Тип работы: Дипломная работа

Предмет: Сети и системы связи

Введение

Актуальность данной темы обусловлена тем, что в настоящее время развитие информационных технологий предполагает необходимость использования коммуникационных систем для решения различных прикладных задач. Так, широкое использование получают системы электронного документооборота, технологии сдачи отчетности через Интернет. Обеспечение совместного доступа к информационным ресурсам является необходимым стандартом функционирования информационных систем и решения задач по защите информации.
В рамках данной работы проведено рассмотрение вопросов проектирования беспроводной сети для организации, оказывающей услуги Интернет-провайдера. Специфика локальных использования вычислительных сетей в условиях Интернет-провайдеров связана с особенностями архитектуры, что предполагает помимо компьютеров, серверов, принтеров наличие также коммуникационного оборудования, использующего ресурсы сети, а также необходимость интеграции удаленных площадок в единую систему.
В качестве критериев эффективности использования ресурсов вычислительной сети можно рассматривать повышение скорости передачи данных, оптимизацию работы приложений, сокращение затрат на обслуживание автоматизированной информационной системы, при этом необходимо обеспечивать соответствие существующим, а также перспективным бизнес-технологиям, учет возможности расширения и перестройки системы к использованию систем нового поколения.
Основу информационной системы составляют вычислительные системы, включающие такие компоненты, как кабельные сети, элементы активного, условно-активного и пассивного сетевого оборудования, компьютерного и периферийного оборудования, оборудования для хранения данных (библиотеки), системного программного обеспечения (операционные системы, СУБД), специализированное ПО (системы мониторинга и сетевого администрирования) и в некоторых случаях прикладные системы.
Наиболее распространенный подход к проектированию информационных систем в настоящее время связан с использованием метода экспертных оценок. В соответствии с данным подходом специалисты в области вычислительных средств, разработчики активного сетевого оборудования и кабельных сетей на основании имеющегося у них опыта и экспертных оценок проводят проектирование вычислительных систем,

обеспечивая решение конкретной задачи или класса задач. Данный подход позволяет сократить затраты на стадии проектирования, быстро оценивать стоимость развертывания информационных систем. При этом решения, полученные с использованием метода экспертных оценок, носят субъективный характер, требования к оборудованию и программному обеспечению также субъективны, как и оценка гарантий работоспособности и развиваемости предлагаемого проекта системы.
Развертывание корпоративных сетей в условиях средних и крупных дает возможности осуществлять централизацию управления информационными ресурсами, реализовывать единые административные политики и политики безопасности, что обеспечивает выполнение требований к безопасности информационной системы.
Объект исследования – ООО "Интерзет".
Предмет исследования – беспроводные применяемые в работе ООО "Интерзет".
Целью данной работы является разработка беспроводной сети для ООО "Интерзет".
Задачи работы:
- провести анализ физических принципов функционирования беспроводных сетей;
- провести анализ основных моделей доступа к сетевым ресурсам посредством беспроводных сетей;
- провести анализ параметров использования сетевых технологий в прикладных задачах, нагрузки на сеть;
- провести анализ деятельности ООО "Интерзет";
- провести анализ локальной вычислительной сети ЛВС ООО "Интерзет"
- провести анализ архитектуры системы информационной безопасности;
- разработать проект беспроводной сети вычислительной сети ООО "Интерзет";
- провести расчет экономической эффективности проекта внедрения беспроводной сети ООО "Интерзет".
Метод исследования – изучение научной и технической литературы по исследуемой тематике, математические методы, а также использование программ – эмуляторов вычислительных сетей.
Результаты работы могут быть применены при построении локальных сетей небольших организаций.
Работа включает: введение, четыре главы, заключение и список использованной литературы.

1. Теоретические аспекты обеспечения сетевой безопасности

1.1. Описание существующих технологий построения беспроводных сетей

В рамках данной работы рассматривается проект совершенствования системы обеспечения сетевой безопасности на примере использования беспроводных технологий. Рассмотрим теоретические аспекты функционирования беспроводных сетей.
Беспроводные технологии в настоящее время получили широкое развитие как в связи с доступностью использования сетевого оборудования данного класса, так и широким распространением мобильных устройств. Также к классу беспроводных технологий относятся технологии доступа, предоставляемые мобильными и спутниковыми операторами.
Основными направлениями использования беспроводных технологий являются:
• технологии складского учета в части проведения инвентаризации остатков, а также обеспечения связи между офисом и складами;
• больницы, санатории, дома отдыха;
• выставочные комплексы и конференц-залы;
• доступ к сети Интернет в гостиницах, кафе, библиотеках, студенческих городках и т.д.;
• реализация гостевого доступа в офисах компаний;
• использование беспроводного доступа в учебных целях.
Одной из основных характеристик беспроводных сетей является дальность ее приема. По дальности действия беспроводные системы принято классифицировать на следующие виды [3]:
- локальные интерфейсы с короткодействующим сигналом (Bluetooth);
- домашние и офисные сети (Wi-Fi);
- региональные городские сети (WiMAX, Mobile Broadband Wi-Fi Access);
- глобальные сети (технологии с максимальной дальностью беспроводной передачи данных на основе использования радиорелейных, сотовых и спутниковых технологий).
В рамках данной работы рассматриваются технологии безопасности беспроводных сетей класса Wi-Fi и Wi-Max, так как именно данные технологии используются в локальной сети СибГУТИ.
Далее приведём обзор наиболее распространенных стандартов беспроводных сетевых технологий.

1. Стандарт 802.11

Разработка данного стандарта приходится на период с 1990 по 1997 годы как результат работы одной из рабочих групп Institute Electrical Equipment Engineering (IEEE). В настоящее время наиболее часто используемыми стандартами данного типа являются 802.11a, 802.11b и 802.11g.

Стандарт IEEE 802.11a был принят в 1999 году и был ориентирован на функционирование в диапазоне частот 5 ГГц и рассчитан на скорость передачи данных до 54 Мбит/с. Диапазон включает две частотные полосы общей шириной 300 МГц, первая из которых 5,15-5,35 ГГц, вторая лежит в диапазоне 5,725-5,825 ГГц. Первая полоса имеет разделение на две полосы по 100 МГц. Таким образом, для реализации возможности передачи данных используются три не перекрывающихся между собой частотных канала по 100 МГц, каждый из которых имеет ограничения по мощности сигнала - 50 мВт в «нижнем» диапазоне, 250 мВт в «среднем» и до 1 Вт в «верхнем». Стандарт 802.11a основан на методике кодирования ортогонального частотного мультиплексирования. Разделение передачи данных по нескольким «несущим» частотам приводит к возможности снижения скорости передачи на каждой из них, что в свою очередь предполагает достаточную защищённость от помех и достижение достаточно высокой пропускной способности.

Стандарт IEEE 802.11b известен по наименованию - Wi-Fi (Wi-Fi Fidelity) также был принят в 1999 году, и его появление положило основу повсеместному распространению беспроводных сетевых технологий в локальных сетях предприятий, а также для реализации доступа к сети Интернет. Данный стандарт предусматривает использование технологии широкополосной модуляции с расширением спектра методом прямой последовательности, как обеспечивающей более стабильное функционирование сети в условиях многократного отражения радиосигналов со скоростью до 11 Мбит/с. При этом применяется метод расширения спектра на основе кодирования с использованием комплементарных кодов, что позволяет реализовать кодирование 8 бит на один символ при скорости передачи данных 11 Мбит/с.

Стандарт IEEE 802.11g был принят в середине 2003 года, как совершенствование стандарта 802.11b. Данный стандарт также использует частотный диапазон 2,4 ГГц, но при этом совместно с технологией мультиплексирования (OFDM) и алгоритмами псевдослучайной скачкообразной перестройки рабочих частот (Frequency Hopping Spread Spectrum - FHSS). Данное совершенствование обеспечивает увеличение скорости передачи информации до 54 Мбит/с. Аппаратное обеспечение технологий 802.11g и 802.11b совместимо, что обеспечивает возможность одновременного подключения к сети устройств, использующих стандарты IEEE 802.11g и IEEE 802.11b. Величина мощности устройств данного типа имеет порядок 10-100 мВт.

Основные технические характеристики стандартов беспроводных технологий приведены в таблице 1.1.

Таблица 1.1 - Сравнительные характеристики стандартов беспроводных технологий

Стандарт/ Характеристика	IEEE 802.11a	IEEE 802.11b	IEEE 802.11g
Физические основы связи	Расширение спектра (скачкообразная перестройка частоты - FHSS)	Расширение спектра (прямая последовательность DSSS)	Расширение спектра (скачкообразная перестройка частоты - FHSS)
Частотные диапазоны	Две полосы частот: 5,15-5,35 ГГц и 5,725-5,825 ГГц	От 2,4 до 2,4835 ГГц	От 2,4 до 2,4835 ГГц
Мощность передачи	50 мВт, 250 мВт, 1000 мВт	100 мВт, 500 мВт	10-100 мВт
Скорость передачи данных	Три обязательные (6, 12 и 24 Мбит/с) и пять дополнительных (9, 18, 24, 48 и 54 Мбит/с)	До 11 Мбит/сек	До 54 Мбит/сек
Дальность	До 300 метров на открытом пространстве	До 100 метров	100 – 300 метров
Ограничение на количество устройств в сети	Теоретически до 255 устройств на одну точку доступа; несколько точек доступа в сети	Теоретически до 255 устройств на одну точку доступа; несколько точек доступа в сети	Теоретически до 255 устройств на одну точку доступа; несколько точек доступа в сети
Возможность использования голосовых каналов по Интернет-протоколу	Присутствует	Присутствует	Присутствует
Технологи защиты	Аутентификация: вызов-ответ между точкой доступа и клиентом по стандарту WEP (Wired Equivalent Privacy. 128-битное кодирование.	Аутентификация: вызов-ответ между точкой доступа и клиентом по стандарту WEP (Wired Equivalent Privacy). 128-битное кодирование.	Аутентификация: вызов-ответ между точкой доступа и клиентом по стандарту WEP (Wired Equivalent Privacy). 128-битное кодирование
Адресация	MAC адрес, 48 бит	MAC адрес, 48 бит	MAC адрес, 48 бит

В результате сравнительного анализа установлено, что:
• IEEE 802.11b – является устаревшей технологией вследствие малой скорости и низкой защищённости.
• IEEE 802.11a – не может быть использован в РФ вследствие отсутствия разрешения на использование данного диапазона частот.
• IEEE 802.11g является оптимальным решением, так как имеет преимущества как в технологиях безопасности, так и скорости передачи данных. Данный протокол поддерживает использование стандартов защиты WPA, WPA2.0 и WEP, использующего длины ключей до 256 бит. Кроме того, данная технология не требует сертификации и разрешений для использования.

2.Технология WiMAX

Данная технология использует стандарт беспроводной связи IEEE 802.16-2004 технология WiMAX (Worldwide Interoperability for Microwave Access) на сегодняшний день используется в большинстве беспроводных сетей уровня города или небольшого района. WiMAX представляет собой широкополосную беспроводную связь, дополняющую оптические линии передачи данных в качестве альтернативного решения проблемы «последней мили» на значительных расстояниях.

Базовыми характеристиками стандарта 802.16 предусматриваются возможности действия сигнала радиосвязи на расстоянии до 50 километров, покрытия с возможностью функционирования вне прямой зоны видимости. Значения пиковой скорости обмена данными может достигать 100 Мбит/с на сектор одной базовой станции.

Интерфейс мобильной беспроводной связи WiMAX основан на применении модуляции OFDMA, либо масштабируемой модуляции SOFDMA (стандарт 802.16e) для поддержки динамически изменяемой ширины канала – от 1.25 до 20 МГц. Фактически функционирование оборудования сетей WiMAX производится в нескольких частотных каналах шириной по 10 МГц в пределах лицензируемого диапазона 2 ГГц - 11 ГГц. Широкий разброс диапазонов выбран для учета специфики разных стран мира. При этом частотные параметры использования сетей WiMax принимаются для каждого государства отдельно в соответствии с особенностями функционирования радиосигналов.

Использование антенных технологий, гибкой схемы работы с каналами, также метода расширенного кодирования и модуляции (Advanced Coding and Modulation - ACM) позволяет добиться скорости приема данных 63 Мбит/с, передачи – 28 Мбит/с на сектор в канале шириной 10 МГц.

Фундаментальной особенностью архитектуры канального MAC-уровня технологии является понятие «качества услуг» (Quality of Service - QoS), что ориентировано на соединение или на сервис.

Таким образом, технологии WiMax обеспечивают более устойчивую связь и высокую мощность сигнала по сравнению с технологиями домашних и офисных беспроводных сетей.

Основным недостатком использования беспроводных сетевых технологий является их уязвимость перед внешними вторжениями, так как использование мобильного устройства позволяет обнаружить наличие сетей, в результате чего растет вероятность попыток несанкционированного подключения к сетям. Так, для проводных технологий требуется доступ к сетевым портам, в беспроводных сетях этого не требуется, что делает их потенциально уязвимыми.

1.2. Основные цели сетевой безопасности

Целями сетевой безопасности являются (рис.1):
- обеспечение целостности данных;
- обеспечение требований конфиденциальности информации;
- обеспечение доступности информации.

Рисунок 1.1. Цели сетевой безопасности

Целостность данных

Одной из главных целей обеспечения сетевой безопасности является обеспечение защиты от несанкционированного изменения, подмены и уничтожения. Целостность информации должна гарантировать сохранность информации как в случае действий злоумышленников, так и влияния случайных факторов. Обеспечение целостности данных является как правило одной из самых сложных задач обеспечения сетевой безопасности.

Конфиденциальность данных

Второй главной целью обеспечения безопасности при использовании сетевых технологий является обеспечение конфиденциальности данных. При проектировании системы защиты конфиденциальности данных необходимо определить и обосновать типы обрабатываемой конфиденциальной информации в системе. Основными видами конфиденциальной информации являются:
- криптографические системы;
- персональные данные;
- коммерческая тайна;
- информация, определенная локальными нормативными актами предприятия.

Доступность данных

Обеспечение доступности информации является необходимым условием функционирования автоматизированных систем. Доступными информационными ресурсами в локальных сетях, как правило, являются:
- Общие сетевые ресурсы и файловые хранилища;
- Принтеры, сканеры;
- Средства управления и администрирования;
- Программные ресурсы.

Таким образом, архитектура информационной безопасности должна одновременно выполнять задачи защиты сетевой информации, а также доступности необходимых компонент для пользователей.
Рассмотрим основные типы угроз сетевой безопасности. По их происхождению принято их классифицировать на угрозы, обусловленные человеческим фактором и угрозы, связанные с особенностью функционирования технических средств.
К угрозам технического характера относят:
- ошибки ПО;
- DoS- и DDoS-атаки;
- Вредоносное программное обеспечение;
- средства несанкционированного съема данных;
- сетевые угрозы.

Ошибки в программном обеспечении

Ошибки ПО являются самым узким местом любой ЛВС. Программное обеспечение серверов, рабочих станций, маршрутизаторов и т. д. разработано людьми, следовательно, оно практически всегда содержит ошибки. С ростом сложности программных продуктов растет вероятность возникновения в нем ошибок и уязвимостей. Большая часть из них не представляет никакой опасности, но некоторые могут быть связаны ошибками проектирования системы безопасности, что приводит к возможности получения злоумышленниками контроля над сетевыми ресурсами, неработоспособности сервера, несанкционированному использованию ресурсов (хранение ненужных данных на сервере, использование в качестве плацдарма для атаки и т.п.). Большая часть подобных уязвимостей может быть устранена с помощью сервисов обновления ПО, регулярно выпускаемых разработчиками. Своевременная установка таких обновлений является необходимым условием безопасности сети.

DoS- и DDoS-атаки

Denial Of Service (отказ в обслуживании) являются особым типом атак, направленных на выведение сетевых ресурсов или серверов из состояния нормальной работоспособности. DoS-атаки могут использовать ошибки в программном обеспечении или путём совершения легитимных операций, но в больших масштабах (например, посылки большого количества электронных сообщений). DDoS - атаки (Distributed Denial Of Service) отличаются от предыдущего поколения использованием огромного количества компьютеров – бот-сетей, расположенных в большой географической зоне. Такие атаки приводят к перегрузке каналов трафиком и мешают прохождению, а зачастую проводят полную блокировку передачи данных по атакуемой сети. Наиболее часто DDos – атаки могут использоваться как средство конкурентной борьбы, а также как один из вариантов информационного оружия.

Вредоносное программное обеспечение.

Вирусы — старая категория опасностей, которая в последнее время в чистом виде практически не встречается. В связи с активным применением сетевых технологий для передачи данных вирусы все более тесно интегрируются с троянскими компонентами и сетевыми червями. В настоящее время компьютерный вирус использует для своего распространения либо электронную почту, либо уязвимости в ПО. А часто и то, и другое. Теперь на первое место вместо деструктивных функций вышли функции удаленного управления, похищения информации и использования зараженной системы в качестве плацдарма для дальнейшего

распространения. Все чаще зараженная машина становится активным участником DDoS-атак. Методов борьбы достаточно много, одним из них является все та же своевременная установка обновлений.
Анализаторы протоколов и «снифферы»
Данная группа включает средства перехвата передаваемой по сети информации. Такие средства могут быть как аппаратными, так и программными. Обычно данные передаются по сети в открытом виде, что позволяет злоумышленнику внутри локальной сети перехватить их. Некоторые протоколы работы с сетью (POPS, FTP) не используют шифрование паролей, что позволяет злоумышленнику перехватить их и использовать самому. При передаче данных по глобальным сетям эта проблема встает наиболее остро. По возможности следует ограничить доступ к

1.ООО "Интерзет". История. [Электронный ресурс]. Режим доступа: http://www.bfsibguti.ru/index.php/we-bf-sibguti/istoriya-bf-sibguti
2. Общие сведения о протоколе PEAP. [Электронный ресурс]. Режим доступа: https://technet.microsoft.com/ru-ru/library/cc754179.aspx
3. D-Link DIR 615. Основные характеристики. [Электронный ресурс]. Режим доступа: http://www.dlink.ru/ru/products/5/2067_d.html
4. Малюк А.А, Пазизин С.В, Погожин Н.С. Введение в защиту информации в автоматизированных системах. – М.: Горячая Линия - Телеком, 2011. – 146 с.
5. Малюк А.А. Информационная безопасность. Концептуальные и методологические основы защиты информации. Учебное пособие. – М.: Горячая Линия - Телеком, 2004. – 280 с.
6. Петраков А.В. Основы практической защиты информации. Учебное пособие. – М.: Солон-Пресс, 2005. – 384 с.
7. Федоров А. В. Проектирование информационных систем. М.: Финансы и статистика, 2003.
8. Хорев П.Б. Методы и средства защиты информации в компьютерных системах. – М.: Академия, 2008. – 256 с.
9. Хорев П.Б. Программно-аппаратная защита информации. – М.: Форум, 2009. – 352 с.
10. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах. – М.: Форум, Инфра-М, 2010. – 592 с.
11. Бройдо В. Л., Ильина О. П. Вычислительные системы, сети и телекоммуникации. – М.: Радио и связь, 2011. - 560 с.
12. Венделева М.А. Сетевые технологии в ИС предприятий. - М.: Юрайт, 2013. - 462 с.
13. Ги, К. Введение в локальные вычислительные сети; М.: Радио и связь - Москва, 2011. - 176 с.
14. Гольдштейн Б. С. Протоколы сетевого доступа. Том 2; СПб.: БХВ-Петербург, 2009. - 288 с.
15. Горнец, Н.Н. ЭВМ и периферийные устройства. Компьютеры и вычислительные системы. М.: ДМК Пресс, 2015. - 184 с.
16. Епанешников А. М., Епанешников В. А. Проектирование локальных вычислительных сетей; М.: Диалог-МИФИ, 2013. - 224 с.
17. Карпова И.П. Сетевые базы данных. - СПб.: Питер, 2013. - 240 с.
18. Колбин Р. В. Организация глобальных и локальных сетей. М.: Бином. Лаборатория знаний, 2011. - 815 с.
19. Котов Г.В. Расчет затрат на проектирование ЛВС. М.: Наука, 2011. - 224 с.
20. Кульгин М.В. Коммутация и маршрутизация IP - трафика.— М.: Компьютер-пресс, 2015. - 99с.
21. Ларионов А.М.; Майоров С.А.; Новиков, Г.И. Архитектура вычислительных комплексов, систем и сетей. М.: Энергоатомиздат, 2014. - 288 с.
22. Малыхина, М.П. Проектирование и использование баз данных. – СПб: БХВ Петербург.2009.
23. Медиаконвертеры Allied Telesis AT-MC102XL. [Электронный ресурс]. Режим доступа: http://allied.ru/cena/allied-telesis-mc101xl?
24. Мелехин В. Ф., Павловский Е. Г. Вычислительные машины, системы и сети. М.: Академия, 2013. - 560 с.
25. Олифер В.Г.; Олифер Н.А. Компьютерные сети: принципы, технологии, протоколы. СПб: Питер, 2011. - 672 с.
26. Поляк-Брагинский А. Модернизация и обслуживание локальных сетей. СПб.: БХВ-Петербург, 2012. - 832 с.
27. Прайс-лист на монтаж локальных сетей. [Электронный ресурс]. Режим доступа: http://www.lansks.ru/montazh_setej_prajs.htm
28. Прончев Г.Б., Бухтиярова И.Н., Брутов В.В., Фесенко В.В. Компьютерные коммуникации. Простейшие

вычислительные сети. М.: КДУ, 2009. - 332 с.
29. Пятибратов А.П., Беляев С.Н. Стандарты беспроводных сетей. М.: Инфра-М, 2010. - 400 с.
30. Пятибратов А.П., Гудыно Л.П., Кириченко А. А. Технологии Wi-Fi и Wi-Max. М.: Инфра-М, 2014. - 736 с.
31. Пятибратов А.П.; Гудыно, Л.П.; Кириченко, А.А. Вычислительные системы, сети и телекоммуникации; М.: Финансы и статистика; Издание 2-е, перераб. и доп. – М.: Инфра-М, 2013. - 512 с.
32. Рассел Дж. Звезда (топология компьютерной сети). — Москва, Книга по Требованию, 2012 г.- 74 с.
33. Растригин Л.А. Вычислительные машины, системы, сети...; М.: Наука. Главная редакция Физико-математической литературы, 2012. - 224 с.
34. Степанов А.Н. Информатика: учебное пособие. – СПб: Питер Пресс, 2012. – 764 с.
35. Стоимость проектирования и монтажа локальных сетей. [Электронный ресурс]. Режим доступа: https://itsm37.ru/tarify_na_montazh_LAN.html
36. Столлингс Вильям Компьютерные сети, протоколы и технологии Интернета; СПб.: БХВ-Петербург, 2011. - 832 с.
37. Таненбаум, Э. Компьютерные сети. - СПб.: Питер, 2013. - 960 с.
38. Флинт Д. Локальные сети ЭВМ: архитектура, принципы построения, реализация; М.: Финансы и статистика, 2013. - 359 с.