Министерство образования Республики Беларусь

Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей

Кафедра электронных вычислительных машин

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
к курсовому проекту
на тему

ЛОКАЛЬНАЯ КОМПЬЮТЕРНАЯ СЕТЬ
ВАРИАНТ 25

БГУИР КП 1–40 02 01 201 ПЗ

Студент Н. Г. Альхимович

Руководитель И. И. Глецевич

МИНСК 2024

Вариант	25
Объект	организация, занимающаяся торговлей компьютерными комплектующими
Форма здания, номера этажей, суммарная площадь одного этажа в квадратных метрах	прямоугольная (с соотношением сторон 1:1,5), 0-1, 210
Количество стационарных пользователей, количество стационарных подключений, количество мобильных подключений	условный заказчик не уверен, условный заказчик не уверен, 20
Сервисы	нет
Прочие оконечные устройства	принтеры, smart-телевизоры
Подключение к Internet	условный заказчик не уверен
Внешняя адресация IPv4, внутренняя адресация IPv4, адресация IPv6	непосредственного подключения к провайдеру нет, публичная подсеть – использовать одну из подходящих подсетей из своего варианта лабораторных работ (если возможно), взаимодействие в рамках внутренней сети
Безопасность	сетевой экран
Надежность	защита от сильных перепадов температуры
Финансы	бюджетная сеть
Производитель сетевого оборудования	Allied Telesis
Дополнительное требование заказчика	задействовать уже имеющийся системный блок (Pentium G2030, PC3-10600 8 GB, HD Video, HD Audio, Gigabit Ethernet)

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Данный курсовой проект посвящен проектированию локальной компьютерной сети небольшой организации, исходя из ряда требований, предъявленных условным заказчиком. В рассматриваемом случае им выступает организация, занимающаяся торговлей компьютерными комплектующими. По завершении выполнения работы необходимо предоставить соответствующую документацию.

Ключевым этапом проектирования является планирование сетевой топологии, а также анализ предлагаемого на рынке сетевого оборудования (прежде всего, маршрутизаторов и коммутаторов) с целью разработки схемы сети с оптимальными показателями отказоустойчивости и производительности в заданных условиях и в соответствии с установленными требованиями, среди которых следует учесть:

- особенности здания и его планировку;
- нагрузку на сеть (предполагаемое количество пользователей);
- поддержку функционирования дополнительных сервисов и оконечных устройств, таких как принтеры и smart-телевизоры;
- обеспечение возможности выхода в Internet;
- тип адресации;
- поддержание надежности и устойчивости сети при изменении внешних условий;
- предотвращение несанкционированного доступа (посредством применения сетевого экрана);
- бюджетные средства, которыми располагает заказчик.

После чего необходимо разработать структурную модель сети с определением числа подсетей в ее составе, а также их взаимосвязей.

На следующей стадии реализации проекта будет произведена разводка кабелей в здании, при этом расход ресурса должен быть минимальным без ущерба качеству связи и доступности сетевого и оконечного оборудования. Кроме того, нужно определить размещение розеток и всех необходимых устройств. В частности, что касается беспроводных маршрутизаторов, необходимо также учитывать зону покрытия, мощность сигнала и возможные препятствия для его проходимости, к примеру: расположенные в радиусе силовые кабели, стены, перекрывающие источники сигнала и пр.

Завершающим этапом проектирования после подбора подходящего под заданные условия и удовлетворяющего всем требованиям условного заказчика оборудования станет его настройка, которая включает:

- установку операционных систем;
- конфигурацию параметров сетевых устройств;
- распределение и назначение IP-адресов.

Принимая во внимание факт неизбежности стремительного развития информационных технологий в целом и сетевого обеспечения в частности, а

также сопутствующего роста требований к скорости и качеству передачи данных; актуальность описанного проекта безусловно подтверждается на практике. В любой современной организации стабильная и эффективная компьютерная сеть является неотъемлемым элементом инфраструктуры, обеспечивающим бесперебойную работу всех подразделений компании.

Таким образом, грамотное проектирование локальной компьютерной сети позволит оптимизировать рабочие процессы, повысить производительность труда сотрудников, минимизировать риски сбоев и расходы на обслуживание и обеспечить высокий уровень информационной безопасности, что особенно важно для сохранения целостности корпоративных данных.

1 ОБЗОР ЛИТЕРАТУРЫ

1.1 Сетевой экран

Для обеспечения безопасности проектируемой компьютерной сети необходимо своевременно блокировать вредоносную активность и предотвращать несанкционированный доступ к конфиденциальным данным организации как в частной сети, так и за ее пределами. Эффективным защитным инструментом выступает сетевой экран.

Он представляет собой систему защиты компьютерной сети в виде программного обеспечения или программно-аппаратного модуля, которая ограничивает прохождение входящего, исходящего и внутрисетевого трафика [1]. Это, по сути, управляемый барьер, который отвечает за фильтрацию сетевого трафика согласно установленным параметрам и принятие решения о пропуске или блокировке проходящих пакетов данных. Помимо этого, сетевой экран может фиксировать сведения о пользовательском доступе в специальных журналах аудита для того, чтобы иметь возможность сверять полученные данные со списком доверенных или запрещенных действий.

Сетевые экраны, как правило, устанавливаются на отдельных компьютерах, имеющих доступ к сети, пользовательских станциях и прочих хостах.

В целях защиты на сетевом уровне модели OSI применяются экранирующие маршрутизаторы, называемые также пакетными фильтрами, оценивающие каждый пакет данных независимо, основываясь на заданных критериях. Для этого анализируются следующие поля заголовков пакетов сетевого и транспортного уровней:

- адрес источника;
- адрес получателя;
- тип пакета;
- флаг фрагментации пакета;
- номер порта источника;
- номер порта получателя.

В процессе обработки отдельно взятого пакета экранирующий маршрутизатор последовательно просматривает таблицу правил контроля подключений до тех пор, пока не найдет то, с которым согласуется вся совокупность параметров, указанных в заголовке пакета [2]. Если подобное не будет обнаружено, то используется правило по умолчанию, а именно: блокировка пакета.

Для защиты на уровне хоста принято использовать программные сетевые экраны, для которых характерны индивидуальные настройки отдельных приложений, установленных на данных устройствах. Расширенная фильтрация трафика в таком случае выполняется на основе протокола HTTP или иных сетевых протоколов.

Хотя такой метод защиты компьютерной сети и обладает рядом преимуществ (относительная простота конфигурирования, минимальное влияние на производительность), но присутствуют и недостатки: разрешение подключений санкционированных приложений (которые тем не менее могут представлять угрозу), зависимость от таблицы правил.

1.2 Защита от сильных перепадов температуры

Сильные перепады температур могут в значительной степени оказать влияние на сетевое оборудование и общее функционирование локальной компьютерной сети, вплоть до снижения производительности, отказа или выхода из строя.

Серверы, коммутаторы и маршрутизаторы, работающие в условиях высокой нагрузки, в большей степени подвержены перегреву. При резком снижении температуры в кондиционируемом помещении возможно образование конденсата на кабелях и компонентах оборудования, что повышает риск короткого замыкания.

Поэтому в случае проектирования сети в условиях температурных колебаний, что в том числе возможно на подвальных этажах или в плохо вентилируемых помещениях, необходимо предусматривать соответствующие меры защиты.

При выборе сетевых устройств следует учитывать допустимые температурные диапазоны эксплуатации, а также наличие встроенных датчиков (для мониторинга внешних условий) или защитных корпусов, чтобы по возможности избежать выбора слишком чувствительного оборудования.

В менее приспособленных с точки зрения поддержания стабильного микроклимата помещениях потребуется предусмотреть установку систем активного охлаждения (кондиционеры), пассивного (ребристые радиаторы на корпусах устройств) и системы вентиляции.

Если рассматривать беспроводное подключение, то необходимо выбирать приемо-передающее оборудование с высоким уровнем защиты (например, стандарта IP67 или выше).

1.3 Сетевое оборудование Allied Telesis

Allied Telesis – это международная компания, специализирующаяся на рынке телекоммуникаций, поставляет решения для сетей Ethernet & IP, а также услуг Triple Play [3]. Является одним из лидеров в разработке и производстве систем оптической транспортировки и широкополосного доступа, которые могут применяться как в корпоративных, так и в городских, региональных сетях поставщиков услуг (операторов связи).

К основным категориям выпускаемого на текущий момент компанией оборудования относятся следующие позиции:

- коммутаторы (рисунок 1.1);
- файрволы и VPN-маршрутизаторы;
- беспроводные решения (рисунок 1.2);
- управляемые и неуправляемые медиаконвертеры;
- сетевые адаптеры;
- трансиверы.

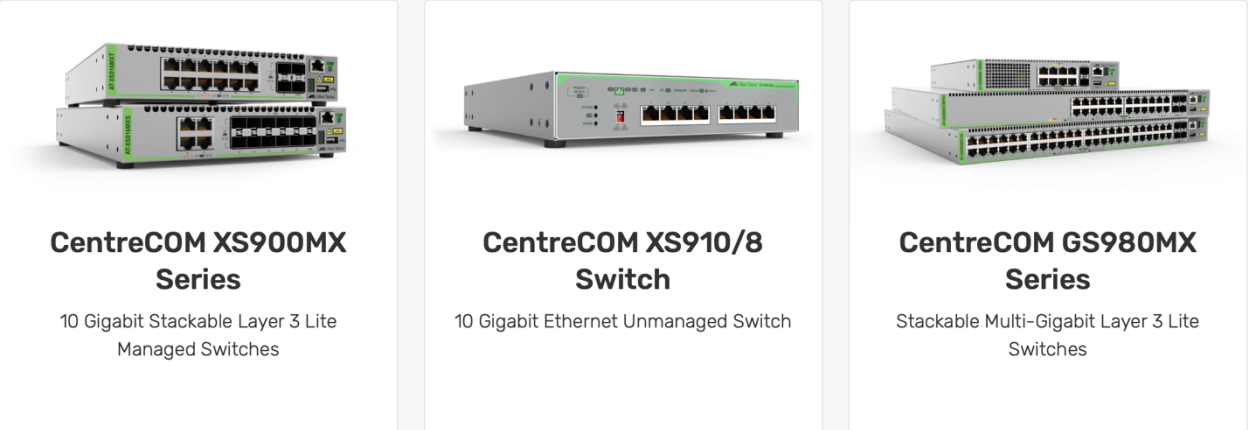

Рисунок 1.1 – Коммутаторы Allied Telesis для небольших предприятий

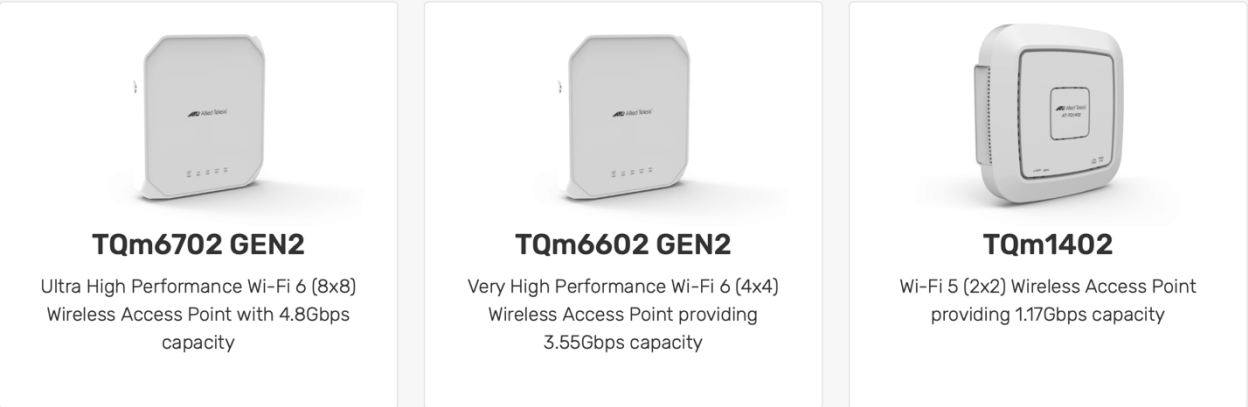

Рисунок 1.2 – Беспроводные точки доступа для малых организаций

Для всех своих продуктов компания предоставляет в свободном доступе техническое описание, спецификации, необходимое ПО и широкий спектр документации [4].

2 СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ

В соответствии с поставленной задачей требуется разработать структуру локальной компьютерной сети для организации, специализирующейся на торговле компьютерными комплектующими, офис которой занимает два этажа общей площадью 420 м^2, один из которых является цокольным.

Необходимо обеспечить возможность 20 мобильных подключений. Информацию о количестве стационарных подключений условный заказчик не предоставил, однако, учитывая выполнение работы для коммерческой организации, доступность стационарных подключений целесообразно обеспечить. Кроме того, дополнительным пунктом в списке требований к проектированию выступает подключение принтеров и smart-телевизоров.

В рамках обеспечения безопасности локальной сети и предотвращения повреждения или утери корпоративных данных, заказчик запросил установку сетевого экрана.

Схема структурная приведена в приложении А. Пунктирной линией выделены зоны, элементы в которых относятся к обозначенному в этой же зоне этажу.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

[1] Что такое брандмауэр или межсетевой экран? [Электронный ресурс]. – Электронные данные. – Режим доступа: https://www.kaspersky.ru/resource-center/definitions/firewall – Дата доступа: 21.09.2024.

[2] Экранирующий маршрутизатор [Электронный ресурс]. – Электронные данные. – Режим доступа: https://studfile.net/preview/321444/page:3/ – Дата доступа: 22.09.2024.

[3] Официальный сайт компании Allied Telesis [Электронный ресурс]. – Электронные данные. – Режим доступа: www.alliedtelesis.com/by/en – Дата доступа: 22.09.2024.

[4] Документация сетевого оборудования Allied Telesis [Электронный ресурс]. – Электронные данные. – Режим доступа: https://www.alliedtelesis.com/by/en/library/search – Дата доступа: 22.09.2024.

[] Вычислительные машины, системы и сети: дипломное проектирование (методическое пособие) [Электронный ресурс]: Минск БГУИР 2019. – Электронные данные. – Режим доступа: https://www.bsuir.by/m/12_100229_1_136308.pdf