МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество
АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ

кафедра телекоммуникационных систем

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

ДИПЛОМНЫЙ ПРОЕКТ

На тему: Организация беспроводной корпоративной сети обмена данными между бизнес центрами гостиниц г. Алматы.

Специальность _____

Выполнил (а) Сидорков Р.Р. ЗРЭук-12
(Фамилия и инициалы) группа

Научный руководитель Белеков С.А. ст. препод. к.х.н.
(Фамилия и инициалы, ученая степень, звание)

Консультанты:

по экономической части:
Бекишева А.У., к.э.н., доцент
(Фамилия и инициалы, ученая степень, звание)
_____ «16» 06 2016 г.
(подпись)

по безопасности жизнедеятельности:
к.т.н. доц. Аймакова
(Фамилия и инициалы, ученая степень, звание)
_____ «02» 06 2016 г.
(подпись)

по применению вычислительной техники:
к.т.н. ст. пр. Ворреилова
(Фамилия и инициалы, ученая степень, звание)
_____ «08» 06 2016 г.
(подпись)

ст. преподаватель ТКС Кондратович А.Т.
(Фамилия и инициалы, ученая степень, звание)
_____ «16» 06 2016 г.
(подпись)

Нормоконтролер: ст. препод. ТКС Кондратович А.Т.
(Фамилия и инициалы, ученая степень, звание)
_____ «16» 06 2016 г.
(подпись)

Рецензент: Касимов Абдуразак Орозгазиевич
(Фамилия и инициалы, ученая степень, звание)
_____ «18» 06 2016 г.
(подпись)

Алматы 2016 г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество

АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ

Факультет радиотехники и связи
Специальность 5В071900 - радиотехника, электроника и телекоммуникации
Кафедра телекоммуникационных систем

ЗАДАНИЕ

на выполнение дипломного проекта

Студент Сидиков Канат Бирлибаевич
(фамилия, имя, отчество)

Тема проекта Организация беспроводной корпоративной сети обмена данными между бизнес центрами гостиниц г. Алматы.

утверждена приказом ректора № ___ от «___» 20___ г.

Срок сдачи законченной работы «___» _____ 20___ г.

Исходные данные к проекту требуемые параметры результатов проектирования (исследования) и исходные данные объекта

1) Стандарт технологий беспроводной связи 802.11
2) Расстояние между гостиницами
3) Маршрутизатор Revolution
4) RWR 500 x

Перечень подлежащих разработке дипломного проекта вопросов или краткое содержание дипломного проекта:

1) Проведение исследование беспроводной сети
2) Расчет затухание
3) Расчет мощности передатчика
4) Расчет шумовой температуры
5) Выбор состава оборудование
6) Тестирование производительности оборудования.
7) Расчеты по безопасности жизнедеятельности
8) Расчеты по экономики

Перечень графического материала (с точным указанием обязательных чертежей)

Задачи проекта

1) Схема корпоративной сети передачи данных масштаба области
2) Схема распределенной сети, объединяющей подразделения компаний на большой территории.
3) Корпоративная сеть с развитой древовидной структурой и общим номерным планом.
4) Тестирование маршрутизатора 8 направлений LAN-WAN
5) Тестирование беспроводной части (шифрование WPA)
6) Расчёт энергетических параметров, расчёт затуханий
7) Расчёт мощности передатчиков.
8) Расчёт шумовой температуры.
9) Состав оборудования
10) Спецификация оборудования станции
11 Безопасность жизнедеятельности.

Рекомендуемая основная литература

1) Фалько А.И. Основы радиоприёма: Учебное пособие.- Новосибирск: СибГУТИ, 2005-186 с.
2) Денисьева О.М., Мирошников Д.Г. Средства связи для последней мили.- М.: Эко Трендз 2000-350 с.
3) Щуко Л.П. Справочник по охране труда.- М.: Энергоатомиздат, 2002-220 с.
4) Гродник Г.А., Голубицкая Е.А. Основы экономики предприятий телекоммуникаций.- М.: Радио и связь, 1997-324 с.

Консультанты по проекту с указанием относящихся к ним разделов

Раздел	Консультант	Сроки	Подпись
БЖД	Аникеева А.А	28.04-02.06.16	
Эконом. часть	Векшуева А.Ч.	16.06.16	
Вопрос. техники	Ефремова Л.С.	02.03-08.06.16	
Тех. часть	Беляков С.А.	10.06.16	

Г Р А Ф И К
подготовки дипломного проекта

№ п/п	Наименование разделов, перечень разрабатываемых вопросов	Сроки представления руководителю	Примечание
1	Анализ и выбор технологий построения сети	19.10.2015	
2	Необходимость построения заданной сети.	25.10.2015	
3	Задание на проектирование	11.11.2015	
4	Радиомаршрутизаторы	28.11.2015	
5	Антенны	13.12.2015	
6	Безопасность данных	21.12.2015	
7	Построение беспроводной сети	09.01.2016	
8	Проведение исследований	17.01.2016	
9	Расчёт энергетических параметров	23.02.2016	
10	Состав оборудования	28.02.2016	
11	Сравнение возможностей проводных и беспроводных сетей.	13.03.2016	
12	Построение сети на базе стандарта IEEE 802.11	19.03.2016	
13	Техническая характеристика выбранного оборудования	25.03.2016	
14	Безопасность излучения СВЧ диапазона	13.04.2016	
15	Стандарты для электромагнитного излучения f, ГГц.	24.04.2016	
16	Технико-экономическое обоснование проекта	25.05.2016	

Дата выдачи задания «19» 09 2015 г.

Заведующий кафедрой _____ _____
(подпись) (Фамилия и инициалы)

Руководитель _____ Белехов С.А.
(подпись) (Фамилия и инициалы)

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

Аңдатпа

Берілген дипломдық жобаның мақсаты Алматы қаласы қонақ үйлердің бизнес орталықтар арасындағы радио-басқару арқылы мәліметтер тарату желісін ұйымдастыру. Жобада желі құрылуының негізгі топологиялары және RadioEthernet желісінің сипаттамалары мен мінездемелері, сонымен қатар таңдалған жабдықтарының техникалық сипаттамасы және құрамы қарастырылған.

Жобаның есептік бөлімінде күшейту коэффициенттері, тарату-шылардың қуаттары, және радиожолының басқа негізгі параметрлері есептелген. Жабдықтардың қажетті санының есебі берілген.

Жобаның техникалы-экономикалық көрсеткіштердің есебі берілген және антенналарды жерге қосу және найзағайдан қорғау сұрақтары қарастырылған.

Аннотация

Целью данного дипломного проекта является организация сети передачи данных между бизнес центрами гостиниц города Алматы посредством радиодоступа. В проекте рассмотрены основные топологии построения сети, описание и характеристики сетей RadioEthernet, а также технические характеристики и состав выбранного оборудования.

В расчётной части проекта рассчитаны затухания, коэффициенты усиления, мощности передатчиков и другие параметры радиолинии. Дан расчёт необходимого количества оборудования.

Дан расчет технико-экономических показателей проекта и рассмотрены вопросы заземления и молниезащиты антенн.

Annotation

The purpose of the given degree project is the organization of a network of data transmission between bisiness senters of Almaty sity hotels by means of a radio access. In the project the basic topology of construction of a network, the description and characteristics of networks of radio Ethernet, and also characteristics and structure of the chosen equipment are considered.

In a settlement part calculation of key parameters of the communication line, such as attenuation, factors of amplification, capacity of transmitters, good qualities and temperatures is resulted. Calculation of necessary quantity of the equipment, technic- economic parameters, grounding and protection against a lightning of aerials is made.

Содержание

Введение……... 7
1 Анализ и выбор технологии построения сети…… 9
1.1 Необходимость построения заданной сети……..... 9
1.2 Сравнение возможностей проводных и беспроводных сетей…….. 10
1.3 Характеристика беспроводных локальных сетей…….. 12
1.4 Характеристика систем широкополосного беспроводного доступа… 13
1.5 Построение сети на базе стандарта IEEE 802.11…… 25
1.6 Задание на проектирование…….. 35
2 Техническая характеристика выбранного оборудования……..... 37
2.1 Радиомаршрутизаторы…… 37
2.2 Антенны……. 39
2.3 Основные возможности и характеристики оборудования……... 43
2.4 Типовые применения оборудования…… 45
2.5 Безопасность данных……..... 47
3 Построение беспроводной сети…….. 51
3.1 Проведение исследований……... 51
3.2 Примеры построения сети и тестирование производительности оборудования ……. 52
3.3 Расчёт энергетических параметров……. 58
3.4 Состав оборудования……. 65
4 Охрана труда……. 66
4.1 Безопасность излучения СВЧ диапазона……..... 66
4.2 Стандарты для электромагнитного излучения…… 69
4.3 Расчёт защитного заземления…… 70
4.4 Молниезащита антенн…… 73
5 Бизнес план…….. 75
Заключение……... 81
Список литературы……..... 82
Приложение А……. 84

Введение

Одна из характерных примет начала XXI века- это стремительное развитие и проникновение во все сферы нашей жизни средств радиосвязи различного назначения, которые уже превратились в предметы первой необходимости. За очень короткий срок они стали мощным инструментом обмена и получения информации, будучи интегрированными в высокотехнологические системы и сети, благодаря постоянно возрастающим потребностям и возможностям оплаты услуг их пользователями.

Беспроводные сети стали целой индустрией, в которой занято огромное количество компаний. Утверждаются новые стандарты, появляется совместимое с ними оборудование. Строятся корпоративные WLAN-сети и точки публичного доступа («хот-споты»). Не отстают производители ноутбуков и карманных компьютеров, которые выпускают все более легкие и ультрапортативные модели, одинаково пригодные для работы в офисе и на природе.

Связать офис, гостиницу, аэропорт или кафе с внешним миром можно самыми разными способами. Компании с солидными офисами, охраной, системами наблюдения вполне могут позволить себе оптоволокно. Проводные технологии проверены временем, недороги, безопасны и производительны. Десятимегабитными, стамегабитными и даже гигабитными сетями Ethernet нынче уже никого не удивишь, сетевые контроллеры стоят достаточно дёшево и нередко входят в стандартную поставку ПК и ноутбуков. Тем не менее они не решают главное - не дают пользователю столь необходимой ему мобильности. То ли дело технологии беспроводных сетей, которые уже давно начали борьбу за массового потребителя [13].

Публичная сеть WLAN (PWLAN) обычно состоит из расставленных точек доступа (базовых станций), подключенных к IP сети оператора, и мобильных клиентов, которые подключаются к своей базовой станции с помощью сетевых карт. Все, что нужно для работы в таком месте- ноутбук с картой беспроводного доступа или PDA с поддержкой стандарта IEEE 802.11.

Поскольку радиус действия оборудования WLAN измеряется десятками метров, эти решения экономически выгодно использовать только в зонах повышенного спроса на услуги беспроводного доступа к сетям передачи данных- так называемых «hot spots».

Среди услуг, которые могут предложить путешественникам операторы мобильной связи и сервис-провайдеры- доступ в интернет, пользование почтовым ящиком, чатом, просмотр видеофильмов и, конечно, услуга доступа к корпоративной сети [14].

В современном телекоммуникационном сообществе не прекращаются дискуссии о возможной судьбе коммерческих зон беспроводного доступа («хот спотов»), созданных на базе беспроводных сетей стандарта IEEE 802.11 (Wi-Fi).

Все это позволяет надеяться на то, что развитие рынка Wi-Fi , по всей вероятности, мало будет отличаться от того, что происходит в странах с уже хорошо развитой инфраструктурой беспроводных сетей общего доступа. Одной из характерных черт такого развития является упор на корпоративных пользователей, то есть пользователей, не оплачивающих услуги из собственных средств. Причем речь в данном случае идет о наиболее активной их части- так называемых «мобильных работниках», которых становится с каждым днем все больше. Одна из основных задач Wi-Fi- предоставить таким пользователям серьезный инструмент для высокоскоростного доступа к ресурсам Интернет и корпоративным сетям.

Безусловно, говорить о массовости такого рынка пока не приходится. Но востребованность таких услуг уже сегодня налицо. Именно ориентированность рынка услуг Wi-Fi на мобильных работников диктует необходимость создания для них возможности использования корпоративных лицевых счетов в максимально большем количестве зон доступа.

В отличие от сетей сотовой связи, в Wi-Fi один, даже очень крупный оператор не может обеспечить значительное локальное и тем более глобальное покрытие в силу самой природы данной технологии. Будущее рынка Wi-Fi услуг выглядит именно как множество участников- операторов с различными бизнес моделями оказания услуг. Эта ситуация создает предпосылки для возникновения рынка услуг Wi-Fi-роуминга в беспроводных сетях стандарта IEEE 802.11.

В числе основных задач, встающих на пути развития новой технологии- интеграция с сетями GPRS, а в будущем- с 3G, сетевая безопасность и биллинг [23].

Преимущества беспроводных сетей перед проводными:

– пользователи могут свободно перемещаться, т.к. беспроводные сети обеспечивают доступ к сетевым ресурсам компании или к Интернет (для «хот-спотов») из любого места;Беспроводные сети, обладающие гибкостью при конфигурации и расширении, могут служить как добавлением, так и заменой проводных сетей при построении сетевой инфраструктуры;беспроводные сети не только обеспечивают мобильный доступ, но и сами мобильны, т.к. можно легко переместить сеть в другое место;

– повышение мотивации и привлекательности работы для корпоративных пользователей.

Сферы применения беспроводных сетей:

– доступ к Интернет в гостиницах, кафе, библиотеках, студенческих городках и т.д.;конференц-залы и выставочные комплексы;«гостевой» доступ к корпоративной сети для клиентов и партнеров;складские помещения и фабрики;

– больницы;

– учебные классы.

В дипломном проекте рассматривается организация беспроводной корпоративной сети обмена данными между бизнес центрами гостиниц г.

Алматы, что приведет несомненно к улучшению качества обслуживания населения услугами гостиничного хозяйства города.

1 Анализ и выбор технологии построения сети

1.1 Необходимость построения заданной сети

Развитие бизнеса, совершенствование информационных технологий, появление многочисленных бизнес- предложений изменили карту корпоративной связи. Современные средства автоматизации производственных процессов требуют наличия собственных корпоративных сетей практически у каждой организации и предприятия, претендующих на выживание и успех в конкурентной среде. В значительной степени именно потребности бизнеса обусловили развитие технологий Интернета, виртуальных частных сетей.

Содружество сетей и технологий рассматривается как явление корпоративного рынка: сопрягаются сети проводной и радиосвязи, спутниковые каналы через ведомственные АТС получают доступ в телефонные сети общего пользования (ТфОП), по выделенным каналам магистральных корпоративных цифровых ВОЛС организуются VPN. Но можно говорить и о содружестве корпоративных сетей и сетей общего пользования, формирующих единую взаимоувязанную сеть связи страны.

Молодая и растущая IP- технология вообще готовится произвести переворот в идеологии использования телекоммуникаций.

Технология корпоративной связи и связи общего пользования всё больше сближаются, конкурируя между собой. Остается надеяться, что выиграет потребитель [22].

Гостиничные хозяйства крупных городов представляют сегодня большие комплексы, предоставляющие не только услуги проживания, питания и отдыха населения, но и бизнес услуги для организаций и населения- организацию встреч, презентаций, видеоконференций и другие. Они постоянно осуществляют модернизацию своего хозяйства: совершенствуют систему бронирования номеров, улучшают обеспечение номеров гостиниц требуемыми в настоящее время разнообразными услугами телекоммуникации- увеличивают количество и качество услуг, предоставляемых населению. Гостиничные комплексы уже не могут существовать как обособленные, без надежной телефонной связи и обмена мультимедейными данными, без возможности передачи видеосообщений между собой.

Город Алматы считается южной столицей Казахстана, является крупнейшим мегаполисом Республики, одним из самых крупных деловых и культурных центров Центральной Азии. Это суперсовременный, стремительно развивающийся город. Здесь сосредоточено большое количество как государственных, так и негосударственных учреждений и

организаций, имеющих свои филиалы и тесные связи с другими организациями как Республики, так и стран зарубежья. В город постоянно приезжает в служебные командировки большое количество людей, которых необходимо разместить для проживания и обеспечить всеми требуемыми им услугами телекоммуникации. Различным организациям часто требуется организовать презентации и видеоконференции. Все это требует наличия во всех гостиничных комплексах бизнес-центров, оснащенных современным оборудованием и имеющих постоянную связь и возможность обмена данными между собой, а также выход на корпоративные и государственные сети телекоммуникации.

Организацию сети передачи данных между гостиничными комплексами города Алматы можно начать с охвата сетью нескольких наиболее крупных и хорошо известных гостиниц: Казахстан, Анкара, Отрар, Алма-Ата, Жетысу, Алатау, Астана, Достык, Амбассадор, Хаятт Ридженси.

Месторасположение гостиниц: гостиница Казахстан- проспект Достык 52, угол проспект Абая; гостиница Анкара- улица Желтоксан 181, угол улица Тимирязева; гостиница Отрар- улица Гоголя 73, угол улица Кунаева; гостиница Алма-Ата- улица Кабанбай батыра 85, угол улица Панфилова; гостиница Жетысу- проспект Абылай-хана 55, угол улица Макатаева; гостиница Алатау- проспект Достык 105, угол улица Хаджи-Мукана; гостиница Астана- улица Байтурсынова 113, угол улица Сатпаева; гостиница Достык- улица Курмангазы 26, угол улица Кунаева; гостиница Амбассадор- улица Желтоксан 121, угол улица Виноградова; гостиница Хаятт Ридженси- улица Сатпаева 26/9.

Как известно, в настоящее время связь между гостиницами осуществляется через телефонную линию Казахтелекома и платятся немалые деньги за аренду каналов. Да и конфиденциальность информации передаваемой по этим каналам остаётся под вопросом. Поэтому организация своей сети передачи данных между гостиницами является в настоящее время актуальной.

1.2 Сравнение возможностей проводных и беспроводных сетей

На сегодняшний день в мире используется большое количество различных технологий и решений, которые позволяют передавать данные на разные расстояния, с разными скоростями.

В качестве среды для передачи информации наиболее распространены оптоволокно и медные провода. Технологии, реализованные на оптоволокне, отличаются высокими скоростями передачи данных, надежностью и высокой стоимостью реализации. Решения, работающие на меди гораздо более медленные но, проложенные для нужд телефонизации, зачастую самый выгодный способ организации связи. В контексте сети передачи данных масштаба города необходимо отметить тот факт, что проводная городская инфраструктура, созданная и развиваемая в основном ТфОП, зачастую не позволяет надеяться на качественную компьютерную связь в любой,

произвольно взятой, точке города. Поэтому радиосредства могут оказаться серьезной альтернативой для решения проблем «последней мили».

Беспроводные технологии позволяют на сегодня передавать данные со скоростями в 2 Мбит/с, 5,5Мбит/с и 11Мбит/с. В области стандартизации беспроводной технологии передачи данных в 1998 году были достигнуты определенные успехи, что позволяет надеяться на серьезное удешевление продуктов массового применения. Радиосистемы, использующие расширение спектра методом прямой последовательности (так называемые RadioEthernet) на сегодняшний день уже достаточно хорошо опробованы для связи локальных сетей, удаленных друг от друга на расстояния в десятки километров. Кроме того, эти системы позволяют строить сети типа точка-многоточка, которые описываются и характеризуются как сети микросотовой связи, в которых абоненты имеют фиксированное положение.

Беспроводная сеть передачи данных состоит из базовых станций, увязанных между собой в единую инфраструктуру и соединенных с информационным центром- источником информации для потребителей, являющихся абонентами этой сети. Структура сети обеспечивает двунаправленный обмен информацией между абонентом и информационным центром (Internet провайдером) либо другим абонентом, подключенным к сети. Таким образом, имеется постоянная связь одного либо нескольких офисов с информационным центром либо другим офисом. Структура сохраняется даже при смене местоположения абонента, главное установить связь с сетью, что возможно из любой точки города.

Рассмотрим характеристики микросотовой системы связи, использующей оборудование, присутствующее сегодня на рынке и имеющее скорость до 11 Мбит/с. Наиболее распространены сегодня устройства, производимые компаниями Aironet Wireless Technology Inc., Lucent Technologies, BreezeCom, Revolution. В ряду устройств, позволяющих построить систему передачи данных, есть как радиобриджи- устройства, подключаемые к компьютерам с помощью стандартных сетевых средств, так и радиокарты- предназначенные для использования как платы расширения стандартных персональных компьютеров. При этом система допускает использование в режиме базовых станций только радиобриджи, а в режиме клиента- и радиобриджи, и радиокарты. Базовая станция, как и в системах сотовой связи, устанавливается так, чтобы обеспечивать покрытие определенной зоны обслуживания. При этом применяются различные типы антенн- от простейших штыревых с круговой диаграммой направленности, до сложных систем секторных антенн, позволяющих изменять диаграмму направленности излучения в зависимости от потребностей.

Каждый радиобридж, работающий в режиме базовой станции на скорости 2 Мбит/с, позволяет обслуживать 10-15 абонентов, при этом средняя скорость работы каждого из абонентов будет не ниже 64 кбит/с. Увеличение количества абонентов допустимо, но приводит к деградации скоростных характеристик канала. Кроме того, в непосредственной близости, на одной

крыше без применения специальных технических мер можно устанавливать до трех комплектов сотообразующего оборудования, а с применением этих мер- до шести. Таким образом, количество обслуживаемых абонентов одной базовой станцией может достигать 45 или даже 90.

Взаимоувязка базовых станций между собой, а также привязка их к информационным ресурсам- поставщикам информации может осуществляться самыми различными способами, как традиционными оптоволоконными или проводными, так и радиосредствами. Применение самого быстродействующего оборудования, работающего со скоростью 11 Мбит/с в сочетании с увеличением плотности расположения базовых станций позволит существенно увеличить количество абонентов и скорость доступа для каждого из них [13].

Организовать связь между гостиницами, разбросанными по городу, посредством наземных каналов будет несколько затруднительно и потребует больше средств. Рассмотренные возможности различных сетей показывают, что для организации обмена данными между гостиницами лучшим вариантом скорее всего является сеть с использованием радиосредств.

С учетом вышесказанного, предлагается осуществить организацию сети передачи данных между вышеперечисленными гостиничными комплексами города Алматы посредством радиодоступа. Предлагается использовать технологию беспроводного Ethernet, а именно- оборудование Revolution 5000 на базе которого можно быстро организовать качественную сеть передачи данных. На дальнейшем этапе развития сети, в зависимости от поступления других заказов от гостиничных комплексов на подключение к этой сети, сеть в быстрые сроки может быть расширена с использованием соответствующих модулей. Поэтому возможность построения такой сети на базе оборудования Revolution 5000, является вполне реальной.

1.3 Характеристика беспроводных локальных сетей

Беспроводные локальные сети классифицируются согласно использованной в них технологии передачи. Все современные продукты рынка локальных сетей относятся к одной из следующих категорий:

– инфракрасные (Infrared - IR) локальные сети;

– отдельная ячейка сети, использующей передачу в инфракрасном диапазоне, ограничена размерами одной комнаты, поскольку инфракрасное излучение не проходит сквозь непрозрачные стены;

– узкополосная СВЧ передача.

Эти локальные сети работают на СВЧ, но не используют расширенный спектр. Некоторые из этих продуктов работают на частотах, требующих лицензии.

Локальные сети с расширенным спектром используют при передаче технологию расширенного спектра. В большинстве случаев эти локальные сети работают на диапазонах ISM (Industrial, Scientific and Medical Radio

Frequency Band- радиочастотные диапазоны для промышленного, научного и медицинского применения).

В настоящее время наиболее популярные беспроводные локальные сети используют технологию расширенного спектра [23].

Оборудование широкополосного доступа использует вполне определенный частотный диапазон. Прежде всего, это диапазон 2,4 ГГц. Обусловлено это тем, что во многих странах этот диапазон свободен от лицензирования и инсталляции оборудования, работающего в этом диапазоне, имеют массовый характер.

Сравнительные характеристики беспроводных локальных сетей приведены в таблице 1.1.

Таблица 1.1- Сравнительные характеристики беспроводных локальных сетей

	Инфракрасное излучение		Расширенный спектр		Радио
	рассеянное	с направленным лучом	перестройка частоты	прямая последовательность	узкополосная СВЧ-передача
Скорость передачи данных, Мбит/с	1-4	1-10	1-3	2-20	10-20
Диапазон волн, м	15-60	25	30-100	30-250	10-40
Длина волны/ частота	800-900 нм		902-928 МГц 2,4-2,5 ГГц 5,7-5,8 ГГц		902-928 МГц 5,2-5,8 ГГц 18,8-9,2 ГГц
Схема модуляции	ASK		FSK	QPSK	FS/QPSK
Излучаемая мощность	----		< 1 Вт		25 мВт

1.4 Характеристика систем широкополосного беспроводного доступа

Под термином «доступ» понимается сетевой доступ, имеющий массовый характер, т.е. сеть доступа. Радиомодемные соединения типа «точка-точка», а также радиорелейные линии связи, являющиеся традиционными средствами решения проблемы «последней мили"» с помощью радиосредств, имеют многочисленные примеры реализации, однако не обеспечивают массовый характер подключений. Поэтому в данном проекте рассматриваются системы беспроводного доступа, являющиеся функционально законченным набором аппаратно-программных средств, реализующие соединения типа «точка-много точек» и образующих сеть доступа.

Спрос на услуги телефонии и доступа в Интернет существует. Он рождает предложение, реализуемое на основе разнотипного оборудования

беспроводного доступа, которое в той или иной мере позволяет решать существующие задачи. Перечень основных классов систем беспроводного доступа и их краткие характеристики представлены в таблице 1.2.

Первые типы систем- это системы фиксированного радиодоступа (WLL-Wireless Local Loop), появившиеся как альтернатива проводной телефонии. К решениям этого класса можно отнести MultiGain Wireless (Innowave ECI Wireless Systems), где передача данных ограничивается полосой 64 кбит/с, ISDN BRI, или, фактически, модемным соединением 56 кбит/с, а также WLL DECT (Digital Enhanced Cordless Telecommunications- цифровые расширенные беспроводные телекоммуникации), где передача данных, организуемая через модемное соединение, имеет скорость еще меньше.

Таблица 1.2- Основные классы систем беспроводного доступа

Тип системы	Диапазон частот	Основная область использования	Достоинства	Недостатки
1	2	3	4	5
WLL DECT	1,88-1,90 ГГц	Доступ к ТфОП. Низкоскоростной доступ к Интернет	Простота легализации сети. Высокока. телефония	Низкая скорость модемного подключения к Интернет
WLL по фирменным стандартам	0,9-5,8 ГГц	Доступ к ТФОП. Низкоскоростной доступ к Интернет	Гибкость в выборе диапазона. Большой выбор оборудования	Несовместимость оборудования от разных производителей
LMDS	26-38 ГГц	Предоставление выделенных каналов. Высокоскоростная передача данных. Доступ к Интернет	Высокая пропускная способность	Высокая стоимость оборудования. Отсутствие единого стандарта. Малая дальность
MMDS	2,3-2,5 ГГц	Высокоскоростная передача данных. Доступ к Интернет. Цифровое телевещание	Высокая пропускная способность. Большая дальность	Высокая стоимость оборудования. Нет единого стандарта
Системы широкополосного беспроводного доступа (BWA)	2,4-10,5 ГГц	Высокоскоростная передача данных. Доступ к Интернет. Пакетная телефония	Большой выбор оборудования и частотных диапазонов	Несовместимость оборудования разных производителей

Продолжение таблицы 1.2

1	2	3	4	5
BLUETOOTH	2,4 ГГц	Беспроводная связь ближнего действия	Дешевизна и простота использования.	Большинство Bluetooth- устройств ограничено радиусом

			Малое энергопотребление	действия 10-30 м. Несовместимость продуктов разных производителей между собой
GPRS	<1,5 ГГц	Пакетная передача данных по беспроводным телефонным сетям и Интернету. Низкоскоростной доступ к Интернет	Обеспечивает мобильный, сравнительно деше- вый доступ в Интернет. Обширная зона покрытия	Нестабильная скорость передачи данных, малая надёжность соединения
Radio Ethernet стандарта IEEE 802.11 b	2,4 ГГц	Высокоскоростной доступ к Интернет. Корпоративные сети	Дешевизна и доступность оборудования. Высокая пропускная способность- до 11 Мбит/с на сектор. Большая дальность. Большой опыт использования оборудования. Совместимость оборудования от разных производителей	Высокая загруженность диапазона, помехи от пиратских радио-средств. Невозможность дальнейшего развития в крупных городах из-за исчерпания диапазона. Проблемы передачи трафика реального времени (голоса) из-за используемого коллизионного протокола
Radio Ethernet стандарта IEEE 802.11 a	5 ГГц	Высокоскоростной доступ к Интернет. Корпоративные сети.	Малая загруженность диапазона. Высокая пропускная способность- до 54 Мбит/с (в turbo режиме 108 Мбит/с) на сектор	Устройства дороже, чем 802.11 b и g. Получение лицензии на вторичной основе. Проблемы передачи трафика реального времени (голоса) из-за используемого коллизионного протокола

Вслед за сетями кабельного телевидения появились системы беспроводного телевещания на базе технологий MMDS (Multichannel Multipoint Distribution Service- многоканальная многоточечная распределительная служба) и LMDS (Local Multipoint Distribution Service). Их можно считать вторым источником BWA.

Компьютерная эра, сопровождавшаяся развитием локальных вычислительных сетей, обусловила появление беспроводных систем типа Wireless LAN, которые позже были стандартизованы комитетом IEEE 802.11

как сети радио-Ethernet. Именно на базе этих трех, ставших уже традиционными, технологий в последнее время получили развитие новые технические средства.

Разница между устройствами WLL и BWA достаточно условна и состоит в следующем. Системы WLL ориентированы преимущественно на предоставление услуг классической телефонии. Передача данных, как правило, осуществляется на уровне модемного подключения. Оборудование BWA, напротив, изначально создавалось для высокоскоростной передачи данных и позволяет формировать телефонные каналы поверх пакетного протокола, в качестве которого обычно применяется IP [23].

Оборудование широкополосного доступа использует вполне определенный частотный диапазон. Прежде всего, это диапазон 2,4 ГГц. Обусловлено это тем, что во многих странах этот диапазон свободен от лицензирования и инсталляции оборудования, работающего в этом диапазоне, имеют массовый характер.

За свободным от лицензирования диапазоном следуют полоса радиочастот 2,5-2,7 ГГц, используемая MMDS, диапазоны 3,5 ГГц, 5,8 ГГц. Как правило, в этих диапазонах работает оборудование операторского класса, имеющее большую абонентскую емкость и расширенный набор услуг (передача данных, мультимедиа, телефонии). Далее следуют частоты в диапазонах от 10 до 38 ГГц. Полоса радиочастот 27,5-29,5 ГГц используется системами LMDS. Эти системы специализированны для целей телевизионного вещания

Системы широкополосного беспроводного доступа типа «точка-много точек», работающие в микроволновом диапазоне до 38 ГГц, обладают уникальной емкостью. Информационные потоки, которыми оперируют подобного рода системы, позволяют характеризовать их радио интерфейс как ATM в эфире.

Используемые частоты обеспечивают работу систем в условиях прямой видимости. Возможности систем, характеристики, а также условия их применения обуславливают фиксированный доступ [27].

Подобные системы обладают очень важным качеством, как легкая расширяемость и масштабируемость. Являясь образующим элементом сети беспроводного доступа, базовая станция (БС) играет важную роль в классификации систем широкополосного беспроводного доступа. Информационная емкость БС позволяет условно разделить все системы беспроводного доступа по группам.

Абонентские устройства (Subscriber Units, SU), обслуживаемые БС и устанавливаемые у пользователя, имеют различный пользовательский интерфейс. Для телефонии используется абонентская линия (FXS), цифровой интерфейс E1, ISDN. Для передачи данных- Ethernet, Frame Relay с синхронным интерфейсом, ISDN.

Абонентские устройства имеют либо встроенную, либо внешнюю присоединяемую направленную антенну. Каждое абонентское устройство или устройство подписчика (SU) работает на свою БС.

Соединения между БС различных сот выполняются с помощью технологий проводного (чаще всего оптические линии связи) или беспроводного доступа (радиорелейные, либо радиомодемные линии связи).

Простота установки, удобство использования и относительно низкая цена беспроводного оборудования начального уровня обусловили спрос на него домашних потребителей. Эти пользователи имеют в квартире доступ в Интернет и как минимум один компьютер- стационарный или мобильный. Для них беспроводное решение- прежде всего альтернатива проводам, которая дает чувство свободы и удобства в собственном доме.

Домашние пользователи ограничиваются установкой одной точки доступа. Она создает зону покрытия в квартире и позволяет любому компьютеру с Wi-Fi адаптером подключиться к точке доступа и установить беспроводной канал. Сама точка доступа по проводному каналу подключена к оборудованию доступа в Интернет. В этом секторе рынка применяются самые простые решения, предлагаемые массой производителей, например LinkSys, ASUS, D-Link.

Кроме устранения проводов домашняя WLAN (рисунок 1.1) дает еще одно преимущество, позволяя объединить в сеть все устройства в квартире. Необходимо только иметь встроенную в них поддержку Wi-Fi. Такими устройствами могут стать домашний телефон, домашний кинотеатр, система безопасности и видеонаблюдения, холодильник и т. п.

Рисунок 1.1- Схема домашней беспроводной сети

Серьезным вопросом домашних WLAN остается их незащищенность от несанкционированного доступа. Основной причиной этого является слабая осведомленность индивидуальных пользователей о встроенных системах

защиты и неумении корректно провести настройку при первоначальной установке Wi-Fi устройств.

Стоит также упомянуть о процедуре регистрации WLAN для внутреннего использования, которая сильно упрощена по сравнению с процедурой получения частотных разрешений для беспроводных сетей фиксированного доступа.

В ИТ-компаниях применять беспроводные системы связи первыми начинают сотрудники, имеющие мобильные компьютеры. Ими движет то же желание, что и у домашних пользователей- избавиться от проводов, создать себе удобное рабочее место. По своей сложности такие системы практически не отличаются от домашних WLAN с той лишь разницей, что на территории офиса может быть установлено несколько точек доступа (рисунок 1.2).

Такая ситуация опасна тем, что установка отдельных точек доступа не инициируется руководством компании, а происходит спонтанно. Руководство не считает целесообразным построение офисной беспроводной сети. Желание же сотрудников в расчет не берется. В результате точки доступа, установленные и подключенные к корпоративной сети, создают серьезные бреши в системе безопасности предприятия.

Оборудование, используемое данным сектором рынка, ввиду минимальных к нему требований, приобретается из нижней ценовой категории. Соответственно и функциональное содержание таких устройств ограничено.

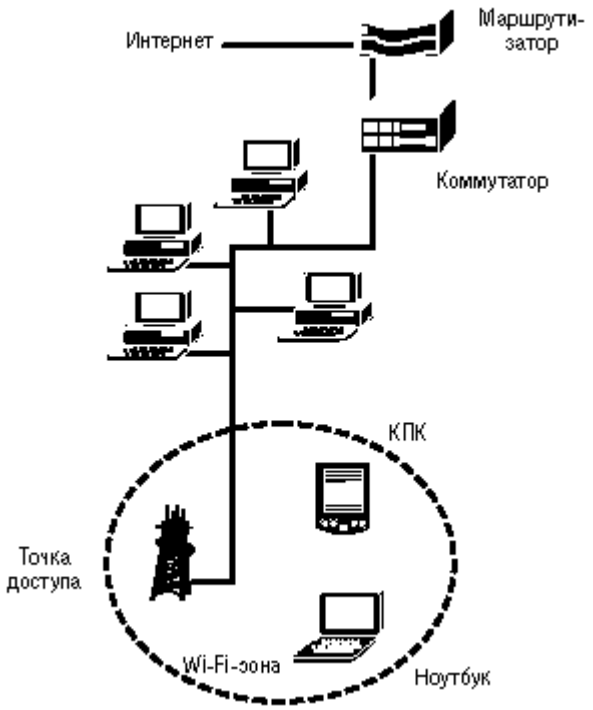


Рисунок 1.2- Схема беспроводной сети в офисе

Серьезные офисные WLAN корпоративного уровня строятся в тех компаниях, руководство которых понимает, для решения какого круга задач данная система предназначена. Оборудование, применяемое при создании

таких систем, имеет богатый функционал и позволяет реализовать большое количество сервисов. Практически всегда офисная WLAN строится как беспроводной сегмент проводной офисной сети с реализаций системы защиты информации от несанкционированного доступа.

Офисные WLAN (рисунок 1.3) корпоративного уровня позволяют обеспечить:

– авторизацию и аутентификацию пользователей;

– создание нескольких беспроводных VPN-сетей с различными типами сервисов;

– доступ сотрудников к корпоративной информации по защищенным беспроводным каналам;

– свободный доступ сотрудников к Интернет-ресурсам;

– свободный или платный доступ гостей компании к Интернет-ресурсам;

– мобильную телефонную связь на территории офиса (аналог DECT-телефонии);

– видеонаблюдение на базе беспроводных (мобильных) видеокамер с архивированием видеоинформации в цифровом виде на корпоративных серверах;

– получение информации о местоположении мобильного сотрудника.

Офисных WLAN такого уровня насчитываются единицы. Обычно их строительство ведут крупные корпоративные заказчики, владеющие большими офисными площадями.

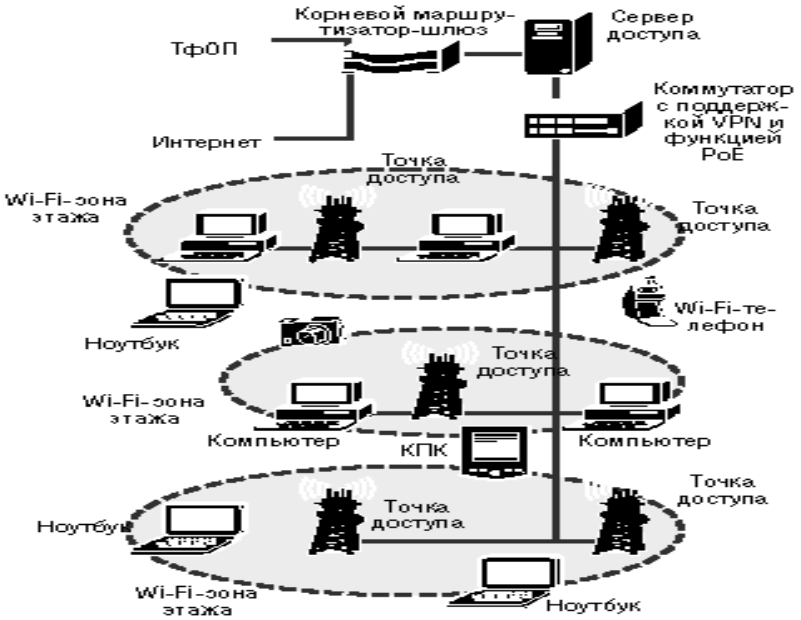


Рисунок 1.3- Схема реальной корпоративной WLAN в многоэтажном здании

Следует отметить, что большие офисные площади-это многоэтажные бизнес-центры класса А и В или целая группа зданий. Часто суммарная площадь

офисных и вспомогательных помещений исчисляется десятками тысяч квадратных метров.

Корпоративная WLAN позволяет:

– создать требуемое количество виртуальных сетей (VLAN) для различных служб заказчика и сервисов в сети;

– назначить определенные права доступа для каждой VLAN;

– назначить определенные квоты каждому пользователю корпоративной WLAN (службе, сотруднику, гостю);

– получить скорость передачи данных на каждого пользователя до 20 Мбит/с;

– включить QoS для VoIP, видеоконференций и видеонаблюдения.

Теперь нужно перечислить, какое же оборудование беспроводного доступа требуется для проекта такого рода.

Точки доступа с поддержкой стандартов IEEE 802.11b/g, диапазон рабочих частот 2,4-2,483 ГГц. Сеть точек доступа формирует Wi-Fi зону во всем здании заказчика. Каждая точка поддерживает несколько VLAN, а каждая VLAN, в свою очередь, обслуживает определенный корпоративный сервис (VLAN администратора, VLAN гостя, VLAN телефонии (VoIP), VLAN- систему безопасности и т. п.). Точки доступа питаются от коммутатора с поддержкой функции PoE (Power over Ethernet).

Оборудование клиентов любого производителя с поддержкой стандартов IEEE 802.11b/g (мобильный, карманный и планшетный ПК, VoIP-телефон, SmartPhone с поддержкой Wi-Fi, Wi-Fi видеокамеры).

Зона публичного беспроводного доступа в Интернет называется хотспотом (HotSpot). Она включает внешний канал доступа в Интернет, систему биллинга и оборудование, формирующее зону покрытия (WLAN). Хотспот предоставляет доступ в Интернет всем желающим при условии, что у них есть мобильные устройства с поддержкой стандарта Wi-Fi.

На рисунке 1.4 представлена принципиальная схема хотспота. В зоне общедоступного беспроводного доступа можно получить доступ в Интернет и к корпоративной информации, а также услугу телефонной VoIP-связи.

Для создания хотспота необходимы:

– внешний канал доступа в Интернет. Подключение ресторана к мультисервисной сети провайдера может быть проводным или беспроводным, создаваемым с помощью радиомаршрутизатора;

– точка доступа с поддержкой стандартов 802.11b/g. Такая точка формирует Wi-Fi-зону, например, в помещении ресторана;

– стандартное абонентское оборудование 802.11b/g.

Современный подход к построению телекоммуникационных систем для крупных и средних компаний с развитой сетью филиалов предполагает создание территориально распределенных корпоративных сетей связи. Радиотехнологии для решения таких задач применяются уже давно. Быстрота развертывания, низкие затраты на строительство и эксплуатацию вызывают

повышенный интерес корпоративного заказчика к радиосетям. Но из-за недостаточной функциональности оборудования этот рынок был довольно узким.

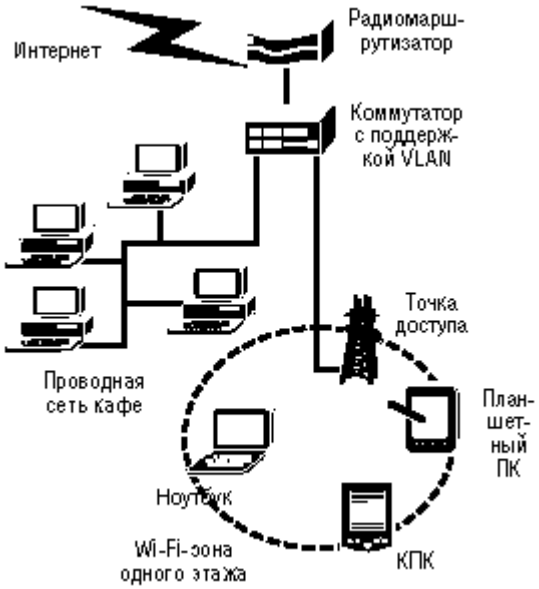


Рисунок 1.4- Схема беспроводной сети в кафе

С появлением нового оборудования и открытием новых частотных диапазонов для использования ситуация изменилась. Корпоративная радиосеть (рисунок 1.5), объединяющая филиальную структуру предприятия, обеспечивает:

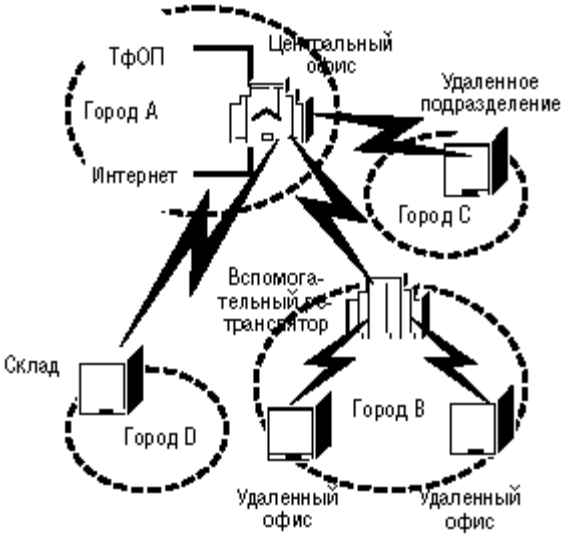


Рисунок 1.5- Схема корпоративной сети передачи данных масштаба области

– передачу мультимедийных потоков данных;

– скорости до 100 Мбит/с;
– маршрутизацию и приоритезацию различных видов трафика;
– интеграцию в рамках единой транспортной инфраструктуры различных типов сетей, таких, как мультимедийная сеть передачи данных, телефонная сеть, системы видеонаблюдения, сбора телеметрической информации и противопожарной безопасности;
– защиту от несанкционированного доступа;
– масштабируемость;
– высокую надежность.

Эти особенности беспроводных сетей ставят их в один ряд с оптоволоконными сетями, и тут уже сети на основе медных проводов не выдерживают конкуренции. Стоимость же и сроки реализации оптоволоконных сетей зачастую таковы, что заказчики даже не рассматривают их как вариант построения сетевой инфраструктуры.

Корпоративная сеть имеет структуру графа. Чтобы получить максимальную скорость обмена данными между центральным офисом и каждой удаленной точкой корпоративной сети, при проектировании обычно граф пытаются привести к схеме «звезда». При такой схеме каналообразующим оборудованием являются радиомаршрутизаторы RWR-5000, диапазон рабочих частот составляет 5,15-5,25 или 5,25-5,35 ГГц, скорости передачи- до 54 Мбит/с, дальность действия одного пролета- до 30 км.

Следует отметить, что топологическая организация сетей может быть и другой. Например, очень крупные сети масштаба области (рисунок 1.6) требуют построения транспортной инфраструктуры высокой пропускной способности, которая должна стать основным связующим звеном районных беспроводных сетей.

В качестве транспортной инфраструктуры используются радиорелейные каналы, замкнутые в SDH-кольцо (скорости передачи- до 155 Мбит/с). Одновременно точки SDH-кольца являются центром коммутации районных широкополосных беспроводных сетей, построенных на базе оборудования широкополосного доступа.

Цель каждого провайдера телекоммуникационных услуг- прийти туда, где находится потребитель его услуг. Для этого нужна разветвленная инфраструктура. Решение данной задачи упрощают беспроводные сети фиксированного доступа. Не повышая стоимости услуг, они позволяют доставить их непосредственно потребителю, обеспечив при этом качество, гарантированность, быстроту подключения и разнообразие ассортимента.

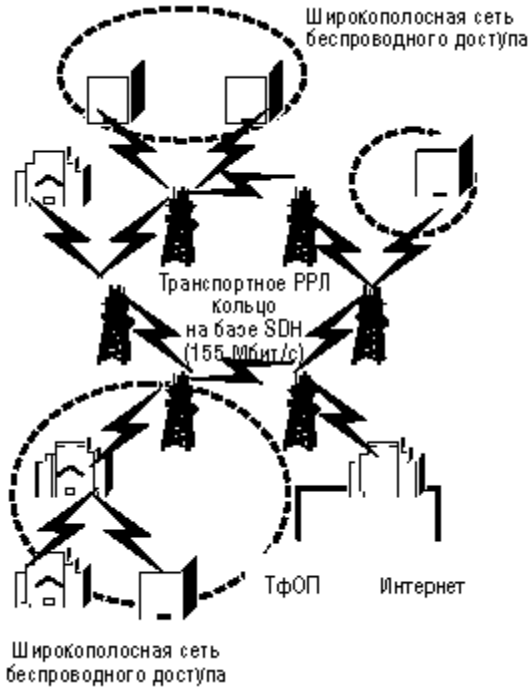


Рисунок 1.6- Схема распределенной сети, объединяющей подразделения компании на большой территории

С появлением нового радиооборудования операторского класса и разработкой правильной технической и финансовой политики по отношению к потребителю радиосети фиксированного доступа начинают успешно конкурировать с проводными и оптоволоконными сетями.

Еще два-три года назад беспроводной фиксированный доступ производился в диапазоне 2,4 ГГц. При этом безлицензионное использование эфира обуславливало полный произвол, о каких-либо гарантиях и качестве услуг не могло быть и речи.

Сегодня, для того чтобы выйти на конечного потребителя, оператору сети беспроводного фиксированного доступа не нужно строить физический канал, достаточно просто установить у пользователя «ответную» часть каналообразующего оборудования.

Современная беспроводная широкополосная городская сеть предоставляет абонентам целый спектр телекоммуникационных услуг:

– каналы от 64 кбит/с до 10 Мбит/с с гарантированной пропускной способностью, поддержку QoS;

– доступ в Интернет;

– организацию корпоративных территориально распределенных сетей для любого количества точек;

– услуги пакетной VoIP-телефонии;

– создание резервных и дублирующих каналов передачи данных на базе беспроводной технологии;

– круглосуточную поддержку.

Схемы подключения абонентов зависят от заказанного набора услуг. Основные из них- доступ в Интернет и VoIP. Трансляция голоса по IP каналу требует обеспечения качества (QoS). Передача данных и голосового трафика осуществляется в одном физическом канале, но благодаря QoS голосовой трафик имеет приоритет. К каналу могут быть подключены как IP, так и аналоговые телефоны (или АТС) через IP шлюз.

Количество одновременно работающих телефонных линий зависит от общей пропускной способности канала. Обычно их бывает до двенадцати. Большее число линий (20-30) требует установки специализированных IP шлюзов, поддерживающих TDVoIP.

Для корпоративных потребителей с развитой структурой филиалов наибольший интерес представляют распределенные корпоративные сети, построенные на базе беспроводных сетей фиксированного доступа операторов. На рисунке 1.7 приведена упрощенная схема.

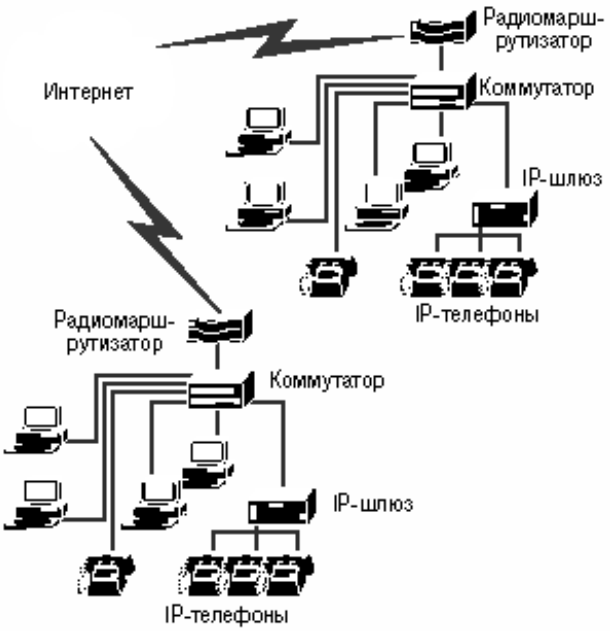


Рисунок 1.7- Корпоративная сеть с развитой филиальной структурой и общим номерным планом

Следует отметить, что беспроводная сеть может поддерживать любое количество удаленных подразделений компании. Кроме того, в рамках самой сети вполне допустимо комбинирование технических решений, применяемых в разных сегментах рынка. Примером может служить построение Wi-Fi на территории одного или нескольких удаленных подразделений компании для использования ее сотрудниками и гостями.

Не все существующие в настоящее время беспроводные технологии действительно мобильны. Например, довольно дешевую спутниковую связь, которая по карману даже частным лицам, мобильной не назовешь- не брать же с собой всюду немаленькую параболическую антенну.

Возможности GSM-сетей ограничены пропускной способностью. GPRS (General Packet Radio Service)с ее пиковыми скоростями в 53,6 кбит/с для приема и 26,8 кбит/с для передачи на практике оказывается довольно капризной, а сеть 3G весьма неспешно движется к потребителю и зачастую тоже неприемлема для передачи больших объемов информации. Крупнейший в Корее оператор мобильной связи SK Telekom предоставляет доступ к сетям 3G, работающим на скорости всего 256 кбит/с.

GPRS (пакетная радиосвязь общего назначения)- это стандарт беспроводной высокоскоростной связи, позволяющий обмениваться пакетными данными, например, электронной почтой или информационным наполнением web-сайтов, по беспроводным телефонным сетям и Интернету. Технологию GPRS часто называют технологией поколения 2,5 (2,5G) (по аналогии с технологией беспроводной связи первого поколения (1G), применявшейся для связи аналоговых сотовых телефонов, а также технологией беспроводной связи второго поколения (2G), которая применяется в цифровых мобильных телефонах). Поддержка технологии GPRS реализована не только в мобильных телефонах: мобильные ПК также могут быть оборудованы адаптером GPRS, обеспечивающим подключение к Интернету.

Bluetooth- технология коротковолновой радиосвязи (2,4 ГГц), действующая на достаточно близком расстоянии (зачастую работает в пределах одной комнаты и не позволяет передавать данные на большие расстояния: подавляющее большинство Bluetooth-устройств ограничено радиусом действия 10-30 м) и упрощающая взаимодействие сетевых устройств друг с другом, а также доступ посредством сетевых устройств в Интернет. Эта технология упрощает синхронизацию данных между сетевыми устройствами и другими компьютерами.

Поскольку технология Bluetooth не предназначена для передачи больших объемов данных, она не подходит в качестве замены локальных или глобальных сетей.

1.5 Построение сети на базе стандарта IEEE 802.11

Комитет по стандартам IEEE 802 сформировал рабочую группу для беспроводных локальных сетей 802.11 в 1990 году. Спецификация физического уровня этого стандарта IEEE 802.11 выпускалась в четыре этапа: первая часть увидела свет в 1997 году, две в 1999, последняя в 2003.

Первая часть, именуемая просто IEEE 802.11 включала описание уровня MAC (Medium Access Control) и три спецификации физического уровня- две в диапазоне 2,4 ГГц и одну в инфракрасном диапазоне, работающие при скоростях 1 и 2 Мбит/с. Остальные три спецификации: IEEE 802.11a, IEEE 802.b и IEEE 802.g используются в настоящее время обеспечивая более высокие скорости доступа.

Как и все стандарты IEEE 802, 802.11 работают на нижних двух уровнях модели ISO/OSI- физическом и канальном уровнях (рисунок 1.8). Любое

сетевое приложение, сетевая операционная система, или протокол (например, TCP/IP), будут так же хорошо работать в сети 802.11, как и в сети Ethernet.

Аббревиатура Wi-Fi (Wireless Fidelity) также широко используется для обозначения беспроводных локальных сетей, оборудование которых соответствует стандартам группы IEEE 802.11 и прошло сертификацию на совместимость в специально созданной для этой цели организации Wi-Fi Alliance (прежнее название- WECA).

Физический уровень. На физическом уровне определены два широкополосных радиочастотных метода передачи, а также метод ортогонального частотного уплотнения. Технологии широкополосного сигнала, используемые в радиочастотных методах, увеличивают надёжность, пропускную способность, позволяют многим несвязанным друг с другом устройствам разделять одну полосу частот с минимальными помехами друг для друга.

Рисунок 1.8 - Уровни модели ISO/OSI и их соответствие стандарту 802.11

В настоящее время используются методы прямой последовательности (Direct Sequence Spread Spectrum, DSSS) и ортогонального частотного уплотнения (Orthogonal Frequency Division Multiplexing). Метод частотных скачков (Frequency Hopping Spread Spectrum, FHSS) не применяется, как устаревший. Эти методы кардинально отличаются и несовместимы друг с другом [21].

В системе DSSS может использоваться до семи каналов со скоростью передачи в каждом 1 или 2 Мбит/с. Количество доступных каналов зависит от ширины полосы, выделяемой государственным органом регулирования. В Европе, например, доступно до 13 каналов, а в Японии- только один. Ширина

полосы каждого канала равна 5 МГц, схема кодирования: DBPSK для скорости 1 Мбит/с и DQPSK- для скорости 2 Мбит/с. Ключевые элементы данного метода перечислены в таблице 1.3.

Таблица 1.3- Расширение спектра методом прямой последовательности

Скорость передачи данных, Мбит/с	Длина раздробленного кода, символов	Вид модуляции	Скорость передачи, симв/с	Информационная скорость, бит/символ
1	11 (последовательность Баркера)	DBPSK	10^6	1
2	11 (последовательность Баркера)	DQPSK	10^6	2
5,5	8 (ССК)	DBPSK	$1{,}375 \cdot 10^6$	4
11	8 (ССК)	DQPSK	$1{,}375 \cdot 10^6$	8

Система DSSS использует раздробленный код, или псевдошумовую последовательность, для расширения скорости передачи данных, а следовательно, полосы сигнала. В стандарте IEEE 802.11 определено использование последовательности Баркера.

Последовательность Баркера (Barker sequence)- это последовательность $\{s(t)\}$ элементов +1 и -1. Длина последовательности равна n, а для автокорреляционного значения $R(\tau)$ справедливо следующее: $|R(\tau)| < 1$ для всех $|\tau| \leq (n - 1)$.

В настоящее время известны следующие последовательности Баркера (таблица 1.4).

Таблица 1.4- Последовательности Баркера

Длина последовательности, символов	Вид последовательности
2	+ +
3	+ + –
4	+ + + –
5	+ + + – +
7	+ + + – – + –
11	+ – + + – + + + – – –
13	+ + + + + – – + + – + – +

В 802.11 используется последовательность Баркера с n=11. Таким образом, каждая двоичная единица отображается в последовательность {+ – + + – + + + – – –}, а каждый двоичный нуль- в последовательность {– + – – + – – – + + +}.

Важной особенностью последовательностей Баркера является их устойчивость к интерференции и эффектам многолучевого распространения [4].

В ортогональной схеме FDM (OFDM), именуемой также модуляцией с множественными несущими, используется несколько несущих сигналов с разными частотами, посредством каждого из которых отправляется некоторое количество битов.

Одним из преимуществ использования большего числа каналов в OFDM-системах является увеличение концентрации спектра и энергетики сигнала внутри полосы пропускания системы, что уменьшает помехи между соседними сотами и частотными каналами и увеличивает общую устойчивость системы передачи к шумам.

Кроме того, при увеличении числа каналов, как следствие большей длительности модулирующих импульсов (при равных скоростях передачи данных), растет и устойчивость к многолучевому распространению сигналов. Многолучевое распространение приводит к искажению фронтов импульсов. Чем меньше длительность искаженного участка сигнала- тем выше вероятность его правильной демодуляции.

Одним из следствий многолучевого распространения является интерференция сигналов в точке приема. В зависимости от задержки и частоты сигнала лучи, пришедшие с разных направлений, могут складываться как в фазе, так и в противофазе, что приводит к увеличению или существенному падению мощности сигнала на разных частотах.

Ключевые элементы данного метода перечислены в таблице 1.5.

Таблица 1.5- Ортогональное уплотнение с частотным разделением

Скорость передачи данных	Вид модуляции	Степень кодирования	Число кодированных битов на поднесущую	Число битов кода на символ OFDM	Число битов данных на символ OFDM
6 Мбит/с	BPSK	1/2	1	48	24
9 Мбит/с	BPSK	3/4	1	48	36
12 Мбит/с	QPSK	1/2	2	6	48
18 Мбит/с	QPSK	3/4	2	96	72
24 Мбит/с	16-QAM	1/2	4	192	96
36 Мбит/с	16-QAM	3/4	4	192	144
49 Мбит/с	64-QAM	2/3	6	288	192
54 Мбит/с	16-QAM	3/4	6	288	216

Для подавления этого эффекта в системах с одной несущей частотой и корреляционных широкополосных системах (DSSS) используются адаптивные эквалайзеры, выравнивающие мощность сигнала во всей полосе рабочих частот. Понятно, что использование таких эквалайзеров приводит к ухудшению отношения сигнал/шум и значительному увеличению сложности системы. Использование OFDM позволяет с минимальными затратами

отбрасывать каналы с неприемлемым соотношением сигнал/шум. Соответственно, увеличение числа каналов приводит к общему увеличению эффективности системы.

Кроме того, с увеличением числа каналов часть из них может быть использована для передачи служебной информации и мониторинга каналов без сколько-нибудь значительной потери скорости передачи данных [22].

В настоящее время существуют три отраслевых стандарта для беспроводной передачи данных, определенных институтом инженеров электротехники и электроники (IEEE).

IEEE 802.11b- это расширение спецификации IEEE 802.11 DSSS, допускающее скорости передачи данных 5,5 и 11 Мбит/с. Скорость передачи раздробленного сигнала равна 11 МГц, т.е. такая же, как в исходной схеме DSSS, следовательно, обе схемы требуют одинаковой полосы. Для получения более высокой скорости при неизменной полосе и скорости передачи раздробленного сигнала используется манипуляция дополнительным кодом (complementary code keying- ССК).

Модуляция ССК является достаточно сложной. Пример схемы ССК приводится на рисунке 1.9 для скорости передачи 11 Мбит/с. Входные данные рассматриваются как восьмибитовые блоки со скоростью 1,375 МГц (8 бит/символ х 1,375 МГц =11 Мбит/с). Шесть битов отображаются в одну из 64 кодовых последовательностей, при этом применяется матрица Уолша 8х8 . Результат, плюс оставшиеся два бита подаются на вход модулятора QPSK (quadrature phase-shift keying- квадратурная фазовая манипуляция).

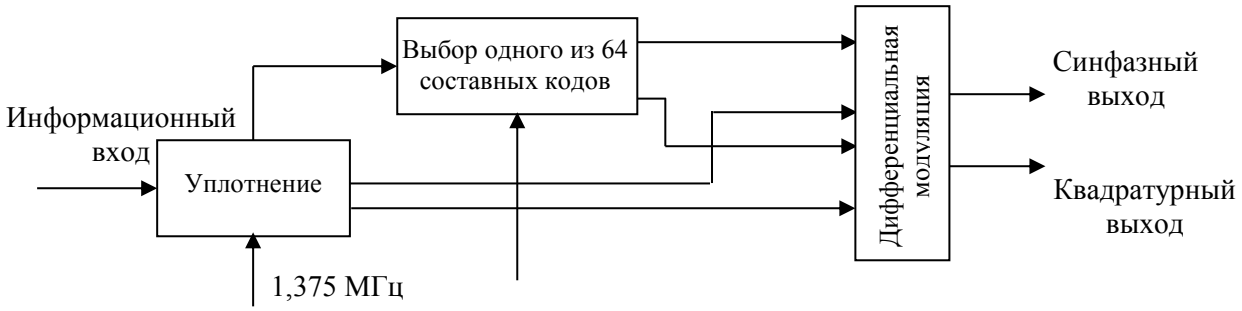


Рисунок 1.9- Схема модуляции ССК для скорости 11 Мбит/с

Для поддержки очень зашумлённых сред, а также работы на больших расстояниях, сети 802.11b используют динамический сдвиг скорости, который позволяет автоматически изменять скорость передачи данных в зависимости от свойств радиоканала. Например, пользователь может подключиться с максимальной скоростью 11 Мбит/с, но в том случае, если повысится уровень помех, или пользователь удалится на большое расстояние, мобильное устройство начнёт передавать на меньшей скорости- 5,5, 2 или 1 Мбит/с. В том случае, если возможна устойчивая работа на более высокой скорости, мобильное устройство автоматически начнёт передавать с более высокой скоростью.

Сдвиг скорости- механизм физического уровня, и является прозрачным для вышестоящих уровней и пользователя.

Спецификация IEEE 802.11a использует полосу 5 ГГц. В отличие от спецификации 2,4 ГГц, здесь применяется не расширенный спектр, а ортогональное частотное уплотнение (OFDM). Имеется до 52 поднесущих, которые модулируются с использованием схем BPSK, QPSK, 16-QAM или 64-QAM, в зависимости от требуемой скорости передачи. Расстояние между поднесущими составляет 0,3125 МГц. В результате повышается пропускная способность канала и качество сигнала.

К недостаткам 802.11a относятся более высокая потребляемая мощность радиопередатчиков для частот 5 ГГц, а так же меньший радиус действия (оборудование для 2,4 ГГц может работать на расстоянии до 300 м, а для 5 ГГц- около 100 м).

Стандарт IEEE 802.11g разработан для более высоких значений пропускной способности беспроводных соединений в 54 Мбит/с. Работая на той же частоте что и 802.11b (2,4 ГГц) он обеспечивает таким образом обратную совместимость обоих стандартов. Используется метод прямой последовательности с разнесением сигнала по широкому диапазону (DSSS) и метод мультиплексирования с ортогональным делением частот (OFDM).

Скорость передачи в 54 Мбит/с достигается в открытой офисной среде на расстоянии до 14 м. При наличии какого-либо препятствия (к примеру, перегородки), которое должно быть преодолено, скорость снижается. Чувствительность при 11 Мбит/с (в случае модуляции CCK/802.11b) и чувствительность при 12 Мбит/с (в случае модуляции OFDM/802.11g), как правило, совпадают, поэтому такая скорость передачи может поддерживаться на расстоянии до 40 м от точки доступа (рисунок 1.10).

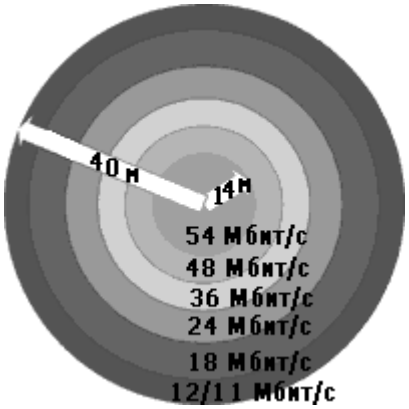


Рисунок 1.10 - Радиус действия в офисной среде

Особенности и преимущества стандарта 802.11g:

- скорость передачи данных- до 54 Мбит/с;
- повышенный уровень безопасности;
- совместимость с более ранними стандартами;

– увеличенная дальность передачи данных.

Результаты сравнения стандартов 802.11 a,b и g сведены в таблицу 1.6.

Таблица 1.6- Результаты сравнения стандартов 802.11 a,b и g

Параметры стандарта	Значения параметров		
	802.11b	802.11a	802.11g
Дата принятия стандарта	сентябрь 1999 г.	сентябрь 1999 г.	июль 2003 г.
Полоса пропускания, МГц	83,5	300	83,5
Полоса частот, ГГц	2,40 – 2,4835	5,15-5,35 5,725-5,825	2,40-2,4835
Количество непересекающихся каналов	3	8	3
Скорость передачи, Мбит/с	1; 2; 5,5; 11; 22	6; 9; 12; 18; 24; 36; 48, 54	1, 2, 5.5, 11, 22, 6, 9, 12, 18, 24, 36, 48, 54
Вид модуляции	DSSS	OFDM	DSSS, OFDM

Канальный уровень (Data Link). Канальный уровень 802.11 состоит из двух подуровней: управления логической связью (Logical Link Control, LLC) и управления доступом к носителю (Media Access Control, MAC). 802.11 использует тот же LLC и 48-битовую адресацию, что и другие сети 802, что позволяет легко объединять беспроводные и проводные сети, однако MAC уровень имеет кардинальные отличия.

MAC уровень 802.11 очень похож на реализованный в 802.3, где он поддерживает множество пользователей на общем носителе, когда пользователь проверяет носитель перед доступом к нему. Для Ethernet сетей 802.3 используется протокол Carrier Sence Multiple Access with Collision Detection (CSMA/CD), который определяет, как станции Ethernet получают доступ к проводной линии, и как они обнаруживают и обрабатывают коллизии, возникающие в том случае, если несколько устройств пытаются одновременно установить связь по сети. Чтобы обнаружить коллизию, станция должна обладать способностью и принимать, и передавать одновременно.

Стандарт 802.11 предусматривает использование полудуплексных приёмопередатчиков, поэтому в беспроводных сетях станция не может обнаружить коллизию во время передачи [21].

Чтобы учесть это отличие, 802.11 использует модифицированный протокол, известный как Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), или Distributed Coordination Function (DCF). CSMA/CA пытается избежать коллизий путём использования явного подтверждения пакета (ACK),

что означает, что принимающая станция посылает ACK пакет для подтверждения того, что пакет получен неповреждённым.

CSMA/CA работает следующим образом. Станция, желающая передавать, тестирует канал, и если не обнаружено активности, станция ожидает в течение некоторого случайного промежутка времени, а затем передаёт, если среда передачи данных всё ещё свободна. Если пакет приходит целым, принимающая станция посылает пакет ACK, по приёму которого отправителем завершается процесс передачи. Если передающая станция не получила пакет ACK, в силу того, что не был получен пакет данных, или пришёл повреждённый ACK, делается предположение, что произошла коллизия, и пакет данных передаётся снова через случайный промежуток времени [21].

Для определения того, является ли канал свободным, используется алгоритм оценки чистоты канала (Channel Clearance Algorithm, CCA). Его суть заключается в измерении энергии сигнала на антенне и определения мощности принятого сигнала (RSSI). Если мощность принятого сигнала ниже определённого порога, то канал объявляется свободным, и MAC уровень получает статус CTS. Если мощность выше порогового значения, передача данных задерживается в соответствии с правилами протокола.

Стандарт предоставляет ещё одну возможность определения не занятости канала, которая может использоваться либо отдельно, либо вместе с измерением RSSI- метод проверки несущей. Этот метод является выборочным, так как с его помощью производится проверка на тот же тип несущей, что и по спецификации 802.11. Наилучший метод для использования зависит от того, каков уровень помех в рабочей области.

Таким образом, CSMA/CA предоставляет способ разделения доступа по радиоканалу. Механизм явного подтверждения эффективно решает проблемы помех. Однако он добавляет некоторые дополнительные накладные расходы, которых нет в 802.3, поэтому сети 802.11 будут всегда работать медленнее, чем эквивалентные им Ethernet локальные сети.

Другая специфичная проблема MAC уровня- это проблема «скрытой точки», когда две станции могут обе «слышать» точку доступа, но не могут «слышать» друг друга, в силу большого расстояния или преград (рисунок 1.11). Для решения этой проблемы в 802.11 на MAC уровне добавлен необязательный протокол Request to Send/Clear to Send (RTS/CTS). Когда используется этот протокол, посылающая станция передаёт RTS и ждёт ответа точки доступа с CTS.

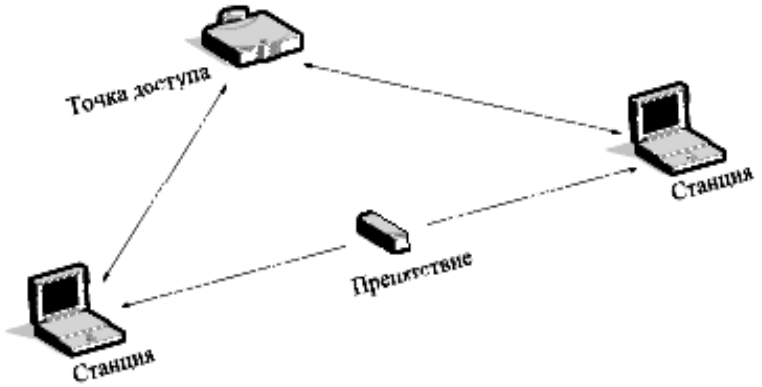


Рисунок 1.11- Иллюстрация проблемы «скрытой точки»

Так как все станции в сети могут «слышать» точку доступа, сигнал CTS заставляет их отложить свои передачи, что позволяет передающей станции передать данные и получить ACK пакет без возможности коллизий. Так как RTS/CTS добавляет дополнительные накладные расходы на сеть, временно резервируя носитель, он обычно используется только для пакетов очень большого объёма, для которых повторная передача была бы слишком дорогостоящей.

Наконец, MAC уровень 802.11 предоставляет возможность расчёта CRC и фрагментации пакетов. Каждый пакет имеет свою контрольную сумму CRC, которая рассчитывается и прикрепляется к пакету. Здесь наблюдается отличие от сетей Ethernet, в которых обработкой ошибок занимаются протоколы более высокого уровня (например, TCP). Фрагментация пакетов позволяет разбивать большие пакеты на более маленькие при передаче по радиоканалу, что полезно в очень «заселённых» средах или в тех случаях, когда существуют значительные помехи, так как у меньших пакетов меньше шансы быть повреждёнными. Этот метод в большинстве случаев уменьшает необходимость повторной передачи и, таким образом, увеличивает производительность всей беспроводной сети. MAC уровень ответственен за сборку полученных фрагментов, делая этот процесс «прозрачным» для протоколов более высокого уровня.

Стандарт 802.11 определяет два типа оборудования- клиент, который представляет собой PCI карточку для настольных компьютеров, PCMCIA карту для ноутбуков или интегрируется в современные КПК, и точку доступа (Access point, AP), которая выполняет роль моста между беспроводной и проводной сетями. Точка доступа обычно содержит в себе приёмопередатчик, интерфейс проводной сети (802.3), а также программное обеспечение, занимающееся обработкой данных.

Этот стандарт также определяет два режима работы сети- режим «Ad-hoc» и клиент/сервер (или режим инфраструктуры- infrastructure mode).

В режиме клиент/сервер (рисунок 1.12) беспроводная сеть состоит как минимум из одной точки доступа, подключенной к проводной сети, и некоторого набора беспроводных оконечных станций.

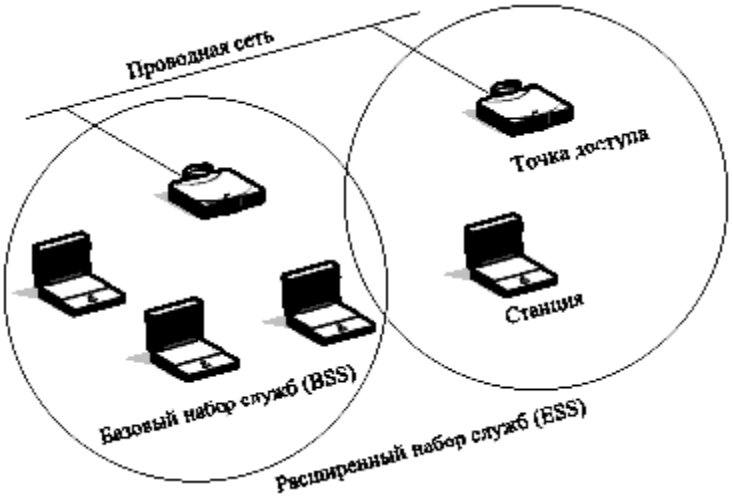


Рисунок 1.12- Архитектура сети «клиент/сервер»

Такая конфигурация носит название базового набора служб (Basic Service Set, BSS). Два или более BSS, образующих единую подсеть, формируют расширенный набор служб (Extended Service Set, ESS). Так как большинству беспроводных станций требуется получать доступ к файловым серверам, принтерам, Интернет, доступным в проводной локальной сети, они будут работать в режиме клиент/сервер.

Режим «Ad-hoc» (также называемый точка-точка, или независимый базовый набор служб, IBSS)- это простая сеть, в которой связь между многочисленными станциями устанавливается напрямую, без использования специальной точки доступа (рисунок 1.13).

Рисунок 1.13- Архитектура сети «Ad-hoc»

Такой режим полезен в том случае, если инфраструктура беспроводной сети не сформирована. Например, сотрудники компании, оснащённые

беспроводными ноутбуками, будут иметь возможность обмениваться необходимой информацией, находящейся на их компьютерах, с коллегами при встрече в любом месте, где по каким-то причинам отсутствует беспроводная точка доступа (в кабинете, приемной или даже в кафетерии и т.д.)

MAC уровень 802.11 несёт ответственность за то, каким образом клиент подключается к точке доступа. Когда клиент 802.11 попадает в зону действия одной или нескольких точек доступа, он на основе мощности сигнала и наблюдаемого значения количества ошибок выбирает одну из них и подключается к ней. Как только клиент получает подтверждение того, что, он принят точкой доступа, он настраивается на радиоканал, в котором она работает. Время от времени он проверяет все каналы 802.11, чтобы посмотреть, не предоставляет ли другая точка доступа службы более высокого качества. Если такая точка доступа находится, то станция подключается к ней, перенастраиваясь на её частоту (рисунок 1.14).

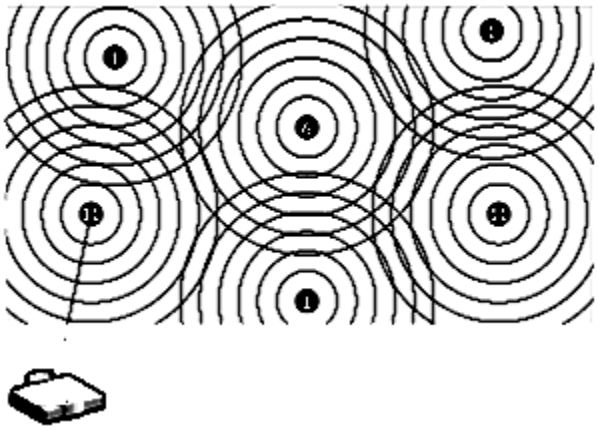


Рисунок 1.14- Подключение к сети и иллюстрация правильного назначения каналов

Переподключение обычно происходит в том случае, если станция была физически перемещена вдаль от точки доступа, что вызвало ослабление сигнала. В других случаях повторное подключение происходит из-за изменения радиочастотных характеристик здания, или просто из-за большого сетевого трафика через первоначальную точку доступа. В последнем случае эта функция протокола известна как «балансировка нагрузки», так как её главное назначение- распределение общей нагрузки на беспроводную сеть наиболее эффективно по всей доступной инфраструктуре сети.

Процесс динамического подключения и переподключения позволяет сетевым администраторам устанавливать беспроводные сети с очень широким покрытием, создавая частично перекрывающиеся «соты».

Таким образом проектируемую беспроводную сеть в дальнейшем можно будет без проблем расширить причём, идеальным вариантом является такой, при котором соседние перекрывающиеся точки доступа будут использовать

разные DSSS каналы, чтобы не создавать помех в работе друг другу (рисунок 1.14).

Потоковые данные, такие как видео или голос, поддерживаются в спецификации 802.11 на MAC уровне посредством Point Coordination Function (PCF). В противоположность Distributed Coordination Function (DCF), где управление распределено между всеми станциями, в режиме PCF только точка доступа управляет доступом к каналу.

В том случае, если установлен BSS с включенной PCF, время равномерно распределяется промежутками для работы в режиме PCF и в режиме CSMA/CA. Во время периодов, когда система находится в режиме PCF, точка доступа опрашивает все станции на предмет получения данных. На каждую станцию выделяется фиксированный промежуток времени, по истечении которого производится опрос следующей станции. Ни одна из станций не может передавать в это время, за исключением той, которая опрашивается. Так как PCF даёт возможность каждой станции передавать в определённое время, то гарантируется максимальная латентность.

Недостатком такой схемы является то, что точка доступа должна производить опрос всех станций, что становится чрезвычайно неэффективным в больших сетях [23].**1.6 Задание на проектирование**

Рассмотренные выше вопросы необходимости организации сети передачи данных между гостиничными комплексами г. Алматы, анализ и характеристика возможных и более перспективных способов ее организации можно сформулировать в задании на проектирование в следующем виде.

В дипломном проекте необходимо рассмотреть вопрос организации сети передачи данных между бизнес-центрами гостиничных комплексов города Алматы: Казахстан, Анкара, Отрар, Алма-Ата, Жетысу, Алатау, Астана, Достык, Амбассадор.

Организацию сети провести с использованием радиодоступа. Использовать технологию беспроводного Ethernet, оборудование Revolution 5000. На базе этого оборудования обеспечить быструю организацию качественной сети передачи данных. Предусмотреть возможность быстрого дальнейшего расширения сети, в зависимости от поступления заказов от других гостиничных комплексов на подключение к этой сети.

В проекте необходимо:

- в разделе характеристики оборудования дать подробное техническое описание выбранного оборудования;

– в разделе проектирования сети провести исследование развертываемой беспроводной сети и рассмотреть вопрос тестирование оборудования, разработать схему подключения бизнес центров гостиниц к сети.

– в разделе технического расчета провести расчеты энергетических параметров проектируемой сети;

2 Техническая характеристика выбранного оборудования

2.1 Радиомаршрутизаторы

Предлагается для проектируемой сети выбрать оборудование компании CompTek- второе поколение высокоскоростных радиомаршрутизаторов Revolu-tion 5000- серию 5000 mini.

Основа серии- новая аппаратная платформа, основанная на мощном процессоре IBM PowerPC с тактовой частотой 200-400 МГц.

Revolution 5000 mini работает в новом частотном диапазоне 5,25-5,35 ГГц Это дает возможность операторам развивать существующие беспроводные сети, а также строить новые, предоставлять своим абонентам более скоростные каналы, новые сервисы, организовывать высокопроизводительные магистральные линии между базовым станциями.

Применение новых алгоритмов обработки радиосигнала позволило повысить пропускную способность радиомаршрутизаторов Revolution более, чем в 4 раза, по сравнению с предыдущими моделями. В настоящий момент максимальная скорость в радиоканале составляет 54 Мбит/с. Таким образом, максимальная производительность шестисекторной базовой станции может достигать 54x6=324 Мбит/с.

Все функциональные возможности серий 2000 и 3000 получили свое продолжение и развитие в новой линейке радиомаршрутизаторов Revolution 5000. Применение более производительной аппаратной платформы позволяет операторам предоставлять новые сервисы абонентам- передачу трафика IP-телефонии, видеоконференций, а также быть уверенными в сохранности инвестиций, сделанных в построение беспроводной сети.

Радиомаршрутизаторы Revolution 5000 mini выпускаются в нескольких модификациях, что дает возможность операторам значительно экономить на стоимости абонентских устройств. В качестве оборудования базовой станции можно использовать устройства с максимальной производительностью, тогда как абонентам предлагать более дешевые, менее производительные модели.

Радиомаршрутизатор Revolution 5000 mini может применяться в качестве любого элемента сети- базовой станции, ретранслятора, абонента. На радиомаршрутизаторах можно строить надежные беспроводные сети произвольной конфигурации. Например, при выборе архитектуры MINT каждая абонентская станция может служить точкой ретрансляции для следующего абонента, что дает уникальную гибкость в построении и развитии сети, а также позволяет серьезно сэкономить на количестве базовых станций.

Радиомаршрутизаторы Revolution 5000 mini имеют всепогодное исполнение, уверенно работающее в условиях сурового климата. Устройство состоит из двух блоков- внешнего (для использования на улице) и внутреннего (для использования внутри помещений). Внешний блок монтируется в непосредственной близости от антенны. Внутренний блок обеспечивает электропитание внешнего блока по кабелю и трансляцию сигналов Ethernet. Внешний и внутренний блоки оборудованы эффективной

защитой внешних линий питания и передачи данных, что значительно снижает вероятность поражения самого Revolution 5000 mini и устройств, подключенных к нему, во время грозы.

Для упрощения технического обслуживания устройства Revolution снабжаются встроенной системой диагностики, выполняющей, в частности, мониторинг радиоканала. Все данные по результатам диагностики посылаются на специальный сервер статистики, на котором работает программа (как правило, unix script), опознающая тревожную информацию. Обнаружив данные о возможной неисправности, программа генерирует системное сообщение, которое посылается на консоль оператора. Причины ухудшения или исчезновения связи могут быть самые разные: ветром развернуло антенну, трактор задел кабель, какая-то неисправность в самом устройстве и др. В подобных случаях посылаемая ремонтная бригада в течение суток (или быстрее) восстанавливает связь.

В Infinet уже разработано и готовится к выпуску управляющее ПО для Revolution, которое позволит получать статистику загрузки каналов, процессоров станций и т.д. в графическом виде. Но и системные сообщения, представляющие собой очень удобный механизм, конечно, тоже сохранятся [27].

Описание модельного ряда маршрутизаторов приведено в таблице 2.1.

Таблица 2.1- Описание модельного ряда маршрутизаторов

Модели	Характеристики
5000-O/5.3-18	Revolution 5000. 5,26-5,34 GHz, Radio 1x18Mbps, 10/100 Eth, Outdoor (-35°..+60°)
5000-O/5.3-24	Revolution 5000. 5,26-5,34 GHz, Radio 1x24Mbps, 10/100 Eth, Outdoor (-35°..+60°)
5000-O/5.3-36	Revolution 5000. 5,26-5,34 GHz, Radio 1x36Mbps, 10/100 Eth, Outdoor (-35°..+60°)
5000-O/5.3-54	Revolution 5000. 5,26-5,34 GHz, Radio 1x54Mbps, 10/100 Eth, Outdoor (-35°..+60°)
5000-O/5.3-18P200	Revolution 5000. 5,26-5,34 GHz, Radio 1x18Mbps, 10/100 Eth, Outdoor (-35°..+60°), up to 200 mW
5000-O/5.3-24P200	Revolution 5000. 5,26-5,34 GHz, Radio 1x24Mbps, 10/100 Eth, Outdoor (-35°..+60°), up to 200 mW
5000-OT/5.3-18	Revolution 5000. 5,26-5,34 GHz, Radio 1x18Mbps, 10/100 Eth, Outdoor (-50°..+60°)
5000-OT/5.3-24	Revolution 5000. 5,26-5,34 GHz, Radio 1x24Mbps, 10/100 Eth, Outdoor (-50°..+60°)
5000-OT/5.3-36	Revolution 5000. 5,26-5,34 GHz, Radio 1x36Mbps, 10/100 Eth, Outdoor (-50°..+60°)
5000-OT/5.3-54	Revolution 5000. 5,26-5,34 GHz, Radio 1x54Mbps, 10/100 Eth, Outdoor (-50°..+60°)
5000-OT/5.3-18P200	Revolution 5000. 5,26-5,34 GHz, Radio 1x18Mbps, 10/100 Eth, Outdoor (-50°..+60°), up to 200 mW
5000-OT/5.3-24P200	Revolution 5000. 5,26-5,34 GHz, Radio 1x24Mbps, 10/100 Eth, Outdoor (-50°..+60°), up to 200 mW

2.2 Антенны

Приемопередающая всенаправленная антенна Omni-5.3-10 типа «коллинеарная антенная решетка» (рисунок 2.1) используется для создания топологий радиосетей типа «точка-много точек». Всепогодное исполнение позволяет использовать эту антенну при температуре внешней среды от -40° до +50°. Служит для организации базовых станций малого и среднего радиуса действия. Имеет разъем N-типа (Female). Технические характеристики антенны Omni-5.3-10 приведены в таблице 2.2.

.

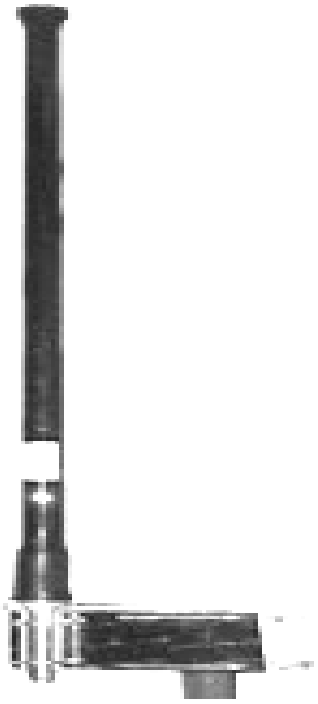


Рисунок 2.1- Вид всенаправленной антенны Omni-5.3-10

Таблица 2.2- Технические характеристики антенны Omni-5.3-10

Характеристики	Значения
1	2
Диапазон частот, МГц	5250÷5350
Коэффициент усиления, дБ	10,0
Максимальная подводимая мощность, мВт	200
Максимальная излучаемая мощность, мВт	190
Ширина диаграммы направленности:	
В вертикальной плоскости, градусов	8
В горизонтальной плоскости, градусов	360
Входное сопротивление, Ом	50
КСВ в рабочем диапазоне частот, не более	1,8
Коэффициент направленности	10
Масса, кг	0,5

Продолжение таблицы 2.2

1	2

Габаритные размеры: ширина-высота, см	3-80
Максимальная скорость ветра, км/час	160
Поляризация	вертикальная
Диапазон рабочих температур, °С	-40 ÷ +50
Разъем	розетка N типа
Тип антенны	коллинеарная
Гарантия	1 год

Диаграмма направленности антенны в вертикальной плоскости приведена на рисунке 2.2, частотные характеристики антенны- на рисунке 2.3.

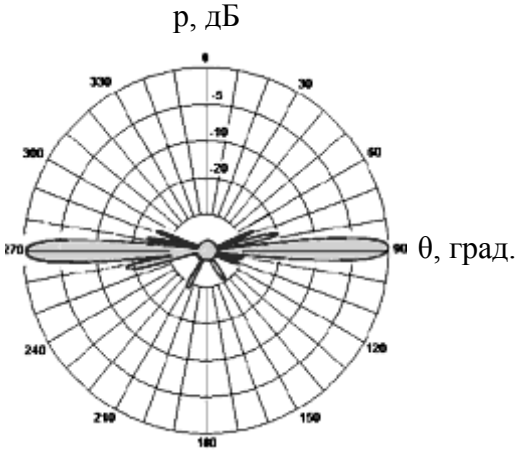


Рисунок 2.2- Диаграмма направленности антенны Omni-5.3-10

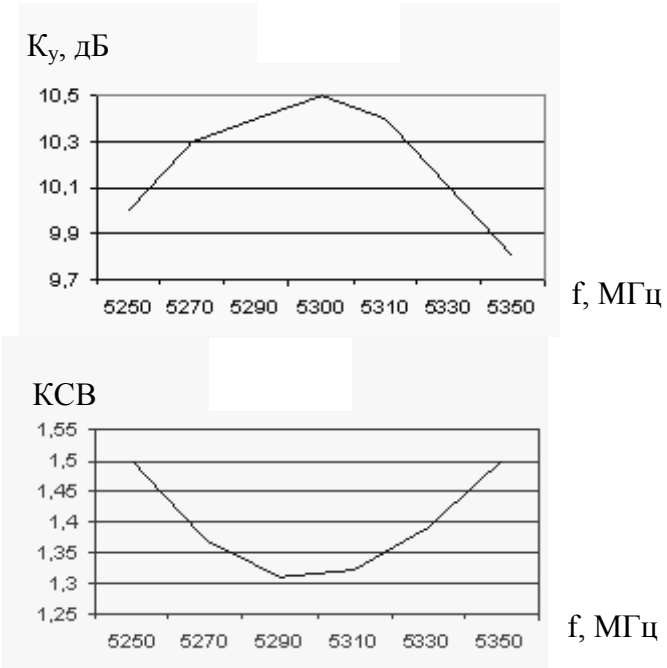


Рисунок 2.3- Частотные характеристики антенны Omni-5.3-10

Узконаправленная антенна ANT-5.2-24 предназначена для использования в аппаратуре передачи данных диапазона 5,25-5,35 ГГц в

качестве приемо-передающей антенны. Высокий коэффициент усиления дает возможность применять данную антенну для подключения удаленных объектов и организации магистральных каналов. Антенна имеет небольшие размеры и легкокрасящееся покрытие, что способствует скрытому монтажу. Антенна крепится на вертикальную трубу диаметром 30-50 мм. Система крепления позволяет регулировать угол наклона антенны относительно трубы.

Диаграмма направленности антенны приведена на рисунке 2.4, технические характеристики антенны- в таблице 2.3.

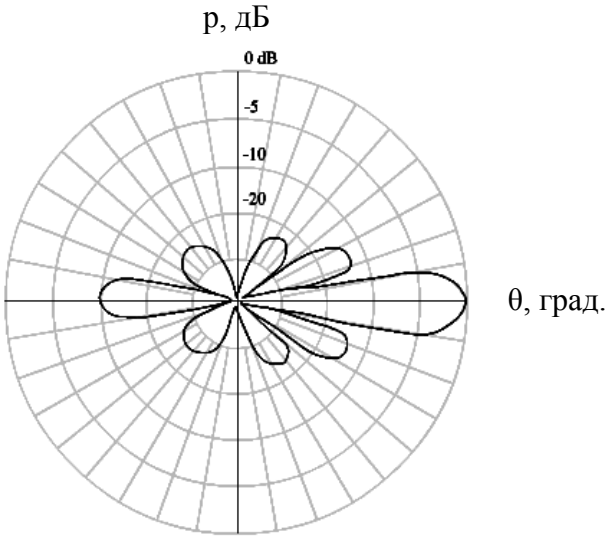


Рисунок 2.4- Диаграмма направленности антенны ANT-5.2-24

Таблица 2.3- Технические характеристики антенны ANT-5.2-24

Характеристики	Значения
Диапазон рабочих частот, МГц	5250÷5350
Максимальная излучаемая мощность, мВт	200
Коэффициент усиления, дБ	20÷24
Коэффициент направленности	30
Коэффициент стоячей волны	<1,5
Ширина диаграммы направленности, градусов	8
Уровень боковых лепестков, дБ	-12
Входное сопротивление, Ом	50
Разъем	N-типа Female
Поляризация	линейная
Вес антенны с креплением, кг	0,9
Размер антенны, см	38,5x38,5
Диаметр мачты для установки, мм	30÷40
Производство	Россия

Частотные характеристики антенны приведены на рисунке 2.5.

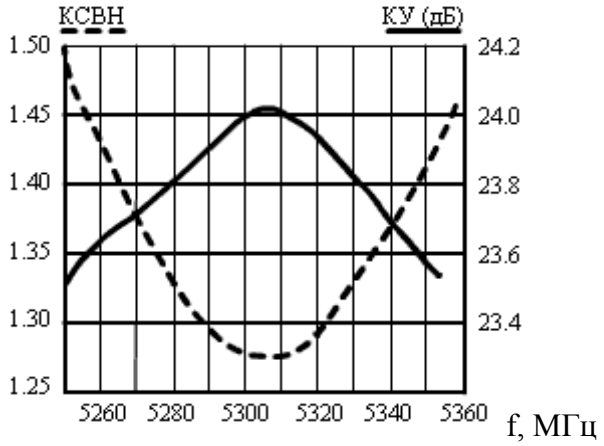


Рисунок 2.5- Частотные характеристики антенны ANT-5.2-24

Антенный двунаправленный усилитель Манус-5202 предназначен для использования совместно с радиомодемами диапазона 5,15-5,35 ГГц, работающими в полудуплексном режиме, компенсации потерь в кабеле, увеличения дальности связи и повышения ее качества в условиях сильных внеполосных помех.

Усилитель имеет в своем составе встроенный фильтр-грозозащитник, обеспечивающий подавление внеполосных помех. Технические характеристики усилителя приведены в таблице 2.4.

Таблица 2.4- Технические характеристики усилителя MANUS-5202

Характеристики	Значения
1	2
Общие характеристики	
Диапазон рабочих частот, ГГц	5,15÷5,35
Режим работы	полудуплекс
Время переключения, мкс	0,5
Диапазон рабочих температур, °С	-40 ÷ +50
Напряжение питания (мин/макс), В	10,5/15
Ток потребления (мин/макс), А	0,15/0,8
Мощность переключения (пороговая), мВт	0,5
Вес усилителя/комплекта, кг	2 / 3,5
Передающий усилитель	
Усиление, дБ	30 ± 10 %
Выходная мощность, мВт	200 ± 10 %
Максимальная входная мощность, дБм	20
Автоматическая регулировка выходной мощности	есть
Приемный усилитель	
Усиление, дБ	34 ± 10 %

Продолжение таблицы 2.4

1	2

Коэффициент шума, дБ	3 ± 10 %
Адаптируемое усиление	есть

2.3 Основные возможности и характеристики оборудования

Основные возможности используемого оборудования:

– использование операционной системы реального времени WANFleX со сверхбыстрым аппаратом маршрутизации;

– универсальность системы. Возможность работы в качестве абонента и точки доступа;

– автоматическое тестирование каналов;

– автоматический выбор наилучшей базовой станции для регистрации по интегральному критерию качества канала;

– IP- роуминг;

– динамическая IP- маршрутизация;

– централизованная служба разрешения удалённого доступа RAPS;

– встроенная система диагностики;

– непрерывное отображение состояния каналов с абонентами;

– непрерывная индикация состояния качества канала с базовой станцией;

– мощный механизм автономного тестирования канала для наведения антенн;

– защита от несанкционированного подключения и доступа;

– разграничение скорости потоков по адресам сетей и/или абонентов;

– назначение приоритетов потокам;

– проверка на соответствие MAC и IP-адресов;

– возможность сбора и отображения статистики по переповторам передачи и приема пакетов в радиосреде;

– возможность оценки радиочастотной обстановки (наличия сигналов) одновременно на нескольких частотных каналах;

– возможность передачи группы мелких пакетов в одном большом (Bursting);

– режим централизованной раздачи полномочий базовой станцией абонентам (Polling);

– поддержка сетевого протокола управления (Simple Network Management Protocol, SNMP) версии 1 (MIB-II);

– возможность потокового сжатия информации для повышения эффективности радиоканала;

– автоматическая приоритезация VoIP-трафика.

Технические характеристики RWR-5000 micro приведены в таблице 2.5.

Таблица 2.5- Технические характеристики RWR-5000 micro

Характеристика	Значение

1	2
Исполнение	Всепогодное
Связь с кабельной сетью	10/100 Ethernet
Локальное управление	Консольный порт, RS-232
Рабочий диапазон частот, ГГц	5,25-5,35
Рабочие номиналы частот, МГц	5260, 5280, 5300, 5320, 5340
Максимальная производительность в радиоканале, Мбит/с	54
Метод кодирования	BPSK, QPSK, 16-QAM, 64-QAM
Пороговая чувствительность приемника, дБм	-90 ÷ -69
Мощность на антенном выходе, дБм	14 ÷ 17
Интерфейс с АФУ	N- type Female

Рабочие частоты оборудования приведены в таблице 2.6.

Таблица 2.6- Рабочие частоты

Номер частоты	Значение центральной частоты, МГц
1	5260
2	5280
3	5300
4	5320
5	5340

Энергетические параметры оборудования приведены в таблице 2.7.

Таблица 2.7- Энергетические параметры

Скорость передачи, кбит/с	Максимальная мощность на антенном выходе, мВт	Чувствительность приемника пороговая, дБм	Вид модуляции	Подавление соседнего канала, дБ	Минимальный уровень по шкале RWR, необходимый для получения максимальной скорости	Минимальное SNR, необходимое для получения максимальной скорости
6	60	- 90	BPSK	16	2	5
9	60	- 89	BPSK	15	3	8
12	60	- 87	QPSK	13	4	10
18	60	- 84	QPSK	11	5	13
24	60	- 81	16-QAM	8	6	16
36	40	- 78	16-QAM	4	7	19
48	30	- 73	64-QAM	0	8	22
54	6	- 69	64-QAM	- 1	9	25

Физические параметры оборудования приведены в таблице 2.8.

Таблица 2.8- Физические параметры

Параметры	Величина
Аппаратная платформа	CPU IBM PowerPC 200-400 MHz, 16MB DRAM
Габариты:	
- внешнего блока, мм	160x235x60
- внутреннего блока, мм	170x190x35
Крепление внешнего блока	На трубу диаметром 30-50 мм
Расстояние между внешним и внутренним блоками	До 100 м при применении витой пары (для прокладки на улице) категории 5 и выше
Интерфейсы СВЧ	Разъем N-типа Female (розетка)
Локальное управление	Консоль 2РМ14КПН4Г
Интерфейс к внутреннему блоку	Разъем 2РМТ18КПН7Ш
Вес:	
- внешнего блока, кг	2
- внутреннего блока, кг	2,5
Диапазон рабочих температур:	
- внешнего блока, ° С	+35 ÷ +60/-50° ÷ +60 в версии ОТ
- внутреннего блока, ° С	0 ÷ +40°
Энергопитание внутреннего блока	210-230 В, 50/60 Гц, 30 Вт

2.4 Типовые применения оборудования

Маршрутизаторы Revolution (рисунок 2.6) серии 5000 предназначены для использования в качестве абонентского устройства, а также организации точек ретрансляции.

Рисунок 2.6- Маршрутизаторы Revolution

Возможные схемы применения маршрутизаторов серии 5000 показаны на рисунках 2.7 и 2.8.

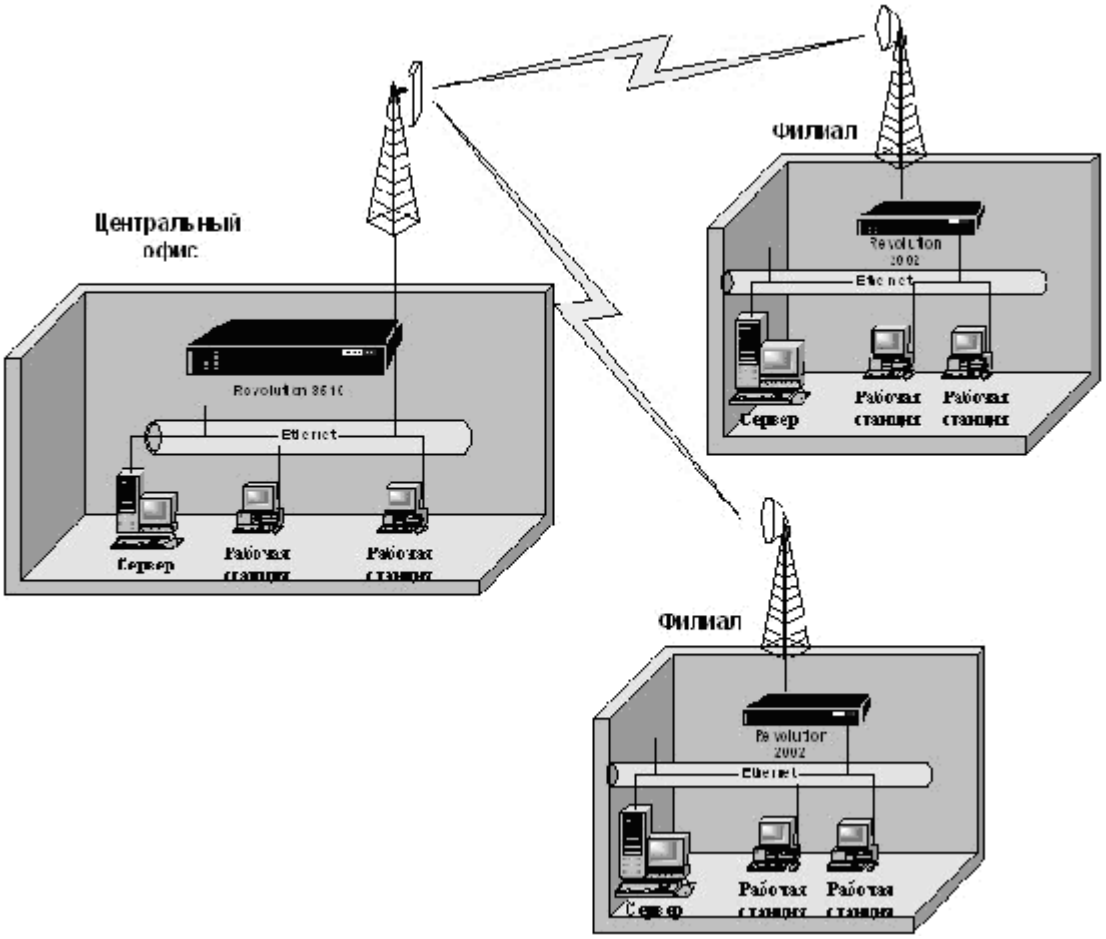


Рисунок 2.7- Применение RWR 500x в качестве клиентского устройства

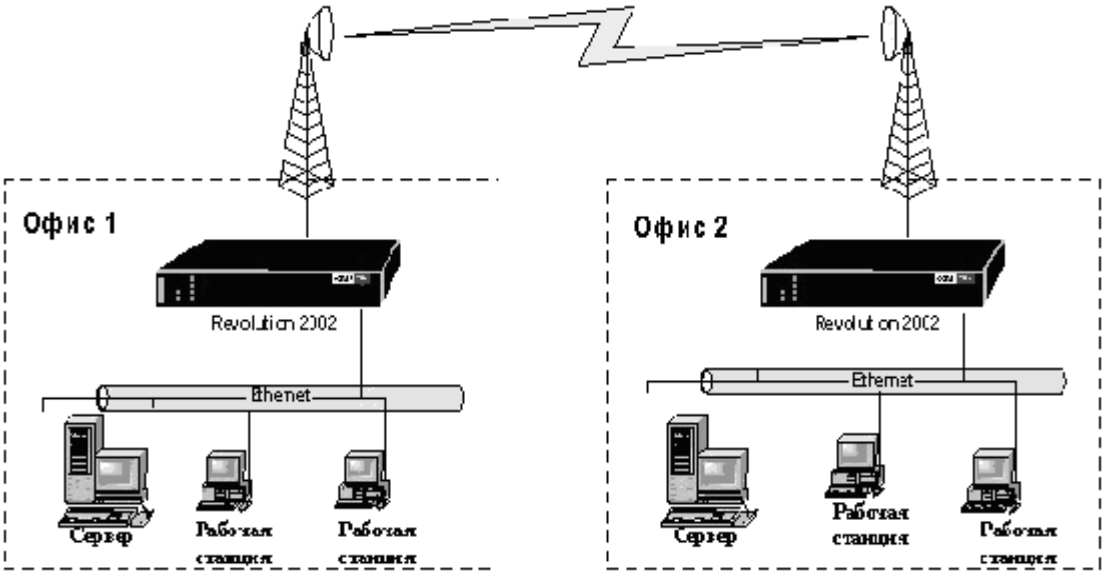


Рисунок2.8- Организация канала точка-точка

Радиомаршрутизаторы Revolution могут использоваться для построения, как магистральных каналов, так и сотовых или микросотовых структур в рамках архитектуры SkyMAN/CA. Характерной особенностью архитектуры

Revolution является то, что маршрутизатор может быть использован в качестве любого элемента беспроводной сети, в частности:

– абонентского устройства, соединяющего LAN абонента с WAN;

– точки доступа к сети для соединения абонентских устройств между собой в единую сеть;

– ретранслятора беспроводного канала для увеличения расстояния между абонентским устройством и точкой;

– доступа или обхода препятствия;

– магистралеобразующего устройства.

Настройка всех параметров устройства выполняется через удобный интерфейс. Для подключения необходимо знать параметры TCP/IP. По умолчанию, у устройства следующие настройки: IP адрес 192.168.2.1, маска подсети 255.255.255.0. Если компьютер, с которого выполняется настройка Revolution не находится в той же подсети, его необходимо настроить (потребуется указать IP адрес вида 192.168.2.X, маска подсети 255.255.255.0). В дальнейшем можно настроить устройство на использование другого IP адреса, но для этого необходимо подключиться к интерфейсу и изменить параметры LAN.

Revolution не поддерживает множественные административные подключения. При попытке такового будет предупреждение о том, что административный вход в систему выполнен с машины с указанным IP-адресом [13].

2.5 Безопасность данных

Стоит уделять особое внимание безопасности данных при беспроводной передаче. Здесь разработчики сделали большой шаг вперёд: кроме стандартной возможности использования WEP шифрования трафика с использованием ключей длиной до 128 бит (64 или 128) маршрутизатор поддерживает новый стандарт безопасности беспроводных сетей - WPA (Wi-Fi Protected Access) и средства аутентификации 802.1x (автоматическое распределение сертификатов сервером - обычно используется сервер RADIUS), что достаточно актуально сегодня. Причём, WPA может использовать не только 802.1x, но и PSK (Pre-Shared key). Имеется возможность совместного использования обоих средств безопасности: WEP и WPA, но в таком случае WEP будет слабым местом всей сети, поэтому такой вариант использоваться не будет.

Следует упомянуть о криптографической дыре в алгоритме шифрования WEP, из-за которой различные зашифрованные пакеты данных имеют сходство, достаточно для того, чтобы, захватив несколько таких пакетов, путём их анализа получить ключ шифрования. Стандарт WPA лишён этой проблемы и обеспечивает более высокую степень защиты данных. Этот стандарт предполагает аутентификацию, шифрование и проверку целостности

переданных данных. Краткие характеристики стандартов безопасности 802.11 представлены в таблице 2.9.

Таблица 2.9- Развитие стандартов безопасности 802.11

Стандарт безопасности	Краткая характеристика	Достоинства	Недостатки
WEP	Шифрование RC4, статичные ключи и необязательная идентификация пользователя	Обеспечение минимальной безопасности	Много дыр безопасности, необходимы дополни-тельные средства
WPA	Шифрование TKIP, динамичные ключи и идентификация пользователей с помощью EAP, RADIUS	Более надежный стандарт, совместимый с WEP; легко интегрируется с существующими WLAN решениями	Промежуточное решение, которое можно использовать до принятия спецификации 802.11i
802.11i	Шифрование AES, WRAP, управление ключами в стандарте 802.11i, обязательная идентификация пользователей	Криптостойкий стандарт, надежный механизм управления ключами	Требуется обнов-лять оборудование, полная несовместимость с существующими Wi-Fi адаптерами

Одним из важных шагов для предотвращения доступа злоумышленников к беспроводной сети должна быть фильтрация MAC адресов. В Revolution реализована, при этом список разрешенных MAC адресов может включать в себя до 32-х записей. Активизировав эту функцию и указав разрешённые MAC адреса, запрещается доступ к сети всем остальным.

На Revolution реализована функция обнаружения атак (Intrusion Detection), позволяющая определять и блокировать внешние атаки: IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan и TCP SYN flooding. Кроме того, можно запретить отсылку ответов на эхо-запросы PING, пришедшие на WAN порт. В случае обнаружения атаки устройство может известить системного администратора, используя электронную почту, или отреагировать на атаку самостоятельно.

Методы повышения защиты.

Рассмотренные возможности выбранного оборудования позволяют обеспечить требуемый уровень безопасности, но для этого необходимо в первую очередь изменить заводские установки, а именно:

– изменить пароль администратора, установленный по умолчанию;

– активизировать фильтрацию по MAC-адресам;

– запретить широковещательную рассылку идентификатора сети (SSID);

– изменить SSID, установленный по умолчанию, и периодически изменять его;

– активизировать функции WEP;

– периодически изменять WEP-ключи;

– активизировать функции WPA;

– установить и настроить персональные межсетевые экраны и антивирусные программы у всех зарегистрированных абонентов;

– выполнить настройку фильтрации трафика на телекоммуникационном оборудовании и межсетевом экране;

– организовать резервное копирование ПО и конфигураций оборудования;

– периодически проводить мониторинг защищенности беспроводной сети с помощью специализированных программ;

– уменьшить зону радиопокрытия (разумеется, до минимально приемлемой). В идеале зона радиопокрытия сети не должна выходить за пределы контролируемой территории [22].

Использование VPN (Virtual Private Network).

Оптимальное решение проблемы является в использовании технологии защищенных частных виртуальных сетей (VPN). Внедрение технологии VPN для обеспечения конфиденциальности и целостности информации, циркулирующей в беспроводной сети, находится в соответствии с требованиями казахстанского законодательства и руководящих документов.

Хотя сама по себе технология защищенных частных виртуальных сетей способна обеспечить жесткую авторизацию пользователя по его цифровому сертификату формата X.509, ее не следует рассматривать как альтернативу решениям на базе протокола 802.1x, это взаимодополняемые решения. Средства VPN обеспечивают защиту на сетевом уровне, а механизмы, реализующие протокол 802.1x, позволяют предотвратить несанкционированный доступ к беспроводной сети на более раннем этапе.

Такая схема помогает построить многоэшелонную защиту. Авторизуя пользователей по протоколу 802.1x, убеждаемся, что имеем дело с легальным пользователем корпоративной WLAN. Реализуя дополнительную авторизацию средствами VPN, понимаем, что допускаем к работе с конфиденциальными ресурсами только тех пользователей, которые имеют на это право. Кроме того, путем активизации функций межсетевого экранирования на VPN-шлюзах можно назначать различные права доступа

внутри группы пользователей, имеющих доступ к конфиденциальной информации.

Технология виртуальных частных сетей, известная также под названием VPN, была разработана для безопасного соединения клиентских систем с серверами по общедоступным каналам Интернета. Для этого в технологии VPN используются мощные, хорошо зарекомендовавшие себя с точки зрения надежности механизмы аутентификации и шифрования. Фактически VPN-соединения представляют собой туннель между двумя конечными точками, защищающий от вторжения, проходящие по каналам Интернета пакеты.

В процессе установки VPN-соединения создаются индивидуальные безопасные каналы между конечными устройствами и шлюзом VPN, которые в случае сетей стандарта 802.11a/b/g располагаются непосредственно за устройством беспроводного доступа. По существу, каждый клиент сети связывается с устройством доступа по отдельному туннелю VPN. Пакеты, направляющиеся по беспроводной сети от одного конечного устройства к другому, проходят через туннель VPN передающей системы в устройство доступа и выходят за пределы шлюза VPN. Затем пакеты передаются по кабельной локальной сети к другому шлюзу VPN, где они шифруются перед передачей системе-получателю через другое устройство беспроводного доступа. Установив за устройствами доступа сети стандарта 802.11a/b/g шлюзы VPN, можно быть уверенным в защищенности любых сообщений, проходящих по радиоканалу.

Основу системы безопасности VPN составляет протокол обмена Интернет ключами (Internet Key Exchange- IKE), входящий в состав набора протоколов IPSec (сокращение от IP Security) и предусматривающий три метода аутентификации для защиты данных и каналов связи. Этот протокол позволяет кодировать заголовки и содержимое пакетов с помощью ключа, обеспечивая практически абсолютную безопасность линии связи. В соответствии с протоколом IKE пакеты шифруются с помощью секретного ключа, заранее известного обеим сторонам, или с помощью стандартного открытого ключа. Кроме того, IKE поддерживает использование цифровых сертификатов, создаваемых такими специализированными организациями, как VeriSign, и обеспечивающих еще более высокий уровень защиты.

Технологии VPN уже получили широкое признание среди компаний, предоставляющих удаленный сетевой доступ по общедоступным каналам Интернета. VPN создает защищенный канал передачи данных между системами и позволяет организациям отказаться от дорогостоящих модемных пулов, традиционно использовавшихся для обеспечения прямого доступа к сети. По мере распространения широкополосного доступа в Интернет, технологии VPN позволят существенно повысить скорость и устойчивость доступа к удаленным сетям.

Однако платой пользователя за внедрение технологии VPN становятся:

– снижение общей пропускной способности сети. По опыту реализованных проектов при использовании в протоколах семейства IPSec

сертифицированных криптоядер снижение производительности составляет от 20 до 30 %;

– в случае подключения к беспроводной сети карманных компьютеров (PDA) и/или беспроводных IP-телефонов найти VPN-агента и криптографическое ядро для этих аппаратных платформ достаточно проблематично. Поэтому на данном этапе будет правильно применять к этим устройствам доступа политику безопасности, исключающую их взаимодействие с конфиденциальными ресурсами банка.

3 Построение беспроводной сети

3.1 Проведение исследований

Перед развертыванием беспроводной сети необходимо провести исследование на месте. Для определения зон покрытия при создании беспроводных сетей, в настоящее время используются два основных подхода-экспериментальный и расчетный. Расчетный требует специального программного обеспечения и серьезного анализа (с точки зрения геометрии помещений, материалов стен и перекрытий и т.д.), но все равно необходимо проводить экспериментальную проверку и, при надобности, корректировать топологию системы (например, при выявлении зон неуверенного приема сигнала или недостаточного перекрытия зон действия базовых станций).

На практике многое зависит от опыта специалистов-установщиков. Можно либо сразу наметить места установки с хорошим перекрытием либо нужно сначала «прощупать» все с помощью специального прибора и компьютера. Это делается в целях экономии, поскольку позволяет избежать установки лишнего оборудования.

Процесс исследования включает в себя:

– анализ карты местности и структурных элементов;

– оценку зоны распространения радиосигнала, включая выбор зон установки компонентов для обеспечения минимальной потери сигнала, определение оптимальной схемы размещения точек доступа и антенн;

– оценку интерференции каналов, включая тестирование для обеспечения отсутствия перекрытия радиопередач;

– выбор положения антенны, включая положения всенаправленной антенны и направленной антенны;

– определение приема, в том числе преодоление интерференции и затухания сигнала посредством размещения в определенных местах нескольких антенн;

– оценку электрических систем, в том числе оценка альтернатив подключения точки доступа к электросети для предотвращения деградации производительности в связи со случайными или неизбежными электрическими проблемами.

Для того чтобы обеспечить зону покрытия, расположению беспроводного устройства Revolution, следует уделить особое внимание. К месту его установки должны быть подведены все необходимые кабели. Причём чем выше место, в котором располагается передатчик, тем больше радиус действия.

Если же окажется так, что всё равно недостаточно зоны покрытия, обеспечиваемой данным устройством, его можно модернизировать. Для увеличения площади покрытия можно заменить стандартные антенны либо на антенны с большим коэффициентом усиления, либо на направленные (секторные). Каких либо серьёзных ограничений по вентиляции и температуре для местоположения устройства нет, так как исполнение выносного блока всепогодное.

3.2 Тестирование производительности оборудования

В месте проведения тестирования другого беспроводного оборудования стандартов 802.11 a ,b или g не было, равно как и других устройств, работающих в диапазоне 5,25-5,35 ГГц. При тестировании использовались следующие конфигурации:

- процессор AMD Athlon 1000;
- память 256 Мб SDRAM;
- проводной стамегабитный сетевой адаптер;
- беспроводный сетевой адаптер стандарта 802.11g;
- операционная система Windows 2000 с установленным SP4;
- значения «качество сигнала» полученные с помощью утилиты SMC.

Конфигурации работали с тестируемым устройством напрямую, без каких либо промежуточных устройств. Для тестирования использовалась утилита NetIQ Chariot [23].

Беспроводная часть.

Условия тестирования производительности:

- шифрование WEP: выключено;
- скорость передачи: автоматическая;
- энергосбережение: выключено.

Результаты беспроводной производительности 802.11g при передаче 1 Мбайт данных представлены в таблице 3.1.

Таблица 3.1- Производительность беспроводной части Revolution

Условия	Качество сигнала, %	Скорость передачи, Мбит/с	Время реакции (10 итераций пакетов по 100 байт), мс	Пропускная способность UDP, кбит/с	Потеря данных потока UDP, %
Условие 1	100	23,59 без WEP 23,47 с WEP	1 (ср.), 3 (макс.)	499	0
Условие 2	75	22,551	1 (ср.), 4 (макс.)	499	0

Ниже представлены диаграммы, выданные утилитой NetIQ Chariot для условий 1 и 4 (рисунки 3.1 и 3.2).

Скорость передачи больших объёмов данных оказалась на уровне других устройств данного стандарта- выше 20 Мбит/с, но ниже 25 Мбит/с. По результатам тестирования скорости при включенном шифровании WEP и при выключенном, стоит отметить, что существенной разницы не замечено. Получившееся различие можно отнести к погрешности измерений.

Рисунок 3.1- Тестирование беспроводной части
при условии 1 (без WEP)

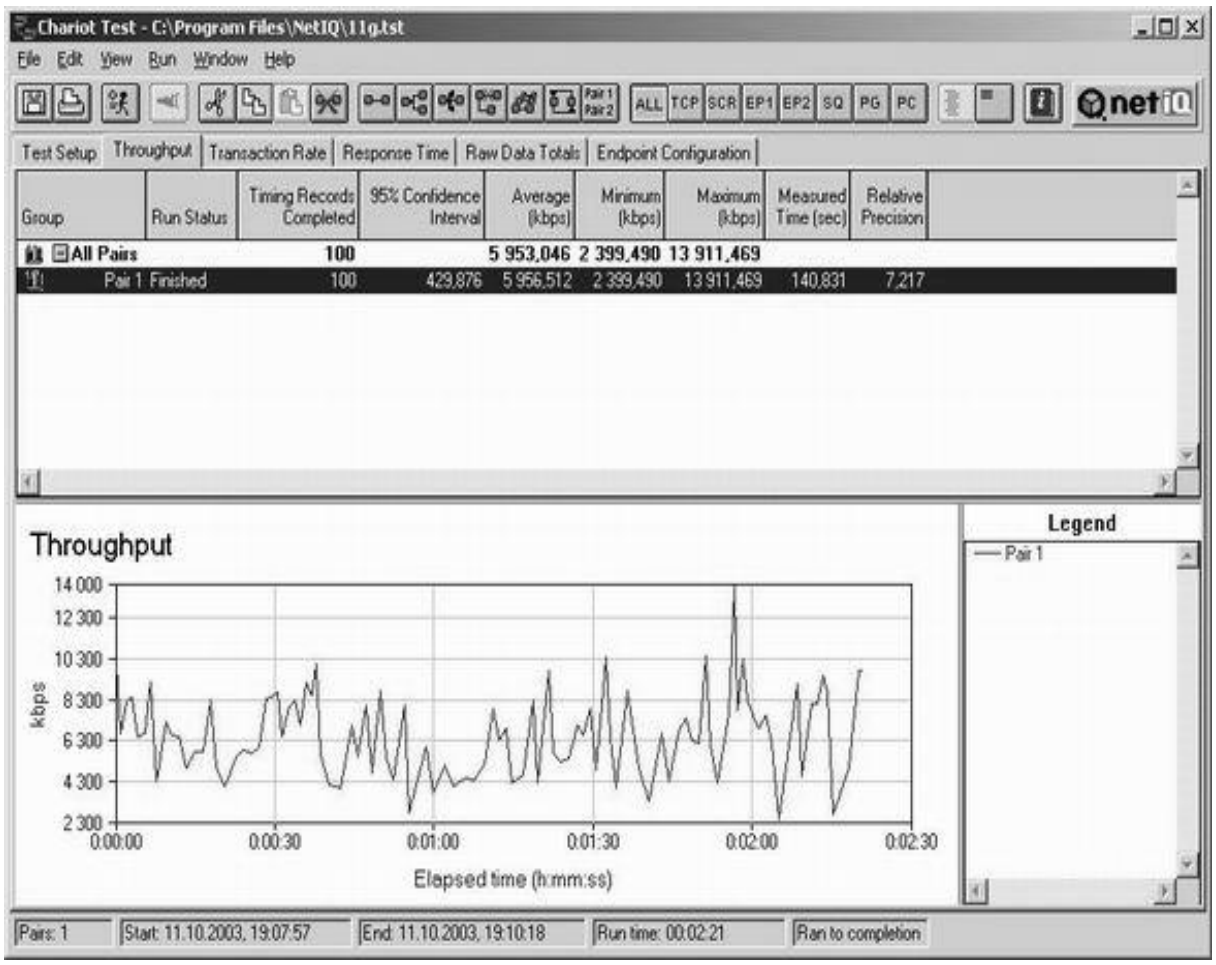


Рисунок 3.2- Тестирование беспроводной части
при условии 4

Таким образом, шифрование WEP практически не сказывается на производительности сети и его рекомендуется использовать для обеспечения хотя бы минимальной защиты сети в целом.

Встроенный коммутатор.

Для данного тестирования использовалось два компьютера, оборудованные 100-мегабитными сетевыми адаптерами Ethernet. Компьютеры располагались в сегменте LAN и были подключены непосредственно к портам устройства, поэтому скорость маршрутизации, а также внешние параметры никак не повлияли на результат этого тестирования (рисунок 3.3).

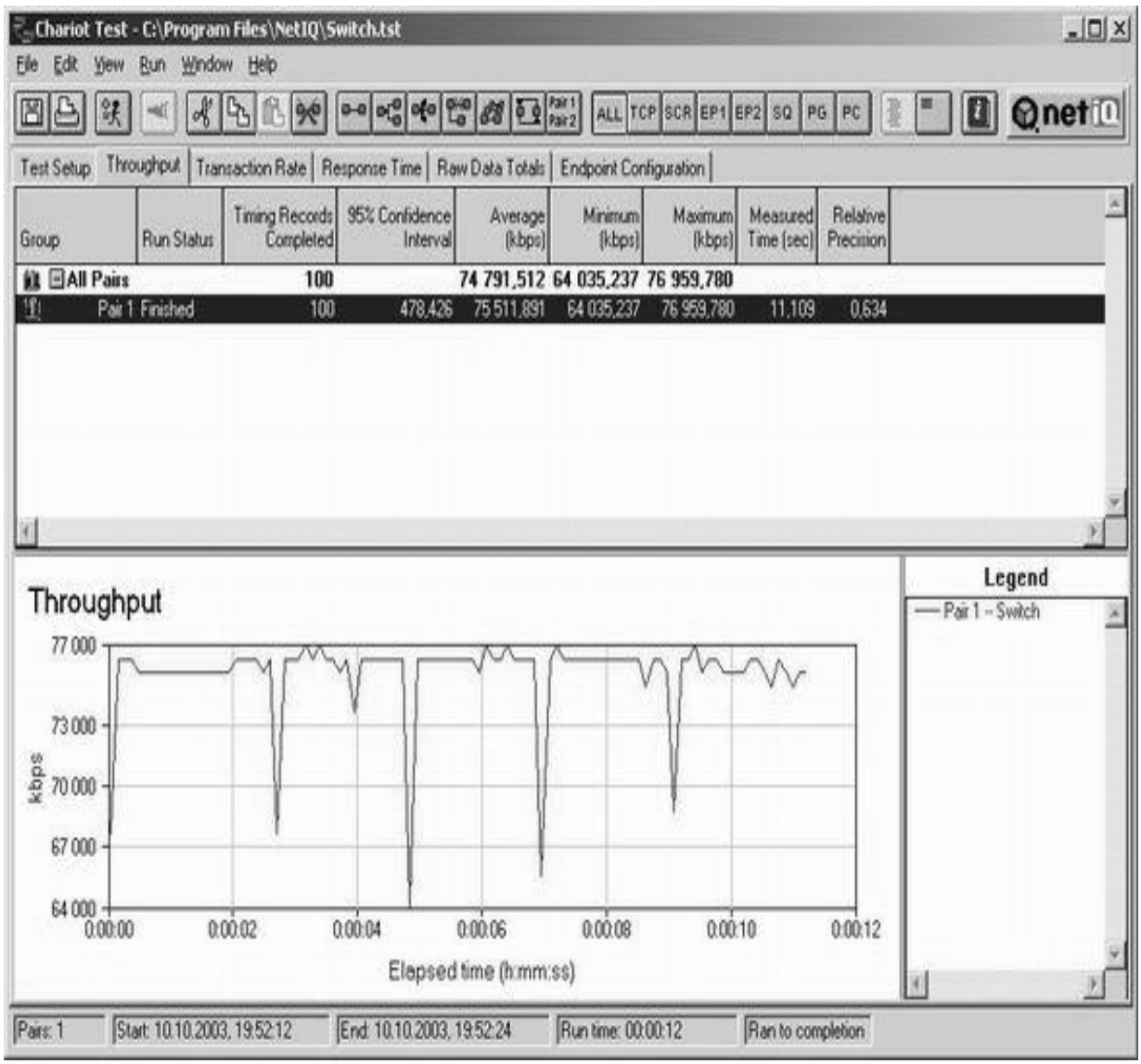


Рисунок 3.3- Тестирование производительности коммутации

Средняя скорость составила 75,512 Мбит/с. Такой показатель скорости характерен для стамегабитного сетевого оборудования, поэтому встроенный коммутатор данного оборудования отвечает нормам сетевого коммутационного оборудования.

Маршрутизация.

При тестировании к маршрутизатору Revolution были подключены только машины, при помощи которых проводилось тестирование. Беспроводная часть также отключена. Размер передаваемых данных составил 1 Мбайт. Результаты теста производительности представлены в таблице 3.2.

Как видно по значениям, представленным в таблице, скорость маршрутизации Revolution является более чем достойной для устройств такого класса. Она оказалась немного выше для направления LAN-WAN (рисунок 3.4), но, как видно, разница минимальна.

Таблица 3.2- Производительность маршрутизации Revolution

Описание теста	Скорость передачи, Мбит/с	Время ответа (10 итераций по 100 байт), мс	Поток UDP. Актуальная пропускная способность, кбит/с	Поток UDP. (Потерянных данных), %
WAN-LAN	34,3	1 (сред.) 5 (макс.)	498	0
LAN-WAN	37,5	1 (сред.) 4 (макс.)	499	0

Рисунок 3.4- Тестирование маршрутизатора в направлении LAN-WAN

Шифрование.

При проведении тестирования выяснилось, что пропускная способность оказалась ниже при использовании WPA шифрования и почти не изменилась при WEP (таблица 3.3).

Таблица 3.3- Зависимость скорости работы от режима работы сети

Режим	Скорость, Мбит/с
Без шифрования	23,590
Шифрование WEP	23,465
Шифрование WPA	18,138

Для наглядности на рисунке 3.5 приведена диаграмма теста.

Рисунок 3.5- Тестирование беспроводной части
(Шифрование WPA)

Таким образом, если скорость незащищённого соединения принять за 100%, скорость соединения при использовании шифрования WEP будет около 99,5%, а скорость при использовании WPA- 76,9%. Цена надёжной защиты составляет 23,1% пропускной способности сети. Однако стоит отметить, что при проникновении в сеть злоумышленника можно понести не только нежеланную утечку данных, но и то же самое, а может даже большее снижение пропускной способности.

Результаты.

Тестирование всех моделей оборудования, в том числе и выбранного нами, проводилось самим производителем. Процесс тестирования выбранного оборудования приведён выше.

Результаты тестирования следующие:

– производительность встроенного коммутатора оказалась очень хорошей. В целом пропускная способность была стабильна, за исключением двух кратковременных падений, которые, произошли не по вине коммутатора;

– скорость маршрутизации оказалась более чем достаточна, измерялась скорость маршрутизации при передаче данных с внешнего интерфейса на внутренний;

– так как предполагается использование защищенной беспроводной сети, с использованием шифрования WPA, средняя пропускная способность Revolution составит 18 Мбит/с. Такая скорость позволит работать до 20 очень активным пользователям, постоянно использующих сеть и работающих с большими файлами [23].

3.3 Расчёт энергетических параметров

Расчёт затухания.

Основная особенность радиолиний связи- затухание радиосигнала на участках линии. Кроме этого, радиосигнал претерпевает случайные изменения вследствие поглощения радиоволн в атмосфере (дождь, снег, туман), их рефракции и деполяризации, фарадеевского вращения плоскости поляризации. На приёмные устройства воздействуют помехи в виде излучений космоса, Солнца, Земли и др. планет.

Правильный и точный учет всех особенностей радиосвязи позволяет выполнить оптимальное проектирование системы связи, обеспечить её надежную работу в наиболее сложных условиях и в то же время исключить излишние энергетические затраты, приводящие к неоправданному усложнению аппаратуры.

Для того чтобы рассчитать затухание энергии сигнала в свободном пространстве, необходимо знать частоты, через которые будет работать сеть.

Полное затухание радиосигналов в линиях радиосвязи определяется потерями в свободном пространстве W_0 и дополнительными потерями $W_{доп}$, обусловленными особенностями функционирования систем радиосвязи:

$$W = W_0 + W_{доп}, \text{ дБ} \tag{3.1}$$

Потери энергии радиоволн при распространении в свободном пространстве определяются в соответствии с выражением:

$$W_0 = 20\lg\left(\frac{4 \cdot \pi \cdot R_i}{\lambda}\right), \text{ дБ} \tag{3.2}$$

где $R_н$ - расстояние между точкой приёма и передачи, м; λ=c/f - длина волны, м; c =$3 \cdot 10^8$ м/с- скорость света; f- частота сигнала, Гц.

Дополнительное затухание радиосигнала на участках радиолинии $W_{доп}$ зависит от многих факторов, проявляющихся независимо друг от друга и может быть представлено в виде суммы:

$$W_{доп} = W_a + W_д + W_н + W_п \qquad (3.3)$$

где W_a - затухание в атмосфере без осадков, дБ;

$W_д$ - затухание в осадках, дБ;

$W_н$ - затухание, учитывающее неточность наведения антенн, дБ;

$W_п$ - затухание за счет деполяризации сигнала в среде распространения, дБ.

Потери энергии радиосигнала в атмосфере без осадков не зависят от времени (имеют место в течение 100% времени работы радиолинии) и определяются по графикам (рисунок 3.6) в зависимости от частоты радиосигнала и угла места антенны.

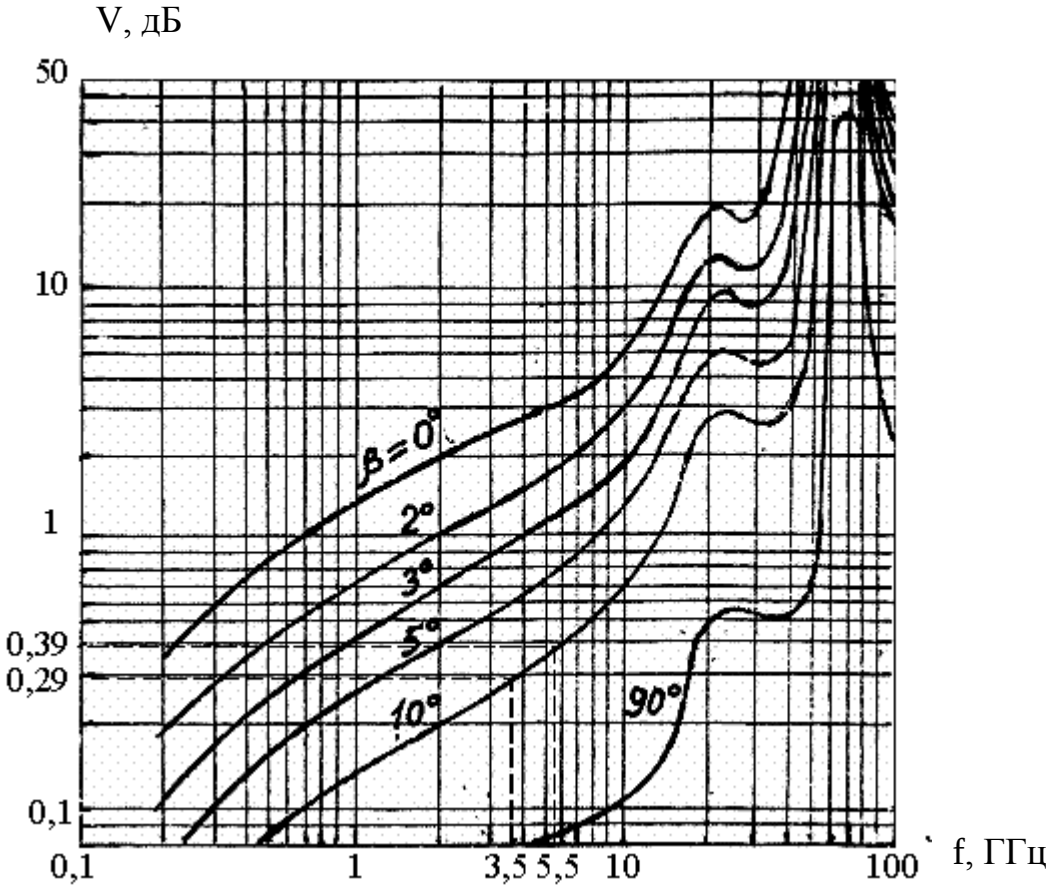


Рисунок 3.6- Графики для определения затухания радиосигнала в атмосфере без осадков

Если угол места для антенн установленных в городе Алматы составляет 30,74 (рассчитано в программе «Orbitron»), то есть $\beta^\circ \geq 10^\circ$, то значения потерь энергии принимаются для кривой $\beta^\circ = 10^\circ$, тем самым заранее завысив потери энергии радиосигнала в атмосфере без осадков. Однако неточность составит не более 0,1 дБ, следовательно на точность расчёта не повлияет [10].

Затухание сигнала в осадках $W_д$ зависит от вида осадков (дождь, снег, туман), размеров зоны их выпадения, интенсивности осадков в зоне и т.д. Как показывает практика, величина затухания сигнала в осадках от 1,5 до 3 дБ.

Дополнительное затухание сигнала за счет неточного наведения антенн $W_н$ обусловлено рефракцией радиоволн. Угловое отклонение, вызванное рефракцией, составляет несколько десятых долей градуса и может быть скомпенсировано при наведении антенн по максимуму сигнала. При других методах наведения с учетом погрешностей конструкции устройства наведения можно принять $W_н$=1 дБ. Затухание за счет деполяризации сигнала в среде распространения – при линейной поляризации не более 0,5 дБ.

По карте города Алматы найдем расстояния от выбранных мест установки точек доступа к сети (промежуточные пункты) и местом установки основного оборудования сети (гостиница Анкара, с самой большой высотой для установки всенаправленной антенны).

Расстояния между местом установки и подключаемыми объектами приведены в таблице 3.4.

Таблица 3.4- Расстояния между объектами подключения

Названия объектов подключения (гостиниц)	Расстояния между промежуточными пунктами и местом установки, км
1 Алма-Ата - Анкара	3,1
2 Казахстан - Анкара	3,7
3 Амбассадор - Анкара	4,2
4 Жетысу - Анкара	4,5
5 Астана - Анкара	0,7
6 Алатау - Анкара	2
7 Отрар - Анкара	4,35
8 Хаятт Ридженси - Анкара	1
9 Достык - Анкара	2,6

Рассчитаем длину волны.

Так как рабочий диапазон частот составляет 5,25-5,35 ГГц, примем f=5,5 ГГц, заранее завысив потери энергии радиоволн в свободном пространстве:

$$\lambda=3\cdot10^{8}/5{,}5\cdot10^{9}=0{,}545\cdot10^{-1}=0{,}055\text{м}$$

Определим затухание сигнала на участках по формулам (3.2) и (3.3):

- Алма-Ата - Анкара:

$$W_0 = 20\lg\left(\frac{4 \cdot 3{,}14 \cdot 3{,}1 \cdot 10^3}{0{,}055}\right) = 56{,}9 \text{ дБ}$$

$$W_{доп} = W_а + W_д + W_н + W_п = 0{,}1+1{,}5+1+0{,}5=3{,}1 \text{ дБ}$$

$$W = W_0 + W_{доп} = 56{,}9+3{,}1=60 \text{ дБ}$$

- Казахстан - Анкара:

$$W_0 = 20\lg\left(\frac{4 \cdot 3{,}14 \cdot 3{,}7 \cdot 10^3}{0{,}055}\right) = 58{,}5 \text{ дБ}$$

$W = 58{,}5 + 3{,}1 = 61{,}6$ дБ

- Амбассадор - Анкара:

$$W_0 = 20\lg\left(\frac{4 \cdot 3{,}14 \cdot 4{,}2 \cdot 10^3}{0{,}055}\right) = 59{,}6 \text{ дБ}$$

$W = 59{,}6 + 3{,}1 = 62{,}7$ дБ

- Жетысу - Анкара:

$$W_0 = 20\lg\left(\frac{4 \cdot 3{,}14 \cdot 4{,}5 \cdot 10^3}{0{,}055}\right) = 60{,}2 \text{ дБ}$$

$W = 60{,}2 + 3{,}1 = 63{,}3$ дБ

- Астана - Анкара:

$$W_0 = 20\lg\left(\frac{4 \cdot 3{,}14 \cdot 0{,}7 \cdot 10^3}{0{,}055}\right) = 44 \text{ дБ}$$

$W = 44 + 3{,}1 = 47{,}1$ дБ

- Алатау - Анкара:

$$W_0 = 20\lg\left(\frac{4 \cdot 3{,}14 \cdot 2 \cdot 10^3}{0{,}055}\right) = 53{,}2 \text{ дБ}$$

W = 53,2 + 3,1 = 56,3 дБ

- Отрар - Анкара:

$$W_0 = 20\lg\left(\frac{4 \cdot 3{,}14 \cdot 4{,}35 \cdot 10^3}{0{,}055}\right) = 59{,}9 \text{ дБ}$$

W = 59,9 + 3,1 = 63 дБ

- Хаятт Ридженси - Анкара:

$$W_0 = 20\lg\left(\frac{4 \cdot 3{,}14 \cdot 1 \cdot 10^3}{0{,}055}\right) = 47{,}2 \text{ дБ}$$

W = 47,2 + 3,1 = 50,3 дБ

- Достык - Анкара:

$$W_0 = 20\lg\left(\frac{4 \cdot 3{,}14 \cdot 2{,}6 \cdot 10^3}{0{,}055}\right) = 55{,}3 \text{ дБ.}$$

W = 55,3 + 3,1 = 58,4 дБ.

Расчёт мощности передатчиков.

Мощности передатчиков можно определить в соответствии с уравнением энергетического баланса [5]:

$$\left|P_{прд}\right| = \left|P_{прм}\right| - W - \Delta P + \left|G_{Аппр}\right|, \text{ дБ} \qquad (3.4)$$

где $P_{прд}$ - мощность сигнала на выходе передатчика, дБ;

$G_{Аппр}$ - усиление антенны, дБ;

W - полное затухание, дБ;

$P_{прм}$- средний уровень сигнала на входе приёмника при $p_{ош}$ не хуже 10^{-9}; ΔP =10 дБ- технологический запас по мощности.

Полученную мощность в децибелах необходимо перевести в ватты.

Из приведённых технических характеристик принимаем:

- $P_{прм}$ = - 69 дБ;
- W = 63,3 дБ- затухание для наихудшего варианта связи;
- $G_{Аппр}$ = 10 дБ- усиление всенаправленной антенны;
- $G_{Аппр}$ = 20 дБ- усиление узконаправленной антенны.

Мощность передатчика промежуточного пункта при использовании всенаправленной антенны:

$P_{прд}$ = 69-63,3-10+10=5,7 дБ, что соответствует мощности 3,7 мВт.

Мощность передатчика удалённого пункта при использовании узконаправленной антенны:

$P_{прд}$ =69-63,3-20+10=4,3 дБ, что соответствует мощности 2,7 мВт.

Из технических характеристик маршрутизатора видно, что мощность передатчика составляет 200 мВт, а расчётные значения: 3,7 мВт и 2,7 мВт, что доказывает возможность применения данного оборудования.

Произведём расчёт коэффициентов полезного действия и проверочный расчёт коэффициентов усиления антенн.

Коэффициентом полезного действия η называется отношение излучаемой мощности к мощности, подводимой к антенне [5]:

$$\eta = P_{\Sigma} / P_0 \qquad (3.5)$$

где P_{Σ}- мощность, излучаемая антенной;
P_0- мощность, подводимая к антенне.

Для всенаправленной антенны:

η = 190/200=0,95

Для узконаправленной антенны:

η = 200/200=1

Коэффициентом усиления ε называется отношение квадрата модуля напряжённости поля, создаваемого идеальным изотропным излучателем (η = 1):

$$\varepsilon = D \cdot \eta \qquad (3.6)$$

где D- коэффициент направленности;
η - коэффициент полезного действия.

Для всенаправленной антенны:

ε =10·0,95=9,5 дБ

Для узконаправленной антенны:

ε =20·1=20 дБ

Из расчётов видно, что приведённые технические характеристики практически совпадают с расчётными.

Расчёт шумовой температуры.

Приемное устройство СВЧ может характеризоваться некоторыми энергетическими параметрами: реальной чувствительностью, пороговой чувствительностью, коэффициентом шума, шумовой температурой и эффективной температурой. Все эти параметры, как известно, имеют определенную связь между собой. Три последних из них характеризуют линейную часть приемного устройства от антенны до детектора. В системах радиосвязи наибольшее распространение получили два последних параметра.

Шумовая температура $T_ш$ оценивает внутренние шумы линейной части приемника, пересчитанные на его вход. Она может быть выражена через коэффициент шума $n_ш$ следующим образом:

$$T_ø = T_0 \cdot (n_ø - 1) \tag{3.7}$$

где T_0 - абсолютная температура среды, в которой работает приемник.

Чем ниже шумовая температура приемника, тем выше его чувствительность. Так как основной вклад в шум приёмного устройства вносит первый каскад, т.е. МШУ (малошумящий усилитель), то коэффициент шума МШУ будет ненамного меньше коэффициента шума всего приёмного устройства. А таким МШУ может служить параметрический усилитель на полупроводниковых диодах ($n_ш$ =2,7) [6].

Так как рабочий диапазон температур составляет примерно -40 ÷ +50 ºС, то получим:

$T_ш$= - 40·(2,7 - 1) = |68| дБ/К

$T_ш$=+50·(2,7 - 1) = |85| дБ/К

Шумовая температура составляет диапазон от 68 до 85 дБ/К.

Для характеристики энергетического потенциала приемного устройства используют понятие добротности:

$$\frac{G}{T} = 10 \cdot \lg\left(\frac{G_{Anпр}}{T_{шi}}\right) = G_{Anпр} - 10 \cdot \lg T_ш , \tag{3.8}$$

где $G_{Anпр}$ - усиление антенн, дБ;

$T_ш$ – шумовая температура К.

Для всенаправленной антенны:

$$\frac{G}{T} = 10 - 10 \cdot \lg 85 = |9| \text{ дБ/К}$$

Для узконаправленной антенны:

$$\frac{G}{T} = 24 - 10 \cdot \lg 85 = |4{,}8| \text{ дБ/К}$$

3.4 Состав оборудования

Оборудование промежуточной станции состоит из:

- всенаправленной антенны типа Omni-5.3-10;
- усилителя типа MANUS-5202;
- радиомаршрутизатора;
- блока питания.

Оборудование базовой и удалённых станций состоит из:

- узконаправленной антенны типа ANT-5.2-24;
- усилителя типа MANUS-5202;
- радиомаршрутизатора;
- блока питания.

Исходя из полученных данных составим спецификацию оборудования станций (таблица 3.5).

Таблица 3.5- Спецификация оборудования станций

№ п/п	Наименование объекта (гостиниц)	Всенаправленная антенна типа Omni-5.3-10	Узконаправленная антенна типа ANT-5.2-24	Усилитель типа MANUS-5202	Радиомаршрутизатор	Блок питания
1	Алма-Ата		1 шт.	1шт.	1шт.	1шт.

Продолжение таблицы 3.5

2	Анкара	1шт.		1шт.	1шт.	1шт.
3	Казахстан		1шт.	1шт.	1шт.	1шт.
4	Амбассадор		1шт.	1шт.	1шт.	1шт.
5	Жетысу		1шт.	1шт.	1шт.	1шт.
6	Астана		1шт.	1шт.	1шт.	1шт.
7	Алатау		1шт.	1шт.	1шт.	1шт.
8	Отрар		1шт.	1шт.	1шт.	1шт.
9	Хаятт Ридженси		1шт.	1шт.	1шт.	1шт.
10	Достык		1шт.	1шт.	1шт.	1шт.

4 Безопасность жизнедеятельности

4.1 Безопасность излучения СВЧ диапазона

Несмотря на обилие статей в отечественных и зарубежных изданиях, посвящённых проблеме воздействия СВЧ излучения, ни одна из них не даёт ответа на вопрос- вредно или безвредно это излучение для человека и каковы критерии «безвредности»?

Если посмотреть на проблему шире, то становится очевидным, что человек в течении всей жизни постоянно находится под воздействием электромагнитных полей, разных по характеру и интенсивности. Более того, микроволновое излучение, генерируемое Солнцем, Галактикой, извержениями вулканов, разрядами молний и другими факторами, существовало на земле и до человека. Поскольку человек всё же выжил и довольно хорошо приспособился к окружающей среде, то можно утверждать, что уровни плотности потока мощности микроволнового излучения, соизмеримы с теми, которые создаются естественными источниками, для человека безвредны.

Наиболее мощный естественный источник излучения- Солнце. Его радиоизлучение распространяется во всём диапазоне частот. Верхней границей радиодиапазона можно считать частоты в области 50 ГГц, поскольку электромагнитные волны более высоких радиочастот практически полностью поглощаются в атмосфере Земли. Таким образом, безвредный уровень плотности потока мощности (ППМ) микроволнового излучения, к которому привык человек за всю историю своего существования на Земле, можно определить следующим образом:

$$W=2\cdot k\cdot T_{Я}\cdot D_F\cdot W/L\cdot 2 \qquad (4.1)$$

где k-постоянная Больцмана;

$T_{Я}$- яркостная температура Солнца в периоды максимальной активности;

D_F- полоса частот радиоизлучения;

W- телесный угол Солнца;

L- средняя длина волны.

W=0,00000005 мВт/см^2

Таким образом, рискнём утверждать, что уровень плотности потока мощности микроволнового излучения, сопоставимый с естественным фоном, явно безвреден для человека.

Теперь перейдём от естественных источников излучения к искусственно созданным человеком. Так, мощность передатчиков Останкинской телебашни достигает P=20 кВт. Усиление в максимуме диаграммы направленности антенн может составлять примерно G=10 дБ. Значение ППМ зависит от расстояния до Останкинской телебашни и формы диаграммы направленности излучающей антенны. В наиболее неблагоприятной зоне это значение на несколько порядков превышает естественный уровень:

$$W=P\cdot G(y)/4p\cdot R\cdot 2 \qquad (4.2)$$

W=0,0064 мВт/см^2

Другой пример- бытовая СВЧ печь. Её мощность обычно чуть меньше одного киловатта. Экранировку излучения печи, по-видимому, трудно обеспечить лучше 40-60 дБ. Располагается она, чаще всего, на кухне, и пока в ней что-то готовится, хозяйка вполне может находиться от неё на расстоянии, например, 0,3 м. Поскольку излучение (частота примерно 2450 МГц) в данном случае ненаправленное, то следует принять значение G не более 1 (или 0 дБ). При использовании приведённой выше формулы получается, что уровень излучения СВЧ-печи соизмерим с излучением от Останкинской телебашни.

Эти примеры ещё раз доказывают, что люди уже в течении многих лет непроизвольно проводят массовый эксперимент по изучению воздействия СВЧ полей на человека, но пока так и не обнаружили отрицательных для себя последствий при плотности потока мощности, менее сотых долей мВт/см^2.

Средства радиосвязи развиваются на протяжении уже почти столетия. Сотовый телефон стал массовым только в последнее десятилетие, и столь короткого промежутка времени явно не достаточно для того, чтобы делать выводы о его вреде или безвредности на основе широкомасштабного эксперимента над людьми. Исходные условия этого эксперимента таковы: мощность сотового телефона в момент соединения может достигать 2 Вт (для аналоговых стандартов и того больше), усиление антенны принимаем равным 1, расстояние до головы примерно 0.03м. Предположим, что мы имеем дело с частотами стандарта GSM 900/1800. Как следует из теории антенн, пользователь находится в дальней зоне излучения антенны своего сотового телефона (длина антенны примерно 1/4, а расстояние на котором сформировалась диаграмма направленности- 1/16). Возвращаясь к предыдущей формуле, получим, что в момент соединения W = 18 мВт/см^2, что

на несколько порядков превышает излучение и СВЧ печи и Останкинской башни. Хорошо, что соединение происходит достаточно быстро, а затем мощность падает почти на порядок, то есть в момент разговора W=2 мВт/см^2. Да и большинство абонентов стараются говорить не более 2-5 минут.

Ещё не так давно на заводах работа регулировщика СВЧ аппаратуры приравнивалась к вредному производству, а допустимая норма ППМ для полного рабочего дня составляла W = 0,01 мВт/см^2. При превышении этого уровня сокращался рабочий день. И хотя все эти льготы, к сожалению, в прошлом, норму уровня плотности потока мощности никто не отменял. Аналогичная по сути, но существенно большая по значению, норма была введена в США- W=10 мВт/см^2. В случае превышения этой нормы рабочий день сокращается. Например, в ВМС США была установлена норма допустимого времени работы в микроволновом поле (300-30000 МГц) повышенной интенсивности T<6000/W·2, где W не более 100мВт/см^2. Если ориентироваться на эту норму, то при W = 2 мВт/см^2, что соответствует излучению сотового телефона в режиме разговора, можно разговаривать по телефону почти круглосуточно.

В 1996 г. Федеральная комиссия по связи (FCC) США установила новые нормы на допустимый уровень ППМ при неконтролируемом использовании излучающих приборов, иными словами- для массового пользователя. Примерно в то же время аналогичные нормы были введены в Европе. Сегодня у нас установлен допустимый уровень ППМ применительно к сотовому телефону- 0,1 мВт/см^2, к базовой станции соты- не более 0,01 мВт/см^2. При этом учитывается, что базовая станция работает практически постоянно, а сотовым телефоном человек пользуется кратковременно.

Также существует норма допустимого облучения человека, выраженная в мощности электромагнитной волны (Вт), приходящейся на 1 кг живого веса- Specific Absorption Rate (SAR). Сегодня эта норма даже вводится для обязательного указания в паспорте сотового телефона. По данным компании Domode, которая опубликовала результаты тестирования более сотни типов сотовых телефонов различных компаний, значение SAR в основном лежит в пределах от 0,28 до 1,5 Вт/кг.

Отметим, что для специалистов, имеющих дело с микроволновым излучением в течении всего рабочего дня, установленные нормы в пять раз больше (предполагается, что на предприятиях налажен контроль уровня излучения).

Значение SAR позволяет оценить допустимый уровень ППМ электромагнитного поля, в котором может находится человек, или уровень ППМ на поверхности кожи:

$$W = r \cdot 10 \cdot (-aL) \cdot SAR \cdot M/S \qquad (4.3)$$

где r- коэффициент отражения по мощности (примерно 0,5);

M- масса тела человека, кг;

S- площадь поверхности тела, $м^2$;
aL- затухание в теле человека на глубине L, дБ.

Для взрослого человека примем M = 70 кг, S = 1 $м^2$. Исходя из допустимого значения SAR для всего тела, несложно получить примерное значение W = 0,28 $мВт/см^2$ при aL = 0. Это значение превышает установленные в России нормы ППМ, но допустимо для США и Европы.

Итак, вопрос о безопасности СВЧ излучения, так и остается дискуссионным уже более 50 лет. Учёные продолжают исследования, а телекоммуникационные компании развивают свою индустрию, где СВЧ излучение занимает далеко не последнее место [24].

4.2 Стандарты для электромагнитного излучения

Следующие независимые организации опубликовали рекомендации касательно электромагнитного излучения радиочастотного диапазона:

– Комитет координации стандартов № 28 при институте инженеров электротехники и электроники (IEEE- Institute of Electrical and Electronics Engineers);

– Комитет по национальной радиологической защите Великобритании- NRPB (National Radiological Protection Boards in the United Kingdom);

– Комитет неионизирующего излучения при ассоциации международной защиты от радиации (IRPA/INIRC- International Radiation Protection Association's International Non-Ionizing Radiation Committee) при поддержке международной организации здоровья (World Health Organization).

В сентябре 1992 года Комитет по Стандартам при IEEE одобрил стандарты IEEE для Уровней Безопасности с учетом воздействия на здоровье человека электромагнитных полей радиочастотного диапазона, 3 кГц до 300 ГГц, IEEE C95.1-1991. Эти Стандарты IEEE появились в результате обсуждения проблем беспроводных сетей с участием 120 биологов, биофизиков, физиологов, физиков, медиков, инженеров- представителей академий, федеральных агентств, отраслей промышленности и прочих заинтересованных организаций. В ноябре 1992 институт американских национальных стандартов одобрил стандарты IEEE C95.1-1991. В документе зафиксировано следующее положение: «Предположения об опасности воздействия электромагнитного излучения в пределах частот и коэффициента поглощения, указанных в предыдущих стандартах ANSI включая ANSI C95.1-1982 не подтвердились».

Измерения показали, что обычное электромагнитное излучение маломощных компактных и мобильных приемопередатчиков и сотовых телефонов не превышает максимально допустимые нормы поглощения энергии, указанные в этом руководстве.

Таким образом, основываясь на настоящих данных, излучения маломощных приемопередатчиков считаются безопасными для пользователей

(по материалам IEEE USAB о влиянии на человека радиочастотных полей от компактных и мобильных телефонов и прочих коммуникационных устройств, 2 декабря, 1992 года).

Результатом исследований в этой области стало единое мнение в отношении вопросов безопасности электромагнитного излучения. Результаты исследований нашли отражение в рекомендациях и стандартах, разработанных комиссиями экспертов, такими как научный комитет № 53 при NCRP, Комитет координации стандартов № 28 при IEEE, IRPA/INIRC и NRPB. Оборудование изготовлено с учетом этих стандартов и рекомендаций и, соответственно, считается безопасным для здоровья.

Широкомасштабные исследования на предмет безопасности электромагнитного излучения в радиочастотном диапазоне проводились в течение долгого времени. Результаты исследований постоянно пересматриваются научными комитетами, где и устанавливаются нормы безопасности. Производители беспроводного оборудования контролируют исследования и участвуют в установлении единых стандартов, обеспечивая функционирование своей продукции в соответствии с этими стандартами. Изготовители оборудования гарантируют безопасность своей продукции.

В беспроводной сети в каждый момент времени только один передатчик является активным, таким образом, мощность излучения всей сети, даже если она имеет 100 хостов, на самом деле эквивалентна мощности излучения одного передатчика. Передатчики беспроводных сетей имеют выходную мощность 0,035 Ватт (35 мВт) в диапазоне 2,4 ГГц, в зависимости от особенностей использования продукта и территориальных ограничений.

Оборудование беспроводных сетей использует пакетный режим передачи/приема, тогда как сотовая связь передает в эфир непрерывно. Например: если пользователь будет посылать информацию в среднем по 100 мегабайт в день, передатчик беспроводных ЛВС будет находиться в прямом эфире около 10 минут. Более того, обычный сотовый телефон имеет выходную мощность 0,600 Вт (600 мВт) или даже выше, что превышает мощность передатчика беспроводных ЛВС более чем в 20 раз [7].

4.3 Расчёт защитного заземления

Выбираем тип заземления в ряд. При этом заземлители располагаются в ряд вдоль длинной стены здания. Здание имеет следующие размеры: длина- 18 м, ширина- 9 м.

Ряд состоит из вертикально расположенных электродов- стальных труб, длиной $l_В$ = 3м, диаметром d = 50 мм, соединённых горизонтальной полосой.

В качестве горизонтального электрода применим стальную полосу сечением 40х4 мм. Глубина заложения электродов в землю t_0 = 0,5. Удельное сопротивление грунта $R_{уд}$ = 100 Ом·м. В качестве естественного заземлителя применяется железобетонная арматура сопротивлением R_E = 20 Ом.

Расчёт производим с учётом коэффициента использования.

Требуемое сопротивление растеканию заземлителя ПУЭ для электроустановок до 1000 В: $R \leq 4$ Ом, при $\rho \leq 100$ Ом·м.

Требуемое сопротивление неестественного заземлителя:

$$R_{ТР} = (R_E \cdot R_З)/(R_E - R_З) \quad (4.4)$$

$R_{ТР} = (20 \cdot 4)/(20-4) = 5$ Ом

Определяем сопротивление растекания тока от вертикального заземлителя по выражению:

$$R_В = 0{,}366 \cdot P_\rho / l \cdot (\lg(2 \cdot l/d) + 0{,}5 \cdot \lg(4 \cdot t+3 \cdot l)/(4 \cdot t+l)) \quad (4.5)$$

где P_ρ- расчётное значение удельного сопротивления грунта, определяемое по формуле:

$$P_\rho = \rho \cdot K_{C(В)} \quad (4.6)$$

где $K_{C(В)} = 1{,}4$- коэффициент сезонности вертикального заземлителя;

l- длина вертикального заземлителя, м;

d- диаметр вертикального стержня, м; t- расстояние от поверхности земли до середины вертикального заземлителя заглубленного в канаве, м;

$\rho = 100$ Ом·м.

$R_В = 0{,}366 \cdot 140/3(\lg(6/0{,}5) + 0{,}5 \cdot \lg(8+6)/(8+3)) = 19{,}33$ Ом

Используя полученное значение сопротивления вертикального заземлителя, определяем их приближённое число, которое необходимо для выполнения заземляющего устройства:

$$n = R_В/R_З \quad (4.7)$$

$n = 19{,}33/4 = 4{,}8 \approx 5$ шт

Составляем предварительную план-схему заземляющего устройства, т. е. размещаем вертикальные заземлители относительно места расположения объекта (приведена на рисунке 4.1).

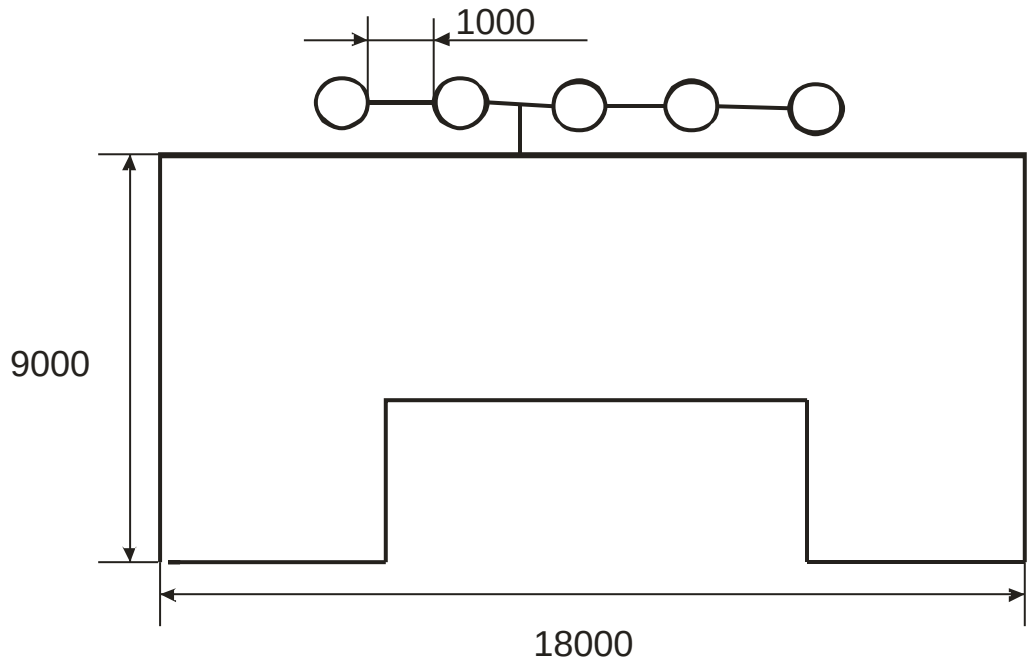


Рисунок 4.1- Предварительная схема заземляющего устройства

Определяем длину полосы $l_Г$. Так как принято расположение заземлителей в ряд, то:

$$l_Г = a\cdot(n - l) \qquad (4.8)$$

где а- расстояние между заземлителями, м.

Примем а = 1, следовательно:

$l_Г = 2$ м

Определяем сопротивление растеканию тока от полосы:

$$R_Г = 0{,}366\cdot P_\rho/l\cdot lg(2\cdot l^2/B\cdot h) \qquad (4.9)$$

где P_ρ- расчётное значение удельного сопротивления грунта;
B- ширина полосы, м;
h- глубина заложения в землю полосы, м.

Коэффициент сезонности принимается для горизонтального заземлителя равным 2,5.

$R_Г = 0{,}366\cdot 250/2\cdot lg(2\cdot 2^2/0{,}04\cdot 0{,}5) = 119{,}04$ Ом
Определим сопротивление заземляющего устройства:

$$R_З = R_В \cdot R_Г / (R_В \cdot \eta_Г + R_Г \cdot \eta_В \cdot n) \quad (4.10)$$

где $\eta_В$, $\eta_Г$- коэффициенты использования вертикальных и горизонтальных заземлителей, $\eta_В = 0,74$, $\eta_Г = 0,67$.

$R_З = 19,33 \cdot 119,04/(19,33 \cdot 0,67 + 119,04 \cdot 0,74 \cdot 5) = 5,07$ Ом

Расчёт заканчивается, если полученное сопротивление равно допустимому или незначительно меньше его. $R_{ТР}$= 5 Ом, $R_Р$=5,07 Ом, ; $R_{ТР} \approx R_Р$.

4.4 Молниезащита антенн

Молния является мощным поражающим фактором. Прямой удар молнии приводит к механическим разрушениям зданий, сооружений, скал, деревьев, вызывает пожары и взрывы, является прямой или косвенной причиной гибели людей. Механические разрушения вызываются мгновенным превращением воды и вещества в пар высокого давления на путях протекания тока молнии в названных объектах. Прямой удар молнии называют первичным воздействием атмосферного электричества. К вторичному воздействию атмосферного электричества относят: электростатическую и электромагнитную индукции; занос высоких потенциалов в здания и сооружения.

Рассмотрим опасные факторы вторичного воздействия атмосферного электричества. Образовавшийся электростатический заряд облака наводит заряд противоположного знака на предметах, изолированных от земли (оборудование внутри и вне зданий, металлические крыши зданий, провода ЛЭП, радиосети, антенны и т.п.). Эти заряды сохраняются и после удара молнии. Они исчезают путём электрического разряда на ближайшие заземлённые предметы, что может вызвать электротравматизм людей, воспламенение горючих смесей и взрывы. В этом заключается опасность электростатической индукции. Явление электромагнитной индукции заключается в следующем. В канале молнии протекает очень мощный и быстро изменяющийся во времени ток. Он создаёт мощное переменное во времени магнитное поле. Такое поле индуцирует в металлических контурах электродвижущую силу разной величины. В местах сближения контуров между ними могут происходить электрические разряды, способные воспламенить горючие смеси и вызвать электротравматизм [18,19].

Занос высоких потенциалов в здание происходит в результате прямого удара молнии в металлокоммуникации, расположенные на уровне земли или над ней вне зданий, но входящие внутрь зданий. Здесь под металлокоммуникациями понимают рельсовые пути, водопроводы, газопроводы, провода ЛЭП, антенны и т.п. Занесение высоких потенциалов внутрь здания сопровождается электрическими разрядами на заземлённое

оборудование, что также может привести к воспламенению горючих смесей и электротравматизму людей.

Требуемая степень защиты зданий, сооружений и открытых установок от воздействия атмосферного электричества зависит от взрывопожароопасности названных объектов и обеспечивается правильным выбором категории устройства молниезащиты и типа зоны защиты объекта от прямых ударов молнии.

Степень взрывопожароопасности оценивается по классификации Правил Устройства Электроустановок (ПУЭ). Инструкция по проектированию и устройству молниезащиты СН 305-77 устанавливает три категории устройства молниезащиты (I, II, III) и два типа (А и Б) зон защиты объектов от прямых ударов молнии. Зона защиты типа А обеспечивает перехват на пути к защищаемому объекту не менее 99,5 % молний, а типа Б- 95 %.

По I категории организуется защита объектов, относимых по классификации ПУЭ к взрывоопасным зонам классов В-I и В-П. Зона защиты для всех объектов (независимо от места расположения объекта и от интенсивности грозовой деятельности в месте расположения) применяется только типа А.

По II категории осуществляется защита объектов, относимых по классификации ПУЭ взрывоопасным зонам классов В-1а, В-16, В-Па. Тип зоны защиты при расположении объектов в местностях со средней грозовой деятельностью 10 часов и более в год определяется по расчётному количеству N поражений объекта молнией в течении года:

- при $N \leq 1$ достаточна зона защиты типа Б;
- при $N > 1$ должна обеспечиваться зона защиты типа А.

Для наружных технологических установок и открытых складов, относимых ПУЭ к зонам класса В-I г, принимается зона защиты типа Б.

По III категории организуется защита объектов, относимых по ПУЭ к пожароопасным зонам классов П-1, П-2, П-2а. При расположении объектов в местностях со средней грозовой деятельностью 20 часов и более в год и при $N > 2$ должна обеспечиваться зона защиты типа А, в остальных случаях типа Б. По III категории осуществляется также молниезащита общественных и жилых зданий, башен, вышек, труб, предприятий, зданий и сооружений сельскохозяйственного назначения. Тип зоны защиты этих объектов определяется в соответствии с указаниями СН 305-77.

Объекты I и II категорий устройства молниезащиты должны быть защищены от всех четырёх видов воздействия атмосферного электричества, а объекты III категории- от прямых ударов молнии и от заноса высоких потенциалов внутрь зданий и сооружений.

Защита от электростатической индукции заключается в отводе индуцируемых статических зарядов в землю путём присоединения металлического оборудования, расположенного внутри и вне зданий, к специальному заземлителю или к защитному заземлению электроустановок;

сопротивление заземлителя растеканию тока промышленной частоты должно быть не более 10 Ом.

Для защиты от электромагнитной индукции между трубопроводами и другими протяжёнными металлокоммуникациями в местах их сближения на расстояние 10 см и менее через каждые 20 м устанавливают (приваривают) металлические перемычки, по которым наведённые токи перетекают из одного контура в другой без образования электрических разрядов между ними.

Защита от заноса высоких потенциалов внутрь зданий обеспечивается отводом потенциалов в землю вне зданий путём присоединения металлокоммуникации на входе в здания к заземлителям защиты от электростатической индукции или к защитным заземлениям электроустановок.

Для защиты объектов от прямых ударов молнии сооружаются молниеотводы, принимающие на себя ток молнии и отводящие его в землю [16]. Так как объектом защиты является штыревая антенна с опорой, то достаточно будет использовать одиночный стержневой молниеотвод. При использовании одиночного стержневого молниеотвода можно определить его высоту, задаваясь радиусом r_x на высоте защищаемого объекта h_x:

$$H = (r_x + 1{,}63 \cdot h_x)/1{,}5 \qquad (4.11)$$

Зададимся радиусом r_x = 3м, достаточным для защиты данного объекта.
h_x = 2,1 м- высота антенны вместе с опорой.

$H = (3 + 1{,}63 \cdot 2{,}1)/1{,}5 = 4{,}3$ м.

5 Бизнес план

Рассчитываем капитальные затраты на приобретение оборудования, доставку, его монтаж и настройку (таблица 5.1).

Таблица 5.1- Капитальные затраты на станционное оборудование

№ п/п	Наименование работ и затрат	Единицы измерения	Количество, шт.	Сметная стоимость, тг	
				за единицу	общая
1	Маршрутизатор	тг.	10	88960	889600
2	Omni-5.3-10	тг.	1	33280	33280
3	ANT-5.2-24	тг.	9	15360	138240
4	MANUS-5202	тг.	1	115200	115200
5	Покупка автомобиля и измерительных приборов	тг.	1		1600000
6	Затраты на изготовление, монтаж и доставку опор под антенны	тг.	10		1900000
	Итого	тг.			4676320

Капитальные затраты составляют: К=4676320 тг.

Рассчитываем годовые эксплуатационные расходы по формуле [20]:

$$C_{экс}=C_{ФОТ} + C_{соц.\ налог}+ C_{эл.}+ C_{мат.}+ C_{ам}+ C_{нал.}+ C_{проч.} \quad (5.1)$$

где $C_{ФОТ}$ - фонд оплаты труда, тг.;
$C_{соц.\ налог}$- отчисления на социальный налог, тг.;
$C_{эл}$- затраты на электроэнергию, тг.;
$C_{мат}$- расходы на материалы, тг.;
$C_{ам}$- амортизационные отчисления, тг.;
$C_{нал}$- налог на имущество, тг;
$C_{проч.}$- прочие расходы, тг.

Расчет фонда оплаты труда приведен в таблице 5.2.

Таблица 5.2- Расчет фонда оплаты труда

Должность	Количество человек	Разряд	Тарификационный коэффициент	Должностной оклад, тг	Сумма за год, тг.
Администратор сети	1	12	4,99	48877	703829
Инженер 1 категории	1	11	4,54	44469	640354
Водитель	1	4	3,10	30364	437242
Итого				123710	1781425

Фонд оплаты труда составляет: $C_{ФОТ}$=1781425 тг.

Отчисления на социальный налог составляют 20 % фонда оплаты труда:

$$C_{соц.\ налог} =0,2\cdot C_{ФОТ} \quad (5.2)$$

$C_{соц.\ налог}$ =0,2·1781425= 356285 тг.

Затраты на электроэнергию $C_{эл.}$ равны:

$$C_{эл.} = W\cdot N_{час}\cdot N_{сут}\cdot N_{мес}\cdot Э_1 \quad (5.3)$$

где W - мощность потребляемая оборудованием в час, 0,5 кВт; $N_{час}$- количество часов в сутки, 24 час.; $N_{сут}$- количество суток в месяце, 30 сут.; $N_{мес}$- количество месяцев в году, 12 мес.; $Э_1$- стоимость 1 кВт·часа электроэнергии, 5,2 тг.

$C_{эл.}$ = 0,5·24·30·12·5,2= 22464 тг.

Расходы на материалы $C_{мат.}$ состоят из стоимости материала на подключение к сети (М) и стоимости топлива на транспортные передвижения (Т).

$$M=M_1 \cdot N_т \quad (5.4)$$

где M_1- стоимости материала на одну точку подключения, 46 тг.; $N_т$- количество точек подключения, 10 точек.

$M=46 \cdot 10=460$ тг.

$$T=E_1 \cdot 253 \cdot 12 \cdot N_1/100 \cdot 12 \quad (5.5)$$

$T=110 \cdot 253 \cdot 12 \cdot 1/100 \cdot 12=40080$ тг.

$C_{мат.}=460+40080=40540$ тг.

Амортизационные отчисления составляют 20 % от суммы капитальных затрат:

$$C_{ам}=0,2 \cdot K \quad (5.6)$$

$C_{ам}= 0,2 \cdot 4676320= 935264$ тг.

Налог на имущество составляет 1 % от остаточной стоимости:
$4676320- 935264 = 3741056 \cdot 0,01 = 37410$ тг.

Плата за лицензию (использование радиочастотных ресурсов) в год:

$П_{лиц} = 20000 \cdot 12= 240000$ тг.

Прочие расходы составляют 4 % от выше перечисленных затрат:

$C_{проч} =3413388 \cdot 0,04= 136535$ тг.

Расчетные значения эксплуатационных затрат сведена в таблицу 5.3.

Таблица 5.3- Эксплуатационные расходы

№ п/п	Наименование показателей	Ед. изм.	Сумма за месяц	Сумма за год	Удельный вес в %
1	Фонд оплаты труда	тг.	123710	1781425	50,1
2	Социальный налог	тг.	29690	356285	10
3	Эл. энергия	тг.	1872	22464	0,6
4	Материалы Топливо	тг. тг.	460 3340	460 40080	1,14
5	Амортизационные отчисления	тг.	77938	935264	26,3
6	Налог на имущество	тг.		37410	1
7	Плата за лицензию (использование радиочастотных ресурсов)	тг.	20000	240000	6,7
8	Прочие расходы	тг.	8951	136535	3,8
	Всего эксплуатационных расходов за год	тг.		3549923	100

Эксплуатационные расходы составляют: $С_{экс}$= 3549923 тг.

Доходы данного проекта условные, так как экономию затрат на использование телефонной линии примем за доходы. Виды доходов приведены в таблице 5.4.

Таблица 5.4- Условные доходы

№	Наименование доходов	Сумма доходов за месяц, тг	Сумма доходов за год, тг.
1	Плата за подключение		94341
2	Ежемесячная абонентная плата	63661	763932
	Итого		858273х10= 8582730

Плата за подключение включает предоставление модема со встроенным маршрутизатором и организацию соединительной линии.

Прибыль определяем разницей между доходами от основной деятельности (без НДС) и эксплуатационными расходами:

$$П = Д_{осн.\ деят.} - С_{экс.} \quad (5.7)$$

П = 8582730 - 3549923 = 5032807 тг.

Рентабельность определяем по формуле:

$$Р = П/С_{экс} \cdot 100\ \% \quad (5.8)$$

$P = 5032807/3549923 \cdot 100 = 141,7\ \%$

Срок окупаемости проекта определяем по формуле:

$$Т_{кп} = К/П \qquad (5.10)$$

$Т_{кп} = 4676320/5032807 = 0,9$ года.

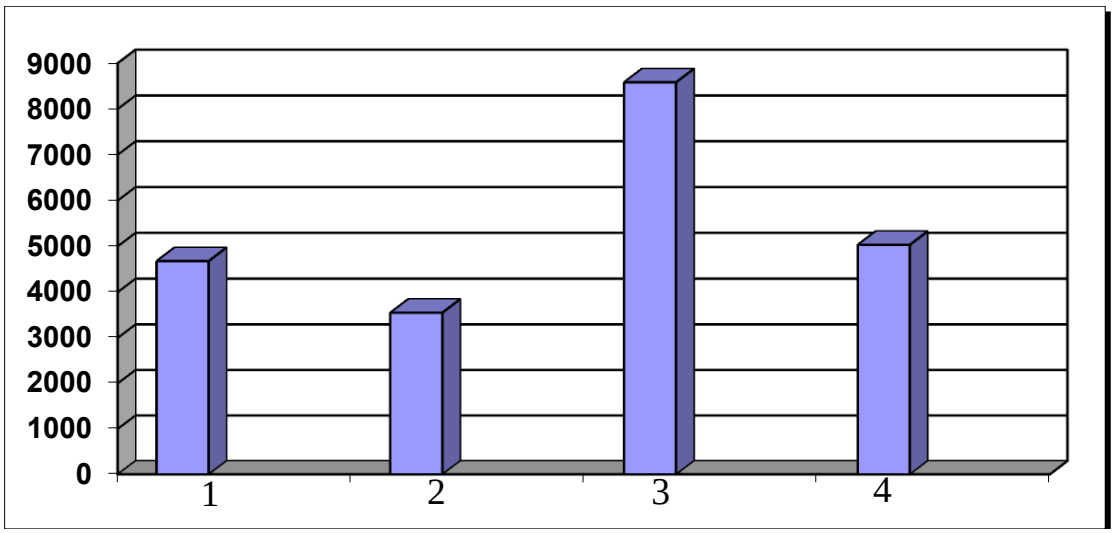
Таблица технико- экономических показателей проекта приведена в таблице 5.5, диаграмма экономических показателей проекта приведена на рисунке 5.1.

Таблица 5.5- Экономические показатели проекта

Название показателей	Единицы измерения	Значения
Капитальные затраты	тыс. тг.	4676,32
Эксплуатационные расходы	тыс. тг.	3549,923
Доходы	тыс. тг.	8582,73
Прибыль	тыс. тг.	5032,807
Срок окупаемости	лет	0,9

Технико- экономическое обоснование проекта показывает его эффективность и окупаемость- срок окупаемости проекта составляет меньше одного года.

Значение, тыс. тг.



Показатель

1- Капитальные вложения
2- Эксплуатационные расходы
3- Доходы
4- Прибыль

Рисунок 5.1- Диаграмма экономических показателей проекта

Заключение

Проектирование беспроводной сети имеет следующие главные цели:

- обеспечение требуемого территориального охвата;
- достижение требуемой скорости и канальной емкости с эффективным использованием радиоспектра;
- достижение высокого качества обслуживания;
- доведение до минимума количества сетевых элементов и оптимизация издержек на сеть.

Проектирование беспроводной сети является, на самом деле, процессом, направленным на нахождение оптимального равновесия между противоречивыми требованиями. Например, для обеспечения идеальной зоны уверенного приёма проектировщику требуется предусмотреть соответствующее количество сетевых элементов, что, с другой стороны, может обойтись слишком дорого для оператора. Поэтому, нахождение правильного равновесия между этими требованиями крайне важно и здесь необходимо иметь опыт и хорошие знания о местном рынке.

Проектирование беспроводной сети решает следующие задачи на разных этапах этого процесса:

- расчёт сетевых элементов на этапе планирования;
- проектирование сети и измерения на этапе развёртывания строительства;
- проверка сети (проверка качества) и оптимизация сети на этапе опытной эксплуатации;
- регулярное тестирование и настройка в период эксплуатации;
- проектирование этапов расширения.

Анализ проектирования таких сетей в разных странах, показывает, что большая часть работ по проектированию продолжается вестись и после пуска сети, даже на этапе уже самой эксплуатации. Многие ключевые факторы качества сети тесно связаны с проектированием. Так как клиенты сетей требуют всё более высокого качества, а конкуренция за рынок ожесточается, операторы просто не могут позволить себе принимать плохо спроектированную сеть. Поэтому инвестиции в более хорошее и тщательное проектирование сети необходимы и обещают в перспективе значительную отдачу.

В заключение хотелось бы отметить, что спроектированная беспроводная сеть передачи данных между бизнес-центрами гостиничных комплексов г. Алматы полностью удовлетворит всем требованиям гостиниц по качеству и объему передаваемых данных.

Список литературы

1 Закон РК «О связи».- Астана: 2004, № 567- 158 с.

2 Закон РК «Об охране труда» от 11.12. 2000 года за № 298- 105 с.

3 Закон РК «Об охране окружающей среды» от 22 января 1993 года за № 1915-12- 75 с.

4 Казахская энциклопедия.- Алматы, 2002- 160 с.

5 Радиорелейные и спутниковые системы передачи. Под ред. А.С. Немировского.- М.: Радио и связь, 1985- 215 с.

6 Фалько А.И. Основы радиоприёма: Учебное пособие.- Новосибирск: СибГУТИ, 2005- 186 с.

7 Денисьева О.М., Мирошников Д.Г. Средства связи для последней мили.- М.: Эко-Трендз, 2000- 350 с.

8 Радиооборудование СЦИ серии 2000S: Учебные материалы в 5 томах.

9 Цыбаев Б.Г., Романов Б.С. Антенны-усилители.- М.: Советское радио, 1980- 280 с.

10 Шередько Е. Ю. Распространение радиоволн и антенно-фидерные устройства.- М.: Связь, 1976- 340 с.

11 Аграновский К.Ю., Златогурский Д.Н. Радиотехнические системы.- М.: Высшая школа, 1979- 432 с.

12 Гоноровский И.С. Радиотехнические цепи и сигналы. 4-е издание.- М.: Радио и связь, 1986- 356 с.

13 Семенов К.Л. Проводные и беспроводные современные технологии связи // Connect! Мир связи.- 2002.- № 6.- с. 15-25.

14 Бакеев Д.Р. Нашествие беспроводных технологий // Информ курьер связь. 2002.- № 11.- с. 15-18.

15 Журавлев В.В. Системы беспроводных технологий // Дискавери».- 1995.- № 8.- с. 39-45.

16 Нормативные документы (СН 305-77. Инструкция по проектированию и устройству молниезащиты).

17 Правила устройства электроустановок (ПУЭ).- М.: Энергоатомиздат, 1997- 430 с.

18 Долин П.А. Основы техники безопасности в электроустановках.- М.: Энергоатомиздат, 1979- 267 с.

19 Щуко Л.П. Справочник по охране труда.- М.: Энергоатомиздат, 2002 220 с.

20 Горелик Р.А., Голубицкая Е.А. Основы экономики предприятий телекоммуникаций.- М.: Радио и связь, 1997- 324 с.

21 http://www.comptek.ru

22 http://www.apc.ru/ Компания APC.

23 http://www.ccc.ru/ Сети и системы связи.

24 http://www.ezop.ru/ Электроэнергетика, защита от помех.

25 http://www.iso.com/ Международная организация по стандартизации.

26 http://www.itu.ru/ Международный союз электросвязи.

27 http://www.mis.ru/ Компания МИС- информаналитика в области телекоммуникаций.

28 http://www.ops.ru/ Издательство «Открытые системы».

Приложение А
Перечень терминов и сокращений

3G- Third Generation (третье поколение)
AP- Access Point (точка доступа)
Ad Hoc- одноранговая сеть
Bluetooth- технология коротковолновой радиосвязи (2,4 ГГц)
CCK- Complementary Code Keying
CSMA/CD- Carrier Sence Multiple Access with Collision Detection
DECT- Digital Enhanced Cordless Telecommunications
DSSS- Direct Sequence Spread spectrum
DCF- Distributed Coordination Function
EAP- Enhanced Authorization Protocol
GPRS- General Packet Radio Service (пакетная радиосвязь общего назначения)
Hot Spot- (хот-спот) точка беспроводного публичного доступа
IEEE- Institute of Electrical and Electronics Engineers
IKE- Internet Key Exchange
Infrastructure Mode- режим работы Infrastructure (с точкой доступа)
IP- Internet Protocol
IPSec- IP Security
LLC- Logical Link Control (управление логическим каналом)
LMDS- Local Multipoint Distribution Service
MAC- Media Access Control (управление доступом к среде)
MMDS- Multichannel Multipoint Distribution Service
NAT- Network Address Translation
OFDM- Orthogonal Frequency Division Multiplexing
OSI- Open Systems Interconnection (взаимодействие открытых систем)
PDA- Personal Digital Assistants
PSK- Pre-Shared Key
QPSK- Quadrature Phase Shift Keying (квадратурная фазовая манипуляция)
RADIUS- Remote Authentication Dial In User Service
SSID- Service Set Identifier
QAM- Quadrature Amplitude Modulation (квадратурная амплитудная модуляция)
TKIP- Temporal Key Integrity Protocol
TCP- Transmission Control Protocol (протокол управления передачей)
UDP- User Datagram Protocol (протокол пользовательских дайтаграмм)
VPN- Virtual Private Network (виртуальная частная сеть)
WAN- Wide Area Network (глобальная сеть)
WEP- Wired Equivalent Privacy
Wi-Fi- Wireless Fidelity
WLAN- Wireless Local Area Network (беспроводная локальная сеть)