МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество
АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ

кафедра_____

«Допущен к защите»
Заведующий кафедрой _____
_____
(Ф.И.О., ученая степень, звание)
_____ «_____»_____20__ г.
(подпись)

ДИПЛОМНЫЙ ПРОЕКТ

На тему: Анализ информационной безопасности стандарта в сетях широкополосной связи стандарта 802.11

Специальность 5В071900

Выполнил (а) Елеубеков Д.М. РЭУ-12-1
(Фамилия и инициалы) группа

Научный руководитель к.т.н проф Байкенов А.С.
(Фамилия и инициалы, ученая степень, звание)

Консультанты:

по экономической части:
Бекмуева А.Ч, к.э.н., доцент
(Фамилия и инициалы, ученая степень, звание)
_____ «07» 06 2016 г.
(подпись)

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

по применению вычислительной техники:
к.т.н, ст.преп. Бородинова Ю.А.
(Фамилия и инициалы, ученая степень, звание)
_____ «07» 06 2016 г.
(подпись)

_____
(Фамилия и инициалы, ученая степень, звание)
_____ «_____»_____20__ г.
(подпись)

Нормоконтролер: Дельмудова Г.Д, ст. пр-ль
(Фамилия и инициалы, ученая степень, звание)
_____ «8» июня 2016 г.
(подпись)

Рецензент: Касимов А.О, к.т.н, доцент КазНИТУ
(Фамилия и инициалы, ученая степень, звание)
_____ «8» 06 20__ г.
(подпись)

Алматы 2016 г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество

АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ

Факультет Радиотехники и связи
Специальность 5В071900-Радиотехника, электроника и телекоммуникации.
Кафедра Телекоммуникационных систем

ЗАДАНИЕ

на выполнение дипломного проекта

Студент Елубеков Дастан Нуматазаулы
(фамилия, имя, отчество)

Тема проекта Анализ информационной безопасности стандарта в сетях широкополосной связи стандарта 802.11

утверждена приказом ректора № 149 от « 19 » 10 2015 г.

Срок сдачи законченной работы « 25 » 05 2016 г.

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

1 Стандарт беспроводной связи IEEE 802.11
2 Стандарты безопасности WEP WPA WPA2
3. Технологию VPN
4. Стандартный протокол IPSec
5. Оборудование Wi-Fi.

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

1. Механизмы аутентификации и безопасности протокола 802.11
2. Архитектура системы при использовании отдельного сервера аутентификации, авторизации и учета.
3. Варианты обеспечения безопасности беспроводных сетей стандарта 802.11
4. Расчет зоны Френеля.
5 Расчет зоны действия сигнала
6 Анализ потерь сигнала в свободном пространстве

Перечень графического материала (с точным указанием обязательных чертежей)

1. Проблемы безопасности Wi-Fi сетей
2. Расчет зоны Френеля
3. Расчет зоны действия сигнала
4. Расчет дальности работы беспроводного канала связи
5. Расчет по графику
6. Доступность канала
7. Расчеты по безопасности жизнедеятельности
8. Расчет экономической эффективности

Рекомендуемая основная литература

1. Шахнович И. Современные технологии беспроводной связи. г. Москва. Техносфера 2006 г. - 245 с.
2. Роман П., Мизри Дж. Основы построения беспроводных локальных сетей стандарта 802.11. - Москва, Санкт-Петербург" Киев, 2004 - 190 с.
3. Безопасность жизнедеятельности: Учебник / Под ред. С.В. Белов - М.: Высшая школа, 1999
4. Голубицкая В.А. Жигульская Л.М. - Экономика связи: Учебник для вузов. - М: Радио и связь, 2000. - 392 с.

Консультанты по проекту с указанием относящихся к ним разделов

Раздел	Консультант	Сроки	Подпись
БЖД	Дикенов К.А.	28.04.16-02.06.16	
Эконом. часть	Бекмаева А.Ч.	03.04.16-07.06.16	
Воп 2. Техника	Борисова Ю.С.	03.04.16-08.06.16	

Г Р А Ф И К
подготовки дипломного проекта

№ п/п	Наименование разделов, перечень разрабатываемых вопросов	Сроки представления руководителю	Примечание
1	Введение	19.10.2015	
2.	Беспроводные сети	22.10.2015	
3	Недостатки беспроводных сетей	29.10.2015	
4	Преимущества беспроводных сетей	10.11.2015	
5	Стандарты и сравнения беспроводных сетей.	17.11.2015	
6.	Организация сетей	25.11.2015	
7.	Канальный уровень	15.12.2015	
8.	Физический уровень	15.12.2015	
9.	Оборудование для Wi-Fi	20.01.2016	
10	Режим работа сети Wi-Fi	12.02.2016	
11	Технология WDS	20.03.2016	
12	Развертывание распределенных беспроводных сетей WDS	25.03.2016	
13	Проблемы безопасности Wi-Fi	13.04.2016	
14	Исследование информационной безопасности в сетях Wi-Fi	16.04.2016	
15.	Аутентификация	25.04.2016	
16	Архитектура систем при использовании отдельного сервера аутентификации и учета	27.04.2016	
17	Варианты обеспечения безопасности стандарта 802.11.	2.05.2016	
18.	Расчет зоны Френеля.	7.05.2016	
19.	Расчет зоны действия сигнала.	15.05.2016	
20	Безопасность жизнедеятельности	23.05.2016	
21	Экономическая эффективность	23.05.2016	

Дата выдачи задания «19» 10 2015 г.

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

Руководитель _____ Байжуманов Т.О.
(подпись) (Фамилия и инициалы)

Задание принял к исполнению
студент _____ Елеубеков Д.Ж.
(подпись) (Фамилия и инициалы)

Аңдатпа

Бұл бітіру жұмысында кеңжолақты байланыс WI-FI желілерінде ақпараттық қауіпсіздікке зерттеу өткізілген. Өткізгішсіз желілердың ақпараттық қорғанышымен үйлесімді шешім табылған, жабдықты таңдау жүзеге асырылған және келесі есептеулер орындалған: сигналдың таралу аймағы, Френель зонасы есептелген.

Сонымен қатар соңғы екі бөлімде өміртіршілік қауіпсіздігі мәселелері мен WI-FI желісінің экономикалық тиімділігі есептелген.

Аннотация

В данной выпускной работе проведено исследование информационной безопасности в сетях широкополосной связи WI-FI. Было найдено оптимальное решение по информационной защите беспроводных сетей, осуществлен выбор оборудования и выполнены следующие расчеты: расчёт зоны покрытия сигнала, расчёт зоны Френеля.

Кроме этого в двух последних главах рассмотрены вопросы безопасности жизнедеятельности и рассчитана экономическая целесообразность сети WI-FI.

Annotation

In this final work conducted research in information security WI-FI broadband networks. the optimal solution for information security of wireless networks found, carried equipment selection and the following calculations: calculation of signal coverage, the calculation of the Fresnel zone.

In addition, in the last two chapters consider health and safety issues and economic feasibility is designed WI-FI network.

Содержание

Введение

Главной целью данного исследования является изучение информационной безопасности в сетях широкополосной связи Wi-Fi, с целью определения оптимальных методов информационной защиты.

Данное исследование вписывается в общемировую тенденцию — за последние пару лет Wi-Fi превратился в одну из самых перспективных технологий на рынке беспроводной связи.

Беспроводная передача данных — это технология, позволяющая создавать сети, полностью соответствующие стандартам для обычных сетей (например Ethernet или Token Ring) без использования кабельной проводки. В качестве среды передачи информации в таких сетях выступают радиоволны СВЧ - диапазона.

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

- Простота развёртывания;
- Гибкость архитектуры сети;
- Быстрота проектирования и реализации;
- Так же, беспроводная сеть не нуждается в прокладке кабелей.

Во всем мире стремительно растет потребность в беспроводных соединениях, особенно в сфере бизнеса. Пользователи с беспроводным доступом к информации — всегда и везде могут работать более производительно и эффективно, чем их коллеги, привязанные к проводным телефонным и компьютерным сетям. Однако, беспроводные сети – являются источником повышенного риска несанкционированного доступа, так как проникнуть в беспроводную сеть значительно проще, чем в проводную — не нужно подключаться к проводам, достаточно оказаться в зоне приема сигнала.

Актуальность этой проблемы определяется в первую очередь бурным развитием сети Интернет, доступ к которой требует не только увеличения пропускной способности, но и мобильности подключения данной услуги.

1 Беспроводные сети

1.1 Недостатки беспроводных сетей

Довольно высокое по сравнению с другими стандартами потребление энергии, что уменьшает время жизни батарей и повышает температуру устройства.

Wi-Fi имеют ограниченный радиус действия. Типичный домашний Wi-Fi маршрутизатор стандарта 802.11b или 802.11g имеет радиус действия 50 м в помещении и 100 м снаружи. Расстояние зависит также от частоты. Wi-Fi в диапазоне 2.4 ГГц работает дальше, чем Wi-Fi в диапазоне 5 ГГц, и имеет радиус меньше, чем Wi-Fi (и пре-Wi-Fi) на частоте 900 МГц. На самом деле, с позиции безопасности, небольшой радиус действия является преимуществом!!! Т.е. с учетом того, что большинство точек доступа либо не имеют защиты, либо используют шифрование WEP с известными уязвимостями (~ 80-90%), для того, чтобы найти сеть, нужно оказаться в зоне ее действия, а чем меньше зона действия - тем сложнее это сделать!

Наложение сигналов закрытой или использующей шифрование точки доступа и открытой точки доступа, работающих на одном или соседних каналах может помешать доступу к открытой точке доступа. Эта проблема может возникнуть при большой плотности точек доступа, например, в больших многоквартирных домах, где многие жильцы ставят свои точки доступа Wi-Fi.

Неполная совместимость между устройствами разных производителей или неполное соответствие стандарту может привести к ограничению возможностей соединения или уменьшению скорости.

1.2 Преимущества беспроводных сетей

Малое время развертывания. Исключаются работы по проектированию и прокладке проводов, поэтому сроки развертывания сети минимальны. Это особенно актуально для малых офисов, для временных сетей в выставочных центрах и т.д.

Минимум нарушений отделки помещений. Практически исключены строительно-монтажные работы, поэтому в интерьер Ваших помещений не будет внесено изменений.

Гибкая конфигурация сети. Вы можете перемещать рабочие места сотрудников, Вы не привязаны к информационной розетке на рабочем столе– нравится работать с ноутбуком на диване – работайте!

Имидж. Беспроводная связь подчеркивает активную позицию бизнеса в информационных технологиях, особенно при проведении переговоров и презентаций.

Скорость. Современная беспроводная связь может работать на скоростях до 108 Мбит/с. Это скорость обычной проводной локальной сети. Для большинства офисных приложений скорости беспроводной сети более чем достаточно, [1].

1.3 Стандарты и компоненты сети

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

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

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

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

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

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

В настоящее время существует множество стандартов семейства IEEE 802.11:

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

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

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

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

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

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

– 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;

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

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

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

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

– 802.11n - Перспективный стандарт, находящийся на сегодняшний день в разработке, который позволит поднять пропускную способность сетей до 100 Мбит/сек;

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

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

1.4 Сравнение стандартов беспроводной сети

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

К началу 2004 года в эксплуатации находилось около 15 млн. радиоустройств 802.11b.

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

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

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

преимуществ 802.11g надо отметить низкую потребляемую мощность, большую дальность действия и высокую проникающую способность сигнала. Можно надеяться и на разумную стоимость оборудования, поскольку низкочастотные устройства проще в изготовлении [2].

1.5 Организация сети

Стандарт IEEE 802.11 работает на двух нижних уровнях модели ISO/OSI: физическом и канальном. Другими словами, использовать оборудование Wi-Fi так же просто, как и Ethernet: протокол TCP/IP накладывается поверх протокола, описывающего передачу информации по каналу связи. Расширение IEEE 802.11b не затрагивает канальный уровень и вносит изменения в IEEE 802.11 только на физическом уровне.

В беспроводной локальной сети есть два типа оборудования: клиент (обычно это компьютер, укомплектованный беспроводной сетевой картой, но может быть и иное устройство) и точка доступа, которая выполняет роль моста между беспроводной и проводной сетями. Точка доступа содержит приемопередатчик, интерфейс проводной сети, а также встроенный микрокомпьютер и программное обеспечение для обработки данных.

1.6 Канальный уровень IEEE 802.11

Подобно проводной сети Ethernet, в беспроводных компьютерных сетях Wi-Fi канальный уровень включает в себя подуровни управления логическим соединением (Logical Link Control, LLC) и управления доступом к среде передачи (Media Access Control, MAC). У Ethernet и IEEE 802.11 один и тот же LLC, что значительно упрощает объединение проводных и беспроводных сетей. MAC у обоих стандартов имеет много общего, однако есть некоторые тонкие различия, принципиальные для сравнения проводных и беспроводных сетей.

В Ethernet для обеспечения возможности множественного доступа к общей среде передачи (в данном случае кабелю) используется протокол CSMA/CD, обеспечивающий выявление и обработку коллизий (в терминологии компьютерных сетей так называются ситуации, когда несколько устройств пытаются начать передачу одновременно).

В сетях IEEE 802.11 используется полудуплексный режим передачи, т.е. в каждый момент времени станция может либо принимать, либо передавать информацию, поэтому обнаружить коллизию в процессе передачи невозможно. Для IEEE 802.11 был разработан модифицированный вариант протокола CSMA/CD, получивший название CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). Работает он следующим образом. Станция, которая собирается передавать информацию, сначала "слушает эфир". Если не обнаружено активности на рабочей частоте, станция сначала ожидает в течение некоторого случайного промежутка времени, потом снова "слушает эфир" и, если среда передачи данных все еще свободна, осуществляет передачу. Наличие случайной задержки необходимо для того, чтобы сеть не зависла, если несколько станций одновременно захотят

получить доступ к частоте. Если информационный пакет приходит без искажений, принимающая станция посылает обратно подтверждение. Целостность пакета проверяется методом контрольной суммы. Получив подтверждение, передающая станция считает процесс передачи данного информационного пакета завершенным. Если подтверждение не получено, станция считает, что произошла коллизия, и пакет передается снова через случайный промежуток времени.

Еще одна специфичная для беспроводных сетей проблема - две клиентские станции имеют плохую связь друг с другом, но при этом качество связи каждой из них с точкой доступа хорошее. В таком случае передающая клиентская станция может послать на точку доступа запрос на очистку эфира. Тогда по команде с точки доступа другие клиентские станции прекращают передачу на время "общения" двух точек с плохой связью. Режим принудительной очистки эфира (протокол Request to Send/Clear to Send - RTS/CTS) реализован далеко не во всех моделях оборудования IEEE 802.11 и, если он есть, то включается лишь в крайних случаях. В Ethernet при передаче потоковых данных используется управление доступом к каналу связи, распределенное между всеми станциями. Напротив, в IEEE 802.11 в таких случаях применяется централизованное управление с точки доступа. Клиентские станции последовательно опрашиваются на предмет передачи потоковых данных. Если какая-нибудь из станций сообщает, что она будет передавать потоковые данные, точка доступа выделяет ей промежуток времени, в который из всех станций сети будет передавать только она.

Следует отметить, что принудительная очистка эфира снижает эффективность работы беспроводной сети, поскольку связана с передачей дополнительной служебной информации и кратковременными перерывами связи. Кроме этого, в проводных сетях Ethernet при необходимости можно реализовать не только полудуплексный, но и дуплексный вариант передачи, когда коллизия обнаруживается в процессе передачи (это повышает реальную пропускную способность сети). Поэтому, увы, при прочих равных условиях реальная пропускная способность беспроводной сети IEEE 802.11b будет ниже, чем у проводного Ethernet. Таким образом, если сетям Ethernet 10 Мбит/с и IEEE 802.11b (максимальная скорость передачи информации 11 Мбит/с) с одинаковым числом пользователей давать одинаковую нагрузку, постепенно увеличивая ее, то, начиная с некоторого порога, сеть IEEE 802.11b начнет "тормозить", а Ethernet все еще будет функционировать нормально.

Поскольку клиентские станции могут быть мобильными устройствами с автономным питанием, в стандарте IEEE 802.11 большое внимание уделено вопросам управления питанием. В частности, предусмотрен режим, когда клиентская станция через определенные промежутки времени "просыпается", чтобы принять сигнал включения, который, возможно, передает точка доступа. Если этот сигнал принят, клиентское устройство включается, в

противном случае оно снова "засыпает" до следующего цикла приема информации.

1.7 Физический уровень IEEE 802.11

Стандарт IEEE 802.11 предусматривает передачу сигнала одним из двух методов - прямой последовательности (Direct Sequence Spread Spectrum, DSSS) и частотных скачков (Frequency Hopping Spread Spectrum, FHSS) различающиеся способом модуляции, но использующие одну и ту же технологию расширения спектра. 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.

Метод FHSS предусматривает изменение несущей частоты сигнала при передаче информации. Для повышения помехоустойчивости нужно увеличить спектр передаваемого сигнала, для чего несущая частота меняется по псевдослучайному закону, и каждый пакет данных передается на своей несущей частоте. При использовании FHSS конструкция приемопередатчика получается очень простой, но этот метод применим, только если пропускная способность не превышает 2 Мбит/с, так что в дополнении IEEE 802.11b остался один DSSS. Из этого следует, что совместно с устройствами IEEE 802.11b может применяться только то оборудование стандарта IEEE 802.11, которое поддерживает DSSS, при этом скорость передачи не превысит максимальной скорости в "узком месте" (2 Мбит/с), коим является оборудование, использующее старый стандарт без расширения. В основе метода DSSS лежит принцип фазовой манипуляции (т.е. передачи информации скачкообразным изменением начальной фазы сигнала). Для расширения спектра передаваемого сигнала применяется преобразование передаваемой информации в так называемый код Баркера, являющийся псевдослучайной последовательностью. На каждый передаваемый бит приходится 11 бит в последовательности Баркера. Различают прямую и инверсную последовательности Баркера. Из-за большой избыточности при кодировании вероятность того, что действие помехи превратит прямую последовательность Баркера в инверсную, близка к нулю. Единичные биты передаются прямым кодом Баркера, а нулевые - инверсным.

Под беспроводные компьютерные сети в диапазоне 2,4 ГГц отведен довольно узкий "коридор" шириной 83 МГц, разделенный на 14 каналов. Для исключения взаимных помех между каналами необходимо, чтобы их полосы отстояли друг от друга на 25 МГц. Несложный подсчет показывает, что в одной зоне одновременно могут использоваться только три канала. В таких условиях невозможно решить проблему отстройки от помех автоматическим изменением частоты, вот почему в беспроводных локальных сетях используется кодирование с высокой избыточностью. В ситуации, когда и эта мера не позволяет обеспечить заданную достоверность передачи, скорость с максимального значения 11 Мбит/с последовательно снижается до одного из

следующих фиксированных значений: 5,5; 2; 1 Мбит/с. Снижение скорости происходит не только при высоком уровне помех, но и если расстояние между элементами беспроводной сети достаточно велико [3].

1.8 Оборудование для Wi-Fi

1.8.1 Точки доступа

Точка доступа рисунок 1.1 соединяет кабельную и беспроводную сеть и позволяет клиентам последней получить доступ к ресурсам кабельной сети. Каждая точка доступа расширяет общую вычислительную мощность системы. Пользователи могут перемещаться между точками доступа, не теряя соединения с сетью, как и при подключении к сети с помощью сотового телефона. Другими словами, точка доступа – это программно-аппаратное устройство, которое выполняет роль концентратора для клиента беспроводной сети и обеспечивает подключение к кабельной сети. Радиус действия в помещении около 50 м, при прямой видимости около 500 м.

Рисунок 1.1 – Точка доступа DWL-8500AP

1.8.2 Сетевые адаптеры

Беспроводной сетевой адаптер рисунок 1.2 для обычного ПК. Радиус действия в помещении около 50 м., при прямой видимости около 300 м.

Рисунок 1.2 – Адаптер DWL-G550

Беспроводной сетевой адаптер для ноутбука рисунок 1.3.

Рисунок 1.3 – Адаптер для ноутбука

В самом простом случае беспроводная сеть может состоять из нескольких ПК, снабженных беспроводными сетевыми картами и совместно использующих принтер, модем или файлы. Такая конфигурация называется одноранговой сетью.

Пример беспроводной сети с использованием точки доступа и сетевых адаптеров, рисунок 1.4.

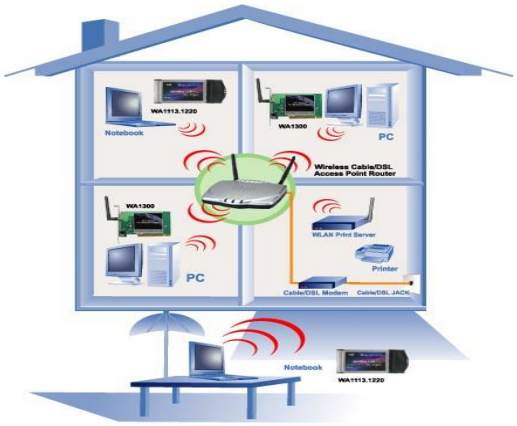


Рисунок 1.4 – Сеть WLAN

1.8.3 Маршрутизаторы

Давно прошли уже те времена, когда персональный компьютер был роскошью, недоступной для большинства людей. Во многих семьях сейчас свой компьютер есть у каждого члена семьи, а у многих еще и ноутбуки вдобавок. В такой ситуации вопрос организации собственной сети выходит на первый план, а от грамотного подбора оборудования и программного обеспечения зависит функциональность и бесперебойная ее работа. Без сети никак не обойтись – ведь интернет-канал практически всегда один (это выгоднее и удобнее), да и покупать отдельно принтер к каждому компьютеру и дублировать объемную информацию тоже нецелесообразно – проще настроить принт- и файл-сервер. Вот тут и приход к нам на помощь маршрутизатор рисунок 1.5.

Рисунок 1.5 – D-Link DSL-G804V

Маршрутизатор нужен для объединения двух или более локальных сетей. Маршрутизатор подключается в сеть по средствам LAN в месте с точкой доступа. Радиус действия в помещении около 50 м., при прямой видимости около 500 м.

1.9 Режимы

1.9.1 Режим AD HOC

В режиме Ad Hoc рисунок 1.6 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.

Однако необходимо иметь в виду, что режим Ad Hoc позволяет устанавливать соединение на скорости не более 11 Мбит/с, независимо от используемого оборудования. Реальная скорость обмена данных будет ниже, и составит не более 11/N Мбит/с, где N -число устройств в сети. Дальность связи составляет не более ста метров, а скорость передачи данных быстро падает с увеличением расстояния.

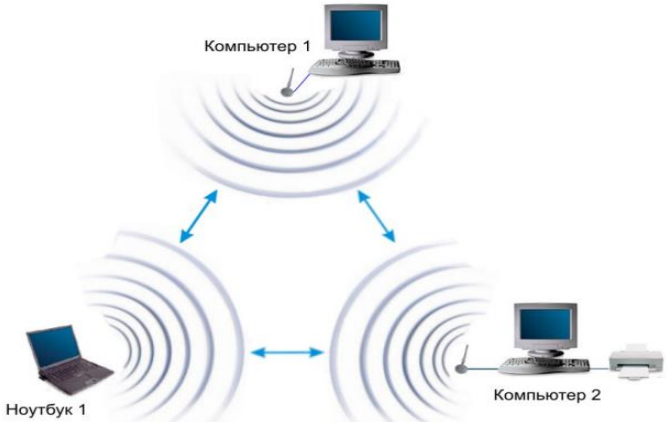


Рисунок 1.6 – Режим Ad Hoc

Для организации долговременных беспроводных сетей следует использовать инфраструктурный режим.

1.9.2 Инфраструктурный режим

В этом режиме точки доступа обеспечивают связь клиентских компьютеров рисунок 1.7. Точку доступа можно рассматривать как беспроводный коммутатор. Клиентские станции не связываются непосредственно одна с другой, а связываются с точкой доступа, и она уже направляет пакеты адресатам.

Рисунок 1.7 – Инфраструктурный режим

Точка доступа имеет порт Ethernet, через который базовая зона обслуживания подключается к проводной или смешанной сети - к сетевой инфраструктуре.

1.9.3 Режимы WDS и WDS WITH AP

Термин WDS (Wireless Distribution System) расшифровывается как «распределённая беспроводная система». В этом режиме 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 одинаковый 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 1.8.

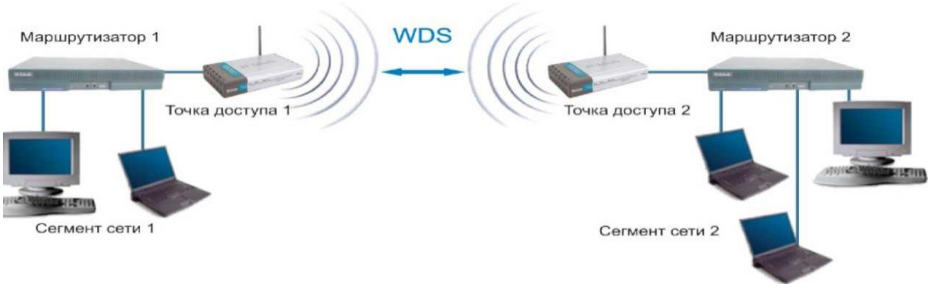


Рисунок 1.8 – Мостовой режим

Режим беспроводного моста, аналогично проводным мостам, служит для объединения подсетей в общую сеть. С помощью беспроводных мостов

можно объединять проводные LAN, находящиеся как на небольшом расстоянии в соседних зданиях, так и на расстояниях до нескольких километров. Это позволяет объединить в сеть филиалы и центральный офис, а также подключать клиентов к сети провайдера Интернет.

Беспроводный 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.

К точке доступа, работающей в режиме моста, подключение беспроводных клиентов невозможно. Беспроводная связь осуществляется только между парой точек, реализующих мост.

Термин WDS with AP (WDS with Access Point) обозначает «распределённая беспроводная система, включая точку доступа», т. е. с помощью этого режима можно организовать не только мостовую связь между точками доступа, но и одновременно подключить клиентские компьютеры рисунок 1.9. Это позволяет достичь существенной экономии оборудования и упростить топологию сети. Данная технология поддерживается большинством современных точек доступа.

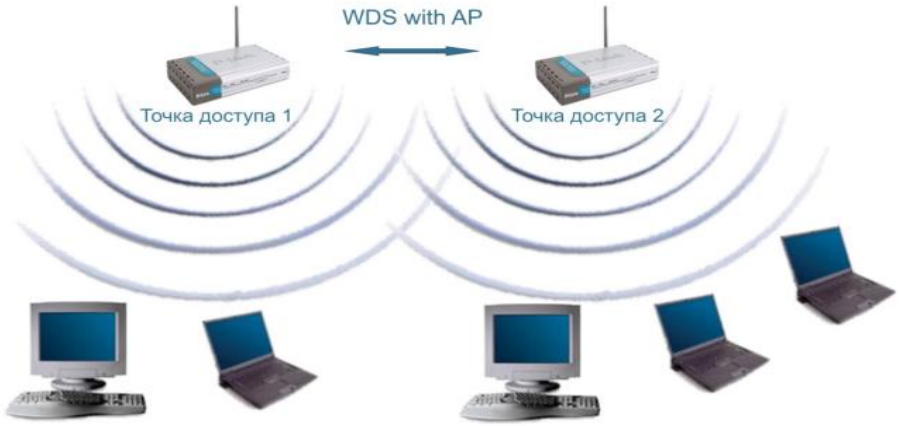


Рисунок 1.9 – Режим WDS with AP

Тем не менее, необходимо помнить, что все устройства в составе одной WDS with AP работают на одной частоте и создают взаимные помехи, что ограничивает количество клиентов до 15-20 узлов. Для увеличения количества подключаемых клиентов можно использовать несколько WDS-сетей, настроенных на разные неперекрывающиеся каналы и соединенные проводами через uplink-порты.

Топология организации беспроводных сетей в режиме WDS аналогична обычным проводным топологиям.

1.9.4 Режим повторителя

Может возникнуть ситуация, когда оказывается невозможно, или неудобно, соединить точку доступа с проводной инфраструктурой, или какое-либо препятствие затруднит осуществление связи точки доступа с местом расположения беспроводных станций клиентов напрямую. В такой ситуации можно использовать точку в режиме повторителя (Repeater) (рисунок 1.10).

Аналогично проводному повторителю, беспроводный повторитель просто ретранслирует все пакеты, поступившие на его беспроводный интерфейс. Эта ретрансляция осуществляется через тот же канал, через который они были получены.

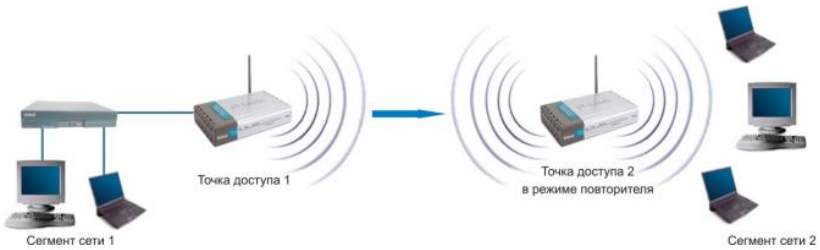


Рисунок 1.10 – Режим повторителя

При применении точки доступа-повторителя следует помнить, что наложение широковещательных доменов может привести к сокращению пропускной способности канала вдвое, потому что начальная точка доступа также «слышит» ретранслированный сигнал.

Режим повторителя не включен в стандарт 802.11, поэтому для его реализации рекомендуется использовать однотипное оборудование (вплоть до версии прошивки) и от одного производителя. С появлением WDS данный режим потерял свою актуальность, потому что функционал WDS заменяет его. Однако его можно встретить в старых версиях прошивок и в устаревшем оборудовании.

1.9.5 Режим клиента

При переходе от проводной архитектуры к беспроводной иногда можно обнаружить, что имеющиеся сетевые устройства поддерживают проводную сеть Ethernet, но не имеют интерфейсных разъемов для беспроводных сетевых адаптеров. Для подключения таких устройств к беспроводной сети можно использовать точку доступа - клиент рисунок 1.11.

Рисунок 1.11 – Режим клиента

При помощи точки доступа-клиента к беспроводной сети подключается только одно устройство. Этот режим не включен в стандарт 802.11, и поддерживаются не всеми производителями.

1.10 Технология WDS

Термин WDS (Wireless Distribution System) расшифровывается как «распределённая беспроводная система». Данная технология поддерживается большинством современных точек доступа. Если говорить упрощённо, то данная технология позволяет точкам доступа устанавливать беспроводное соединение не только с беспроводными клиентами, но и между собой.

Технология WDS – позволяет одновременно подключать беспроводных клиентов, к точкам, работающим в режиме Bridge (мост точка-точка) и Multipoint Bridge (мост точка-много точек). Однако скорость передачи данных у беспроводных клиентов, в таком режиме будет порядка 1/3 от скорости передачи данных между точками доступа.

Соединения WDS рисунок 1.12 основываются на MAC-адресах и используют специальный тип кадров, в которых задействованы все четыре поля для MAC-адресов, определённые стандартом 802.11, вместо трех, как при обычной передаче данных между точкой доступа и клиентом. Напомним, что при взаимодействии клиентов с точкой доступа заголовок каждого кадра содержит MAC-адреса узла-отправителя, узла-получателя и самой точки доступа. В случае использования WDS-технологии в каждый кадр, кроме MAC-адреса узла-отправителя и узла-получателя, вставляются также MAC-адреса ассоциированной с узлом точки доступа и взаимодействующей с ней точки доступа.

Технология WDS может использоваться для реализации двух режимов беспроводных соединений между точками доступа: режима беспроводного моста (радиомоста) и режима беспроводного повторителя.

Рисунок 1.12 – Технология WDS

Режим беспроводного моста позволяет точкам доступа работать только с другими точками доступа, но не с клиентскими адаптерами. Режим беспроводного повторителя позволяет точкам доступа работать как с другими точками доступа, так и с клиентскими адаптерами.

Понятно, что рассматриваемая нами архитектура распределённой беспроводной сети подразумевает функционирование обеих точек доступа в режиме беспроводных повторителей.

1.11 Развертывание распределённых беспроводных сетей (WDS)

Беспроводные сети, называемые также Wi-Fi- или WLAN (Wireless LAN)-сети, обладают, по сравнению с традиционными проводными сетями, немалыми преимуществами, главным из которых, конечно же, является простота развёртывания. Так, беспроводная сеть не нуждается в прокладке кабелей (часто требующей штробления стен); трудно оспорить такие достоинства беспроводной сети, как мобильность пользователей в зоне её действия и простота подключения к ней новых пользователей. В то же время беспроводные сети на современном этапе их развития не лишены серьёзных недостатков. Прежде всего, это низкая, по сегодняшним меркам, скорость соединения, которая к тому же серьёзно зависит от наличия преград и от расстояния между приёмником и передатчиком; плохая масштабируемость, а также, если речь идёт об использовании беспроводной сети в помещениях, довольно ограниченный радиус действия сети.

Один из способов увеличения радиуса действия беспроводной сети заключается в создании распределённой сети на основе нескольких точек беспроводного доступа. При создании таких сетей в домашних условиях появляется возможность превратить всю квартиру в единую беспроводную зону и увеличить скорость соединения вне зависимости от количества стен (преград) в квартире [4].

1.12 Проблемы безопасности Wi-Fi сетей

Как и любая компьютерная сеть, Wi-Fi – является источником повышенного риска несанкционированного доступа. Кроме того, проникнуть в беспроводную сеть значительно проще, чем в обычную, — не

нужно подключаться к проводам, достаточно оказаться в зоне приема сигнала.

Беспроводные сети отличаются от кабельных только на первых двух - физическом (Phy) и отчасти канальном (MAC) - уровнях семиуровневой модели взаимодействия открытых систем. Более высокие уровни реализуются как в проводных сетях, а реальная безопасность сетей обеспечивается именно на этих уровнях. Поэтому разница в безопасности тех и других сетей сводится к разнице в безопасности физического и MAC-уровней.

Хотя сегодня в защите Wi-Fi-сетей применяются сложные алгоритмические математические модели аутентификации, шифрования данных и контроля целостности их передачи, тем не менее, вероятность доступа к информации посторонних лиц является весьма существенной. И если настройке сети не уделить должного внимания злоумышленник может:

- заполучить доступ к ресурсам и дискам пользователей Wi-Fi-сети, а через неё и к ресурсам LAN;
- подслушивать трафик, извлекать из него конфиденциальную информацию;
- искажать проходящую в сети информацию;
- воспользоваться интернет-траффиком;
- атаковать ПК пользователей и серверы сети, внедрять поддельные точки доступа;
- рассылать спам, и совершать другие противоправные действия от имени вашей сети.

Для защиты сетей 802.11 предусмотрен комплекс мер безопасности передачи данных.

На раннем этапе использования Wi-Fi сетей таковым являлся пароль SSID (Server Set ID) для доступа в локальную сеть, но со временем оказалось, что данная технология не может обеспечить надежную защиту.

Главной же защитой долгое время являлось использование цифровых ключей шифрования потоков данных с помощью функции Wired Equivalent Privacy (WEP). Сами ключи представляют из себя обыкновенные пароли с длиной от 5 до 13 символов ASCII. Данные шифруются ключом с разрядностью от 40 до 104 бит. Но это не целый ключ, а только его статическая составляющая. Для усиления защиты применяется так называемый вектор инициализации Initialization Vector (IV), который предназначен для рандомизации дополнительной части ключа, что обеспечивает различные вариации шифра для разных пакетов данных. Данный вектор является 24-битным. Таким образом, в результате мы получаем общее шифрование с разрядностью от 64 (40+24) до 128 (104+24) бит, в результате при шифровании мы оперируем и постоянными, и случайно подобранными символами. Но, как оказалось, взломать такую защиту можно соответствующие утилиты присутствуют в Интернете (например, AirSnort, WEPcrack). Основное её слабое место — это вектор инициализации.

Поскольку мы говорим о 24 битах, это подразумевает около 16 миллионов комбинаций, после использования этого количества, ключ начинает повторяться. Хакеру необходимо найти эти повторы (от 15 минут до часа для ключа 40 бит) и за секунды взломать остальную часть ключа. После этого он может входить в сеть как обычный зарегистрированный пользователь.

Как показало время, WEP тоже оказалась не самой надёжной технологией защиты. После 2001 года для проводных и беспроводных сетей был внедрён новый стандарт IEEE 802.1X, который использует вариант динамических 128-разрядных ключей шифрования, то есть периодически изменяющихся во времени. Таким образом, пользователи сети работают сеансами, по завершении которых им присылается новый ключ. Например, Windows XP поддерживает данный стандарт, и по умолчанию время одного сеанса равно 30 минутам. IEEE 802.1X - это новый стандарт, который оказался ключевым для развития индустрии беспроводных сетей в целом. За основу взято исправление недостатков технологий безопасности, применяемых в 802.11, в частности, возможность взлома WEP, зависимость от технологий производителя и т. п. 802.1X позволяет подключать в сеть даже PDA-устройства, что позволяет более выгодно использовать саму идею беспроводной связи. С другой стороны, 802.1X и 802.11 являются совместимыми стандартами. В 802.1X применяется тот же алгоритм, что и в WEP, а именно — RC4, но с некоторыми отличиями. 802.1X базируется на протоколе расширенной аутентификации (EAP), протоколе защиты транспортного уровня (TLS) и сервере доступа Remote Access Dial-in User Server. Протокол защиты транспортного уровня TLS обеспечивает взаимную аутентификацию и целостность передачи данных. Все ключи являются 128-разрядными по умолчанию.

В конце 2003 года был внедрён стандарт Wi-Fi Protected Access (WPA), который совмещает преимущества динамического обновления ключей IEEE 802.1X с кодированием протокола интеграции временного ключа TKIP, протоколом расширенной аутентификации (EAP) и технологией проверки целостности сообщений MIC. WPA — это временный стандарт, о котором договорились производители оборудования, пока не вступил в силу IEEE 802.11i. По сути, WPA = 802.1X + EAP + TKIP + MIC, где:

– WPA — технология защищённого доступа к беспроводным сетям;

– EAP — протокол расширенной аутентификации (Extensible Authentication Protocol);

– TKIP — протокол интеграции временного ключа (Temporal Key Integrity Protocol);

– MIC — технология проверки целостности сообщений (Message Integrity Check).

Стандарт TKIP использует автоматически подобранные 128-битные ключи, которые создаются непредсказуемым способом и общее число вариаций которых достигает 500 миллиардов. Сложная иерархическая система алгоритма подбора ключей и динамическая их замена через каждые

10 Кбайт (10 тыс. передаваемых пакетов) делают систему максимально защищённой.

От внешнего проникновения и изменения информации также обороняет технология проверки целостности сообщений (Message Integrity Check).

Достаточно сложный математический алгоритм позволяет сверять отправленные в одной точке и полученные в другой данные. Если замечены изменения и результат сравнения не сходится, такие данные считаются ложными и выбрасываются.

Правда, TKIP сейчас не является лучшим в реализации шифрования, поскольку в силу вступают новые алгоритмы, основанные на технологии Advanced Encryption Standard (AES), которая, уже давно используется в VPN. Что касается WPA, поддержка AES уже реализована в Windows XP, пока только опционально.

Помимо этого, параллельно развивается множество самостоятельных стандартов безопасности от различных разработчиков, в частности, в данном направлении преуспевают Intel и Cisco. В 2004 году появляется WPA2, или 802.11i, который, в настоящее время является максимально защищённым.

Таким образом, на сегодняшний день у обычных пользователей и администраторов сетей имеются все необходимые средства для надёжной защиты Wi-Fi, и при отсутствии явных ошибок (пресловутый человеческий фактор) всегда можно обеспечить уровень безопасности, соответствующий ценности информации, находящейся в такой сети.

Сегодня беспроводную сеть считают защищенной, если в ней функционируют три основных составляющих системы безопасности: аутентификация пользователя, конфиденциальность и целостность передачи данных. Для получения достаточного уровня безопасности необходимо воспользоваться рядом правил при организации и настройке частной Wi-Fi-сети:

- шифровать данные путем использования различных систем;
- Максимальный уровень безопасности обеспечит применение VPN;
- использовать протокол 802.1X;
- запретить доступ к настройкам точки доступа с помощью беспроводного подключения;
- управлять доступом клиентов по MAC-адресам;
- запретить трансляцию в эфир идентификатора SSID;
- располагать антенны как можно дальше от окон, внешних стен здания, а также ограничивать мощность радиоизлучения;
- использовать максимально длинные ключи;
- изменять статические ключи и пароли;
- использовать метод WEP-аутентификации “Shared Key" так как клиенту для входа в сеть необходимо будет знать WEP-ключ;
- пользоваться сложным паролем для доступа к настройкам точки доступа;

– по возможности не использовать в беспроводных сетях протокол TCP/IP для организации папок, файлов и принтеров общего доступа;

– Организация разделяемых ресурсов средствами NetBEUI в данном случае безопаснее;

– не разрешать гостевой доступ к ресурсам общего доступа,

– использовать длинные сложные пароли;

– не использовать в беспроводной сети DHCP. Вручную распределить статические IP-адреса между легитимными клиентами безопаснее;

– на всех ПК внутри беспроводной сети установить файерволлы, не устанавливать точку доступа вне брандмауэра, использовать минимумпротоколов внутри WLAN (например, только HTTP и SMTP);

– регулярно исследовать уязвимости сети с помощью специализированных сканеров безопасности (например NetStumbler).

Так же угрозу сетевой безопасности могут представлять природные явления и технические устройства, однако только люди (недовольные уволенные служащие, хакеры, конкуренты) внедряются в сеть для намеренного получения или уничтожения информации и именно они представляют наибольшую угрозу [5].

2 Исследование информационной безопасности в сетях Wi-Fi

2.1 Механизмы аутентификации и безопасности протокола 802.11

2.1.1 Алгоритм конфиденциальности проводного эквивалента

В беспроводной локальной сети вопрос прослушивания имеет особую важность — ведь уловить передачу так просто! Для обеспечения современного уровня безопасности стандарт IEEE 802.11 включает схему WEP. Для обеспечения конфиденциальности (а также целостности данных) используется алгоритм, основанный на алгоритме шифрования RC4.

Алгоритм обеспечения целостности — это простая 32-битовая последовательность циклической проверки чётности с избыточностью (CRC), присоединяемая к концу кадра MAC (рис. 14.8, *а).* Для процесса шифрования 40-битовый секретный ключ делится между двумя сообщающимися сторонами. К секретному ключу присоединяется вектор инициализации (IV). Получившийся блок — это начальное число генератора псевдослучайной последовательности (PRNG), определенного в RC4.

Генератор создает последовательность битов, длина которой равна длине кадра MAC плюс CRC. Побитовое применение операции исключающего ИЛИ к кадру MAC и псевдослучайной последовательности даёт шифрованный текст. К данному тексту присоединяется вектор инициализации, и результат передаётся. Вектор инициализации периодически меняется (при каждой новой передаче), следовательно, меняется псевдослучайная последовательность, что усложняет задачу расшифровки перехваченного текста.

После получения сообщения приемник извлекает вектор инициализации и присоединяет его к совместно используемому секретному ключу, после чего генерирует ту же псевдослучайную последовательность, что и источник. К полученному таким образом ключу и поступившим данным побитово применяется операция исключающего ИЛИ, результатом которой является исходный текст. Данный алгоритм основан на следующем свойстве исключающего ИЛИ:

$$A + B + B = A$$

Таким образом, если взять исходный текст, применить к нему и ключевой последовательности операцию исключающего ИЛИ, а затем применить операцию исключающего ИЛИ к результату и той же ключевой последовательности, то в итоге получится исходный текст. В заключение приемник сравнивает поступившую последовательность CRC и CRC вычисленную по восстановленным данным: если величины совпадают, данные считаются неповреждёнными.

2.1.2 Аутентификация

Стандарт IEEE 802.11 предлагает два типа аутентификации: "открытая система" и "общий ключ". Аутентификация открытых систем просто позволяет двум сторонам договориться о передачи данных без

рассмотрения вопросов безопасности. В этом случае одна станция передает другой управляющий кадр MAC, именуемый кадром аутентификации. В данном кадре указывается, что имеет место аутентификация открытых систем. Другая сторона отвечает собственным кадром аутентификации — и процесс завершен. Таким образом, при аутентификации открытых систем стороны просто обмениваются информацией о себе.

Аутентификация с общим ключом требует, чтобы две стороны совместно владели секретным ключом, не доступным третьей стороне. Процедура аутентификации между двумя сторонами, A и B, выглядит следующим образом.

1) A посылает кадр аутентификации, в котором указан тип "общий ключ" и идентификатор станции (или идентификатор сети SSID, если одна из сторон – точка доступа), определяющий станцию-отправителя.

2) B отвечает кадром аутентификации, который включает 128-октетный текст запроса. Текст запроса создается с использованием генератора случайных чисел WEP. Ключ и вектор инициализации, используемые при генерации текста запроса, не важны, поскольку далее в процедуре они не используются.

3) A передает кадр аутентификации, который включает полученный от B текст запроса. Кадр шифруется с использованием схемы WEP.

4) B получает зашифрованный кадр и дешифрует его, используя WEP и секретный ключ, которым владеют A и B. Если дешифрование прошло успешно (совпали CRC), B сравнивает принятый текст запроса с текстом, который был послан на втором этапе процедуры. После этого B передает **A** сообщение аутентификации, содержащее код состояния (успех или неудача).

В стандарте IEEE 802.11 предусматриваются аутентификация устройства (радиокарты) по ее MAC-адресу и аутентификация сети по ее названию (SSID), однако такую систему нельзя назвать надежно защищенной — к примеру, одно и то же устройство (радиокарта) может обслуживать различных пользователей. Соответственно, необходима аутентификация пользователя. При построении сложных узлов доступа, включающих беспроводные сегменты, последние гармонично вписываться в систему безопасности и идентификации существующего проводного сегмента, тем более, что средства безопасности и идентификации, включённые в стандарты 802.11, на современном этапе совершенно не достаточны. Из этого можно сделать единственно правильный вывод: в беспроводном сегменте необходимо использовать для безопасности и идентификации протоколы, хорошо зарекомендовавшие себя в проводных ЛВС. В скором времени к этим средствам можно будет добавить технологии, находящиеся в процессе утверждения институтом IEEE, такие как WPA, 802.1x, которые в итоге должны выльется в новый стандарт защищённых беспроводных сетей 802.11i . Рассмотрим подробно задачи системы идентификации и учёта.

2.2Аутентификация

Аутентификация *(*англ. authentication - идентификация*)* - процесс проверки имени пользователя и пароля или другого идентификатора из известного пространства имен. Именем может являться имя отправителя сообщения, идентификатор узла сети и т. д. 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 или процесс сообщает сведения о себе. Проверка подлинности или аутентификация – есть процедура проверки достоверности предъявленных данных.

В зависимости от строгости требований по безопасности в системах ААА могут применяться различные базовые способы (алгоритмы) аутентификации. Рассмотрим некоторые из них. Обычная аутентификация**.**

При этом способе пользователь, подлинность которого требуется проверить, посылает серверу, услугами которого он желает воспользоваться, пару логин – пароль. После получения данной информации сервер может либо сам исполнить роль аутентификатора, либо передать эти данные дальше – специальному серверу аутентификации. Если аутентификация прошла успешно, сервер услуг сообщает пользователю подтверждение и продолжает работу с ним, в противном случае производится попытка повторной аутентификации или просто прекращение связи.

Такой способ аутентификации прост в реализации, удобен при использовании его людьми. Однако во многих случаях он не обеспечивает требуемый уровень безопасности, так как не абсолютно защищен от прослушивания канала связи. Его использование целесообразно в случае одновременного применения средств шифрации или при затрудненном доступе к линии связи.

Аутентификация с использованием общего секрета**.** Метод заключается в том, что сервер, к которому пытается подключиться пользователь, передает ему некоторое случайное число или комбинацию символов. В свою очередь пользователь (или, скорее, терминал пользователя), по известному алгоритму производит шифрацию или расчет хэш-функции поступивших от сервера данных и передает полученную комбинацию обратно. Расчет производится с помощью общего для пользователя и сервера «секрета» или ключа, который не передается по сети.

Сервер, приняв информацию от клиента, проводит точно такой же расчет и сравнивает полученные результаты. Если они совпадают, работа с пользователем продолжается.

Под хэш-функциями понимаются функции, отображающие сообщения произвольной длины в значения фиксированной длины, которые часто

называют хэш-кодами. Таким образом, у всякой хэш-функции h имеется большое количество пар значений $x \neq y$ (x<>y) таких, что h(x)=h(y).

Так, даже зная исходные данные и полученные после расчета практически невозможно точно определить «секрет».При таком подходе к решению проблемы опасность прослушивания канала существенно уменьшается (при шифрации) или даже вообще устраняется (при вычислении хэша).

Представленные выше методы являются базовыми методами аутентификации. Необходимо отметить, что выполнение задач 3А можно возложить на сам сервер услуг или воспользоваться отдельным специальным сервером, что позволяет строить масштабируемые системы аутентификации, авторизации и учета.

Существует два возможных варианта использования отдельных серверов 3А: применение серверов аутентификации прозрачных для пользователя и не прозрачных для оного. Ниже оба этих варианта рассмотрены более подробно.

2.2.1 Применение сервера аутентификации, непрозрачного для пользователя

Непрозрачность сервера аутентификации состоит в том, что пользователь взаимодействует с ним отдельно от сервера услуг, что выливается в отдельный этап аутентификации.

Рассмотрим подробнее суть метода: пользователь для аутентификации первоначально обращается не к северу услуг, а к специальному серверу 3А. Далее происходит проверка его подлинности по одному из описанных выше способов (обычная аутентификация, либо с использованием общего секрета) в результате которой пользователь получает некоторый блок данных.

Эта информация представляет собой так называемый "билет", зашифрованный секретным ключом сервера услуг и копию *части* информации из билета, зашифрованную секретным ключом пользователя. Пользователь должен расшифровать вторую порцию данных и переслать ее вместе с билетом серверу. Сервер услуг, расшифровав "билет", может сравнить его содержимое с дополнительной информацией, переданной пользователем. Совпадение свидетельствует о том, что пользователь смог расшифровать предназначенные ему данные – ведь содержимое "билета" никому, кроме сервера услуг и сервера 3А, недоступно, и продемонстрировал знание своего секретного ключа. Значит, пользователь - именно тот субъект, за кого себя выдает.

Пропуск и данные для пользователя могут содержать так называемый сессионный ключ, который будет использоваться для шифрации данных во время обмена информацией между пользователем и сервером услуг. Кроме защиты информации при передаче это позволяет пользователю доверять серверу, так как сессионный ключ зашифрован секретом сервера услуг.

Такой метод, преимущественно используется в Интернет, когда необходимо разгрузить большое число серверов услуг от задач 3А и когда клиент не может полностью доверять серверу услуг.

Так же при этом нет необходимости в том, что бы пользователь заранее устанавливал какие-либо отношения с сервером услуг. Ему достаточно быть зарегистрированным на сервере аутентификации.

2.2.2 Применение сервера аутентификации, прозрачного для пользователя

В этом случае с точки зрения пользователя аутентификация происходит на сервере услуг. При этом на самом деле сервер услуг просто передает запрос дальше – специальному серверу 3А и осуществляет дальнейшую работу с пользователем, основываясь на ответе этого сервера 3А. Практически всегда тот же сервер используется и для решения задач учета предоставленных услуг.

Такой подход позволяет строить масштабируемые системы аутентификации и учета, кроме того, удобен для пользователя, в отличие от предыдущего. Этот метод широко используется провайдерами Internet и IP – телефонии. Этапы аутентификации: 1 – запрос доступа к серверу услуг; 2 – передача запроса серверу ААА; 2 – положительный или отрицательный ответ по результатам проверки данных, полученных от пользователя; 4 – соответствующий ответ пользователю (положительный, либо прекращение связи).

В настоящее время вопросам защиты информации при аутентификации и вообще данных аутентификации уделяется должное внимание. Данные защищаются таким образом, что, даже обладая достаточными вычислительными мощностями крайне сложно получить пароли или секреты, используемые в системах 3А. Получают распространение аппаратные ключи.

Существует несколько конкретных технологий, обеспечивающих описанные выше способы аутентификации. Они будут рассмотрены далее.

2.2.3 Авторизация

Авторизация (англ. authorization) – процесс определения конкретных прав пользователя, таких как права на доступ к некоторым ресурсам (услугам), которые могут быть предоставлены давшему соответствующую информацию (информацию, удостоверяющую возможность получения определенных прав). Примером может служить определение максимально допустимого времени пребывания на линии в случае предоставления Dial-up услуг, максимально допустимый объём входящего трафика.

Кроме того, во время авторизации может производиться согласование и настройка некоторых параметров, необходимых пользователю для работы с сервером услуг. Примером является определение IP-адреса терминала пользователя, настройка шлюзов и DNS-серверов при подключении по коммутируемым линиям СТОП к провайдеру Интернет. Авторизация может быть совмещена с процессом аутентификации или проходить отдельно. Это зависит от конкретной технологии 3А. Эти понятия тесно взаимосвязаны. В

литературе часто употребляется только понятие "авторизация", как более ёмкое.

2.2.4 Учёт

Учёт (англ. accounting) - процесс сбора информации об использовании ресурсов в целях последующего анализа, определения стоимости, биллинга или же для мониторинга сети. Во всех известных технологиях 3А процедуры учета отделены от аутентификации и авторизации. Более того – возможно независимое использование их друг от друга. Процедура учета предоставленных услуг может быть логически связана с процедурами аутентификации и авторизации. Это выражается в наличии в сообщениях аутентификации и учета определенных общих идентификаторов. Будет ли использоваться такая логическая связь или нет, будут ли использованы функции аутентификации и учета вместе или только что-то одно – зависит от обстоятельств, например от схемы расчета провайдера услуг со своими абонентами и партнерами.

Можно говорить о двух вариантах организации системы идентификации и учёта: задачи 3А могут возлагаться как на сам сервер услуг, так и на специальный сервер, при этом решение о возможности предоставления услуги принимается либо серверами услуг и аутентификации совместно, либо только сервером аутентификации, а сервер услуг полностью руководствуется этим решением.

В последние годы с резким увеличением числа пользователей Интернет более оправдывает себя второй метод. Разделение функций идентификации и обслуживания пользователей позволяет снизить нагрузку на сервер услуг и добиться стабильной работы сервера, предотвращая его перегрузку

2.3 Архитектура системы при использовании отдельного сервера аутентификации, авторизации и учёта

В этом разделе рассматривается архитектура системы идентификации и учёта в случае использования сервера AAA, прозрачного для пользователя, как варианта, нашедшего наибольшее применение при предоставлении пользователю популярнейших на сегодняшний день услуг – удалённого доступа в сеть Интернет и IP – телефонии.

Основным компонентом системы является модуль логики задач идентификации и учёта. На него возлагается осуществление процессов аутентификации, авторизации и учёта, то есть умение обрабатывать запросы на разрешение доступа к тому или иному ресурсу, определять субъектов на основании данных, представленных в запросе.

Необходимым компонентом системы также является база данных, которая хранит в себе пространство определённых имён (информация аутентификации) и информацию обо всех службах, предоставляемых провайдером, которые могут быть запущены по требованию пользователя с указанием прав каждого пользователя.

За выполнение задач, связанных с запуском определённого сервиса отвечает непосредственно сервер услуг, запуск происходит на основании информации, полученной от системы идентификации и учёта.

С точки зрения аппаратной реализации системы вышеперечисленные компоненты концентрируются на отдельном сервере, получившим название сервера аутентификации.

Такой способ организации системы идентификации и учёта позволяет строить масштабируемые системы с использованием нескольких серверов аутентификации, связанных между собой. Реально такие системы пока находят малое практическое применение, но с постоянным увеличением числа пользователей сети Интернет широкое применение таковых можно ожидать уже в недалёком будущем.

Наиболее распространенный вариант реализации архитектуры системы идентификации и учёта с использованием отдельного сервера аутентификации – сервер AAA прозрачен для пользователя. Именно такая разновидность аутентификации используется большинством провайдеров при предоставлении услуг удалённого доступа и IP – телефонии. Доступ пользователя к указанным видам обслуживания происходит в четыре этапа: 1 - запрос доступа к серверу услуг; 2 – передача запроса серверу AAA; 3 - положительный или отрицательный ответ по результатам проверки данных, полученных от пользователя; 4 – соответствующий ответ пользователю.

2.3.1 Технология RADIUS

RADIUS – протокол уровня представлений функциональной модели системы аутентификации. На его основе реализована самая распространенная на сегодняшний день технология аутентификации пользователей при пользовании услугами удалённого доступа в сеть Интернет. Изначально концепция RADIUS состояла в обеспечении удаленного доступа через коммутируемое телефонное соединение. Со временем выкристаллизовались и другие области применения этой технологии. К ним относятся серверы виртуальных частных сетей (Virtual Private Network, VPN) — они в большинстве своем поддерживают Radius, — а также точки доступа беспроводных локальных сетей (Wireless LAN, WLAN).

Как видно из названия раздела, RADIUS используется при сценарии прозрачного для пользователя сервера аутентификации. На сегодняшний день данная технология является доминирующей, а существующие аналогичные решения, уступают решениям на базе RADIUS по скорости обработки запросов и в возможности построения распределенных систем. Системы на основе RADIUS производятся всеми ведущими поставщиками оборудования для провайдеров Интернет. Данная технология является общепризнанной.

2.3.2 Особенности протокола RADIUS

Протокол RADIUS (Remote Authentication Dial In User Service) был разработан компанией Livingston Enterprises Inc. в качестве протокола идентификации серверного доступа и учёта.

RADIUS – технология, обеспечивающая построение распределенных систем аутентификации, то есть проверки возможности предоставления доступа в сеть пользователю, и учета услуг предоставленных данному пользователю провайдерами Интернет.

Единственным более – менее внушительным конкурентом RADIUS в настоящее время является протокол TACACS – Terminal Access Controller Access Control System. Этот протокол, также обеспечивающий функции аутентификации, проверку полномочий и учёт, применялся еще до создания RADIUS, но после появления последнего TACACS находится на вторых ролях, прежде всего потому, что она является собственной технологией компании Cisco Systems, не допуская , соответственно, локализации и усовершенствования (добавления новых функций) под определённые типы оборудования других компаний. Сейчас TACACS (обновленный с целью поддержки новых функций) помимо Cisco использует еще ряд производителей. Кроме того, эта технология по-прежнему достаточно надежна для создания единой точки проверки полномочий пользователей и администрирования при удаленном доступе. Тем не менее RADIUS остается доминирующим методом аутентификации.

Технология RADIUS позволяет централизованно управлять аутентификацией, определением полномочий и контролем за работой удаленных пользователей. Короче говоря, RADIUS создает единую точку наблюдения и проверки всех удаленных пользователей, а сервер RADIUS разрешает или запрещает пользователю доступ в соответствии с принятыми в данной компании критериями.

Большинство продуктов RADIUS имеют также функции учета, например они хранят журналы, где регистрируются все запросы на аутентификацию и результаты выполнения этих запросов, вплоть до конкретного порта, через который пользователь устанавливал соединение. Подобные функции учета позволяют узнать, кто из пользователей в данный момент имеет соединение с сервером удаленного доступа, а также получить любую информацию о предыдущих сеансах (в том числе об их длительности).

Можно выделить основные черты RADIUS: в системе RADIUS функции идентификации и авторизации совмещены, учетные функции протокола RADIUS могут использоваться независимо от функций идентификации и авторизации. Учетные функции RADIUS позволяют в начале и в конце каждой сессии отправлять данные о количестве ресурсов (то есть времени, пакетов, байтов и т.д.), использованных в ходе этой сессии. Провайдер услуг Интернет (ISP) может использовать программные средства контроля доступа и учета RADIUS для удовлетворения специальных требований безопасности и биллинга.

Протокол RADIUS основан на технологии "клиент – сервер". Клиентом обычно является сервер доступа, сервер VPN или точка доступа беспроводной локальной сети, а сервером RADIUS считается "демон"

(deamon), работающий на машине UNIX или NT. Для других серверов RADIUS или идентификационных серверов других типов сервер RADIUS может выступать в роли клиента-посредника (proxy). Концепция службы идентификации удаленных пользователей подразумевает, что клиент RADIUS отсылает серверу RADIUS параметры доступа пользователя в англоязычной документации они часто называются.

2.4 Варианты обеспечения безопасности беспроводных сетей стандарта 802.11

Нельзя не остановиться еще на одной проблеме беспроводных сетей, касающейся их информационной безопасности. Обеспечение безопасности радиосети, как и любой другой коммуникационной системы, сводится к решению трех проблем — защиты от подключения к сети нелегальных пользователей, предотвращения несанкционированного доступа к ресурсам сети зарегистрированных потребителей и гарантированной поддержки целостности и конфиденциальности данных, передаваемых по радиоканалам. При этом не будем рассматривать случаи, касающиеся преднамеренного нарушения физической целостности сети. Для решения первых двух задач сегодня применяются процедуры аутентификации (authentication), авторизации (authorization) и учета (accounting), рассмотренные в предыдущей части главы.

Один из мифов, имеющий весьма древние корни, гласит, что радиосети плохо защищены и их пользователи весьма уязвимы для атак хакеров. В действительности же такая оценка слишком примитивна и не отражает нынешнего состояние развития технологии и рынка.

Источники угроз для беспроводных сетей — природные явления, технические устройства и злоумышленники. Результатами деструктивных действий или негативных внешних влияний для радиосетей могут стать нарушение их физической целостности, прослушивание (сканирование) трафика и несанкционированное подключение.

Целостность беспроводной сети способны нарушить случайные или преднамеренные помехи в радиоканале. Как правило, их источником является промышленное и бытовое СВЧ-оборудование, которое эксплуатируется на легальной либо нелегальной основе. Разумеется, угроза нарушения физической целостности радиосети уменьшается внутри зданий, где легче проконтролировать посторонние источники излучения. Что же касается наружных систем, контроль за источниками излучения осуществляет государственная служба радиоконтроля. Таким образом, задача восстановления физической целостности радиосети вполне решаема с помощью административных мер.

Прослушивание трафика возможно в любой точке зоны видимости радиосети. Однако более сложная, чем в проводной сети, структура сигнала, используемая средствами RadioEthernet, обеспечивает некоторую дополнительную защиту за счет усложнения синхронизации подслушивающих устройств. С другой стороны, поскольку структура

сигнала зафиксирована в стандарте, саму по себе ее нельзя считать средством защиты. Для уменьшения угрозы подслушивания стандарт IEEE 802.11 предусматривает шифрование трафика по алгоритму WEP (Wired Equivalent Privacy).

2.4.1 WEP

WEP состоит из пяти элементов.

– Секретный ключ (WEP-ключ — распространяется среди всех абонентов сети).

– Алгоритмы шифрования и дешифровки, которые используют поточную схему кодирования на основе алгоритма RC4.

– Вектор инициализации длиной 24 бит. Он объединяется с WEP-ключом, в результате чего получается входная последовательность (длиной 64 или 128 бит) алгоритма RC4. При этом WEP случайным образом выбирает для любого передаваемого пакета уникальный вектор инициализации (в ряде вариантов для каждого последующего пакета его значение изменяется на единицу).

– Инкапсуляция — передача вектора инициализации и закодированного сообщения от отправителя к адресату.

– Проверка целостности. Ее результаты шифруются вместе с открытым текстом и передаются адресату в составе закодированного сообщения.

Первоначально 802.11 обеспечивал контроль доступа на MAC уровне (второй уровень в модели ISO/OSI), и механизмы шифрования, известные как WEP, целью которых является обеспечение беспроводной сети средствами безопасности, эквивалентными средствам безопасности проводных сетей. Когда включен WEP, он защищает только пакет данных, но не защищает заголовки физического уровня, так что другие станции в сети могут просматривать данные, необходимые для управления сетью. Для контроля доступа в каждую точку доступа помещается так называемый ESSID (или WLAN Service Area ID), без знания которого мобильная станция не сможет подключиться к точке доступа. Дополнительно точка доступа может хранить список разрешённых MAC адресов, называемый списком контроля доступа (Access Control List, ACL), разрешая доступ только тем клиентам, чьи MAC адреса находятся в списке.

Для шифрования данных стандарт предоставляет возможности шифрования с использованием алгоритма RC4 с 40-битным разделяемым ключом. После того, как станция подключается к точке доступа, все передаваемые данные могут быть зашифрованы с использованием этого ключа. Когда используется шифрование, точка доступа будет посылать зашифрованный пакет любой станции, пытающейся подключиться к ней. Клиент должен использовать свой ключ для шифрования корректного ответа для того, чтобы аутентифицировать себя и получить доступ в сеть. Выше второго уровня сети 802.11 поддерживают те же стандарты для контроля доступа и шифрования (например, IPSec), что и другие сети 802.

Для несанкционированного подключения злоумышленнику достаточно оказаться в зоне радиовидимости и иметь оборудование того же типа, на базе которого построена сеть. С целью снижения вероятности вторжения предусмотрены контроль за доступом по MAC-адресам всех устройств и использование уже упомянутого алгоритма WEP. Функции контроля за доступом реализуются с помощью точки доступа, поэтому возможны только в рамках инфраструктурной топологии сети. Механизм контроля подразумевает заблаговременное составление таблицы MAC-адресов разрешенных пользователей в точке доступа и обеспечивает передачу данных только между зарегистрированными беспроводными адаптерами.

Построение узла доступа требует создания непрерывной зоны покрытия в пределах офисного здания, кафе и любого другого помещения Данное решение часто требует размещения достаточно большого количества точек доступа. И, в таком случае, актуальной становится задача мониторинга и управления беспроводной сетью. Следовательно, уже на этапе проектирования необходимо заложить в решение использование средств централизованного управления и мониторинга состояния сети, что в дальнейшем позволит существенно снизить совокупную стоимость владения системой.

Другим основным вопросом при построении беспроводных сетей, безусловно, является вопрос обеспечения требуемого уровня безопасности информации, циркулирующей в сети. В первую очередь, причина остроты вопроса в используемой среде передачи данных - радиоэфире. В отличие от обычных сетей, в которых информация передается по проводам, осуществить перехват информации в радиоэфире намного проще - достаточно иметь комплект оборудования, аналогичный комплекту оборудования абонента беспроводной сети. Поэтому в спецификации стандартов 802.11 особое внимание уделено вопросам безопасности - определен протокол обеспечения безопасности беспроводных сетей WEP (Wired Equivalent Privacy).

Чтобы подступиться к решению этого вопроса, определим доступные меры и средства, позволяющие сделать беспроводную сеть как можно более безопасной. Для этого необходимо:

- Уменьшить зону радиопокрытия (разумеется, до минимально приемлемой). В идеале, зона радиопокрытия сети не должна выходить за пределы контролируемой территории.
- изменить пароль администратора, установленный по умолчанию;
- активизировать фильтрацию по MAC-адресам;
- запретить широковещательную рассылку идентификатора сети (SSID);
- изменить идентификатор сети (SSID), установленный по умолчанию;
- периодически изменять идентификатор сети (SSID);
- активизировать функции WEP;
- периодически изменять WEP-ключи;
- установить и настроить персональные межсетевые экраны и антивирусные программы у абонентов беспроводной сети;

– выполнить соответствующие настройки фильтрации трафика на телекоммуникационном оборудовании и межсетевых экранах;

– обеспечить резервирование оборудования, входящего в состав беспроводной сети;

– обеспечить резервное копирование ПО и конфигураций оборудования

– осуществлять периодический мониторинг состояния защищенности беспроводной сети с помощью специализированных средств анализа защищенности для беспроводных сетей.

Все эти методы защиты сегодня можно реализовать на оборудовании практически любого производителя, представленного на рынке беспроводных сетей стандарта 802.11 и имеющего логотип Wi-Fi.

Назовём комплекс вышеперечисленных мер защиты "начальным" уровнем, ниже которого опускаться категорически нельзя при проектировании корпоративной беспроводной сети. Даже реализовав этот уровень, учитывая известные технические и технологические проблемы протокола WEP, и, как следствие, низкий уровень сложности взлома подобной сети, беспроводную сеть с "начальным" уровнем безопасности лучше всего рассматривать как далеко не безопасную сеть. И, как следствие, точки доступа такой сети (даже при использовании WEP) не следует соединять с внутренней проводной сетью, - они должны находиться по внешнюю сторону от межсетевого экрана. Таким образом, обрабатывать конфиденциальную информацию в сети с описанным выше начальным уровнем безопасности нельзя.

Чтобы исправить ситуацию, некоторые производители (например, Agere Systems, D-Link, US Robotics,), с целью улучшения базового уровня защищенности, предлагают использовать более длинные ключи шифрования протокола WEP - 128, 152 или даже 256 бит. Но это часто приводит к отсутствию совместимости с оборудованием стандарта 802.11 других производителей. Кроме того, с точки зрения злоумышленника, трафик протокола WEP представляет из себя набор исходных данных для решения задачи криптоанализа типа "вскрытие с использованием выбранного ключа".

А учитывая то, что злоумышленнику известен алгоритм смены ключей, определенный протоколом WEP, на решение этой задачи он затратит несколько часов. После чего возможно несанкционированное подключение к нашей беспроводной сети. Мало того, заменить MAC-адрес своей карты доступа на MAC-адрес карты доступа легального пользователя, для злоумышленника не составит особого труда, а нам станет фактически не возможно обнаружить подобный взлом. Увеличение длины ключа даже до 256 бит, лишь увеличивает количество пакетов, которые должен прослушать злоумышленник (например, используя анализаторы пакетов AirMagnet или AiroPeek), и время, необходимое злоумышленнику для криптоанализа.

Поточный шифр RC4, лежащий в основе WEP-шифрования и разработанный американцем Рональдом Райвестом в 1987 году, получил широкое распространение благодаря удачному сочетанию

криптографической стойкости и высокого быстродействия. Уязвимости реализации протокола RC-4 в WEP изучаются криптографами достаточно давно. По мнению многих экспертов необходимо заменить криптографический инструментарий протокола WEP на более прочный. И уже сегодня на рынке есть решения, позволяющие сделать использование протокола WEP более безопасным.

Например:

– использование некоторых протоколов стандарта 802.1x (о них речь пойдет ниже), позволяет решить проблему динамической смены ключей шифрования для беспроводных устройств.

– протокол MIC (Message Integrity Check) позволяет защитить WEP-пакеты от их изменения и подделки, в процессе передачи.

– протокол TKIP (Temporal Key Integrity Protocol), также разработаный с целью улучшения ситуации с безопасностью протокола WEP, предполагает использование уникальной ключевой последовательности для каждого устройства, а также обеспечивает динамическую схему ключа каждые 10 000 пакетов. Однако, так же как и WEP, протокол TKIP использует для шифрования криптографический алгоритм RC4. Отметим, что для использования протокола TKIP нет необходимости отказываться от имеющегося оборудования 802.11, достаточно лишь обновить программное обеспечение (разумеется, если производитель реализовал поддержку этого протокола).

2.4.2 WPA

Осознание проблем протокола WEP пришло не вчера, и еще в мае 2001 г. группа IEEE Task Group I (TGi) начала работу над новым проектом IEEE 802.11i (MAC Enhancements for Enhanced Security), призванным обеспечить достаточную безопасность в беспроводных сетях. Однако окончательное утверждение протокола пока откладывается. Основные производители Wi-Fi-оборудования устав ждать ратификацию стандарта IEEE 802.11i, совместно с IEEE в ноябре 2002 г. анонсировали спецификацию Wi-Fi Protected Access (WPA). WPA базируется на компонентах ожидаемого стандарта IEEE 802.11i, которые к настоящему времени уже стабильны и не подвергаются переработке, а также могут быть развернуты в существующих сетях 802.11 без внесения аппаратных изменений в устройства. В WPA включены следующие компоненты IEEE 802.11i: протоколы IEEE 802.1x и TKIP (Temporal Key Integrity Protocol).

802.1x использует протокол EAP (Extensible Authentication Protocol), изначально разрабатывавшийся для работы поверх PPP (Point-to-Point Protocol) для передачи сообщений между тремя участниками аутентификации в ЛВС-окружении. Этот вид инкапсуляции известен как EAP over LANs, или EAPOL. EAP нельзя назвать методом аутентификации. Он определяет основную протокольную структуру для выбора специфического метода аутентификации. При использовании EAP аутентификатору не требуется "понимать" детали различных методов

аутентификации. В данном случае он выступает только как промежуточное звено, которое переупаковывает EAP-пакеты при их следовании между саппликантом (supplicant -- объект на конце сегмента "точка--точка", которому необходима аутентификация: это может быть клиентское ПО на компьютере, PDA или другом беспроводном устройстве) и сервером аутентификации. Такая технология предоставляет разработчикам возможность выбора между разными видами аутентификации, что является несомненным преимуществом. EAP (Extensible Authentication Protocol) - расширяемый протокол аутентификации позволяет проводить аутентификацию на основе: одноразовых паролей (OTP - one-time passwords), токенов, цифровых сертификатов, смарт-карт. Стандарт 802.1x определяет инкапсуляцию EAP во фреймы сети.

Temporal Key Integrity Protocol (TKIP) -- второй протокол, предусмотренный спецификацией WPA. TKIP предназначен для решения основных проблем WEP в области шифрования данных. Для совместимости с существующим аппаратным обеспечением TKIP использует тот же алгоритм шифрования, что и WEP -- RC4. TKIP подразумевает несколько способов повышения защищенности беспроводных сетей: динамические ключи, измененный метод генерации ключей, более надежный механизм проверки целостности сообщений, увеличенный по длине вектор инициализации, нумерация пакетов.

В отличие от WEP, где для контроля целостности передаваемых данных использовалась CRC-32, TKIP применяет так называемый Message Integrity Code (MIC), обеспечивающий криптографическую контрольную сумму от нескольких полей (адрес источника, адрес назначения и поля данных). Так как классические MIC-алгоритмы (например, HMAC-MD5 или HMAC-SHA1) для существующего беспроводного оборудования являлись очень "тяжелыми" и требовали больших вычислительных затрат, то специально для использования в беспроводных сетях Нильсом Фергюсоном (Niels Ferguson) был разработан алгоритм Michael. Для шифрования он применяет 64-битный ключ и выполняет действия над 32-битными блоками данных.. Для обеспечения целостности данных в протоколе TKIP, помимо механизма MIC, предусмотрена еще одна функция, отсутствовавшая в WEP, -- нумерация пакетов. В качестве номера используется TKIP Sequence Counter (TSC) и имеет длину 48 бит, в отличие от 24 бит в WEP.

Основным и самым важным отличием TKIP от WEP является механизм управления ключами, позволяющий периодически изменять ключи и производить обмен ими между всеми участниками сетевого взаимодействия: саппликантом, аутентификатором и сервером аутентификации. В процессе работы и аутентификации на разных этапах взаимодействия и для различных целей генерируются специализированные ключи.

Итак, наш узел доступа, состоящий из проводного и беспроводного сегментов, имеет в своём распоряжении сервер RADIUS, выполняющий функции 3А и беспроводные устройства, поддерживающие спецификацию

802.1x. Теперь рассмотрим алгоритм, по которому работает тандем RADIUS+WEP в беспроводной сети в соответствии со стандартом IEEE 802.1x.

Особенностью подобной системы является то, что пароли, ключи и другие закрытые данные никогда не передаются в открытой форме по беспроводным каналам. Это сильно ограничивает все попытки подслушивания и анализа передаваемого трафика в целях установления структуры сети, передаваемых паролей или получения другой закрытой информации. Для повышения стойкости шифрования трафика в системе применяются разовые WEP-ключи, уникальные как для конкретного пользователя, так и для каждой сессии его связи с сетью. Такой способ распределения ключей существенное затрудняет криптоанализ передаваемого трафика. Протокол EAP устанавливает последовательность действий которая показана на рисунке 2.1.

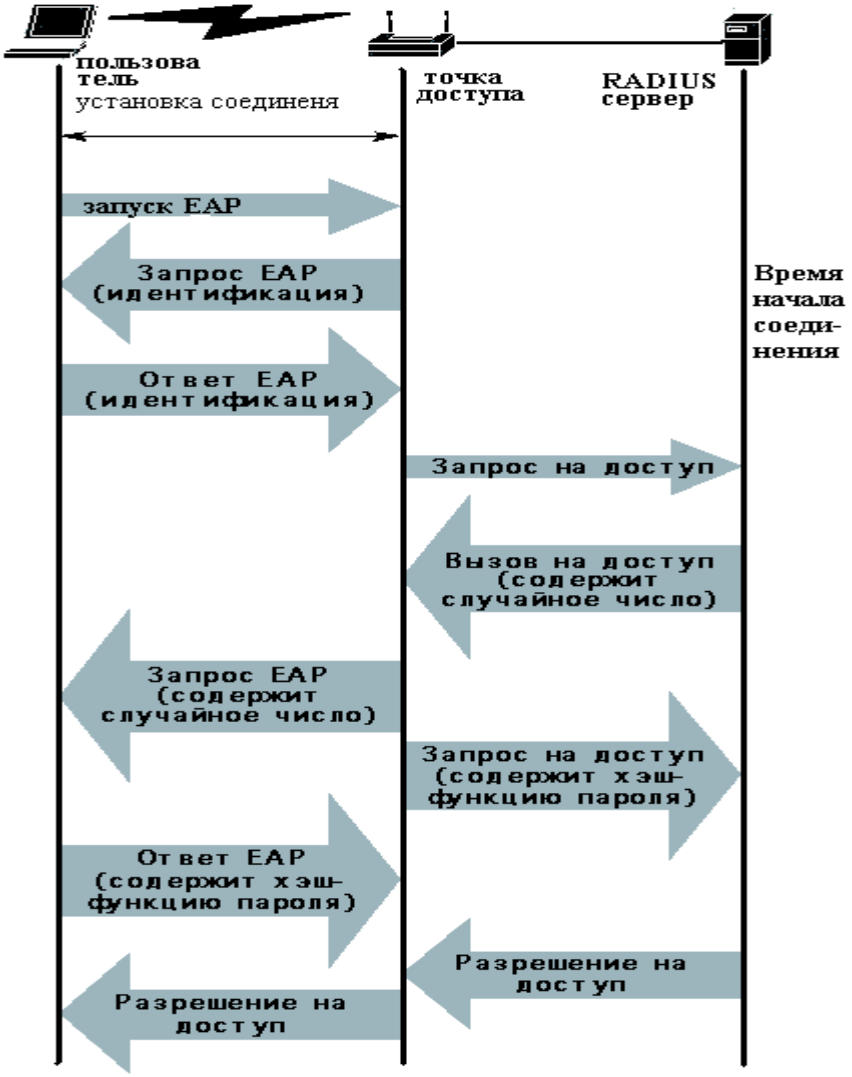


Рисунок 2.1 – Последовательность действий при проведении аутентификации и авторизации абонента сети по протоколу EAP

Итак, применение стандарта IEEE 802.1x в радиосетях позволяет добиться существенного повышения уровня безопасности радиосетей, что выражается в минимизации рисков, связанных с утратой и подделкой оборудования, с эмуляцией хакерами «фальшивого» узла для внедрения в сеть. Другими преимуществами (реализуемыми с помощью динамического алгоритма WEP) являются простота и легкость распределения ключей среди пользователей, повышение стойкости передаваемого трафика к криптоанализу. Использование сервера RADIUS дает возможность управления допуском всех клиентов к сетевым ресурсам из единого центра.

Очевидно, что после аутентификации абонента беспроводной сети ему будет необходимо присвоить соответствующую его категории политику безопасности. Одной из возможных реализаций подобного подхода является: использование технологии, определенной стандартом 802.1q и позволяющей поместить авторизованных абонентов беспроводной сети в различные VLAN.

2.4.3 VPN

Как было сказано выше, одной из базовых технологий защиты информации в беспроводных сетях является криптография. Оптимальное решение проблем безопасности видится в использовании технологии защищенных частных виртуальных сетей (VPN), которая наравне с протоколами 802.1x устраняет недостатки WEP.

Производители оборудования при построении беспроводных сетей с максимальным уровнем защищенности рекомендуют использовать VPN решения на базе семейства протоколов IPSec. Есть еще 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.

Несмотря на то, что сама по себе технология защищенных частных виртуальных сетей способна обеспечить жесткую авторизацию пользователя по его цифровому сертификату формата X.509, ее не следует рассматривать как альтернативу решениям на базе протокола 802.1x. Это взаимодополняющие решения. Поскольку средства VPN обеспечивают защиту на сетевом уровне, а использование решений на базе протокола 802.1x позволяет предотвратить несанкционированный доступ к беспроводной сети на более раннем этапе. Подобное решение позволяет построить многоэшелонированную защиту: авторизуя пользователей по протоколу 802.1x мы убеждаемся, что имеем дело с легальным пользователем нашей беспроводной сети, а реализуя дополнительную авторизацию средствами VPN мы убеждаемся, что допускаем к работе с конфиденциальными ресурсами пользователей, которые имеют на это право. Кроме этого, использование функций межсетевого экранирования на устройстве VPN-шлюз, позволит нам назначать различные права доступа

внутри группы пользователей, имеющих доступ к конфиденциальной информации, как это показано в таблице 2.1. Необходимо также заметить, что сам протокол 802.1x имеет ряд уязвимостей к атакам типа "man-in-the-middle" и "session hijacking".

Поэтому нелишним будет повторить: использование технологии VPN позволяет создать внешнюю защитную оболочку беспроводной сети передачи данных.

Таблица 2.1 – Разграничение доступа посредством использования VPN

Абоненты беспроводной сети	Доступ к конфиденциальной информации	Доступ к публичной информации (в т.ч. Internet)
Сотрудник	+	+
Гость	-	+
Злоумышленник	-	-

Как всегда, вопрос обеспечения требуемого уровня безопасности и вопрос удобства и простоты использования находятся на разных чашах весов. Посмотрим, что является "платой" в случае использования технологии VPN:

Снижение общей пропускной способности сети. В случае использования в протоколах семейства IPSec сертифицированных криптоядер, снижение производительности составит ориентировочно от 20 до 30%.

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

Варианты использования.

Можно выделить четыре основных варианта построения сети VPN, которые используются во всем мире:

1) Вариант "Intranet VPN", который позволяет объединить в единую защищенную сеть несколько распределенных филиалов одной организации, взаимодействующих по открытым каналам связи. Именно этот вариант получил широкое распространение во всем мире, и именно его в первую очередь реализуют компании-разработчики.

2) Вариант "Remote Access VPN", который позволяет реализовать защищенное взаимодействие между сегментом корпоративной сети (центральным офисом или филиалом) и одиночным пользователем, который подключается к корпоративным ресурсам из дома (домашний пользователь) или через notebook (мобильный пользователь). Данный вариант отличается от первого тем, что удаленный пользователь, как правило, не имеет

статического адреса, и он подключается к защищаемому ресурсу не через выделенное устройство VPN, а прямиком со своего собственного компьютера, на котором и устанавливается программное обеспечение, реализующее функции VPN.

3) Вариант "Client/Server VPN", который обеспечивает защиту передаваемых данных между двумя узлами (не сетями) корпоративной сети. Особенность данного варианта в том, что VPN строится между узлами, находящимися, как правило, в одном сегменте сети, например, между рабочей станцией и сервером. Такая необходимость очень часто возникает в тех случаях, когда в одной физической необходимо создать несколько логических сетей. Например, когда надо разделить трафик между финансовым департаментом и отделом кадров, обращающихся к серверам, находящимся в одном физическом сегменте. Этот вариант похож на технологию VLAN, которая действует на уровне выше канального.

4) Последний вариант "Extranet VPN" предназначен для тех сетей, к которым подключаются так называемые пользователи "со стороны", уровень доверия к которым намного ниже, чем к своим сотрудникам.

Последний случай как раз и является основным при построении узла доступа на основе беспроводной связи.

Оценка степени влияния

При работе виртуальных частных сетей криптошлюзы осуществляют преобразование трафика, при этом многие характеристики с точки зрения конечного пользователя меняются не лучшую сторону. Интеграция VPN вносит следующие изменения в работу сети:

- Снижение пропускной способности сети
- Накладные расходы на преобразование трафика
- Задержки при передаче пакетов

Рассмотрим подробнее эти параметры.

Снижение пропускной способности сети возникает по разным причинам. Первая заключается в недостаточной производительности самого криптошлюза, хотя, как правило, при выборе таких устройств этому параметру уделяется большое внимание. Устройства VPN должны обладать достаточной пропускной способностью для того, чтобы минимизировать свое влияние при передаче информации в сети.

Вторая причина определяется типом трафика и обусловлена накладными расходами на преобразование трафика. Они возникают при обработке пакета за счет добавления нового IP-заголовка к туннелируемому пакету. Эта величина зависит от протокола, используемого в системе, и составляет фиксированное количество байт. Дополнительная нагрузка на сеть определяется процентным приростом длины пакета по отношению к исходной. В этом и заключается причина снижения пропускной способности в зависимости от типа трафика.

Например, протокол IPSec добавляет (для алгоритма ГОСТ 28147-89) при преобразовании минимум 54 байта. Для IP-пакета длиной 1500 байт

(стандартный пакет передачи данных) прирост составит порядка 4%, а для 56 байтного пакета (IP-телефония) - накладные расходы составят уже около 100%.

На российском рынке некоторые компании представляют протоколы собственной разработки (например, протокол шифрования данных семейства криптомаршрутизаторов "Континент-К"). Как правило, они лишены многих недостатков IP-Sec, имеют меньшее увеличение длины пакета, нередко также используют режим сжатия полей данных и/или заголовка.

Задержки при передаче пакетов обусловлены многими причинами. Роль VPN здесь далеко не всегда является доминирующей, ведь задержки определяются работой узлов на различных уровнях - от физического до транспортного. При условии работы через Интернет основными местами возникновения задержек являются узлы доступа к Интернету и шлюзы между провайдерами.

Все задержки, возникающие при криптографической обработке трафика, можно разделить на три типа:

– задержки при установлении защищенного соединения между VPN-устройствами.

– задержки, связанные с зашифрованием и расшифрованием защищаемых данных, а также преобразованиями, необходимыми для контроля их целостности.

– задержки, связанные с добавлением нового заголовка к передаваемым пакетам.

Реализация первого, второго и четвертого вариантов построения VPN предусматривает установление защищенных соединений не между абонентами сети, а только между VPN-устройствами. С учетом криптографической стойкости используемых алгоритмов смена ключа возможна через достаточно длительный интервал времени. Поэтому задержки первого типа на скорость обмена данными при использовании средств построения VPN практически не влияют. Разумеется, этот тезис касается стойких алгоритмов шифрования, использующих ключи не менее 128 бит (Triple DES, ГОСТ 28147-89 и т.д.).

Задержки второго типа начинают играть роль только при передаче данных по высокоскоростным каналам (от 10 Мбит/сек). Во всех остальных случаях быстродействие программной или аппаратной реализации выбранных алгоритмов шифрования и контроля целостности обычно достаточно велико и в цепочке операций "зашифрование пакета - передача пакета в сеть" и "прием пакетов из сети - расшифрование пакета" время зашифрования (расшифрования) значительно меньше времени, необходимого для передачи данного пакета в сеть.

Ещё проблема связана с добавлением дополнительного заголовка к каждому пакету, пропускаемому через VPN-устройство. Для протокола IPSec дополнительный заголовок для алгоритма ГОСТ 28147-89 составит 54 байта.

Для уменьшения влияния этого фактора многие разработчики стараются укоротить длину заголовка.

Характерен пример с IP-телефонией. Передаваемые IP-пакеты имеют длину 56 байт (Стандарт H.323). Теперь представим себе, что в существующую сеть, изначально не рассчитанную на какое-либо вмешательство, мы пытаемся интегрировать VPN. Каждый пакет при преобразовании снабжается новым заголовком, при этом, например, для IPSec, как уже упоминалось, увеличение пакета составит более 100%. Решение данной проблемы возможно в двух направлениях. Вариант быстрый, но дорогой - увеличение пропускной способности канала. Он позволяет снять многие проблемы, но при построении беспроводной сети этот параметр жёстко закреплён выбранным нами протоколом из семейства 802.11. Например, в 802.11g максимум составляет 54 Мбит/с, а реальная скорость колеблется в диапазоне 22-40 Мбит/с. Однако есть другой вариант. Он заключается в использовании протоколов с минимальными накладными расходами на туннелирование. При этом остальные параметры устройств VPN должны соответствовать требованиям заказчика.

Существует несколько способов защиты беспроводной сети с помощью VPN. Обычно все беспроводные станции логически размещаются вне узла доступа, и каждая станция связывается через соединение PPTP и брандмауэр с VPN-сервером. VPN-сервер обеспечивает прохождение трафика между клиентами, которые имеют действующее VPN-соединение с узлом доступа. Клиенты не могут установить соединение до тех пор, пока беспроводная станция не будет успешно аутентифицирована на VPN-сервере (как правило, для этого необходимо ввести имя пользователя и пароль). После того как соединение установлено, все пересылаемые через соединение данные шифруются. Еще один распространенный вариант — использование IPSec для организации соединений каждой беспроводной станции с AP. В данной конфигурации для аутентификации обычно применяется секретная последовательность символов, а для генерации и обновления ключей шифрования — функции управления соединением.

К сожалению приходится отметить, что средства построения VPN не являются полноценными средствами обнаружения и блокирования атак. Они могут предотвратить ряд несанкционированных действий, но далеко не все возможности, которые могут использовать хакеры для проникновения в корпоративную сеть. Они не могут обнаружить вирусы и атаки типа "отказ в обслуживании" (это делают антивирусные системы и средства обнаружения атак), а как показывает практика, это самое уязвимое место беспроводных сетей, они не могут фильтровать данные по различным признакам (это делают межсетевые экраны) и т.д. На это можно возразить, что эти опасности не страшны, так как VPN не примет незашифрованный трафик и отвергнет его. Однако на практике это не так. Во-первых, в большинстве случае средство построения VPN используется для защиты лишь части трафика, например, направленного в удаленный филиал. Остальной трафик (например,

к публичным Web-серверам) проходит через VPN-устройство без обработки. А во-вторых, статистика утверждает, что до 80% всех инцидентов, связанных с информационной безопасностью, происходит по вине авторизованных пользователей, имеющих санкционированный доступ в корпоративную сеть. Из чего следует вывод, что атака или вирус будут зашифрованы наравне с безобидным трафиком.

Итак, основной вывод из всего вышесказанного: процесс построения любой из подсистем обеспечения безопасности информации достаточно сложный и трудоемкий, тем более в области беспроводных сетей. Причина тому - отсутствие устоявшихся стандартов в области безопасности, поддерживаемых всеми производителями. Но уже сейчас можно сказать, что технологии сегодняшнего дня позволяют построить беспроводную сеть, приближающуюся по уровню безопасности к обычным проводным сетям и полностью соответствующую требованиям руководящих документов. Выбор конкретной модели безопасности из вышеописанных должен делаться на основе большого числа факторов. При построении же узла доступа в Internet следует, по моему мнению, остановиться на варианте VPN + 802.1x как показано на рисунке 2.2. Где первое слагаемое обеспечивает надёжную защиту от внешних воздействий, второе – чёткую авторизацию допущенных пользователей. Тем более, что данная схема позволит с наименьшими затратами перейти в ближайшем будущем на работу по протоколу 802.11i.

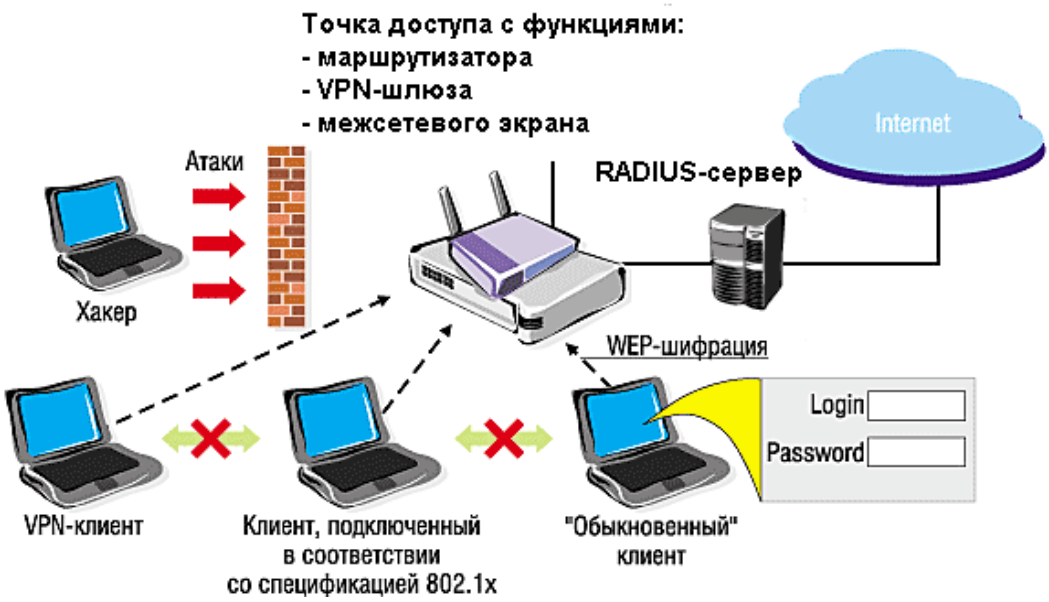


Рисунок 2.2

2.5 Расчет зоны Френеля

Радиоволна в процессе распространения в пространстве занимает объем в виде эллипсоида вращения с максимальным радиусом в середине пролета, который называют зоной Френеля. Естественные (земля, холмы, деревья) и искусственные (здания, столбы) преграды, попадающие в это

пространство, ослабляют сигнал. Радиус первой зоны Френеля в самой широкой части может быть рассчитан с помощью формулы (2.1):

$$R = \sqrt{\frac{c \cdot S \cdot D}{f \cdot (S + D)}} \qquad (2.1)$$

где R – радиус зоны Френеля (м);
S– расстояние от первой точки доступа до препятствия (м);
D – расстояние от второй точки доступа до препятствия (м);
c – скорость света (м/с);
f – частота (ГГц).

Расстояние от первой точки до стены 5 м.От второй до стены 15 м.

$$R = \sqrt{\frac{3 \cdot 10^8 \cdot 5 \cdot 15}{2.4 \cdot 10^9 \cdot (5 + 15)}} = 0.7 \text{ м.}$$

Замечания: обычно блокирование 20% зоны Френеля вносит незначительное затухание в канал. Свыше 40% затухание сигнала будет уже значительным, следует избегать попадания препятствий на пути распространения.

Этот расчет сделан в предположении, что земля плоская. Он не учитывает кривизну земной поверхности. Для протяженных каналов следует проводить совокупный расчет, учитывающий рельеф местности и естественные преграды на пути распространения. В случае больших расстояний между антеннами следует стараться увеличивать высоту подвеса антенн, принимая во внимание кривизну земной поверхности.

2.6 Расчет зоны действия сигнала

2.6.1 Расчет дальности работы беспроводного канала связи. Расчёт по графику

Эта методика позволяет определить теоретическую дальность работы беспроводного канала связи, построенного на оборудовании D-LINK стандартов 802.11 *b* и *g* (частота *2.4 ГГц*) и 802.11 *a* (частота 5 *ГГц*). Следует отметить, что расстояние между антеннами, получаемое по формуле – максимально достижимое теоретически, а так как на беспроводную связи влияет множество факторов, получить такую дальность работы, особенно в черте города, практически невозможно.

Для определения дальности связи необходимо рассчитать суммарное усиление тракта и по графику определить соответствующую этому значению дальность. Усиление тракта в дБ определяется по формуле (2.2):

$$Y_{дБ} = P_{t,дБ} + G_{t,дБ} + G_{r,дБ} - P_{\min,дБ} - L_{t,дБ} - L_{r,дБ} \qquad (2.2)$$

где $P_{t,дБ}$ – мощность передатчика;

$G_{t,дБ}$ – коэффициент усиления передающей антенны;

$G_{r,дБ}$ – коэффициент усиления приемной антенны;

$P_{\min,дБ}$ – реальная чувствительность приемника;

$L_{t,дБ}$ – потери сигнала в коаксиальном кабеле и разъемах передающего тракта;

$L_{r,дБ}$ – потери сигнала в коаксиальном кабеле и разъемах приемного тракта.

По графику, приведённому на рисунке 2.3, находим необходимую дальность работы беспроводного канала связи.

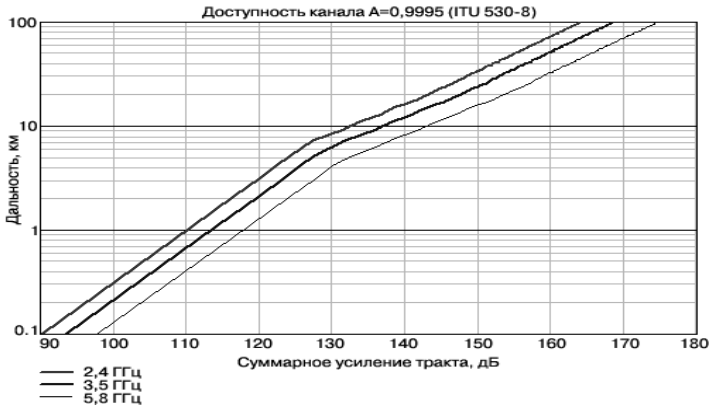


Рисунок 2.3 – Доступность канала

Разберем каждый параметр на примере:

– $P_{t,дБ}$ – мощность передатчика – мощность беспроводной точки доступа или адаптера в dBm. Эта информация берется в спецификации на оборудование. Для оборудования D-LINK DWL-8500AP это от 15 dBm. Для беспроводных адаптеров G550 это от 16 dBm;

– $G_{t,дБ}$ – коэффициент усиления передающей антенны (дБи). D-LINK предлагает антенны для внешнего и внутреннего использования от 2 до 10 дБи. (В нашем случае равен 5 Дби);

– $G_{r,дБ}$ – коэффициент усиления приемной антенны. Тоже что и $G_{t,дБ}$ но "на другой стороне" радиолинка;

– $P_{\min,дБ}$ – чувствительность приемника, которую также можно найти в спецификации на оборудование. Чувствительность приемника зависит от скорости, на котором работает оборудование и задается со знаком "минус";

– $L_{t,дБ}$, $L_{r,дБ}$ – потери в коаксиальном кабеле и разъемах приемного или передающего тракта. Рассчитать потери можно следующим образом: предлагаемый кабель BELDEN 9880 имеет затухание 0,24 дБ/м т.е. при 4-метровой длине кабеля затухание в нем составит 1.44 дБ. Также следует

прибавить к потерям по ~ 0,5 - 1,5 дБ на каждый разъем. Итого 6-метровый кабель между антенной и точкой доступа имеет потери $0{,}96 + 2 * 1{,}5 = 3{,}96$ дБ;

Поскольку расстояние между точками доступа одинаково, рассчитаем потери между двумя точками. Мы имеем две точки доступа DWL-8500AP. Оконечные точки находятся на одинаковом расстоянии от центральной, поэтому расчёт для каждой пары точек доступа будет одинаковым.

$P_{t,dB}$ = 15 dBm;

$G_{t,dB}$ = 5 дБи;

$G_{r,dB}$ = 5 дБи;

$P_{\min,dB}$ = -71 dBm;

$L_{t,dB}$ = 3,96 дБ;

$L_{r,dB}$ = 3,96 дБ;

Отсюда по формуле (2.2) найдём потери:

$$Y_{дБ} = 14+5+5-(-71)-3{,}96-3{,}96 = 88{,}08 \text{ дБ}.$$

По графику (для 2.4 GHz) определяем соответствующую этому значению дальность. Получаем дальность равную ~100 метрам.

Мы проводили расчет для скорости 54 Mbps.

При скорости 6 Mbps:

$P_{\min,дБ}$ = -87 dBm;

тогда:

$$Y_{дБ} = 15+5+5-(-87)-3{,}96-3{,}96 = 104{,}08 \text{ дБ}.$$

По графику для 2.4 GHz определяем соответствующую этому значению дальность. Получаем дальность равную ~500 метрам.

Рассчитаем суммарное усиление тракта для компьютеров находящихся в кабинетах. Кабинеты расположены симметрично относительно точки доступа подключаемой к серверу. Затухание вносимое офисной стеной примем равным 6 дб, тогда потери в каждом направлении

$$Y_{дБ} = P_{t,дБ} + G_{t,дБ} + G_{r,дБ} - P_{\min,дБ} - L_{t,дБ} - L_{r,дБ} - L_{стены,dB} \qquad (2.3)$$

где $P_{t,dB}$ = 16 дБмВт;

$G_{t,dB}$ = 5 дБи;

$G_{r,dB}$ = 5 дБи;

$P_{\min,dB}$ = -66 дБмВт;

$L_{t,dB}$ = 0 дБ;

$L_{r,dB}$ = 0 дБ;

$L_{стены,dB}$ = 6 дБ;

Отсюда по формуле (2.3) найдём потери:

$$Y_{дБ} = 16+5+5-(-66)-6=86 \text{ дБ}.$$

По графику для 2.4 GHz определяем соответствующую этому значению дальность. Получаем дальность равную ~90 метрам. Расчет для скорости 54 Mbps.

При скорости 6 Mbps:

$P_{\min,дБ}$ = -87 дБмВт;

тогда:

$$Y_{дБ} = 16+5+5-(-87)-6=107 \text{ дБ}.$$

По графику (для 2.4 GHz) определяем соответствующую этому значению дальность. Получаем дальность равную ~850 метрам.

2.6.2 Расчет по формуле

Без вывода приведём формулу для расчёта дальности. Она берётся из инженерной формулы (2.3) расчёта потерь в свободном пространстве:

$$FSL = 33 + 20(\lg F + \lg D) \qquad (2.4)$$

где FSL (free space loss) – потери в свободном пространстве (дБ);

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

D – расстояние между двумя точками (км).

FSL определяется суммарным усилением системы. Оно считается следующим образом:

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

Для каждой скорости приёмник имеет определённую чувствительность. Для небольших скоростей (например, 1-2 мегабита) чувствительность наивысшая: от –90 дБмВт до –94 дБмВт. Для высоких скоростей, чувствительность намного меньше. В качестве примера приведём несколько характеристик обычных точек доступа 802.11a,b,g:

6 Мбит/с: -90dBm

9 Мбит/с: -84dBm

12 Мбит/с: -82dBm

18 Мбит/с: -80dBm

24 Мбит/с: -77dBm

36 Мбит/с: -73dBm

48 Мбит/с: -72dBm

54 Мбит/с: -72dBm

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

SOM (System Operating Margin) – запас в энергетике радиосвязи (дБ). Учитывает возможные факторы отрицательно влияющие на дальность связи, такие как: температурный дрейф чувствительности приемника и выходной мощности передатчика; всевозможные погодные аномалии.

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

Центральная частота канала F берётся из таблицы 2.2.

Таблица 2.2 - Вычисление центральной частоты

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

В итоге получим формулу (2.5) дальность связи:

$$D = 10^{\left(\frac{FSL}{20} - \frac{33}{20}\lg F\right)} \tag{2.5}$$

D=0.042km=42 м.

Также написана программа на языке Delphi 7 для расчета зоны Френеля и дальности связи рисунок 2.4. Приложение А.

Рисунок 2.4 – Расчёт на Delphi 7

2.7 Анализ потерь сигнала в свободном пространстве

Для любого типа беспроводной связи передаваемый сигнал рассеивается по мере его распространения в пространстве. Следовательно, мощность сигнала, принимаемого антенной с постоянной эффективной площадью, будет уменьшаться по мере удаления от передающей антенны. Для спутниковой связи упомянутый эффект является основной причиной снижения интенсивности сигнала. Даже если предположить, что все прочие причины затухания и ослабления отсутствуют, переданный сигнал будет затухать по мере распространения в пространстве. Причина этого – распространение сигнала по всё большей площади. Данный тип затухания называют потерями в свободном пространстве и вычисляют через отношение мощности излучённого сигнала P_t к мощности полученного сигнала P_r. Для вычисления того же значения децибелах следует взять десятичный логарифм от указанного отношения, после чего умножить полученный результат на 10.

Для идеальной изотропной антенны потери в свободном пространстве составляют по формуле (2.6):

$$\frac{P_t}{P_r} = \frac{(4\pi d)^2}{\lambda^2} = \frac{(4\pi f^2 d)^2}{c^2} \tag{2.6}$$

где P_t – мощность сигнала передающей антенны;

P_r – мощность сигнала, поступающего на антенну приемника;

λ – длина волны несущей;

d – расстояние, пройденное сигналом между двумя антеннами;

c – скорость света ($\approx 3 \cdot 10^8$ м/с).

Приведённое выражение можно записать в следующем виде:

$$\begin{aligned} L_{дБ} &= 10\lg\frac{P_t}{P_r} = 20\lg\left(\frac{4\pi d}{\lambda}\right) = -20\lg(\lambda) + 20\lg(d) + 21{,}98\ дБ = \\ &= 20\lg\left(\frac{4\pi f d}{c}\right) = 20\lg(f) + 20\lg(d) - 147{,}56\ дБ \end{aligned} \tag{2.7}$$

На рисунке 2.5 приводится зависимость потерь сигнала в свободном пространстве от пройденного расстояния.

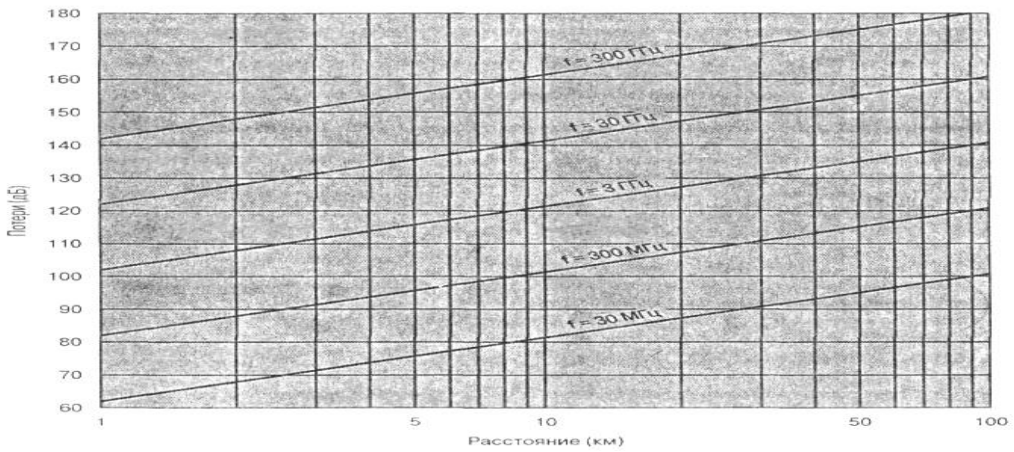


Рисунок 2.5 – Потери мощности сигнала

Функция зависимости затухания от расстояния между антеннами примет вид по формуле (2.8):

$$L_{дБ} = 20\lg\left(\frac{4\pi \cdot 24d}{3}\right) = 20\lg(32\pi d) \tag{2.8}$$

Полученные параметры расчётов занесём в таблицу 2.3:

Таблица 2.3 – Значения расстояния и потерь

D (м)	L (дБ)
20	66,06
90	79,13
160	84,12
230	87,28
300	89,58
370	91,41
440	92,91
510	94,19
580	95,31
650	96,30
720	97,19
790	97,99
860	98,73
930	99,41
1000	100,04

Изходя из полученных данных построим график зависимости представленный на рисунке 2.6.

Рисунок 2.6 – График зависимости потерь от расстояния

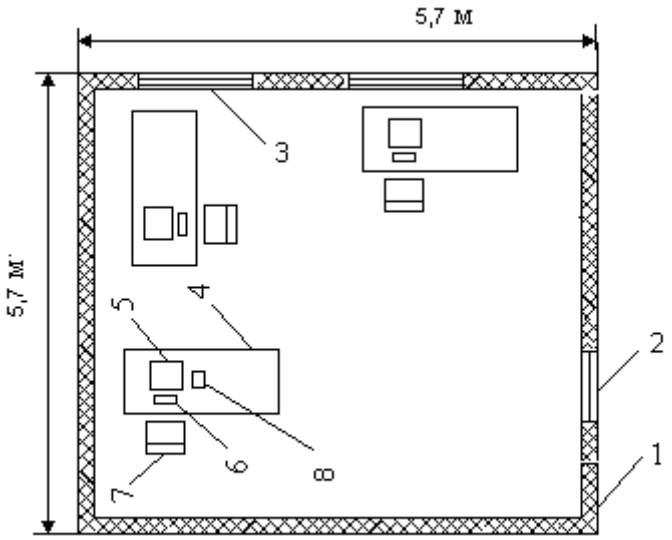
Используемые в данной работе антенны находятся на расстоянии 20 м друг от друга. На графике изображённом на рисунке 2.5 показана зависимость затухания от растояния между антеннами начиная с 1 км. Исходя из этого проведём исследование изменения затухания на расстояниях меньше 1 км, используя частоту несущей 2,4 ГГц.

3 Безопасность жизнедеятельности

3.1 Анализ условий труда

3.1.1 Характеристика помещения

Оборудование сервера исследуемой локальной сети размещается на четвёртом этаже четырёхэтажного здания. Высота этажей 3.2 м. Стены кабинета окрашены в белый цвет, и имеются большие окна и верхние люминисцентные лампы. Поэтому помещение производит светлое, легкое впечатление, не смотря на тот факт что окна выходят на северную сторону. Верхнее освещение работает даже днем, и чтобы снизить пагубность влияния на зрение двух разнотипных источника света, в кабинете имеются плотные жалюзи. План помещения и размещения оборудования представлен на рисунке 3.1.



Стена; дверной проем; окно деревянное двойное раздельное; компьютерный стол; компьютер; клавиатура; стул; точка доступа Wi-Fi

Рисунок 3.1 – План помещения и размещения оборудования

В помещении «серверной» помимо места системного администратора находится 5 учебных мест, таким образом, максимальное число находящихся в «серверной» человек равно 6.

Площадь комнаты контроля $S_{контр}$=5.7·5.7=32.49 м^2, объем - $V_{контр}$=32.49·3.2=103.97 м^3. На одного человека приходится площадь 32,49/6= 5,42 м^2 и объем 17,33 м^3. Это больше минимальных площади и объема приходящихся на одного работающего, установленных нормами (объем - не менее 15 м^3, площадь - не менее 4.5м^2).

3.1.2 Оценка микроклимата

Согласно, ГОСТ 12.1.005-88 работы, производимые системным администратором, относятся к категории I б лёгкой физической (таблица 3.1).

Аппаратура, установленная в «серверной» выделяет большое количество тепла. В результате в летнее время года помещение нуждается в выводе избыточного тепла. Для создания благоприятного микроклимата в помещениях установлены настенные кондиционеры, характеристики которых приведены в таблице 3.2. Они позволяют охлаждать воздух, автоматически поддерживать заданную температуру, изменять скорость движения воздушного потока и направлять его, обеспечивая воздухообмен с наружной средой [12].

Таблица 3.1 - Категории работ по энергозатратам организма

Работа	Категория	Энергозатраты организма, Дж/с	Характеристика работы
Легкая физическая	I б	138 – 172	Производится сидя, стоя или связана с ходьбой и сопровождается некоторым физическим напряжением

Таблица 3.2 - Характеристики установленных кондиционеров

Модель	Мощность охлаждения, кВт	Мощность нагрева, кВт	Мощность потребляемая, кВт	Расход воздуха, куб.м/час
SANYO SAP-K181GJHA	5	5.75	2.25/1.96	760

Оптимальные нормы параметров микроклимата в холодный и тёплый периоды года с учётом категории работы приведены в таблице 3.3. Регулирование параметров микроклимата производится автоматически по регулируемым характеристикам. Изменение контролируемых характеристик производится оператором.

Таблица 3.3 - Оптимальные нормы параметров микроклимата

Период работы	Температура, ^{0}С	Скорость движения воздуха, м/с, не более
Холодный	21-23	0.1
Теплый	22-24	0.2

В качестве нагревательных приборов в обоих помещениях установлены регистры из гладких труб. Имеющаяся система кондиционирования поддерживает температуру в пределах оптимальных норм параметров микроклимата. В помещения подается объем наружного воздуха до 100 куб.м

на одного рабочего. Скорость движения воздуха в помещениях в любой период года не превышает 0.1 м/с.

Поэтому микроклиматические условия обслуживания оборудования согласно ГОСТ 12.0.005-88 охарактеризованы как оптимальные.

3.1.3 Оценка освещенности

Работа системного администратора в основном заключается в управлении и наблюдении за аппаратурой и при необходимости устранении мелких неполадок в работе оборудования. Таким образом, выполняемую работу операторов относим к работе со средней точностью, т.е. к IV разряду зрительной работы [13].

Естественное освещение создается благодаря двум окнам размерами 170×240 см, окна начинаются с высоты один метр. В качестве светопропускающего материала имеем стекло оконное листовое двойное. В качестве солнцезащитного устройства используются убирающиеся регулируемые жалюзи.

Так как окна выходят на теневую сторону и из-за климатических условий, в помещениях принята система общего освещения четырьмя светильниками по четыре люминесцентные лампы II группы ЛД, мощностью 40 Вт и световым потоком $Ф_л$=2340 лм, уровень освещенности которых 150 лк.

Оптимальные параметры освещенности помещений приведены в таблице 3.4.

Для достижения уровня нормируемой освещенности - 300 лк, соответствующей IV разряду зрительной работы увеличивается количество источников света.

Таблица 3.4 – Оптимальные параметры освещенности помещений

Характе-ристика зрительной работы	Разряд	Контраст объекта с фоном	Характе-ристика фона	При комбини-рованном освещении, лк	При общем освещении, лк
Средней точности 0.5-1.0	IV	большой	светлый	300	300

3.1.4 Оценка пожарной безопасности

В помещении существует вероятность возникновения пожара, причина которых:

- неисправности электропроводки, розеток и выключателей которые приводят к короткому замыканию или пробою изоляции;
- использование поврежденных (неисправных) электроприборов;
- возникновение пожара вследствие попадания молнии в здание;
- возгорание здания вследствие внешних воздействий.

В помещении имеется огнетушитель ОП-10, предназначенный для тушения пожаров и загораний нефтепродуктов, ЛВЖ и ГЖ, растворителей, твердых веществ, а также электроустановок под напряжением до 1000 В [14].

Исходя из приведенного анализа, для помещения проводится реконструкция системы освещения и разрабатывается меры по профилактике пожара и план эвакуации людей.

Для исключения возникновения пожара по приведенным выше причинам:

- вовремя выявляются неисправности в электропроводке, проводится плановый осмотр и своевременно устраняются все неисправности;
- своевременно проводится качественный ремонт электроприборов, не используются неисправные электроприборы;
- на станции проводится противопожарный инструктаж, на котором работников знакомят с правилами противопожарной безопасности, а также обучают использованию первичных средств пожаротушения.

На четвёртом этаже здания одновременно находятся более 20 человек, поэтому разработаны и на видных местах вывешены планы (схемы) эвакуации людей в случае пожара, а также предусмотрена система (установка) оповещения людей о пожаре. План эвакуации приведен на рисунке 3.2.

Необходимое время эвакуации людей из производственных зданий (мин) приведено в таблице 3.5. Наше предприятие относится к категории В.

Таблица 3.5 – Необходимое время эвакуации людей из производственных зданий (мин)

Категория производства	Объем помещений, тыс.м^3				
	до 15	30	40	50	60 и более
А, Б, Е	0,50	0,75	1	1,5	1,75
В	1,25	2	2	2,5	3
Г, Д	не ограничивается				

3.2 Техническое решение по обеспечению безопасности жизнедеятельности

3.2.1 Расчет искусственного освещения

Расчет выполнен по методическим указаниям [15] и СНиП РК 2.04-05-2002 [16].

Расчет искусственного общего освещения выполняется по методу коэффициента использования светового потока. Разряд зрительной зоны работы определен IV-ой средней точности, поэтому будет экономична система общего освещения, при которой светильники располагаются в верхней зоне, обеспечивающей равномерную освещенность рабочего помещения высотой 3.2 м и площадью 37.1 м^2 для кабинета контроля и 39.7 м^2 для технического помещения.

На основании этих требований проведем расчет системы общего освещения рабочего места оператора. Расчет будем проводить по световому потоку, так имеется заданное значение освещенности документа 300 лк.

Нормируемая минимальная освещенность определяется по формуле (3.1):

$$E_{\min} = \frac{F_Л n \eta Z}{SK}, \qquad (3.1)$$

где $F_л$ - световой поток одной лампы;

n - число ламп в помещении;

η - коэффициент использования светового потока, т.е. доля светового потока всех ламп, падающая на освещаемую поверхность;

Z - коэффициент неравномерности освещения;

S - площадь поля освещаемого помещения;

K - коэффициент запаса, учитывающий снижение освещенности в процессе эксплуатации системы освещения (загрязнение светильников, старение ламп).

Коэффициент использования светового потока представляет собой отношение светового потока, достигающего освещаемой поверхности, к полному световому потоку в помещении. Зависит от коэффициентов отражения стен ρ_c и потолка ρ_n, показателя помещения, который вычисляется по формуле (3.2):

$$\varphi = \frac{AB}{H_p(A+B)}, \qquad (3.2)$$

где A - длина помещения;

B - ширина помещения;

H_p - высота подвеса светильников над рабочей поверхностью (условно рабочей поверхностью считается горизонтальная поверхность на высоте 0.8 м от пола). Люминесцентные светильники будут установлены на высоте 3 м от пола.

Так как нормируется минимальная освещенность рабочей поверхности, то при расчетах вводится коэффициент неравномерности освещения Z. Для люминесцентных ламп Z = 0.9 [5].

Задавшись числом ламп, из формулы (3.1) имеем:

$$F_л = \frac{E_{min} SK}{Z\eta}, \qquad (3.3)$$

Для этой категории работ при общем освещении наименьшая освещенность E_{min}=300 лк (люкс) [15].

Коэффициент пульсации освещенности не более 15%.

Коэффициент запаса K=1.5.

Коэффициент неравномерности освещения Z=0.9.

Определим необходимое число светильников при общей системе освещения для кабинета контроля.

Помещение имеет следующие размеры: длина A=5,7 м, ширина B=5,7 м.

Подвесной потолок оборудуем двухламповыми светильниками АОД с люминесцентными лампами естественной цветности с улученной цветопередачей ЛЕЦ 40. В таблице 3.4 приведены характеристики этой лампы.

Таблица 3.4 – Характеристики лампы ЛЕЦ 40

Тип, марка	Мощность, Вт	Световой поток, лм	Длина, мм не более	Диаметр, мм не более	Средняя продолжительность горения, час	Температура, К (цветовая)
ЛЕЦ 40	40	2200	1213.6	40	10000	3900

Коэффициенты отражения светового потока от стен и потолка соответственно равны: $p_{ст}$=50 %, $p_{пт}$=70 %.

Для помещения с ЭВМ уровень рабочей поверхности над полом равен 0.8 м. При этом H_p=2.8 (высота подвеса над рабочей поверхностью).

Площадь помещения: S=32,49 м^2.

Для светильников АОД с лампами ЛЕЦ 40 световой поток, создаваемый одной лампой $F_л$=2200 лм (люмен).

Определим сначала показатель помещения по формуле 3.2:

$$\varphi = \frac{5.7 \cdot 5.7}{2.8 \cdot (5.7 + 5.7)} = 2.29$$

Теперь для полученного показателя помещения, коэффициентов отражения потолка и стен находим по таблице [15] коэффициент использования светового потока η=0.63.

Из формулы 3.1 получаем формулу для вычисления необходимого числа светильников (по две лампы) в помещении:

$$n = \frac{300 \cdot 32.49 \cdot 1.5}{2 \cdot 2200 \cdot 0.63 \cdot 0.9} = 6$$

Рассчитаем систему освещения для данного помещения, по средней удельной мощности.

Определим мощность осветительной установки (3.4):

$$W = W_0 \cdot S, \tag{3.4}$$

$$W = 12 \cdot 32.49 = 389.88, \text{ Вт}$$

где W_0 = 11÷15 Вт/кв.м – средняя удельная мощность светильника.

Необходимое количество светильников с лампами выбранной мощности равно (3.5):

$$n = \frac{W}{2W_0}, \tag{3.5}$$

$$n = \frac{389.88}{2 \cdot 40} = 4.87 < 6$$

Определяем по формуле 3.1 $E_{расч}$:

$$E_{расч} = \frac{2 \cdot 2200 \cdot 6 \cdot 0.63 \cdot 0{,}9}{32.49 \cdot 1.5} = 307.15, \text{ лк} > E_{\min} = 300, \text{ лк}$$

Таким образом, для организации системы искусственного освещения нашего помещения устанавливаем шесть светильников типа АОД с лампами ЛЕЦ 40.

Разделив *n* на число рядов, определяем число светильников устанавливаемых в каждом ряду. Поскольку длина светильника известна, то нужно найти длину всех светильников ряда.

Если эта длина близка к геометрической длине ряда, он получается сплошным; если меньше длины ряда, то светильники размещаются с разрывами; если больше длины ряда, то увеличивается число рядов.

Светильники устанавливаем в два ряда.

Число светильников в каждом ряду: $N_p = n/2 = 3$.

Длина светильника АОД=1.3 м, длина одного ряда 3·1.3=3,9 м.

Расстояние между рядами светильников определим по формуле (3.6):

$$L = \lambda \cdot h, \tag{3.6}$$

где λ - коэффициент неравномерности, равный 1.3;

h - высота подвеса.

$$L = 1.3 \cdot 2.8 = 3.64, \text{ м}$$

План размещения светильников в кабинете контроля показан на рисунке 3.3.

Светильники установим в два ряда.

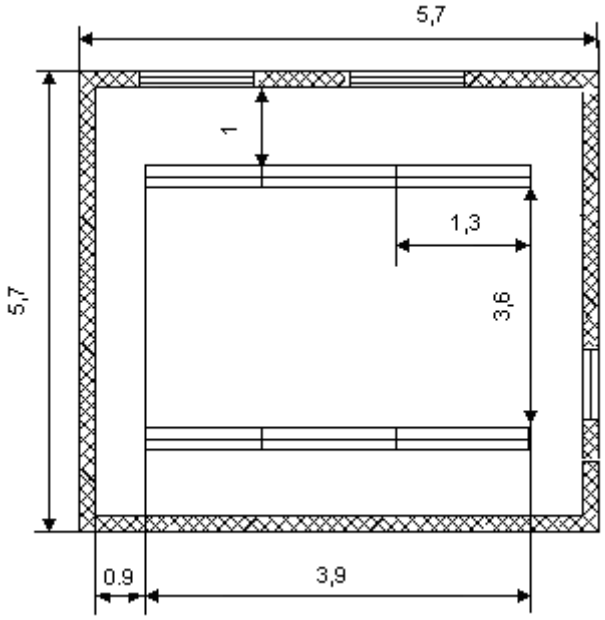


Рисунок 3.3 – План расположения светильников в кабинете контроля и техническом помещении после реконструкции

3.2.2 Расчет автоматического пожаротушения

Расчет выполнен по справочным указаниям [14] и СНиП РК 2.02-05-2001 [19].

В качестве огнетушащего вещества применяется комбинированный углекислотно-хладоновый состав. Расчетная масса комбинированного углекислотно-хладонового состава m_d кг, для объемного пожаротушения определяется по формуле (3.7):

$$m_d = k \cdot g_n \cdot V \,, \tag{3.7}$$

где k = l,2 - коэффициент компенсации не учитываемых потерь углекислотно-хладонового состава;

g_n = 0,4 – нормативная массовая концентрация углекислотно - хладонового состава;

V – объем помещения;

$$V = A \cdot B \cdot H \,, \tag{3.8}$$

где А = 5,7 м – длина помещения,

В = 5,7 м – ширина помещения,

Н = 3,2 м – высота помещения.

$$V = 5.7 \cdot 5.7 \cdot 3.2 = 103.97 \text{ , м}^3$$

$$m_d = 1.2 \cdot 0.4 \cdot 103.97 = 50 \text{ кг}$$

При наличии постоянно открытых проемов, площадь которых составляет от 1% до 10% площади ограждающих конструкций помещений, следует принять дополнительный расход 5 кг на 1м^2 углекислотно-хладонового состава, равный 5 кг на 1 м^2 площади проемов.

Расчетное число баллонов ξ определяется из расчета вместимости в 20-литровый баллон 12,5 кг углекислотно-хладонового состава.

Внутренний диаметр магистрального трубопровода d_i мм, определяется по формуле:

$$d_i = 12 \cdot \sqrt{2} = 17, \text{ мм}$$

Эквивалентная длинна магистрального трубопровода l_2 м, определяется по формуле (3.9):

$$l_2 = k_1 \cdot l, \tag{3.9}$$

где k_1=1,2 - коэффициент увеличения длины трубопровода для компенсации не учитывающих местных потерь;

l=5,7 м – длина трубопровода по проекту.

$$l_2 = 1.2 \cdot 5.7 = 6.8, \text{ м.}$$

Площадь сечения выходного отверстия оросителя A_3 мм^2, определяется по формуле (3.10):

$$A_3 = \frac{S}{\xi_1}, \tag{3.10}$$

где S – площадь сечения магистрального трубопровода, мм^2;

ξ_1 – число оросителей.

$$A_3 = \frac{3.14 \cdot 8.5^2}{5} = 45.4$$

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

Расчетное время подачи углекислотно-хладонового состава t мин, определяется по формуле (3.11):

$$t = \frac{m_d}{60Q}, \qquad (3.11)$$

$$t = \frac{50}{60 \cdot 1.4} = 0.6$$

Масса основного запаса углекислотно-хладонового состава m кг, определяется по формуле (3.12):

$$m = 1.1 \cdot m_d \cdot \left(1 + \frac{k_2}{k}\right), \qquad (3.12)$$

где $к_2$=0,2 – коэффициент учитывающий остаток углекислотно-хладонового состава в баллонах и трубопроводах тогда,

$$m = 1.1 \cdot 50 \cdot \left(1 + \frac{0.2}{1.2}\right) = 64.2 \text{, кг}$$

Таким образом, из полученных результатов для обеспечения нормального функционирования системы автоматического пожаротушения потребуется 5 баллонов углекислотно-хладонового состава вместимостью 20 литров, с массой смеси 12,5 кг и рабочим давлением 12,5 МПа. В помещении установлено 5 оросителей, продолжительность выпуска заряда составляет 0,5 с.

Расстояние между двухструйными насадками не более 4-х метров, а от насадок до стен не более 2-х метров.

4 Технико-экономическое обоснование проекта

4.1 Преимущества беспроводной сети по технологии Wi-Fi

В данном проекте рассматривается проектирование беспроводной сети на базе технологии Wi-Fi.

Беспроводные локальные сети все больше становятся популярными среди пользователей. В течение нескольких лет они проходили процесс стандартизации, повышалась скорость передачи данных, цена становилась доступнее.

Сегодня беспроводные сети позволяют предоставить подключение пользователей там, где затруднено кабельное подключение или необходима полная мобильность. При этом беспроводные сети взаимодействуют с проводными сетями. В настоящее время необходимо принимать во внимание беспроводные решения при проектировании любых сетей - от малого офиса до предприятия. Это, возможно, сэкономит и средства и трудозатраты и время.

Постоянно расширяющийся спектр оборудования, усовершенствование стандартов и улучшение защиты делает возможным применение Wi-Fi практически в любом месте. Новейшее оборудование соответствует высочайшим требованиям безопасности, устойчивости и высокой скорости.

Беспроводные сети позволяют предоставить подключение пользователей там, где затруднено кабельное подключение или необходима полная мобильность. При этом беспроводные сети взаимодействуют с проводными сетями. В настоящее время необходимо принимать во внимание беспроводные решения при проектировании любых сетей - от малого офиса до предприятия. Это, возможно, сэкономит и средства и трудозатраты и время.

Преимущества Wi-Fi:

– отсутствие проводов. Передача данных в сети осуществляется по воздуху на очень высокой частоте, которая не воздействует на человека и не создает помехи для электронной техники;

– мобильность. Так как беспроводная сеть не привязана к проводам, Вы можете свободно изменять местоположение Ваших компьютеров в зоне покрытия точки доступа, не беспокоясь о нарушениях связи. Сеть легко монтируется и демонтируется, при переезде в другое помещение Вы можете даже забрать свою сеть с собой;

– уникальность технологии. Возможна установка в местах, где прокладка проводной сети по тем или иным причинам невозможна или нецелесообразна, например, на выставках, залах для совещаний;

4.2 Организационный план

Организационный план является неотъемлемой частью бизнес-плана.

В данной выпускной работе будет произведен расчет затрат на покупку, доставку, установку и запуск оборудования беспроводной сети на

базе технологии Wi-Fi, производства компании D-Link. Оборудование этой компании очень хорошо зарекомендовали себя на рынке информационных технологий своей надежностью, функциональностью и гибкостью систем.

Сегодня компании могут предложить оборудование для построения сети Wi-Fi стандарта IEEE 802.11a/b/g:

1) программное обеспечение (Operations Support System (OSS)):Программное обеспечение сервера заведует всеми функциям: конфигурацией, авторизацией. Сервер OSS удаленно управляет всеми сессиями пользователей для публичного доступа в пределах сети рекламного агентства;

2) коммутатор:Для агрегирования трафика в проекте используется коммутатор 2-го уровня. В качестве такого устройства выбрано оборудование DWS-3526-24-SMI-PoE;

3) точка доступа (Access Point):В качестве точки доступа используется оборудование D-Link DWL-8500 AP Wireless Access Point 802.11b/g, работающее в диапазоне 2,4 до 2,4835 ГГц соответствующее рекомендациям IEEE 802.11b и g (Wi-Fi). Радиус покрытия одной точки доступа составляет до 500 метров вне помещения и может масштабироваться за счет установки дополнительных точек доступа;

4) беспроводные Wi-Fi адаптеры: В качестве беспроводных Wi-Fi адаптеров будут использоваться устройство D-Link DWL-G550 Wireless Adapter 802.11g, а также встроенные беспроводные адаптеры в ноутбуках сотрудниках фирмы [15].

4.3 Производственный план

4.3.1 Затраты на оборудование

Для осуществления данного проекта необходимо будет установить 3 точки доступа в здании.

Общая стоимость оборудования необходимого для построения сети составляет 285000 тенге.

Таблица 4.1 - Наименование и стоимость оборудования

Наименование оборудования	Кол-во, шт	Цена за единицу, тенге	Стоимость, тенге
Программное обеспечение Operations Support System	1	25000	25000
Точка доступа D-Link DWL-8500 AP	3	31000	93000
Беспроводной адаптер D-Link DWL-G550	10	5600	56000
Коммутатор DES-3526-24-ports	2	47000	94000
Кабель UTP Cat.5E	1	13000	13000

катушка 305 м			
Розетка RJ-45 DIN двойная UTP Cat.5E	10	400	4000
Итого			285000

4.3.2 Капитальные затраты

Капитальные затраты определим по формуле:

$$K = Ц + K_M + K_У, \quad (4.1)$$

где Ц – цена оборудования сети; $К_М$ – стоимость рабочих мест в год;

$К_У$ – стоимость монтажа и установки оборудования (5% от стоимости оборудования)

Анализ капитальных затрат:

Стоимость оборудования сети составит: Ц = 285000 тенге;

Таблица 4.2 – Расчет затрат на организацию рабочего места

Наименование	Цена за единицу, тенге	Кол-во, шт.	Стоимость, тенге
Компьютер (системный блок, монитор)	50000	2	100000
Компьютерный стол	9 500	2	19000
Стул	2 500	2	5000
Шкаф	12 000	1	12 000
Итого:			136000

Общая стоимость организации рабочего места: 136000 тенге. Из них 100000 было потрачено на приобретение компьютеров.

Таблица 4.3 – Капитальные затраты

Наименование затрат	Стоимость, тенге	Удельный вес, %
Стоимость оборудования, (Ц)	285000	66,31
Стоимость рабочих мест, (Км)	136000	30,58
Установка и монтаж оборудования, (Ку)	14250	3,11
Итого	435250	100,00

Рассчитаем капитальные затраты по формуле (4.1):

К = 285000 + 136000 + 14250 = 435250 тенге.

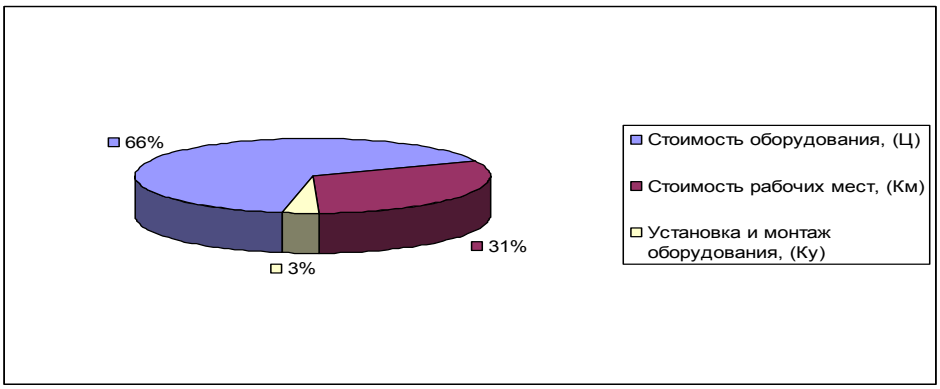


Рисунок 4.1 – Структура капитальных затрат

Капитальные затраты для организации сети составляют 435250 тенге. Большая часть которых была потрачена на приобретение оборудования и составила 66% от общей суммы. 31% ушло на организацию рабочего места и 3 % затрачено на установку и монтаж оборудования.

4.4 Финансовый план построения сети

Финансовый план является частью бизнес-плана, который включает в себя расчет доходов, эксплуатационных расходов, прибыли, рентабельности и срока окупаемости.

Целью данной разработки является получение максимальной прибыли, при минимальных издержках и высоком качестве предоставляемых услуг, с учетом того, что бы цена была приемлемой для пользователей.

Далее представлены расчеты, показывающие стоимость внедрения, экономическую эффективность использования и срок окупаемости.

4.4.1 Расчет годовых эксплуатационных расходов

Эксплуатационные расходы определим по формуле:

$$Э = ЗП + С_Н + А + М + С_{ЭЛ} + С_{АДМ} \quad (4.2)$$

где ЗП - основная и дополнительная заработная плата персонала с отчислением на социальное страхование, пенсионный фонд;

А - амортизационные отчисления;

М - затраты на материалы и запасные части;

$С_{ЭЛ}$ - электроэнергия со стороны производственных нужд;

$С_{АДМ}$ - прочие административные управленческие и эксплуатационные расходы.

Для вычисления заработной платы в таблице 4.4 приведем среднемесячные оклады обслуживающего персонала.

Таблица 4.4 – Среднемесячные оклады обслуживающего персонала

Список персонала	Количество	Ежемесячная з.пл, тенге	З.пл в год, тенге	Всего, тенге
Инженер-программист	1	65 000	842 640	780000
Сетевой администратор	1	60 000	780 360	720000
Итого				1 500 000

В годовой фонд заработной платы включается дополнительная заработная плата (работа в праздничные дни, сверхурочные и т.д.) в размере 30% от основной заработной платы.

Дополнительная заработная плата рассчитывается по формуле:

$$ЗП_{ДОП} = ЗП_{ОСН} * 0,3 \quad (4.3)$$

где $ЗП_{ОСН}$ - годовой фонд основной заработной платы

Подставив значения в (4.3) найдем годовой фонд дополнительной заработной платы

$$ЗП_{ДОП} = 1500000*0,3 = 450000 \text{ тенге.}$$

При расчете фонда заработной платы следует учесть премии для выплаты рабочим (15%):

$$П = ЗП_{ОСН}*0,15 \quad (4.4)$$

$$П = 1500000*0,15 = 225000 \text{ тенге}$$

Фонд оплаты труда складывается из основной, дополнительной заработной платы, а также с учетом премий:

$$ФОТ = ЗП_{ОСН} + ЗП_{ДОП} + П \quad (4.5)$$

Определим фонд оплаты труда по формуле (4.5)

$$ФОТ = 1500000 + 450000 + 225000 = 2175000 \text{ тенге.}$$

Отчисления на социальный налог:

$$Сн = 0,11\ (ФОТ - 0,1 \cdot ФОТ) \quad (4.6)$$

$$Сн = 0,11 \cdot (2175000 - 0,1 \cdot 2175000) = 215325 \text{ тенге.}$$

Суммарная заработная плата с учетом отчислений на социальный налог:

$$ЗП = ФОТ + Сн = 2175000 + 215325 = 2390325 \text{ тенге.}$$

Сумма амортизационных отчислений начисляется по единым нормам, которые устанавливаются в процентах от стоимости основных фондов:

$$A_0 = \frac{ф \cdot H_A}{100\%} \qquad (4.7)$$

где Ф – балансовая стоимость основных фондов, тенге;

$Н_А$ – норма амортизационных отчислений.

Найдем амортизационные отчисления для оборудования, компьютеров и офисной мебели из (4.7).

Для оборудования построения сети амортизация составляет 25% от цены оборудования:

$$А_1 = 285000*0,25= 71250 \text{ тенге.}$$

Амортизация компьютеров составляет 40% от цены:

$$А_2 = 100000*0,4 = 40000 \text{ тенге.}$$

Амортизация офисной мебели составляет 15% от цены:

$$А_3 = 40000*0,15 = 6000 \text{ тенге.}$$

$$А = А_1 + А_2 + А_3 = 71250+ 40000 + 6000 = 117250 \text{ тенге.}$$

Затраты на электроэнергию рассчитаем по следующей формуле:

$$С_{ЭЛ.} = W*T*S \qquad (4.8)$$

где W- потребляемая мощность W = 1750 Вт;

T - количество часов работы T = 8760 ч/год;

S - стоимость киловатт-часа электроэнергии S = 18,86 тенге / квт-час.

Рассчитаем затраты на электроэнергию по (4.8):

$$С_{ЭЛ} = 1,75*8760*18,86 = 289124 \text{ тенге.}$$

Мощность, потребляемая на прочие нужды, берется в размере 5% от мощности, потребляемой основным оборудованием. Стоимость электроэнергии, потребляемой на прочие нужды:

$$С_{ЭЛ.пр} = С_{эл}*0,05 \quad (4.9)$$

$$С_{ЭЛ.пр} = 289124*0,05 = 14456 \text{ тенге.}$$

Общие затраты на электроэнергию:

$$С_{эл.общ} = С_{эл} + С_{ЭЛ.пр} \quad (4.10)$$

$$С_{эл.общ} = 289124 + 14456 = 303580 \text{ тенге.}$$

Затраты на материалы и запасные части принимают в размере 5% от стоимости системы:

$$М = 285000*0,05 = 14250 \text{ тенге.}$$

Стоимость административных расходов составляет 10% от ФОТ:

$$С_{АДМ} = ФОТ*10\% \quad (4.12)$$

$$С_{АДМ} = 2175000*0,1 = 217500 \text{ тенге.}$$

Таким образом, эксплуатационные расходы исходя из (4.2) составят:

$$Э = 2390325 + 117250 + 303580 + 14250 + 217500= 3042950 \text{ тенге.}$$

Сведем данные по эксплуатационным расходам в таблицу 4.5 и определим удельный вес каждой статьи расходов.

Таблица 4.5 – Эксплуатационные расходы

Статьи эксплуатационных затрат	Стоимость, тенге	Удельный вес, %
Заработная плата персонала	2390325	78,55
Амортизационные отчисления	117250	3,85
Затраты на материалы и запасные части	14250	0,47
Затраты на электроэнергию	303580	9,98
Административные расходы	217500	7,15
Итого:	3042	100,00

На рисунке 4.2 приведена структура эксплуатационных расходов.

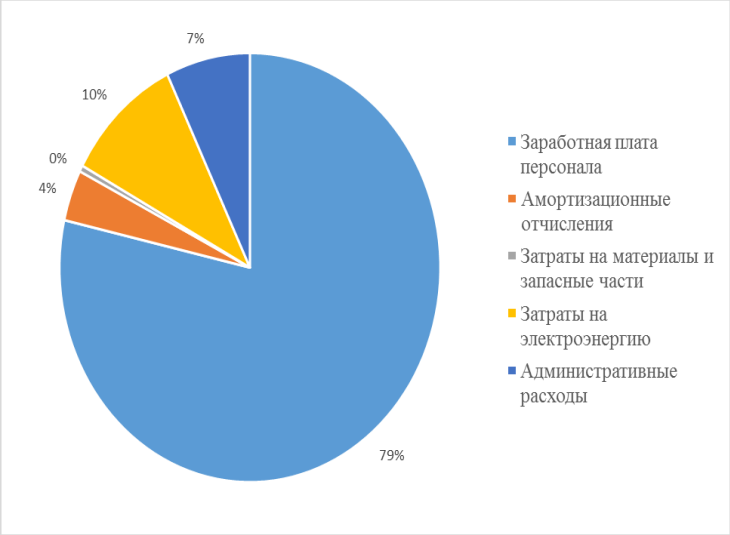


Рисунок 4.2 – Структура эксплуатационных затрат

Таким образом, годовые эксплуатационные расходы составили 3042905 тенге львиная доля, которых была затрачена на заработную плату персоналу и составила 78,55 %. Это связанно с тем, что на данную работу требуются высококвалифицированные специалисты. И во избежание перехода их в конкурирующую фирму мы вынуждены платить им высокую заработную плату. 7,15% - административные расходы. Амортизационные отчисления составили 3,85%. Это связанно с тем, что у нас низкая себестоимость оборудования. 9,98% ушло на затраты на электроэнергию. И совсем малая часть затрат была затрачена на материалы и запасные части [16].

4.4.2 Расчет доходов от внедрения технологии беспроводного доступа Wi-Fi

Внедрения мобильных ПК в рамках предприятия проводилось с целью повышения производительности и сокращения всех видов расходов, включая расходы на развертывание. Однако в процессе реализации этой программы оказалось, что достигается высокая окупаемость вложений компании. Теперь для выполнения тех же задач сотрудникам требуется времени меньше на 2-4 часов в неделю. Это связанно с минимизацией передачи данных между различными отделами предприятия, а также мгновенный отклик заказчика и отдела по работе с клиентами.

По данным на конец прошлого года, производство сократило время сдачи заказов на 110 часов в год (1 год - 2000 часов), что привело к выполнению дополнительных проектов, заказов и соответствующим доходам. Дополнительные часы принесли доход в размере Д =6676000 тенге.

4.4.3 Прибыль и срок окупаемости

Прибыль предприятия - это доходы предприятия от основной деятельности за вычетом эксплуатационных расходов. Прибыль предприятия облагается корпоративным налогом, который в Казахстане составляет 20%.

Прибыль предприятия до налогообложения.

Доход от основной деятельности определим по формуле:

$$ЧД = Д – Э \quad (4.13)$$

где Д - годовой доход от продажи карт оплаты,

Э – эксплуатационные расходы.

$$ЧД = 6676000 – 3042950 = 3633050 \text{ тенге.}$$

Чистый доход остающийся в распоряжении предприятия – это прибыль после налогообложения.

Сумма, отчисляемая на подоходный налог с прибыли составит:

$$Н = ЧД *20\% \quad (4.14)$$

$$Н = 3633050*0,2 = 726610 \text{ тенге.}$$

Сумма прибыли после налогообложения составит:

$$П = ЧД – Н \quad (4.15)$$

где Н – корпоративный налог в размере 20% от суммы чистого дохода

$$П = 3633050 – 726610= 2906640 \text{ тенге.}$$

Рентабельность проекта составит:

$$P = \frac{П}{Э} \cdot 100\% \quad (4.16)$$

$$P = \frac{2906640}{3042905} \cdot 100\% = 95,5\ \%$$

Срок окупаемости – это величина, показывающая, за какой период времени произойдет возврат денежных средств (капитальных вложений), затраченных на организацию предприятий. Срок окупаемости определим как отношение капитальных затрат к чистой прибыли предприятия, [17].

$$T = \frac{K}{П} \quad (4.19)$$

$$T = \frac{435250}{2906640} = 0,15 \text{ года} = 2 \text{ месяца.}$$

Все экономические показатели по проекту создания сети на базе технологии Wi-Fi сведем в таблицу 4.6.

Таблица 4.6 – Показатели экономической эффективности проекта

	Показатели	Сумма, тенге
1	Капитальные затраты	435250
2	Доход	6676000
3	Эксплуатационные расходы	3042905
4	Прибыль до налогообложения	3633050
5	Прибыль после налогообложения	2906640
6	Срок окупаемости, год	0,15
7	Рентабельность, %	95,5%

Вывод:

Согласно расчётам мы получаем, что рентабельность данного проекта составляет 95,5 %. То есть проект считается рентабельным.

Таким образом, средства, вложенные проектирование беспроводной сети на базе технологии Wi-Fi, компания вернет вложенные средства за 2 месяца.

В ходе проведенной работы нами было выявлено, что для организации локальной сети на базе технологии Wi-Fi в магазине нужно будет вложить капитальные затраты в размере 435250 тенге. При этом эксплуатационные расходы составят 3042905 тенге. Следовательно, средства, вложенные в проектировку беспроводной сети на базе технологии Wi-Fi, окупятся за 2 месяца.

Заключение

Локальные беспроводные сети все больше и больше приобретают популярность среди пользователей. В течение нескольких лет они проходили процесс стандартизации, повышалась скорость передачи данных, появлялись новые методы защиты, цена на оборудование становилась доступнее. В настоящее время беспроводные решения принимаются во внимание при проектировании любых сетей - от малого офиса до предприятия. Это, зачастую, экономит и средства, и трудозатраты, и время.

Потребность в беспроводном доступе к локальным сетям растёт по мере увеличения числа мобильных устройств, таких как ноутбуки и PDA, а так же с ростом желания пользователей быть подключенными к сети без необходимости использования сетевого провода в своем компьютере.

В данной работе проводилось исследование информационной безопасности беспроводных сетей. Было найдено конкретное решение проблемы безопасности беспроводных сетей на базе технологии WI-FI, выбрано конкретное оборудование для построения сети и приведены его параметры и характеристики. Рассмотренные вопросы представляют большой практический интерес.

На сегодняшний день разработка и внедрение локальных вычислительных сетей является одной из самых интересных и важных задач в области информационных технологий. Все больше возрастает стоимость информации и зависимость предприятий от оперативной и достоверной информации. Также актуальность рассмотренной проблемы объясняется резким увеличением количества пользователей с мобильными устройствами, так как им требуется быстрый, высокоскоростной и безопасный доступ к ресурсам уже построенных проводных локальных сетей или доступ в Интернет.

Список литературы

1 Щербаков А.К. «Wi-Fi :Все, что вы хотели знать, но боялись спросить» Москва «Бук-Пресс» 2005 г. – 151 с.

2 Сюваткин В.С., Есипенко В.И. WiMAX – технология беспроводной связи: теоретические основы, стандарты, применение. Санкт – Петербург: БХВ – Петербург, 2005. – 356с.

3 Шахнович И. Современные технологии беспроводной связи. Москва. Техносфера 2006 г. – 245 с.

4 http://www.dlink.ru/

5 http://www.wifialliance.org/

6 http://www.thg.ru/

7 Рошан П., Лиэри Дж. Основы построения беспроводных локальных сетей стандарта 802.11. – Москва*Санкт-Петербург*Киев, 2004. – 190с.

8 http://www.intuit.ru/

9 Безопасность жизнедеятельности: Учебник/Под ред. С.В.Белов. – М: Высшая школа, 1999.

10 Н.И. Баклашов, Н.Ж. Китаева, Б.Д. Терехов. Охрана труда на предприятиях связи и охрана окружающей среды: Учебник для вузов – М.: Радио и связь, 1989. – 288 с.

11 Кошулько Л.П., Суляева Н.Г., Генбач А.А. Производственное освещение. Методические указания к выполнению раздела "Охрана труда" в дипломном проекте, (для студентов энергетических специальностей всех форм обучения) – Алма-ата, изд. РУМК, 1989. – 40 с

12 СНиП РК 2.02-05-2002 Естественное и искусственное освещения. Комитет по делам строительства министерства индустрии и торговли республики Казахстан-Астана,2002.

13 Хакимжанов Т.Е. Безопасность жизнедеятельности. Расчёт аспирационных систем. Методическое указания к выполнению раздела в дипломном проекте. Алматы,2002.

14 СНиП РК 4.02-42-2006 Отопление, вентиляция и кондиционирование. Комитет по делам строительства министерства индустрии и торговли республики Казахстан-Астана,2006.

15 Голубицкая Е.А., Жигульская Г.М. - Экономика связи: Учебник для вузов.- М.: Радио и связь, 2000.- 392с.

16 Буров В.П., Новиков О.К. Бизнес-план: методика составления. – М.: ЦИПКК, 1995.

17 Экономика предприятия / Под ред. О.С. Срапионова, В.Н. М.: Радио и связь, 1998.-195с;

Приложение А
Листинг программы расчёта на Delphi 7

```
unit Unit1;
interface
uses
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls, Forms,
  Dialogs, ExtCtrls, StdCtrls;
type
  TForm1 = class(TForm)
    Label1: TLabel;
    Label2: TLabel;
    Label3: TLabel;
    Label4: TLabel;
    Label5: TLabel;
    Label6: TLabel;
    Edit1: TEdit;
    Edit2: TEdit;
    Edit3: TEdit;
    Edit4: TEdit;
    Edit5: TEdit;
    Edit6: TEdit;
    Label7: TLabel;
    Button1: TButton;
    Image1: TImage;
    Edit7: TEdit;
    Button2: TButton;
    Edit8: TEdit;
    Edit9: TEdit;
    Label8: TLabel;
    Label9: TLabel;
    Label10: TLabel;
    Edit10: TEdit;
    Edit11: TEdit;
    Button3: TButton;
    Edit12: TEdit;
    Edit13: TEdit;
    Label11: TLabel;
    Image2: TImage;
    Label12: TLabel;
    Label13: TLabel;
    Label14: TLabel;
    Label15: TLabel;
    Label16: TLabel;
```

```
    Label17: TLabel;
    Label18: TLabel;
    Label19: TLabel;
    Label20: TLabel;
    Label21: TLabel;
    Label22: TLabel;
    Label23: TLabel;
    Label24: TLabel;
    Label25: TLabel;
    Label26: TLabel;
    Label27: TLabel;
    Label28: TLabel;
    Label29: TLabel;
    procedure Button1Click(Sender: TObject);
    procedure Button2Click(Sender: TObject);
    procedure Button3Click(Sender: TObject);
  private
    { Private declarations }
  public
    { Public declarations }
  end;
var
  Form1: TForm1;
  p,pmin,gpr,gper:integer;
  Y,D,lpr,lper,fsl,S,D1,f1,R,F:real;
  a:real;
implementation
{$R *.dfm}
procedure TForm1.Button1Click(Sender: TObject);
begin
F:= strtoint (edit9.text);
p:= strtoint(edit1.Text);
gpr:= strtoint(edit2.Text);
gper:= strtoint(edit3.Text);
pmin:= strtoint(edit4.Text);
lpr:= strtofloat(edit5.text);
lper:= strtofloat(edit6.Text);
Y:=p+gpr+gper-lpr-lper-pmin;
edit7.Text:=floattostr(Y);
fsl:=Y-15;
D:=exp(((fsl-33)/20-ln(F)/ln(10))*ln(10));
edit8.Text:=floattostr(D);
```

```
end;
procedure TForm1.Button2Click(Sender: TObject);
begin
halt;
end;
procedure TForm1.Button3Click(Sender: TObject);
begin
S:= strtofloat (edit10.Text);
D1:= strtofloat (edit11.Text);
f1:= strtoint (edit12.text);
a:=S*D1/(S+D1);
R:=17.3*sqrt(a/f1);
edit13.text:=floattostr(R);
end.
```