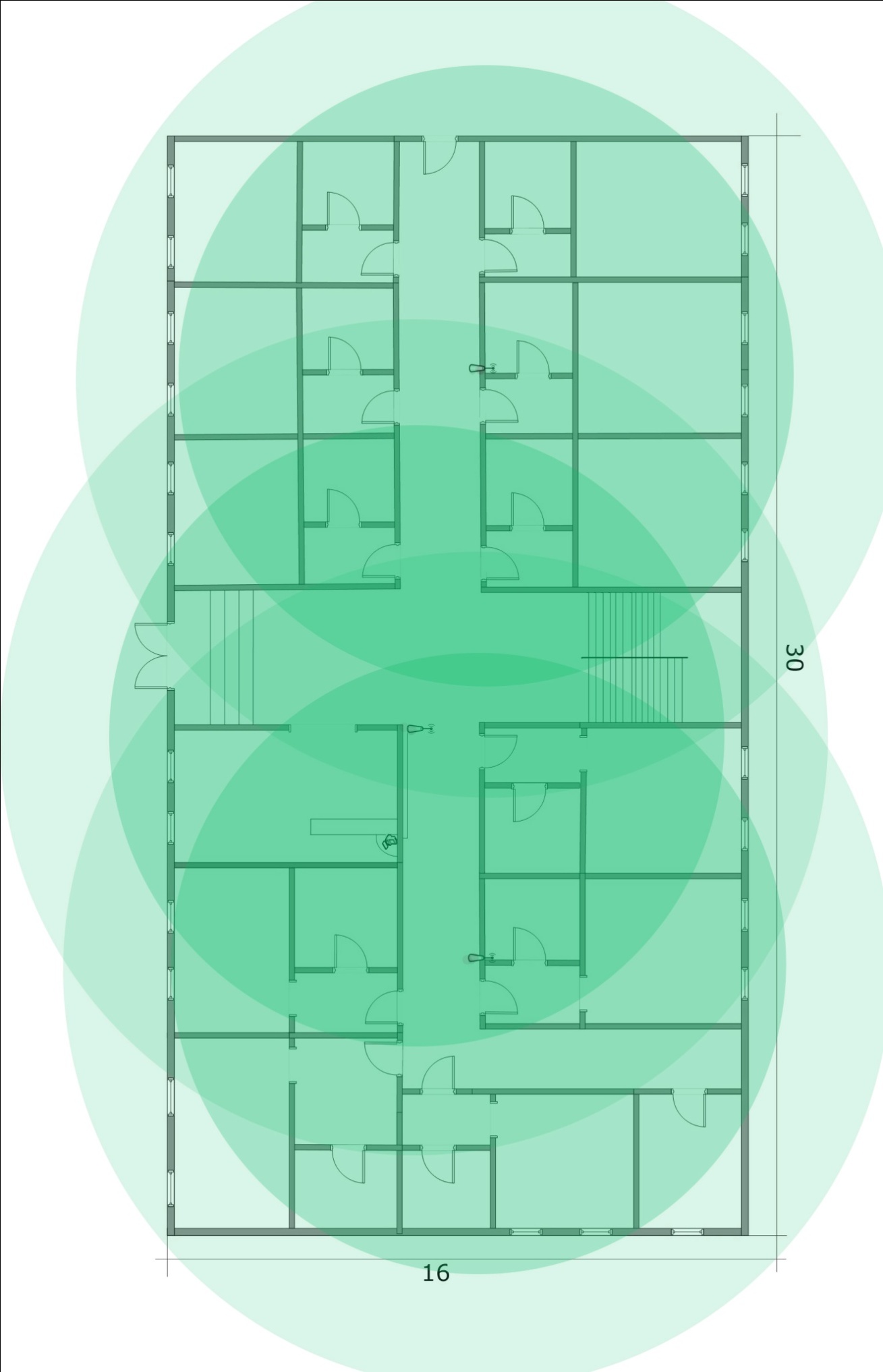


Рисунок 5.3 – Размещение точек доступа

## **5.2 Установка и настройка беспроводной точки доступа D-Link DWL - 2100AP**

Перед тем, как перейти к настройке, необходимо провести подготовительную работу. Ниже приведены три обязательных и два дополнительных шага, которые рекомендуется пройти.

1. Необходимо убедиться, что беспроводные клиенты могут подключаться и передавать данные через все точки доступа. Подобную проверку достаточно просто сделать, если подключить точки доступа к сети через Ethernet-порты. Тогда можно будет гарантировать работу беспроводной сети.

Задать для каждой точки доступа постоянный IP-адрес.

2. Присвоить статические IP-адреса, которые должны быть исключены из диапазона DHCP-сервера, иначе можно оказаться в ситуации, когда в сети будет два одинаковых адреса.

3. Установить на всех точках доступа один и тот же (свободный) канал. Поскольку все точки доступа в сети WDS обмениваются данными между собой, они должны использовать один канал. Для сетей 802.11b и 11g рекомендуется использовать 1, 6 или 11 каналы. Необходимо убедиться, что канал не используют соседние сети.

4. Задать одинаковые SSID для точек доступа (для удобства настройки и наглядности сначала можно задать различные SSID). Точки доступа WDS устанавливают соединения на основании MAC-адресов, поэтому смогут работать независимо от того, какие идентификаторы SSID заданы.  С технической точки зрения, каждая точка доступа в сети WDS является частью одной зоны обслуживания (ESS) и должна иметь один и тот же SSID.

4.Задать динамическое получение IP – адреса для беспроводных клиентов, чтобы любой пользователь мог легко

Самый простой способ узнать MAC-адреса точек доступа сети - воспользоваться утилитой, которая поставляется в комплекте с адаптером. Среди закладок с различными параметрами непременно можно встретить и список доступных точек доступа и их MAC-адреса. Иногда закладка называется "Просмотр доступных сетей" (Site Survey), или "Сети" (Networks), как в случае NETGEAR WG511T(рисунок 5.4).

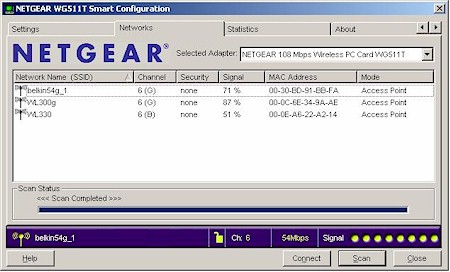


Рисунок 5.4 - Поиск MAC-адресов точек доступа

Если клиентская утилита не позволяет просматривать MAC-адреса, то можно воспользоваться интерфейсом администрирования точки доступа. Здесь стоит обратить внимание на обстоятельство, что некоторые модели отображают два MAC-адреса: для проводного и беспроводного интерфейсов. Если дело так и обстоит, то необходимо убедиться, что записан именно MAC-адрес беспроводного интерфейса.

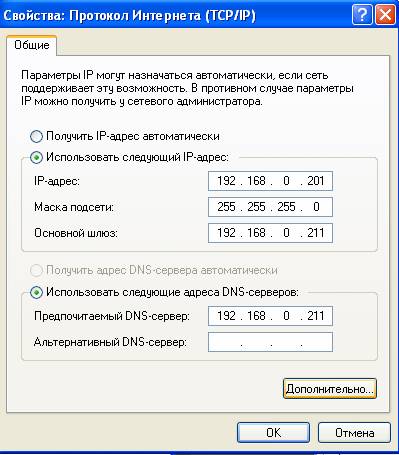


Рисунок 5.5 –Задание статического IP-адреса и маски подсети

В свойствах протокола TCP/IP должны быть записаны сетевые адреса из той же подсети где находится точка доступа: (рисунок 5.5). В точке доступа DWL-2100AP есть возможность просканировать диапазон для обнаружения точек доступа находящихся неподалёку. Для этого введем его IP-адрес в строку браузера (по умолчанию 192.168.0.50, логин admin, пароль admin).

Затем необходимо выбрать вкладку Wireless, указать режим Wireless Client и нажть Scan. (рисунок 5.6).

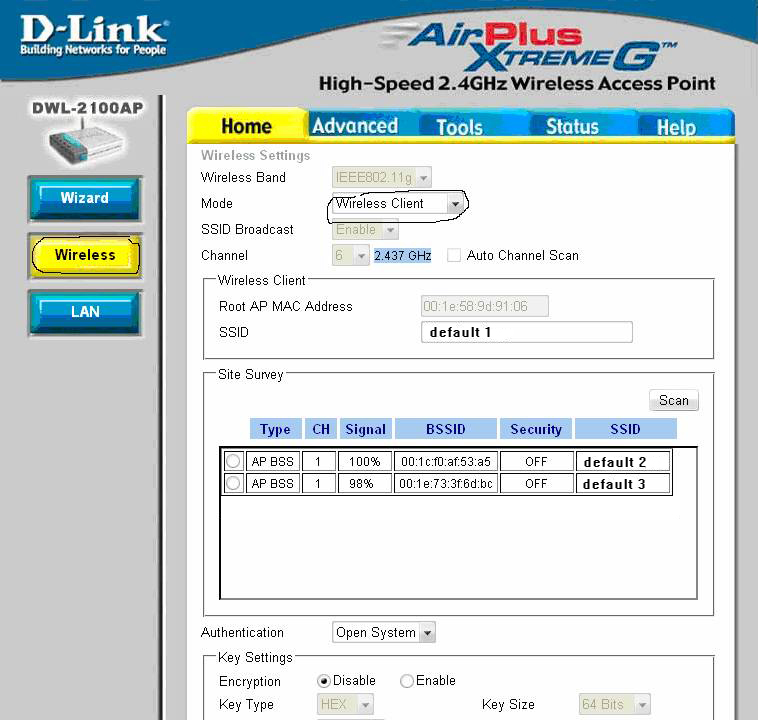


Рисунок 5.6 – Сканирование диапазона

В эфире сети в данном случае вещают 3 точки доступа, которые поддерживают режим WDS.

Для создания моста с выбранными точками доступа (топология кольцо) необходимо скопировать их MAC-адреса в буфер обмена и записать в блокнот. Далее выбирается параметр Mode: WDS with AP и копируем MAC – адреса удалённых точек доступа в ячейки.

# 6 ЭКОНОМИЧЕСКОЕ ОБОСНОВАНИЕ РАЗРАБОТКИ

## **6.1 Общая информация о сети**

Главной целью данной ВКР является организация сети беспроводного доступа в Санаторий им. Г. К. Орджоникидзе во втором корпусе целью предоставления современных услуг связи: высокоскоростной доступ в Интернет, на базе технологии Wi-Fi.

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:

- создать удобства и преимущества, связанные с локальной мобильностью;

- получение прибыли.

## **6.2 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 данной вкр, 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:

- Безопасность;

- Расширяемость;

- Управление;

- Продвинутые возможности;

- Высокая скорость;

- 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.

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

## **6.3 Финансовый план**

6.3.1 Расчет капитальных вложений

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

 (6.1)

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 6.1

Таблица 6.1 - Смета затрат на приобретение основного оборудования для реализации работы.

|  |  |  |  |
| --- | --- | --- | --- |
| Наименование | *Количество, шт.* | Цена за ед., руб. | Сумма, руб.  (без НДС) |
| точка доступа Ubiquiti UniFi | 10шт | 55 000 | 550 000 |
| ADSL D-Link 2500U | 2шт | 10 000 | 20 000 |
| Беспроводной коммутатор Ubiquiti TOUGHSwitch | 2шт | 12 500 | 24 000 |
| Fujitsu-Siemens PRIMERGY TX200 S3 | 2шт | 25 000 | 50 000 |
| Кабельная продукция UTP 5e | 200 м | 35 | 7 000 |
| Прочие материалы |  |  | 100 000 |
| ИТОГО: |  |  | 751 000 |

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

Ктр=0,03 \* Ко=0,03\*751 000=22 530 руб.

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

Км=0,01 \* Ко=0,01\*751 000=7 510 руб.

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

Кпр=0,005 \* Ко=0,005\*751 000= 3 750 руб.

Общая сумма капитальных вложений по реализации работы составляет:

ΚƩ . 751 000+22 530+7 510+3 750= 784 790 руб. (6.2)

6.3.2 Эксплуатационные расходы

Текущие затраты на эксплуатацию данной системы связи определяются по формуле:

 (6.3)

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 состоят 2 инженера-техника. Месячная зарплата у инженера-техника составляет 30 000 руб. Заработная плата сотрудников приведена в таблице 6.2

Таблица 6.2 – Заработная плата сотрудников

|  |  |  |  |
| --- | --- | --- | --- |
| Должность | Количество | Месячная заработная плата, руб. | Годовая заработная плата, руб. |
| Инженер-техник | 2 | 30 000 | 720 000 |

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

 (6.3)

где: Зосн - основная заработная плата,

Здоп - дополнительная заработная плата.

Основная заработная плата в год составляет:

Зосн = 720 000 руб.

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

 (6.4)

Здоп = 0.1\*720000= 72 000 руб

Общий фонд оплаты труда за год составит:

ФОТ=720 000 + 72 000 =792 000 руб.

Расчет затрат по социальным отчислениям.

Ставка на социальный налог 30.2%.

Ос = 792 000\*0,302= 239 184 руб.

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:

, (6.5)

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

ЗДОП.НУЖ. – затраты на дополнительные нужды;

Затраты электроэнергии на оборудование рассчитывается по формуле

, (6.6)

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

Т – время работы;

S – тариф, равный 1 кВт/час = 5.2 руб.

22 – количество рабочих дней в месяце;

12 – количество месяцев в году.

Зэл.обор.=5.2\*16.8 \* 22 \* 12 = 23 063 руб.

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

 (6.7)

где: ЗЭЛ.ОБОР - затраты на электроэнергию для оборудования;

Затраты на электроэнергию для дополнительных нужд:

Здоп.нуж = 0,05 \* 23 063 = 1 153 руб.

Тогда суммарные затраты на электроэнергию будут равны:

Э = 23 063 + 1 153 = 24 216 руб.

Расчет накладных затрат

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

 (6.8)

где: ФОТ – фонд оплаты труда;

Тогда накладные затраты составят:

Н=0.75\*(792 000 +239 184 + 23 063)=790 685 руб.

Результаты расчета годовых эксплуатационных расходов проекта по построению сети Wi-Fi, представлены в таблице 6.3

Таблица 6.3 – Годовые эксплуатационные расходы

|  |  |
| --- | --- |
| Показатель | Сумма руб. |
| ФОТ | 792 000 |
| Отчисления на социальные нужды (Ос) | 239 184 |
| Затраты на электроэнергию (Э) | 24 216 |
| Накладные расходы (Н) | 790 685 |
| ИТОГО | 1 846 085 |

6.3.1 Расчет доходов

Рассчитаем условный доход, полученный от внедрения сети.

Услуга Wi-Fi предоставляет возможность пользователям ноутбуков, карманных персональных компьютеров и смартфонов, имеющих порт Wi-Fi, получить беспроводный доступ в сеть Интернет. Оплата услуги через терминал по ежемесячным тарифам.

По статистическим данным каждый пользователь Сети в среднем за месяц использует тариф интернета за 1000 руб.

Доход от реализации услуг рассчитывается по формуле

 (6.9)

где: T – месячная абонентская плата клиентов;

N – количество клиентов, По статистическим данным в среднем в корпусе насчитывается 400 клиентов(всего проживает 500 человек);

n – число месяцев;

Д = (1000х12)\*400=4 800 000руб.

Оценки эффективности от реализации проекта производится на основе следующих показателей:

Чистый доход;

Чистый приведенный доход;

Срок окупаемости без дисконтирования;

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:

 (6.10)

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:

 (6.11)

Прибыль от реализации услуг рассчитывается по формуле:

 (6.12)

где: Д - реальный доход от внедрения услуг в год, ∑Э – эксплуатационные

расходы.

Прибыль от реализации услуг в соответствии с формулой (6.12)

составила

П = 4 800 000 – 1 846 085 = 2 953 915 руб.

КПН в соответствии с формулой (5.11) составил

КПН=0.2\*2 953 915 =590 783 руб.

Тогда чистая прибыль после налогообложения в соответствии с формулой (6.10) составит:

ЧП = 2 953 915 – 590 783 = 2 363 132 руб.

Таблица 6.4 - Показатели доходов без учёта дисконтирования

|  |  |  |
| --- | --- | --- |
| Наименование показателя | 1 год | 2 год |
| Доходы от реализации услуг, руб. | 4 800 000 | 4 800 000 |
| Эксплуатационные расходы, руб. | 1 846 085 | 1 846 085 |
| Прибыль, руб. | 2 953 915 | 2 953 915 |
| Чистая прибыль, руб. | 2 363 132 | 2 363 132 |
| Чистый денежный поток, руб. | 1 177 500 | 2 355 000 |
| Капитальные вложения, руб. | 751 000 | 0 |
| Чистые поступления, руб. | -125 364 | 2 229 636 |

По графику на рисунке 6.1 графически определяется срок окупаемости средств, вложенных в проект. Без дисконтирования срок окупаемости равен 13 месяцев. График построен по данным таблицы 6.4

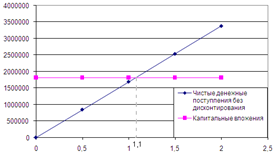


Рис 6.1 - График определения срока окупаемости проекта без учета дисконтирования

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:

 (6.13)

где ЧД– чистый доход от внедрения .

Кпр – коэффициент дисконтирования, который рассчитывается по формуле:

 (6.14)

где t- год после внедрения ;

r – ставка дисконта составляет 0,20

Коэффициент дисконтирования для двух лет:





Тогда приведенный чистый доход для первых двух лет будет равен:

ПЧД1 = 0.83 \*1 177 500 =977 325 руб.

ПЧД2 = 0.69 \* 2 355 000 = 1 624 950 руб.

Результаты расчета показателей дохода с дисконтированием представленны в таблице 6.5

Таблица 6.5 - Показатели доходов с учётом дисконтирования от реализации работы

|  |  |  |
| --- | --- | --- |
| Наименование показателя | 1 | 2 |
| Доходы от реализации услуг, руб. | 4 800 000 | 4 800 000 |
| Эксплуатационные расходы, руб. | 1 846 085 | 1 846 085 |
| Прибыль, руб. | 2 953 915 | 2 953 915 |
| Чистая прибыль, руб. | 2 363 132 | 2 363 132 |
| Чистый денежный поток, руб. | 1 177 500 | 2 355 000 |
| Коэффициент привидения | 0,83 | 0,69 |
| Приведенный чистый доход с учетом дисконтирования, руб. | 977 325 | 1 624 950 |
| Капитальные вложения, руб. | 751 000 | 0 |
| Чистые поступления, руб. | -413 486 | 1 211 464 |

По графику на рисунке 6.2 графически определяется срок окупаемости капиталовложений с учётом дисконтирования, который составил 1,3 года. График построен на основании данных таблицы 6.5

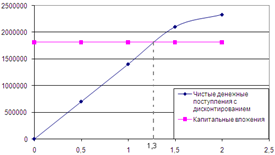


Рисунок 1.2 – График определения срока окупаемости работы с учетом дисконтирования

Коэффициент экономической эффективности вкр рассчитывается по формуле:

Eр =  (6.15)

И составил: Ер = (4 800 000 – 1 846 085)/751 000 = 3,9

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

Таким образом, коэффициент экономической эффективности от реализации работы составил 3,9 при нормативном значении 5, 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**

В данной части выпускной работы был представлен бизнес-план в котором рассматривается вопрос о внедрении сети беспроводного доступа во втором корпусе Санатории им. Г. К. Орджоникидзе.

# 7 БЕЗОПАСНОСТЬ И ЭКОЛОГИЧНОСТЬ РАБОТЫ

## **7.1 Параметры микроклимата в серверном кабинете**

Параметры микроклимата могут меняться в широких пределах, в то время как необходимым условием жизнедеятельности человека является поддержание постоянства температуры тела благодаря свойству терморегуляции, т.е. способности организма регулировать отдачу тепла в окружающую среду. Основной принцип нормирования микроклимата - создание оптимальных условий для теплообмена тела человека с окружающей средой. В санитарных нормах СН-245/71 установлены величины параметров микроклимата, создающие комфортные условия. Эти нормы устанавливаются в зависимости от времени года, характера трудового процесса и характера производственного помещения (значительные или незначительные тепловыделения). Для рабочих помещений с избыточным тепловыделением до 20 *ккал*/*м*3 допустимые и оптимальные значения параметров микроклимата приведены в таблице 1. В настоящее время для обеспечения комфортных условий используются как организационные методы, так и технические средства. К числу организационных относятся, рациональная организация проведения работ в зависимости от времени года и суток, а также организация правильного чередования труда и отдыха. В связи с этим рекомендуется вокруг здания организовывать. В настоящее время для обеспечения комфортных условий используются как организационные методы, так и технические средства. К числу организационных относятся, рациональная организация проведения работ в зависимости от времени года и суток, а также организация правильного чередования труда и отдыха. В связи с этим рекомендуется вокруг здания организовывать.

Таблица 1 − Допустимые и оптимальные значения параметров микроклимата

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Время года | Зона | Температура  воздуха, 0 C | Относительная  влажность, % | Скорость движения воздуха, м/с |
| Холодный период | Оптимальная | 18 - 21 | 60 - 40 | < 0.2 |
| Переходный период | Допустимая | 17 - 21 | < 75 | < 0.3 |
| Теплый период года (t > 100 C) | Оптимальная | 20 - 25 | 60 - 40 | < 0.3 |
| Допустимая | < 28 в 13 часов самого жаркого мес. | < 75 | < 0.5 |

Технические средства могут включать вентиляцию, кондиционирование воздуха, отопительную систему.

## **7.2 Электромагнитные поля и источники ионизирующих излучений помещения серверного кабинета.**

Напряженность электромагнитного поля не превышает 5 *кВ*/*м*, и, согласно ГОСТ 12.1.002-84 допускается пребывание в данном помещении в течение всего рабочего дня. Экраны дисплеев как источники электромагнитного излучения не представляют большой опасности даже при длительном воздействии на человека, если расстояние от экрана превышает 30 *см*.

Электромагнитные излучения на расстоянии 0,5 *м* вокруг монитора:

- по электрической составляющей в диапазоне 5 *Гц* - 2 *кГц* составляют 25 *В*/*м*, а в диапазоне 2 *кГц* - 400 *кГц* – 2,5 *В*/*м*.

- по магнитной составляющей в диапазоне 5 *Гц* – 2 *кГц* составляют 250 *нТл*, а в диапазоне 2 *кГц* - 400 *кГц* – 25 *нТл*.

Поверхностный электростатический потенциал составляет не более 500В, что соответствует допустимым значениям параметров излучений от видеомониторов. Напряженность электромагнитного поля не превышает допустимые дозы.

По норме, напряженность ЭМП в диапазоне частот 60 *кГц* – 300 *кГц* на рабочих местах персонала в течение рабочего дня не должна превышать установленных предельно – допустимых уровней ПДУ:

- по электрической составляющей в диапазоне (0,06–3) *МГц* составляют 50 *В*/*м*, (3–30) *МГц* – 20 *В*/*м*, (30–50) *МГц* составляют 10 *В*/*м*, (50–300) *МГц* составляют 5 *В*/*м*.  
- по магнитной составляющей в диапазоне (0,06–1,5) *МГц* составляют   
5 *А*/*м*, а в диапазоне (30–50) *МГц* составляют 0,3 *А*/*м*.

Ионизирующее излучение вызывает в организме цепочку обратимых и необратимых изменений. В данной организации нет непосредственных источников ионизирующего излучения. Поэтому она относится к категории В облучаемых лиц – население страны, края, области. Предельно допустимой дозой является 3 бэра за календарный год.

Ионизирующее излучение, при норме 60 *мкР*/*ч*, в отделе у – излучения от монитора: Фон =18 *мкР*/*час*.Излучения от компьютера: через защитный экран на расстоянии 2 *см* –20 *мкР*/*час*, без экрана на расстоянии 0 *см* – 25 *мкР*/*час*.  
γ+β – излучения: Фон 21 *мкР*/*час*, γ – излучения сзади монитора 19 *мкР*/*час.*

## **7.3 Пожароопасность и взрывоопасность**

Согласно НПБ 105-95 все объекты в соответствии с характером технологического процесса по взрывопожарной и пожарной опасности делятся на пять категорий. Данное здание относится к категории Д “негорючие вещества и материалы в холодном состоянии”. На объекте данной категории возникновение отдельных пожаров будет зависеть от степени огнестойкости зданий, а образование сплошных пожаров – от плотности застройки. По функциональной пожарной опасности здания и помещения подразделяются на классы в зависимости от способа их использования и от того, в какой мере безопасность людей в них, в случае возникновения пожара, находится под угрозой, с учётом их возраста, физического состояния, сна или бодрствования, вида основного функционального контингента и его количества. Данное здание относится к классу Ф4.3 – учреждения органов управления. Здание относится ко второй степени огнестойкости, так как выполнено из кирпича и бетона. Взрывчатые вещества в данном здании не хранятся.

## **7.4 Описание рабочего места сетевого администратора**

Рабочее место – это место временного или постоянного, периодического пребывания работающих в процессе трудовой деятельности. Различают постоянное и непостоянное рабочее место. Постоянное рабочее место – место, на котором работающий находится большую часть рабочего времени (более 50% или более 2 часов непрерывно). Непостоянное рабочее место – место на котором работающий находится меньшую часть своего рабочего времени (менее 50% или менее 2 часов непрерывно). При правильной организации рабочего места производительность труда сетевого администратора возрастает с 8% до 20%.

Согласно ГОСТ 12.2.032-78 конструкция рабочего места и взаимное расположение всех его элементов должно соответствовать антропометрическим, физическим и психологическим требованиям. Большое значение имеет также характер работы. В частности, при организации рабочего места программиста должны быть соблюдены следующие основные условия:   
– оптимальное размещение оборудования, входящего в состав рабочего места;   
– достаточное рабочее пространство, позволяющее осуществлять все необходимые движения и перемещения;

– необходимо естественное и искусственное освещение для выполнения поставленных задач;

– уровень акустического шума не должен превышать допустимого значения.

Главными элементами рабочего места сетевого администратора являются компьютерный стол и кресло. Основным рабочим положением является положение сидя. Рабочее место для выполнения работ в положении сидя организуется в соответствии с ГОСТ 12.2.032-78.

Рабочая поза сидя вызывает минимальное утомление сетевого администратора. Рациональная планировка рабочего места предусматривает четкий порядок и постоянство размещения предметов, средств труда и документации. То, что требуется для выполнения работ чаще, расположено в зоне легкой досягаемости рабочего пространства. Моторное поле - пространство рабочего места, в котором могут осуществляться двигательные действия человека. Максимальная зона досягаемости рук - это часть моторного поля рабочего места, ограниченного дугами, описываемыми максимально вытянутыми руками при движении их в плечевом суставе. Оптимальная зона - часть моторного поля рабочего места, ограниченного дугами, описываемыми предплечьями при движении в локтевых суставах с опорой в точке локтя и с относительно неподвижным плечом. На рисунке ниже, показаны зоны досягаемости рук в горизонтальной плоскости.

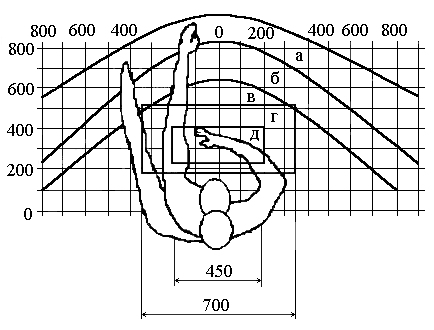


Рисунок 1 – Зоны досягаемости рук в горизонтальной плоскости

На рис.1 приняты следующие обозначения:

– а - зона максимальной досягаемости;

– б - зона досягаемости пальцев при вытянутой руке;

– в - зона легкой досягаемости ладони;

– г - оптимальное пространство для грубой ручной работы;

– д - оптимальное пространство для тонкой ручной работы.

Оптимальное размещение предметов труда и документации в зонах досягаемости рук:

– *дисплей* - размещается в зоне а (в центре);

– *клавиатура*, *мышь* - в зоне г, д;

– *системный блок* - размещается в зоне б (слева);

– *принтер* - находится в зоне а (справа);

– *документация* - в зоне легкой досягаемости ладони - в (слева) - литература и документация, необходимая при работе или в выдвижных ящиках стола – литература, неиспользуемая постоянно.

### 7.5 Охрана окружающей среды при использовании ЭВМ

При производстве, эксплуатации и утилизации ЭВМ возникают вредные факторы, отрицательно влияющие на окружающую среду.  
На этапе разработки происходит косвенное влияние, за счёт потребления энергии на освещение и работу вычислительной техники. Производящие электроэнергию электростанции наносят огромный вред окружающей среде. Для уменьшения влияния вредных факторов необходимо сокращение потребляемой электроэнергии за счёт рационального использования средств вычислительной техники и планирования рабочего дня.

Основными влияющими факторами являются загрязнения на этапе производства. Наибольшую опасность представляет загрязнение атмосферы токсичными газами (оксид углерода, фтористый водород) и аэрозолями (свинец и его соединения), которые выделяются при проведении монтажных работ. В этом случае в рабочей зоне воздух находится в состоянии насыщения вредными элементами, а удаляемый из помещений вентиляционный воздух может стать причиной загрязнения атмосферного воздуха.

Для предотвращения этого используются различные методы защиты атмосферы. Основными из них являются: локализация токсичных веществ у источников загрязнения и очистка загрязненного воздуха. В свою очередь эти методы представляют целый набор мероприятий по очищению окружающей среды. Устройства для локализации примесей представляют собой местные отсосы и укрытия с отсосами. В тех случаях, когда источник вредных выбросов заключен внутри пространства, огражденного жесткими стенками, отсосы выполняются в виде вытяжных шкафов, кожухов, витринных отсосов. Если по условиям технологии или обслуживания источник вредности нельзя заключить в кожух, то над таким источником или около него устанавливается вытяжной зонт. Очистка загрязненного воздуха может осуществляться сухими или мокрыми пылеуловителями, фильтрами, электрическими фильтрами. В нашем случае могут использоваться сухие пылеуловители типа СК-ЦИ-33, СК-ЦИ-34М или ЦИ-15, ЦИ- 24. Могут использоваться также мокрые пылеуловители типа СЦВ-20. В качестве фильтров можно применить фильтры типа “Фильтр 330 ” и “ Фильтр 550 ”. Очень эффективной является электрическая очистка воздуха от примесей. Этот метод основан на ударной ионизации газа в рабочей зоне коронирующего разряда, передаче зарядов ионов частицам примесей, и осаждении последних на осадительных и коронирующих электродах. В нашем случае в качестве электрофильтра можно применить фильтр типа УГМ (унифицированные, горизонтальные, малогабаритные).

Также на этапе изготовления существует опасность загрязнения гидросферы. При травлении печатных плат используют различные химические составы (хлорное железо и т.д.), часть которых попадает в сточные воды, следовательно, необходимо разработать очистные мероприятия. В соответствии с видами процессов, происходящих при очистке, все существующие методы принято делить на механические, физико-химические и биологические. При механической очистке сточных вод от взвешенных веществ используют процеживание, отстаивание, фильтрование и т.п. В настоящее время существенно увеличилась роль физико-химических методов (флотация, экстракция, нейтрализация, ионообменная и электрохимическая очистки) в связи с использованием оборотных систем водоснабжения. Биологическая очистка сточных вод применяется для выделения из них тонкодисперсных и растворенных органических веществ основана на способности микроорганизмов использовать для питания, содержащиеся в сточных водах органические вещества (кислоты, спирты, углеводы и т.п.). внашем случае можно применить электрохимическую очистку и сорбцию для защиты водных ресурсов от загрязнения отходами производства.

На всех этапах изготовления устройства существует опасность загрязнения литосферы. При нарезке, пайке, травлении печатных плат, изготовлении и покраске корпуса остаются отходы, содержащие свинец, олово и их соединения, органические горючие (обтирочные материалы, ветошь, обрезки пластмасс, оргстекла, остатки лакокрасочных материалов), которые необходимо складировать в определенном месте и в дальнейшем отправлять на переработку на полигон. Переработку промышленных отходов производят на специальных полигонах, создаваемых в соответствии с требованиями СНиП 2.01.28-85 и предназначенных для централизованного сбора, обезвреживания и захоронения токсичных отходов.

На этапе эксплуатации ЭВМ не является источником вредных выбросов, шума и вибрации, ионизирующего и СВЧ излучения. ЭВМ обладает относительно малым энергопотреблением, что способствует сбережению электроэнергии на этапе эксплуатации.

После окончания срока эксплуатации происходит утилизация ЭВМ.

Вывод: В данном разделе ВКР проанализированы безопасность и экологичность ЭВМ по всему технологическому циклу. При условии соблюдения всех мер, данная система безопасна и экологична, в случае возникновения чрезвычайных ситуаций предусмотрены меры по их устранению.

# ЗАКЛЮЧЕНИЕ

В своей ВКР я произвел обоснование проекта «Проектирование беспроводной сети Wi-Fi на основе стандарта 802.11n». В работе был сделан анализ сети беспроводного доступаWi-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 десяти точек доступа. Выбор обусловлен условиями технических параметров оборудования. В расчетной части дипломного проекта произведены расчеты эффективной изотропной излучаемой мощности и зона покрытия сети.

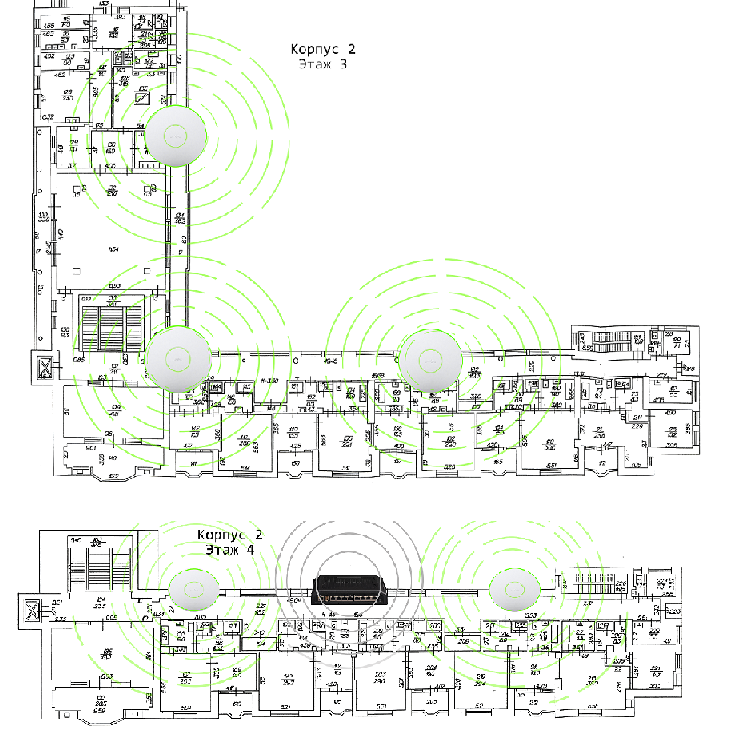
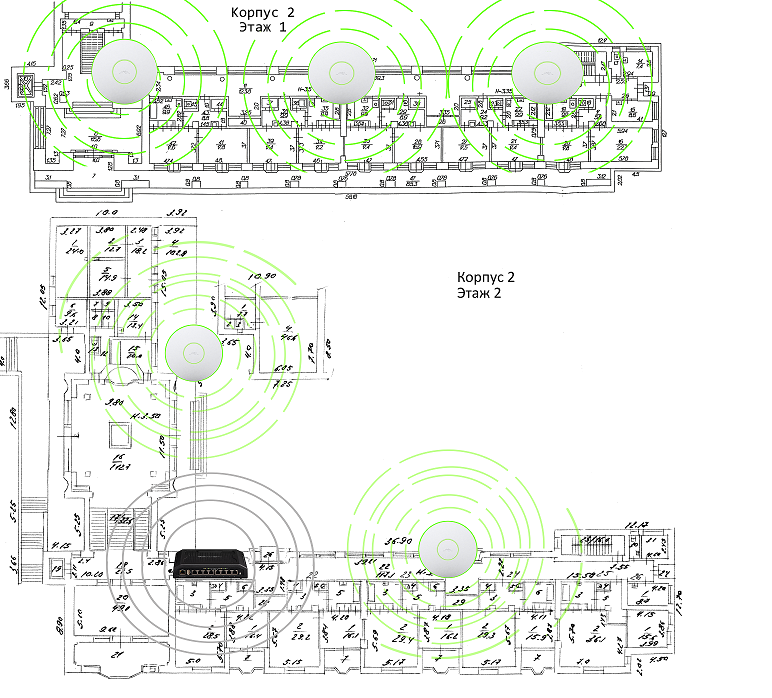
В разделе безопасности и жизнедеятельности был проведены: анализ условий труда, расчет системы искусственного освещения и пожарной безопасности.

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 2002.  
7«WLAN: практическое руководство для администраторов и профессиональных пользователей» / Томас Мауфер, 2005  
8 «Беспроводные сети. Первый шаг» / Джим Гейер. – М.: Издательство: Вильямс, 2005  
9 «Современные технологии и стандарты подвижной связи» / Кузнецов М.А., Рыжков А.Е. – СПб.: Линк, 2006

10 «Базовые технологии локальных сетей» / В.Г. Олифер: Питер, 1999  
11СайткомпанииApertoNetworks.: [http://www.ApertoNetworks..com](http://www.axxcelera.com)  
12 Шахнович С. Современные беспроводные технологии. - ПИТЕР, 2004  
13 Голубицкая Е.А., Жигуляская Г.М. Экономика связи. – М.: Радио и связь, 1999.



# ПРИЛОЖЕНИЕ А План здания с точками доступа

# ПРИЛОЖЕНИЕ Б- 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.