Аннотация

Целью данного проекта является проектирование сети беспроводного радиодоступа стандарта WLAN (IEEE 802.11) для передачи голосовых данных на территории НПУ ОАО «Связьтранснефть».

В проекте рассматривается сравнительный анализ стандартов беспроводной связи 802.11. Тестирование сети для передачи голосовых потоков, настройки качества обслуживания сети.

В проекте производится выбор месторасположения точек доступа, рассчитываются уровни затухания сигнала, количество оборудования и зоны радиопокрытия сети и полоса пропускания для речевой информации.

В конструкторской части приведены результаты тестирования беспроводной сети для голосовых потоков, зоны радиопокрытия зданий, структурная схема модернизированной сети, измерены уровни сигнала в разных точках здания в виде графиков и таблиц.

Производится расчет экономической эффективности внедрения беспроводной сети. По результатам анализа опасных и вредных факторов при эксплуатации беспроводного оборудования сети делается вывод о том, что проектируемое сеть отвечает нормам безопасности действующих нормативных документов РФ. Расчет уровня электромагнитного поля в рабочей зоне показывает, что никаких организационных и технических мероприятий по его снижению не требуется.

Содержание

Введение………........…………………………........………………...........…...........9

1. Обзор технологий…..........................................………….............................…..11
   1. Методы и технологии модуляции сигнала...............…............................12
   2. Режимы и особенности организации ……………………….…………14
      1. Независимая конфигурация (Ad-Hoc)………………….….……. ..14
      2. Инфраструктурная конфигурация ………………………...………14
   3. Стандарты IEEE 802.11...….…….............…………………………...........16
   4. Архитектура IEEE 802.11……....…...........................................…........…..18
   5. Безопасность беспроводных сетей..................……………………………19
      1. Протокол безопасности WEP…………………………….…………20
      2. Протокол безопасности WPA………………………………………22
      3. Идентификатор точки доступа и МАС-фильтрация………………23
   6. Основы передачи голосовых данных по IP сетям………………………25

1.6.1 Особенности пакетного преобразования голоса………………….25

1.6.2 Системы традиционной и пакетной телефонии…………..………..27

1.6.3 Аппаратные и программные IP-телефоны………………………….28

### 1.6.4 Требования к качеству обслуживания для голоса………………….29

* 1. Выбор оборудования……………………………………………………..31
     1. Коммутатор Cisco Catalyst 2960……………………………………..33
     2. Cisco Aironet 1300 Series Outdoor Access Point/Bridge……………33
     3. Точка доступа Cisco Aironet 1200……………………………………34
     4. Маршрутизатор Cisco 2801 Security Bundle………………………35
     5. Cisco Access Point 1121-G-A-K9……………………..…….……….37
     6. IP Phone 7920……………………………………………….………..41

1. Техническое предложение………………………..………........….........………42
2. Расчетная часть.………………….....………..........…..…………….………….47
   1. Расчёт радиопокрытия…………………........………………..….........….47
      1. Расположение оборудования…………………………………………47
      2. Методика расчета…………………………………………..…..…...50
      3. Расчет зоны радиопокрытия 1-го здания ………………….…….. 53
      4. Расчет зоны радиопокрытия 2-го здания………………………….58
         1. Расчёт точек доступа 1 этажа………………………………..58

3.1.4.2. Расчёт точек доступа 2 этажа………………………………….61

3.1.4.3. Расчёт затухания на 3 этаже…………………………………..64

3.1.4.4. Результаты расчета ……………………………………………67

* 1. Расчет полосы пропускания для речевой информации………….……..67

1. Конструкторско-технологическая часть…………………………….………71
   1. Тестирование производительности сети для VoIP……………….……..71
      1. Методика тестирования………………………………………..……71
      2. Анализ воздействия установки приоритета на VoIP трафик……74
2. Технико-экономическое обоснование проекта…………….…………………76
   1. Расчет капитальных вложений………………………………………….….77
   2. Текущие расходы…………………………………………………………...78
      1. Расчёт заработной платы………………………………………...…...79
      2. Расчет амортизационных отчислений..…………………………..…79
      3. Расчет затрат на оплату электроэнергии…………………………....80
      4. Расчет затрат на уплату налога на имущество……………………...81
   3. Расчет показателей экономической эффективности ……………….…….81
3. Безопасность и экологичность проекта………..………………………….…..84
   1. Идентификация и анализ опасных и вредных факторов…………………85

6.1.1. Повышенное значение напряжения ……………………………….85

6.1.2. Повышенный уровень электромагнитного излучения ……………86

6.1.3. Опасность воздействия статических зарядов на человека……….87

### 6.1.4. Недостаточная освещенность рабочей зоны………………………88

6.1.5. Повышенный уровень шума, создаваемый вспомогательным оборудованием участка сети…………………………………………………….89

6.1.6. Опасность возникновения пожара …………………………………90

6.2. Инженерное обеспечение безопасных условий труда……………..90

6.2.1. Защита от повышенного напряжения ………………………………90

6.2.2. Защита от электромагнитного излучения………………………….91

6.2.3. Мероприятия по обеспечению необходимых параметров освещения в помещениях …………………………………………………………………….91

6.2.4. Мероприятия по защите от производственного шума……………92

6.3 Расчет воздействия электромагнитного излучения на посетителей и сотрудников……………………………………………………………………….94

Заключение………………………………………………………….................……98

Список использованных источников.………………………….....….........…........99

Приложение А……………………………………………………………………101

Приложение Б…………………………………………………………………….102

Приложение В……………………………………………………………………104

Введение

В этом дипломном проекте рассматривается построение беспроводной локальной сети связи стандарта WLAN 802.11 на территории НПУ ОАО «Связьтранснефть». Производится ряд инженерных технических расчетов, анализ различного телекоммуникационного оборудования и выбор оптимальных проектных решений.

Задачами проекта являются:

1. Связать большое количество стационарных и портативных компьютеров, для облегчения работы персонала офиса;
2. Повышение надежности сети путем резервирования и замены старого оборудования;
3. Обеспечить всем пользователям этой локальной сети высокоскоростной доступ в мировую сеть Internet;
4. Реализовать передачу голосовых данных по сетям IP;
5. Настроить качество обслуживания сети для передачи голосового трафика.

В последние годы беспроводные локальные сети заняли существенную нишу на рынке локальных сетей. Все больше и больше организаций считают, что беспроводные сети являются необходимым дополнением традиционных проводных локальных сетей, удовлетворяющим требованиям мобильности, возможности передислокации, организации эпизодических сетей и охвата мест труднодоступных при использовании проводных методов.

Благодаря функции роуминга между точками доступа пользователи могут

перемещаться по территории покрытия сети Wi-Fi без разрыва соединения.

WLAN(Wireless Local Area Network)-сети имеют ряд преимуществ перед обычными кабельными сетями:

− WLAN-сеть можно очень быстро развернуть, что очень удобно при проведении презентаций или в условиях работы вне офиса;

− пользователи мобильных устройств, при подключении к локальным беспроводным сетям, могут легко перемещаться в рамках действующих зон сети;

− скорости современных сетей довольно высоки (до 108 Мб/с), что позволяет их использовать для решения очень широкого спектра задач;

− WLAN-сеть может оказаться единственным выходом, если невозможна прокладка кабеля для обычной сети.

В моём проекте компьютеры (как стационарные, так и мобильные) установлены в различных комнатах офиса и их количество очень высоко, поэтому необходимо расширить сеть. Так же учитывается возможность работы с ноутбуком на всей территории предприятия.

После анализа технологий и оборудования предлагаемого для создания беспроводных сетей WLAN, мной был выбран стандарт 802.11g. Он позволяет соединять два и несколько компьютеров (как мобильных, так и стационарных), со скоростью 54 Mбит/c, на частоте 2,4 ГГц, имеет совместимость с устройствами стандарта 802.11b и обеспечивает высокий уровень безопасности.

# Обзор технологий

Под аббревиатурой Wi-Fi (от английского словосочетания Wireless Fidelity, которое можно дословно перевести как «высокая точность беспроводной передачи данных») в настоящее время развивается целое семейство стандартов передачи цифровых потоков данных по радиоканалам.

С увеличением числа мобильных пользователей возникает острая необходимость в оперативном осуществлении коммуникаций между ними, в обмене данными, в быстром получении информации. Поэтому естественным образом происходит интенсивное развитие технологий беспроводных коммуникаций, рынок которых на данный момент развивается быстрыми темпами. Особенно это актуально в отношении беспроводных сетей. Или так называемых WLAN-сетей (Wireless Local Area Network). Сети Wireless LAN – это беспроводные сети (вместо обычных проводов в них используются радиоволны). Установка таких сетей рекомендуется там, где развертывание кабельной системы невозможно или экономически нецелесообразно.

Беспроводные сети особенно целесообразны на предприятиях, где сотрудники активно перемещаются по территории во время рабочего дня с целью обслуживания клиентов или сбора информации (крупные склады, агентства, офисы продаж, учреждения здравоохранения и др.).

Благодаря функции роуминга между точками доступа пользователи могут

перемещаться по территории покрытия сети Wi-Fi без разрыва соединения.

WLAN-сети имеют ряд преимуществ перед обычными кабельными сетями:

* WLAN-сеть можно очень быстро развернуть, что очень удобно при проведении презентаций или в условиях работы вне офиса;
* пользователи мобильных устройств, при подключении к локальным беспроводным сетям, могут легко перемещаться в рамках действующих зон сети;
* скорости современных сетей довольно высоки (до 108 Мб/с), что позволяет их использовать для решения очень широкого спектра задач;
* WLAN-сеть может оказаться единственным выходом, если невозможна прокладка кабеля для обычной сети.

Вместе с тем необходимо помнить об ограничениях беспроводных сетей. Это, как правило, всё-таки меньшая скорость, подверженность влиянию помех и более сложная схема обеспечения безопасности передаваемой информации.

Сегмент Wi-Fi сети может использоваться как самостоятельная сеть, либо в составе более сложной сети, содержащей как беспроводные, так и обычные проводные сегменты.

Wi-Fi сеть может использоваться:

* для беспроводного подключения пользователей к сети;
* для объединения пространственно разнесенных подсетей в одну общую сеть там, где кабельное соединение подсетей невозможно или нежелательно;
* для подключения к сетям провайдера интернет-услуги вместо использования выделенной проводной линии или обычного модемного соединения.

**1.1.Методы и технологии модуляции сигнала**

Одна из основных проблем построения беспроводных систем – это решение задачи доступа многих пользователей к ограниченному ресурсу среды передачи. Существует несколько базовых методов доступа, основанных на разделении между станциями таких параметров, как пространство, время, частота и код. Каждый новый стандарт использует новые, более быстрые и надежные спецификации для физического уровня:

* DSSS (Direct Sequence Spread Spectrum, расширение спектра прямой последовательностью) — определяет работу устройств в диапазоне радиочастот по радиоканалам с широкополосной модуляцией с прямым расширением спектра методами прямой псевдослучайной последовательности;
* FHSS (Frequency Hopping Spread Spectrum, расширение спектра за счет скачкообразного изменения частоты) — определяет работу устройств в диапазоне радиочастот по радиоканалам с широкополосной модуляцией со скачкообразной перестройкой частоты псевдослучайными методами;
* OFDM (Orthogonal Frequency Division Multiplexing, ортогональное мультиплексирование с разделением частот) — определяет работу устройств в диапазоне радиочастот по радиоканалам с использованием подканалов с разными несущими частотами;
* РВСС (Packet Binary Convolutional Coding, двоичное пакетное свёрточное

кодирование) — метод двоичного пакетного свёрточного кодирования;

технология кодирования Баркера — описывает способ кодирования данныхс помощью последовательностей Баркера;

* ССК (Complementary Code Keying, кодирование с помощью комплементарных кодов) — описывает способ дополнительного кодирования битов передаваемой информации;
* CCK-OFDM — описывает способ кодирования данных с помощью гибридного метода, что позволяет увеличить скорость передачи сигнала при невысокой избыточности данных;
* QAM (Quadrature Amplitude Modulation, квадратурная амплитудная модуляция) — описывает способ квадратурной амплитудной модуляции сигнала, который работает на скорости выше 48 Мбит/с.

Метод ортогонального частотного мультиплексирования (OFDM) является одним из «продвинутых» и скоростных методов передачи данных. В отличие от методов DSSS и FHSS, с его помощью можно параллельно передавать данные по нескольким частотам радиодиапазона. При этом информация разбиваются на части, что позволяет не только увеличить скорость, но и улучшить качество передачи. Данный метод модуляции сигнала может работать в двух диапазонах — 2,4 и 5 ГГц.

**1.2. Архитектура беспроводных сетей**

На сегодняшний день используется два варианта беспроводной архитектуры или, проще говоря, варианта построения сети: *независимая* конфигурация (Ad-Hoc) и *инфраструктурная* конфигурация. Отличия между ними незначительные, однако, они кардинально влияют на такие показатели, как количество подключаемых пользователей, радиус сети, помехоустойчивость и т. д.

**1.2.1 Независимая конфигурация (Ad-Hoc)**

Режим независимой конфигурации (IBSS — Independent Basic Service Set, независимый базовый набор служб), который часто называют «точка-точка», — самый простой в применении. Соответственно, самым простым является построение и настройка сети с использованием независимой конфигурации.

Чтобы объединить компьютеры в беспроводную сеть, достаточно оборудовать каждый компьютер адаптером беспроводной связи. Как правило, такими адаптеры изначально комплектуются переносные компьютеры, что сводит построение сети к настройке соответствующих ресурсов и ограничений.

Пример такой конфигурации приведен на Рисунке 1.1.



Рисунок 1.1 - Режим независимой конфигурации

**1.2.2 Инфраструктурная конфигурация**

Инфраструктурная конфигурация, или, как ее еще часто называют, «режим клиент/сервер», — более перспективный и быстроразвивающийся вариант беспроводной сети. Инфраструктурная конфигурация имеет много преимуществ, среди которых возможность подключения достаточно большого количества пользователей, хорошая помехоустойчивость, высокий уровень контроля подключений и многое другое. Кроме того, имеется возможность использования комбинированной топологии и проводных сегментов сети.

Помимо того, что на компьютерах должны быть установлены адаптеры беспроводной связи, для организации беспроводной сети с использованием инфраструктурной конфигурации необходимо иметь как минимум одну точку доступа (Access Point).

В этом случае конфигурация называется базовым набором служб (BSS — Basic Service Set). Точка доступа может работать автономно или в составе проводной сети и может выполнять функцию моста между проводным и беспроводным сегментами сети. При такой конфигурации сети компьютеры «общаются» только с точкой доступа, которая управляет передачей данных между компьютерами, пример такой конфигурации приведен на Рисунке 1.2.



Рисунок 1.2 - Инфраструктурный режим BSS

Конечно, одной точкой доступа сеть может не ограничиваться, что и случается по мере роста сети. В этом случае базовые наборы служб образуют единую сеть, конфигурация которой носит название расширенного набора служб (ESS — Extended Service Set). При такой конфигурации сети точки доступа обмениваются между собой информацией, передаваемой с помощью проводного соединения или с помощью радиомостов. Это позволяет эффективно организовывать трафик между сегментами сети (фактически — точками доступа), структура соединения приведена на Рисунке 1.3.



Рисунок 1.3 - Инфраструктурный режим ЕSS

**1.3 Стандарты IEEE 802.11**

На сегодняшний день существуют несколько разновидностей стандарта IEEE 802.11, которые предписывают использование определенных методов и скоростей передачи данных, методов модуляции, мощности передатчиков, полос частот, на которых они работают, методов аутентификации, шифрования и многое другое.

Существуют следующее группы стандартов:

* IEEE 802.11 a, IEEE 802.11 b и IEEE 802.11 g описывают работу сетевого оборудования (физический уровень);
* IEEE 802.11d , IEEE 802.11е, IEEE 802.11i, IEEE 802.11J, IEEE 802.11h и IEEE 802.11 r — параметры среды, частоты радиоканала, средства безопасности, способы передачи мультимедийных данных и т. д.;
* IEEE 802.11 f и IEEE 802.11 c — принцип взаимодействия точек доступа между собой, работу радиомостов и т. п.

### 1.3.3. IEEE 802.11g

Проект стандарта IEEE 802.11g был утвержден в октябре 2002 г. Этот стандарт предусматривает использование диапазона частот 2,4 ГГц, обеспечивая скорость передачи 54 Мбит/с и превосходя, таким образом, ныне действующий стандарт 802.11b. Кроме того, он гарантирует обратную совместимость со стандартом 802.11b. Обратная совместимость стандарта IEEE 802.11g может быть реализована в режиме модуляции DSSS, и тогда скорость передачи будет ограничена одиннадцатью мегабитами в секунду либо в режиме модуляции OFDM, при котором скорость составляет 54 Мбит/с.

При разработке стандарта 802.11g рассматривались несколько конкурирующих технологий: метод ортогонального частотного разделения OFDM и метод двоичного пакетного сверточного кодирования PBCC.

В протоколе 802.11g предусмотрена передача на скоростях 1, 2, 5,5, 6, 9, 11, 12, 18, 22, 24, 33, 36, 48 и 54 Мбит/с. Некоторые из данных скоростей являются обязательными, а некоторые – опциональными. Кроме того, одна и та же скорость может реализовываться при различной технологии кодирования. Ну и как уже отмечалось, протокол 802.11g включает в себя как подмножество протоколы 802.11 b.

Технология кодирования PBCC опционально может использоваться на скоростях 5,5; 11; 22 и 33 Мбит/с. Вообще же в самом стандарте обязательными являются скорости передачи 1; 2; 5,5; 6; 11; 12 и 24 Мбит/с, а более высокие скорости передачи (33, 36, 48 и 54 Мбит/с) — опциональными.

Отметим, что для обязательных скоростей в стандарте 802.11g используется только кодирование CCK и OFDM, а гибридное кодирование и кодирование PBCC является опциональным.

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

Таким образом, данный стандарт является наиболее приемлемым при построении беспроводных сетей.

**1.4 Архитектура IEEE 802.11**

Институт инженеров по электротехнике и электронике IEEE (Institute of Electrical and Electronics Engineers) сформировал рабочую группу по стандартам для беспроводных локальных сетей 802.11 в 1990 году. Эта группа занялась разработкой всеобщего стандарта для радиооборудования и сетей, работающих на частоте 2.4 ГГц со скоростями доступа 1 и 2 Мбит/с. Работы по созданию стандарта были завершены через 7 лет и в июне 1997 года была ратифицирована первая спецификация 802.11.

Естественно, что стек протоколов стандарта IEEE 802.11 соответствует обшей структуре стандартов комитета 802. то есть состоит из физического уровня и канального уровня с подуровнями управления доступом к среде MAC (Media Access Control) и логической передачи данных LLC (Logical Link Control). Как и у всех технологий семейства 802. технология [802.11](http://S02.ll) определяется нижними двумя уровнями, то есть физическим уровнем и уровнем MAC, а уровень LLC выполняет свои стандартные общие  
для всех технологий LAN функции ,как показано на Рисунке 1.4.



Рисунок 1.4 - Структура стандарта 802.11

На физическом уровне существует несколько вариантов спецификаций, которые отличаются используемым частотным диапазоном, методом кодирования и как следствие — скоростью передачи данных. Все варианты физического уровня работают с одним и тем же алгоритмом уровня MAC, но некоторые временные параметры уровня MAC зависят от используемого физического уровня.

В сетях 802.11 уровень MAC обеспечивает два режима доступа к разделяемой среде:

* распределенный режим DCF (Distributed Coordination Function);
* централизованный режим PCF (Point Coordination Function).

**1.5 Безопасность беспроводных сетей**

Беспроводные сети используют радиоволны, которые распространяются по законам физики и принципу действия передающих антенн в зоне радиуса сети. Контролировать поведение радиоволн практически невозможно. Это означает, что любой человек, у которого есть компьютер или переносное устройство с радиоинтерфейсом, может подключиться к сети, находясь в радиусе ее действия. Вычислить местоположение этого пользователя практически невозможно, поскольку он может быть как рядом, так и на значительном удалении от сети (при использовании антенны с усилителем).

Именно тот факт, что подключиться к беспроводной сети может любой, требует серьезного отношения к обеспечению достаточного уровня безопасности. Чтобы обеспечить минимальный уровень безопасности в беспроводной сети, необходимо использовать следующие механизмы:

* механизм аутентификации рабочей станции — позволяет определить, кто подключается к беспроводной сети и имеет ли он право на такое подключение;
* механизм защиты информации посредством ее шифрования с помощью специальных алгоритмов.

Если хотя бы один из описанных механизмов не используется, то можно сказать, что сеть является абсолютно незащищенной. Это незамедлительно приведет к негативным последствиям. Как минимум, злоумышленник увеличит трафик сети (Интернет, файловые ресурсы), а при наиболее неблагоприятных условиях сможет навредить другой сети, которая подключена к выбранной беспроводной сети.

На сегодняшний день стандартами предусмотрено использование нескольких механизмов безопасности, позволяющих в той или иной мере защитить беспроводную сеть.

**1.5.1 Протокол безопасности WEP**

Протокол безопасности *WEP* (Wired Equivalent Privacy, секретность, эквивалентная секретности проводной сети) — первый протокол безопасности, описанный стандартом IEEE 802.11. Для шифрования данных этот протокол использует ключ с разрядностью от 40 до 104 бит. Кроме того, он дополнительно использует шифрование, основанное на алгоритме кодирования RC4 — алгоритм обеспечения целостности данных. Что касается шифрования для обеспечения целостности данных, то шифрованием его можно назвать с натяжкой, поскольку для этого процесса используется статическая последовательность длиной 32 бита, которая присоединяется к каждому

пакету данных, увеличивая при этом его и без того объемную служебную часть.

Отдельно стоит упомянуть о процессе аутентификации, поскольку без него защиту передаваемой информации нельзя считать минимально достаточной. Изначально стандарт IEEE 802.11 описывает два варианта аутентификации: аутентификация для открытых систем с открытым ключом и аутентификация с общим ключом.

**Аутентификация с открытым ключом**

Фактически этот метод аутентификации не предусматривает никаких средств безопасности соединения и передачи данных. Выглядит это следующим образом. Когда двум компьютерам нужно установить связь, отправитель посылает получателю специально сформированный пакет данных, называемый кадром аутентификации. В свою очередь адресат, получив такой пакет, понимает, что требуется аутентификация с открытыми ключами и в ответ отправляет аналогичный кадр. На самом деле эти кадры аутентификации, естественно, отличаются друг от друга и по сути содержат только информацию об отправителе и получателе информации.

**Аутентификация с общим ключом**

Данный уровень аутентификации подразумевает использование общего ключа секретности, которым владеют только отправитель и получатель информации. В этом случае процесс аутентификации выглядит следующим образом. Чтобы начать передачу данных, отправителю необходимо «договориться» с получателем. Для этого он посылает кадр аутентификации, содержащий информацию о себе и тип ключа шифрования. Получив кадр аутентификации, адресат в ответ посылает пробный текст, зашифрованный с помощью указанного ключа (используется 128-битный ключ алгоритма шифрования WEP). Получив пробный зашифрованный текст, отправитель пытается его декодировать с помощью договоренного ключа шифрования. Если изначальный текст совпадает с результатом расшифровки (используются контрольные суммы зашифрованного и расшифрованного сообщений),

то отправитель посылает получателю сообщение об успехе аутентификации.

Только после этого данные передаются с использованием указанного ключа

шифрования. Кажется, все выглядит достаточно просто и эффективно. На самом же деле практическое использование метода шифрования WEP показало, что алгоритм кодирования имеет явные прорехи в механизме безопасности, которые нельзя скрыть даже с помощью длинного ключа шифрования.

Благодаря сторонним тестировщикам и хакерам оказалось, что, проанализировав достаточно большой объем трафика сети (3-7 млн пакетов), можно вычислить ключ шифрования. В таком случае не спасет даже 104-битный ключ шифрования. Остается только радоваться тому факту, что развитие компьютерных технологий и стандартов не стоит на месте

и на смену старым технологиям приходят новые. Конечно, это совершенно не означает, что протокол безопасности WEP не годится совсем. Для небольших беспроводных сетей, состоящих из нескольких компьютеров, такой защиты вполне достаточно, поскольку трафик сети в этом случае сравнительно

небольшой и для его анализа и взлома ключа шифрования нужно потратить

значительно больше времени. Что же касается больших, развернутых беспроводных сетей, то использование в них протокола WEP небезопасно и крайне не рекомендуется. Стоит также учитывать, что в Интернете представлено множество специализированных утилит, которые позволяют взломать защиту WEP-протокола и обеспечить доступ к беспроводной

сети. Именно поэтому для обеспечения нужного уровня безопасности

лучше использовать более современные протоколы шифрования, в частности протокол безопасности WPA. Конечно, можно использовать ключи шифрования максимальной длины, но не стоит забывать о том, что это чревато уменьшением скорости передачи данных за счет увеличения их избыточности.

**1.5.2. Протокол безопасности WPA**

Протокол безопасности WPA пришел не смену протоколу безопасности WEP в силу понятных причин, главной из которых является практическая незащищенность WEP. Именно эта незащищенность сдерживала развитие и распространение беспроводных сетей. Однако с выходом протокола WPA все стало на свои места. Протокол безопасности *WPA* (Wi-Fi Protected Access, защищенный доступ Wi-Fi) был стандартизирован в 2003 году и сразу стал востребован. Главным отличием протокола WPA от WEP стало наличие динамической генерации ключей шифрования, что позволило кодировать каждый отправляемый пакет собственным ключом шифрования. Кроме того, каждое устройство в сети снабжается дополнительным ключом, который меняется через определенный промежуток времени. Аутентификация происходит с применением протокола аутентификации ЕАР (Extensible Authentication Protocol, расширяемый протокол аутентификации) с помощью службы (сервера), дистанционной аутентификации RADIUS или предварительно согласованного общего ключа. При этом аутентификация подразумевает вход пользователя после ввода логина и пароля, которые проверяются на сервере аутентификации RADIUS. Для шифрования данных используется модернизированный алгоритм шифрования RC4, основанный на протоколе краткосрочной целостности ключей TKIP.

Это позволяет не только повысить уровень защищенности данных, но и сохранить обратную совместимость с протоколом безопасности WEP.

Шифрование базируется на использовании случайного вектора инициализации

IV (Initialization Vector, вектор инициализации) и WEP-ключа, которые складываются и в дальнейшем используются для кодирования пакетов. Результатом такого складывания может стать огромное количество разных ключей, что позволяет добиться практически стопроцентной защиты данных.

Кроме того, протокол безопасности WPA поддерживает усовершенствованный

стандарт шифрования AES. Этот стандарт использует защищенный алгоритм кодирования, который намного эффективнее алгоритма RC4. Однако за это приходится платить повышенным трафиком и, соответственно, уменьшением пропускной способности сети.

**1.5.3. Идентификатор точки доступа и МАС-фильтрация**

Каков бы ни был уровень безопасности, его всегда недостаточно. Однако это совсем не означает, что этот уровень должен быть настолько высоким, насколько возможно. Всегда должен быть достигнут компромисс, особенно если учесть, что каждый дополнительный алгоритм защиты «съедает» у сети часть пропускной способности, что снижает скорость передачи данных в сети. Обеспечением минимального уровня безопасности можно считать использование идентификатора точки доступа и МАС-фильтрации адресов устройств.

**Идентификатор точки доступа**

Любая точка доступа, которая участвует в работе беспроводной сети, характеризуется идентификатором расширенного сервисного набора (ESSID — Extended Service Set ID), который представляет собой восьмибитный код. Если в сети присутствует несколько точек доступа, то в целях безопасности всем им присваивается одинаковый идентификатор. Фактически ESSID — это название вашей беспроводной сети, которое вы можете изменять, используя как буквы, так и цифры. Вы можете изменить это название в любой момент, не забывая при этом сообщить каждому подключенному компьютеру ESSID. Компьютер, который не будет знать ESSID, не сможет подключиться к вашей сети.

Чтобы еще больше усложнить задачу взломщикам сети, можно настроить точку

доступа таким образом, чтобы она не транслировала ESSID в эфир.

**МАС-фильтрация**

«Природным» способом защиты беспроводной сети можно считать фильтрацию по МАС-адресу. Дело в том, что МАС-адрес (Media Access Control, управление доступом к среде) — уникальный идентификатор, который присвоен любому сетевому оборудованию. Этот идентификатор используется с момента появления первых сетевых устройств, и изменить его невозможно. Итак, применяя фильтр по МАС-адресам в точке доступа, вы можете эффективно отсеивать «непрошеных гостей», тем самым дополнительно защищая свою беспроводную сеть.

При развертывании беспроводных LAN важно обеспечить максимальную их защищенность и удобство для сотрудников.

**1.6. Основы передачи голосовых данных по IP сетям**

Основными преимуществами трансляции голосового потока по сетям передачи данных с коммутацией пакетов являются:

* существенное уменьшение стоимости предоставления услуги — поскольку в этом случае отпадает необходимость организации дополнительных каналов и их обслуживании;
* возможность построения единой сети для предоставления комплекса интегрированных услуг;
* возможность широкого применения дешевых интеллектуальных терминалов и предоставления новых видов услуг;
* обеспечение единства администрирования.

Эти и другие побудительные причины привели к появлению комплекса спецификаций, регламентирующих передачу мультимедийного трафика по сетям с коммутацией пакетов. Поскольку на начальном этапе разработки и внедрения этих спецификаций наиболее быстрыми темпами развивались именно системы передачи телефонного трафика по сети Интернет, за этими спецификациями закрепилось неофициальные наименования "IP-телефония" или "Голос по IP" — VoIP (Voice over IP).

**1.6.1 Особенности пакетного преобразования голоса**

Само по себе применение технологий пакетной передачи голосового сигнала не всегда может обеспечить желаемую эффективность использования пропускной способности канала передачи данных. Например, при передаче трафика VoIP через сеть Ethernet каждый блок передаваемых голосовых данных  
будет снабжен блоком, состоящим, как минимум, из 38 байтов управляющих  
данных. Поскольку, в общем случае, эффективность использования канала  
определяется соотношением размеров блоков полезной и управляющей информации в передаваемом пакете, для ее повышения целесообразно увеличивать информационное наполнение каждого передаваемого пакета. При передаче голосового сигнала, однако, повышение эффективности использования канала приводит к появлению алгоритмической задержки, вызванной необходимостью накопления данных перед их отправкой в пакете. В Таблице 1.1 приведены характеристики кодеков, наиболее часто используемых в сетях VoIP. Как видно из таблицы, применение эффективных кодеков приводит к увеличению -задержки передачи сигнала в канале. Сама по себе задержка в несколько десятков миллисекунд не оказывает влияния на процесс телефонного разговора. Допустимыми, в частности, признаны значения задержки, не превышающие 150 мсек. Однако следует учитывать, что в процессе передачи пакета по сети задержка будет только увеличиваться. Наиболее неприятным последствием увеличения задержки распространения оцифрованного голосового сигнала является усиление влияния эхо-сигнала на качество телефонного разговора.

Таблица 1.1 – Характеристики кодеков

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Обозначение кодека | Размер нагрузки (байт) | Информа- ционная скорость (Кбит/с) | Алгоритми- ческая задержка  (МС) | Скорость передачи данных в канале (Кбит/с)1 | |
|  |  |  |  | Ethernet2 | IP3 |
| 1 | 2 | 3 | 4 | 5 | 6 |
| G.711 | 160 | 64 | 20 | 80 | 64.8 |
| G.723.1 (6.3) | 24 | 6.3 | 37.5 | 17.1 | 6.9 |
| G.723.1 (5.3) | 20 | 5.3 | 37.5 | 16 | 5.9 |
| G.726-32 | 160 | 32 | 20 | 42.7 | 32.8 |
| G726-24 | 160 | 24 | 20 | 34.7 | 24.8 |
| G.726-16 | 160 | 16 | 20 | 26.7 | 16.8 |
| G.729 (8) | 20 | 8 | 25 | 18.7 | 8.8 |
| G.729 (6.4) | 16 | 6.4 | 25 | 17.1 | 7.2 |

Стандарт G.711 описывает методику кодирования голосовых данных на 64 Кбит/с. Стандарт кодирования G.711 подразумевает немедленное преобразование голосовых данных в формат, необходимый для цифровой голосовой передачи по открытой телефонной сети. В первую очередь .отметим, что, как и для ТфОП, минимально необходимым для оборудования VolP является ИКМ-кодирование G.711. Это означает, что любое устройство VolP должно поддерживать этот тип кодирования.

**1.6.2 Системы традиционной и пакетной телефонии**

Обязательным требованием к системе пакетной телефонии, естественно, является полная поддержка всего комплекса услуг традиционной телефонии с  
наименьшими затратами и достаточным качеством. Среди этих услуг, которые должны обеспечивать системы пакетной телефонии, в первую очередь  
следует выделить:

* *Организацию междугородних и международных телефонных переговоров*

Высокая стоимость этой услуги, предоставляемой в современных телефонных сетях, объясняется необходимостью резервирования пропускной  
способности 64 Кбит/сек на всем протяжении вызова. Разнообразные системы пакетной телефонии позволяют в 3—5 раз сократить стоимость телефонного разговора только за счет уменьшения объемов передаваемых данных.

* *Организацию и проведение телефонных конференций*

Внедрение систем пакетной телефонии значительно увеличивает функциональные возможности терминального оборудования. Вследствие этого,  
участники телефонной конференции, организованной в системе пакетной  
телефонии, могут получить в свое распоряжение дополнительные функции, например, возможность параллельного обмена текстовыми сообщениями.

* *Создание и обслуживание центров автоматизированной обработки телефонных вызовов*

Применение пакетной телефонии существенно упрощает и снижает стоимость построения центров обработки телефонных вызовов.

**1.6.3 Аппаратные и программные IP-телефоны**

Программные и аппаратные IP-телефоны выполняют функции оконечных  
устройств — терминалов в телефонных сетях с коммутацией пакетов. Используя IP-телефон, пользователь может организовать прямое телефонное  
соединение с абонентами сети пакетной телефонии, и — через шлюз с абонентами традиционной телефонной сети. Для того чтобы начать использование IP-телефона, пользователь должен установить адресные параметры, определяющие его положение в сети Интернет, а также, при необходимости, — IP-адрес шлюза и параметры используемых кодеков. В дополнение к обычным сервисам аппарата традиционной телефонии IP-телефоны поддерживают множество дополнительных возможностей и функций:

* автоматическую синхронизацию календаря по протоколу NTP;
* использование пароля для ограничения доступа к терминалу;
* удаленный контроль и управление телефонным терминалом по протоколам HTTP, SNMP и Telnet;
* загрузку обновлений программного обеспечения по протоколу FTP.

Аппаратные IP-телефоны представляют собой отдельные устройства, внешнее отличие которых от традиционных телефонных аппаратов заключается в наличии разъема для подключения к сети Ethernet. Некоторые аппаратные IP-телефоны имеют в своем составе встроенный коммутатор, обеспечивающий расширение порта Ethernet 10/100 Base Т. При установке такого IP-телефона у абонента, он подключается к тому порту Ethernet, куда была прежде подключена рабочая станция абонента. После этого рабочая станция включается в сеть Ethernet через порт расширения IP-телефона, что позволяет сохранить в организации общее число портов, используемых для подключения абонентов ЛВС. Электропитание аппаратных IP-телефонов выполняется от внешнего источника или через сетевой кабель Ethernet от коммутатора, который поддерживает электропитание по сети Ethernet — РоЕ (Power over Ethernet). Программные IP-телефоны представляют собой аппаратно-программный комплекс, основной частью которого является персональный компьютер абонента, функционирующий под управлением сетевой операционной системы. На персональном компьютере программно реализуются основные функции IP-телефона:

* управление телефонным вызовом;
* индикация состояния телефонного вызова;
* прямое и обратное преобразование голосового сигнала в поток пакетов.

Поскольку программный IP-телефон использует тот же интерфейс подключения к локальной сети, что и персональный компьютер, то для подключения этого телефона к локальной сети не требуется внесения никаких изменений. Дополнительным преимуществом программного IP-телефона является возможность применения специализированных приложений в процессе обработки телефонного вызова. Для повышения удобства использования программного IP-телефона пользователь может подключить к компьютеру по интерфейсу USB телефонную трубку или гарнитуру. Основным недостатком программного IP-телефона следует считать невозможность приема телефонных вызовов при выключенном компьютере. Этот недостаток, впрочем, не имеет существенного значения при использовании программных IP-теле-  
фонов в составе центра обработки телефонных вызовов.

### 1.6.4 Требования к качеству обслуживания для голоса

Определяя требования QoS корпоративного VoIP трафика рекомендуется придерживаться следующих правил:

* односторонняя задержка не должна превышать 150 мс, в соответствии со International Telecommunication Union (ITU) ;
* колебания задержки (jitter) должны быть менее 30 мс;
* для каждого разговора (в зависимости от частоты квантования, кодека и заголовка второго уровня) требуется 21-106 Кбит/с гарантированной приоритетной полосы пропускания;
* для трафика сигнализации требуется 150 Бит/с (плюс заголовок второго уровня) гарантированной полосы пропускания.

На качество голосовой связи напрямую влияют все три фактора качества QoS: потери пакетов, задержка и вариации задержки.

Потери пакетов вызывают кратковременные пробелы в разговоре. Стандартные алгоритмы кодирования используемые в Cisco DSP (Digital Signal Processor) с помощью алгоритмов маскирования могут восстановить потери до 30 мс. Таким образом, потери двух и более последовательных 20 мс сэмплов приведут к заметной деградации качества голоса. Предположив случайное распределение сбросов пакетов в одном речевом потоке, сброс 1-го процента в голосовом потоке привела бы в среднем к потери, которую нельзя было бы восстановить каждые 3 минуты. Аналогично, уровень сброса 0,25 процента привел бы в среднем к потери, которую нельзя было бы восстановить каждые 53 минуты.

Задержка более 200 мс может вызвать деградацию качества голосовой связи. Если общая задержка в канале становится слишком большой, разговор по телефону начинает напоминать переговоры по спутниковому каналу связи или по симплексному радиоканалу. В стандарте Международного Союза Электросвязи для технологии VoIP говорится, что задержка величиной в 150 мс в одном направлении является приемлемой для качество голосовой связи. Было продемонстрировано, что разница в качестве голоса между сетями с задержкой в 150 мс и 200 мс является незначительной и практически незаметной для пользователя. Cisco рекомендует ориентироваться на ITU стандарт 150 мс, но если существуют ограничения не позволяющие добиться такого бюджета, то размер задержки может быть увеличен до 200 мс без значительной деградации качества связи

Что же касается колебаний задержки, то для их выравнивания в устройствах Cisco для IP-телефонии используются адаптивные буферы.

Однако они могут компенсировать колебания задержки лишь в пределах от 20 до 50 мс. При централизованной обработке вызовов IP-телефоны используют контрольные каналы TCP для связи с Cisco CallManager. Если эти весьма небольшие каналы не получат достаточной полосы пропускания, качество обслуживания абонентов будет ухудшаться. Сети с коммутацией пакетов не обеспечивают гарантированной пропускной способности, поскольку не обеспечивают гарантированного пути между точками связи. Для приложений, где не важен порядок и интервал прихода пакетов, например, e-mail, время задержек между отдельными пакетами не имеет решающего значения. IP-телефония является одной из областей передачи данных, где важна динамика передачи сигнала, которая обеспечивается современными методами кодирования и передачи информации, а также увеличением пропускной способности каналов, что приводит к возможности успешной конкуренции 1Р -телефонии с традиционными телефонными сетями.

**1.7 Выбор оборудования.**

По мере того, как работники становятся более мобильными, а бизнес-приложения – более интерактивными, инновационные услуги и приложения начинают играть все более важную роль в обеспечении динамики бизнеса и его уникального позиционирования на рынке. Беспроводные решения Cisco позволяют компаниям организовать для своих сотрудников доступ к корпоративной сети в тех местах, где им это больше всего необходимо. Модель [Cisco Unified Wireless Network](mhtml:file://D:\Новая%20папка%20(2)\МОЙ%20ДИПЛОМ\оборудование\Почему%20именно%20Cisco_%20-%20Беспроводные%20сети%20-%20Cisco%20Systems.mht!/global/RU/netsol/ns340/ns394/ns348/ns337/networking_solutions_package.html) (унифицированная беспроводная сеть Cisco) предлагает экономичное решение, позволяющее удовлетворить растущие потребности в беспроводных сетях. Наиболее полный в отрасли ассортимент беспроводных решений может послужить экономичной платформой для удовлетворения текущих потребностей организаций и одновременно предложить максимально безболезненный вариант перехода к новой инфраструктуре, способной обеспечить защиту инвестиций в ранее приобретенное оборудование. Гибкая архитектура решения позволяет администраторам сети спроектировать инфраструктурные модели, позволяющие удовлетворить специфические потребности организаций независимо от того, какую сеть они предполагают развернуть – простую или высокоинтегрированную.

Cisco реализует в беспроводной локальной сети целый ряд интеллектуальных сетевых функций, в том числе Wi-Fi Multimedia (WMM), управление качеством обслуживания (QoS), виртуальные локальные сети и быстрый, защищенный роуминг на уровнях 2 и 3, позволяющий обеспечить прозрачную мобильность пользователей. Дополнительные функциональные возможности позволяют организациям:

* Приоритезировать беспроводной трафик, чтобы гарантировать безопасную доставку информации нужным адресатам
* Сегментировать беспроводные сети, чтобы обеспечить поддержку различных категорий пользователей и приложений
* Обеспечить прозрачный переход между подсетями (сетевыми сегментами) с целью организации прозрачного роуминга

Основу любой сети, естественно, составляет оборудование — активное и пассивное. Именно оно позволяет подключать компьютер к сети, передавать данные, маршрутизировать пакеты в комбинированных сетях и т. д. К сетевому оборудованию, которое используется в беспроводных сетях, относятся сетевой адаптер, точка доступа, мост, маршрутизатор, принт-сервер и многое  
другое. Кроме того, сюда же можно отнести антенны, служащие для усиления или узкой направленности сигнала

Основу беспроводной локальной сети составляют следующие компоненты:

– Точка доступа (Access Point) – представляет собой концентратор, обеспечивающий подключение нескольких беспроводных клиентов к локальной сети или Интернету. Для охвата сетью всех площадей здания обычно требуется несколько точек доступа. Одна точка, находящаяся внутри помещения, способна обслуживать пользовательские устройства в диапазоне примерно 45 метров, в зависимости от условий распространения радиоволн. На эти условия, в свою очередь, могут влиять такие факторы, как структура стен, место расположение точки доступа и т.д.

– Беспроводный телефон (Wireless LAN Phone) – абонентское устройство, поддерживающее технологию передачи речи с использованием Интернет – протокола (Voice over Internet Protocol (VoIP)) и работающее на базе той же беспроводной инфраструктуры, что и сетевой адаптер.

– Соединения между зданиями (Building-to-Building Bridges) – элементы инфраструктуры, обычно используемые в сетях с «многоточечной» (point-to-multipoint) конфигурацией.

**1.7. 1 Коммутатор Cisco Catalyst 2960 24.**

Новое семейство коммутаторов второго уровня Cisco Catalyst 2960 с фиксированной конфигурацией позволяет подключать рабочие станции к сетям Fast Ethernet и Gigabit Ethernet на скорости среды передачи, удовлетворяя растущие потребности в пропускной способности на периферии сети. Для агрегации применяются комбинированные гигабитные uplink-порты, которые могут объединяться в единый канал по технологии Gigabit Ethernet Channel. Данная серия коммутаторов ориентирована в первую очередь на предприятия малого и среднего бизнеса, а также филиалы крупных компаний для решения задачи реализации уровня доступа к сети. По сравнению с популярной серией коммутаторов Catalyst 2950 модели семейства 2960 обеспечивают более широкий набор функций обеспечения безопасности и качества обслуживания, а также управление полосой пропускания. Основные функции:

* Обеспечивает работу на уровне 2 (Layer 2) с возможностью предоставления сервисов уровней 2-4 (Layer 2-4)  
  Layer 2 switching with intelligent Layer 2-4 services;
* Поддержка интеллектуальных функций на границе сети, например, адаптируемые списки контроля доступа (ACL) и расширенный функционал по обеспечению безопасности сети;
* Гигабитные порты двойного назначения позволяют использовать как медные соединения, так и оптические, используя единый порт. Каждый фисксированный порт двойного назначения позволяет или организовать медное соединение на скорости 10/100/1000 и оптическое через SFP-based гигабитный порт, одновременно активен только 1 порт;
* Улучшенный набор функций по обеспечению контроля качества сервисов позволяет оптимально управлять сетью и ее пропускной способностью;
* Коммутаторы поддерживают функции выборочного ограничения скорости для пользователей, создания списков контроля доступа и группового предоставления сервисов;
* Высокий уровень безопасности сети обеспечивается поддержкой широкого спектра методов идентификации и авторизации пользователей, технологий шифрования данных и составления списков доступа для пользователей, портов и MAC адресов;
* Программное обеспечение Cisco Network Assistant позволяет легко настраивать и модернизировать оборудование.
  + 1. **Cisco Aironet 1300 Series Outdoor Access Point/Bridge.**

Cisco Aironet®1300 Series является универсальным беспроводным устройством, сочетающим в себе функциональность беспроводного моста, точки доступа и клиентского моста для рабочих групп (workgroup bridge, WGB).

Cisco Aironet®1300 работает в соответствии с стандартом IEEE 802.11g (который включает в себя совместимость со стандартом IEEE 802.11b), и позволяет получить эффективную высокоскоростную беспроводную связь как для стационарных, так и для мобильных сетей и клиентов. Cisco Aironet®1300 можно монтировать прямо на улице, что повышает дальность связи. Спроектированное специально для жестких погодных условий, но также пригодное для применения внутри помещений, оборудование Cisco Aironet 1300 Series является идеальным решением для беспроводных сетей (WLANs), в которых необходимо применение точек доступа находящихся вне здания. Устройства Cisco Aironet 1300 Series являются WiFi-сертифицированными в качестве точки доступа (в стандарте IEEE 802.11b).

Основные характеристики :

* скорость 54 Мбит/с в диаппазоне 2.4 ГГц;
* дальность до 32 километров при скорости 11 Мбит/с;
* суммарная пропускная способность около 28 Мбит/с;
* максимальная мощность передатчика 100 мВт для стандарта 802.11b и 30 мВт для стандарта 802.11g;
* установка в автомобилях: при скоростях движения более 100 км/ч на скоростях передачи 12 и 24 Мбит/с с размером пакета 128 байт пакетная скорость возникновения ошибки Packet Error Rate (PER) составляет 1 процент;
* поддержка антенной избыточности;
* гибкость и простота в установке ;

Небольшие размеры и малый вес обеспечивают простоту установки. Информативные световые индикаторы (LEDs) служат для регулировки и диагностики оборудования. Удобный крепежный кронштейн позволяет облегчить процесс установки, настенный и напольный комплекты крепежа предоставляют широкий набор решений для установки оборудования

* + 1. **Точка доступа Cisco Aironet 1200**

Точка доступа Cisco Aironet серии 1200 - это однодиапазонная "облегченная" или автономная точка доступа с разъемами для антенн с двойным разнесением, предназначенная для установки в сложных радиочастотных средах. Это однодиапазонное решение, работающее в стандарте 802.11g, обеспечивает высокий уровень универсальности, пропускной способности, защищенности и функциональности корпоративного класса, соответствующий запросам компаний, использующих промышленные беспроводные сети. Это модульное устройство можно модернизировать на месте до уровня двухдиапазонного устройства с поддержкой стандартов 802.11a/g путем добавления модуля модернизации 802.11a на основе CardBus. Этот модуль можно легко установить на любой точке доступа Cisco Aironet серии 1200, изначально сконфигурированной для работы в стандарте 802.11g. Данная точка поставляется либо в "облегченном", либо в автономном варианте. Во втором случае ее впоследствии можно будет модернизировать до "облегченного" варианта на месте.

Сочетание универсальности, высокой пропускной способности, защищенности и функциональности корпоративного класса позволяет использовать это устройство для организации доступа к беспроводной сети в более сложных радиочастотных средах. Данная точка поставляется либо в "облегченном" (lightweight), либо в автономном варианте. Во втором случае ее впоследствии можно будет модернизировать до "облегченного" варианта на месте. Поддержка работы в обоих режимах – "облегченном" и автономном – позволяет почувствовать такие преимущества общей аппаратной платформы, как простота и эффективность, даже в случае смешанной инфраструктуры доступа, включающей в себя как "облегченные", так и автономные точки доступа. Специальная предназначенная для беспроводных сетей, работающих в условиях повышенной защищенности или требующих наличия специализированных внешних антенн, точка доступа Cisco Aironet серии 1200AG имеет разъемы для разнесенных антенн, работающих в диапазонах 2.4 и 5 ГГц. Это позволяет увеличить дальность действия, обеспечить универсальность покрытия и предложить более гибкие варианты установки. Точки доступа Cisco Aironet серии 1200AG сочетают универсальность с прекрасными показателями мощности передатчика, чувствительности приемника и распределения задержки для сред с высокой многоканальностью. Это позволяет гарантировать надежную работу сети и обеспечить высокую пропускную способность в самых сложных условиях.

* + 1. **Маршрутизатор Cisco 2801 Security Bundle**

Главной особенностью новых Cisco 2801 является их многофункциональность по предоставлению высококачественных сервисов. Равно как и маршрутизаторы младших серий, Cisco 2801 имеет аппаратную поддержку по шифрованию трафика, интегрированные DSP-слоты (digital-signal-processor) для обработки голосовых потоков, систему IPS (intrusion prevention system) и функции firewall (на базе Cisco IOS Software Firewall).  
 Функции безопасности при передаче голоса, видео и данных.  
В последнее время маршрутизаторы играют очень важную роль в стратегии безопасности сетей, ввиду необходимости обеспечения безопасной передачи данных по сетям общего доступа. Серия Cisco 2800, благодаря Cisco IOS® Software Advanced Security Feature Set, может выполнять ряд функций по обеспечению сетевой безопасности, среди которых стоит отметить firewall, intrusion prevention, IPSec VPN, Secure Shell (SSH) 2.0 и SNMPv3, network admissions control (NAC), Voice and Video Enabled VPN (V3PN), Dynamic Multipoint VPN (DMVPN) и Easy VPN. Обеспечение функций IP Communications на базе Cisco 2800. Cisco 2800 может легко интегрироваться в корпоративные сети среднего и крупного уровня для обеспечения сервисов IP на базе одной платформы. Так, например, решение на базе интегрированного Cisco CallManager Express (CME) обеспечивает задачу по обеспечению VoIP с использованием до 72 Cisco IP-phones . Cisco 2801 - маршрутизатор с интеграцией сервисов, обеспечивающий все потребности небольших офисов и филиалов (до 24 рабочих мест) в современных коммуникациях. Может выполнять функции:

* маршрутизатора доступа и маршрутизатора локальной сети;
* центра IP-телефонии и голосовой почты (в вариантах Voice bundle и Voice Security bundle);
* интегрированного решения для обеспечения безопасности (в вариантах Security bundle и Voice Security bundle);
  + межсетевой экран;
  + система предотвращения вторжений;
  + шифрование и создание VPN-туннелей;
  + система Cisco NAC и фильтрация по URL;
* центр беспроводного доступа -беспроводное подключение ноутбуков и WLAN-телефонов. (При установке модулей HWIC-AP-G-E, HWIC-AP-AG-E или подключении точек доступа).

В приведённой ниже таблице указаны максимальные возможности шасси Cisco 2801. В зависимости от варианта поставки (Bunlde) и установки дополнительных модулей характеристики могут отличаться от приведённых в таблице 1.1 Таблица 1.1 - Возможности маршрутизатора Cisco 2801

|  |  |
| --- | --- |
| Производительность: | |
| Маршрутизация пакетов: | • 90.000 пакетов/сек  • 46.08 Мбит/сек |
| Производительность в приложениях VPN со встроенным ускорителем шифрования: | • до 150 VPN-туннелей,  • 3DES, AES - 50 Mbps |
| Производительность в приложениях VPN при установленном модуле AIM-VPN/SSL-2: | • до 1500 VPN туннелей  • 3DES, AES до 160 Mbps |
| Производительность межсетевого экрана: | 127 Mbps |
| Число телефонов в IP-PBX CallManager Express или Survivable Remote Site Telephony: | До 24 IP-телефонов |
| Число одновременных звонков по цифровым каналам: | Дс 30 |
| Число аналоговых телефоных линий: | До 16 FXS или FXO |
| Число ящиков голосовой почты: | До 50 |

* + 1. **Cisco Access Point 1121-G-A-K9**

Характеристики Cisco Access Points 1121-G-A-K9 1100 Series 802.11g AP представлены в таблице 1.2

Таблица 1.2 – Характеристики оборудования

|  |  |  |
| --- | --- | --- |
| Part Number | 802.11b:AIR-AP1120B-A-K9 | 802.11g: AIR-AP1121G-A-K9 |
| Скорость передачи | 1, 2, 5.5, 11 Мбит/c | 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 и 54 Мбит/c |
| Диапазон частот | 2.412-2.462 ГГц | 2.412-2.462 ГГц |
| Чувствительность приемника | 1 Мбит/с: -94 дБ/м;  2 Мбит/с: -91 дБ/м;  5.5 Мбит/с: -89 дБ/м;  11 Мбит/с: -85 дБ/м | 1 Мбит/с: -95 дБ/м;  2 Мбит/с: -91 дБ/м;  5.5 Мбит/с: -89 дБ/м;  6 Мбит/с: -90 дБ/м;  9 Мбит/с: -84 дБ/м;  11 Мбит/с: -88 дБ/м;  12 Мбит/с: -82 дБ/м;  18 Мбит/с: -80 дБ/м;  24 Мбит/с: -77 дБ/м;  36 Мбит/с: -73 дБ/м;  48 Мбит/с: -72 дБ/м;  54 Мбит/с: -72 дБ/м |
| Мощность передатчика | CCK:  100 мВт (20 дБ/м);  50 мВт (17 дБ/м);  30 мВт (15 дБ/м);  20 мВт (13 дБ/м);  5 мВт (7 дБ/м);  1 мВт (0 дБ/м) | CCK:  100 мВт (20 дБ/м);  50 мВт (17 дБ/м);  30 мВт (15 дБ/м);  20 мВт (13 дБ/м);  10 мВт (10 дБ/м);  5 мВт (7 дБ/м);  1 мВт (0 дБ/м);  OFDM:  30 мВт (15 дБ/м);  20 мВт (13 дБ/м);  10 мВт (10 дБ/м);  5 мВт (7 дБ/м);  1 мВт (0 дБ/м); |

Продолжение таблицы 1.2

|  |  |  |
| --- | --- | --- |
| Зона охвата | В помещении:  27 м при 54 Мбит/с;  29 м при 48 Мбит/с;  30 м при 36 Мбит/с;  42 м при 24 Мбит/с;  54 м при 18 Мбит/с;  64 м при 12 Мбит/с;  67 м при 11 Мбит/с;  76 м при 9 Мбит/с;  91 м при 6 Мбит/с;  94 м при 5.5 Мбит/с;  107 м при 2 Мбит/с;  125 м при 1 Мбит/с  Вне помещения:  34 м при 54 Мбит/с;  60 м при 48 Мбит/с;  69 м при 36 Мбит/с;  100 м при 24 Мбит/с;  122 м при 18 Мбит/с;  145 м при 12 Мбит/с;  150 м при 11 Мбит/с;  168 м при 9 Мбит/с;  198 м при 6 Мбит/с;  201 м при 5.5 Мбит/с;  210 м при 2 Мбит/с;  213 м при 1 Мбит/с | В помещении:  27 м при 54 Мбит/с;  29 м при 48 Мбит/с;  30 м при 36 Мбит/с;  42 м при 24 Мбит/с;  54 м при 18 Мбит/с;  64 м при 12 Мбит/с;  67 м при 11 Мбит/с;  76 м при 9 Мбит/с;  91 м при 6 Мбит/с;  94 м при 5.5 Мбит/с;  107 м при 2 Мбит/с;  125 м при 1 Мбит/с  Вне помещения:  34 м при 54 Мбит/с;  60 м при 48 Мбит/с;  69 м при 36 Мбит/с;  100 м при 24 Мбит/с;  122 м при 18 Мбит/с;  145 м при 12 Мбит/с;  150 м при 11 Мбит/с;  168 м при 9 Мбит/с;  198 м при 6 Мбит/с;  201 м при 5.5 Мбит/с;  210 м при 2 Мбит/с;  213 м при 1 Мбит/с |
| Размер, Ш x В x Г | 10.4x20.5x3.8 см | 10.4x20.5x3.8 см |
| Вес | 297 г | 297 г |
| Системная память | 16 MB RAM, 8 MB FLASH | 16 MB RAM, 8 MB FLASH |
| Энергоснабжение | 100-240 В, 50-60 Гц (сеть), 33-57 В (Power over Ethernet) | 100-240 В, 50-60 Гц (сеть), 33-57 В (Power over Ethernet) |
| Энергопотребление | 4.9 Вт, RMS | 4.9 Вт, RMS |
| Рабочая температура | 0-40 °C | 0-40 °C |

* + 1. **IP Phone 7920**

Cisco расширяет возможности передачи голоса и функциональность унифицированных коммуникаций в масштабе всего предприятия с помощью мощного, инновационного конвергентного беспроводного решения, в основе которого лежит интеллектуальная беспроводная инфраструктура. Беспроводной IP-телефон Cisco Unified 7920 представляет собой удобное в эксплуатации устройство с поддержкой стандарта IEEE 802.11b, которое обеспечивает полноценную голосовую связь в сочетании с Cisco Unified CallManager и точками доступа Wi-Fi (IEEE 802.11b) Cisco Aironet серий 1200, 1100, 350 и 340. Будучи неотъемлемой частью беспроводного решения унифицированных коммуникаций Cisco, беспроводной IP-телефон Cisco Unified 7920 прозрачно реализует такие интеллектуальные услуги, как безопасность, мобильность, управление качеством обслуживания (QoS) и сетевое администрирование в масштабе всей сети Cisco.

# Техническое предложение

Стремительное развитие систем радиотелефонной связи в последнее десятилетие превратило беспроводную связь с подвижными и стационарными объектами из особого вида обслуживания для избранных в услугу связи.

Чтобы оценить наиболее выгодный и надежный вид связи, в частном случае для организации телефонной связи внутри отдельного предприятия, необходимо провести сравнительный анализ существующих систем связи.

**Сотовая связь стандарта GSM.**

Стандарт GSM тесно связан со всеми современными стандартами цифровых сетей, в первую очередь с ISDN (Integrated Services Digital Network) и IN (Intelligent Network). Основные функциональные элементы GSM входят в разрабатываемый сейчас международный стандарт глобальной системы подвижной связи UMTS (Universal Mobile Telecommunications System).

GSM по существу является цифровой системой передачи данных, речь кодируется и передается в виде цифрового потока. Абоненты GSM могут осуществлять обмен информацией с абонентами ISDN, обычных телефонных сетей, сетей с коммутацией пакетов, и сетей связи с коммутацией каналов, используя различные методы и протоколы доступа, например, X.25 или X.32. Возможна передача факсимильных сообщений, реализуемых при использовании соответствующего адаптера для факс-аппарата. Уникальной возможностью GSM, которой не было в старых аналоговых системах, является двунаправленная передача коротких сообщений SMS (Short Message Service), (до 160 байт), передаваемых в режиме с промежуточным хранением данных.   
Текущие спецификации в виде дополнительных возможностей описывают услуги по переносу информации и предоставлению связи (например, перенаправление вызова в случае недоступности подвижного абонента), Однако есть и недостатки такой системы связи:

- дороговизна связи и дополнительных услуг;

- недостаточный уровень сигнала в помещениях;

**Спутниковая сотовая связь**

Главное отличие мобильных спутниковых телефонов от мобильных телефонов других систем (например, сотовых) - это наличие у абонента телефонной связи независимо от наличия и состояния каких - либо местных телефонных сетей. Другими словами, пользователю спутникового телефона доступна качественная телефонная связь практически из любой точки земного шара. Это достигается непосредственной передачей радиосигнала с телефонного аппарата на один из спутников той или иной глобальной системы связи.

На сегодняшний день можно говорить о четырех системах спутниковой связи: "Инмарсат" (Inmarsat), "Иридиум"(Iridium), "Глобал Стар" (Global Star) и "Айко"(ICO),характеристики которых приведены в таблице 2.1

Таблица 2.1 – характеристики систем спутниковой связи

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Описание | Инмарсат | Ир ид пум | Глобалстар | Нью АЙКО |
| 1 | 2 | 3 | 4 | 5 |
| Орбита | Геостационарная | Низко- орбитальная | Низко- орбитальная | Средне- орбитальная |
| Высота орбиты | 36,500 | 780 | 1,414 | 10,000 |
| Глобальное покрытие | Да | Да | Да | Да |
| Начало эксплуатации | 1982 | 1998-2000 28.03.2001 | 2000 | 2003 |
| Голос (Кбит/с) | 4.8 | 4.8 | 4.8 | 4.8 |
| Факс (Кбит/с) | 2.4-64 | нет | 2.4 | 2.4 |
| Данные (Кбит/с) | 0.6-64 | 2.4 | 9.6 | 9.6 |
| ISDN | Да | Нет | Нет | данных нет |
| Пакетная передача | Да | Нет | Нет | данных нет |
| Короткие сообщения | Нет | Да | Да | Да |
| Пеиджинг | Нет | Да | Нет | Нет |
| Размер с | "ноутбук" | "трубка" | "трубка" | "трубка" |
| Цена (US $) | >3000 | >1500 | >1000 | >1000 |
| Стоимость минуты (US $) | 0.19-7.5 | 0.85-1.80 | 1.8-4.0 | 1.0-3.0 |
| Вес (кг) | 2.2 | 0.375 | 0.35 | 0.2-0.3 |

**Транкинговая радиосвязь**

Транкинговая (trunk - магистральная, или соединительная линия связи) подвижная радиосвязь - это профессиональная (и поэтому недешевая) мобильная радиосвязь. Смысл транкинговой подвижной радиосвязи состоит в возможности доступа большого числа абонентов к ограниченному количеству каналов радиосвязи и присвоении каждой радиостанции индивидуального абонентского номера, по которому осуществляется вызов абонента.

Мы живем в такое время, когда доступ к информации является важнейшим фактором обеспечения оперативности и эффективности работы организаций. Поэтому необходимо обеспечить соответствие уровня мобильного доступа к информации растущему уровню мобильности современных организаций. Это касается и доступа в Интернет, и использование решений на базе Интернета. В рамках сегмента транкинговых цифровых систем широкое распространение получил стандарт "ТЕТРА", или в переводе - "наземное транкинговое радио" (Terrestrial Trunked Radio).

Области применения тарнкинговой связи крупные коммерческие и государственные организации, например службы автоинспекции, различные ремонтные службы, компании, специализирующиеся в области промышленного альпинизма (обслуживание высотных зданий) и так далее. Систему транкинговой связи можно развернуть как в крупном городе, так и в удалённом, малонаселённом пункте. Однако для преприятия малого масштаба организация транкинговой связи является слишком дорогим удовольствием.

**Однако для организации телефонии на предприятия, необходимо сравнить радиосвязь стандарта DECT и Wi-Fi, так как именно эти 2 стандарта являются явно конкурирующими между собой.**

### Достоинства и недостатки DECT и Wi-Fi

DECT - системы микросотовой связи на территории предприятия, абонентского беспроводного доступа - Wireless Local Loop (WLL) к телекоммуникационной сети как альтернатива проводному подключению, бытовые телефоны. Wi-Fi - для организации беспроводных ЛВС (WLAN) и организации беспроводного доступа к сети Интернет.

**Преимущества Wi-Fi**

1. Позволяет развернуть сеть без прокладки кабеля, может уменьшить стоимость развёртывания и расширения сети. Места, где нельзя проложить кабель, могут обслуживаться беспроводными сетями.
2. Wi-Fi-устройства широко распространены на рынке и устройства разных производителей могут взаимодействовать на базовом уровне сервисов.
3. Wi-Fi сети поддерживают роуминг, поэтому клиентская станция может перемещаться в пространстве, переходя от одной точки доступа к другой.
4. Wi-Fi - это набор глобальных стандартов. В отличие от сотовых телефонов, Wi-Fi оборудование может работать в разных странах по всему миру.

**Недостатки Wi-Fi:**

1. Wi-Fi имеют ограниченный радиус действия. Типичная домашняя Wi-Fi точка доступа стандарта 802.11b или 802.11g имеет радиус действия 90 м в помещении и до 300 м снаружи. Расстояние зависит также от частоты. Wi-Fi в диапазоне 2.4 ГГц работает дальше, чем Wi-Fi в диапазоне 5 ГГц.
2. 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.
3. Неполная совместимость между устройствами разных производителей или неполное соответствие стандарту может привести к ограничению возможностей соединения или уменьшению скорости.

**Преимущества стандарта DECT:**

1. Возможность создания различных систем на основе DECT:  
    - домашние беспроводные многотерминальные системы, которые также подходят для малого офиса,  
    - микросотовые беспроводные корпоративные системы (офисные и учрежденческие АТС с радиодоступом),  
    - микросотовые системы общего пользования (СТМ),  
    - системы фиксированного радиодоступа (WLL) и др.
2. Обеспечение перехода из соты в соту без разрыва соединения (хэндовер);  
   6. Возможность обслуживания одной трубки в разных сетях (частных и общего пользования);
3. Отсутствие канала управления - устойчивость к радиопомехам;
4. Низкий уровень излучения - безопасность для здоровья.

К недостаткам DECT, пожалуй, можно отнести - низкую скорость передачи данных. По сравнению с Wi-Fi - очень низкую, сравнительные характеристики приведены в таблице 2.2.

**Таблица 2.2 - сравнительные характеристики DECT и Wi-Fi**

|  |  |  |
| --- | --- | --- |
|  | **DECT** | **Wi-Fi** |
| Диапазон частот | 1,9 ГГц | 2,4 ГГц |
| Мощность излучения | 10мВт | 100мВт |
| Скорость передачи данных | до 128 Кбит/с | до 54 Мбит/с |
| Хендовер | бесшовный | с разрывом или задержкой |
| Случаи взлома радио канала | Неизвестны | известны |
| Частотное планирование сети | Не требуется | необходимо |

**3.1. Расчёт радиопокрытия**

**3.1.1 Расположение оборудования**

В беспроводных системах возможен прием, сигналов при отсутствии прямой видимости между персональным компьютером (ПК) и точкой доступа (ТД). Особенностью распространения радиоволн, когда оборудование находится внутри помещения, является замкнутость пространства и наличие множества отражений и, соответственно, большого количества сигналов с примерно равными амплитудами на входе антенны приемника .

Параметры потерь распространения определяются на основе результатов измерений, так как теоретический анализ практически невозможен из-за отличий материалов стен и перекрытий, расположения предметов в помещениях, изменения обстановки из-за перемещений оборудования и т. д.

В общем случае к потерям в условиях прямой видимости необходимо добавить при прохождении стен и перекрытий:

, [дБ], (3.1)

где  – количество этажей между абонентом и точкой доступа;

– количество стен межу абонентом и точкой доступа;

 и  – потери энергии при прохождении радиоволной перекрытия или стены соответственно.

Формула расчета потерь распространения дает только ориентировочное значение затухания и имеет ряд ограничений.

В данной работе используется модель распространения радиоволн, которая кроме количества этажей, учитывает количество стен между ТД и ПК. Потери, дБ, в такой модели рассчитываются по формуле

, [дБ], (3.2)

где  – потери при распространении в свободном пространстве, дБ;

*R* – расстояние по прямой между ТД и ПК, м;

λ – длина волны, м;

 – погонное затухание (зависит от типа здания см. таблицу 3.4) на один метр длины, дБ;

– эмпирическая постоянная величина;

 – количество типов стен;

потери при прохождении стены  -го типа;

количество стен го типа;

потери при прохождении этажа, дБ;

количество этажей, между ТД и ПК.

Значения коэффициента меньше единицы и, например, для диапазона 1,8…3,0 ГГц эмпирическая постоянная b=0,46.

Значения затуханий в различных конструкциях приведены в приложении А.

При построении начального приближения сети целесообразно  
использовать данные об ориентировочном размере зоны обслуживания в  
соответствии с таблицей 3.1, числе каналов точек доступа.

Таблица 3.1 - Средние размеры зоны обслуживания и число пользователей на одну ТД

|  |  |  |
| --- | --- | --- |
| Тип зоны распространения | Ориентировочный радиус зон обслуживания, м | Число каналов |
| Здание | 20-50 | 64 |
| Открытая местность | 50-300 | 64 |

Полученное таким образом приближение сети уточняется в процессе расчета зон обслуживания точек доступа, при заданных требованиях к сети.

Каждая точка доступа рассчитана, примерно, на 30-60 человек (в зависимости от модели устройства), одновременно работающих в сети. Точки доступа соединяются с коммутаторами по кабелю UTP5E, расположенному над фальшпотолком или под фальшполом в специализированных кабель – каналах.

С учетом технических характеристик оборудования, было решено взять по 3 точки доступа на этаже в двух этажном здании и по 2 точки доступа на этаже в трех этажном здании. Такое количество ТД на каждом этаже обеспечит покрытие всей территории зданий и при наибольшей интенсивности нагрузки обеспечит необходимое количество каналов.

Точка доступа может быть установлена на стене или на потолке, желательно в невидимом месте, чтобы она не мешала постоянно находящимся в помещении людям. Также нельзя устанавливать оборудование рядом с электрическими приборами или устройствами, которые могут создавать радиочастотные помехи (например, рядом с микроволновой печью). Также должно быть определено предварительно, в каких зонах время от времени может ожидаться большое скопление пользователей системы. Прежде, чем проект размещения ТД будет закончен, каждая ТД может быть размещена только после тщательного исследования конструкции здания (материал из которого сделана конструкция, например, из бетона с железной арматурой, кирпичная стена, и т.д.).

Учитывая вышеупомянутые условия, было решено разместить ТД, как показано на рисунке 3.1 на этом же рисунке изображена ориентировочная зона покрытия этажей 1-го здания.





Рисунок 3.1 - Ориентировочная зона покрытия 1-го здания и расположение точек доступа

**3.1.2. Методика расчета уровня сигнала**

Рассчитаю уровень сигнала, выраженный через усредненную мощность сигнала (УМС). Расчет производится для самых удаленных от ТД точек здания.

Для определения зоны обслуживания необходимо знать следующие исходные данные и характеристики оборудования:

* мощность передатчика;
* чувствительность приемника;
* коэффициент усиления антенны.

Для удобства дальнейших расчетов приведем мощность передатчика, выраженную в Вт, в мощность в дБм.

, [дБм],

 дБм.

Остальные величины, их значения и способ определения даны в таблице 3.2.

Таблица 3.2 - Данные и характеристики оборудования

|  |  |  |  |
| --- | --- | --- | --- |
| Параметры | Направление передачи | | Формула  для расчета |
| ТД→ПК | ТД→ПК |
| Мощность передатчика , мВт | 100 |  |  |
| Мощность передатчика , дБм | 20 | 20 |  |
| Чувствительность приемника , дБм | -94 | -89 |  |

Так как номинальная мощность передатчика сетевого адаптера в персональном компьютере и средняя мощность точки доступа равны, результаты расчета затухания в прямом и обратном каналах будут примерно одинаковы. Рассчитаем УМС только для прямого канала связи, и на основании расчетов определю зону уверенного приема в здании, сравнивая УМС с чувствительностью приемника.

Для каждого направления определим уровень вносимого затухания при прохождении сигнала от передатчика ТД до самой удаленной точки здания, с учетом всех препятствий, встречающихся на данном направлении. Сравнивая мощность сигнала в этой точке с чувствительностью приемника можно судить о размерах зоны уверенного приема.

Расчет производится по формуле (3.2):

, [дБ],

где  – потери при распространении в свободном пространстве, дБ;

*R* – расстояние по прямой межу ТД и ПК, м;

λ – длина волны, м;

 – погонное затухание (зависит от типа здания см. таблицу 3.4.) на один метр длины, дБ;

 – эмпирическая постоянная величина;

 – количество типов стен;

 – потери при прохождении стены  -го типа;

 – количество стен го типа;

 – потери при прохождении этажа, дБ;

 – количество этажей, между ТД и ПК.

В случае, когда ПК и ТД находятся на одном этаже, формула примет вид:

,[дБ],

где  – потери при распространении в свободном пространстве, дБ;

*R* – расстояние по прямой между ТД и ПК, м;

λ – длина волны, м;

L\* – погонное затухание на один метр длины (зависит от типа здания см. таблицу 3.4.), дБ;

Lстi – потери, при прохождении стены i-го типа, дБ;

nстi – число стен i-го типа.

**3.1.3. Расчет зоны радиопокрытия 1-го здания**

Общее количество абонентов подключенных к локальной сети в первом здании порядка 60. В начальном приближении принимаем, что в часы наибольшей нагрузки в зоне действия одной точки доступа находится примерно 20-30 ПК абонентов. В свою очередь одна точка доступа может обслуживать до 60 абонентов. Коммутатор установлен на втором этаже офиса компании, является двенадцати портовым.

Необходимо учесть, что первое здание состоит из двух этажей, в среднем на каждом этаже находится по 30 персональных компьютеров. Имеется большое количество различных перекрытий и перегородок, которые вносят в полезный сигнал некоторую долю затухания.

Для полного и равномерного радиопокрытия помещений было принято решение использовать по три точки доступа на каждом этаже. Таким образом, получается шесть точек доступа. Места расположения точек доступа были выбраны исходя из количества компьютеров их плотности и архитектуры самого офиса.

**3.1.3.1. Расчет точек доступа на первом этаже**

Для дальнейших расчетов необходимо знать количество и тип препятствий, на пути распространения радиоволн, вносимое ими затухание, расстояние до самой удаленной точки. Эти данные для 1 этажа здания представлены в таблице 3.3.

Таблица 3.3 - Данные для расчета зоны радиопокрытия 1 этажа (ТД 1)

|  |  |  |  |
| --- | --- | --- | --- |
| Направление распространения, град | Количество стен nст | Потери, при прохождении стены Lст, дБ | Расстояние R, м |
| 1 | 2 | 3 | 4 |
| 0 | 0 | 0 | 11 |
| 30 | 1 | 15 | 12 |
| 60 | 1 | 15 | 16,5 |
| 90 | 1 | 15 | 14,5 |
| 120 | 2 | 15 | 17 |
| 150 | 2 | 15 | 13,5 |
| 180 | 1 | 15 | 11,5 |
| 210 | 1 | 15 | 13,5 |
| 240 | 1 | 15 | 15,5 |
| 270 | 0 | 0 | 14 |
| 300 | 0 | 0 | 15,5 |
| 330 | 0 | 0 | 12,5 |

В направлении 120º самая удаленная точка в помещении находится в 17 м от ТД, до которой остается две кирпичные стены, при прохождении которой мощность сигнала уменьшается в сумме на 30 дБ. Рассчитаем затухание сигнала в данном направлении, учитывая затухание сигнала при распространении в свободном пространстве и наличие препятствий на пути распространения. Расчет производится по формуле (3.2):



УМС PУММС в данной точке рассчитывается по формуле:

, [дБ],

Таблица 3.4 - Результаты расчета

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Направление распространения, град | Расстояние R, м | Общие потери распространения, дБ | УМС, дБ | Прием |
| 1 | 2 | 3 | 4 | 5 |
| 0 | 11 | 66,36945 | -46,3694 | Уверенный |
| 30 | 12 | 82,62522 | -62,6252 | Уверенный |
| 60 | 16,5 | 87,64127 | -67,6413 | Уверенный |
| 90 | 14,5 | 85,51895 | -65,519 | Уверенный |
| Продолжение таблицы 3.4 | | | | |
| 1 | 2 | 3 | 4 | 5 |
| 120 | 17 | 103,1506 | -83,1506 | Уверенный |
| 150 | 13,5 | 99,39827 | -79,3983 | Уверенный |
| 180 | 11,5 | 82,00555 | -62,0055 | Уверенный |
| 210 | 13,5 | 84,39827 | -64,3983 | Уверенный |
| 240 | 15,5 | 86,59823 | -66,5982 | Уверенный |
| 270 | 14 | 69,96415 | -49,9642 | Уверенный |
| 300 | 15,5 | 71,59823 | -51,5982 | Уверенный |
| 330 | 12,5 | 68,22979 | -48,2298 | Уверенный |

Как видно из расчетов, во всех точках уровень сигнала больше порогового, например в направлении 120º, уровень сигнала -83,15 дБм, это значение больше порогового значения чувствительности приемника сетевого адаптера в ПК, равного -94 дБм, следовательно, та часть помещения, где расположена ТД, находится в зоне уверенного радиоприема. Расчет точки доступа 2. Для дальнейших расчетов необходимо знать количество и тип препятствий, на пути распространения радиоволн, вносимое ими затухание, расстояние до самой удаленной точки. Эти данные представлены в таблице 3.5.

Таблица 3.5 - Данные для расчета зоны радиопокрытия отдела конструкторов (ТД 2)

|  |  |  |  |
| --- | --- | --- | --- |
| Направление распространения, град | Количество стен nст | Потери, при прохождении стены Lст, дБ | Расстояние R, м |
| 1 | 2 | 3 | 4 |
| 0 | 1 | 15 | 10 |
| 30 | 1 | 15 | 12,5 |
| 60 | 1 | 15 | 22 |
| 90 | 1 | 9 | 19,5 |
| 120 | 1 | 9 | 22 |
| 150 | 0 | 15 | 13,5 |
| 180 | 0 | 15 | 12,5 |
| 210 | 1 | 15 | 12 |
| 240 | 1 | 15 | 7,5 |
| 270 | 1 | 15 | 6,5 |
| 300 | 1 | 15 | 7,5 |
| 330 | 1 | 15 | 11 |

В направлении 120º ТД излучает прямо в кирпичную стену (толщина 120мм), при прохождении которой мощность сигнала уменьшается на 9 дБ. Рассчитаем затухание сигнала в данном направлении, учитывая затухание сигнала при распространении в свободном пространстве, наличие препятствий на пути распространения. Расчет производится по формуле (3.2):



УМС PУМС в данной точке рассчитывается по формуле:

, [дБ],

В направлении 60º самая удаленная точка в помещении находится в 22 м от ТД. Рассчитаем затухание сигнала в данном направлении, учитывая затухание сигнала при распространении в свободном пространстве, наличие препятствий на пути распространения. Расчет производится по формуле (3.2):



УМС PУММС в данной точке рассчитывается по формуле:

, [дБ],

Таблица 3.6 - Результат расчета

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Направление распространения, град | Расстояние R, м | Общие потери распространения, дБ | УМС, дБ | Прием |
| 1 | 2 | 3 | 4 | 5 |
| 0 | 10 | 80,04159 | -60,0416 | Уверенный |
| 30 | 12,5 | 83,22979 | -63,2298 | Уверенный |
| 60 | 22 | 92,89005 | -72,89 | Уверенный |
| 90 | 19,5 | 84,59228 | -64,5923 | Уверенный |
| 120 | 22 | 86,89005 | -66,89 | Уверенный |
| 150 | 13,5 | 69,39827 | -49,3983 | Уверенный |
| 180 | 12,5 | 68,22979 | -48,2298 | Уверенный |
| 210 | 12 | 82,62522 | -62,6252 | Уверенный |
| 240 | 7,5 | 76,29282 | -56,2928 | Уверенный |
| 270 | 6,5 | 74,54986 | -54,5499 | Уверенный |
| 300 | 7,5 | 76,29282 | -56,2928 | Уверенный |
| 330 | 11 | 81,36945 | -61,3694 | Уверенный |

Как видно из расчетов, во всех точках уровень сигнала больше порогового, в направлении 60º, уровень сигнала -72,89 дБм, это значительно больше порогового значения чувствительности приемника сетевого адаптера в ПК, равного -94 дБм, следовательно, та часть помещения, где расположена ТД, находится в зоне уверенного радиоприема. Расчет точки доступа 3.Для дальнейших расчетов необходимо знать количество и тип препятствий, на пути распространения радиоволн, вносимое ими затухание, расстояние до самой удаленной точки. Эти данные представлены в таблице 3.7.

Таблица 3.7 - Данные для расчета зоны радиопокрытия ТД 3

|  |  |  |  |
| --- | --- | --- | --- |
| Направление распространения, град | Количество стен nст | Потери, при прохождении стены Lст, дБ | Расстояние R, м |
| 1 | 2 | 3 | 4 |
| 0 | 1 | 15 | 12 |
| 30 | 1 | 15 | 14 |
| 60 | 1 | 15 | 23,5 |
| 90 | 0 | 15 | 20 |
| 120 | 0 | 15 | 23 |
| 150 | 0 | 15 | 13,5 |
| 180 | 0 | 15 | 11,5 |
| 210 | 1 | 15 | 13,5 |
| 240 | 1 | 15 | 8,5 |
| 270 | 1 | 15 | 7,5 |
| 300 | 1 | 15 | 8,5 |
| 330 | 1 | 15 | 14 |

В направлении 60º ТД3 излучает в кирпичную стену, при прохождении которой мощность сигнала уменьшается на 15 дБ. В этом направлении находится самая удаленная точка в помещении на расстоянии 23,5 м. Рассчитаем затухание сигнала в данном направлении. Расчет производится по формуле (3.2):



УМС PУМС в данной точке рассчитывается по формуле:

, [дБ],

Таблица 3.8 - Результаты расчета

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Направление распространения, град | Расстояние R, м | Общие потери распространения, дБ | УМС, дБ | Прием |
| 1 | 2 | 3 | 4 | 5 |
| 0 | 12 | 82,62522 | -62,6252 | Уверенный |
| 30 | 14 | 84,96415 | -64,9642 | Уверенный |
| 60 | 23,5 | 94,21295 | -74,2129 | Уверенный |
| 90 | 20 | 76,06219 | -56,0622 | Уверенный |
| 120 | 23 | 78,77615 | -58,7761 | Уверенный |
| 150 | 13,5 | 69,39827 | -49,3983 | Уверенный |
| 180 | 11,5 | 67,00555 | -47,0055 | Уверенный |
| 210 | 13,5 | 84,39827 | -64,3983 | Уверенный |
| 240 | 8,5 | 77,87997 | -57,88 | Уверенный |
| 270 | 7,5 | 76,29282 | -56,2928 | Уверенный |
| 300 | 8,5 | 77,87997 | -57,88 | Уверенный |
| 330 | 14 | 84,96415 | -64,9642 | Уверенный |

Как видно из расчетов, во всех точках уровень сигнала больше порогового, например в направлении 60º, уровень сигнала -74,21 дБм, это значительно больше порогового значения чувствительности приемника сетевого адаптера в ПК, равного -94 дБм, следовательно, та часть помещения, где расположена ТД, находится в зоне уверенного радиоприема.

На основе полученных результатов расчета можно утверждать, что для полного и наилучшего покрытия помещений, необходимо 3 точки доступа, пользователи, находящиеся на этом этаже находятся в зоне уверенного приема.

Аналогично проводятся расчеты, для 2 этажа первого здания. Иллюстрация уточненной зоны радиопокрытия представлена на плакате.

**3.1.4. Расчет зоны радиопокрытия 2-го здания**

**3.1.4.1. Расчёт точек доступа 1 этажа**

Общее количество абонентов подключенных к локальной сети во втором здании порядка 105. В начальном приближении принимаем, что в часы наибольшей нагрузки в зоне действия одной точки доступа находится примерно 20-40 ПК абонентов. В свою очередь одна точка доступа может обслуживать до 60 абонентов.

Необходимо учесть, что второе здание состоит из трех этажей, в среднем на каждом этаже находится по 35 персональных компьютеров. Имеется большое количество различных перекрытий и перегородок, которые вносят в полезный сигнал некоторую долю затухания.

Очевидно, что полное и равномерное радиопокрытие помещений невозможно с использованием одной точки доступа. Поэтому было принято решение использовать несколько точек доступа по две на каждом этаже с целью достижения поставленной задачи. Таким образом, получается шесть точек доступа. Места расположения точек доступа были выбраны исходя из количества компьютеров их плотности и архитектуры самого офиса.

Расчёт затухания сигнала проводится по формуле 3.2 без учёта количества этажей.



Для дальнейших расчетов необходимо знать количество и тип препятствий, на пути распространения радиоволн, вносимое ими затухание, расстояние до самой удаленной точки. Эти данные представлены в таблице 3.9.

Таблица 3.9 - Данные для расчета зоны радиопокрытия ТД 1

|  |  |  |  |
| --- | --- | --- | --- |
| Направление распространения, град | Количество стен nст | Потери, при прохождении стены Lст, дБ | Расстояние R, м |
| 1 | 2 | 3 | 4 |
| 0 | 2 | 15 | 17 |
| 30 | 2 | 15 | 18,5 |
| 60 | 2 | 15 | 18 |
| 90 | 1 | 15 | 14,5 |
| 120 | 1 | 15 | 16 |
| 150 | 1 | 15 | 17 |
| 180 | 0 | 15 | 14,5 |
| 210 | 0 | 15 | 17 |
|  |  |  |  |
| Продолжение таблицы 3.9 | | | |
| 240 | 1 | 15 | 18 |
| 270 | 1 | 15 | 14,5 |
| 300 | 1 | 15 | 16 |
| 330 | 2 | 15 | 18,5 |

Рассчитаем затухание в самой удаленной точке помещения для ТД 1 первого этажа:

 дБ,

Результаты расчётов вносим в таблицу 3.10.

Таблица 3.10 - Результаты расчета

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Направление распространения, град | Расстояние R, м | Общие потери распространения, дБ | УМС, дБ | Прием |
| 1 | 2 | 3 | 4 | 5 |
| 0 | 17 | 103,1506 | -83,1506 | Уверенный |
| 30 | 18,5 | 104,635 | -84,635 | Уверенный |
| 60 | 18 | 104,147 | -84,147 | Уверенный |
| 90 | 14,5 | 85,51895 | -65,519 | Уверенный |
| 120 | 16 | 87,12399 | -67,124 | Уверенный |
| 150 | 17 | 88,15057 | -68,1506 | Уверенный |
| 180 | 14,5 | 70,51895 | -50,519 | Уверенный |
| 210 | 17 | 73,15057 | -53,1506 | Уверенный |
| 240 | 18 | 89,14704 | -69,147 | Уверенный |
| 270 | 14,5 | 85,51895 | -65,519 | Уверенный |
| 300 | 16 | 87,12399 | -67,124 | Уверенный |
| 330 | 18,5 | 104,635 | -84,635 | Уверенный |

Таблица 3.11 - Данные для расчета зоны радиопокрытия ТД 2

|  |  |  |  |
| --- | --- | --- | --- |
| Направление распространения, град | Количество стен nст | Потери, при прохождении стены Lст, дБ | Расстояние R, м |
| 1 | 2 | 3 | 4 |
| 0 | 2 | 15 | 14,5 |
| 30 | 2 | 15 | 17 |
| 60 | 1 | 15 | 11 |
| 90 | 1 | 15 | 10 |
| 120 | 1 | 15 | 11,5 |
| Продолжение таблицы 3.11 | | | |
| 150 | 2 | 15 | 20 |
| 180 | 1 | 15 | 17 |
| 210 | 1 | 15 | 21,5 |
| 240 | 0 | 15 | 15 |
| 270 | 0 | 15 | 14,5 |
| 300 | 2 | 15 | 17 |
| 330 | 2 | 15 | 15,5 |

Рассчитаем затухание в самой удаленной точке помещения для ТД 2 первого этажа:

 дБ,

Результаты расчётов вносим в таблицу 3.12

Таблица 3.12 - Результаты расчета

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Направление распространения, град | Расстояние R, м | Общие потери распространения, дБ | УМС, дБ | Прием |
| 1 | 2 | 3 | 4 | 5 |
| 0 | 14,5 | 100,519 | -80,519 | Уверенный |
| 30 | 17 | 103,1506 | -83,1506 | Уверенный |
| 60 | 11 | 81,36945 | -61,3694 | Уверенный |
| 90 | 10 | 80,04159 | -60,0416 | Уверенный |
| 120 | 11,5 | 82,00555 | -62,0055 | Уверенный |
| 150 | 20 | 106,0622 | -86,0622 | Уверенный |
| 180 | 17 | 88,15057 | -68,1506 | Уверенный |
| 210 | 21,5 | 92,44036 | -72,4404 | Уверенный |
| 240 | 15 | 71,06342 | -51,0634 | Уверенный |
| 270 | 14,5 | 70,51895 | -50,519 | Уверенный |
| 300 | 17 | 103,1506 | -83,1506 | Уверенный |
| 330 | 15,5 | 101,5982 | -81,5982 | Уверенный |

По результатам расчетов 1 этажа можно судить о том, что обеспечивается полное радиопокрытие помещения.

**3.1.4.2. Расчёт точек доступа 2 этажа**

Расчёты для второго этажа провожу по формуле 3.2 без учета количества этажей.



Данные по препятствиям 2 этажа представлены в таблице 3.13

Таблица 3.13 - Данные для расчета зоны радиопокрытия ТД 1

|  |  |  |  |
| --- | --- | --- | --- |
| Направление распространения, град | Количество стен nст | Потери, при прохождении стены Lст, дБ | Расстояние R, м |
| 1 | 2 | 3 | 4 |
| 0 | 0 | 15 | 17 |
| 30 | 0 | 15 | 18,5 |
| 60 | 0 | 15 | 18 |
| 90 | 0 | 15 | 14,5 |
| 120 | 2 | 15 | 16 |
| 150 | 1 | 15 | 17 |
| 180 | 2 | 15 | 14,5 |
| 210 | 2 | 15 | 17 |
| 240 | 2 | 15 | 18 |
| 270 | 1 | 15 | 14,5 |
| 300 | 1 | 15 | 16 |
| 330 | 1 | 15 | 18,5 |

Рассчитаем затухание в самой удаленной точке помещения для ТД 1 первого этажа:

 дБ,

Результаты расчётов вносим в таблицу 3.14

Таблица 3.14 - Результаты расчета

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Направление распространения, град | Расстояние R, м | Общие потери распространения, дБ | УМС, дБ | Прием |
| 1 | 2 | 3 | 4 | 5 |
| 0 | 17 | 73,15057 | -53,1506 | Уверенный |
| 30 | 18,5 | 74,63503 | -54,635 | Уверенный |
| 60 | 18 | 74,14704 | -54,147 | Уверенный |
| 90 | 14,5 | 70,51895 | -50,519 | Уверенный |
| 120 | 16 | 102,124 | -82,124 | Уверенный |
| 150 | 17 | 88,15057 | -68,1506 | Уверенный |
| 180 | 14,5 | 100,519 | -80,519 | Уверенный |
| Продолжение таблицы 3.14 | | | | |
| 210 | 17 | 103,1506 | -83,1506 | Уверенный |
| 240 | 18 | 104,147 | -84,147 | Уверенный |
| 270 | 14,5 | 85,51895 | -65,519 | Уверенный |
| 300 | 16 | 87,12399 | -67,124 | Уверенный |
| 330 | 18,5 | 89,63503 | -69,635 | Уверенный |

Как видно из расчетов, во всех точках уровень сигнала больше порогового, например в направлении 210º, уровень сигнала -83,15 дБм, это значительно больше порогового значения чувствительности приемника сетевого адаптера в ПК, равного -94 дБм, следовательно, та часть помещения, где расположена ТД, находится в зоне уверенного радиоприема.

Таблица 3.15- Данные для расчета зоны радиопокрытия ТД 2

|  |  |  |  |
| --- | --- | --- | --- |
| Направление распространения, град | Количество стен nст | Потери, при прохождении стены Lст, дБ | Расстояние R, м |
| 1 | 2 | 3 | 4 |
| 0 | 0 | 15 | 14,5 |
| 30 | 0 | 15 | 17 |
| 60 | 0 | 15 | 11 |
| 90 | 0 | 15 | 10 |
| 120 | 2 | 15 | 11,5 |
| 150 | 2 | 15 | 20 |
| 180 | 2 | 15 | 17 |
| 210 | 2 | 15 | 21,5 |
| 240 | 2 | 15 | 15 |
| 270 | 1 | 15 | 14,5 |
| 300 | 1 | 15 | 17 |
| 330 | 1 | 15 | 15,5 |

Рассчитаем затухание в самой удаленной точке помещения для ТД 2 первого этажа:

 дБ,

Результаты расчётов вносим в таблицу 3.16.

Таблица 3.16 - Результаты расчета

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Направление распространения, град | Расстояние R, м | Общие потери распространения, дБ | УМС, дБ | Прием |
| 1 | 2 | 3 | 4 | 5 |
| 0 | 14,5 | 70,51895 | -50,519 | Уверенный |
| 30 | 17 | 73,15057 | -53,1506 | Уверенный |
| 60 | 11 | 66,36945 | -46,3694 | Уверенный |
| 90 | 10 | 65,04159 | -45,0416 | Уверенный |
| 120 | 11,5 | 97,00555 | -77,0055 | Уверенный |
| 150 | 20 | 106,0622 | -86,0622 | Уверенный |
| 180 | 17 | 103,1506 | -83,1506 | Уверенный |
| 210 | 21,5 | 107,4404 | -87,4404 | Уверенный |
| 240 | 15 | 101,0634 | -81,0634 | Уверенный |
| 270 | 14,5 | 85,51895 | -65,519 | Уверенный |
| 300 | 17 | 88,15057 | -68,1506 | Уверенный |
| 330 | 15,5 | 86,59823 | -66,5982 | Уверенный |

Как видно из расчетов, во всех точках уровень сигнала больше порогового значения чувствительности приемника сетевого адаптера в ПК, равного -94 дБм, следовательно, та часть помещения, где расположена ТД, находится в зоне уверенного радиоприема.

На основе полученных результатов расчета можно утверждать, что для полного и наилучшего покрытия помещений, достаточно 2 точек доступа, пользователи, находящиеся на этом этаже находятся в зоне уверенного приема.

**3.1.4.3. Расчёт затухания на 3 этаже**

Для дальнейших расчётов необходимо знать количество и тип препятствий. Эти данные для третьего этажа представлены в таблице 3.17.

Расчёт затухания сигнала на третьем этаже провожу по формуле 3.2 без учёта количества этажей.



Таблица 3.17 - Данные для расчета зоны радиопокрытия ТД 1

|  |  |  |  |
| --- | --- | --- | --- |
| Направление распространения, град | Количество стен nст | Потери, при прохождении стены Lст, дБ | Расстояние R, м |
| 1 | 2 | 3 | 4 |
| 0 | 0 | 15 | 17 |
| 30 | 1 | 15 | 18,5 |
| 60 | 1 | 15 | 18 |
| 90 | 1 | 15 | 14,5 |
| 120 | 2 | 15 | 16 |
| 150 | 2 | 15 | 17 |
| 180 | 2 | 15 | 14,5 |
| 210 | 3 | 15 | 17 |
| 240 | 2 | 15 | 18 |
| 270 | 0 | 15 | 14,5 |
| 300 | 0 | 15 | 16 |
| 330 | 0 | 15 | 18,5 |

Рассчитаем затухание в самой удаленной точке помещения для ТД 1 первого этажа:

 дБ,

Результаты расчётов вносим в таблицу 3.18

Таблица 3.18 - Результаты расчета

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Направление распространения, град | Расстояние R, м | Общие потери распространения, дБ | УМС, дБ | Прием |
| 1 | 2 | 3 | 4 | 5 |
| 0 | 17 | 73,15057 | -53,1506 | Уверенный |
| 30 | 18,5 | 89,63503 | -69,635 | Уверенный |
| 60 | 18 | 89,14704 | -69,147 | Уверенный |
| 90 | 14,5 | 85,51895 | -65,519 | Уверенный |
| 120 | 16 | 102,124 | -82,124 | Уверенный |
| 150 | 17 | 103,1506 | -83,1506 | Уверенный |
| 180 | 14,5 | 100,519 | -80,519 | Уверенный |
| 210 | 17 | 103,1506 | -83,1506 | Уверенный |
| 240 | 18 | 104,147 | -84,147 | Уверенный |
| 270 | 14,5 | 70,51895 | -50,519 | Уверенный |
| 300 | 16 | 72,12399 | -52,124 | Уверенный |
| 330 | 18,5 | 74,63503 | -54,635 | Уверенный |

Таблица 3.19 - Данные для расчета зоны радиопокрытия ТД 2

|  |  |  |  |
| --- | --- | --- | --- |
| Направление распространения, град | Количество стен nст | Потери, при прохождении стены Lст, дБ | Расстояние R, м |
| 1 | 2 | 3 | 4 |
| 0 | 0 | 15 | 14,5 |
| 30 | 0 | 15 | 17 |
| 60 | 0 | 15 | 11 |
| 90 | 0 | 15 | 10 |
| 120 | 2 | 15 | 11,5 |
| 150 | 2 | 15 | 20 |
| 180 | 2 | 15 | 17 |
| 210 | 2 | 15 | 21,5 |
| 240 | 2 | 15 | 15 |
| 270 | 1 | 15 | 14,5 |
| 300 | 1 | 15 | 17 |
| 330 | 1 | 15 | 15,5 |

Рассчитаем затухание в самой удаленной точке помещения для ТД 2 третьего этажа:

 дБ,

Результаты расчётов вносим в таблицу 3.20.

Таблица 3.20 - Результаты расчета

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Направление распространения, град | Расстояние R, м | Общие потери распространения, дБ | УМС, дБ | Прием |
| 1 | 2 | 3 | 4 | 5 |
| 0 | 14,5 | 70,51895 | -50,519 | Уверенный |
| 30 | 17 | 73,15057 | -53,1506 | Уверенный |
| 60 | 11 | 66,36945 | -46,3694 | Уверенный |
| 90 | 10 | 65,04159 | -45,0416 | Уверенный |
| 120 | 11,5 | 97,00555 | -77,0055 | Уверенный |
| 150 | 20 | 106,0622 | -86,0622 | Уверенный |
| 180 | 17 | 103,1506 | -83,1506 | Уверенный |
| 210 | 21,5 | 107,4404 | -87,4404 | Уверенный |
| 240 | 15 | 101,0634 | -81,0634 | Уверенный |
| 270 | 14,5 | 85,51895 | -65,519 | Уверенный |
| 300 | 17 | 88,15057 | -68,1506 | Уверенный |
| 330 | 15,5 | 86,59823 | -66,5982 | Уверенный |

**3.1.4.4. Результаты расчёта**

Охватить все вероятные случаи распространения радиоволн не представляется возможным, по этому процесс определения модели распространения является творческим, а оценка входящих в них параметров должна основываться на результатах измерений. По произведенным расчетам можно сделать вывод о том, что покрытием обеспечивается 100% площади зданий. Таким образом, на мой взгляд, нет необходимости ставить дополнительные точки доступа.

* 1. **Расчет полосы пропускания для речевой информации**

Для расчета необходимой полосы пропускания для речевого трафика используем предложенную телефонную нагрузку предприятия . В таблице 3.21 представлена среднемесячная продолжительность исходящих междугородних телефонных разговоров.

Таблица 3.21 - Среднемесячная продолжительность телефонных разговоров

|  |  |
| --- | --- |
| Направление вызовов | Продолжительность, ч. |
| 1 | 2 |
| Салават | 200 |
| Туймазы | 180 |
| Чекмагуш | 150 |

Общая полоса пропускания, бит/с, определяется по формуле:

*F* = *nf*, (3.3)

где *n* – количество каналов;

*f* – полоса пропускания, необходимая для организации одного канала.

Для определения необходимой полосы пропускания для речевого трафика нужно найти необходимое количество каналов. Для этого необходимо найти интенсивность нагрузки в час наибольшей нагрузки (ЧНН).

Интенсивность нагрузки в ЧНН, Эрл, определяется по формуле:

 (3.4)

где *A* – общая продолжительность разговоров в месяц, ч;

*N* = 24 день – количество рабочих дней в месяце;

*m* = 0,19 – коэффициент концентрации нагрузки в ЧНН для офисных АТС.

Согласно статистике предприятия, ежемесячная продолжительность разговоров составляет 530 ч. Тогда интенсивность нагрузки в ЧНН будет равна



По таблице 3.22 Эрланга для обслуживания нагрузки с интенсивностью 4,19 с вероятностью блокировки 0,001 (рекомендуемой МСЭ) требуется 11 соединений.

Таблица 3.22 - Таблица Эрланга

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Количество каналов | Вероятность блокировки | | | |
| 0,001 | 0,005 | 0,01 | 0,05 |
| 1 | 0,003 | 0,005 | 0,011 | 0,053 |
| 2 | 0,055 | 0,106 | 0,153 | 0,382 |
| 3 | 0,123 | 0,349 | 0,456 | 0,9 |
| 4 | 0,4 | 0,702 | 0,87 | 1,525 |
| 5 | 0,653 | 1,132 | 1,361 | 2,219 |
| 6 | 1,274 | 1,622 | 1,909 | 2,961 |
| 7 | 1,654 | 2,158 | 2,501 | 3,738 |
| 8 | 2,484 | 2,73 | 3,128 | 4,543 |
| 9 | 3,053 | 3,333 | 3,783 | 5,371 |
| 10 | 3,648 | 3,961 | 4,462 | 6,216 |
| 11 | 4,267 | 4,611 | 5,16 | 7,077 |
| 12 | 4,904 | 5,279 | 5,876 | 7,95 |
| 13 | 5,559 | 5,964 | 6,608 | 8,835 |
| 14 | 5,982 | 6,664 | 7,352 | 9,73 |
| 15 | 6,712 | 7,376 | 8,108 | 10,63 |

Выбор кодека является определяющим для расчета полосы пропускания для организации одного канала. В таблице 3.23 приведены параметры основных стандартов кодеков, используемых в VoIP.

Таблица 3.23 – Параметры различных стандартов кодеков

|  |  |  |  |
| --- | --- | --- | --- |
| Кодек | Полоса пропускания, бит/с | Размер голосового кадра, байт | Оценка MOS (в идеальных условиях) |
| G.711 | 64 000 | 240 | 4,45 |
| G.711 | 64 000 | 160 | 4,45 |
| G.726r32 | 32 000 | 120 | 4,3 |
| G.726r32 | 32 000 | 80 | 4,3 |
| G.729 | 8 000 | 40 | 4,04 |
| G.729 | 8 000 | 20 | 4,04 |

Факторами, которые также необходимо учитывать при расчете полосы пропускания, являются размеры заголовков протоколов различных уровней. Протоколы, используемые для передачи VoIP перечислены в таблице 3.24.

Заголовок сетевого уровня и заголовок транспортного уровня, заголовки сетевого и транспортного уровней определяются следующими протоколами: IP, UDP , RTP. Информация, содержащаяся в этих заголовках, равняется 40 байтам.

При использовании технологии Ethernet объем информации второго уровня равен 18 байтам (МАС-адрес отправителя (6 байт), МАС-адрес получателя (6 байт), поле определения типа фрейма (2 байта) и проверочная комбинация (4 байта)).

Суммарный размер заголовков составляет 58 байт. Значения требуемой пропускной способности с учетом размеров заголовков для различных кодеков указаны в таблице 3.24

Таблица 3.24 – Параметры различных стандартов кодеков

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Кодек | Размер голосового кадра, байт | Размер посылки (с учетом заголовков), байт | Количество кадров в секунду, кадры | Полоса пропускания, бит/с |
| G.711 | 240 | 298 | 33 | 78 700 |
| G.711 | 160 | 218 | 50 | 87 200 |
| G.726r32 | 120 | 178 | 33 | 47 000 |
| G.726r32 | 80 | 138 | 50 | 55 200 |
| G.729 | 40 | 98 | 25 | 19 600 |
| G.729 | 20 | 78 | 50 | 31 200 |

С увеличением размера кадра качество передачи речи снижается из-за добавляемой задержки, однако при этом сокращается количество служебной информации.

**4. Конструкторско-технологическая часть**

**4.1 Тестирование производительности сети для VoIP**

Беспроводные сети 802.11 («беспроводные LAN» или «WLAN») становятся все более популярными в корпоративной сетевой среде. Как следствие, их широкое распространение требует от них быть безопасными, гибкими в настройках и отвечать высоким требованиям производительности. В то же самое время, развертывание беспроводных сетей должно занимать мало времени и быть экономически выгодным. По этим причинам тестирование перед развертыванием WLAN - необходимый шаг, чтобы гарантировать беспрепятственную интеграцию новой инфраструктуры.   
Для беспроводных сетей существует большое число важных показателей, которым она должна удовлетворять; однако, ни один не более важен, чем тестирование безопасности перед развертыванием. Данный план тестирования направлен на проведение испытаний оборудования для беспроводных сетей и в частности VoIP, и уделяет особое внимание особенностям, обычно свойственным точкам доступа корпоративного уровня.

Этот план тестирования сосредоточен на проверке функциональных возможностей и производительности WLAN.

**4.1.1 Методика тестирования**

Предлагаемая испытательная методология заключается в настройке тестовой сети, существующей топологии, как показано на рисунке 3.1



Рисунок 3.1 – Топология теста

Необходимо выбрать функциональные оконечные точки, соответствующие операционной системе устройств, и установить одну функциональную оконечную точку (E1) на проводной стороне сети и другую оконечную точку (E2) на беспроводной стороне сети. Значение E1 и E2 может быть изменено. Однако надо отметить, что, если используется режим отчетов в реальном времени, E2 может создать дополнительную нагрузку на сеть RF, отсылая результаты во время выполнении тестов. Кроме того, результаты испытаний могут быть потеряны из-за процесса роуминга между точками доступа.

### Определение производительности сетей 802.11

Одним из основных точек отсчёта в тестировании является пропускная способность. В радиосреде 802.11 есть большое количество факторов (например, форма антенны, рассеивание, помехи), которые нужно учитывать при проведении оценочных испытаний эффективности различных устройств и сетей. Кроме того, стандарт IEEE 802.11 подразумевает различные значения скорости (например, 802.11b = 11 Мбит/с), которые важны при сравнении результатов. Из-за особенностей стандарта 802.11 (например, дополнительные данные в пакетах, таких как преамбулы, заголовки) максимальная производительность STA-уровня всегда - меньше чем пропускная способность link-уровня, частные случае которых приведены в таблице 3.1 и на рисунке 3.2.

Таблица 3.1 - пропускная способность некоторых стандартов 802.11

|  |  |  |  |
| --- | --- | --- | --- |
| Стандарты | Максимальная скорость соединения (Maximum Link Rate) | Максимальная скорость передачи TCP-пакетов (Maximum TCP Rate) | Максимальная скорость передачи UDP-пакетов (Maximum UDP Rate) |
| 1 | 2 | 3 | 4 |
| 802.11b | 11 Мбит/с, | 5.9 Мбит/с, | 7.1 Мбит/с, |
| 802.11g (with b) | 54 Мбит/с, | 14.4 Мбит/с | 19.5 Мбит/л |
| 802.11g (only) | 54 Мбит/с. | 24.4 Мбит/с. | 30.5 Мбит/с. |
| 802.11a | 54 Мбит/с, | 24.4 Мбит/с | 30.5 Мбит/с, |
| 802.11a | 108 Мбит/с | 42.9 Мбит/с | 54.8 Мбит/с |

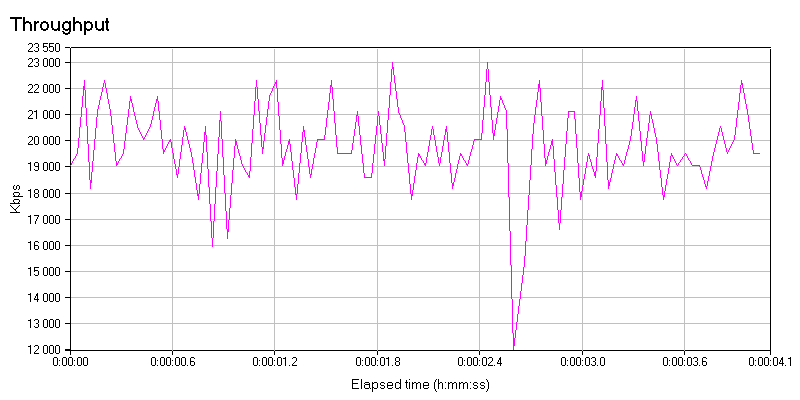


Рисунок 3.2 – пропускная способность стандарта 802.11g

### Определение деградации качества голоса при увеличении нагрузки прикладным трафиком

Переход к VoIP обусловлен желанием использовать существующую сеть передачи данных и для трафика приложений и для передачи голосовых данных. Это означает, что эффективное тестирование производительности VoIP не может быть сделано в условиях изоляции, так как не так много сетей передают только VoIP. Часто при добавлении нагрузочного трафика , например передачи данных, отражается на качестве голосовых данных. Необходимые условия предъявляемые к VoIP :

* чувствительность к задержкам ≤ 150 мс
* чувствительность к джиттеру ≤ 30 мс
* чувствительность к потери пакетов ≤ 1%

**Методология теста:**

Установив серию VoIP пар (35 пар). Запустили тест и проверили показатели VoIP, такие как Lost Data, Jitter. На рисунке 3.2 показан уровень потери данных для чистой VoIP.

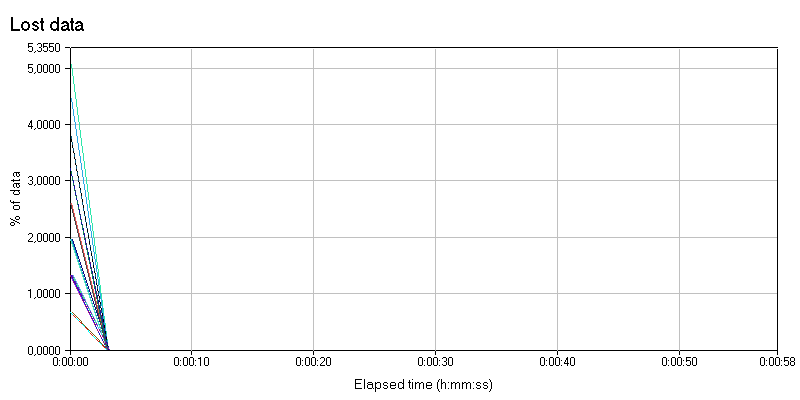


Рисунок 3.3 – показатели потери данных

После добавили нагрузочный трафик приложений . Выполнили тест и определите новые показатели VoIP. На рисунке 3.4 явно наблюдаются потери данных для VoIP пакетов выше допустимого уровня.

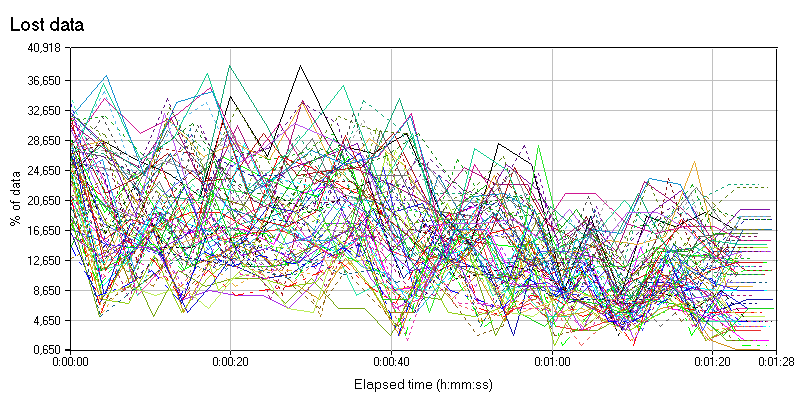


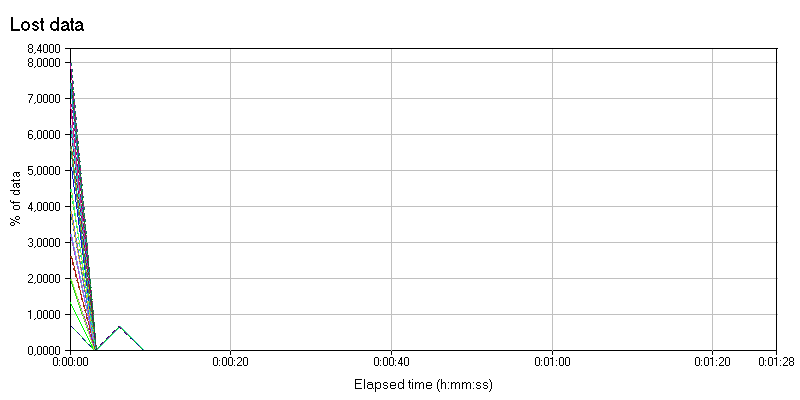
Рисунок 3.4 – Показатели потери данных VoIP пакетов при добавлении нагрузочных приложений.

**4.1.2** **Анализ воздействия установки приоритета на VoIP трафик**

Значимость и QoS-чувствительность пакетированных голосовых данных вызвала широкое распространение использования VoIP QoS механизмов на многих предприятиях, в различных правительственных сетях. Настройка параметров качества в сетях позволяет измерить и качественные усовершенствования от применения QoS относительно не-QoS, и так же определить влияние приоретизации VoIP трафика на работу существующих приложений.

В нашем случае мы настроили QoS точки доступа с приоритетом для VoIP пакетов.

Запустили тот же тест с серией VoIP пар (35 пар) и прикладным трафиком. Проверили показатели VoIP, такие как Lost Data, Jitter. Уровень потери данных с настройкой QoS очевидно понизился до допустимого значения. Это можно пронаблюдать на рисунке 3.5.



Рисунке 3.5 – показатель уровня потери данных

Исходя из вышеизложенного, можно заключить, что при организации  
контроля качества услуг с приоритетом для голосового трафика осуществляются необходимые параметры качества сети. Более подробные графики можно увидеть на плакатах.

Конфигурации настройки CallManagera и QoS для точки доступа приведены в Приложении Б и В.

**5. Технико-экономическое обоснование проекта**

В данном дипломном проекте рассматривается построение беспроводной сети стандарта IEЕЕ 802.11 на территории НПУ ОАО «Связьтранснефть». Задачами проекта являются, связать большое количество стационарных и портативных компьютеров, заменить старые коммутаторы ПЛС на современные, обеспечить резервирование, для надежности и облегчения работы персонала офиса, осуществить передачу голоса по беспроводным локальным сетям для налаживания оперативной и экономичной связи между своими сотрудниками. Обеспечить всему персоналу этой локальной сети высокоскоростной доступ в мировую сеть Internet.

В настоящее время, беспроводные сети становятся всё популярнее. Использование беспроводной технологии передачи данных Wi-Fi позволяет избавиться от большого количества проводов, улучшится качество связи в помещениях, где GSM-сигналы слабые, а сигналы Wi-Fi, напротив, достаточно сильны. Системы беспроводной связи позволяют повысить производительность, оперативность, мобильность работы, а также позволяют подключать новых абонентов, без затруднений.

При анализе целесообразности, данный проект следует рассматривать как некоммерческий продукт в том смысле, что он не предназначен для продажи с целью получения прибыли. Это упрощение сделано для того, чтобы показать прибыльность внедрения беспроводной сети связи, где ценность сети определяется сэкономленными ею средствами.

Экономическая целесообразность внедрения проекта заключается в экономии средств предприятия:

- обеспечение услуг телефонии на базе сети передачи данных позволяет избавиться от необходимости эксплуатации раздельных сетей для передачи данных и телефонной связи;

- уменьшаются расходы на замену, прокладку новых проводных линий;

- появится собственная беспроводная сеть.

**5.1. Расчет капитальных вложений**

Капитальные расходы – это расходы, связанные с покупкой необходимого оборудования для организации беспроводной системы связи и монтажных работ по установке оборудования. Также к ним относятся расходы, связанные с покупкой лицензии (при необходимости) и дополнительным обучением технического персонала.

В проектируемой сети капитальные вложения сокращены, это связано с отсутствием необходимости подготовки кадров, и отсутствием затрат на строительство и реконструкцию помещения, так как оборудование будет располагаться в уже существующем здании, пригодном, для размещения данного оборудования. Беспроводная сеть работает в не лицензируемом диапазоне частот 2,4 ГГц, поэтому покупка лицензии также не требуется.

Объем капитальных расходов, связанных с покупкой оборудования, стоимость монтажных и строительных работ приведены в таблицах 5.1 и 5.2. Стоимость оборудования и работ приняты на основе данных, полученных в ходе преддипломной практики.

Таблица 5.1 - Затраты на оборудование

|  |  |  |  |
| --- | --- | --- | --- |
| Наименование оборудования | Количество, шт | Стоимость, руб | Сумма, руб |
| 1 | 2 | 3 | 4 |
| Cisco Aironet 1230 (802.11abg) | 14 | 18 396 | 257 544 |
| Коммутатор Сisco Catalyst 2960 24 LAN | 9 | 30 984 | 278 856 |
| Кабель «витая пара» | 500 | 6 | 3 000 |
| Маршрутизатор Cisco 2801 Voice Bundle | 1 | 96 378 | 96 378 |
| Cisco Aironet adapter 2.4 Ггц | 70 | 4 080 | 285 600 |
| Телефон Cisco IP Phone 7911G | 70 | 7 007 | 490 490 |
| Итого: |  |  | 1 411 268 |

Таблица 5.2 - Смета монтажных работ

|  |  |  |  |
| --- | --- | --- | --- |
| Наименование работ | Количество | Стоимость, руб. | Сумма, руб. |
| Монтаж точек доступа | 12 | 1160,0 | 13920 |
| Прокладка проводки и кабеля | 500 м | 100,0 | 50000 |
| Монтаж сервера и коммутатора | 5 | 3000 | 12000 |
| Итого: 75920 | | | |

Итак, затраты на станционные сооружения и оборудование составляют 1411270 рублей. На монтаж выделяется приблизительно 76 000 рублей. Всего капитальные затраты составят 1 487 270 рублей.

**5.2. Текущие расходы**

Текущие расходы компании - это расходы, связанные с эксплуатацией оборудования сети и его техническим обслуживанием, а именно:

- заработную плату персонала, непосредственно работающего с данным оборудованием;

- часть амортизационных отчислений, предназначенных на капитальный

ремонт;

- амортизационные отчисления по сопутствующим капитальным  
вложениям без учета затрат на доставку и монтаж, включаемых в балансовую

стоимость;

- затраты на техническое обслуживание и текущий ремонт;

- затраты на потребляемую энергию;

- затраты на материалы и запасные части.

**5.2.1. Расчет заработной платы**

Вследствие того, что имеется два здания, то на обслуживание сети будет задействовано два инженера. При вводе в эксплуатацию дополнительного оборудования заработная плата, которая высчитывается по формуле (5.1) персонала увеличится на 2 100 рублей.

Таким образом, годовая зарплата увеличится на

 (5.1)

где  – увеличение заработной платы всех работников;



отчисления на социальное страхование определяются по формуле (5.2):

 (5.2)

где Н – норматив отчислений на социальное страхование (26%).



**5.2.2. Расчет амортизационных отчислений**

Амортизационные отчисления – это процесс постепенного перенесения стоимости средств труда по мере их физического и морального износа на стоимость производимых с их помощью продукции, работ и услуг в целях аккумуляции денежных средств для последующего полного восстановления. Амортизационные отчисления производятся по установленным нормам амортизации, их размер устанавливается за определенный период по конкретному виду основных фондов (группе, подгруппе) и выражается, как правило, в процентах к их балансовой стоимости. Расчет величины амортизационных отчислений будем производить по формуле 5.3:

 [руб], (5.3)

где  – балансовая стоимость материальных активов;

tn – длительность периода амортизации, в нашем случае tn=1 месяц;

ta – срок амортизации.

Период амортизации точек доступа равен 10 годам.

1 411 268·1/120 = 11 760 тыс.руб

Период амортизации коммутаторов равен 7 годам.

 1 411 268·1/84 = 16 800 тыс.руб

Результаты расчета амортизационных отчислений приведены в таблице 5.3.

Таблица 5.3 - Результаты расчета амортизационных отчислений

|  |  |  |
| --- | --- | --- |
| Виды основных фондов | Срок службы, года | Амортизационные отчисления, руб |
| 1 | 2 | 3 |
| Точки доступа | 10 | 11 760 |
| Коммутаторы | 7 | 16 800 |

**5.2.3. Расчет затрат на оплату электроэнергии**

Затраты на оплату потребляемой от сети электроэнергии определяются по формуле 5.4:

 (5.4)

где N – потребляемая мощность, кВт/ч;

Тг – время работы объекта в год;

Сэл – тариф, за 1 кВт в час для предприятий.

Исходя из технических характеристик, для оборудования беспроводной сети получаем:

N=0,2 кВт/ч;

Тг=8760 часов;

Сэл=1,53 рубля.



Затраты на электроэнергию, при внедрении на предприятие беспроводной сети, увеличивается на 2680,56 рублей в год.

**5.2.4 Расчет затрат на уплату налога на имущество.**

Объектом данного налога являются основные средства предприятия, т.е. та инфраструктура, которую мы создали на этапе инвестирования, считаем этот налог с балансовой стоимости основных фондов. В нашем случае он будет равен:



эксплуатационные расходы сведены в таблицу 5.4.

Таблица 5.4 - Эксплуатационные расходы

|  |  |
| --- | --- |
| Наименование затрат | Сумма затрат, руб. |
| 1 | 2 |
| Заработная плата | 50 400 |
| Отчисления на социальное страхование | 14 364 |
| Затраты на электроэнергию | 2 681 |
| Амортизационные отчисления | 28 560 |
| Расходы на материалы и запасные части | 30 000 |
| Затраты на уплату налога на имущество | 28 225 |
| Итого: | 88 971,76 |

**5.3. Расчет показателей экономической эффективности капитальных вложений**

При внедрении беспроводной локальной сети, произойдет экономия по материалы. Ниже приведен расчет экономической эффективности использования разработки.

Показатели экономии эксплуатационных расходов при использовании беспроводной сети приведен в таблице 5.5.

Таблица 5.4 – сравнительный анализ проводной и беспроводной связи

|  |  |  |  |
| --- | --- | --- | --- |
| Наименование затрат | Единица измерения | (локальная сеть) | (беспроводная сеть) |
| 1 | 2 | 3 | 4 |
| Затраты на сетевое оборудование:  - switch\hub Cisco Catalyst 2960  - точка доступа Cisco Aironet 1200  - цена 1 шт.  Итого: | шт.  шт.  руб.  руб. | 35  -  30 984  1084440 | -  12  18 396  220428 |
| Затраты на провод:  - кабель витая пара (категория 5е)  - цена 1 бухты (500 м)  Итого: | м  руб.  руб. | 5х500  8500  42500 | -  -  - |
| Затраты на разъемы RJ-45:  - разъем  - цена 1 упаковки (100 шт.)  Итого: | шт.  руб.  руб. | 300  2000  6000 | -  -  - |
| Затраты на розетки RJ-45:  - розетки  - цена за единицу  Итого | шт  руб.  руб. | 150  84  12500 | -  -  - |
| Затраты на кабельные каналы:  - кабельные каналы  - цена 1 метра  Итого: | м  руб.  руб. | 2500  15  37500 | -  -  - |
| Затраты на проведение монтажных работ | руб. | 128000 | - |
| Всего расходы | руб. | 1310940 | 220428 |

Коэффициент эффективности капитальных вложений показывает величину ежегодного экономического эффекта, в нашем случае на экономии эксплуатационных затрат.

Коэффициент эффективности капитальных вложений (Ер) определяется по формуле 5.5:

, (5.5)

где  - экономия эксплуатационных расходов:

К – капитальные затраты на разработку.



Срок окупаемости капитальных затрат есть величина обратная коэффициенту экономической эффективности.

Расчетный срок окупаемости:

 года

Рассчитаем период окупаемости проектируемой сети, за счет средств сэкономленных на телефонной связи между филиалами компании. За минуту эфирного времени абонент обычной телефонной сети платит 4,90 рубля, а по услуге IP-телефонии 2,00 руб. По статистике среднее время междугородних звонков за один день составляет 20 минут. Рассчитаем сколько наговаривают сотрудники в течении месяца:

*Р1*=20\*4,90\*26=2548

*Р2*=20\*2,00\*26=1040

Экономия эксплуатационных расходов составит *Р1- Р2*=1508

Разделив капитальные затраты необходимые для осуществления проекта на 1508, получим 987 дней или 2,7 года.

На основании проделанных расчётов можно сделать вывод, что срок окупаемости беспроводной сети стандарта IEEE 802.11 на территории НПУ ОАО «Связьтранснефть» наступит менее чем через три года работы. Кроме того, замена старого оборудования, расширение и резервирование сети повышают надежность связи, как мобильной, так и передачи данных, благодаря чему будут сэкономлены огромные средства.

**6. Безопасность и экологичность проекта**

В рамках дипломного проекта осуществляется проектирование беспроводной локальной сети стандарта IEЕЕ 802.11 на территории НПУ ОАО «Связьтранснефть». Работа по обслуживанию данной системы сопровождается постоянным контактом с радиоэлектронными средствами, а также персональным компьютером.

В данном разделе осуществляется анализ вредных и опасных производственных факторов, степень их воздействия. Кроме того, в разделе описываются различные средства защиты, уменьшающие воздействия этих факторов на человека.

Для производственных процессов на территории помещения НПУ характерны следующие опасные и вредные производственные факторы:

* повышенное значение напряжения в электрической цепи, замыкание которой может произойти через тело человека, источниками опасности поражения электрическим током могут оказаться незаземленные электроустановки и оголенные провода;
* повышенный уровень электромагнитных излучений, источниками электромагнитных излучений могут быть высокочастотные генераторы, формирующие несущую частоту для передачи сообщений и непосредственно, передающие антенны;
* повышенный уровень шума на рабочем месте, источниками являются устройства ввода информации, системы вентиляции и кондиционирования;
* повышенная или пониженная температура воздуха рабочей зоны;
* пожарная опасность в помещении – неисправность электропроводки или электрооборудования;
* повышенный уровень статического электричества;
* недостаточная освещенность рабочего места.

**6.1. Идентификация и анализ опасных и вредных факторов**

**6.1.1. Повышенное значение напряжения в электрической цепи, замыкание которой может произойти через тело человека**

Источниками возможного поражения персонала электрическим током являются действующие электропитающие установки, оборудование беспроводной и проводной локальной сети включенное в сети переменного или постоянного тока.

Действие электрического тока на живую ткань носит разносторонний и своеобразный характер. Проходя через организм человека, электроток производит термическое, электролитическое, механическое и биологическое действия.

Электротравматизм по сравнению с другими видами производственного травматизма составляет небольшой процент, однако, по числу травм с тяжелым, и особенно летальным, исходом занимает одно из первых мест.

ГОСТ [12] устанавливает предельно допустимые напряжения прикосновения и токи, протекающие через тело человека при нормальном режиме работы электроустановок постоянного и переменного тока частотой 50 и 400 Гц. Допустимым считается ток, при котором человек может самостоятельно освободиться от электрической цепи.

Электробезопасность электрического оборудования и кабелей. Физическая сущность изоляции как средства защиты состоит в исключении возможности перемещения зарядоносителей по телу человека путем создания между ним и токоведущими частями или проводами, находящимися под напряжением, среды, обладающей надежно связанными зарядоносителями. То есть, это средство защиты либо исключает возможность соединения с телом человека элементов, обладающих любой проводимостью, либо ограничивает эту проводимость значением, при котором возникающее движение зарядоносителеи – электрический ток – не превышает значений, опасных для человека.

**6.1.2. Повышенный уровень электромагнитного излучения оборудования участка сети**

Источниками электромагнитных излучений могут быть высокочастотные генераторы, формирующие несущую частоту для передачи сообщений и непосредственно, передающие антенны.

Влияние электромагнитного излучения мониторов на здоровье пользователей ПЭВМ является одним из вредных факторов. Монитор, как электронно-лучевое устройство излучает свет в оптическом диапазоне и, помимо этого, является потенциальным источником электромагнитного излучения в диапазоне радиочастот, сверхнизких частот, а также ионизирующего воздействия и электростатических полей [12].

Степень и характер воздействия ЭМИ на организм определяются плотностью потока энергии, частотой излучения, продолжительностью воздействия, режимом облучения (непрерывный, прерывистый, импульсный), размером облучаемой поверхности, индивидуальными особенностями организма, наличием сопутствующих факторов.

В зависимости от частоты падающего электромагнитного излучения ткани организмов проявляют различные электрические свойства и ведут себя как проводник или как диэлектрик. Систематическое воздействие электромагнитных излучений, превышающих допустимые величины, может оказать неблагоприятные влияния на человека, выражающиеся в функциональных нарушениях нервной, эндокринной и сердечно-сосудистой систем.

Следует иметь в виду, что совершенствование мониторов за прошедшее с этого момента время, шло в сторону снижения выхода электромагнитного излучения.

По данным отечественных исследователей, возле монитора могут образовываться электромагнитные поля радиочастот (5-10 МГц), создаваемые системой модуляции луча. Наиболее высокая напряженность их электрического поля (сотни В/м) фиксируются на расстоянии 10-15 см от боковых, верхних и задних поверхностей дисплея. У экрана и клавиатуры на расстоянии 30-70 см, где находится оператор, эти значения не превышают 1 В/м (при нормируемых значениях для данного диапазона частот (30 В/м)).

Вблизи компьютера обнаруживаются также импульсные магнитные поля сверхнизкой (50-100 Гц) и низкой (15-53 кГц) частот, создаваемые системой вертикальной и горизонтальной развертки электронного луча (от единиц до десятков В/м).

Наиболее высокие значения составляющих электромагнитных полей фиксируются на расстоянии 10-15 см от боковых, верхних и задних поверхностей дисплея и в меньшей степени перед экраном.

Нормирование электромагнитных излучений радиочастоты проводится по [12] и [13].

**6.1.3. Опасность воздействия статических зарядов на человека**

Статическое электричество может причинять вред, как на производстве, так и в быту, так что зачастую с ним приходится бороться. Микроразряды возникают, когда человек ходит по полу, покрытому полимерным покрытием, или снимает синтетическую одежду.

Воздействие статического электричества на человека связано с протеканием через него слабого тока (несколько миллиампер). При этом электротравм никогда не наблюдается. Однако вследствие рефлекторной реакции на ток возможна механическая травма при ударе о рядом расположенные элементы конструкций, падение с высоты и т. д. Исследование биологических эффектов показало, что наиболее чувствительны к электростатическому полю центральная нервная система, сердечно-сосудистая система, анализаторы.

Кроме того, статическое электричество образуется и накапливается путем трения, когда предметы трутся друг о друга, передвигаются в сухом воздухе или отделяются один от другого.

Когда такое электричество исходит от предметов или людей, могут произойти разряды, которые вызывают неприятные ощущения, а в худших случаях повреждают чувствительное оборудование.

Нормирование уровней напряженности электростатического поля (ЭСП) осуществляется в соответствии с ГОСТом в зависимости от времени пребывания персонала на рабочих местах [15].

### 6.1.4. Недостаточная освещенность рабочей зоны

На рабочих местах используется как естественное, так и искусственное освещение. Применение одного местного освещения внутри зданий не допускается, так как образуются резкие тени, зрение быстро утомляется и создается опасность травматизма.

Освещение является одним из важнейших условий нормальной жизнедеятельности. Правильно устроенное освещение обеспечивает хорошую видимость и создает благоприятные условия труда. Неудовлетворительное освещение вызывает преждевременное утомление, притупляет внимание работающего, снижает производительность труда, ухудшает качественные показатели и может оказаться причиной несчастного случая. Неудовлетворительное освещение в течение длительного времени может также привести к ухудшению зрения.

**6.1.5. Повышенный уровень шума, создаваемый вспомогательным оборудованием участка сети**

Источниками шума на рабочем месте считаются: устройства ввода информации, системы вентиляции и кондиционирования.

Шум на производстве способствует снижению внимания и увеличению числа ошибок при выполнении работы. Сильный шум оказывает влияние на быстроту реакции, сбор информации и аналитические процессы, из-за шума снижается производительность труда и ухудшается качество работы.

Гигиеническое нормирование шума осуществляется в соответствии с [20] и Санитарными нормами [21].

**6.1.6. Опасность возникновения пожара**

Объекты должны иметь системы пожарной безопасности, направленные на предотвращение воздействия на людей опасных факторов пожара, в том числе их вторичных проявлений на требуемом уровне.

Требуемый уровень обеспечения пожарной безопасности людей с помощью указанных систем должен быть не менее 0,999999 предотвращения воздействия опасных факторов в год в расчете на каждого человека, а допустимый уровень пожарной опасности для людей должен быть не более 10-6 воздействия опасных факторов пожара, превышающих предельно допустимые значения, в год в расчете на каждого человека [22].

Объекты, пожары на которых могут привести к массовому поражению людей, находящихся на этих объектах и окружающей территории, опасными и вредными производственными факторами, а также опасными факторами пожара и их вторичными проявлениями, должны иметь системы пожарной безопасности, обеспечивающие минимально возможную вероятность возникновения пожара.

Опасными факторами, воздействующими на людей и материальные ценности, являются:

* пламя и искры;
* повышенная температура окружающей среды;
* токсичные продукты горения и термического разложения;
* дым;
* пониженная концентрация кислорода.

К вторичным проявлениям опасных факторов пожара, воздействующим на людей и материальные ценности, относятся:

* осколки, части разрушившихся аппаратов, агрегатов, установок, конструкций;
* радиоактивные и токсичные вещества и материалы, вышедшие из разрушенных аппаратов и установок;
* электрический ток, возникший в результате выноса высокого напряжения на токопроводящие части конструкций, аппаратов, агрегатов;
* опасные факторы взрыва, происшедшего вследствие пожара.

**6.2. Инженерное обеспечение безопасных условий труда**

Рассмотрим методы и мероприятия, которые обеспечат защиту сотрудников НПУ от опасных и вредных факторов.

**6.2.1. Защита от повышенного напряжения в электрической цепи и замыкания, которое может произойти через тело человека**

Повышение электробезопасности в установках достигаем путем применения систем защитного заземления, зануления, защитного отключения и других средств и методов защиты, в том числе знаков безопасности и предупредительных знаков и плакатов [22].

Надежность работы электрического оборудования зависит, прежде всего, от состояния изоляции токоведущих частей. Ее повреждение является основной причиной многих несчастных случаев. Обеспечение надежности изоляции в моей работе достигается за счет:

* правильного выбора материала изоляции и ее геометрии (толщина, форма), обусловленной в первую очередь значением рабочего напряжения и конструкцией оборудования;
* надежной профилактики в процессе работы;
* правильной оценки условий эксплуатации.

**6.2.2. Защита от электромагнитного излучения**

К организационным мероприятиям по защите от действия электромагнитных полей относятся:

1. Выбор режимов работы излучающего оборудования, обеспечивающих уровень излучения, не превышающий предельно допустимый.

2. Защита временем – применяется, когда нет возможности снизить интенсивность излучения в данной точке до предельно допустимого уровня. Путем обозначения, оповещения и т.п. ограничивается время нахождения людей в зоне выраженного воздействия электромагнитного поля. В действующих нормативных документах предусмотрена зависимость между интенсивностью плотности потока энергии и временем облучения.

3. Защита расстоянием – применяется, если невозможно ослабить воздействие другими мерами, в том числе и защитой временем. Метод основан на падении интенсивности излучения, пропорциональном квадрату расстояния до источника. Защита расстоянием положена в основу нормирования санитарно-защитных зон – необходимого разрыва между источниками поля и жилыми домами, служебными помещениями и т.п. Границы зон определяются расчетами для каждого конкретного случая размещения излучающей установки при работе её на максимальную мощность излучения. В соответствии с [14]

зоны с опасными уровнями излучения ограждаются, на ограждениях устанавливаются предупреждающие знаки с надписями: «Не входить, опасно!».

**6.2.3. Мероприятия по обеспечению необходимых параметров освещения в помещениях**

Так как основной персонал офиса большую часть рабочего времени проводит за компьютерами, необходимо, что бы каждое рабочее место было в достаточной степени освещено. Это достигается за счет установления в каждом кабинете офиса ламп и светильников.

Производственное освещение должно обеспечивать отсутствие в поле зрения работающего резких теней. Тени необходимо смягчать, применяя, например, светильники со светорассеивающими молочными стеклами.

В соответствие с [16], к системам производственного освещения предъявляются следующие требования:

* соответствие уровня освещенности рабочих мест характеру выполняемой зрительной работы;
* достаточно равномерное распределение яркости на рабочих поверхностях и окружающем пространстве;
* отсутствие резких теней, прямой и отраженной блеклости;
* постоянство освещенности во времени;
* оптимальная направленность излучаемого осветительными приборами светового потока.

**6.2.4. Мероприятия по защите от производственного шума**

Одним из наиболее простых и часто применяемых методов защиты от шума является звукопоглощение – применение пористых материалов, обладающих большим значением коэффициента поглощения, и звукоизоляция – уменьшение уровня шума с помощью защитного устройства, которое устанавливается между источником и приемником и имеет большую отражающую и (или) поглощающую способность.

**6.2.5. Методы по обеспечению пожаробезопасности**

* На каждом этаже должен быть план эвакуации при пожаре.
* На каждом этаже устанавливается по несколько огнетушителей и каждый сотрудник должен знать где они установлены.
* Проводятся проверки на износ электропроводки и электрооборудования.
* Проводятся беседы с персоналом офиса по их действию во время пожара.
* Отводятся специальные места для курения.

Автоматические установки пожаротушения (АУПТ) предназначены для своевременной ликвидации очагов возгорания при поступлении сигнала о пожаре в помещение с круглосуточным дежурством обслуживающего персонала (ПЭБ) [15].

Защита автоматическими установками газового пожаротушения подлежит оборудование связи, установленное на площадках НПУ.

Защищаемые помещения имеют небольшие объемы и достаточную герметичность. Эти условия дают возможность применить для тушения пожара систему газового объёмного пожаротушения модульного типа.

По определению ГОСТа [22], установка пожаротушения или противопожарная установка - это совокупность стационарных технических средств для тушения пожара за счет выпуска огнетушащего вещества.

Конструктивно автоматические установки пожаротушения состоят из резервуаров наполненных необходимым количеством огнетушащего состава, устройств управления и контроля, системы трубопроводов и насадков-распылителей. Количество распылителей, длины трубопроводов и объём емкостей для огнетушащего вещества определяются расчётами.  
Подразделяются системы автоматического пожаротушения, прежде всего, по используемому огнетушащему веществу:

* газовое пожаротушение (СО2, аргон, азот, фреоны);
* водяное пожаротушение (вода);
* пенное пожаротушение и водо-пенное пожаротушение (вода с пенообразователями);
* порошковое пожаротушение (порошки специального химического состава);
* аэрозольные системы пожаротушения (подобны порошкам, но частицы на порядок меньше по размерам);
* системы тонкодисперсной воды (тонкораспыленной воды).

В качестве газового огнетушащего вещества мы применяем двуокись углерода (СО2). Газ СО2 не агрессивен по отношению к защищаемому оборудованию и предназначен для использования при тушении пожаров класса А, В, С и электрооборудования, находящегося под напряжением.

Автоматические установки газового пожаротушения контейнеров-аппаратных «Север» выполнены на базе модулей газового пожаротушения высокого давления МГП-16-60, производства ЗАО «Артсок», г.Москва.

Для надежности работы установок газового пожаротушения необходимо предусмотреть мероприятия по максимальному предотвращению утечки СО2 во время тушения пожара (автоматическое закрытие вентиляционных отверстий и т.д.)

Нормативная объемная огнетушащая концентрация принята - 34,9% по объему защищаемых помещений.

Пуск установок происходит автоматически от электрических извещателей, путем срабатывания электромагнитных клапанов, расположенных на модулях, при подаче напряжения от блока управления на электромагнит.

Кроме автоматического пуска установки снабжены устройствами дистанционного и местного пуска.

Выпуск двуокиси углерода в объемы защищаемых помещений производится через насадки типа С-Р-В-14-3/8"-А с фильтром с распылением газового огнетушащего вещества на 3600. Насадки монтируются вертикально вниз.

**6.3 Расчет воздействия электромагнитного излучения на посетителей и сотрудников**

Рассчитаем мощность электромагнитного излучения, воздействующего на сотрудников участка сети. Источниками данного воздействия являются персональная ЭВМ и точка доступа модели Сisco Aironet 1200 (802.11g). характеристики оборудования приведены в таблице 6.

Таблица 6 - Характеристики оборудования

|  |  |  |  |
| --- | --- | --- | --- |
| Характеристика | ПЭВМ | Беспроводной IP Phone 7920 | Точка доступа Cisco Aironet 1200 |
| 1 | 2 | 3 | 4 |
| частота излучения | *fПЭВМ*≈70 МГц | *fБТ*≈2400 МГц | *fТД*≈2400 МГц |
| мощность излучения | *PПЭВМ*≈1 Вт | *PБТ*≈0,01 Вт | *PТД*≈0,1 Вт |
| расстояние от излучателя до точки измерения | *RПЭВМ≈*0,7 м  (в соответствии с ГОСТ) | *RБТ*≈0,02 м | *RТД* > 2 м |

Уровни допустимого воздействия электромагнитного поля на человека установлены [2]. Согласно данному ГОСТу, электромагнитные поля частот от 60 кГц до 300 МГц характеризуются напряженностями электрического Е(В/м) и магнитного Н(А/м) полей, а при частотах от 300 МГц до 300 ГГц характеризуются плотностью потока энергии.

Рассмотрим воздействие электромагнитного поля на оператора со стороны ПЭВМ.

Напряженность электромагнитного поля в диапазоне частот 60 кГц - 300 МГц на рабочих местах персонала в течение рабочего дня не должна превышать установленных предельно допустимых значений:

* по электрической составляющей: *ЕПДУ*=5 В/м;
* по магнитной составляющей: *НПДУ*=0,3 А/м.

При расчете величин *Е* и *Н* сначала определяем длину волны (*λ*, м) электромагнитного излучения:



где  – скорость распространения электромагнитной волны.

Далее определим радиус ближней зоны электромагнитного излучения, то есть зоны, где еще не сформирована электромагнитная волна:



Так как *R=r*, то расчет *Е* и *Н* необходимо производить для пограничной зоны. В этой зоне волновое сопротивление для электрической составляющей поля (*ZВЭ*) много меньше *Z0* (*Z0*=377 Ом).

В данном случае *ZВЭ*=1 Ом, а *ZВМ*=500 Ом.

Расчет напряженности электрического поля определяют по формуле 6.1:

 (6.1)

где  – плотность потока мощности.

Подставив данные в формулу (6.1), получаем:



расчет напряженности магнитного поля определяют по формуле 6.2:

 (6.2)

Таким образом получили, что *E < EПДУ* и *H < HПДУ.*

Следовательно, воздействие электромагнитного излучения на оператора со стороны ПЭВМ соответствует нормам.

Рассмотрим воздействие электромагнитного поля на оператора со стороны точки доступа и беспроводного IP-телефона.

Предельно допустимые значения ППЭ ЭМП в диапазоне частот 300 МГц - 300 ГГц следует определять исходя из допустимой энергетической нагрузки и времени воздействия по формуле 6.3:

 (6.3)

где  – предельно допустимое значение плотности энергии, Вт/м2;

 – предельно допустимая величина энергетической нагрузки,

равная 2 Вт · ч/м2 (200 мкВт · ч/см2);

*К* – коэффициент ослабления биологической эффективности, равный: 1 – для всех случаев воздействия, исключая облучение от вращающихся и сканирующих антенн; 10 – для случаев облучения от вращающихся и сканирующих антенн с частотой вращения или сканирования не более 1 Гц и скважностью не менее 50;

*Т* – время пребывания в зоне облучения за рабочую смену, ч.

Во всех случаях максимальное значение не должно превышать 10 Вт/м2 (1000 мкВт/см2).

В диапазоне частот 300 МГц – 300 ГГц интенсивность ЭМП характеризуется поверхностной плотностью потока энергии (далее плотность потока энергии – ППЭ), энергетическая нагрузка представляет собой произведение плотности потока энергии поля на время его воздействия, как показано в формуле 6.4:

*ЭНППЭ = ППЭ⋅Т*, (6.4)

Плотность потока энергии для точечного источника равнонаправленного действия на рабочем месте определяют следующим образом:

Для точки доступа



Для беспроводного телефона



где *Р* – мощность ТД, Вт;

*R* – расстояние от источника электромагнитного поля до пользователя, м.

Подставив данные в формулу 6.4, получаем:

*ЭНППЭтд* =0,00199⋅8=0,0159 Вт⋅ч/м2.

*ЭНППЭбт* =1,99⋅1=1,99 Вт⋅ч/м2

Подставив данные в формулу 6.3, получаем:





Что значительно меньше нормы в 10 Вт/м2. В разделе выявлены опасные и вредные факторы при техническом обслуживании БЛС. Проведен анализ противопожарных мероприятий. В работе проведен расчетвоздействия электромагнитного излучения на посетителей и сотрудников. В результате проведённых расчётов было доказано, что от точки доступа, работающей на максимально возможной мощности, в течении 8 часов, обслуживающий персонал и клиенты не будут подвергать опасности своё здоровье, а также влияние беспроводного телефона, не превышает нормы .Это обеспечит безопасность сотрудников и пользователей, если к тому же будут соблюдаться условия, описанные в ГОСТах: [12,13, 14, 15, 16, 17,18, 19,20, 21,22 ]. При использовании предложенных мероприятий, улучшатся условия труда, и они будут соответствовать нормативным требованиям.

**Заключение.**

Спроектированная беспроводная локальная сеть стандарта IEEE 802.11 удовлетворяет всем поставленным требованиям. При реализации этой сети мы получим:

* высокую надежность локальной сети;
* удобство обслуживания;
* возможность персоналу мобильно и быстро подключаться к сети;
* обмен данными производится на скорости до 10 Мбит/с;
* качественная и дешевая телефонная связь.

Реальная ценность технологии VoIP для предприятия будет заключаться не только в снижении расходов на оплату междугородных и международных телефонных разговоров, но и в уменьшении затрат на сетевое администрирование при одновременном повышении эффективности и продуктивности труда. Система также безопасна для рабочего персонала офиса и посетителей, потому что является маломощной, и действует на ограниченном пространстве.

**Список использованных источников**

1. GALAXY Communications Радиотехнологии будущего - <http://www.senao-engenius.ru/index.php?id=4>
2. The IEEE 802.11 Working Group on Broadband Wireless Access Standards - http://www.ieee802.org/11/
3. Symbol Technologies - http://www.shtrih-center.ru/index.html.
4. WIRELESSRU Сетевое оборудование - <http://www.wireless.ru:80/wireless>
5. Беспроводные сети - <http://www.comptek.ru/wireless/aironet/air1300.html>.
6. Все о Wi-Fi - http://www.wi-fi.ru/s.php/234.htm
7. Ерохин Г.А., Чернышев О.В. Антенно-фидерные устройства и распространения радиоволн. – М.: Радио и связь, 1996. – 352с.
8. Князев А.Д. Элементы теории и практики обеспечения электромагнитной совместимости радиоэлектронных средств. – М.: Радио и связь, 1984. – 336с.
9. Ратынский М.В. Основы сотовой связи. – М.: Радио и связь, 1996. – 245с.
10. Мухин А.М. Энциклопедия мобильной связи. Том 1. – СПб : Наука и техника, 2001. – 235с.
11. Маковеева М.М. Системы связи с подвижными объектами. – М.: Радио и связь, 2002. – 440с.
12. ГОСТ 12.1.038-82 ССБТ (с изменениями от 01.07.88) «Электробезопасность. Предельно допустимые уровни напряжений прикосновения и токов».
13. ГОСТ 12.1.006-84 ССБТ «Электромагнитные поля радиочастот. Общие требования к безопасности».
14. ГОСТ 12.1.026-84 ССБТ «Электромагнитные поля радиочастот. Общие требования к безопасности».
15. ГОСТ 12.1.045-84 ССБТ «Электростатические поля. Допустимые уровни на рабочих местах и требования к проведению контроля».
16. СНиП 23-05-95 «Естественное и искусственное освещение».
17. ГОСТ 12.2.007-75 ССБТ «Изделия светотехнические. Требования безопасности».
18. ГОСТ 12.1.005-88 (2001) ССБТ «Общие санитарно-гигиенические требования к воздуху рабочей зоны»
19. СанПиН 2.2.4.548-96 «Гигиенические требования к микроклимату производственных помещений»
20. ГОСТ 12.1.003-83 ССБТ с дополнениями 1989 года «Шум. Общие требования безопасности».
21. СН 2.2.4./2.1.8.562-96 «Шум на рабочих местах, в помещениях жилых, общественных зданий и на территории жилой застройки».
22. ГОСТ 12.1.006-76 ССБТ «Электромагнитные поля радиочастот. Общие требования безопасности».

# Приложение А

## Характеристики типов стен

|  |  |  |
| --- | --- | --- |
| Тип стены | Среднее значение ослабления, дБ | Условное обозначение |
| Кирпичная стена 120мм. | 9 | 1 |
| Кирпичная стена 380мм. | 12 | 2 |
| Армированное стекло | 8 | 3 |
| Железобетонная стена (проёмы есть) | 17 | 4 |
| Железобетонная стена (проёмов нет) | 30 | 5 |
| Деревянная стена | 6 | 6 |

## Характеристики типов помещений

|  |  |  |
| --- | --- | --- |
| Тип здания | Погонное затухание , дБ/м | Пример |
| Старые здания | 0.7 | Жилые здания |
| Коммерческие | 0.5 | Современные офисы |
| Атриум | 0.2 | Музеи, ж/д вокзалы |

# Приложение Б

**Конфигурация настройки CallManagerа.**

*sh start*

*Using 1936 out of 245752 bytes*

*version 12.4*

*service timestamps debug datetime msec*

*service timestamps log datetime msec*

*no service password-encryption*

*hostname Router*

*boot-start-marker*

*boot-end-marker*

*no aaa new-model*

*resource policy*

*ip subnet-zero*

*ip cef*

*no ip dhcp use vrf connected*

*ip dhcp pool ITS*

*network 172.16.0.0 255.255.255.0*

*option 150 ip 172.16.0.1*

*default-router 172.16.0.1*

*voice-card 0*

*no dspfarm*

*interface FastEthernet0/0*

*no ip address*

*shutdown*

*duplex auto*

*speed auto*

*interface FastEthernet0/1*

*ip address 172.16.0.1 255.255.255.0*

*duplex auto*

*speed auto*

*interface Serial0/0/0*

*no ip address*

*shutdown*

*clock rate 125000*

*interface Serial0/0/1*

*no ip address*

*shutdown*

*clock rate 125000*

*interface Serial0/1/0*

*no ip address*

*shutdown*

*clock rate 125000*

*interface Serial0/1/1*

*no ip address*

*shutdown*

*clock rate 125000*

*ip classless*

*no ip http server*

*no ip http secure-server*

*control-plane*

*voice-port 0/2/0*

*voice-port 0/2/1*

*voice-port 0/3/0*

*voice-port 0/3/1*

Продолжение приложения Б

*telephony-service*

*max-ephones 10*

*max-dn 10*

*ip source-address 172.16.0.1 port 2000*

*auto assign 1 to 10*

*create cnf-files version-stamp Jan 01 2002 00:00:00*

*max-conferences 8 gain -6*

*transfer-system full-consult*

*ephone-dn 1*

*number 0001*

*ephone-dn 2*

*number 0002*

*ephone-dn 3*

*number 0003*

*ephone-dn 4*

*number 0004*

*ephone-dn 5*

*number 0005*

*ephone-dn 6*

*number 0006*

*ephone-dn 7*

*number 0007*

*ephone-dn 8*

*number 0008*

*ephone-dn 9*

*number 0009*

*ephone-dn 10*

*number 0010*

*ephone 1*

*mac-address 001E.4A92.A439*

*type 7940*

*button 1:1*

*ephone 2*

*mac-address 0040.96B5.DE13*

*type CIPC*

*button 1:2*

*ephone 3*

*ephone 4*

*ephone 5*

*ephone 6*

*ephone 7*

*ephone 8*

*ephone 9*

*ephone 10*

*line con 0*

*line aux 0*

*line vty 0 4*

*login*

*scheduler allocate 20000 1000*

*end*

# Приложение В

**Конфигурация настройки QoS точки доступа**

**с приоритетом VoIP пакетов.**

*Building configuration...*

*Current configuration : 2606 bytes*

*version 12.3*

*no service pad*

*service timestamps debug datetime msec*

*service timestamps log datetime msec*

*service password-encryption*

*hostname ap*

*enable secret 5 $1$1l8I$2p5wvSBQGAkUaSK8Xdlf..*

*ip subnet-zero*

*no aaa new-model*

*dot11 ssid tsunami*

*authentication open*

*guest-mode*

*dot11 phone*

*username Cisco password 7 062506324F41*

*class-map match-all \_class\_video\_policy0*

*match ip precedence 1*

*class-map match-all \_class\_video\_policy1*

*match ip dscp cs7*

*class-map match-all \_class\_VoWLAN0*

*match ip protocol 119*

*policy-map VoWLAN*

*class \_class\_VoWLAN0*

*set cos 6*

*policy-map video\_policy*

*class \_class\_video\_policy0*

*set cos 5*

*class \_class\_video\_policy1*

*set cos 5*

*bridge irb*

*interface Dot11Radio0*

*no ip address*

*service-policy input VoWLAN*

*service-policy output VoWLAN*

*no ip route-cache*

*ssid tsunami*

*traffic-stream priority 5 sta-rates nom-5.5 nom-6.0 nom-11.0 nom-12.0 nom-24.0 nom-54.0*

*speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0*

*power client 50*

*power local cck 50*

*power local ofdm 30*

*packet max-retries 3 0 fail-threshold 100 500 priority 5 drop-packet*

*packet max-retries 3 0 fail-threshold 100 500 priority 6 drop-packet*

*station-role root*

*dot11 qos class background local*

*cw-min 6*

*fixed-slot 10*

*dot11 qos class best-effort local*

*cw-min 4*

*dot11 qos class video local*

Продолжение приложения В

*cw-min 3*

*cw-max 5*

*fixed-slot 3*

*transmit-op 0*

*admission-control*

*admit-traffic signaling infinite*

*dot11 qos class voice local*

*cw-min 2*

*cw-max 4*

*transmit-op 0*

*dot11 qos class background cell*

*cw-min 8*

*fixed-slot 12*

*dot11 qos class best-effort cell*

*cw-min 6*

*dot11 qos class video cell*

*cw-min 4*

*cw-max 6*

*fixed-slot 5*

*transmit-op 0*

*admission-control*

*dot11 qos class voice cell*

*cw-min 2*

*cw-max 4*

*transmit-op 0*

*bridge-group 1*

*bridge-group 1 subscriber-loop-control*

*bridge-group 1 block-unknown-source*

*no bridge-group 1 source-learning*

*no bridge-group 1 unicast-flooding*

*bridge-group 1 spanning-disabled*

*interface FastEthernet0*

*no ip address*

*service-policy output VoWLAN*

*no ip route-cache*

*duplex auto*

*speed auto*

*bridge-group 1*

*no bridge-group 1 source-learning*

*bridge-group 1 spanning-disabled*

*interface BVI1*

*ip address 172.16.0.210 255.255.0.0*

*no ip route-cache*

*ip http server*

*no ip http secure-server*

*bridge 1 route ip*

*line con 0*

*line vty 0 4*

*end*