Министерство образования и науки Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г.ЧЕРНЫШЕВСКОГО»

Кафедра дискретной математики и
информационных технологий

Разработка корпоративной сети компании «Эрс-тревел»

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

Студента 5 курса 521 группы

направления 09.03.01 «Информатика и вычислительная техника»

факультета компьютерных наук и информационных технологий

Морозова Андрея Александровича

Научный руководитель
к. ф.-м.н., доцент _____ А.Д. Панферов
дата, подпись

Заведующий кафедрой
к. ф.-м.н., доцент _____ Л.Б. Тяпаев
дата, подпись

Саратов 2016

Введение. В современном мире предприятия не могут существовать без сетей. Сети обеспечивают единое информационное пространство, объединяя территориально разнесенные филиалы с головным офисом. Обеспечивают возможность организовывать мелкие вынесенные филиалы или выездную работу с клиентами индивидуальных менеджеров. Современный уровень развития сетевых технологий делает возможным организацию виртуальных рабочих мест, доступных 24 часа в сутки вне зависимости от текущей локации сотрудника. В том числе все большее распространение принимает работа из дома.

Информационные технологии во многих сферах деятельности существенно меняют саму технологию бизнес-процессов. Меняются формы взаимодействия с клиентами и поставщиками. В сочетании с аналитическими методами обработки информационных массивов обеспечивается существенная оптимизация использования материальных и финансовых ресурсов.

Построение современной корпоративные сети требует использования оборудования и программного обеспечения ведущих мировых производителей. Необходимо обеспечивать их высокую эффективность, надежность, безопасность и модернизационный потенциал.

Целью выпускной квалификационной работы поставлена задача разработать концептуальный проект корпоративной сети для коммерческой организации, работающей в сфере туристического бизнеса. Особенности бизнес процессов в этой сфере деятельности позволяют применить разнообразные подходы и технические решения, что делает эту задачу интересной именно с точки зрения демонстрации возможностей современных сетевых технологий.

Для достижения указанной цели в выпускной квалификационной работе решены следующие задачи:

- описание структуры предприятия
- выбор и описание технических решений для построения корпоративной сети

- изучение принципов по обеспечению безопасности в корпоративных сетях
- выбор решения для обеспечения защищенного VPN подключения в сети

Основное содержание. Компания «Эрс-тревел», специализируется на предоставлении туристических услуг. Центральный офис компании находится в Москве. Он занимается организацией туров. Имеется сеть филиалов в Москве и регионах, которые осуществляют продажи клиентам. Базы данных и обработка бизнес-информации сосредоточены в центральном офисе. Сайт компании расположен на внешнем хостинге и администрируется из центрального офиса. Удаленная работа из офисов осуществляется в КИС (Корпоративная информационная система) с подключением через VPN.

Помещения для центрального офиса и филиалов предоставляются арендодателями. Головной офис компании «Эрс-тревел» состоит из 7 помещений и располагается на одном этаже. Помещения оборудованы электрическими и сетевыми розетками, кабельной разводкой, датчиками задымленности и системой пожаротушения. Одно из помещений отведено под ЦОД, в котором установлено климатическое оборудование. Общее число компьютеров – 12, в каждом кабинете имеется МФУ. Доступ к глобальной сети в головном офисе предоставляется арендодателем, а в филиалах по договору с местными поставщиками интернет услуг. Филиалы состоят из одного помещения, в котором имеется Wi-Fi маршрутизатор, предоставляемый местными провайдерами, с подключенным к нему МФУ. Для невыездной работы сотрудники филиалов используют настольные ПК и личные ноутбуки, которые также используются для работы по выезду.

Необходимо определить требования к СКС и механизмам организации беспроводного доступа. Структурированная кабельная система является основой для всех информационных систем, обеспечивающих функционирование офиса. Сама по себе СКС – это совокупность

коммутационного оборудования связанного между распределенными элементами офиса. В состав СКС входит:

- Кабельная проводка (витая пара, оптическое волокно);
- Коммутационные панели;
- Конечная сетевая инфраструктура (розетки и разъемы).

На сегодняшний день большинство оконечного сетевого оборудования (сетевые карты настольных и портативных ПК, принтеров, IP-телефоновточек доступа) имеют предел в 1 Гбит/сек. Поэтому в качестве кабеля для СКС хорошо подходит категория 5e, которая как раз и обеспечивает скорость в 1 Гбит/сек.

Активное сетевое оборудование играет центральную роль в функционировании корпоративной сети. Оно должно отвечать потребностям компании, допускать масштабирование и просто управляться.

При выборе оборудования надо руководствоваться несколькими критериями:

- Количество портов;
- Скорость работы;
- Поддерживаемые технологии.

В современном офисе должна присутствовать еще и беспроводная сеть. Она обеспечит мобильность работников компании и предоставит доступ к сети для гостей и клиентов. При организации Wi-Fi необходимо учитывать несколько серьезных вещей:

- Безопасность. К организации безопасности надо подойти с особой тщательностью. В современных условиях взлом недостаточно хорошо организованной системы безопасности может быть причиной финансового краха компании. На сеть могут совершать атаки как конкуренты, с целью заполучить важную информацию, так и частные лица.

- Стабильность связи. Не достаточно просто установить точку доступа на ближайшую стену в помещении. Надо учитывать такие факторы как помехи от бытовых приборов, помехи от точек доступа находящихся в радиусе действия вашей беспроводной сети. Также количество пользователей играют роль в скорости доступа к сети. При большом количестве пользователей, следует использовать более мощное оборудование.

При проектировании сети Wi-Fi необходимо иметь ввиду, что использование радиочастотного диапазона в нашей стране (как и во всех остальных странах) регулируется специальным законодательством. Хотя используемые Wi-Fi диапазоны частот не требуют лицензирования, существуют определенные ограничения (например, допустимая мощность точек доступа), которые надо обязательно соблюдать.

Проведем сравнение характеристик коммутаторов для сети центрального офиса. На сегодняшний день существует множество компаний, выпускающих сетевое оборудование. Прежде чем выбирать оборудование для нашей компании надо определиться сколько может потребоваться портов с учетом запаса на плановое и внеплановое расширения парка устройств, обеспечение отказоустойчивости при выходе некоторого количества портов из строя и т.п. Для этого надо посчитать количество рабочих мест и к каждому добавить 1-2 порта на реализацию дополнительных сервисов и про запас. Также не стоит забывать про периферийные устройства – принтеры, сканеры, факсы. Ещё стоит добавить по порту на каждую Wi-Fi точку доступа, причем необходимо заранее определиться с их количеством. Для этого стоит провести тестирование «на местности» и определить зоны покрытия внутри арендуемого для компании помещения. Собрав эту информацию можно определиться с характеристиками оборудования необходимого для реализации проекта. Оценочный подсчет количества портов можно выполнить исходя из данных о нашей компании. Не критично, если некоторые порты останутся незадействованными, они нам пригодятся в случае расширения.

Наиболее подходящими для нас из представленных на рынке моделей являются 48-портовые коммутаторы, обеспечивающие возможность подключения всех имеющихся рабочих мест с периферией, и имеющими запас свободных портов. Рассмотрим некоторые модели управляемых коммутаторов от основных производителей, представленные на рынке: HP-3COM 1620-48G; Cisco SG300-52; D-Link DGS-1210-52. И приведем сравнительную таблицу основных характеристик.

Устройство	HP-3COM 1620-48G	Cisco SG300-52	D-Link DGS-1210-52
Кол-во портов	48	52	52
Матрица коммутации	96 Гбит/сек	104 Гбит/сек	104 Гбит/сек
Число MAC-адресов	16384	16384	16384
Уровень коммутатора	Layer 2	Layer 3	Layer 2

Так как к сети не предъявляется повышенного требования безопасности, то самым экономически выгодным вариантом является коммутатор D-Link DGS-1210-52, который обладает широким функционалом, при низкой стоимости среди конкурентов.

Далее, рассмотрим протоколы IPSec для обеспечения защищенных соединений. IP Security (IPSec) – это набор протоколов, которые можно разделить на две группы: протоколы защиты данных и протоколы обмена ключами. IPSec работает на сетевом уровне модели OSI, обеспечивая шифрование и аутентификацию пакетов IP, пересылаемых между сторонами – такими как роутеры Cisco, сетевые экраны PIX Firewall, клиенты Cisco VPN, а также другими сетевыми продуктами, поддерживающими IPSec.

Возможности IPSec VPN:

- Конфиденциальность данных. Отправитель может шифровать пакеты данных перед тем, как передавать их по сети.

- Целостность. Для обеспечения целостности данных получатель может аутентифицировать отправителя информации и пакеты IPSec, чтобы быть уверенным в том, что данные не были изменены в пути.
- Защита от воспроизведения. Получатель данных IPSec может обнаруживать и отвергнуть воспроизведенные пакеты, не допуская их фальсификации и проведения атак внедрения посредника.

IPSec использует стандартный способ аутентификации и шифрования соединений между взаимными сторонами. Чтобы обеспечить защиту связей, IPSec применяет стандартные алгоритмы шифрования и аутентификации. В IPSec используются открытые стандарты согласования ключей шифрования и управления соединениями, что дает возможность взаимодействия между сторонами. Технология IPSec предлагает методы, позволяющие сторонам IPSec «договориться» о согласованном использовании сервисов. Чтобы указать согласуемые параметры, в IPSec используются ассоциации защиты.

Ассоциация защиты (SA – Security Association) представляет собой совокупность параметров соединения сторон с целью обеспечить безопасную передачу трафика. Действующие параметры SA сохраняются в базе данных ассоциаций защиты (SAD – Security Association Database) обеих сторон. Два компьютера каждый на своей стороне хранят режим SA, протокол, алгоритмы и ключи, используемые в SA. Каждое SA используется только однонаправленно. Для двунаправленной связи требуется два SA. Каждое SA осуществляет один режим и протокол, таким образом, если для одного пакета нужно использовать два протокола (AH и ESP), то требуется два SA.

Протокол IKE (Internet Key Exchange – обмен Internet-ключами) это гибридный протокол, предоставляющий специальный сервис для IPSec: аутентификацию сторон IPSec, согласование параметров ассоциаций защиты IKE и IPSec, а также выбор ключей для алгоритмов шифрования, используемых в пределах IPSec. Протокол IKE ссылается на протоколы ISAKMP (Internet Security Association and Key Management Protocol – протокол управления ассоциациями и ключами защиты в сети Internet) и Oakley, которые

используются для управления процессом создания и обработки ключей шифрования, применяемых в преобразованиях IPSec. Также IKE применяется для формирования ассоциаций защиты между потенциальными сторонами IPSec. IKE и IPSec используют ассоциации зашиты, чтобы указать параметры связи.

Протокол AH (Authentication Header – заголовок аутентификации). Протокол зашиты, предоставляющий аутентификацию и (как опцию) сервис выявления воспроизведения. Протокол AH работает как цифровая подпись и дает гарантию, о целостности данных в пакете IP. AH не обеспечивает сервис шифрования и дешифрования данных. Также он может использоваться самостоятельно или вместе с протоколом ESP.

Протокол ESP (Encapsulating Security Payload). Протокол защиты, предоставляющий секретность и защиту данных, и (как опцию) сервис аутентификации и выявления воспроизведения. Продукты Cisco используют ESP для шифрования полезного содержания IP-пакетов. Протокол ESP может использоваться самостоятельно или совместно с AH.

Протоколы AH и ESP IPSec могут работать или в туннельном, или в транспортном режимах. Туннельный режим используется для связи между шлюзами IPSec, и в этом случае средствам IPSec приходится создавать совершенно новый заголовок IPSec. Транспортный режим обычно применяется между клиентом и сервером VPN, и при этом используется существующий заголовок IP.

В результате проделанной работы для организации корпоративной сети рассматриваемого назначения считаю целесообразным придерживаться изложенных ниже рекомендаций

В центральном офисе использовать структурированную кабельную систему на основе кабеля витой пары категории 5e с одним узлом коммутации и маршрутизации для обеспечения доступа к сети для 12 компьютеров на рабочих местах сотрудников, до пяти многофункциональных печатающих устройств (МФУ) и двух беспроводных точек доступа. Количество точек

доступа, необходимых для полного покрытия территории центрального офиса подлежит уточнению по месту при конкретизации арендуемого помещения в зависимости от его планировки, материалов стен и помеховой обстановки. В качестве коммутатора использовать D-Link DGS-1210-52. Он позволит надежно и эффективно коммутировать трафик. Для маршрутизации и организации VPN туннеля использовать межсетевой экран Cisco ASA5510, который обладает широкими возможностями по обеспечению безопасности и высокой производительностью.

Для филиалов, в количестве 20 штук, находящихся в разных регионах, доступ в интернет должен предоставляться местным провайдером. С провайдером следует заключить договор о предоставлении необходимого сетевого оборудования, а именно, беспроводного маршрутизатора с не менее чем 3-мя свободными LAN портами.

В качестве периферийного устройства использовать HP LaserJet Pro M477fdw, который сочетает в себе цветной лазерный принтер, сканер, копир и факс. Он имеет сетевые интерфейсы Ethernet и Wi-Fi.

При организации беспроводного соединения в центральном офисе предлагается использовать точки доступа Ubiquiti UniFi AC. Места их установки определить по результатам оценки зон помех и наилучшего покрытия.

Для возможности подключения к сети центрального офиса через VPN соединения необходимо предусмотреть на всех компьютерах соответствующее программное обеспечение.

Заключение. В рамках выпускной квалификационной работы мною был разработан концептуальный проект информационной сети компании «Эрс-тревел» и описана её структура.

В ходе выполнения работы были рассмотрены современные тенденции в развитии сетевых технологий и их роль в обеспечении деятельности коммерческих предприятий. Проанализированы технологии, применяемые в компьютерных сетях с проводной базовой инфраструктурой и их беспроводных

сегментов. Поскольку в современных корпоративных информационных системах очень большое внимание уделяется вопросам безопасности, соответствующие вопросы были проанализированы. Так, было рекомендовано использовать межсетевой экран на базе оборудования Cisco ASA5510. Рассмотрены детали настройки протокола IPSec.

Представленный вариант реализации корпоративной сети учитывает текущие потребности компании и обеспечивает возможности дальнейшего масштабирования в случае роста бизнеса компании

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Исаев Г.Н. / Информационные технологии / Г.Н. Исаев. - М.: Омега-Л, 2012

2 Новые информационные технологии / Под редакцией В.П. Дьяконова. / М.: Солон-Пресс, 2005

3 Олифер В.Г., Олифер Н.А. / Компьютерные сети. Принципы, технологии, протоколы. / СПб.: Питер, 2010

4 Поляк–Брагинский А. В. / Сеть своими руками. 3–е издание. / Спб.: BHV, 2008

5 Пролетарский А.В., Баскаков И.В., Чирков Д.Н. / Беспроводные сети Wi–Fi. / М.: Бином, 2007

6 Таненбаум Э., Уэзеролл Д. / Компьютерные сети. / Спб.:Питер, 2012

7 Д. Стрельцов / Как обжать сетевой кабель LAN своими руками [Электронный ресурс] URL: http://hobbyits.com/wan-lan-wi-fi/kak-obzhat-setevoj-kabel-lan-svoimi-rukami.html

8 Биячуев Т.А. под ред. Л.Г. Осовецкого / Безопасность корпоративных сетей. / СПб: СПб ГУ ИТМО, 2006

9 Браун, С. / Виртуальные частные сети / С. Браун - Н.: Лори, 2001