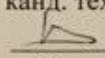



ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ МОРДОВСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМ. Н. П. ОГАРЁВА»

Институт электроники и светотехники
Кафедра инфокоммуникационных технологий и систем связи

УТВЕРЖДАЮ
Зав. кафедрой ИКТСС
канд. техн. наук, доц.
 В.В. Никулин
« 10 » июня 2019 г.

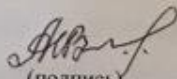
БАКАЛАВРСКАЯ РАБОТА

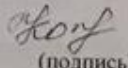
**ПРОЕКТИРОВАНИЕ БЕСПРОВОДНОЙ СЕТИ ШИРОКОПОЛОСНОГО
ДОСТУПА В ПРОЛЕТАРСКОМ РАЙОНЕ Г. САРАНСКА
НА ОСНОВЕ ТЕХНОЛОГИИ Wi-Fi**

Автор бакалаврской работы  (подпись) 10.06.19. (дата) А. И. Наумов
инициалы, фамилия

Обозначение работы БР-02069964-11.03.02-14-19

Направление 11.03.02 Инфокоммуникационные технологии и системы связи

Руководитель работы  (подпись) 10.06.19. (дата) А. С. Иванцев
канд. физ-мат. наук, доц. инициалы, фамилия


Нормоконтролер  (подпись) 10.06.19. (дата) Е. А. Кошечкина
канд. культурологии, доц. инициалы, фамилия

Саранск

2019

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ МОРДОВСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. Н. П. ОГАРЁВА»

Институт электроники и светотехники
Кафедра инфокоммуникационных технологий и систем связи

УТВЕРЖДАЮ
Зав. кафедрой ИКТСС
канд. техн. наук, доц.
 В.В. Никулин
« 14 » 12 2019 г

ЗАДАНИЕ НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ

Студент: Наумов Андрей Игоревич

1 Тема «Проектирование беспроводной сети широкополосного доступа в Пролетарском районе г. Саранска на основе технологии Wi-Fi»

Утверждена приказом № 10335-с от 14 декабря 2018 года

2 Срок представления проекта к защите 10 июня 2019 года

3 Исходные данные для выпускной квалификационной работы 1) беспроводная сеть ПД; 2) количество абонентов: 100; 3) район проектирования: г. Саранск, Пролетарский район

4 Содержание выпускной квалификационной работы

4.1 Принципы функционирования сетей беспроводного доступа

4.2 Технико-экономическое предложение

4.3 Проектирование сети беспроводного доступа

4.4 Технико-экономическое обоснование бакалаврской работы

5 Перечень графического материала

5.1 Принципы функционирования сетей беспроводного доступа

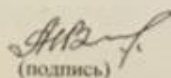
5.2 Частотно-территориальный план

5.3 Структурная схема проектируемой сети

5.4 Характеристики оборудования

5.5 Схема аутентификации пользователей


Руководитель проекта
канд. физ-мат. наук, доц.


(подпись)

17.12.18.
(дата)

А. С. Иванцев
инициалы, фамилия

Задание принял к исполнению


(подпись)

17.12.18
(дата)

А. И. Наумов
инициалы, фамилия

РЕФЕРАТ

Бакалаврская работа содержит 79 страницы, 25 рисунков, 13 таблиц, 11 использованных источников.

СЕТЬ БЕСПРОВОДНОГО ДОСТУПА, КОММУТАТОР, БАЗОВАЯ СТАНЦИЯ, АНТЕННА, АДАПТЕР, КАБЕЛЬ, ИНТЕРНЕТ.

Объектом исследования является сеть беспроводного доступа на основе беспроводного оборудования 2.4 ГГц (IEEE 802.11n).

Цель работы – проектирование беспроводной сети в Пролетарском районе г. Саранске, предназначенной для беспроводного доступа к информационным ресурсам сети Internet и Региональной Сети Передачи Данных (Intranet).

Метод исследования – анализ оборудования для проектирования сети беспроводного доступа.

Полученные результаты – изучен принцип работы стандарта IEEE 802.11, разработана структурная схема сети, а также произведены расчеты затухания антенно-фидерного тракта, эффективной изотропно-излучаемой мощности, энергетического запаса радиоканала для сети беспроводного доступа г. Саранска на основе беспроводного оборудования 2.4 ГГц (IEEE 802.11n).

Степень внедрения – данная работа носит в основном научно-исследовательский характер. Однако разработанные принципы могут быть использованы при проектировании реальных задач.

Область применения: для предоставления беспроводного доступа к информационным ресурсам сети Internet и Региональной Сети Передачи Данных (Intranet) корпоративных и индивидуальных пользователей, объединения корпоративных сетей в единую сеть.

БР-02069964-11.03.02-14-19								
<i>Изм.</i>	<i>Лист</i>	<i>№ Докум.</i>	<i>Подпись</i>	<i>Дата</i>	Проектирование беспроводной сети широкополосного доступа в Пролетарском районе г. Саранска на основе технологии Wi-Fi	<i>Лит.</i>	<i>Лист</i>	<i>Листов</i>
<i>Разраб.</i>		<i>Наумов</i>	<i>Наумов</i>	<i>10.06.09</i>				
<i>Провер.</i>		<i>Иванцев</i>	<i>Иванцев</i>	<i>10.06.09</i>			4	79
<i>Н.Контр.</i>		<i>Кошечкина</i>	<i>Кошечкина</i>	<i>10.06.09</i>		ИЭС, ИКТСС гр. 431		
<i>Утверд.</i>		<i>Никитин</i>	<i>Никитин</i>	<i>10.06</i>				

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	7
1 Принципы функционирования сетей беспроводного доступа	9
1.1 Анализ существующих беспроводных технологий	9
1.2 Стандарт IEEE 802.11	11
1.2.1 Обзор существующих стандартов семейства IEEE 802.11	11
1.2.2 Технологии расширения спектра	17
1.2.3 Режимы работы стандарта IEEE 802.11	21
1.2.4 Механизм доступа к среде	24
1.2.5 Физический уровень (Physical layer) стандарта IEEE 802.11	25
1.2.6 Канальный уровень (Data Link layer) стандарта IEEE 802.11	26
1.2.7 Организация микросотовых сетей	27
1.3 Безопасность беспроводных сетей	29
1.4 Частотное регулирование для беспроводных сетей	33
2 Технико-экономическое предложение	36
2.1 Точка доступа	38
2.2 Антенно-фидерное устройство	40
2.3 Коммутатор Ethernet	45
2.4 Аппаратно-программные средства	46
2.5 Бесперебойное питание	47
2.6 Оконечное оборудование абонента	48
3 Проектирование сети беспроводного доступа	53
3.1 Частотно-территориальное планирование	53
3.2 Структурная схема проектируемой сети	55
3.2.1 Беспроводной клиент	59
3.2.2 Точка доступа	60
3.2.3 Коммутатор	62
3.2.4 Подсистема мониторинга и управления	62
3.2.5 Кэширующий сервер	63
3.2.6 Биллинговая система	64

					БР – 02069964 – 11.03.02 – 14 – 19	Лист
Изм.	Лист	№ докум.	Подпись	Дата		5

3.3	Аутентификация пользователей	65
3.4	Антенно-фидерная система	67
3.5	Электропитание	69
3.6	Заземление и молниезащита	69
3.7	Оценка сделанных предложений	70
3.7.1	Расчет затухания на АФТ	71
3.7.2	Расчет эффективной изотропно-излучаемой мощности	71
3.7.3	Расчет суммарного усиления радиосистемы	72
3.7.4	Расчет дальности работы беспроводного канала связи	73
3.7.5	Расчет суммарных потерь радиосистемы	75
3.7.6	Расчет энергетического запаса радиоканала	75
4	Технико-экономическое обоснование бакалаврской работы	76
4.1	Расчет капитальный затрат	76
	ЗАКЛЮЧЕНИЕ	78
	СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	79

ВВЕДЕНИЕ

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

На современном этапе развития сетевых технологий, технология беспроводных сетей Wi-Fi является наиболее удобной в условиях требующих мобильность, простоту установки и использования. Wi-Fi (от англ. wireless fidelity – беспроводная связь) – стандарт широкополосной беспроводной связи семейства 802.11 разработанный в 1997 г. Именно благодаря этой технологии Интернет становится мобильным и дает пользователю свободу перемещения.

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

- простота развёртывания;
- гибкость архитектуры сети, когда обеспечивается возможность динамического изменения топологии сети при подключении, передвижении и отключении мобильных пользователей без значительных потерь времени;
- быстрота проектирования и реализации, что критично при жестких требованиях к времени построения сети;
- так же, беспроводная сеть не нуждается в прокладке кабелей (часто требующей дробления стен).

В то же время беспроводные сети на современном этапе их развития не лишены серьёзных недостатков. Прежде всего, это зависимость скорости соединения и радиуса действия от наличия преград и от расстояния между приёмником и передатчиком. Один из способов увеличения радиуса действия беспроводной сети заключается в создании распределённой сети на основе нескольких точек беспроводного доступа, а использование внешних направленных

					<i>БР – 02069964 – 11.03.02 – 14 – 19</i>	<i>Лист</i>
<i>Изм.</i>	<i>Лист</i>	<i>№ докум.</i>	<i>Подпись</i>	<i>Дата</i>		7

антенн позволяет эффективно решать проблему препятствий, ограничивающих сигнал [1].

Технологии беспроводного доступа находят все более широкое применение в современном обществе. Для РФ и Приволжского федерального округа в частности при недостаточно развитой кабельной инфраструктуре, сложной топографии удаленных районов и возникающими трудностями с прокладкой традиционных кабельных сетей, развитие беспроводных сетей является одной из наиболее актуальных.

Сегодня беспроводные сети активно создаются и используются практически во всех крупных городах страны: Москве, Екатеринбурге, Тольятти, Тюмени, Сургуте, Краснодаре, Нижнем Новгороде. Сооружаются сети в Новосибирске, Самаре, Иркутске, Кургане, Ростове и в других крупных региональных центрах.

Целью данной работы является проектирование сети беспроводного доступа в Пролетарском районе г. Саранска, с целью повышения уровня информатизации, предоставления современных услуг связи: высокоскоростной доступ в Интернет на базе технологии Wi-Fi.

					<i>БР – 02069964 – 11.03.02 – 14 – 19</i>	<i>Лист</i>
<i>Изм.</i>	<i>Лист</i>	<i>№ докум.</i>	<i>Подпись</i>	<i>Дата</i>		8

1 Принципы функционирования сетей беспроводного доступа

Беспроводные технологии стремительно завоевывают мир со скоростью и широтой охвата, превосходящими все ожидания. В последнее время мы наблюдаем все возрастающий интерес операторов, корпоративных пользователей и обычных людей к новым возможностям беспроводных технологий и сетей. Индустрия «мобилизации и беспроводизации всего и вся» очень быстро развивается и проникает в нашу повседневную реальность. То, что недавно казалось практически невозможным и фантастичным, воспринимается как само собой разумеющееся [2].

1.1 Анализ существующих беспроводных технологий

Для решения вопроса, какую технологию построения сети беспроводного доступа использовать в рамках данного дипломного проекта, необходимо иметь четкое представление о функциональной реализации имеющихся технологий, их преимуществах и недостатках.

Современные беспроводные технологии условно можно разбить на несколько типов (рисунок 1.1).

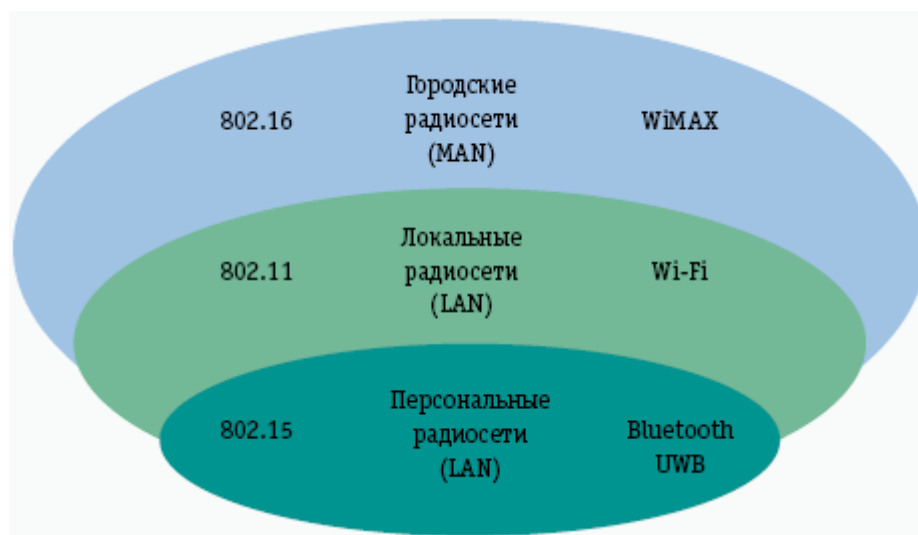


Рисунок 1.1 – Стандарты беспроводного соединения

Наиболее «короткодействующие», предназначенные для связи оборудования в пределах рабочего места, например, связи сотового телефона и ноутбука или компьютера и принтера, относят к классу персональных беспроводных сетей (Wireless Personal Area Network, WPAN). Наиболее распространенная технология из этой категории – Bluetooth. Эта технология имеет типичный радиус действия до 10 м и скорость передачи информации до 1 Мбит/с. Очевидно, что такие сети обслуживаются самим пользователем или системным (сетевым) администратором без привлечения телекоммуникационного оператора.

Следующим по «дальности» типом беспроводных коммуникаций являются беспроводные локальные сети (Wireless Local Area Network, WLAN), которые также называют Wi-Fi сетями – по названию ассоциации (форума) производителей соответствующего этой технологии оборудования – Wireless Fidelity. Основное предназначение таких систем, отвечающим стандартам семейства 802.11 – развертывание беспроводных сетей внутри помещений, хотя не исключено их использование на открытых площадках. Типовые дальности связи между отдельными устройствами сетей стандарта 802.11 обычно не превышают 100 м, однако при использовании специальных усилителей мощности для передатчиков и направленных антенн предельные дальности могут составлять до десятков км. Базовая услуга – доступ в Internet или корпоративную сеть [3].

Для построения распределенных беспроводных операторских сетей масштаба города (Wireless Metropolitan Area Networks, WMAN) или крупных корпоративных сетей используют оборудование, относящееся к классу фиксированного широкополосного беспроводного доступа (Fixed Broadband Wireless Access, FBWA). Характерный радиус действия базовой станции – до 10 км. К этой категории относится оборудование семейства стандартов 802.16, которое сертифицирует WiMAX форум.

Главное при развертывании беспроводной сети – это полностью определить предъявляемые к системе требования и выбрать ту технологию, которая наилучшим образом этим требованиям соответствует.

Все более широкое распространение в стране приобретает технология

					БР – 02069964 – 11.03.02 – 14 – 19	Лист
Изм.	Лист	№ докум.	Подпись	Дата		10

Wi-Fi – ее применяют как проводные, так и беспроводные операторы для обеспечения покрытия территории и привлечения в свою сеть новых пользователей. Технология в равной степени актуальна как для городов-миллионеров, так и для небольших городов. Поэтому в рамках дипломного проекта при проектировании сети беспроводного доступа в городе Саранск будем использовать именно эту технологию.

1.2 Стандарт IEEE 802.11

Институт инженеров по электротехнике и электронике (Institute of Electrical and Electronics Engineers, IEEE) сформировал рабочую группу по стандартам для беспроводных локальных сетей 802.11 в 1990 году. Эта группа занялась разработкой всеобщего стандарта для радиооборудования и сетей, работающих на частоте 2,4 ГГц со скоростями доступа 1 и 2 Мбит/с. Работы по созданию стандарта были завершены через 7 лет, и в июне 1997 года ратифицирована первая спецификация 802.11. Стандарт IEEE 802.11 являлся первым стандартом для продуктов WLAN от независимой международной организации, разрабатывающей большинство стандартов для проводных сетей.

Однако к тому времени заложенная первоначально скорость передачи данных в беспроводной сети уже не удовлетворяла потребностям пользователей. Для того, чтобы сделать технологию Wireless LAN популярной, дешёвой, а главное, удовлетворяющей современным жёстким требованиям бизнес-приложений, разработчики были вынуждены создать новый стандарт.

1.2.1 Обзор существующих стандартов семейства IEEE 802.11

В настоящее время существует множество стандартов семейства IEEE 802.11:

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

					БР – 02069964 – 11.03.02 – 14 – 19	Лист
Изм.	Лист	№ докум.	Подпись	Дата		11

2) 802.11a – высокоскоростной стандарт WLAN. Поддерживает передачу данных со скоростями до 54 Мбит/с по радиоканалу в диапазоне около 5 ГГц;

3) 802.11b – самый распространенный стандарт. Поддерживает передачу данных со скоростями до 11 Мбит/с по радиоканалу в диапазоне около 2,4 ГГц;

4) 802.11c – стандарт, регламентирующий работу беспроводных мостов. Данная спецификация используется производителями беспроводных устройств при разработке точек доступа;

5) 802.11d – стандарт определяет требования к физическим параметрам каналов (мощность излучения и диапазоны частот) и устройств беспроводных сетей с целью обеспечения их соответствия законодательным нормам различных стран;

6) 802.11e – создание данного стандарта связано с использованием средств мультимедиа. Он определяет механизм назначения приоритетов разным видам трафика, таким как аудио- и видеоприложения. Требование качества запроса, необходимое для всех радио интерфейсов IEEE WLAN;

7) 802.11f – данный стандарт, связанный с аутентификацией, определяет механизм взаимодействия точек связи между собой при перемещении клиента между сегментами сети. Другое название стандарта – Inter Access Point Protocol. Стандарт, описывающий порядок связи между равнозначными точками доступа;

8) 802.11g – устанавливает дополнительную технику модуляции для частоты 2,4 ГГц. Предназначен для обеспечения скоростей передачи данных до 54 Мбит/с по радиоканалу в диапазоне около 2,4 ГГц;

9) 802.11h – разработка данного стандарта связана с проблемами при использовании 802.11a в Европе, где в диапазоне 5 ГГц работают некоторые системы спутниковой связи. Для предотвращения взаимных помех стандарт 802.11h имеет механизм «квазиинтеллектуального» управления мощностью излучения и выбором несущей частоты передачи. Стандарт, описывающий управление спектром частоты 5 ГГц для использования в Европе и Азии;

10) 802.11i (WPA2) – целью создания данной спецификации является повышение уровня безопасности беспроводных сетей. В ней реализован набор защитных функций при обмене информацией через беспроводные сети, в частности,

					БР – 02069964 – 11.03.02 – 14 – 19	Лист
Изм.	Лист	№ докум.	Подпись	Дата		12

технология AES (Advanced Encryption Standard) – алгоритм шифрования, поддерживающий ключи длиной 128, 192 и 256 бит;

11) 802.11j – спецификация предназначена для Японии и расширяет стандарт 802.11a добавочным каналом 4,9 ГГц;

12) 802.11n – скорость до 600 Мбит/с, диапазон 2,4 или 5 ГГц, обратная совместимость с 802.11a/b/g;

13) 802.11r – основной особенностью этого стандарта является то, что он позволяет во время роуминга 802.1x клиента избежать обмена данными с Radius сервером, тем самым ускоряя процесс роуминга.

Из всех существующих стандартов беспроводной передачи данных IEEE 802.11, в настоящее время на практике используются наиболее часто 802.11n [5].

IEEE 802.11a

Стандарт IEEE 802.11a был принят в 1999 году. Он ориентирован на работу в диапазоне 5 ГГц и способен обеспечить скорость передачи данных до 54 Мбит/с. В стандарте 802.11a применена технология построения радиоканала на основе мультиплексирования с ортогональным разделением частот (Orthogonal Frequency Division Multiplexion, OFDM). Ее суть заключается в том, что передача информации осуществляется не по одному высокоскоростному каналу, а с помощью ряда независимых радиосигналов. Такое разделение посылаемой информации по нескольким «несущим» частотам приводит к возможности снижения скорости передачи на каждой из них, что в свою очередь обеспечивает большую помехозащищенность связи при достижении общей высокой пропускной способности.

В стандарте определены три обязательные скорости передачи данных (6, 12 и 24 Мбит/с) и пять дополнительных (9, 18, 24, 48 и 54 Мбит/с). Имеется возможность одновременного использования двух каналов; скорость при этом удваивается.

					БР – 02069964 – 11.03.02 – 14 – 19	Лист
Изм.	Лист	№ докум.	Подпись	Дата		13

IEEE 802.11b

Работа над стандартом 802.11b была закончена в 1999 году, и именно с ним связано название Wi-Fi (Wireless Fidelity, беспроводная связь). Именно его появление привело к широкому распространению WLAN для организации локальных сетей и доступа в Internet. Для работы сетей Wi-Fi стандартом предусмотрено использование частотного диапазона от 2,4 до 2,4835 ГГц, который во многих странах предназначен для безлицензионного использования в промышленности, науке и медицине (диапазон ISM – Industrial, Scientific, Medical).

Стандартом 802.11b предусмотрено применение только технологии DSSS, как обеспечивающей более устойчивую работу сети в условиях многократного отражения радиосигналов, а также более эффективной с позиций быстродействия (развитие технологии FHSS позволило пока достичь на практике скоростей передачи данных лишь порядка 3 Мбит/с).

По сравнению с базовым стандартом, в котором предусматривалась передача данных на скоростях 1 и 2 Мбит/с, в стандарте 802.11b обязательными являются также скорости 5,5 и 11 Мбит/с.

IEEE 802.11g

Этот стандарт принят в середине 2003 года, является логическим развитием 802.11b и предполагает передачу данных в том же частотном диапазоне. Кроме того, стандарт 802.11g полностью совместим со стандартом 802.11b, то есть любое устройство 802.11g должно поддерживать работу с устройствами 802.11b. Целью создания данного стандарта было достижения скорости передачи данных 54 Мбит/с. Как и IEEE 802.11b, стандарт IEEE 802.11g разработан для работы в частотном диапазоне 2,4 ГГц. IEEE 802.11g предписывает обязательные и возможные скорости передачи данных: обязательные – 1, 2, 5.5, 6, 11, 12, 24 Мбит/с; возможные – 33, 36, 48, 54 Мбит/с.

Для достижения таких показателей используется кодирование с помощью

					БР – 02069964 – 11.03.02 – 14 – 19	<i>Лист</i>
<i>Изм.</i>	<i>Лист</i>	<i>№ докум.</i>	<i>Подпись</i>	<i>Дата</i>		14

последовательности дополнительных кодов (ССК), метод ортогонального частотного мультиплексирования (OFDM), метод гибридного кодирования (ССК-OFDM) и метод двоичного пакетного сверточного кодирования (PBCC).

IEEE 802.11n

Одним из наиболее распространенных на сегодняшний день является стандарт 802.11n, работы над которым были начаты еще в 2004 году и окончательно утверждены 11 сентября 2009 г.

Основной особенностью стандарта 802.11n является дальнейшее повышение скорости передачи данных (до 300 Мбит/с и выше). Оборудование стандарта 802.11n может работать как в диапазоне 5 ГГц, так и в диапазоне 2,4 ГГц, хотя рекомендуемым диапазоном является диапазон 5 ГГц благодаря большему числу доступных каналов и меньшей интерференции с многочисленным оборудованием, работающим сегодня в диапазоне 2,4 ГГц.

Для достижения высоких скоростей в технологии 802.11n применено несколько новых механизмов:

1) *улучшенное кодирование OFDM и сдвоенные частотные каналы.* Вместо каналов с полосой в 20 МГц применены каналы с полосой 40 МГц (для обратной совместимости допускается также работать с каналами 20 МГц). Расширение полосы в два раза должно приводить к повышению битовой скорости в два раза, но выигрыш здесь больше за счет усовершенствований в кодировании OFDM: вместо 52 первичных несущих частот на полосу в 20 МГц здесь используется 57 таких частот, а на полосу в 40 МГц соответственно 114. Это приводит к повышению битовой скорости с 54 до 65 Мбит/с для каналов 20 МГц и до 135 Мбит/с для каналов 40 МГц.

2) *уменьшение межсимвольного интервала.* Для надежного распознавания кодовых символов в технологиях 80.11a/g используется межсимвольный интервал в 800 нс. Технология 802.11n позволяет передавать данные с таким же межсимвольным интервалом, а также с межсимвольным интервалом в 400 нс, что повышает битовую скорость для каналов 40 МГц до 150 Мбит/с.

					БР – 02069964 – 11.03.02 – 14 – 19	Лист
Изм.	Лист	№ докум.	Подпись	Дата		15

3) *применение техники MIMO* (Multiple Input Multiple Output – множественные входы и выходы). Эта техника основана на использовании одним сетевым адаптером нескольких антенн с целью лучшего распознавания сигнала, пришедшего к приемнику разными путями. Техника MIMO принципиально изменила отношение к сигналам, пришедшим разными путями, – эти сигналы комбинируются и путем цифровой обработки из них восстанавливается исходный сигнал.

Техника MIMO не только способствует улучшению соотношения сигнал/помеха. Благодаря возможности обрабатывать сигналы, пришедшие разными путями, для создания избыточного сигнала для каждого потока можно передавать с помощью нескольких антенн несколько независимых потоков данных. Эта способность систем MIMO называется пространственным мультиплексированием. Для систем MIMO принято использовать обозначение: $T \times R : S$. Здесь T – количество передающих антенн узла, R – количество принимающих антенн узла, а S – количество потоков данных, которые пространственно мультиплексируются. Проект стандарта 802.11n предусматривает различные варианты системы MIMO вплоть до 4x4:4, что позволило бы повысить битовую скорость до 600 Мбит/с.

Помимо усовершенствований физического уровня, стандарт 802.11n вводит одно усовершенствование на уровне MAC – это возможность агрегирования нескольких кадров данных в один кадр. Такая техника повышает эффективность передачи пользовательских данных при той же битовой скорости протокола за счет сокращения накладных расходов на шифрование отдельных кадров и на их индивидуальное подтверждение положительными квитанциями со случайными паузами между передачей кадров.

Стандарт 802.11n определяет индекс модуляции и схемы кодирования MCS (Modulation and Coding Scheme). MCS – простое целое число, присваиваемое каждому варианту модуляции. Каждый вариант определяет тип модуляции радиочастоты (Type), скорость кодирования (Coding Rate), защитный интервал (Short Guard Interval) и значения скорости передачи данных. Сочетание всех этих

					БР – 02069964 – 11.03.02 – 14 – 19	Лист
Изм.	Лист	№ докум.	Подпись	Дата		16

факторов определяет реальную физическую скорость передачи данных, начиная от 6,5 Мбит/с до 600 Мбит/с.

Тип модуляции и скорость кодирования определяют, как данные будут передаваться в радиоэфир. Новые методы модуляции и кодирования, как правило, более эффективные и поддерживают более высокие скорости передачи данных, но устаревшие методы и скорости все еще поддерживаются для обратной совместимости. Некоторые значения индекса MCS показаны в таблице 1.1.

Таблица 1.1 – Значения индекса MCS

MCS Index	Пространственные потоки	Тип модуляции	Скорость кодирования	Скорость передачи в канале Мбит/с			
				Канал 20 МГц		Канал 40 МГц	
				800 нс	400 нс	800 нс	400 нс
0	1	BPSK	1/2	6,50	7,20	13,50	15,00
1	1	QPSK	1/2	13,00	14,40	27,00	30,00
2	1	QPSK	3/4	19,50	21,70	40,50	45,00
3	1	16-QAM	1/2	26,00	28,90	54,00	60,00
4	1	16-QAM	3/4	39,00	43,30	81,00	90,00
5	1	64-QAM	2/3	52,00	57,80	108,00	120,00
6	1	64-QAM	3/4	58,00	65,00	121,50	135,00
7	1	64-QAM	5/6	65,00	72,20	135,00	150,00
8	2	BPSK	1/2	13,00	14,40	27,00	30,00
9	2	QPSK	3/4	26,00	28,90	54,00	60,00
10	2	QPSK	3/4	39,00	43,30	81,00	90,00
11	2	16-QAM	1/2	52,00	57,80	108,00	120,00
12	2	16-QAM	3/4	78,00	86,70	162,00	180,00
13	2	64-QAM	2/3	104,00	115,60	216,00	240,00
14	2	64-QAM	3/4	117,00	130,00	243,00	270,00
15	2	64-QAM	5/6	130,00	144,40	270,00	300,00

1.2.2 Технологии расширения спектра

Незащищенность от помех обычного радиосигнала вызвала к жизни разработку (сначала для военных применений) совершенно иного принципа радиопередачи, называемого технологией широкополосного или шумоподобного сигнала (обоим вариантам термина соответствует аббревиатура ШПС). После многих лет успешного оборонного использования эта технология нашла и гражданское применение.

Идея ШПС состоит в том, что для передачи информации используется значительно более широкая полоса частот, чем это требуется при обычной (в узком частотном канале) передаче. Разработано два принципиально различающихся между собой метода использования такой широкой полосы частот – метод прямой последовательности (Direct Sequence Spread Spectrum, DSSS) и метод частотных скачков (Frequency Hopping Spread Spectrum, FHSS). Оба эти метода предусматриваются и стандартом 802.11 (Radio-Ethernet).

Метод DSSS делит диапазон 2,4 ГГц на 14 частично перекрывающихся каналов. Для того чтобы несколько каналов могли использоваться одновременно в одном и том же месте, необходимо, чтобы они отстояли друг от друга на 25 МГц (не перекрывались), для исключения взаимных помех. Таким образом, в одном месте может одновременно использоваться максимум 3 канала. Данные пересылаются с использованием одного из этих каналов без переключения на другие каналы. Чтобы компенсировать посторонние шумы, используется 11-ти битная последовательность Баркера.

Основной принцип технологии расширения спектра (Spread Spectrum, SS) заключается в том, чтобы от узкополосного спектра сигнала, возникающего при обычном потенциальном кодировании, перейти к широкополосному спектру, что позволяет значительно повысить помехоустойчивость передаваемых данных. Рассмотрим более детально, как это происходит.

При потенциальном кодировании информационные биты 0 и 1 передаются прямоугольными импульсами напряжений. Прямоугольный импульс длительности T имеет спектр, ширина которого обратно пропорциональна длительности импульса и описывается формулой:

$$T = \frac{\sin(\pi f T)}{\pi f T}. \quad (1.1)$$

Чем меньше длительность импульса, тем больший спектральный диапазон занимает такой сигнал. Чтобы повысить помехоустойчивость передаваемого

					БР – 02069964 – 11.03.02 – 14 – 19	Лист
Изм.	Лист	№ докум.	Подпись	Дата		18

сигнала, можно воспользоваться методом перехода к широкополосному сигналу, добавляя избыточность в исходный сигнал. Для этого в каждый передаваемый информационный бит встраивают определенный код, состоящий из последовательности так называемых чипов (рисунок 1.2).

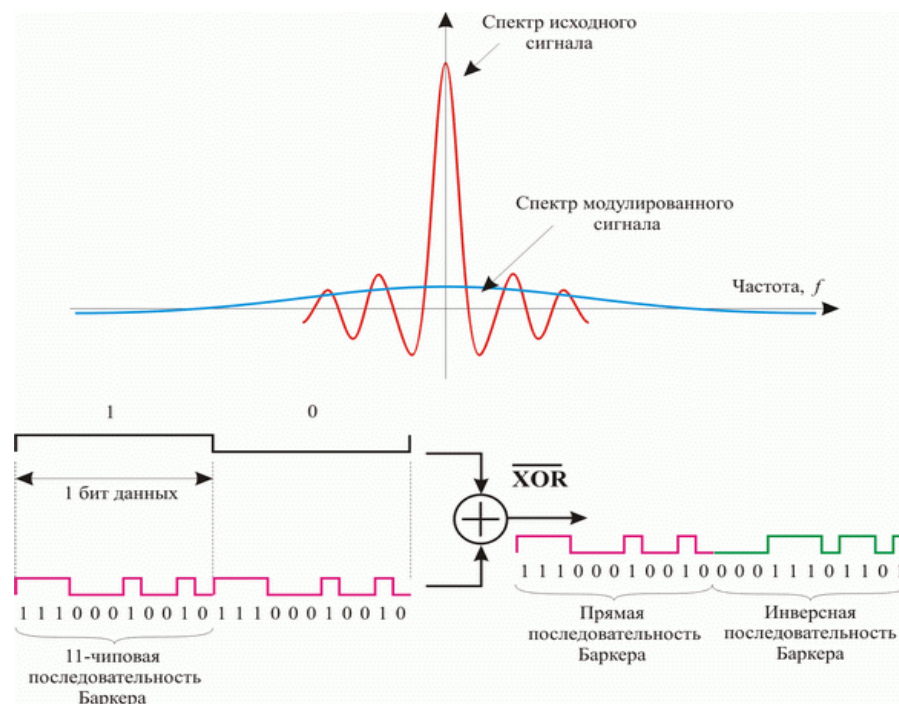


Рисунок 1.2 – Изменение спектра сигнала при добавлении шумоподобного кода

Информационный бит, представляемый прямоугольным импульсом, разбивается на последовательность более мелких импульсов-чипов. В результате спектр сигнала значительно расширяется, поскольку ширину спектра можно с достаточной степенью точности считать обратно пропорциональной длительности одного чипа. Такие кодовые последовательности часто называют шумоподобными кодами.

Для передачи единичного и нулевого символов сообщения используются, соответственно, прямая и инверсная последовательности Баркера, состоящие из 11 бит. В приёмнике полученный сигнал умножается на код Баркера (вычисляется корреляционная функция сигнала), в результате чего он становится узкополосным,

поэтому его фильтруют в узкой полосе частот, равной удвоенной скорости передачи. Основным смыслом использования кода Баркера заключается в том, чтобы гарантировать высокую степень достоверности принимаемой информации и при этом передавать сигнал практически на уровне помех.

При использовании метода частотных скачков (Frequency Hopping Spread Spectrum, FHSS) полоса 2,4 ГГц делится на 79 каналов по 1 МГц. Отправитель и получатель согласовывают схему переключения каналов (на выбор имеется 22 схемы), и данные посылаются последовательно по различным каналам с использованием этой схемы. Каждая передача данных в сети 802.11 происходит по разным схемам переключения, а сами схемы разработаны таким образом, чтобы минимизировать шансы того, что два отправителя будут использовать один и тот же канал одновременно.

Метод FHSS позволяет использовать очень простую схему приёмопередатчика, однако ограничен максимальной скоростью 2 Мбит/с. Это ограничение вызвано тем, что под один канал выделяется ровно 1 МГц, что вынуждает FHSS системы использовать весь диапазон 2,4 ГГц. Это означает, что должно происходить частое переключение каналов, что, в свою очередь, приводит к увеличению накладных расходов.

На рисунке 1.3 приведён пример передачи сигнала со скачкообразной перестройкой частоты (frequency hopping, FH). Для передачи FH-сигнала резервируются определённое количество каналов. Как правило, используют 2^k несущих частот, которые составляют 2^k каналов. Расстояние между несущими частотами (Δf , следовательно, ширина каждого канала) обычно равно ширине полосы входного сигнала. При передаче каждый канал используется в течение фиксированного интервала времени; в стандарте IEEE 802.11 этот интервал равен 300 мс. В течение такого интервала производится передача некоторого количества закодированных определённым образом битов (возможно, частей битов). Последовательность использования каналов задаётся кодом расширения, и, поскольку приёмник и передатчик используют один и тот же код, переходы между каналами выполняются синхронно.

					БР – 02069964 – 11.03.02 – 14 – 19	Лист
Изм.	Лист	№ докум.	Подпись	Дата		20

Метод частотных скачков, так же как и описанный выше метод прямой последовательности, обеспечивает конфиденциальность и некоторую помехозащищенность передач. Помехозащищенность обеспечивается тем, что если на каком-нибудь из 79 подканалов передаваемый пакет не смог быть принят, то приемник сообщает об этом, и передача этого пакета повторяется на одном из следующих (в последовательности скачков) подканалов.

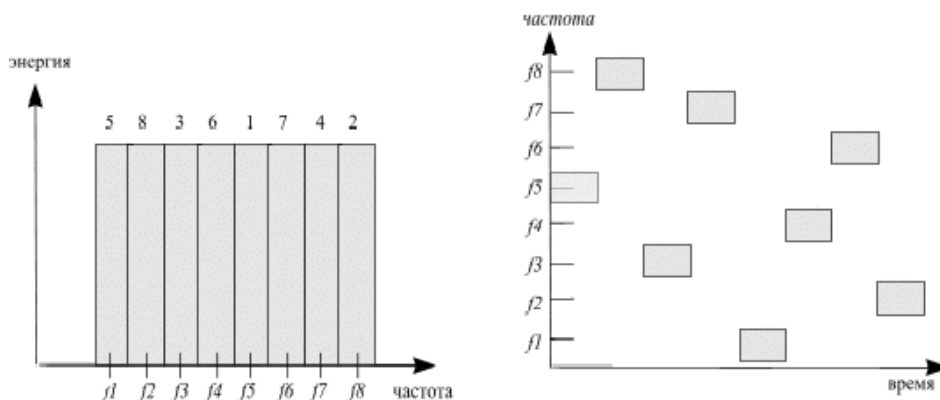


Рисунок 1.3 – Пример скачкообразной перестройки частоты

С другой стороны, поскольку при использовании метода частотных скачков, в отличие от метода прямой последовательности, на каждом подканале передача ведется на достаточно большой мощности (сравнимой с мощностью обычных узкополосных передатчиков), про этот метод нельзя сказать, что он не мешает другим видам передач.

1.2.3 Режимы работы стандарта IEEE 802.11

Стандарт IEEE 802.11 определяет несколько режимов работы сети.

В режиме «Ad-hoc» (рисунок 1.4) клиенты устанавливают связь непосредственно друг с другом. Устанавливается одноранговое взаимодействие по типу «точка-точка», и компьютеры взаимодействуют напрямую без применения точек доступа. При этом создается только одна зона обслуживания, не имеющая интерфейса для подключения к проводной локальной сети. Основное достоинство

данного режима – простота организации: он не требует дополнительного оборудования (точки доступа). Режим может применяться для создания временных сетей для передачи данных.

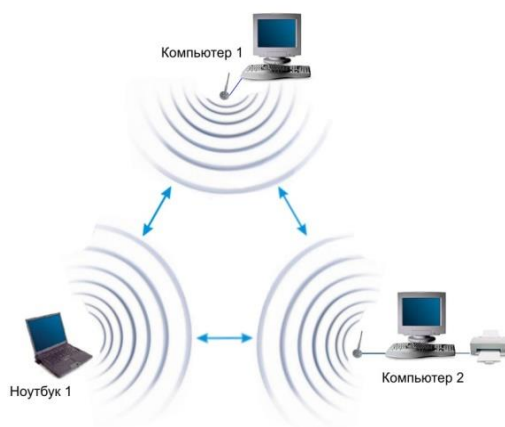


Рисунок 1.4 – Режим «Ad-hoc»

Значительно большими возможностями обладают сети, работающие в инфраструктурном режиме (Infrastructure Mode), основу которых составляет сотовая архитектура, подобная той, что используется в мобильной связи. При этом такие сети могут состоять как из одной, так и из множества ячеек. В этом режиме устройства пользователей напрямую друг с другом не связываются, а взаимодействуют через точку доступа.

Точка доступа имеет порт Ethernet, через который базовая зона обслуживания может подключается к проводной или смешанной сети – к сетевой инфраструктуре (рисунок 1.5).

В режиме «распределенная беспроводная система» (Wireless Distribution System, WDS) точки доступа соединяются только между собой, образуя мостовое соединение. При этом каждая точка может соединяться с несколькими другими точками. Все точки в этом режиме должны использовать один и тот же канал, поэтому количество точек, участвующих в образовании моста, не должно быть чрезмерно большим. Подключение клиентов осуществляется только по проводной сети через uplink-порты точек (рисунок 1.6).

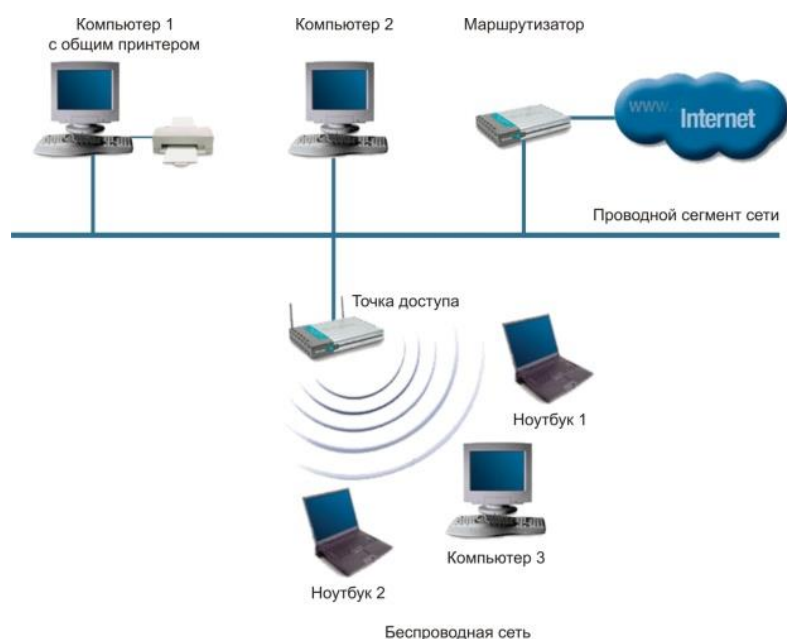


Рисунок 1.5 – Инфраструктурный режим

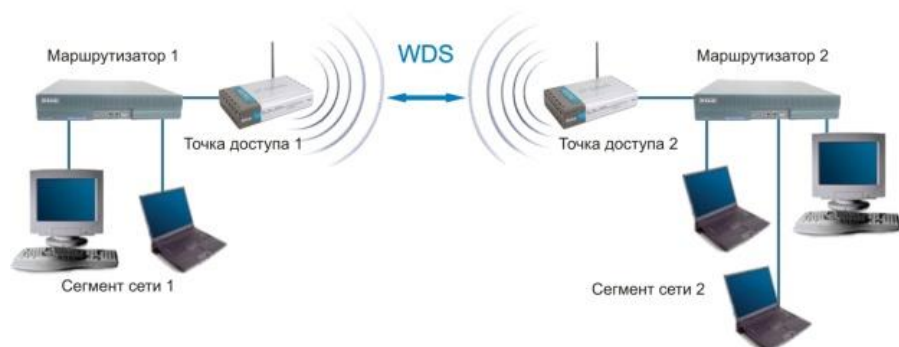


Рисунок 1.6 – Мостовой режим

Режим беспроводного моста, аналогично проводным мостам, служит для объединения подсетей в общую сеть. С помощью беспроводных мостов можно объединять проводные LAN, находящиеся как в соседних зданиях, так и на расстоянии до нескольких километров.

Беспроводной мост может использоваться там, где прокладка кабеля между зданиями нежелательна или невозможна. Данное решение позволяет достичь значительной экономии средств и обеспечивает простоту настройки

и гибкость конфигурации при перемещении офисов.

Термин WDS with AP (WDS with Access Point) означает «распределенная беспроводная система, включающая точку доступа», то есть с помощью этого режима можно не только организовать мостовую связь между точками доступа, но и одновременно подключить клиентские компьютеры (рисунок 1.7). Это позволяет достичь существенной экономии оборудования и упростить топологию сети. Данная технология поддерживается большинством современных точек доступа.

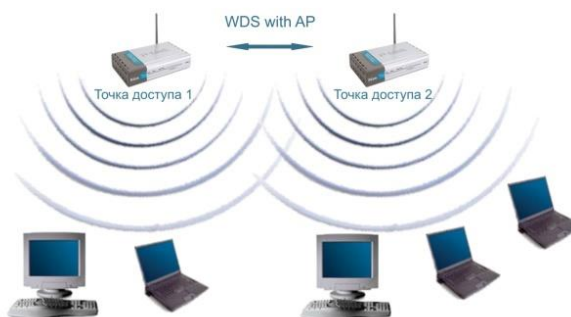


Рисунок 1.7 – Режим WDS with AP

Теоретически, к каждой точке доступа может быть подключено до 255 пользователей (это количество продиктовано ограничениями IP-протокола), однако на практике данное число оказывается существенно меньше и реально составляет 20-30 пользователей.

1.2.4 Механизм доступа к среде

Для обеспечения возможности совместной работы в сети большого количества пользовательских устройств без взаимных помех, стандартом определен специальный механизм их перехода в режим передачи с предварительным уведомлением о намерении посылки данных – множественный доступ с контролем несущей и предотвращением коллизий (Carrier Sense Multiple Access with Collision Avoidance, CSMA/CA).

Каждая станция самостоятельно определяет момент своего выхода в эфир и

занятия среды, при этом перед началом передачи эфир прослушивается станцией и в случае, если он свободен, станция начинает передачу. Последовательные попытки передачи данных каждой станции разделены интервалом задержки, а также случайным отложенным временем (Backoff time). В случае коллизии, когда в эфир одновременно выходят две станции, реализуется механизм избегания коллизий. Обе станции прекращают передачу, каждая из них выжидает случайный промежуток времени, прослушивая среду. Далее станция, у которой интервал оказался меньше, снова выходит в эфир. Поскольку вероятность совпадения случайного промежутка времени у разных станций мала, данный метод позволяет многократно снизить вероятность возникновения повторных коллизий.

1.2.5 Физический уровень (Physical layer) стандарта IEEE 802.11

На физическом уровне стандарт 802.11 охватывает три альтернативы:

- передачу с использованием инфракрасного излучения (Diffuse Infra-Red, DFIR);
- передачу по радио с использованием расширения спектра методом прямой последовательности (Direct Sequence Spread Spectrum, DSSS);
- передачу по радио с использованием расширения спектра методом частотных скачков (Frequency Hopping Spread Spectrum, FHSS).

Обе разновидности передачи по радио с использованием расширения спектра методом прямой последовательности (DS) и методом частотных скачков (FH) используют частотный диапазон 2,400 – 2,4835 ГГц. Диапазон 2,4 ГГц был выбран потому, что во всем мире данный диапазон выделен для нелицензируемого использования, а также в данном диапазоне возможно создание и производство приемо-передающего радиооборудования, обладающего низкой стоимостью, небольшой излучаемой мощностью и работающего на скоростях, близких к скоростям в обычных проводных Ethernet сетях.

Стандарт IEEE 802.11 работает на двух нижних уровнях модели взаимодействия открытых систем (Open Systems Interconnection Reference Model,

					<i>БР – 02069964 – 11.03.02 – 14 – 19</i>	<i>Лист</i>
<i>Изм.</i>	<i>Лист</i>	<i>№ докум.</i>	<i>Подпись</i>	<i>Дата</i>		25

OSI) – физическом и канальном (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.



Рисунок 1.8 – Уровни модели OSI

1.2.6 Канальный уровень (Data Link) стандарта IEEE 802.11

Канальный уровень стандарта IEEE 802.11 состоит из двух подуровней: управления логической связью (Logical Link Control, LLC) и управления доступом к среде (Media Access Control, MAC).

Подуровень MAC получает блок данных от подуровня LLC и отвечает за выполнение функций, связанных с доступом к среде, и за передачу данных, также отвечает за выявление ошибок и отклонение кадров с ошибками. Подуровень LLC может отслеживать, какие кадры были успешно приняты и повторно передавать остальные.

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 определении мощности принятого сигнала. Если мощность принятого сигнала ниже определённого порога, то канал объявляется свободным, и MAC-подуровень получает статус «свободен к пересылке» (Clear To Send, CTS). Если мощность выше порогового значения, то передача данных задерживается в соответствии с правилами протокола.

Наконец, MAC-подуровень 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-подуровень ответственен за сборку полученных фрагментов, делая этот процесс «прозрачным» для протоколов более высокого уровня.

1.2.7 Организация микросотовых сетей

Семейство стандартов IEEE 802.11 позволяет организовать беспроводные сети с несколькими точками доступа, аналогичные по принципу работы сетям сотовой связи.

Если клиентская станция попадает в зону действия нескольких точек доступа, она выбирает из них ту, с которой качество связи выше (в качестве критериев качества связи используются мощность сигнала и коэффициент ошибок), и настраивается на ее частоту. Однако периодически клиентская станция тестирует качество связи с другими точками доступа, и, если отыскивается точка доступа с качеством выше, чем имеется на данный момент, происходит перенастройка на ее частоту (рисунок 1.9). Подуровень MAC канального уровня

					БР – 02069964 – 11.03.02 – 14 – 19	Лист
Изм.	Лист	№ докум.	Подпись	Дата		27

управляет процессом передачи клиента от одной точки доступа к другой.

Имеются три частотных канала, которые можно одновременно использовать в одном и том же месте. Соответственно, точки доступа, каждая из которых настроена на один из этих трех каналов, можно разместить таким образом, что соседние точки доступа будут работать на разных частотах. Однако при этом иногда возникает паразитное взаимное влияние между точками доступа, расположенными не в соседних сотах, а через соту. Эта проблема может быть решена, если использовать то обстоятельство, что на самом деле выделено 14 каналов и размещение в частотном спектре трех каналов, а также защитных интервалов между ними, можно варьировать [4].

Переподрключение обычно происходит в том случае, если станция была физически перемещена вдали 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».

Процесс динамического подключения и переподрключения позволяет сетевым администраторам устанавливать беспроводные сети с очень широким покрытием, создавая частично перекрывающиеся «соты». Идеальным вариантом является такой, при котором соседние перекрывающиеся точки доступа будут использовать разные DSSS каналы, чтобы не создавать помех в работе друг другу.

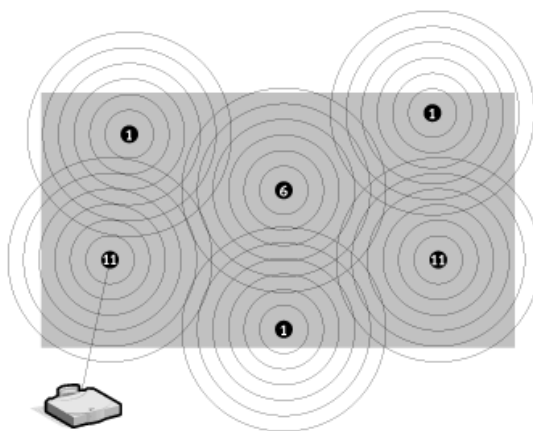


Рисунок 1.9 – Беспроводная сеть с несколькими точками доступа

1.3 Безопасность беспроводных сетей

При построении сетей с использованием беспроводных технологий передачи данных особое внимание уделяется безопасности и защите информации. Это связано с тем, что данные в таких сетях передаются в среде, доступной для прослушивания потенциальными недоброжелателями.

Аутентификация

Аутентификация (англ. Authentication – идентификация) – процесс проверки имени пользователя и пароля или другого идентификатора из известного пространства имен. Говоря более просто: аутентификация – это проверка того, что субъект является тем, за кого он себя выдает.

Аутентификация, как идентификация и проверка подлинности пользователей, – это основное средство защиты информационных систем от постороннего вмешательства. Под идентификацией обычно понимается процедура, посредством которой пользователь сообщает сведения о себе (рисунок 1.10).

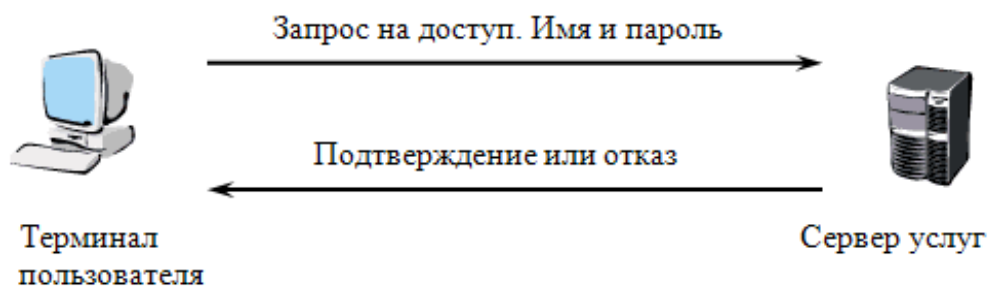


Рисунок 1.10 – Аутентификация

Фильтрация MAC-адресов

Фильтрация MAC-адресов, которая поддерживается всеми современными точками доступа и беспроводными маршрутизаторами, позволяет повысить уровень безопасности беспроводной сети. Для реализации данной функции в настройках

точки доступа создаётся таблица MAC-адресов беспроводных адаптеров клиентов, авторизованных для работы в данной сети.

MAC-адрес – это уникальный идентификатор, «прошитый» производителем внутрь каждого сетевого устройства без возможности его изменения. Каждому производителю выделен отдельный диапазон MAC-адресов и ведётся база данных, препятствующая выпуску устройств с одинаковыми идентификаторами. Считается, что в мире не может быть двух устройств с одинаковыми MAC-адресами. Используя такой фильтр списка MAC-адресов в точке доступа, можно разрешить только лишь определенным клиентам подключаться к сети.

Режим скрытого идентификатора сети SSID

Ещё одна мера предосторожности, которую часто используют в беспроводных сетях – это режим скрытого идентификатора сети.

Каждой беспроводной сети назначается свой уникальный идентификатор (Service Set Identifier , SSID), который представляет собой название сети. Когда пользователь пытается войти в сеть, то драйвер беспроводного адаптера прежде всего сканирует эфир на наличие в ней беспроводных сетей. При использовании режима скрытого идентификатора сеть не отображается в списке доступных, и подключиться к ней можно только в том случае, если, во-первых, точно известен её SSID, и, во-вторых, заранее создан профиль подключения к этой сети.

Протокол WEP

Все современные беспроводные устройства (точки доступа, беспроводные адаптеры и маршрутизаторы) поддерживают протокол безопасности WEP (Wired Equivalent Privacy), который был изначально заложен в спецификацию беспроводных сетей IEEE 802.11. Данный протокол является своего рода аналогом проводной безопасности (во всяком случае, расшифровывается он именно так), однако реально никакого эквивалентного проводным сетям уровня безопасности он, конечно же, не предоставляет.

					БР – 02069964 – 11.03.02 – 14 – 19	Лист
						30
Изм.	Лист	№ докум.	Подпись	Дата		

Протокол WEP позволяет шифровать поток передаваемых данных на основе алгоритма RC 4 с ключом размером 64 или 128 бит.

Данные ключи имеют так называемую статическую составляющую длиной от 40 до 104 бит и дополнительную динамическую составляющую размером 24 бита, называемую вектором инициализации (Initialization Vector, IV).

Протокол безопасности WEP предусматривает два способа аутентификации пользователей: Open System (открытая) и Shared Key (общая). При использовании открытой аутентификации никакой аутентификации, собственно, и не существует, то есть любой пользователь может получить доступ в беспроводную сеть. Однако, даже при использовании открытой системы допускается использование WEP-шифрования данных.

Протокол WPA

Протокол WEP имеет ряд серьёзных недостатков и не является для взломщиков труднопреодолимым препятствием. Поэтому в 2003 году был представлен следующий стандарт безопасности — WPA (Wi-Fi Protected Access). Главной особенностью этого стандарта является технология динамической генерации ключей шифрования данных, построенная на базе протокола TKIP (Temporal Key Integrity Protocol), представляющего собой дальнейшее развитие алгоритма шифрования RC4. По протоколу TKIP сетевые устройства работают с 48-битовым вектором инициализации (в отличие от 24-битового вектора WEP) и реализуют правила изменения последовательности его битов, что исключает повторное использование ключей. В протоколе TKIP предусмотрена генерация нового 128-битного ключа для каждого передаваемого пакета. Кроме того, контрольные криптографические суммы в WPA рассчитываются по новому методу под названием MIC (Message Integrity Code). В каждый кадр здесь помещается специальный восьмибайтный код целостности сообщения, проверка которого позволяет отражать атаки с применением подложных пакетов. В итоге получается, что каждый передаваемый по сети пакет данных имеет собственный уникальный

					БР – 02069964 – 11.03.02 – 14 – 19	Лист
Изм.	Лист	№ докум.	Подпись	Дата		31

ключ, а каждое устройство беспроводной сети наделяется динамически изменяемым ключом.

Кроме того, протокол WPA поддерживает шифрование по стандарту AES (Advanced Encryption Standard), то есть по усовершенствованному стандарту шифрования, который отличается более стойким криптоалгоритмом, чем это реализовано в протоколах WEP и TKIP.

VPN

Виртуальная частная сеть или просто VPN (Virtual Private Network) – это технология, при которой происходит обмен информацией с удаленной локальной сетью по виртуальному каналу через сеть общего пользования с имитацией частного подключения «точка-точка». Под сетью общего пользования можно подразумевать как Интернет, так и другую интрасеть.

Есть один аргумент в пользу использования технологии VPN для защиты информации, циркулирующей в беспроводной сети. Создав на базе VPN продуктов внешнюю защитную оболочку, собственник приобретает уверенность в том, что он защищен не только от известных уязвимостей встроенных протоколов защиты беспроводных сетей, но и от тех, которые могут появиться в дальнейшем.

Механизм шифрования WPA2, или 802.11i

Стандарт 802.11i использует концепцию Robust Security Network (RSN), предусматривающую, что беспроводные устройства должны обеспечивать дополнительные возможности. Это потребует изменений в аппаратной части и программном обеспечении, то есть сеть, полностью соответствующая RSN, станет несовместимой с существующим оборудованием WEP.

802.11i приложим к различным сетевым реализациям и может задействовать TKIP, но по умолчанию RSN использует AES (Advanced Encryption Standard) и CCMP (Counter Mode CBC MAC Protocol) и, таким образом, является более мощным расширяемым решением.

					БР – 02069964 – 11.03.02 – 14 – 19	Лист
Изм.	Лист	№ докум.	Подпись	Дата		32

В концепции RSN применяется AES в качестве системы шифрования, подобно тому, как алгоритм RC4 задействован в WPA. Однако механизм шифрования куда более сложен и не страдает от проблем, имевшихся в WEP.

AES – блочный шифр, оперирующий блоками данных по 128 бит. CCMP – протокол безопасности, используемый AES. Он является эквивалентом TKIP в WPA. CCMP вычисляет MIC, прибегая к хорошо известному и проверенному методу Cipher Block Chaining Message Authentication Code (CBC-MAC). Изменение даже одного бита в сообщении приводит к совершенно другому результату.

Стандарт 802.11i разработан на базе проверенных технологий. Механизмы безопасности были спроектированы с нуля в тесном сотрудничестве с лучшими специалистами по криптографии и имеют все шансы стать тем решением, которое необходимо беспроводным сетям. Хотя ни одна система безопасности полностью от взлома не гарантирована, 802.11i – это решение, на которое можно полагаться; оно свободно от слабостей предыдущих систем.

При профессиональной организации защищённых беспроводных сетей не приемлемо использование только одного средства защиты. Защита информации должна быть комплексной и охватывать всё пространство возможных угроз для сетей WLAN.

1.4 Частотное регулирование для беспроводных сетей

На сегодняшний день в России все технологии и процессы, связанные с передачей данных по радио достаточно жестко регламентированы, будь то производство оборудования, его импорт и последующая продажа или использование.

Порядок выделения полос радиочастот и присвоения радиочастот для территориально распределенных беспроводных сетей определен статьей 24 закона «О связи», в соответствии с которой выделение полос радиочастот для РЭС гражданского назначения осуществляется Государственной комиссией по радиочастотам (ГКРЧ), а присвоение (назначение) необходимых радиочастот для

					БР – 02069964 – 11.03.02 – 14 – 19	<i>Лист</i>
<i>Изм.</i>	<i>Лист</i>	<i>№ докум.</i>	<i>Подпись</i>	<i>Дата</i>		33

РЭС гражданского применения федеральным органом исполнительной власти в области связи (Мининформсвязи России).

Первым этапом в процессе частотных присвоений является получение частного решения ГКРЧ об использовании запрашиваемого диапазона частот. ГКРЧ осуществляет предварительную оценку ЭМС с заинтересованными министерствами и ведомствами для создаваемой сети и выносит решение о возможности использования запрашиваемого диапазона.

Для диапазона 2,4 ГГц получение частного решения ГКРЧ не требуется, благодаря наличию Обобщенного решения ГКРЧ от 25.09.2000 (протокол № 2/7) «Об уточнении условий использования полосы радиочастот 2400 - 2483,5 МГц».

Диапазона 5 ГГц, в соответствии с решением ГКРЧ от 15 июля 2010, выделен для разработки, производства и модернизации юридическими и физическими лицами РЭС фиксированного беспроводного доступа без оформления отдельных решений ГКРЧ для каждого конкретного типа РЭС при условии, что основные технические характеристики разрабатываемых, производимых и модернизируемых РЭС соответствуют определенным техническим характеристикам.

Следующим этапом частотных присвоений является оформление «Заключения экспертизы о возможности использования радиоэлектронных средств и об электромагнитной совместимости», выдаваемое Главным радиочастотным центром (ФГУП ГРЧЦ).

Основным документом, регламентирующим присвоение радиочастот, является положение о порядке проведения экспертизы, рассмотрения материалов и принятия решения о присвоении (назначении) радиочастот или радиочастотных каналов для радиоэлектронных средств в пределах выделенных полос радиочастот, утвержденные решением Государственной комиссии по радиочастотам.

ФГУП ГРЧЦ осуществляет координацию необходимых согласований ЭМС с действующими РЭС гражданского и военного назначения, а также международные согласования в случае необходимости.

Завершающим этапом частотных присвоений является получение разрешения на использование радиочастот в Мининформсвязи России (Федеральном агентстве

					БР – 02069964 – 11.03.02 – 14 – 19	Лист
Изм.	Лист	№ докум.	Подпись	Дата		34

связи при Министерстве информатизации и связи). Для получения разрешения необходимо направить письмо с приложением заключения экспертизы о возможности использования радиоэлектронных средств и об электромагнитной совместимости, выданного ФГУП ГРЧЦ.

Разрешение на использование радиочастот выдается, как правило, на 5 лет, но не более срока действия лицензии на предоставление услуг связи. Разрешение служит основанием для: получения разрешений на приобретение на территории Российской Федерации РЭС отечественного или зарубежного производства, на ввоз из-за границы РЭС, получения оборудования в аренду (лизинг); проведения работ по проектированию, строительству (монтажу) РЭС; получения разрешения на эксплуатацию РЭС в установленном порядке.

					БР – 02069964 – 11.03.02 – 14 – 19	Лист
Изм.	Лист	№ докум.	Подпись	Дата		35

2 Технико-экономическое предложение

Критерии, которыми следует руководствоваться при выборе оборудования для сети беспроводного доступа, могут быть сформулированы следующим образом:

- оборудование должно производиться компанией, имеющей опыт разработки и производства аналогичного оборудования предыдущих поколений;
- производитель должен владеть патентами на используемые в оборудовании технологии;
- технические характеристики оборудования, предоставляемые производителем, должны быть непротиворечивыми, для пакетных радиосетей обязательно указание реальной (эффективной) пропускной способности;
- базовая станция должна иметь возможность секторирования и поэтапного наращивания производительности, для чего точки доступа должны иметь возможность подключения внешней антенны;
- оборудование должно быть сертифицировано на территории России в системе «Связь»;
- должна быть возможность получения разрешения на использование частот в диапазонах, используемых оборудованием;
- оборудование должно обеспечивать гарантированное качество обслуживания, необходимое для передачи информации реального времени (голос, видео);
- должна быть гарантия того, что производство оборудования не будет свернуто внезапно и в самый неподходящий момент;
- система должна обладать приемлемой для российских потребителей стоимостью, причем в первую очередь важна минимальная стоимость абонентского оборудования.

На сегодняшний день на российском рынке представлено огромное количество беспроводного оборудования. Указанным выше критериям удовлетворяет оборудование целого ряда производителей: 3Com, Asus, Asante, D-Link, Gigabyte, Multico, TRENDnet, ZyXEL, и др. Среди них можно выделить

					БР – 02069964 – 11.03.02 – 14 – 19	Лист
Изм.	Лист	№ докум.	Подпись	Дата		36

несколько наиболее крупных и значимых. Это фирмы Cisco, D-Link, ZyXEL, Linksys и TRENDnet.

Все сертифицированное оборудование Wi-Fi должно быть функционально совместимо, поэтому логично предположить, что все устройства обеспечивают приблизительно одинаковые возможности. Однако это мнение ошибочно. Базовые функции всех устройств одинаковы, но реализация, управление и администрирование этих функций сильно различаются. Так что, в конечном итоге выбор поставщика должен зависеть от того, какие функции оборудования наиболее важны для проектируемой сети.

Выбранное оборудование должно иметь оптимальную, экономически оправданную стоимость и в то же время быть достаточно гибким, обладать достаточным потенциалом наращивания производительности, обладать возможностью поддержки будущих протоколов работы беспроводной сети.

Из всего сказанного выше следует, что при выборе конкретной модели беспроводного устройства в первую очередь стоит обратить внимание не на производителя, а на функциональные возможности устройства и, конечно же, на цену.

Анализ технического задания говорит о том, что необходимо обеспечить покрытие в радиусе 300-400 м. Данному требованию удовлетворяет оборудование любого из перечисленных производителей, однако наименьшей стоимостью обладает оборудование фирмы D-Link.

Компания D-Link является всемирно известным разработчиком и производителем сетевого и телекоммуникационного оборудования и предлагает широкий набор решений для домашних пользователей, корпоративного сегмента и провайдеров интернет-услуг. Оборудование D-Link имеет все необходимые сертификаты, включая сертификаты в области связи, Госстандарта России и Санитарно-эпидемиологической службы РФ. Поэтому в дипломном проекте будем использовать оборудование именно этой фирмы.

					БР – 02069964 – 11.03.02 – 14 – 19	Лист
Изм.	Лист	№ докум.	Подпись	Дата		37

2.1 Точка доступа

При выборе узла доступа Wi-Fi следует убедиться, что его можно дополнить внешней антенной. Встроенные антенны вполне годятся для дома, но не для улицы, так как их эффективный диапазон, как правило, невелик. Необходимо также учитывать такие характеристики, как устойчивость к погодным условиям и совместимость узла доступа с технологией Power over Ethernet (PoE питание по кабелю Ethernet), которая значительно облегчает подвод электропитания [9].

Подходящим высокопроизводительным решением по организации беспроводной сети вне здания является двухдиапазонная мост/точка доступа D-Link DAP-3690 (802.11n) Outdoor (рисунок 2.1).



Рисунок 2.1 – Внешняя беспроводная точка доступа/мост D-Link AirPremier DAP-3690

Внешняя беспроводная точка доступа D-Link AirPremier DAP-3690 соответствует стандартам IEEE 802.11a/b/g/n и может работать на частоте 2,4 ГГц или 5 ГГц. DAP-3690 способна покрывать большие расстояния и обеспечивать беспроводную связь на скорости до 300 Мбит/с, предоставляя широкополосный доступ в Internet.

Точка доступа D-Link AirPremier DAP-3690 разрабатывалась для работы в сложных климатических условиях. Обладая прочным, водонепроницаемым корпусом и встроенным обогревателем с температурным датчиком, DAP-3690

					БР – 02069964 – 11.03.02 – 14 – 19	Лист
Изм.	Лист	№ докум.	Подпись	Дата		38

является наиболее защищенной точкой доступа для построения беспроводных сетей вне зданий. Также обеспечивается экономически эффективная система подачи питания для точки доступа по кабелю Ethernet в соответствии со стандартом IEEE 802.3at Power-over-Ethernet для обеспечения электропитанием точки доступа в местах, где нет установленных силовых розеток. DAP-3690 включает функцию WDS (Wireless Distribution System), которая может быть настроена для работы в одном из следующих режимов: беспроводная точка доступа (AP), мост точка – точка (PtP), мост точка – много точек (PtMP), и беспроводный клиент. При использовании разнообразных внешних антенн с высоким коэффициентом усиления для сетей с различными требованиями DAP-3690 станет идеальным решением для подключения абонентов.

DAP-3690 обеспечивает шифрование WEP с ключом 64/128-бит. Кроме того, управление доступом к сети 802.1x на основе портов для аутентификации пользователей и WPA (Wi-Fi Protected Access) помогают обеспечить оптимальный уровень безопасности. Также поддерживается балансировка нагрузки и резервирование каналов связи. Управление точкой доступа осуществляется при помощи web-интерфейса и Telnet. Поддержка сетевого управления по протоколу SNMP v.3 и мониторинга сетевого трафика в реальном времени посредством ПО сетевого управления D-Link D-View 6.0 делает точку доступа привлекательным решением для построения беспроводных сетей.

Это устройство имеет очень хорошую производительность и идеально выполняет все поставленные перед ней задачи по обеспечению надежной и безопасной передачи данных (таблица 2.1).

Таблица 2.1 – Основные характеристики внешней беспроводной точки доступа/моста D-Link AirPremier DAP-3690

Производитель	D-Link
Модель	AirPremier DAP-3690
Стандарты	IEEE 802.11a/b/g/n
Полоса частот	2,4 ГГц (от 2,4 ГГц до 2,4835 ГГц) 5 ГГц (от 5,15 ГГц до 5,35 ГГц, от 5,47 ГГц до 5,85 ГГц)

Окончание таблицы 2.1

Основные характеристики	
Тип устройства	точка доступа / мост
Сетевое управление	- HTTP - SNMP 3.0 - Telnet - Secure (SSH)
Скорость беспроводного соединения	IEEE 802.11a: 6,9,12,18,24,36,48,54 Мбит/с; IEEE 802.11b: 11, 5.5, 2, и 1 Мбит/с; IEEE 802.11g: 6,9,12,18,24,36,48,54 Мбит/с; IEEE 802.11n: MCS0 – MCS15 (см. таблицу 1.1).
Чувствительность приемника	IEEE 802.11n: 2,4ГГц/HT-20 16dBm при MCS0/8, MCS1/9, MCS2/10, MCS3/11, MCS4/12 14dBm при MCS 5/13 13dBm при MCS 6/14 12dBm при MCS 7/15 2,4ГГц/HT-40 14dBm при MCS0/8, MCS1/9, MCS2/10, MCS3/11, MCS4/12 13dBm при MCS 5/13 12dBm при MCS 6/14 11dBm при MCS 7/15
Мощность передатчика	20 dBm (100 мВт)
Безопасность данных	- Шифрование 64/128/-бит WEP - Аутентификация 802.1x - Управление доступом на основе MAC-адресов - WPA, WPA2 - Обнаружение незарегистрированных точек доступа -Разделение WLAN
Дополнительные характеристики	
Интерфейсы	Порт 10/100/1000 BASE-TX
Технические характеристики	
Рабочая температура	От -40° до 60° С
Размеры	250 x 220 x 70 мм
Сертификаты	FCC, CE, IC, C-Tick, NCC, UL, Wi-Fi, IP67

2.2 Антенно-фидерные устройства

Штатные антенны беспроводных устройств не всегда способны обеспечить требуемую зону покрытия Wi-Fi-сети.

					БР – 02069964 – 11.03.02 – 14 – 19	Лист
Изм.	Лист	№ докум.	Подпись	Дата		40

Для увеличения радиуса действия проектируемой беспроводной сети в данном проекте предлагается использование внешних антенн.

Необходимо отметить, что вынос антенны приводит к возникновению негативных факторов: затуханию сигнала на кабельных сборках и увеличению уровня паразитных шумов, значительно ухудшающих характеристики исходной радиосистемы. Вместе с тем, подключенные антенны (особенно с большими коэффициентами усиления) во многом компенсируют все эти негативные факторы. То есть, важным этапом при проектировании беспроводной сети является выбор антенны. От правильного выбора этого устройства будет зависеть качество связи, дальность действия и скорость передачи данных.

Outdoor оборудование, как правило, имеет мощные передатчики около 100–400, поэтому дополнительное усиление сигнала путем включения в антенно-фидерный тракт усилителя в основном не требуется (лишь только в некоторых специфических случаях). В проекте использование усилителя не предусмотрено в силу того, что точка доступа D-Link AirPremier DAP-3690 имеет выходную мощность 100 мВт, что позволяет при использовании внешней антенны обеспечить необходимую зону радиопокрытия для установления связи.

В качестве внешней антенны предлагается использовать секторную MIMO антенну ZyXEL ANT1314 с коэффициентом усиления 14 дБ (рисунок 2.2, таблица 2.2).



Рисунок 2.2 – Внешний вид секторной антенны ANT1314

					БР – 02069964 – 11.03.02 – 14 – 19	Лист
Изм.	Лист	№ докум.	Подпись	Дата		41

Таблица 2.2 – Основные технические характеристики секторной антенны ANT1314

Диапазон частот, МГц	2400 - 2500
Коэффициент усиления	14 ± 0,5 дБи
Ширина диаграммы направленности	- В вертикальной плоскости 13° - В горизонтальной плоскости 60°
Входное сопротивление	50 Ом
Масса	800 г
КСВН (VSWR)	не более 2,0:1
Физические размеры антенны	560 x 120 x 145 мм
Макс. скорость ветра	216 км/ч
Поляризация	линейная, ± 45°
Диапазон рабочих температур	-40° +80°
Разъемы	два N-type (Female)

Выбор модели антенны определялся необходимой площадью радиопокрытия (согласно техническому заданию, необходимо подключить абонентов в радиусе 300 - 400 м), исходя из коэффициента усиления антенны и ее конструктивных особенностей. Разумеется, при выборе учитывалась и цена.

При использовании секторной антенны ANT1314 с беспроводной точкой доступа D-Link AirPremier DAP-3690 с мощностью передатчика 20 дБм (100 мВт), мощность сигнала в направлении максимального усиления составит 20 дБм + 14 дБи – $W_{АФТ} = 20 \text{ дБм} + 14 \text{ дБи} - 2,26 \text{ дБ} = 31,74 \text{ дБм}$ (1493 мВт), то есть почти в 5 раз больше, чем в случае использования штатной изотропной антенны, где мощность сигнала в направлении максимального усиления составляет 20 дБм + + 5 дБи = 25 дБм (316 мВт).

Для соединения точки и антенны потребуются переходник с разъемами RP-N plug и N plug длиной 3 метра ANT24-ODU3M (рисунок 2.3, таблица 2.3). Эти кабели подойдут как для частоты 2,4 ГГц, так и на 5 ГГц и могут быть использованы и для наружного применения. На точке DAP-3690 четыре разъема RP-N jack. Два из них предназначены для подключения антенны работающей в диапазоне 2,4 ГГц, а два в диапазоне 5 ГГц. На антенне ANT1314 также два разъема N plug. Для обеспечения работы в режиме 802.11n необходимо задействовать оба антенных разъема. Поэтому кабелей ANT24-ODU3M для подключения антенны ANT1314

потребуется также 2 штуки. Поскольку вся эта конструкция будет находиться на улице, то не стоит забывать и про модули грозозащиты, которых тоже потребуется 2 штуки. Модули грозозащиты, которые позволяют защитить приёмо-передающее оборудование от грозовых разрядов, входят в комплект поставки точек доступа.



Рисунок 2.3 – Коаксиальный кабель D-Link ANT24-ODU3M

Таблица 2.3 – Основные технические характеристики коаксиального кабеля ANT24-ODU03M

Волновое сопротивление	50 Ом
Вносимое затухание на частотах от 2.4 до 2.5 ГГц	От 0.85 до 1 дБ
Рабочая среда	На улице и в помещении
Устойчивость к атмосферным воздействиям	Да
Оболочка кабеля	Черный полиэтилен
Рабочий диапазон температур	От -40 до +85 °С
Разъемы	RP-N и N -тип

В данном проекте для установки внешних антенн на кровле к/т «Луч» предлагается использовать модель телескопической мачты с системой крепежа на бетонную крышу 06114, изготовленной специально для Российского рынка российскими инженерами компании VINON (рисунок 2.4, таблица 2.4). Умеренная цена и гарантии качества стали причиной выбора продукции данной фирмы.

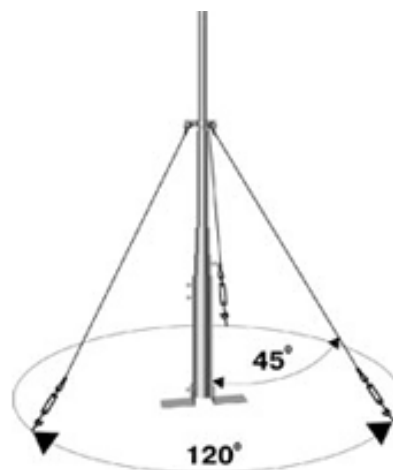


Рисунок 2.4 – Мачта связи с системой крепежа на бетонную крышу 06114

При переходе на диапазон 5 ГГц достаточно будет лишь заменить антенны на подходящие. Например, подходящим вариантом является Zyxel ANT3315.

Таблица 2.4 – Основные характеристики мачты связи с системой крепежа на бетонную крышу 06114

Тип мачты	Мачта антенная телескопического типа полимер стандарт 6
Материал	Углеродистая сталь ГОСТ 10705-80
Тип покрытия	Антикоррозийное
Покрытие	Полиэфирная порошковая краска Arsonsisi
Цвет	Синий
Количество колен	3
Длина колена	2 м
Диаметр колен	32, 40, 45 мм
Количество ярусов растяжек	1
Высота ярусов	3820 мм
Толщина стенки трубы	1,5 мм
Рабочая высота	5710 мм
Общие размеры	6000 мм
Транспортировочная длина	2,07 м
Вес	8,2 кг
Место установки	Бетонная крыша
Максимальная нагрузка на мачту	10 кг
Сфера применения	<ul style="list-style-type: none"> - эфирное и спутниковое телевидение; - сотовая связь; - транкинговая связь - электроэнергетика - WI-FI

Изм.	Лист	№ докум.	Подпись	Дата
------	------	----------	---------	------

БР – 02069964 – 11.03.02 – 14 – 19

Лист

44

2.3 Коммутатор Ethernet

При большом числе клиентов требуется большое число точек доступа. Для обеспечения разгрузки сети следует использовать коммутатор Ethernet. В настоящее время коммутаторы являются основным строительным блоком для создания компьютерных сетей. Сетевой коммутатор – это устройство, соединяющее нескольких узлов компьютерной сети в пределах одного или нескольких сегментов. Коммутатор работает на втором канальном уровне модели OSI.

Критерии, которыми следует руководствоваться при выборе коммутатора, могут быть сформулированы следующим образом:

- наличие портов 1000BASE-T Gigabit Ethernet;
- поддержка стандарта IEEE 802.3at (PoE);
- поддержка стандарта IEEE 802.1Q;
- возможность управления;

В данном проекте предлагается использование коммутатора серии D-Link DGS-1500 SmartPro (рисунок 2.5, таблица 2.5). Коммутаторы данной серии удовлетворяют всем выше перечисленным критериям. Это решение совмещает в себе самые передовые отраслевые стандарты с централизованной архитектурой и современными функциями, при помощи которых можно создать защищенную, выгодную с точки зрения затрат инфраструктуру.



Рисунок 2.5 – Коммутатор серии D-Link DGS-1500-28P SmartPro

Таблица 2.5 – Основные характеристики D-Link DGS-1500-28P SmartPro

Модель	D-Link DGS-1500-28P SmartPro
Количество	24 порта 10/100/1000 Мбит/с с функцией PoE, 4 порта SFP
PoE	- Стандарт PoE: 802.3af & 802.3at - Функции портов PoE: 15,4 Вт или 30 Вт на портах от 1 до 24
VLAN	- 802.1Q - Группы VLAN - Макс. 4К статических групп VLAN - Макс. 4094 VID GVRP VLAN до 256 динамических VLAN - Asymmetric VLAN
Управление	- Web-интерфейс GUI - Single IP Management - Compact CLI через Telnet - SNMP
Максимальная потребляемая мощность	- 447 Вт (PoE включен) - 30,1 Вт (PoE отключен)
Пропускная способность коммутатора	56 Гбит/с
Форм-фактор	Для установки в стандартную 19-дюймовую стойку, высота 1U
Габариты (Д x Ш x В)	440 мм x 310 мм x 44 мм
Вес	2,9 кг
Питание на входе:	100-240 В переменного тока, 50/60 Гц, внутренний универсальный источник питания
Рабочая температура	От -5° до +50°С

2.4 Аппаратно-программные средства

Основным элементом центра управления проектируемой сети является персональный компьютер, который также будет выполнять функции сервера. В связи с тем, что на него будет приходить большой поток данных, необходимо использовать аппаратные средства с высокими характеристиками.

Основное значение, конечно, придается процессору, так как это «мозг» компьютера. Предлагается выбрать процессор Intel Xeon E3-1270V3, основные характеристики которого представлены в таблице 2.6.

Такие характеристики процессора позволят работать серверу с очень большой производительностью. Также немаловажным аспектом является выбор материнской платы, так как она должна отвечать характеристикам процессора и дать ему

					БР – 02069964 – 11.03.02 – 14 – 19	Лист
Изм.	Лист	№ докум.	Подпись	Дата		46

возможность использовать все свои функции в полном объеме. Наиболее подходящей является материнская плата ASUS P9D-C/4L. Она обладает четырьмя слотами под память стандарта DDR3 ECC, усовершенствованной шиной PCI-Express, четырьмя портами 10/100/1000 Мбит/сек. и скоростной шиной для подключения винчестеров SATA RAID. Для данного сервера предлагается установить два модуля ОЗУ по 4 ГГб класса DDR3 ECC (DDR3 PC3-12800). Жесткий диск предполагается использовать Seagate Barracuda (ST1000DM003) 7200 64Mb SATA, размером 1 Тб. Такой объем позволит хранить огромное количество документов, нормативных баз и различных справочников. Согласно требованиям материнской платы предъявляемых к блоку питания подходящем вариантом является Chieftec A-80 (CTG-600-80P) мощностью 600 Вт. Данной мощности будет достаточно для питания всех основных составляющих сервера.

Таблица 2.6 – Основные характеристики процессора Intel Xeon E3-1270V3

Тактовая частота	3.5 ГГц
Гнездо процессора	Socket LGA1150
Кэш L1	64 Кб x4
Кэш L2	256 Кб x4
Кэш L3	8 Мб
Частота шины CPU	5000 МГц
Максимальный объем оперативной памяти	32 Гб
Дополнительные инструкции	SSE, SSE2, SSE3, SSE4.2, расширения AVX 2.0, AES, EVP, Intel Virtualization
Количество ядер	4 ядра
Тип поддерживаемой памяти	DDR3 ECC PC3-8500, PC3-10600
Рассеиваемая мощность	80 Вт
Технология изготовления	0.022 мкм

2.5 Бесперебойное питание

Для временного обеспечения питания аппаратуры при перебоях в подаче электроэнергии необходимо предусмотреть наличие бесперебойного питания. Это позволит обеспечить корректировку напряжения и частоты электропитания. Источники бесперебойного питания надежно защищают от потери информации,

					БР – 02069964 – 11.03.02 – 14 – 19	Лист
Изм.	Лист	№ докум.	Подпись	Дата		47

повреждений вычислительного и телекоммуникационного оборудования, сбоев технологического режима, выхода техники из строя при нарушении электроснабжения. Данная проблема особенно актуальна, поскольку в проекте предлагается использовать сервер.

Проведем расчет необходимой мощности ИБП. Коммутатор с включенным PoE потребляет 447 Вт. Мощность источника питания сервера 600 Вт. С учетом КПД (85%) источника питания сервера и потребляемой мощностью монитора максимальная потребляемая мощность сервера будет примерно составлять 730 Вт. Таким образом, мощность ИБП должна быть не менее 1177 Вт.

В данном проекте предлагается использовать ИБП Vanguard RM VRT-1500XL с максимальной выходной мощностью 1350 Вт (рисунок 2.6). Этот ИБП удовлетворяет требования предъявляемые к мощности. А возможность раздельного управления сегментами нагрузки позволяет осуществлять поэтапное отключение оборудования при пропадании входного напряжения. При этом энергия аккумуляторных батарей используется наиболее эффективно.



Рисунок 2.6 – ИБП Vanguard RM VRT-1500XL

2.6 Оконечное оборудование абонента

Для подключения к беспроводной сети Wi-Fi достаточно обладать ноутбуком или карманным персональным компьютером (ПКП) с подключенным Wi-Fi адаптером. Простейший вариант подключения удаленного компьютера к беспроводной сети представляет собой USB-адаптер с выходом на внешнюю антенну, ВЧ-кабель, и направленную антенну. Самый перспективный вариант –

					БР – 02069964 – 11.03.02 – 14 – 19	Лист
Изм.	Лист	№ докум.	Подпись	Дата		48

устройства, интегрированные непосредственно в материнскую плату компьютера. В настоящее время такие адаптеры используются на подавляющем большинстве мобильных компьютеров. Беспроводные адаптеры представлены на рисунке (рисунок 2.7).



Рисунок 2.7 – Беспроводные адаптеры:
а – с USB портом, б – встроенный в материнскую плату

Примерный комплект клиентского оборудования с USB -адаптером:

- 1) USB-адаптер – 1 шт.
- 2) Антенна направленная – 1 шт.
- 3) ВЧ-кабель – 1 шт.

В данном проекте предлагается использовать двухдиапазонный беспроводной 802.11n PCIe-адаптер фирмы D-Link <DWA-566> (рисунок 2.8).



Рисунок 2.8 – D-Link < DWA-566>

Адаптер D-Link < DWA-566> основан на последней усовершенствованной

технологии, применяемой в чипах для беспроводного оборудования, с улучшенными функциями безопасности для защиты беспроводного соединения от внешних вторжений. Эта беспроводная сетевая карта стандарта 802.11n поддерживает скорость беспроводного соединения до 300 Мбит/с при работе с другими устройствами стандарта 802.11n, обеспечивая высокую пропускную способность, позволяющую передавать интенсивный поток данных.

Технология PCI Express обеспечивает высокую пропускную способность и увеличенную производительность и позволяет подключать адаптер DWA-566 к любому PCIe слоту компьютера – x1, x4, x8, или x16. Это гарантирует отсутствие «узких мест» между процессором компьютера и адаптером беспроводной сети. Адаптер DWA-566 поддерживает WEP-шифрование данных, а также WPA и WPA2 для аутентификации пользователей беспроводной сети, обеспечивая высокий уровень защиты данных и канала связи.

В комплект поставки DWA-566 входит программа настройки, позволяющая компьютеру обнаружить доступные беспроводные сети, а также создать и сохранять детализированные профили подключения для наиболее часто используемых сетей. При использовании с другими продуктами серии D-Link сетевая карта автоматически подключится к сети.

В таблице 2.7 указаны основные характеристики данного устройства.

Таблица 2.7 – Основные характеристики D-Link < DWA-566 >

Производитель	D-Link
Модель	DWA-566
Основные характеристики	
Стандарты	IEEE 802.11a/b/g/n
Интерфейсы	PCIe x1, соответствие стандартным слотам PCIe x1/x4/x8/x16
Антенна	Съемная дипольная антенна с коэффициентом усиления 2 дБи
Диапазон частот	- Диапазон 2.4 ГГц: от 2.4 до 2.4835 ГГц - Диапазон 5 ГГц: от 5.15 до 6.825 ГГц
Скорость беспроводного соединения	IEEE 802.11n: 6.5~300 Мбит/с
Безопасность	- Wi-Fi Protected Access (WPA и WPA2) - WEP-шифрование данных 64/128-бит - Wi-Fi Protected Setup - PIN и PBC

Окончание таблицы 2.7

Выходная мощность передатчика	2.4ГГц/НТ 20 -18± 2dBm при MCS0/MCS8 -18± 2dBm при MCS1/MCS3/MCS9/MCS11 -18± 2dBm при MCS4/MCS12 -18± 2dBm при MCS5/MCS13 -17± 2dBm при MCS6/MCS14 -16± 2dBm при MCS7/MCS15
Чувствительность приемника	2.4ГГц/НТ 20 - 80dBm при MCS0 - 77dBm при MCS1 - 75dBm при MCS2 - 72dBm при MCS3 - 68dBm при MCS4 - 64dBm при MCS5 - 63dBm при MCS6 - 62dBm при MCS7
Дополнительные характеристики	
Рабочая температура	От 0° до 40°С
Вес	42.5 г
Сертификаты	FCC Class B, IC, -Wi-Fi - Wi-Fi Protected Setup - CE - C-Tick

Для увеличения дальности связи предлагается использовать абонентскую направленную антенну серии «Bester-Polyaris 2400-21» с сетевым адаптером D-Link <DWA-525>. Данная антенна параболического типа с усилением 21 дБ и устойчива к воздействию внешней среды. Обладает надежным крепежом, что дает возможность работы с вертикальной и горизонтальной поляризацией (рисунок 2.9). Основные характеристики антенны представлены в таблице 2.8.

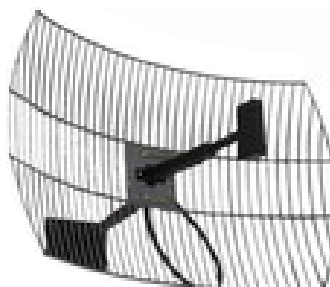


Рисунок 2.9 – Абонентская направленная антенна
серии «Bester-Polyaris 2400-21»

Таблица 2.8 – Основные характеристики антенны Bester-Polyaris 2400-21

Модель антенны «Bester-Polyaris»	2400-21
Диапазон частот, МГц	2300-2500
Поляризация	линейная (выбирается при установке)
Коэффициент усиления, дБ	21
Макс. подводимая мощность, Вт	50
Ширина диаграммы направленности	- В вертикальной плоскости 8° - В горизонтальной плоскости 8°
Входное сопротивление, Ом	50
Масса, кг	2,6
Габаритные размеры рефлектора, мм	800x460x130
Исполнение	всепогодное
Макс. скорость ветра, км/час	126

Доводить до каждого абонента отдельный радиоканал типа «точка-точка» нецелесообразно, так как высокоскоростной канал будет стоить дорого по технологическим причинам, а через низкоскоростной информация будет передаваться слишком медленно. Поэтому гораздо эффективнее предоставить один общий высокоскоростной канал типа «точка-много точек» в распоряжение сразу нескольких абонентов, которые будут использовать его совместно в коллизийном режиме, как в локальной сети Ethernet.



Рисунок 2.10 – Оконечное оборудование абонента

Применение стандарта Radio-Ethernet решает проблему подсоединения абонентов к большой сети передачи данных, или, как говорят связисты, проблему «последней мили», т.е. соединения между абонентом и ближайшим узлом «большой сети» (рисунок 2.10).

3 Проектирование сети беспроводного доступа

Для организации городской сети общего пользования, предназначенной для оказания услуг беспроводного доступа к информационным ресурсам, планируется развернуть беспроводную сеть общего пользования в Пролетарском районе г. Саранска для подключения отдельных пользователей к Региональной Сети Передачи Данных (РСПД) Республики Мордовия и выхода в международную информационную сеть Internet.

Зона обслуживания данной сети будет ограничиваться территорией, в пределах которой может быть установлена связь абонентских комплектов с базовыми станциями радиодоступа.

Архитектура сети открытая, что позволит добавлять новые базовые станции, а, следовательно, расширять зону охвата услугами и увеличивать количество абонентов без остановки функционирования сети.

В качестве исходных данных для проектирования сети беспроводного доступа г. Саранска используем техническое задание на разработку проекта.

3.1 Частотно-территориальное планирование

Для обеспечения зоны радиопокрытия, обеспечивающей стопроцентную вероятность установления связи, на первом этапе развертывания сети необходимо установить базовую станцию на территории Пролетарского района г. Саранска для подключения отдельных абонентов первого, второго, и шестого микрорайонов.

Проанализировав местность района, было решено, что в силу географических особенностей г. Саранска, а также расположения существующей застройки в данном районе города, не мешающей установлению прямой видимости, организовать узел Radio-Ethernet доступа на кровле здания к/т «Луч», расположенного по адресу: ул. Веселовского, 40А.

Карта с результатом исследования и с указанным на ней местом, с

					БР – 02069964 – 11.03.02 – 14 – 19	Лист
Изм.	Лист	№ докум.	Подпись	Дата		53

координатами: северная широта $54^{\circ}13'$ и восточная долгота $45^{\circ}08'$, где мы будем размещать оборудование сети беспроводного доступа, приведена на рисунке 3.1.

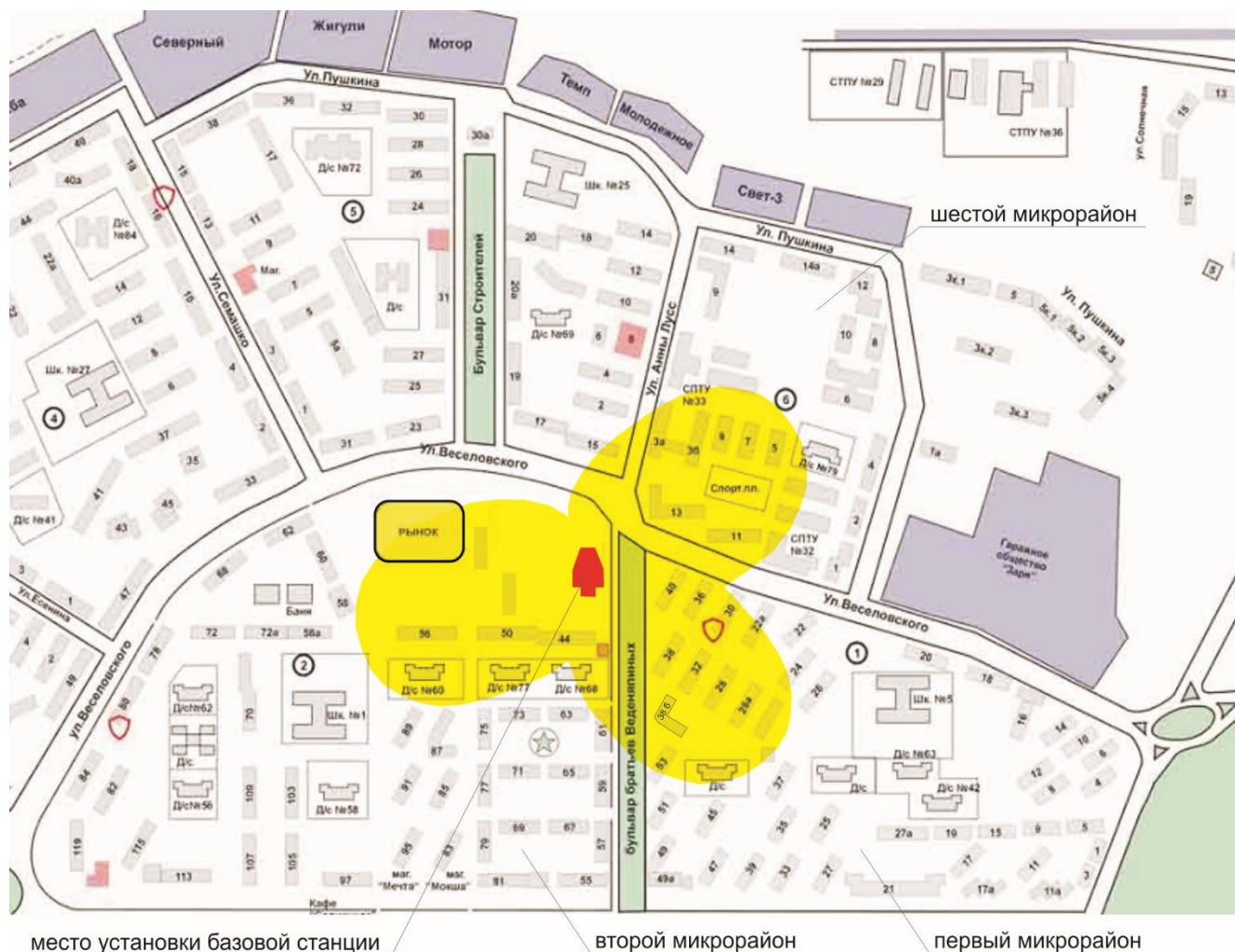


Рисунок 3.1 – Месторасположение здания для размещения оборудования сети беспроводного доступа

При проведении частотно-территориального планирования необходимо учитывать, что для базовой станции радиодоступа, устанавливаемой на данном этапе в Пролетарском районе и включающей в себя три Wi-Fi устройства радиодоступа (точки доступа), необходим подбор частот для исключения возможности создания взаимных помех. Имеются три частотных канала, которые можно одновременно использовать в одном и том же месте. Соответственно, точки доступа (ТД), каждая из которых настроена на один из этих трех каналов, можно

разместить таким образом, что они будут работать на разных частотах.

Интерференция – физическое явление, которое возникает при наложении двух (или более) волн от одинаковых источников и приводит к усилению или ослаблению амплитуды волны. Поэтому борьба с интерференцией – одна из основных задач при частотном планировании, то есть распределении частот по сотам (ячейкам).

Согласно частотно-территориальному плану, ТД №1 будет работать на первом канале ($f = 2412$ МГц), ТД №2 – на шестом ($f = 2437$ МГц), а ТД №3 – на одиннадцатом ($f = 2462$ МГц).

3.2 Структурная схема проектируемой сети

Построение сети беспроводного доступа г. Саранска подразумевает сопряжение беспроводного канального сегмента сети и существующей инфраструктуры сетевого и каналобразующего оборудования Internet-провайдера. В проекте беспроводной части СПД подразумевается связывание этого сегмента с уже существующей сетью Internet-провайдера на уровне базовых станций по порту Ethernet.

В результате проведенного анализа оборудования различных фирм производителей по техническим и стоимостным характеристикам было принято решение о проектировании сети абонентского радиодоступа с использованием комплекса оборудования беспроводного доступа стандарта IEEE 802.11n фирмы D-Link, имеющего сертификат соответствия № РОСС ТW.АЯ46.В06652.

Далее перед нами ставится задача разработки структурной схемы проектируемой сети. Структурную схему разработаем для зданий, расположенных в непосредственной близости от базовых станций. С учетом вышеизложенных вариантов развертывания и особенностей беспроводных сетей, необходимо выбрать такой режим, который бы наилучшим образом обеспечил выполнение следующих основных требований:

- тип связи: Wi-Fi (IEEE 802.11n);
- радиус действия: 300–400м;

- количество абонентов: до 100 абонентов;
- пропускная способность: до 300 Мбит/с для 802.11n;
- частотный диапазон: 2400 - 2483,5 МГц.

Данным проектом предусматривается организация узла Radio-Ethernet доступа.

Базовая станция (БС) в общем случае представляет собой комплект оборудования, позволяющего предоставить доступ к опорной сети по беспроводному каналу нескольким удаленным клиентам. При этом БС, как правило, имеет за собой опорную сеть с выходом в Internet и может предоставлять радиодоступ в Internet подключенным к ней удаленным клиентам.

В простейшем варианте БС оснащается двумя всенаправленными антеннами 2-5 дБ усиления (может быть использован усилитель для увеличения радиуса действия) и устройством радиодоступа. Подключение клиентов в рамках данного проекта предполагает использование другого варианта. С одной стороны, поставленную задачу решила бы базовая станция с всенаправленной антенной, однако есть одно «но». Всенаправленная антенна предполагает небольшие расстояния при равномерном излучении на 360 градусов. В условиях городской застройки это приводит к высокому уровню промышленных помех и, как следствие, еще большему сокращению расстояния качественной связи. Поэтому имеет смысл использовать секторные антенны.

Одним из эффективных способов организации базовой станции является использование нескольких Wi-Fi устройств радиодоступа с секторными антеннами. В проекте предусмотрено использование трех точек доступа D-Link AirPremier DAP-3690 и трех секторных антенн ANT1314. Такой вариант наиболее актуален для сетей с высоким абонентским трафиком и позволяет подключать до 100 беспроводных Wi-Fi клиентов. Использование нескольких Wi-Fi устройств радиодоступа позволяет существенно увеличить скорости передачи и качество обслуживания клиентов.

На установленной на кровле здания к/т «Луч» телескопической мачте с

					БР – 02069964 – 11.03.02 – 14 – 19	Лист
						56
Изм.	Лист	№ докум.	Подпись	Дата		

системой крепежа на бетонную крышу 06114 монтируются три беспроводные точки доступа AirPremier DAP-3690. Портом 1000Base-T базовые станции подключаются к коммутатору, расположенному в технологическом помещении на техническом этаже к/т «Луч». К базовым станциям подключаются антенно-фидерные устройства.

Варианты необходимого клиентского Wi-Fi оборудования зависят от архитектуры подключаемой сети (одиночный компьютер или локальная сеть), режима доступа в сеть (постоянный, или только при включенном компьютере), требований к администрированию.

Простейший вариант подключения удаленного компьютера по Wi-Fi к сети представляет собой портативный компьютер со встроенным Wi-Fi адаптером. Возможен вариант и USB-радиокарточки с выходом на внешнюю антенну. Варианты подключения беспроводных клиентов были рассмотрены в Главе 2.

Все абоненты находятся в зоне прямой видимости, что позволит им обеспечить необходимое качество связи без использования усилителей. Посредством комплектов абонентского оборудования потребители подключаются по радиоканалу к одной из точек доступа и становятся абонентами сети.

Типичная архитектура сети Wi-Fi включает в себя несколько точек доступа, соединенных между собой кабельными сетями и подключенных выделенным каналом к сети Internet-провайдера. Структурная схема проектируемой сети беспроводного доступа г. Саранска показана на рисунке 3.2.

Управление сетью будет осуществляться из центра управления. Рабочее место оператора, обслуживающего работу сети, будет размещаться в технологическом помещении на техническом этаже к/т «Луч». Основным элементом центра является персональный компьютер со средствами ввода и вывода информации, связанный со всеми точками доступа и управляющий ими с помощью ПО сетевого управления D-Link D-View 6.0, входящего в состав оборудования беспроводного доступа.

Оператору будут доступны (без прерывания связи) следующие функции:

- ввод/вывод в/из обслуживания абонентов;
- прописка абонентов;
- техническое обслуживание;

					БР – 02069964 – 11.03.02 – 14 – 19	Лист
Изм.	Лист	№ докум.	Подпись	Дата		57

- диагностика сети.

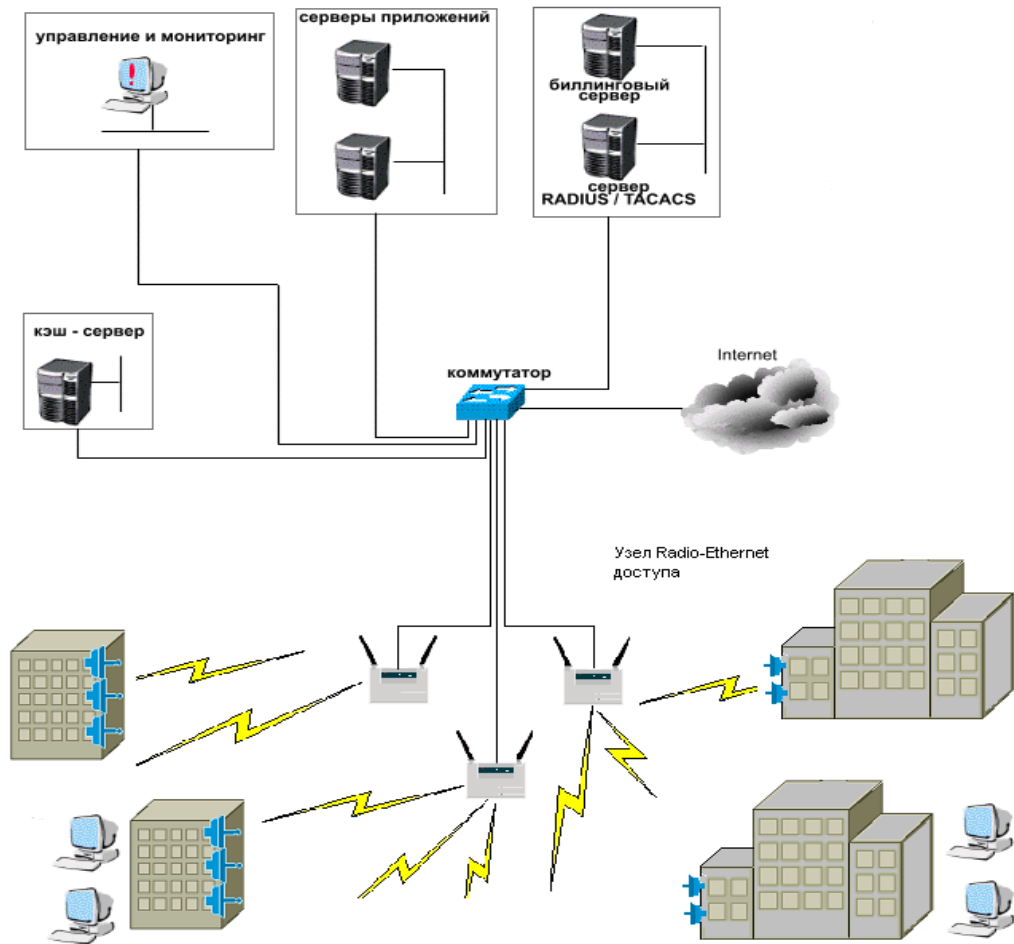


Рисунок 3.2 – Структурная схема проектируемой сети

Программное обеспечение позволяет производить удаленную конфигурацию и диагностику работы оборудования базовых станций. Центр управления осуществляет функции контроля качества соединений, нагрузки каналов, контроля эфира:

- аутентификация абонентов;
- ограничение скорости для каждого удаленного абонента;
- IP-маршрутизация и поддержка виртуальных сетей.

Все услуги телематических служб будут осуществляться с использованием стандартных программных средств (Linux) и стандартного технологического оборудования, сертифицированного для применения в ЛВС.

В области служебных серверов находятся автоматизированная система расчета (биллинговая система) и сервер RADIUS (TACACS).

Сервера приложений свободно доступны со стороны внешней сети. Этот сегмент включает в себя: www – сервер, обеспечивающий абонентов оператора связи и остальных интересующихся пользователей сети Интернет необходимой информацией; общедоступный ftp – сервер; почтовый сервер и сервер DNS.

Между всеми подсистемами узла связи определены интерфейсы.

В локальной сети узла на уровне сетевого интерфейса, который включает физический и канальный уровень модели OSI, в зависимости от подсистемы, это может быть Ethernet, Fast Ethernet или Gigabit Ethernet. Для пользователей, которые подключаются к серверу удаленного доступа, на канальном уровне используется протокол PPP (Point-to-Point Protocol).

На сетевом уровне применяется Internet Protocol.

Управление и мониторинг обеспечиваются с помощью протокола прикладного уровня SNMP (Simple Network Management Protocol).

Интерфейс между серверами удаленного доступа и биллинговой системой реализуется с помощью протокола RADIUS (Remote Authentication Dial In User Service).

Теперь подробнее рассмотрим все элементы Radio-Ethernet доступа, необходимые для обеспечения требуемых услуг.

3.2.1 Беспроводной клиент

На рисунке 3.2 представлена обобщенная схема сети, на которой показаны абоненты, представляющие собой рабочие станции, то есть персональный компьютер, в составе которого: системный блок, устройства ввода-вывода информации, адаптер D-Link <DWA-566>, имеющий выход на внешнюю антенну.

Компьютер абонента должен удовлетворять определенным требованиям по частоте, памяти и другим характеристикам. Эти требования следующие: процессор не ниже Pentium III 800 Mhz, память не менее 128Mb, операционная система

					БР – 02069964 – 11.03.02 – 14 – 19	Лист
Изм.	Лист	№ докум.	Подпись	Дата		59

Windows 7, XP или Vista (32/64 bit). Остальные параметры не так нормированы, но должны быть на должном уровне. Конфигурация станций может меняться в зависимости от вида работ, выполняемых на ней.

3.2.2 Точка доступа

Взаимодействие клиента и точки доступа происходит следующим образом. Когда клиент попадает в зону действия точки доступа, он на основе мощности сигнала и наблюдаемого значения количества ошибок выбирает и подключается к ней. Как только клиент получает подтверждение того, что он принят точкой доступа, он настраивается на радиоканал, в котором она работает.

К точке доступа можно подключить порядка 30-40 абонентов. Теоретически, можно и 100 (пользователи делят между собой полосу пропускания), но все 100 абонентов одновременно не смогут загрузить большой объем информации. Для того чтобы избежать таких проблем, необходимо применять сегментное деление пользователей на несколько точек доступа.

Если часть клиентов находится в зоне покрытия сразу нескольких точек доступа, то распределение клиентов по ним складывается практически спонтанно. В результате при достаточно высокой плотности размещения клиентов возможна ситуация, когда одни клиенты будут работать в условиях жесткого лимита, а другие не будут использовать всю доступную (и на данный момент невостробованную) полосу пропускания находящейся рядом точки доступа.

Распределить нагрузку можно, используя специальный режим Load Balancing. В этом случае несколько (до трех) точек устанавливаются в пределах одной, незначительно расширенной по площади зоны покрытия. Между собой точки соединяются стандартным кабелем и способны обмениваться служебной информацией и передавать друг другу пользователей.

Рассчитаем пропускную способность на каждого пользователя в сети стандарта IEEE 802.11n.

					БР – 02069964 – 11.03.02 – 14 – 19	Лист
Изм.	Лист	№ докум.	Подпись	Дата		60

Если 35 пользователей одновременно подключаются к одной точке доступа, поддерживающей стандарт IEEE 802.11n, с максимальной пропускной способностью 300 Мбит/с, то теоретически пользователи делят между собой все 300 Мбит/с. Но в действительности полоса пропускания гораздо меньше 300 Мбит/с, так как речь идет о «технической» скорости передачи битов в физическом канале. Кроме информации, сообщение должно содержать служебную часть. К тому же, необходимо время для установления связи и синхронизации. Реальная скорость передачи информации, как правило, не превышает 50-60% технической. Поскольку точки доступа будут работать в частотном диапазоне 2,4 ГГц с шириной канала 20 МГц, то возможная максимальная скорость будет составлять 144,4 Мбит/с (см. таблицу 1.1). В среднем реальная скорость не превысит 80 Мбит/с.

В данном проекте предполагается, что точки доступа будут работать в режиме с высокой пропускной способностью НТ (High Throughput), который предполагает отсутствие поблизости (в зоне покрытия) работающих устройств 802.11b/g, использующих ту же полосу частот. Таким образом, в этом режиме разрешены к использованию только клиенты 802.11n, что позволит воспользоваться преимуществами повышенной скорости и увеличенной дальностью передачи данных, обеспечиваемыми стандартом 802.11n.

Воспользуемся формулой (3.1) и определим максимальную пропускную способность на одного абонента сети:

$$C_{max} = \frac{V_p}{n}, \quad (3.1)$$

где C_{max} – максимальная пропускная способность на одного пользователя, Мбит/с;

V_p – реальная скорость передачи информации, Мбит/с;

n – число абонентов, подключенных к одной точке доступа.

Если подставим в формулу (3.1) значения, то получим:

$$C_{max} = \frac{80}{35} = 2,3 \text{ Мбит/с.}$$

					БР – 02069964 – 11.03.02 – 14 – 19	Лист
Изм.	Лист	№ докум.	Подпись	Дата		61

3.2.3 Коммутатор

Коммутатор Ethernet располагается в монтажном шкафу на техническом этаже к/т «Луч», от которого идет кабель к отдельным точкам доступа. Каждая точка доступа подсоединяется непосредственно к порту коммутатора с помощью кабеля FTP cat.5e.

При построении узла Radio-Ethernet доступа будут использоваться три точки доступа, таким образом возникает необходимость соединения нескольких узлов сети. Решается данная задача использованием коммутатора. Коммутатор Ethernet работает на канальном (втором) уровне модели OSI и представляет собой устройство для организации сетей большого размера. В отличие от концентратора, который распространяет трафик от одного подключенного устройства ко всем остальным, коммутатор передает данные только непосредственно получателю (исключение составляет широковещательный трафик всем узлам сети и трафик для устройств, для которых не известен исходящий порт коммутатора). Это повышает производительность и безопасность сети, избавляя остальные сегменты сети от необходимости (и возможности) обрабатывать данные, которые им не предназначались.

3.2.4 Подсистема мониторинга и управления

Подсистема мониторинга и управления позволяет осуществлять контроль за состоянием портов, своевременное обнаружение канальных сбоев, предоставление и исследование статистической информации о работе протоколов и служб. Кроме того, средства конфигурирования существенно снижают время, необходимое для Установки нового или обновления уже имеющегося оборудования. Сокращается число ошибок, возникающих при этих процессах.

Подсистема мониторинга и управления отображает:

– информацию о сеансах работы пользователей, регистрацию входа в систему и статистику подключений;

					БР – 02069964 – 11.03.02 – 14 – 19	Лист
Изм.	Лист	№ докум.	Подпись	Дата		62

- информацию уровня сетевых протоколов (IP);
- информацию о коммутаторах, концентраторах, мостах;
- информацию о точках подключения.

Такой исчерпывающий подход позволяет сетевым администраторам, обслуживающим данную сеть, иметь полное представление о работе сети, включая выявление неисправностей с анализом их причин, мониторинг производительности или планирование мощности (емкости).

Сетевые администраторы должны иметь возможность проводить сетевой мониторинг в реальном масштабе времени и день за днем накапливать данные о реальной производительности сети. Различные приложения следят за разными аспектами работы сети. Сбор данных может быть автоматизирован и может проводиться в фоновом режиме по заранее составленному графику.

Обеспечивается непрерывный мониторинг всех имеющихся в сети устройств. При возникновении проблемы и выявлении отказов оператору выдается предупреждение. Оператор должен быть в состоянии мгновенно установить, в каком месте сети и/или в каком устройстве возникла неисправность.

3.2.5 Кэширующий сервер

Использование кэширующего сервера обеспечивает снижение нагрузки на внешние каналы и, следовательно, сокращение затрат.

Успех бизнеса провайдера Internet во многом зависит от его способности справляться с ежедневным ростом трафика, кроме того, делать это без понижения производительности. Поэтому, провайдеры любого уровня рано или поздно приходят к необходимости использования специализированных серверов, которые кэшируют содержимое web-страниц. Кэширование позволяет построить надежную инфраструктуру, способную справляться с ростом трафика без необходимости наращивания пропускной способности внешних каналов.

Кэш-сервер действует следующим образом. Предположим, пользователь скопировал из внешней сети какую-либо информацию, однако во время этого

					<i>БР – 02069964 – 11.03.02 – 14 – 19</i>	<i>Лист</i>
						63
<i>Изм.</i>	<i>Лист</i>	<i>№ докум.</i>	<i>Подпись</i>	<i>Дата</i>		

процесса данная информация передавалась не только на рабочую станцию пользователя, но и сохранялась на кэш – сервере. Поэтому, если через непродолжительное время другой пользователь попытается скопировать информацию из внешней сети, она будет передана ему из кэш – сервера.

Этим обеспечивается снижение нагрузки на внешние каналы на 30 – 70 %.

3.2.6 Биллинговая система

Биллинговая система - программный комплекс, осуществляющий учет объема потребляемых абонентами услуг, расчет и списание денежных средств в соответствии с тарифами компании.

Задачи, которые должна решать полнофункциональная биллинговая система:

- сбор информации о потребляемых услугах (аккаунтинг);
- аутентификация и авторизация абонентов;
- контроль денежных средств на счетах абонентов и списание средств в соответствии с действующей тарифной сеткой;
- пополнение счетов абонентов;
- внесение изменений в тарифы;
- предоставление статистики по операциям.

Система биллинга должна взаимодействовать с точками доступа и желательно с пограничными маршрутизаторами провайдера и серверами телематических служб. При взаимодействии с пограничными маршрутизаторами провайдера система биллинга получает информацию об объёме внешнего трафика, принятого и переданного с отдельных IP-адресов. Трафик, проходящий по различным внешним каналам, учитывается отдельно, что даёт возможность гибкой тарификации в зависимости от стоимости их использования.

					БР – 02069964 – 11.03.02 – 14 – 19	Лист
Изм.	Лист	№ докум.	Подпись	Дата		64

3.3 Аутентификация пользователей

Для организации процесса аутентификации пользователей существует множество способов. В данном проекте предлагается решение этой задача программными средствами, установленными на компьютере. Существуют и специализированные аппаратные решения, но сути дела это не меняет – подобные устройства в первую очередь не обладают достаточной гибкостью, а во вторых, цена их не ниже, чем цена компьютера (без ПО). Теперь перейдем к рассмотрению специализированного программного обеспечения, выбор которого основан на так называемых open-source решениях.

Функцию контроллера доступа, которая либо выпускает пользователя из локальной сети в интернет, либо нет, будет выполняться программой Chillispot. Это бесплатное ПО с открытым исходным кодом. Chillispot выполняет три функции – во-первых, для организации локальной сети запускает свой собственный DHCP-сервер, во вторых, служит шлюзом, который выпускает авторизованных клиентов в интернет, а неавторизованных отправляет на страницу авторизации, и в третьих, предоставляет саму страницу авторизации. DHCP сервер используется для того, чтобы максимально упростить клиенту задачу подключения к узлу Radio-Ethernet. Страница авторизации позволяет клиенту ввести логин и пароль. Шлюз сверяет предоставленные клиентом данные с базой учетных записей узла Radio-Ethernet, и, если все верно, выпускает клиента в интернет. Для работы Chillispot необходим, во-первых, работающий веб-сервер, так как страница авторизации – это обычная веб-страница, а во-вторых, сервер авторизации и учета.

Разновидностей серверов авторизации, аутентификации и учета (RADIUS) существует множество. Но из числа бесплатных и с открытым исходным кодом наиболее популярным является FreeRADIUS. Этот сервер легко настраивается на работу с практически любой базой данных SQL и позволяет легко организовать взаимодействие с практически любым биллингом, который может писать и читать данные в базах данных SQL.

Биллинговая система также является важным компонентом узла Radio-

					БР – 02069964 – 11.03.02 – 14 – 19	Лист
Изм.	Лист	№ докум.	Подпись	Дата		65

Ethernet и во многом определяет его возможности. Корректная работа узла Radio-Ethernet возможна лишь в случае, если все три выше перечисленные системы правильно настроены на взаимную работу. В качестве биллинговой программы предполагается использовать Easyhotspot. Вспомогательными службами в данном случае выступают веб-сервер и сервер баз данных. Из числа широко и бесплатно доступных, а также, легко устанавливаемых были выбраны Apache и MySQL.

Рассмотрим процесс взаимодействия всей системы. Предположим, клиент подключается к узлу Radio-Ethernet и пытается попасть на какой-то сайт в интернете. Chillispot перехватывает DNS-запрос клиента и проверяет авторизован ли он. Если клиент не авторизован (не вводил логин и пароль ранее), то он перенаправляется на страницу авторизации (сиреневая стрелка на рисунке 3.3). На странице авторизации клиент вводит выданные ему логин и пароль. Страница авторизации отдает полученные от клиента логин и пароль Chillispot (сиреневая стрелка). Chillispot полученные логин и пароль отправляет на проверку серверу авторизации и учета RADIUS (зеленая стрелка). Сервер RADIUS полученные данные (логин и пароль) сверяет с данными, хранящимися в базе учетных записей в сервере MySQL (синяя стрелка). По результатам проверки возможны два варианта. Первый – логин и/или пароль не верны. В этом случае сервер RADIUS отвечает Chillispot отказом и последний не пускает клиента в интернет, а снова выводит ему страницу авторизации. В случае, когда пароль и логин совпадают с данными, присутствующими в базе учетных записей сервер RADIUS считывает из базы учетных записей все атрибуты, которые там найдет для указанного клиента (поиск идет по логину). Атрибуты эти можно разделить на две группы. К первой относятся атрибуты для проверки – check, ко второй – reply. В итоге, если логин и пароль клиента верны, сервер RADIUS сначала выполняет соответствующие проверки для всех тех атрибутов, которые относятся к группе check. И только когда эти проверки завершены успешно, клиент имеет право получить доступ в интернет. В этом случае сервер RADIUS отправляет контроллеру доступа Chillispot положительный ответ. И в этот ответ RADIUS добавляет еще и все те атрибуты, которые были считаны для данного клиента и относятся к группе reply.

					БР – 02069964 – 11.03.02 – 14 – 19	Лист
Изм.	Лист	№ докум.	Подпись	Дата		66

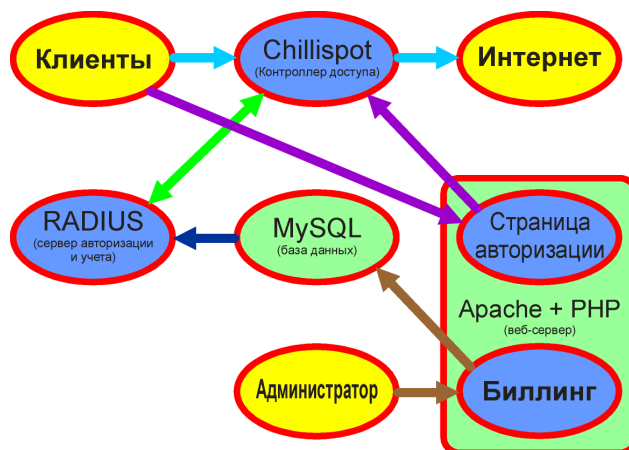


Рисунок 3.3 – Схема аутентификации пользователей

Теперь несколько слов об атрибутах. К атрибутам группы check относятся (для случая работы с контроллером доступа Chillispot) например, такие как Max-All-Session или Simultaneous-Use. Первый из них определяет максимальную суммарную длительность всех сессий клиента в интернете. Второй, определяет число клиентов, подключенных к интернету одновременно с указанными логином и паролем. Атрибуты reply указывают контроллеру доступа с какими параметрами подключать клиента к интернету. Типичным примером могут служить атрибуты WISPr-Bandwidth-Max-Down и WISPr-Bandwidth-Max-Up. Эти атрибуты ограничивают максимальную скорость передачи данных к/от клиента соответственно.

3.4 Антенно-фидерная система

Антенно-фидерная система (АФС) проектируемого объекта построена на базе трех секторных приемо-передающих антенн ANT1314. Антенны предназначены для работы в составе приемо-передающих систем в сети радиодоступа в диапазоне 2.4 ГГц.

АФС состоит из трех секторов. Антенна сектора 1 (подключена к ТД №1 и направлена в сторону шестого микрорайона) ориентирована в направлении азимута 45°, сектора 2 (подключена к ТД №2 и направлена в сторону первого микрорайона) – в направлении азимута 135°, сектора 3 (подключена к ТД №3 и направлена в

сторону второго микрорайона) – в направлении азимута 260° (рисунок 3.4). Благодаря такому расположению антенн в пространстве достигается максимальная площадь покрытия.

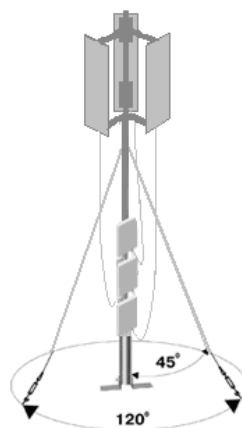


Рисунок 3.4 – Антенно-фидерная система

Каждая ТД подключается к отдельной антенне. В качестве фидеров используется пара кабелей типа ANT24-ODU3M с вносимым затуханием на частоте 2.4 ГГц не более 1 дБ.

Антенно-фидерный тракт проектируемой сети представлен на рисунке 3.5.



Рисунок 3.5 – Антенно-фидерный тракт проектируемой беспроводной сети

Цифрами обозначено:

1) точка доступа D-Link AirPremier DAP-3690;

- 2) кабель ANT24-ODU3M;
- 3) модуль грозозащиты (в комплекте с точкой доступа);
- 4) антенна секторная ANT1314.

Антенны размещены на телескопической мачте с системой крепежа на бетонную крышу 06114, установленной на кровле здания к/т «Луч». Точки доступа размещаются там же.

3.5 Электропитание

Основными потребителями электрической энергии на объекте являются: коммутатор, точки доступа, компьютер.

Электропитание проектируемого оборудования базовой станции осуществляется от источника бесперебойного питания, который расположен в монтажном шкафу. ИБП запитан от сети переменного тока 220В частотой 50 Гц от существующей стойки питания, находящейся на техническом этаже здания к/т «Луч».

Электроснабжение базовой станции запроектировано в соответствии с действующими «Правилами устройства электроустановок ПУЭ», ГОСТ Р 50571.1-93 «Электроустановки зданий. Основные положения» и СНиП 3.05.06-85 «Электротехнические устройства».

3.6 Заземление и молниезащита

Для защиты антенно-фидерных трактов, выходов приемопередатчиков от наведенного электромагнитного импульса грозовых разрядов в проекте предусмотрено использование модулей грозозащиты.

Заземление проектируемого оборудования предусматривается от существующих заземляющих устройств (шины защитного заземления стойки питания), расположенных на техническом этаже здания к/т «Луч». Для защитного заземления электрооборудования в помещении используется провод заземления ПВЗ-6.0.

					БР – 02069964 – 11.03.02 – 14 – 19	Лист
Изм.	Лист	№ докум.	Подпись	Дата		69

Молниезащитное заземление телескопической мачты обеспечить сварным соединением с заземлителями токоотводом из стали круглого сечения диаметром 10 мм.

Заземление оборудования выполнено в соответствии с требованиями по обеспечению безопасности ГОСТ 50571.3-94 «Электроустановки зданий. Защита от поражения электрическим током» и ПУЭ.

3.7 Оценка сделанных предложений

Сделанное в данном проекте предложение по организации узла Radio-Ethernet доступа позволяет решить задачу подключения отдельных пользователей, не имеющих проводных каналов доступа к сети общего пользования оператора связи, к Региональной Сети Передачи Данных (РСПД) Республики Мордовия и выхода в международную информационную сеть Internet.

Преимуществом сети является максимальная простота и удобство в установке и эксплуатации. Оборудование запроектировано в соответствии с современными требованиями управления системой, содержит встроенные механизмы установки и поддержки при внедрении, обеспечивающие простой и быстрый запуск. При возникновении необходимости в увеличении емкости сети предложенное решение демонстрирует свою превосходную способность к масштабированию, удовлетворяя новые требования к площади покрытия, плотности абонентов и пропускной способности.

Проведем расчет радиоканала передачи данных, который включает в себя следующие этапы:

- 1) расчет затухания в антенно-фидерном тракте;
- 2) расчет эффективной изотропно-излучаемой мощности;
- 3) расчет суммарного усиления радиосистемы;
- 4) расчет дальности работы беспроводного канала связи;
- 5) расчет суммарных потерь радиосистемы;
- 6) расчет энергетического запаса радиоканала.

					БР – 02069964 – 11.03.02 – 14 – 19	Лист
						70
Изм.	Лист	№ докум.	Подпись	Дата		

3.7.1 Расчет затухания в антенно-фидерном тракте (АФТ)

Потери в АФТ приемника и передатчика складываются из следующих величин: затухание в кабеле; затухание в разъемах; затухание в дополнительном антенно-фидерном оборудовании (разветвителях, согласующих устройствах и др.).

И определяются по следующей формуле:

$$W_{АФТ} = W_C L + W_{CC} N + W_{доп}, \quad (3.2)$$

где W_C – погонное затухание сигнала в кабеле на рабочей частоте, дБ/м;

L – длина кабеля, м;

W_{CC} – потери в разъеме, дБ;

N – количество разъемов, шт;

$W_{доп}$ – потери в дополнительном антенно-фидерном оборудовании, дБ.

В проектируемой беспроводной сети отсутствует усилитель, и антенно-фидерный тракт состоит только из пассивных элементов (рисунок 3.5). Расстояние, на которое возможно вынести антенну в данном случае, сильно ограничивается мощностью передатчика точки доступа и затуханием, вносимым пассивными элементами. При выносе антенны на большое расстояние как принятый антенной, так и переданный передатчиком сигнал может полностью поглотиться кабельными сборками и переходниками. Затухание на трех разъемах берём за 1,2 дБ, грозозрядник имеет затухание порядка 0,2 дБ.

По формуле (3.2) потери в АФТ приемо-передатчика составляют:

$$W_{АФТ} = 0,285 \cdot 3 + 0,4 \cdot 3 + 0,2 = 2,26 \text{ дБ.}$$

3.7.2 Расчет эффективной изотропно-излучаемой мощности

Эффективная изотропно-излучаемая мощность (Effective Isotropic Radiated Power, EIRP) – реальная выходная мощность, излучаемая антенной,

					БР – 02069964 – 11.03.02 – 14 – 19	Лист
						71
Изм.	Лист	№ докум.	Подпись	Дата		

рассчитываемая как $IR +$ коэффициент усиления антенны.

Эффективная изотропно-излучаемая мощность определяется по формуле:

$$EIRP = P_{нрд} - W_{АФТнрд} + G_{нрд}, \quad (3.3)$$

где $P_{нрд}$ – выходная мощность передатчика, дБм;

$W_{АФТнрд}$ – потери сигнала в АФТ передатчика, дБ;

$G_{нрд}$ – усиление антенны передатчика, дБи.

Исходные данные для расчета представлены в таблице 3.1

Таблица 3.1 – Исходные данные для расчета ЭИИМ

Обозначение	Наименование	Ед. изм.	Значение
$P_{нрд}$	выходная мощность передатчика	дБм	20
$G_{нрд}$	коэффициент усиления антенны	дБи	14
$W_{АФТнрд}$	потери сигнала в АФТ передатчика	дБ	2,26

По формуле (3.3) эффективная изотропно-излучаемая мощность составляет:

$$EIRP = 20 - 2,26 + 14 = 31,74 \text{ дБм.}$$

3.7.3 Расчет суммарного усиления радиосистемы

Для того чтобы определить суммарное усиление радиосистемы, необходимо знать следующие параметры:

- выходную мощность передатчика;
- чувствительность приемного тракта удаленной точки;
- коэффициенты усиления антенн передатчика и приёмника;
- коэффициенты усиления усилителей (при их наличии);
- потери сигнала в АФТ передатчика и приемника.

Суммарное усиление радиосистемы вычисляется по формуле:

$$G_{\Sigma} = P_{\text{прд}} - P_{\text{прм}} + G_{\text{прд}} + G_{\text{прм}} - W_{\text{АФТпрд}} - W_{\text{АФТпрм}}, \quad (3.4)$$

где $P_{\text{прд}}$ – выходная мощность радиопередатчика, дБм;

$P_{\text{прм}}$ – чувствительность приемника, дБм;

$G_{\text{прд}}$ – усиление антенны передатчика, дБи;

$G_{\text{прм}}$ – усиление антенны приемника, дБи;

$W_{\text{АФТпрд}}$ – потери сигнала в АФТ передатчика, дБ;

$W_{\text{АФТпрм}}$ – потери сигнала в АФТ приемника, дБ.

Исходные данные для расчета суммарного усиления радиосистемы представлены в таблице 3.2.

Таблица 3.2 – Исходные данные для расчета суммарного усиления радиосистемы

Обозначение	Наименование	Ед. изм.	Значение
$W_{\text{АФТпрд}}$	Потери сигнала в АФТ передатчика	дБ	2,26
$W_{\text{АФТпрм}}$	Потери сигнала в АФТ приемника	дБ	2,26
$G_{\text{прд}}$	Усиление антенны передатчика	дБи	14
$G_{\text{прм}}$	Усиление антенны приемника	дБи	14
$P_{\text{прд}}$	Выходная мощность передатчика	дБм	20
$P_{\text{прм}}$	Чувствительность приемника	дБм	-72

По формуле (3.4) суммарное усиление радиосистемы составляет:

$$G_{\Sigma} = 20 - (-72) + 14 + 14 - 2,26 - 2,26 = 115,5 \text{ дБм.}$$

3.7.4 Расчет дальности работы беспроводного канала связи

Формула расчета дальности берется из инженерной формулы расчета потерь в свободном пространстве (Free Space Loss):

$$W_0 = 33 + 20(\lg F + \lg D), \quad (3.5)$$

где W_0 – потери в свободном пространстве (дБ);

F – центральная частота канала, на котором работает система связи (МГц);

D – расстояние между двумя точками (км).

W_0 определяется суммарным усилением системы (формула 3.4) и вычисляется по формуле:

$$W_0 = G_{\Sigma} - SOM, \quad (3.6)$$

где SOM (System Operating Margin) – в энергетике запас радиосвязи (дБ), который учитывает возможные факторы, отрицательно влияющие на дальность связи, такие как:

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

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

$$W_0 = 115,5 - 10 = 105,5 \text{ дБ.}$$

В итоге получим формулу дальности связи:

$$D = 10^{\left(\frac{W_0 - 33}{20} - \lg F\right)}. \quad (3.7)$$

По формуле (3.7) максимальная дальность работы беспроводного канала связи составляет:

$$D = 10^{\left(\frac{105,5 - 33}{20} - \lg 2400\right)} \approx 1,8 \text{ км.}$$

					<i>БР – 02069964 – 11.03.02 – 14 – 19</i>	<i>Лист</i>
<i>Изм.</i>	<i>Лист</i>	<i>№ докум.</i>	<i>Подпись</i>	<i>Дата</i>		74

3.7.5 Расчет суммарных потерь радиосистемы

Расчет потерь в радиосистеме можно произвести, используя следующую формулу:

$$W_{\Sigma} = W_{АФТпрд} + W_{АФТпрм} + W_0, \quad (3.8)$$

где $W_{АФТпрд}$ – потери сигнала в АФТ передатчика, дБ;

$W_{АФТпрм}$ – потери сигнала в АФТ приёмника, дБ;

W_0 – потери при распространении радиоволн, дБ.

$$W_0 (D=0,4) = 33 + 20(\lg 2400 + \lg 0,4) = 89 \text{ дБ.}$$

По формуле (3.8) суммарные потери радиосистемы составляют:

$$W_{\Sigma} = 2,26 + 2,26 + 89 = 93,52 \text{ дБ}$$

3.7.6 Расчет энергетического запаса радиоканала

Суммарное усиление радиоканала должно быть больше суммарных потерь:

$$G_{\Sigma} > W_{\Sigma}. \quad (3.9)$$

Разность величин G_{Σ} и W_{Σ} определяет энергетический запас радиоканала:

$$Z = G_{\Sigma} - W_{\Sigma}. \quad (3.10)$$

По формуле (3.10) энергетический запас радиоканала составляет:

$$Z = 115,5 - 93,52 = 21,98 \text{ дБ.}$$

По результатам расчетов можно сделать выводы: затухание в АТФ не столь велико, что позволяет получить хорошее суммарное усиление; дальность системы связи вполне удовлетворяет ТЗ, значение энергетического запаса радиоканала говорит о том, что выполняется условие (3.9).

					БР – 02069964 – 11.03.02 – 14 – 19	Лист
Изм.	Лист	№ докум.	Подпись	Дата		75

4 Технико-экономическое обоснование бакалаврской работы

В настоящее время любое проектное решение может рекомендоваться к строительству, если оно экономически целесообразно.

В данном разделе приводится расчет основных технико-экономических показателей.

Экономические расчеты производятся в следующем порядке:

1) расчет капитальных затрат;

4.1 Расчет капитальных затрат

Капитальные затраты состоят из следующих составляющих:

- стоимость оборудования;
- стоимость монтажных работ;
- прочие затраты (техническая документация, обучение специалистов, реклама) [10].

Стоимость оборудования необходимого для построения сети беспроводного доступа представлена в таблице 4.1.

Таблица 4.1 – Оборудование сети беспроводного доступа

Наименование работ и затрат	Един. изм.	Кол-во	Цена за ед., руб.	Общая стоимость, руб.
1 Внешняя беспроводная точка доступа/мост D-Link AirPremier DAP-3690	шт.	3	25600	76680
2 Антенна секторная ZyXEL ANT1314	шт.	3	14200	42600
3 Коммутатор D-Link DGS-1500-28P	шт.	1	24800	25000
4 Компьютер	шт.	1	45000	45000
5 ИБП Vanguard RM VRT-1500XL	шт.	1	20350	20350
6 Кабель ANT24-ODU3M	шт.	6	1260	7560

Окончание таблицы 4.1

Наименование работ и затрат	Един. изм.	Кол-во	Цена за ед., руб.	Общая стоимость, руб.
7 Кабель витая пара, FTP-4pair-Cat.5e (уличный)	м.	100	23,26	2325
8 Шкаф 19» настенный 9U 600x600x490мм (ШхГхВ) (SYSMATRIX WR 6609.710)	шт.	1	6300	6300
9 Разъем RG-45	шт.	10	10	100
10 ПО Easyhotspot	шт.	1	4000	4000
11 Мачта связи с системой крепежа на бетонную крышу 06114	шт	1	2600	2600
12 Провод ПВ 3-6.0	м	15	23	345
Итого	руб.	-	-	232860

Таким образом, затраты на оборудование составляют $K_{об} = 229716$ руб.

Затраты на строительные работы и монтаж оборудования составляют 10 % от общей стоимости оборудования, получаем:

$$K_{м.об.} = 0,1 \cdot 232860 = 23286 \text{ руб.}$$

Прочие затраты (техническая документация, обучение специалистов, реклама) берутся из расчета 15% от стоимости оборудования, таким образом получаем:

$$K_{пр} = 0,15 \cdot 232860 = 34929 \text{ руб.}$$

Затраты на транспортные расходы входят в стоимость оборудования.

Общие капитальные затраты проекта составляют:

$$K_{кап.з.} = K_{об} + K_{м.об} + K_{пр}. \quad (4.1)$$

По формуле (4.1) получаем:

$$K_{кап.з.} = 232860 + 23286 + 34929 = 291075 \text{ руб.}$$

ЗАКЛЮЧЕНИЕ

Развитие сетей Wi-Fi стремительно набирает темп. В нашей стране уже работают тысячи беспроводных сетей, а к нескольким десяткам действующих региональных операторов каждый месяц добавляются новые. С каждым днем этот процесс будет становиться все более интенсивным. В ближайшем будущем беспроводные сети потеснят «проводные» благодаря своей «гибкости», удобности, простоте подключения новых рабочих станций, но не смогут полностью «заменить» – они лишь займут свое место наравне с ними и будут использоваться для решения определенного круга задач.

В рамках бакалаврской работы были изучены состав и принцип функционирования сети беспроводного доступа, а также решена задача подключения абонентов к международной информационной сети Internet на примере Пролетарского района г. Саранска с использованием данной сети.

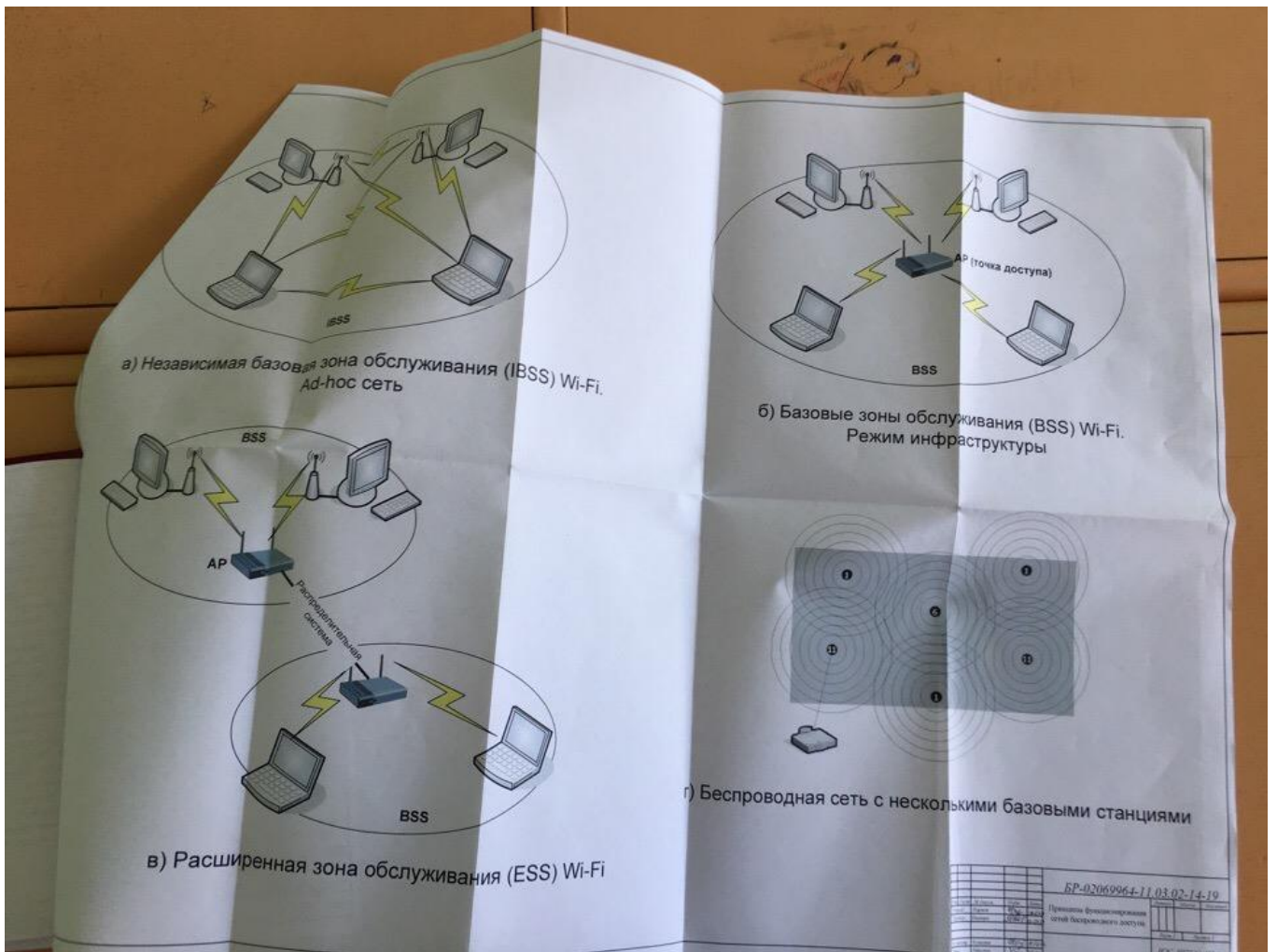
В проектной части бакалаврской работы разработана структурная схема сети, а также произведены расчеты затухания антенно-фидерного тракта, эффективной изотропно-излучаемой мощности, энергетического запаса радиоканала, дальности работы беспроводного канала связи, суммарных потерь радиосистемы для сети беспроводного доступа г. Саранска.

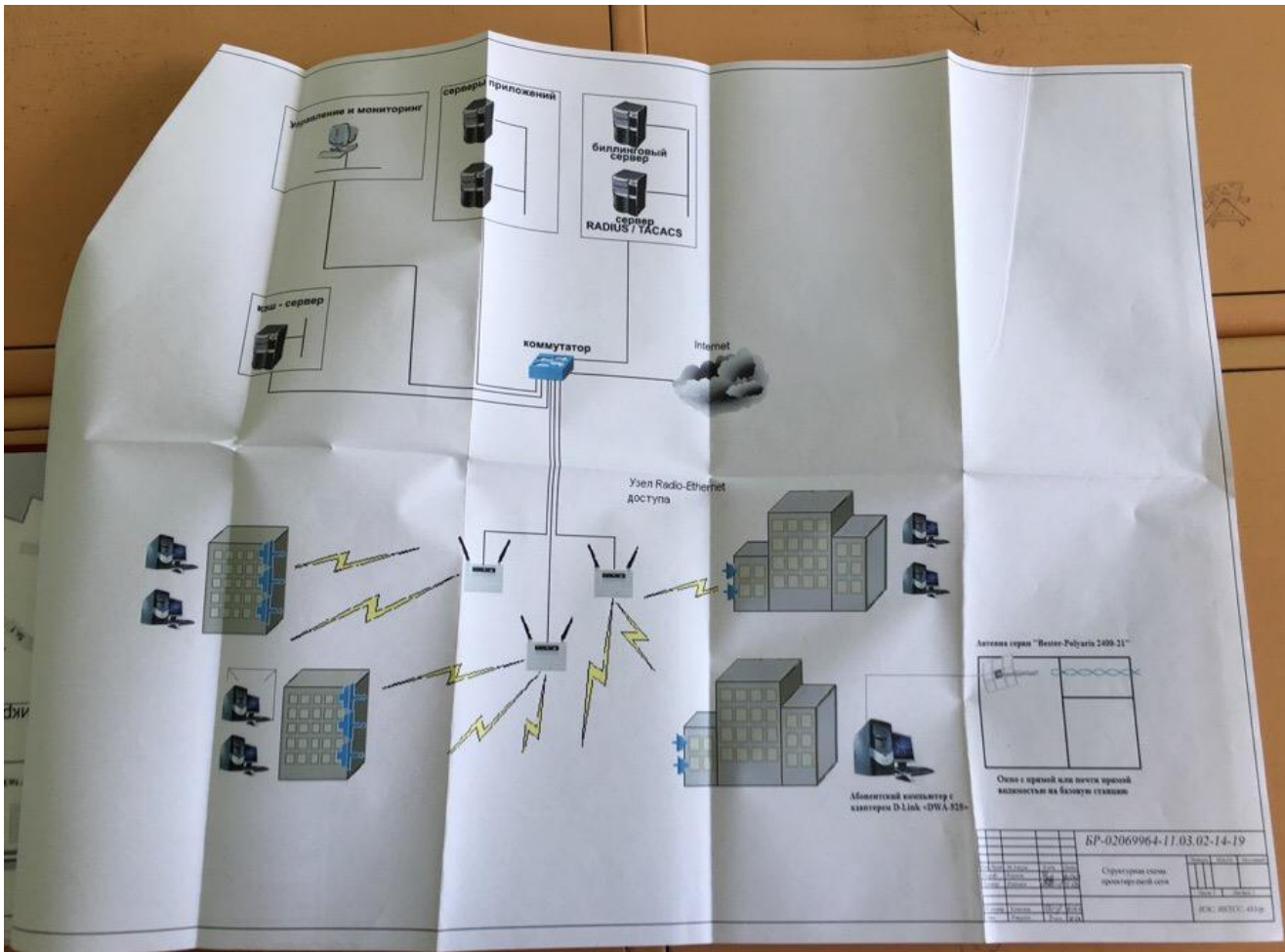
					БР – 02069964 – 11.03.02 – 14 – 19	Лист
						78
Изм.	Лист	№ докум.	Подпись	Дата		

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

- 1 Вишнеvский В. М. Широкополосные сети передачи информации / В. М. Вишнеvский. – М. : Техносфера, 2005. – 592 с.
- 2 Гейер Дж. Беспроводные сети. Первый шаг / Дж. Гейер. – М. : Вильямс, 2005. – 192 с.
- 3 Григорьев В. А. Сети и системы беспроводного доступа / В. А. Григорьев, О. И. Лагутенко, Ю. А. Распопов. – М. : Экотрендз, 2005. – 381с.
- 4 Компьютерные сети. Принципы, технологии, протоколы : учебник / В. Г. Олифер, Н. А. Олифер. – 4-е изд. – СПб. : Питер, 2010. – 944 с.
- 5 Педжман Р. Основы построения беспроводных локальных сетей стандарта 802.11. / Р. Педжман, Л. Джонатан. – М. : Вильямс, 2004. – 304 с.
- 6 Столлингс В. Беспроводные линии связи и сети / В. Столлингс. – М. : Вильямс, 2003. – 640 с.
- 7 Чепульский Ю. П. Аттестация рабочих мест / Ю. П. Чепульский, В. И. Бекасов. – М. : Альфа-Композит, 1998. – 304 с.
- 8 Широкополосные беспроводные сети передачи информации / В. Вишнеvский [и др.]. – М. : Экотрендз, 2005. – 592 с.
- 9 Пролетарский А. В. Беспроводные сети Wi-Fi / А. В. Пролетарский, И. В. Баскаков. – М: БИНОМ, 2007. – 216 с.
- 10 Березина А. В. Методические указания к выполнению экономического раздела / Сост. А. В. Березина. – Тольятти: Волжский университет им В. Н. Татищева, 2004. – 21 с.
- 11 Никулин В. В. Методические указания по подготовке выпускной квалификационной работы по направлению подготовки 11.03.02 «Инфокоммуникационные технологии и системы связи» / В. В. Никулин, С. В. Осипов. – Саранск : Изд-во Мордов. ун-та, 2016. – 28 с.

					БР – 02069964 – 11.03.02 – 14 – 19	Лист
Изм.	Лист	№ докум.	Подпись	Дата		79





Оборудование для построения сети беспроводного доступа




Рисунок 1 – Внешняя беспроводная точка доступа D-Link AirPremier DWL-2700AP

Основные характеристики		
Интерфейсы	Порт 10/100/1000 BASE-TX	
Сетевое управление	- HTTP	
	- SNMP 3.0	
	- Telnet	
	- Secure (SSH)	
Чувствительность приемника	IEEE 802.11n: 2.4ГГц/HT-20 16dBm при MCS0/8, MCS1/9, MCS2/10, MCS3/11, MCS4/12 14dBm при MCS 5/13 13dBm при MCS 6/14 12dBm при MCS 7/15	
	Мощность передатчика	20 dBm (100 мВт)
	Дополнительные характеристики	
	<ul style="list-style-type: none"> - Шифрование 64/128-бит WEP - Аутентификация 802.1x - Управление доступом на основе MAC-адресов - WPA, WPA2 - Обнаружение незарегистрированных точек доступа - Разделение WLAN 	




Рисунок 2 – Внешний вид секторной антенны ANT1314

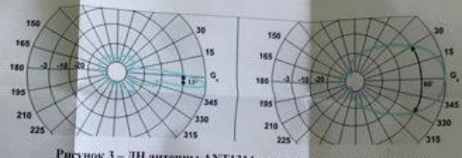


Рисунок 3 – ДН антенны ANT1314 в вертикальной (Е-плоскость) и горизонтальной (H-плоскость) плоскостях




Рисунок 4 – Коаксиальный кабель D-Link ANT24-ODU3M

Основные характеристики	
Волновое сопротивление	50 Ом
Вносимое затухание на частотах от 2.4 до 2.5 ГГц	От 0.85 до 1 дБ
Рабочая среда	На улице и в помещении
Устойчивость к атмосферным воздействиям	Да
Оболочка кабеля	Черный полиэтилен
Рабочий диапазон температур	От -40 до +85 °С
Разъемы	RP-N и N - тип


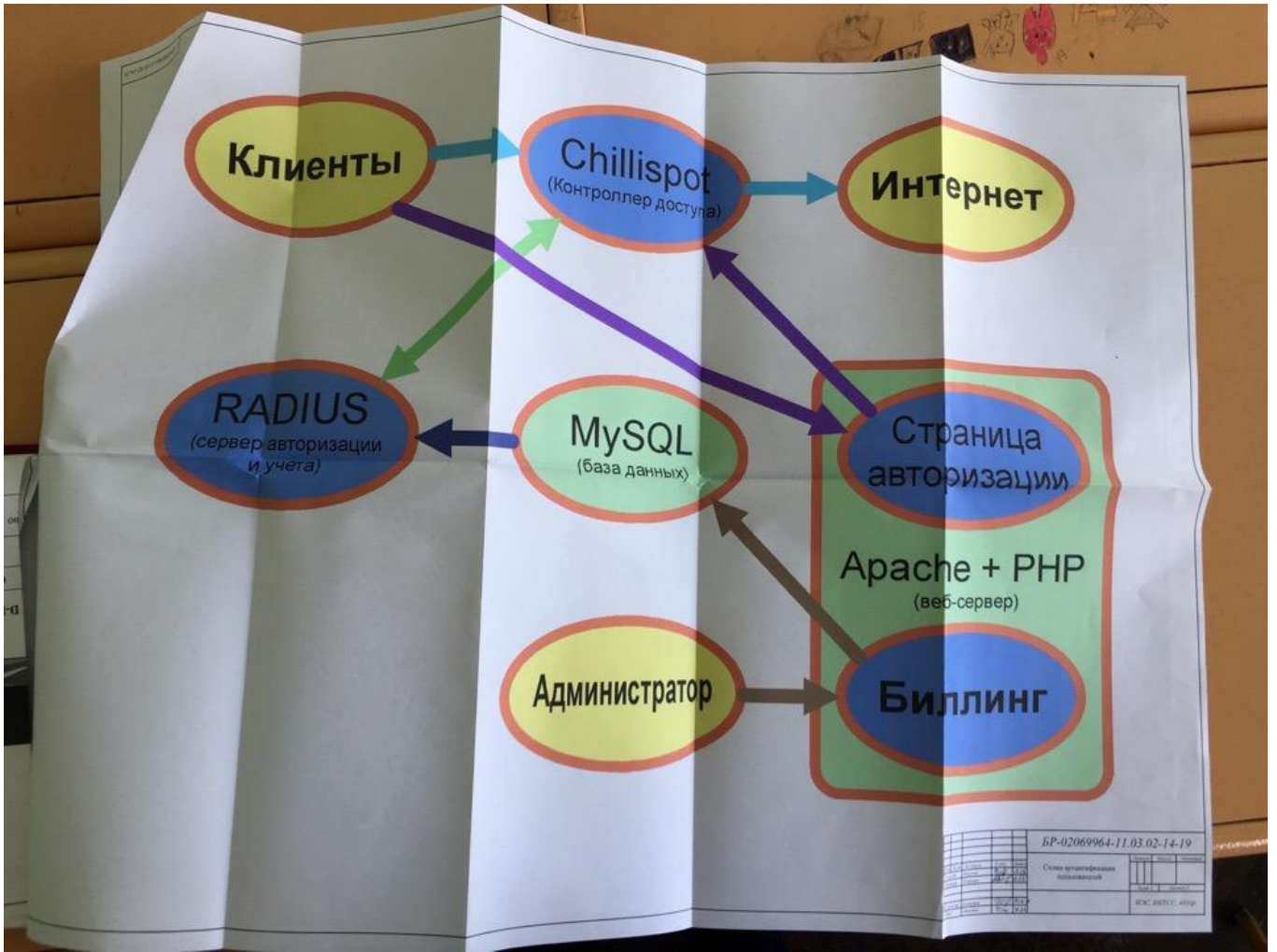


Рисунок 5 – Коммутатор D-Link DGS-1500-28P SmartPro

Основные характеристики	
Модель	D-Link DGS-1500-28P SmartPro
Количество	24 порта 10/100/1000 Mbit/s с функцией PoE, 4 порта SFP
PoE	- Стандарт PoE: 802.3af & 802.3at - Функция хранения PoE: 15.4 Вт/порт/30 Вт на порт/от 1 до 24
VLAN	- 802.1Q
	- Группы VLAN <ul style="list-style-type: none"> • Макс. 4K статических групп VLAN • Макс. 4094 VID
	- GVRP VLAN до 256 динамических VLAN
	- Asymmetric VLAN
Управление	- Web-интерфейс GUI
	- Single IP Management
	- Compact CLI через Telnet
	- SNMP

BP-02069964-11.03.02-14-19

ИСК. ИТЕСС. 419-р



ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
МОРДОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. Н.П. ОГАРЁВА»
(ФГБОУ ВО «МГУ им. Н.П. Огарёва»)

ОТЧЕТ

*о результатах проверки бакалаврской работы обучающегося
на наличие заимствований*

Автор работы: Наумов Андрей Игоревич

Тема работы: «Проектирование беспроводной сети широкополосного
доступа в Пролетарском районе г.Саранска на основе технологии Wi-Fi»

Руководитель: Иванцев Анатолий Степанович

Представленная работа прошла проверку на наличие заимствований в
системе «Антиплагиат. ВУЗ»

Результаты автоматической проверки:	оригинальность	68,78%
	цитирования	1,65%
	заимствования	29,57%

Результаты анализа полного отчета на наличие заимствований:

правомерные заимствование: 29,57%

корректные цитирования: 1,65%

неправомерные заимствования: нет

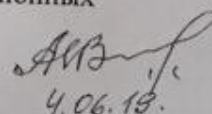
признаки обхода системы: нет

Общее заключение об итоговой оригинальности работы и возможности
ее допуска к защите:

итоговая оригинальность работы составляет 68,78% что согласно
Положению о проверке работ обучающихся ФГБОУ ВО «МГУ им. Н.П.
Огарёва» на наличие заимствований, позволяет допустить студента Наумова
А.И. к предварительной защите и защите ВКР в ГЭК.

Руководитель

к. ф.-м. н., доцент кафедры инфокоммуникационных
технологий и систем связи



А.С. Иванцев

4.06.19.

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
МОРДОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. Н.П. ОГАРЁВА»

ОТЗЫВ НАУЧНОГО РУКОВОДИТЕЛЯ
о выпускной квалификационной работе
выпускника института электроники и светотехники
Наумова Андрея Игоревича

Тема выпускной квалификационной работы «Проектирование беспроводной сети широкополосного доступа в Пролетарском районе г. Саранска на основе технологии Wi-Fi».

Бакалаврская работа Наумова А.И. посвящена проектированию сети беспроводного доступа на основе оборудования стандарта IEEE 802.11 (Wi-Fi).

Актуальность темы бакалаврской работы обусловлена постоянным повышением спроса на услуги Интернет-доступа.

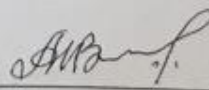
В результате проделанной работы был произведен анализ и выбор оборудования, разработана функционально-структурная схема сети, описан процесс проектирования сети беспроводного доступа на основе оборудования стандарта IEEE 802.11n.

К недостаткам работы относятся малая мощность превышения источника бесперебойного питания.

Студент Наумов А.И. в процессе работы показал достаточный уровень подготовки при решении поставленной задачи. При выполнении расчетов проявил умение пользоваться технической и справочной литературой.

Бакалаврская работа заслуживает высокой оценки, результаты работы заслуживают практического внедрения, а Наумов А.И. заслуживает присвоения квалификации бакалавра по направлению подготовки 11.03.02 «Инфокоммуникационные технологии и системы связи».

Руководитель бакалаврской работы,
доцент, канд. физ.-мат. наук


А. С. Иванцев