МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(дипломная работа)

На тему «Разработка аналитической модели по обеспечению качества обслуживания в ЗТКС»

Исполнитель Майоров Олег Николаевич
(фамилия, имя, отчество)

Руководитель кандидат технических наук
(ученая степень, ученое звание)

Хейстонен Дмитрий Павлович
(фамилия, имя, отчество)

«К защите допускаю»

Заведующий кафедрой _____
(подпись)

доктор технических наук, профессор
(ученая степень, ученое звание)

Бурлов Вячеслав Георгиевич
(фамилия, имя, отчество)

«17» февраля 2017г.

Санкт–Петербург

2017

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(дипломная работа)

На тему«Разработка аналитической модели по обеспечению качества обслуживания в ЗТКС»

ИсполнительМайоров Олег Николаевич
(фамилия,имя,отчество)

Руководителькандидат технических наук
(ученая степень, ученое звание)

Хейстонен Дмитрий Павлович
(фамилия, имя, отчество)

«Кзащитедопускаю»

Заведующийкафедрой_____

(подпись)

_____доктор технических наук, профессор_____
(ученаястепень,ученое звание)

_____Бурлов Вячеслав Георгиевич_____
(фамилия,имя,отчество)

«_»_20г.

Санкт–Петербург

2017

РЕФЕРАТ

Пояснительная записка 84 стр., 16 рис., 1 табл., 31 ист., 4 прил.

Объектом исследования является защищенная локальная вычислительная сеть, в архитектуре которой присутствует коммутационное устройство, поддерживающее функции приоритезации трафика.Предметом исследования в выпускной квалификационной работе выступают методы обеспечения качества обслуживания в защищенной телекоммуникационной сети.

Целью данной работы является разработка аналитической модели по обеспечению качества обслуживания в ЗТКС.

В условиях наличия в локальной корпоративной сети конфиденциальной информации, сеть должна быть защищена путем специализированных средств обеспечения безопасности. Использование данных средств влияет на вероятностно временные характеристики (ВВХ) доставки пакетов. Встает вопрос обеспечения качества обслуживания в данной сети.

В ходе работы были рассмотрены теоретические основы построения ЗТКС, проанализированы основные физические факторы, отвечающие за обеспечение качества обслуживания, рассмотрены основные показатели качества обслуживания.Была построена архитектура защищенной телекоммуникационной корпоративной сети. Так же была разработана аналитическая модель по обеспечению качества обслуживания в данной сети для двух типов трафика – чувствительного к задержкам и эластичного. Были предложены практические рекомендации по выбору активного сетевого оборудования для данной сети.

В целях обеспечения безопасности персонала при работе с данной сетью и оборудованием, обеспечивающим ее корректную работу, были предложены некоторые мероприятия по обеспечению безопасности жизнедеятельности.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В ходе написания теоретической части работы многие данные были взяты из технических характеристик конкретного сетевого оборудования. Поскольку параметры различного оборудования могут сильно отличатся друг от друга, большая часть данных была взята с сайта «CISCO.COM», поскольку большинство устройств данного производителя имеют общую «схему» работы и многие их функции дублируются в различных моделях.

К информационной безопасности предъявляется множество особых требований, таких как целостность, конфиденциальность, доступность, ограниченный доступ, недопустимость утечки, защита носителей информации и прочее. Все эти вопросы изучаются специальностью «Информационная безопасность телекоммуникационных систем». Она включает в себя множество различных аспектов, касаемо защиты информации: инженерно-технические, программные, аппаратные, организационно-правовые и криптографические. Большая роль отведена защите информации внутри компьютерных сетей и систем связи. При этом любая сеть, в том числе и защищенная, должна отвечать неким критериям, отвечающим за ее корректную работу. В том числе удовлетворять такому параметру как «качество обслуживания» (QoS(QualityofService)). Любая телекоммуникационная сеть может столкнуться с проблемой недостаточной пропускной способности. Например, при видеоконференции с использованием неких средств обеспечения безопасности, таких как криптопротоколы, само соединение не должно быть нарушено. В данном случае важным фактором является сведение задержек при передаче к минимуму. В этом случае встает вопрос обеспечения заданного качества обслуживания в этой сети.

Темой данной выпускной квалификационной работы было выбрано «Построение аналитической модели по обеспечению качества обслуживания в ЗТКС».

Цель работы:

- Обеспечение заданных показателей качества обслуживания в защищенной телекоммуникационной сети.

Задачи работы:

- Анализ основных принципов построения защищенных телекоммуникационных компьютерных вычислительных сетей, сетей связи и локальных вычислительных сетей.
- Выявление основных сложностей при обеспечении показателей качества обслуживания (QoS) в компьютерной вычислительной сети.
- Построение архитектуры защищенной корпоративной сети.
- Построение аналитической модели для обеспечения необходимого/заданного качества обслуживания в данной сети на основе алгоритмовприоритезации и обработки очередей, а также на основе «теории массового обслуживания».

Объект исследования:

Объектом исследования является разработанная защищенная локальная вычислительная сеть, в архитектуре которой присутствует коммутационное устройство, поддерживающее функции приоритезации входящего трафика.

Предмет исследования:

Предметом исследования в выпускной квалификационной работе выступают методы обеспечения заданных показателей качества обслуживания в защищенной телекоммуникационной сети для разнородного трафика.

Актуальность:

Актуальность данной работы обусловлена тем, что защищенная компьютерная сеть любого объекта, будь это сеть обширного государственного учреждения или же сравнительно небольшого структурного подразделения частной фирмы подвергается непосредственному влиянию средств обеспечения безопасности, что снижает вероятностно-временные характеристики доставки

пакетов. В следствии этого, такая сеть нуждается в обеспечении того или иного качества обслуживания, в зависимости от требований, предъявляемых к ней.

1. Понятие защищенной телекоммуникационной сети

Телекоммуникационная система – это совокупность аппаратных и программных средств, совмещенных между собой с общую систему для обмена некой информацией на некотором расстоянии.

В различных источниках понятие информационной безопасности имеет множество различных определений и трактовок. Это обусловлено тем, что информационная безопасность (ИБ) является одним из ключевых аспектов в разнообразных сферах деятельности человека. Сам факт существования любой информации предполагает возможность её защиты тем или иным способом, в зависимости от ее ценности, способа представления, места ее нахождения и многих других факторов. Любая информация может представлять ценность, как для ее правообладателя, так и для злоумышленника, то есть того, в чьи руки она попасть не должна.Определение понятия «безопасность» в Доктрине информационной безопасности РФ, которое следует из определения в федеральном законе «О безопасности» от 5 марта 1992 года:«Информационная безопасность РФ — состояние защищенности ее национальных интересов в информационной сфере, определяющейся совокупностью сбалансированных интересов личности, общества и государства».«Безопасность — состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз».

В 2016 году вышла новая «доктрина информационной безопасности Российской Федерации», утверждена УказомПрезидента Российской Федерации от 5 декабря 2016 г. №646, в которой звучит следующее определение информационной безопасности [1]:

«Информационная безопасность Российской Федерации (далее - информационная безопасность) - состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан,

суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства;»

Следующее определение ИБ наиболее популярно и просто [2]: «Информационная безопасность — все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, подотчётности, аутентичности и достоверности информации или средств её обработки. Безопасность информации определяется отсутствием недопустимого риска, связанного с утечкой информации по техническим каналам, несанкционированными и непреднамеренными воздействиями на данные или на другие ресурсы автоматизированной информационной системы, используемые в автоматизированной системе.» В нем содержатся три основных критерия, присущие понятию информационная безопасность.Это минимум требований к ИБ:

- Конфиденциальность – возможность ознакомится непосредственно с информацией (конкретно с данными, имеющими ценность и несущими смысловую нагрузку, а не с последовательностью бит их представляющих) имеют только лишь те лица (список лиц, организации и т.д.), кто владеют полномочиями на право доступа к ней.
- Целостность - Устойчивость информации к несанкционированному или случайному воздействию на нее в процессе обработки техническими средствами, результатом которого может быть уничтожение, искажение или подделка информации.
- Доступность – возможность получения доступа к защищаемой информации с целью ее изменения, изучения или удаления в соответствующий санкционированный для работы период времени.

Так же в некоторых источниках уделяется внимание понятию достоверность.Достоверность – Точная принадлежность защищаемой информации к субъекту, являющемуся ее источником или от которого она получена.

Основные термины и определенияинформационной безопасности[27].

Автоматизированная система - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Аттестация - процесс комплексной проверки выполнения заданных функций автоматизированной системы по обработке защищаемой информации на соответствие требованиям стандартов и/или нормативных документов в области защиты информации и оформления документов о ее соответствий выполнять функции по обработке защищаемой информации на конкретном объекте информатизации.

Безопасность информации - состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность, т.е. сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней, целостность и доступность информации при ее обработке техническими средствами.

Выделенные помещения - помещения (служебные кабинеты, актовые, конференц-залы и т.д.) специально предназначенные для обработки речевой информации (обсуждения, совещания, и т.д.), содержащей сведения, составляющие государственную тайну.

Доступность информации - состояние информации, характеризуемое способностью технических средств и информационных технологий обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия.

Защищаемые помещения - помещения (служебные кабинеты, актовые, конференц-залы и т.д.), специально предназначенные для проведения конфиденциальных мероприятий, в ходе которых обрабатывается речевая информация, содержащая сведения конфиденциального характера.

Целостность информации - устойчивость информации к несанкционированному или случайному воздействию на нее в процессе обработки техническими средствами, результатом которого может быть уничтожение, искажение или подделка информации.

Защита информации - деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Конфиденциальность информации - субъективно определяемая характеристика, указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и и обеспечиваемая способностью системы сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на право доступа к ней.

Контролируемая зона - это пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание сотрудников и посетителей организации, а также транспортных средств.

Классификация АС по уровню защищенности - деление АС на соответствующие классы по условиям их функционирования с точки зрения защиты информации в целях разработки и применения обоснованных мер по достижению требуемого уровня защиты информации.

Конфиденциальная информация - информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Коммерческая тайна - конфиденциальная информация, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов,сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Несанкционированный доступ к информации (НСД) - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых

средствами вычислительной техники (СВТ) или автоматизированной системой (АС).

Объект информатизации - совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров

Персональные данные - информация (зафиксированная на материальном носителе) о конкретном человеке, которая отождествлена или может быть отождествлена с ним. К персональным данным относятся биографические и опознавательные данные, личные характеристики, сведения о семейном, социальном положении, образовании, профессии, служебном и финансовом положении, состоянии здоровья и прочие.

Руководящий документ по защите информации (РД) - документ, излагающий систему взглядов, основных принципов,которые закладываются в основу проблемы защиты информации от несанкционированного доступа, являющегося частью общей проблемы безопасности информации.

Средство вычислительной техники - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Служебная тайна - защищаемая по закону конфиденциальная информация, ставшая известной в государственных органах и органах местного самоуправления только на законных основаниях и в силу исполнения их представителями служебных обязанностей, а также служебная информация о деятельности государственных органов, доступ к которой ограничен федеральным законом или в силу служебной необходимости.

Система защиты информации - совокупность программных и технических средств, создаваемая и поддерживаемая для обеспечения защиты

средств вычислительной техники или автоматизированных систем от несанкционированного доступа к информации.

Сертификация средств защиты информации - деятельность по подтверждению соответствия требованиям государственных стандартов или иных нормативных документов по защите информации, утвержденных уполномоченными государственными структурами.

Специальные проверки (СП) - проверки компонентов оборудования, осуществляемая с целью поиска и изъятия закладочного устройства.

Специальные исследования (СИ) - выявление с использованием контрольно-измерительной аппаратуры возможных технических каналов утечки защищаемой информации от основных и вспомогательных технических средств и систем и оценка соответствия защиты информации требованиям нормативных документов по защите информации.

ФСТЭК - Федеральная служба по техническому и экспортному контролю - организация,являющаяся федеральным органом исполнительной власти,осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по вопросам:

1. Обеспечения безопасности информации в системах информационной телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства в информационной сфере (далее - безопасность информации в ключевых системах информационной инфраструктуры);

2. Противодействия иностранным техническим разведкам на территории Российской Федерации (далее - противодействие техническим разведкам);

3. Обеспечения защиты (не криптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом,предотвращения ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания,

уничтожения, искажения и блокирования доступа к ней на территории Российской Федерации (далее - техническая защита информации);

4. Защиты информации при разработке, производстве, эксплуатации и утилизации не информационных излучающих комплексов, систем и устройств;

5. Осуществления экспортного контроля.

1.2.Анализ теоретических основ построения телекоммуникационных сетей

ТКС (телекоммуникационная система) представляет из себя средства передачи сравнительно больших объемов информации (обычно в цифровом виде) с помощью специализированных каналов связи или радио эфира[31]. При этом телекоммуникационная система должна обслуживать большое количество пользователей (начиная от нескольких тысяч и более). Понятие телекоммуникационной сети включает в себя следующие системы передачи информации: телевизионное вещание (общее, спутниковое, кабельное), телетелефонные сети общего пользования (ТфОП), системы связи на основе сотовых сетей (макро- и микро-сотовые), спутниковые системы связи и навигационное оборудование, волоконные сети передачи информации.

В состав типичной телекоммуникационной системы входят следующие составляющие: серверы, компьютеры (хосты), каналы связи и активное оборудование, такое как модемы, маршрутизаторы, коммутаторы, концентраторы, сетевые мосты, повторители и так далее.

Важной частью телекоммуникационной системы(ТКС) является СКС(структурированная кабельная система) [31]. Это совокупность каналов связи и различного коммутационного оборудования, которая обязательно должна соответствовать требованиям определенных нормативных документов.СКС включает в себя набор каналов передачи информации (кабелей) и коммутационного оборудования. Так же должна присутствовать некая схема для совместного использования этих элементов с целью регулярного расширения структуры сети. СКС является физической основой

инфраструктуры объекта (здания или нескольких соседних зданий) и позволяет объединить в одну систему множество различных сетей разного рода, таких как локальные сети, системы видеонаблюдения, системы безопасности, телефонные сети и так далее. Можно сказать, что СКС это физическая основа ТКС.

СКС представляет собой систему из кабелей, смонтированную и расположенную на территории здания или нескольких соседних зданиях. СКС состоит из структурных подсистем. В ее состав входят следующие основные элементы:

Главный кросс (МС) чаще всего находится в главном аппаратном помещении. Предназначен для установления соединения между кабелями так называемого «городского ввода» и кабелями магистральных систем различных уровней. В международном эквиваленте имеет название «распределитель кампуса».

Кабели магистральной подсистемы первого, второго и т.д. уровней – это кабели соединяющие главный кросс, промежуточные кроссы и т.д., в зависимости от размеров самой СКС.

Промежуточные кроссы (IC) соединены с распределителем кампуса кабелями магистральной подсистемы.

Горизонтальные кроссы (HC) и кабели горизонтальной подсистемы.Группа соединителей, обслуживающих кабели горизонтальной системы и позволяющие выполнять их подключение к кабелям магистральной системы и сетевому оборудованию с помощью коммутационных шнуров и перемычек. Так же его называют распределитель этажа. Это название используется в международном стандарте и является эквивалентом термину горизонтальный кросс.

Консолидационные точки (CP). Консолидационная точка разделяет горизонтальную кабельную линии на два участка: фиксированный участок от ЭРП до консолидационной точки, который остается неизменным на протяжении срока службы СКС и участок от консолидационной точки до телекоммуникационной розетки, который может время от времени изменяться.

Телекоммуникационные розетки (ТО);

Правильное построение СКС при проектировании телекоммуникационной сети должно удовлетворять заданным показателям качества обслуживания. Основным требованиям к телекоммуникационным системам является отсутствие такого фактора, как прерывание связи. При этом может допускаться возможное ухудшение качества связии может затрачиваться некоторое время на установку соединения.

1.2. Основные факторы отличия различных видов телекоммуникационных сетей

Телекоммуникационные системы можно примитивно разделить на следующие виды:

- Телеграфная связь.
- Телефонная связь.
- Радиосвязь.
- Спутниковая связь.
- Компьютерные сети.

Старейшим способом передачи информации с помощью технических средств на большие расстояния является телеграфная связь. При том, что телеграфный аппарат был изобретен в начале XIX века, во многих сферах этот способ передачи сообщений используется и по настоящее время. Данный способ передачи информации является основой современных технических средств телекоммуникаций.

В 1876 году, после первого запатентованного Александром Беллом телефонного аппарата, началось бурное развитие телефонных сетей, которое не прекращается и по настоящее время. На то время он назывался «говорящий телеграф». Сейчас по каналам телефонной сети общего пользования передается не только речевая информация, но и факсимильные сообщения, и цифровые данные. Изначально телефонные сети предназначены для передачи

по ним аналоговых сигналов. Аналоговый сигнал является непрерывным и может принимать значения из некоторого диапазона. Например, аналоговым сигналом является человеческая речь; в телефоне, телевизоре, радиоприемнике информация также существует в аналоговой форме. Недостатком такой формы представления информации является ее подверженность помехам.

Цифровая же форма сигнала кардинально отличается от аналоговой формы. В ее основе лежат лишь два числовых значения. 0 – отсутствие электрического сигнала и 1 – его наличие. Для передачи таких сигналов по телефонным каналам связи нужны специальные устройства для преобразования цифрового сигнала в аналоговый и наоборот. Такие устройства называются модемы или модуляторы и демодуляторы, соответственно. Таким образом, телефонные сети являются основой более сложных сетей – компьютерных.

Так же телефонные сети послужили основой и еще для одного вида передачи данных. Это сети мобильной связи. Они формируются из телефонной связи и радиосвязи. Так же их называют сотовые сети. Такое название они получили из-за специфичных особенностей организации таких сетей. Сотовые сети представляют собой систему, состоящую из большого числа передатчиков (вышек связи). Каждый передатчик покрывает лишь определенную территорию (зону покрытия). Если схематично обозначить линии пересечения этих зон, получится нечто похожее на соты. Перемещаясь в зоне покрытия сети, «абонент» попадает то в зону действия одного передатчика, то другого. Связь при этом не прерывается, поскольку происходит автоматическое переключение от одного передатчика к другому. Так же системы сотовой связи в качестве каналов передачи информации могут задействовать как телефонные сети общего пользования, так и спутниковую связь. Применяются эти каналы для связи между различными узлами сети, а так же для связи с «главным терминалом». Связь абонента с передатчиком осуществляется по радиоканалам на частотах примерно от 900 до 2100 МГц. На высоких частотах организованы так называемые 3G и 4G сети.Радиосвязь в деятельности большинства организаций редко применяется непосредственно для передачи информации

между двумя конечными абонентами. Однако каналы радиосвязи являются важной составной частью вычислительных сетей - в первую очередь сети Интернет и корпоративных сетей большой протяженности.

Спутниковые телекоммуникационные системы получили большее распространение в различных сферах. С каждым днем появляется все больше спутниковых сетей. Часто они используются как канал передачи данных в других системах связи, в частности при создании глобальных вычислительных компьютерных сетей. Большое распространение спутниковые сети получили в сфере телевиденья. Основным и самым дорогостоящим оборудованием в спутниковых системах являются непосредственно сами искусственные спутники. Спутники, используемые для работы спутниковых сетей, делятся на три основных типа, в зависимости от их высоты полета и орбиты:

- Спутники на низких круговых орбитах (низколетящие спутники).
- На эллиптических орбитах.
- Геостационарные спутники.

Самыми многочисленными сетями на сегодняшний день являются компьютерные вычислительные сети. Этот класс телекоммуникационных сетей начал широко развиваться в настоящее время, в связи с появлением множества новых технологий. Поэтому компьютерным сетям уделяется особое внимание в современной науке и технике. Самая распространенная классификация компьютерных вычислительных сетей – это классификация по территориальному признаку. По этому признаку сети разделяют на два основных вида:

- Локальные (Local Area Network — LAN).
- Глобальные (Wide Area Network — WAN).

Локальные сети (LocalAreaNetwork — LAN) являются совокупностью компьютеров, находящихся на сравнительно небольшой территории. Обычно в пределах одного здания и принадлежащих одной организации. Как правило, в

таких сетях имеет место дорогое телекоммуникационное оборудование, за счет малого расстояния между отдельными компьютерами. Это в свою очередь обеспечивает высокую скорость и качество передачи информации.

Глобальные сети (WideAreaNetwork — WAN) как правилосостоят из большого числа узлов. Они могут находиться в разных городах, регионах, странах и даже континентах. Для функционирования таких сетей могут использоваться другие каналы связи, такие, как например спутниковая связь. Это значительно упрощает процесс организации WAN и снижает их стоимость, за счет того, что исключаются расходы на дополнительные каналы связи, которые должны быть проложены на большие расстояния. Так же использование сторонних каналов позволяет сделать глобальную сеть доступной для большого числа абонентов. Работа глобальной сети основана на мощном вычислительном оборудовании.

Городские (региональные) сети (MetropolitanAreaNetwork — MAN) используются для соединения локальных сетей, находящихся территориально близко друг к другу (в пределах одного населенного пункта) и для связи локальных и глобальных сетей.

Так же можно выделить сети, используемые для обеспечения связи далеко удаленных друг от друга пользователей, но находящихся в пределах одной организации. Их называют корпоративные сети. Например, любая компания, имеющая два или более филиала нуждается в такой сети для оперативного обмена данными. Такие сети создаются для конкретной организации, в зависимости от ее потребностей. Корпоративные сети используют для передачи данных другие сети: телефонные, локальные и сеть Интернет.

LAN(Локальные вычислительные сети)

Главной отличительной особенностью локальных сетей является тот факт, что все ее составляющие, такие как компьютеры, каналы связи, сетевое оборудование, обычно находятся в ограниченных пределах.

Наличие в какой либо фирме, или другой организации локальной вычислительной сети дает ей ряд преимуществ, таких как:

- Возможность работы различных пользователей с одними и теми же файлами, документами или базами данных.
- Возможность быстрого обмена информацией между пользователями данной сети.
- Возможность создавать «распределенные базы данных». Это такие базы данных, информация которых физически расположена не на одном, а на нескольких компьютерах.

В процессе построения сети LAN для определенной организации необходимо знать какие функции будут возлагаться на данную сеть, и какие с её помощью будут решаться задачи. Как правило, крупные компании нанимают специальные фирмы (системные интеграторы) для решения подобных вопросов. Целью подобных фирм является разработка подходящей архитектуры и топологии сети, подбор необходимого коммуникационного оборудования, отвечающего всем запросам клиента.

Так же очень важным моментом является экономический вопрос построения локальной сети на предприятии. Системные интеграторы должны предложить клиенту оптимальное оборудование с точки зрения «цена - качество». После разработки архитектуры сети, готовая модель проходит тестирование на реальном сетевом оборудовании в специально оборудованном помещении. Только после всех проверок переходят непосредственно к стадии создания физической локальной сети.

Классификация локальных вычислительных сетей.

Чаще всего с точки зрения физического устройства ЛВС разделяют по типу канала связи, используемого между узлами сети. В качестве каналов связи на сегодняшний день существует три наиболее распространенных типа кабеля. Это витая пара, коаксиальный кабель и оптоволоконный кабель. При

выборе подходящего для конкретной ЛВС типа кабеля, обычно учитывают следующие их показатели:

- Стоимость установки и обслуживания сети с данным типом кабеля. Стоимость самого кабеля, стоимость его установки и последующего обслуживания.
- Скорость передачи данных. Максимальная пропускная способность данного типа кабеля.
- Максимальное расстояние передачи. Имеется в виду то расстояние, на которое информация может передаваться по данному типу кабеля без специальных устройств для усиления сигнала (повторителей или репитеров).
- Помехозащищенность и безопасность данного типа кабеля.

Самым простым и дешевым типом кабеля является витая пара (twistedpair). Данный кабель представляет собой несколько жил, изолированных и скрученных между собой с большим количеством витков на единицу длины. Это делается с целью уменьшения помех. На сегодняшний день существует около 12 категорий витой пары. Они отличаются друг от друга количеством жил, способом экранирования и частотным диапазоном. Все эти показатели влияют на пропускную способность и на стоимость, соответственно. В кабелях категории 5 и выше жилы вьются с различным шагом ветвления для снижения наводок сплетенных пар кабеля друг на друга. Самый распространенный кабель на данный момент – это кабель категории «5е». Его пропускная способность составляет 100 Мбит/сдля кабеля с двумя парами и 1000 Мбит/с для кабеля с четырьмя парами. Такиестандартыпередачиназываются Fast Ethernet (100BASE-TX)иGigabit Ethernet (1000BASE-T). Такжесуществуютстандарты10 Gigabit Ethernet (10GBASE-T) и100 Gigabit Ethernet (40GBASE-T).

Коаксиальный кабель применяется для передачи данных на большие расстояния по сравнению с витой парой, поскольку имеет большую помехозащищенность. Сейчас этот тип кабеля практически не используется для построения вычислительных сетей, так его пропускная способность в локальных сетях ограничена и составляет не более 10 Мбит/с. Главной сферой его применения стало кабельное телевиденье, где сведение помех к минимуму так же является главной задачей, а пропускная способность коаксиального кабеля вполне достаточна.

Самый дорогой тип телекоммуникационного кабеля – это оптоволоконные кабели. Применение оптического волокна для телекоммуникаций обусловлено в основном высокой пропускной способностью такого канала. Абсолютный рекорд скорости передачи информации по оптоволоконному кабелю на сегодняшний день составляет 5,1 Тбит/сна одну жилу. С помощью специального алгоритма передачи через 50 потоков удалось добиться скорости в 255 Тбит/спри длине самого кабеля в 1 километр.Так же к преимуществам этого кабеля можно отнести высокую защищенность, так как информацию, передаваемую по оптоволоконному кабелю очень сложно перехватить по ходу ее следования сторонним оборудованием и низкие показатели затухания при передаче на большие расстояния.

WAN (глобальные вычислительные сети).

Безусловно, самой большой из существующих ныне глобальных сетей, является сеть Internet, которая начала развиваться в 1969 году на основе сети ARPAnet (AdvancedResearchProjectAgency). Эта сеть разрабатывалась специальным подразделением министерства обороны США AdvancedResearchProjectsAgency (DARPA). Сеть предназначалась для связи удаленных подразделений оборонной промышленности, научных центров и военных государственных учреждений между собой. При создании этой сети большой упор ставился на ее безопасность, и предполагалась, что она должна

была продолжать функционировать даже в условиях ядерной войны.Основные принципы построения сети ARPAnet:

- Каждый из узлов должен быть соединен с другими. Это создает множество путей от одного узла к другому.
- В каждом узле есть таблицы перенаправления пакетов, которые автоматически обновляются. Этот факт может характеризовать каждый узел как «надежный».
- Пакет, передаваемый на узел, не соседний с передающим, отправляется на ближайший узел к узлу получателю. В случае если тот не доступен, на следующий в списке перенаправления пакетов и так далее.

В некоторых источниках вычислительные сети делятся на три класса. Это объектовые сети, магистральные сети и граничные сети.

- Объектовые сети- крупные локальные сети объекта с повышенным уровнем электромагнитных и электрических излучений. Такие сети размещаются на значительной площади и в основном предназначены для объединения терминалов различного типа, устройств управления, контроля и защиты, крупных ЭВМ с мощной периферией.
- Магистральная сеть - Совокупность сегментов сети, узлов и отдельных станций, которые подключаются к общей высокоскоростной линии связи через мосты, маршрутизаторы и концентраторы каналов.
- Граничная сеть или защитная подсеть – изолированная, несопряженная подсеть, которая размещается между защищенной и незащищенной сетями. В ней управление соединениями и пакетами достигается применением двух пакетных фильтров. Ее часто называют демилитаризованной зоной.

Сети связи специального назначения.

Это сети электросвязи, предназначенные для производственных потребностей органов государственной врасти Российской Федерации. Они отдельны от сетей общего пользования. Все сети общественного пользования, расположенные на территории Российской Федерации образуют «единую сеть электросвязи Российской Федерации». Она может использоваться для нужд государства в любое необходимое время. Все взаимодействия государства с сетями общего пользования регулируются законодательством Российской Федерации. Часто в государственных телефонных сетях есть так называемые «прямые телефоны». Такие телефоны обеспечивают соединение только лишь с одним абонентом. В таких случаях нет нужды в коммутации вызова.

Федеральный закон от 07.07.2003 N 126-ФЗ "О связи"[3]

Статья 16. Сети связи специального назначения.

1. Сети связи специального назначения предназначены для нужд органов государственной власти, нужд обороны страны, безопасности государства и обеспечения правопорядка. Эти сети не могут использоваться для возмездного оказания услуг связи, услуг присоединения и услуг по пропуску трафика, если иное не предусмотрено законодательством Российской Федерации.

(в ред. Федеральных законов от 08.12.2011 N 424-ФЗ, от 02.03.2016 N 44-ФЗ)

2. Связь для нужд органов государственной власти, нужд обороны страны, безопасности государства и обеспечения правопорядка осуществляется в порядке, определенном законодательством Российской Федерации, ее обеспечение является расходным обязательством Российской Федерации.

(п. 2 в ред. Федерального закона от 08.12.2011 N 424-ФЗ)

3. Подготовка и использование ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования сетей связи специального назначения осуществляются в порядке, установленном Правительством Российской Федерации.

3.1. Сети связи специального назначения могут быть присоединены к сети связи общего пользования без перевода в категорию сети связи общего пользования.

Владельцу сети связи специального назначения может быть выделен ресурс нумерации из ресурса нумерации сети связи общего пользования.

В случае присоединения сетей связи специального назначения к сети связи общего пользования на основании указанного в пункте 1 статьи 18 настоящего Федерального закона договора стороны такого договора обеспечивают пропуск трафика по указанным сетям связи в рамках исполнения такого договора с учетом ограничения использования сетей связи специального назначения, указанного в пункте 1 настоящей статьи.

(п. 3.1 введен Федеральным законом от 02.03.2016 N 44-ФЗ)

4. Центры управления сетями связи специального назначения обеспечивают их взаимодействие с другими сетями единой сети электросвязи Российской Федерации в порядке, установленном федеральным органом исполнительной власти в области связи.

Телекоммуникационное оборудование.

Любая телекоммуникационная сеть нуждается в специальных сетевых устройствах, обеспечивающих и регулирующих ее корректную работу. Эти устройства используются для передачи аудио, видео и другой информации между устройствами разного типа. Телекоммуникационное оборудование используется при организации телефонной связи, мобильной связи и при передаче в глобальной сети Internet. Сетевое оборудование можно разделить на пассивное и активное оборудование.

К пассивному оборудованию относится все оборудование не питающееся от электросети. Так же оно передает сигнал без его усиления. Пассивное сетевое оборудование, в свою очередь, так же можно разделить на две группы. Первая - это сетевое оборудование, являющееся каналами передачи

информации. В нее входят телекоммуникационные розетки, кабели различных типов, коммутационные панели (кросс-панели). Самый используемый тип кабеля на сегодняшний день – это витая пара. Этот кабель может быть как экранированным, так и нет, в зависимости от назначения сети. Существует три типа экранирования витой пары.

- UTP (unfoiledtwistedpair) – экранирование полностью отсутствует.
- FTP (foiledtwistedpair) – Экранирование каждой отдельный пары. Защищает от наводок между соседними парами.
- STP (shielded unfoiled twisted pair) – Кабельэкранированвнешне. Защищает от внешних электромагнитных излучений и наводок.
- S/FTP или SFTP (shieldedfoiledtwistedpair) – Экранированы как отдельные пары жил, так и весь кабель.

Вторая группа – это вспомогательное оборудование, используемое при построении структурированной кабельной системы. Включает в себя различные кронштейны, кабель-каналы, телекоммуникационные шкафы, хомуты и так далее.

Активное сетевое оборудование, в свою очередь, отвечает, непосредственно, за все этапы и нюансы передачи информации. К нему относят маршрутизаторы, коммутаторы, повторители, модемы, хабы, межсетевые экраны серверы и т.д.Если речь идет о компьютерных вычислительных сетях, работа которых основана на пакетной передачи данных, то сетевые устройства выполняют огромное множество разнообразных функций. От поиска наиболее подходящего маршрута для трафика до объединения в одну сеть огромного количества пользователей.

Самым распространенным видом сетевых устройств являются так называемые сетевые коммутаторы (свитчи) и маршрутизаторы. Оба этих устройства могут выступать в качестве сетевого концентратора. То есть выполнять функции объединения компьютеров в сети Ethernet. Сами сетевые концентраторы, как отдельные устройства очень примитивными в настоящее время сильно устарели. Принцип их работы заключается в том, что пакет,

полученный от одного узла сети, рассылается всем остальным, которые подключены к хабу. А решение, адресован ли был пакет именно этому компьютеру, принимается уже самим компьютером. Если пакет был адресован не ему, он просто отбрасывается. Сетевые концентраторы работают только лишь на физическом уровне модели OSI.

Сетевой коммутатор или «свитч» является более функциональным устройством. Он так же объединяет несколько узлов одной сети, но в отличии от хаба, он передает данные именно получателю. То есть в нем присутствует некая программная составляющая. В памяти свитча хранятся таблицы марштрутизации, с помощью которых он соотносит MAC адреса узлов со своими выходными портами. Изначально (при начале работы коммутатора) таблицы маршрутизации пусты. Они заполняются в ходе его работы. Это уменьшает время обработки кадров. Сетевыми коммутаторами принято называть устройства, работающие на канальном уровне модели OSI и оперирующие так называемыми «кадрами».

Маршрутизатор (роутер) устройство, работающее на третьем (сетевом) уровне сетевой модели OSI. Маршрутизатор рассылает пакеты между сегментами сети, так же пользуясь таблицами маршрутизации, как и коммутатор. Так же он способен соединять между собой сети различных архитектур. Все решения о пересылки пакетов принимаются исходя из правил, заданных «администратором». Важной особенностью маршрутизаторов является наличие большого объема внутренней памяти, что позволяет строить огромное множество маршрутов. В основном скорость обработки данных в маршрутизаторе меньше, нежели в коммутаторе. Это обусловлено тем, что зачастую маршрутизатор руководствуется не только IP и MAC адресами, а проверяет весь пакет данных целиком. Это обусловлено тем, что роутер может выполнять множество других функций от функции межсетевого экрана, до обеспечения приоритезации трафика. К слову не правильно отличать коммутаторы от маршрутизаторов только лишь по уровню модели OSI, а котором они работают. Существуют коммутаторы, работающие и на сетевом

уровне. Поэтому иногда сложно провести грань между понятиями коммутатор и маршрутизатор. Многие специалисты предпочитают делить все сетевые устройства по уровням, на которых они работают.

Устройство уровня L1 – это все устройства, которые работают на физическом (первом) уровне модели OSI. В них вообще отсутствуют какие либо механизмы маршрутизации. Они воспринимают лишь электрический сигнал на входном порту, который в итоге передается дальше через выходные. Такие устройства получили большое распространение во время появления сетей стандарта Ethernet. Так же к ним относятся повторители (репитерsы), просто усиливающие входной сигнал.

Устройства уровня L2 – эти устройства работают на канальном (втором) уровне модели OSI. Они выполняют физическую адресацию и работают с кадрами (фреймами). Устройства второго уровня выполняет адресацию только лишь по MAC-адресам, так как IP-адрес является частью третьего уровня. Их как раз, обычно называют коммутаторами. Но, поскольку существуют коммутаторы так же и третьего уровня, целесообразно говорить «коммутаторы L2».

Устройства уровня L3 – устройства, работающие на сетевом (третьем) уровне сетевой модели OSI,поэтому имеют возможность определять наикратчайший маршрут для передачи пакета. Они оперируют IP-адресами. Такие устройства принято называть маршрутизаторами или коммутаторами L2.

Устройства уровня L4 – Устройства, отвечающие за безопасность передаваемых данных. На основании информации, находящейся в заголовке пакета они могут относить трафик к различным приложениям прикладного уровня. Так же они могут принимать решения о каких либо действиях с различным трафиком, например о его перенаправлении. Эти устройства работают с протоколами транспортного уровня TCP и UDP. Но часто коммутаторы L4 используют в своей работе данные более высоких уровней.Главной особенностью устройств 4 уровня является то, что они имеют возможность оперировать списками контроля доступа и фильтровать их. Это

повышает безопасность передаваемых данных. Часто их называют «интеллектуальные коммутаторы». Доступ к уровню 4 имеют, например коммутаторы компании CISCO серии 7500. Коммутаторы уровня 4 могут управлять выделением пропускной способности для различных типов пакетов. Это позволяет реализовать службы QoS и выравнивать загрузку сетевых каналов. Функции настройки QOSприоритезации трафика имеются на большинстве современных маршрутизаторов в средней ценовой категории.

1.3. Анализ основных методов обеспечения безопасности информации в сети

Для того, чтобы понять и выявить основные методы обеспечения безопасности в сети, нужно для начала выявить угрозы которым может быть подвержена сеть. Угрозы безопасности данных можно разделить на два основных типа:

- Технические.
- Физические (человеческий фактор).

В дальнейшем будут рассматриваться только технические угрозы. Их можно формально разделить на пять основных групп:

- Ошибки в программном обеспечении.
- Разнообразные хакерские атаки(DoS- и DDoS-атаки).
- Компьютерные вирусы, черви, «троянские кони».
- Анализаторы протоколов и прослушивающие программы («снифферы»).
- Технические средства съема информации.

Ошибки в программном обеспечении серверов или маршрутизаторов встречаются практически всегда, так как в этом случае играет роль человеческий фактор. Можно полагать, что чем сложнее само программное обеспечение, тем больше вероятность присутствия в нем ошибки, в том числе и в системе безопасности. Некоторые такие ошибки могут быть использованы злоумышленником в своих целях.

DoSи DDoSатаки могут так же сильно навредить сети и оборудованию, находящемуся в ней. А так же и информации представляющей некую ценность. Суть таких атак заключается в перегрузки активного оборудования сети или каналов связи, путем отправления большого количества различных запросов со множества удаленных компьютеров. В следствие этого каналы связи или же буферные ресурсы оборудования забиваются «паразитным» трафикам, и доступ к пользователей к ресурсам данной сети становится невозможным.

В

Для распространения вирусов и прочих вредоносных программ злоумышленникобычно использует либо уязвимости программного обеспечения, либо рассылку по таким ресурсам, как электронная почта. В настоящее время компьютерные вирусы стали менее распространены, в связи с появлением более простых для злоумышленника видов атак.

Так называемые «снифферы» могут быть как аппаратными так и программными. Принцип их действия заключается в перехвати сетевого трафика. Так как большинство данных передаются в сети в открытом виде, злоумышленник может их легко перехватить. Например, многие приложения и ресурсы не используют шифрования при передаче паролей, что позволяет легко узнать эти пароли.

Технические средства съема информации довольно слабо распространены, но представляют наибольшую угрозу, так такие средства обеспечения безопасности, как шифрование, для них бессильны. Ими могут являться различные жучки, например клавиатурные или же специальные устройства, устанавливаемые на провода ПК и считывающие с них полезную информацию на основе ПЭМИН.

На основе данных угроз можно сделать следующие выводы. Для обеспечения безопасности в сети необходимо обеспечить два основных критерия безопасности:

- Внутреннюю безопасность.
- Внешнюю безопасность.

Исходя из общедоступной информации можно сделать выводы, что не малую часть потерь, которые несут предприятия, в следствии неправомерных действий злоумышленников, составляют те, на которые так или иначе повлияли собственные сотрудники. Но сеть так же должна быть защищена от неправомерных действий внешних атак злоумышленников.

Исходя из перечисленных угроз, можно выявить следующие методы обеспечения безопасности информации в сети:

1. Установка в сети межсетевого экрана.

Межсетевой экран является первостепенным устройством, которое должен преодолеть злоумышленник. Основной принцип его действия заключается в фильтрации нежелательных пакетов. Межсетевые экраны можно разделить по уровню контроля доступа на три основных типа:

- Сетевые экраны, фильтрующие пакеты на основе простых правил. Это могут быть адреса отправителя или же номер входного порта.
- Сетевые экраны, которые работает на сеансовом уровне модели OSI. Он отфильтровывает все пакеты TCP/IP, которые счел подозрительными на основании заданных заранее алгоритмов.
- Сетевые экраны, которые работают на прикладном уровне. Они производят фильтрацию пактов на основании даннах, передаваемых внутри пакета.

2. Использование технологий VPN.

Во многих случаях защищаемая сеть требует связи с другой локальной сетью или же к ней необходимо иметь доступ удаленно. При таком доступе к сети по факту должны использоваться открытые каналы связи, например сеть Интернет. Технология VPNпозволяет обезопасить доступ к сети из вне. Это осуществляется за счет так называемого туннелирования и шифрования трафика. Функции реализатораVPNможет выполнять межсетевой экран, если он поддерживает такие функции.

3. Использование системы обнаружения атак (IDS).

Системы IDSпредставляют из себя аппаратное или же программное средство, целью которого является выявление неавторизованного доступа в сеть. Такие системы могут выявить как факт сканирования портов оборудования, так и попытки несанкционированного управления системой. В таких случаях система IDScообщает системному администратору (или администратору безопасности) о факте НСД и, при наличии у нее таких полномочий, может сама изменить политику межсетевого экрана или же напросто заблокировать все подключения.

4. Защита от вирусов.

Антивирусная защита, в большей степени обеспечивает безопасность отдельных ПК. Более продвинутые антивирусные пакеты рассчитаны на централизованное обеспечение безопасности. Современные антивирусы могут выполнять функции программного межсетевого экрана, реализовывать фильтрацию спама и предупреждать о вредоносном ПО, а так же подозрительных сайтах. На некоторых моделях межсетевых экранов так же могут быть установлены антивирусные программные обеспечения.

4. Использование функций «черных и белых списков».

Данные функции могут быть реализованы как в антивирусном пакете, так и с помощью стороннего программного обеспечения. Принцип их действия заключатся в наличии определенного списка в который внесены конкретные приложения или сайты. В случае использования «черных списков» разрешается запуск любых приложений кроме тех, которые внесены в данный список. Принцип работы «белых списков» обратных. В нем внесены только лишьте приложения, работа которых разрешена.

5. Своевременное обновление программного обеспечения.

Данный факт является очень важным пи обеспечении безопасности в сети. Различное программное обеспечение регулярно обновляется производителем, так как злоумышленники с определенной периодичностью находят в нем изъяны.

6. Обеспечение физической безопасности сети.

При физическом доступе к сетевым устройствам, злоумышленник может легко получить доступ к самой сети и, как следствие к конфиденциальной информации. Так же злоумышленник может получить доступ к информации, в следствии некорректного обращения сотрудников с носителями информации. Например, после замены жестких дисков, старые должны утилизироваться. Физическая безопасность информации должна регулироваться политикой безопасности организации.

2. Определение понятие качества обслуживания в телекоммуникационных сетях

Обычно при выборе поставщика услуг доступа в Интернет, сетевого оборудования, подходящей топологии сети, встает вопрос не только цены, но и многих, разнообразных технических параметров. Во многих случаях недостаточно просто «быстрого» канала передачи данных. В этом случае к нему применяется такой термин, как «качественный». А вслед за ним появляется такое понятие, как QualityofService или, коротко, QoS. В процессе развития современных телекоммуникационных сетей в первую очередь внимание уделяется повышению качества обслуживания. А главной проблемой в этом является разнообразие запросов различных пользователей и сетевых приложений. В современных ТКС это происходит с помощью разнообразных технологий и протоколов почти на всех уровнях сетевой модели OSI. Одним из важных инструментов являются протоколы маршрутизации, работающие на сетевом уровне сетевой модели OSI. От их работы на прямую зависят показатели качества обслуживания».

QoS (англ. quality of service — качество обслуживания) — это понятие имеет множество различных определений в различных источниках. Ясчелнаиболееправильнымисодержательнымопределениеамериканскойкомпании CISCO [4]: "QoS – quality of service refers to the ability of a network to provide better service to selected network traffic over various underlying technologies…". Что можно перевести это как: "QoS – способность сети обеспечить необходимый сервис заданному трафику в определенных технологических рамках".

«Умение» конкретной сети отвечать различным запросам от разных сетевых приложений и обеспечивать различные уровни обслуживания для них, а так же контролировать характеристики производительности классифицируется по трём категориям (сервисным моделям QOS):

1. Негарантированная доставка данных (best-effortservice)

В принципе, данная сетевая модель не является механизмом QOS, поскольку не дает гарантию доставки пакета и в ней отсутствует какое либо разделение сетевого трафика на классы. При передаче используются все доступные ресурсы сети, при их нехватке происходит перегрузка и некоторые пакеты «отбрасываются» из-за переполнения очереди в маршрутизаторе. Теоретически от этой проблемы можно избавиться путем увеличения пропускной способности сети. Но, как известно, многие типы трафика очень «чувствительны» к задержкам, например голосовой трафик. А любая сеть, даже со сравнительно большой пропускной способностью может испытать на себе перегрузки из-за резких «всплесков» трафика.

2.Дифференцированное обслуживание (differentiatedservice)

Основой работы модели дифференцируемого обслуживания является факт разделения трафика на так называемые классы. Это осуществляется с помощью классификаторов и формирователей трафика на «краю» сети. Классификаторы и формирователи выполняют функции классификации и маркировки пакетов, а так же функции управления интенсивностью. Для определения типа трафика используется метка DSCP, находящаяся в поле заголовка IPv4 пакета. Так же важной частью модели является политика пошагового обслуживания (Per-HopBehavior). С помощью нее выполняются такие функции, как отбрасывание пакетов и распределение сетевых ресурсов, то есть определяет к какой именно очереди отнести конкретный пакет.Политика пошагового обслуживания представляет из себя алгоритм действий, применимых к пакетам на каждом узле его следования в сети. Существуют 4 типа политики пошагового обслуживания.

- Default PHB
- ExpeditedForwarding PHB (EF)
- AssuredForwarding PHB (AF)
- ClassSelector PHB (CS)

DiffServ можно кратко охарактеризовать как приоритезацию трафика (Prioritization).

3.Гарантированное обслуживание (guaranteedservice) или интегрированное **(**IntegratedService (IntServ)).

Главный признак IntServ это гарантированная пропускная способность. Данная модель предполагает резервирование сетевых ресурсов. Предварительно выполняется резервирование ресурсов сети на всем пути движения данных пакетов. Часто эта модель обслуживания называется «жестким QOS» из-за того, что к ресурсам сети предъявляются жесткие требования. Резервирование сетевых ресурсов осуществляется с помощью протокола RSVP, который еще до непосредственной передачи данных рассылает по маршрутизаторам, находящимся на пути следования пакетов, специальное служебное сообщение в формате протокола RSVP. Это сообщение содержит в себе информацию о требуемой пропускной способности и типе передаваемой информации. Протокол RSVP играет большую роль как в сервисной модели гарантированного обслуживания, так и в технологии QOS в общем.

2.1. Анализ основных показателей качества обслуживания в локальной вычислительной сети

На сегодняшний день существует четыре основных показателя применимых к качеству обслуживания в сетях передачи данных [12]:

- Полоса пропускания (Bandwidth), описывает номинальную пропускную способность среды передачи информации, определяет ширину канала. Измеряетсяв bit/s (bps), kbit/s (Kbps), Mbit/s (Mbps), Gbit/s (Gbps).
- Задержка при передаче пакета (Delay), измеряется в миллисекундах.
- Колебания (дрожание) задержки при передаче пакетов — джиттер (Jitter**).**
- Потеря пакетов (Packetloss). Определяет количество пакетов, потерянных в сети во время передачи.

Обычно любое соединение, нуждающееся в гарантированном качестве обслуживания, требует от сети, чтобы та резервировала определенную минимальную полосу пропускания для этого соединения. Примером являются приложения прикладного уровня модели OSI, использующиеся для передачи речи. Они запрашивают, к примеру, минимальную пропускную способнсть 64 Кбит/с. Если на каком либо участке соединения полоса пропускания,в следствии каких либо причин, меньше 64Кбит/с, работа приложения будет практически не возможна. Можно явно провести аналогию пропускной способности канала, например, с водопроводной трубой или чем-то подобным. В ее рамках Bandwidth – это ширина трубы, а Delay – длина.

Задержки при передаче пакета (packetdelay), или латентность (latency) делятся на три составляющие: задержка сериализации, задержка распространения и задержки коммутации. Задержка сериализации (serializationdelay). Это время, которое нужно сетевому устройству для передачи пакета при заданной ширине полосы пропускания. На задержку сериализации влияют такие параметры как ширина полосы пропускания канала и размер передаваемого пакета. Например, передача пакета размером 64 байт при заданной полосе пропускания 3 Мбит/с занимает всего лишь 171 нс. Передача того же самого пакета размером 64 байт, но уже при заданной полосе пропускания 19,2 Кбит/с занимает уже 26 мс. Довольно часто задержку сериализации называют еще задержкой передачи (transmissiondelay).

Задержка распространения (propagationdelay). Это время, которое нужнопередаваемому биту информации для того, чтобы достигнуть приемного устройства.То есть время, затраченное на весть путь от пункта «А» в пункт «В». На задержку распространения влияют от расстояния между приемником и передатчиком и от используемой среды передачи, но не зависит от полосы пропускания. Измеряется она в миллисекундах [мс]. К примеру, у трансконтинентальных сетей США задержка распространения около 30 см.

Задержка коммутации (switchingdelay). Это время, в течении которого пакет находится на обработке в устройстве. То есть время от получения

устройством пакета, до момента его передачи следующему устройству. Обычно задержка коммутации составляет не более 10 мс.

Так же можно выделить отдельно задержку очереди. Это время, которое пакет находится в очереди в маршрутизаторе. Но это время входит в параметр задержка коммутации.

Как правило, у каждого пакета из одного потока трафика, задержка разная. Это обусловлено постоянным изменением состояния промежуточных сетей и сетевого оборудования[12].

Если в сети имеют место перегрузки, то есть пропускной способности не хватает для всего трафика, проходящего через нее, появляются так называемые «очереди» в маршрутизаторах. Задержка нахождения в очередях влияет на общую задержку при передачи. Этот факт приводит к возникновению разницы в задержках при передачи пакетов одного и того же потока трафика. Колебания задержки называется джиттерпакетов (packetjitter). Это параметр имеет большое значение, потому, что с ним напрямую связано максимальное время задержки при приеме пакетов получателем.

Компенсировать дрожание можно путем «буферизации» пакетов. Это нужно, например, для работы приложения, использующих потоковое видео или для IP-телефонии [12].

Потеря пакетов во время их передачи, происходит в сетевых устройствах в следствии их перегрузки. Отбрасывание пакета может произойти в случае переполнения буфера входной или выходной очереди маршрутизатора.

Исходя из вышесказанного, можно сформулировать некоторые требования, предъявляемые к ТКС, нуждающейся в обеспечении качества обслуживания:

- Поддержка многопутевой маршрутизации (multipathrouting) для обеспечения сбалансированной загруженности ТКС и повышения качества обслуживания в целом;

- Переход к потоковым (flowbased) моделям и методам маршрутизации ввиду того, что современный сетевой трафик имеет преимущественно потоковую природу;
- Использование композитных метрик, максимально учитывающих соотношение требований относительно численных значений различных QoS-показателей;
- Максимальный учет особенностей обработки пакетов на маршрутизаторах сети, в том числе специфику процессов организации и обработки очередей;
- Обеспечение высокой масштабируемости маршрутных решений, т. е. способности сохранять в заданных пределах свою эффективность в условиях роста территориальной распределенности ТКС, числа и типов обслуживаемых трафиков пользователей и др.

2.2.Анализ основных функции моделей QOS.

Базовые функции QOS являются основой работы всех QOS систем, в их список входят: классификация, разметка, управление перегрузками, предотвращение перегрузок и регулирование. Функции классификации и разметки чаще всего обеспечиваются на входных портах сетевого оборудования, а управление и предотвращение перегрузок – на выходных портах.

Функция классификации и разметки (ClassificationandMarking).

Функция классификации пакетов (PacketClassification) заключается в присвоении конкретному пакету определенного класса трафика.Не менее важной функцией является функция маркировки пакетов, которая назначает каждому пакету определенную метку соответствующего приоритета.В зависимости от уровня сетевой модели OSI, на котором эти функции реализуются, эти задачи решаются по-разному.

Классификация и разметка на канальном уровне сетевой модели OSI (Layer 2ClassificationandMarking).

Коммутаторы Ethernet (Layer 2) используютпротоколы второго уровня модели OSI(канального). Такие протоколы канального уровня, какEthernet не имеют в себе поле приоритета в чистом виде. Поэтому на Ethernet портах (AccessPort) возможна лишь внутренняя (по отношению к коммутатору) классификация по номеру входящего порта и отсутствует какая-либо маркировка.

Более функциональным в плане реализации QOS, является протокол IEEE 802.1P, который работает на основе стандарта 802.1Q. Они работаю в связке между собой следующим образом: 802.1D описывает технологию мостов и является базовой для 802.1Q и 802.1P. 802.1Q описывает технологию виртуальных сетей (VLAN), а 802.1P обеспечение качества обслуживания. В целом, включение поддержки 802.1Q, автоматически дает возможность использования 802.1P.

Классификация и разметка на сетевом уровне сетевой модели OSI (Layer 3 ClassificationandMarking).

Маршрутизирующее оборудование третьего уровня работает непосредственно с протоколом IP и IP-пакетами. В заголовке IP-пакета с целью маркировки трафика предусмотрено специальное поле «TypeofServise (ToS)». Оно состоит из о1 байта, то есть из 8 бит. Это поле может быть заполнено различными способами, в зависимости от требований, предъявляемых к классификации трафика: IP Precedence или DSCP (DiffServCodePoint).Эти способы называются классификаторами. При заполнении заголовка способом IP Precedence (IPP), выделяется 3 бита и поле принимает значения от 0 до 7. Таким образом возможно задать 8 типов обслуживания. Со временем этого количества оказалось недостаточно, и был разработан классификатор, названный DSCP. Он, в свою очередь, состоит уже из 6 бит, то есть может принимать значения от 0 до 63. Таким образом, использование дополнительных трех бит в разы увеличивает количество возможных классов трафика. Так же поле заголовка

DSCP может быть записано в буквенной форме с использованием ключевых слов BE, AF, EF. Последние два бита обычно не используются, но иногда отвечают за сообщение о явной перегрузке сети.

<table>
<tr><td colspan="8">Type Of Servise</td></tr>
<tr><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td></tr>
<tr><td colspan="3">IP Precedence</td><td>D</td><td>T</td><td>R</td><td colspan="2">Not used</td></tr>
<tr><td colspan="6">DSCP</td><td colspan="2">Flow Control</td></tr>
</table>

Рисунок 1 - Сравнение классификаторов DSCP и IP Precedence

Так же в поле TOS биты с 4 по 2 отвечают за следующие значения:

- 4 – отвечает за время задержки IP-пакеты (значение 0 – нормальная задержка, значение 1 – низкая задержка).
- 3 – отвечает за пропускную способность всего маршрута (значение 0 – низкая пропускная способность, 1 – высокая).
- 2 – отвечает за надежность передачи пакета (0 – нормальная, 1- высокая).

По умолчанию поле DSCP представляет собой последовательность нулей. Поле DSCP так же имеет совместимость с IP- Precedence (полем IP приоритета). При согласовании IP- Precedence и DSCP преобразуются три первых, самых значимых бита.

Управление перегрузками (CongestionManagement) и механизмы очередей.

Перегрузки (Congestions).

Основная причина возникновения перегрузки – это скопление трафика, то есть когда скорость входящего трафика превышает скорость исходящего, а также из-за несогласованности скоростей на сетевых интерфейсах. Такие ситуации называются «узкими местами» в сети.Перегрузки в сетевом оборудовании могут возникать как из-за ограниченных внутренних ресурсов

сетевого устройства (ограниченные ресурсы процессора), так и из-за ограниченной скорости выходных интерфейсов. В первом случае пакеты помещаются во входную очередь маршрутизатора, во втором – в выходную очередь. Так как на изменение размера входных и выходных очередей влияет множество факторов, процесс изменения размера очереди является вероятностным процессом. Изучению очередей, в общем, посвящена отдельная область прикладной математики, которая называется теория массового обслуживания. С её помощью возможно организовать алгоритмы для некоторых простых ситуация, но для реальных условиях в сетевых устройствах требуются более сложные модели.

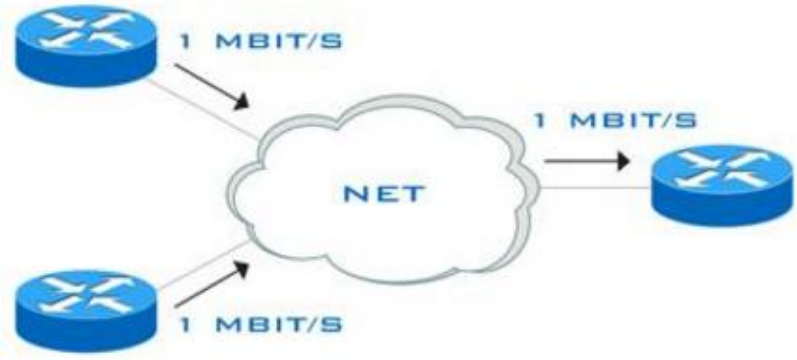

Рисунок 2 - Возникновение очереди в сетевом оборудовании

Устранение перегрузок осуществляется путем управления пропускной способностью сети с помощью механизмов управления очередями. Принцип действия таких механизмов заключается в том, что пакеты ставятся в отдельные очереди, которые в свою очередь обрабатываются с помощью специальных алгоритмов. Проще говоря, управление перегрузками является порядком, в котором пакеты выходят из сетевого интерфейса, основанного на приоритетах, заданных механизмами управления очередями. . Если перегрузки отсутствуют, то механизмы обработки очередей не работают за не имением не то причин.

Методы обработки очередей.

Layer 2 Queuing.

Работа коммутатора по обработке входящих пакетов заключается в следующем: изначально пакет приходит на входной порт коммутатора, далее он обрабатывается неким механизмом коммутации, с помощью которого определяется дальнейший маршрут следования этого пакета. Далее пакет попадает в аппаратную очередь уже выходных портов коммутатора, которая представляет временную память, в которой хранятся пакеты до того, как они попадут на сам выходной порт. За тем пакеты, хранящиеся во временной памяти, направляются на выходной порт по определенным алгоритмам и покидают сетевое устройство. Механизмы обработки очередей отвечают именно за этап, на котором пакеты извлекаются из памяти. С помощью них пакеты могут покидать очереди в определенном порядке, то есть реализовываться приоретизация. Как правило, каждый порт имеет возможность создавать определенное, ограниченное количество очередей. Изначально все очереди равноправные и нуждаются в настройке. Обычно это реализуется с помощью стандарта IEEE 802.1p. Следующим шагом является конфигурация обработчика очередей, так называемого «Scheduler». При этом чаще всего используется или строгий приоритет (StrictPriorityQueuing), при котором один пакет в любом случае имеет приоритет над другим, или же так называемый алгоритм WeightedRoundRobin (WRR). Так же необходимо задать приоритет поступающим пакетам на входном интерфейсе коммутатора. Это делается по входному порту или по CoS. Реализуется это так:

При попадании в коммутатор, если это обычный пакет Ethernet, он не имеет метки приоритета. Такая метка выставляется коммутатором, например по номеру входного порта. Если же порт, в который поступил пакет транковый, то пакет может быть уже с меткой приоритета. Коммутатор может принять пакет с уже готовой меткой или же заменить ее на нужную. В итоге, пакет находится в коммутаторе, имея метку приоритета

Из входного интерфейса пакет попадает на этап коммутации, где определяется его дальнейший маршрут. За тем он попадает в одну из очередей

выходного интерфейса, в зависимости от его метки приоритетности. За тем механизм обработки очередей извлекает пакеты в соответствии с их приоритетами. Таким образом из наиболее приоритетной очереди за определенный промежуток времени будет извлечено больше пакетов, чем из менее приоритетной.

Layer 3 Queuing.

На третьем уровне (сетевом) пакеты обрабатываются устройствами маршрутизации. Обычно маршрутизация осуществляется программно, но может и аппаратно. При программной реализации функция маршрутизации отсутствуют аппаратные ограничения на максимальное количество возможных очередей, а так же появляется больше возможностей для детальной настройки самих механизмов обработки очередей. Процесс обработки пакетов заключается в их маркировке, классификации, распределению по очередям и последующей обработке с помощью механизма обработки очередей.

Существуют четыре основных метода (алгоритма) обработки очередей. Каждый из них создан для конкретных задач и влияет на качество обслуживания конкретного типа сетевого трафика. Эти алгоритмы могут работать как по отдельности, так и в комбинации друг с другом.

FIFO.

Самый простой принцип построения очередей. При возникновении перегрузки, пакеты помещаются в очередь в таком же порядке, как они поступили на входной порт коммутатора. Точнее сказать, они передаются на выход в порядке поступления, так как очередь представляет из себя временную память. От сюда и название алгоритма FIFO - FirstIn - FirstOut. Данный алгоритм по умолчанию применяется во всех коммутаторах и маршрутизаторах, поскольку прост в реализации и не нуждается в дополнительных настройках пользователя. Минусом алгоритма FIFO является

невозможность реализации дифференцированного качества обслуживания в принципе.

Очереди приоритетов.

PriorityQueuing (PQ) позволяет обеспечивать абсолютный приоритет одного пакета над другим. Этот механизм обработки очередей позволяет производить разделение трафика на N классов, которым в свою очередь соответствуют N выходных очередей. Классификация трафика может осуществляться различными способами. Например, разбиение пакетов на классы может осуществляться исходя из типа протокола пакета, адреса отправителя, в зависимости от порта на который пришел пакет или в зависимости от наличия у пакета метки приоритета, заданной отправителем. В любом случае, данный метод обработки очередей требует от пакета наличия в нем поля для записи туда значения, присвоенного пакеты при расстановке приоритетов. Этим значением так же будут пользоваться все устройства на пути следования пакета в сети, если их политики соответствуют политике данного сетевого устройства. В случае, если несколько устройств на маршруте имеют различную локальную политику, приоритет этого пакета будет изменяться в зависимости от каждого устройства осуществляющего приоритезацию. Помимо различного сетевого оборудования приоритет может устанавливаться приложениями прикладного уровня отправителя. После процедуры классификации входящий трафик помещается в очередь, в соответствии с заданным ему приоритету. Как правило, обычно трафик делится на четыре класса и размещается в четыре очереди: low, normal, medium и high. Каждая вышестоящая очередь имеет абсолютный приоритет над очередью, чей приоритет ниже. То есть пока очередь «high» не будет полностью очищена, обработка не переходит к нижестоящей очереди. Размер буферной памяти каждой очереди ограничен неким предельным значением и когда буфер переполнен, пакет, поступающий в буфер, отбрасывается.

Как правило, по умолчанию для всех очередей предусмотрены равные по объему значения буферной памяти, однако многие модели сетевого оборудования позволяют настраивать размер очередей, например оборудование фирмы «ciscosystems»[5]. Чем выше приоритет у трафика (чем в более приоритетной очереди он находится), тем выше у него показатели качества обслуживания на конечном узле. В случае, когда пропускная способность выходного интерфейса и производительность вычислительных (внутренних) блоков сетевого устройства не меньше, чем интенсивность входного трафика, пакеты, имеющие наивысший приоритет получают необходимую для них пропускную способность. Более низкоприоритетные классы, в свою очередь, получат меньшую пропускную способность и, соответственно обеспечивают более низкое качество обслуживания. Построить график ухудшение качества обслуживания при понижении класса трафика, довольно сложно. Это объясняется тем, что интенсивность трафика более высокой очереди может быть разной, а соответственно процент загруженности полосы пропускания будет различным. Приоритетное обслуживание, как правило используется для передачи чувствительного к задержками трафика небольшой интенсивности. Это позволяет оставлять достаточно пространства для всего остального (нижестоящего по приоритету) трафика. Примером можно привести IP-телефонию или голосовой трафик любого другого типа.

Произвольные очереди или взвешенные настраиваемые очереди (CQ)

Главным отличием настраиваемых очередей является возможность задать пороговый минимум пропускной способности выходного интерфейса. Доля пропускной способности, отведенной под определенный вид трафика, называется его «весом». Реализуется данный механизм путем циклической последовательной обработки всех очередей.

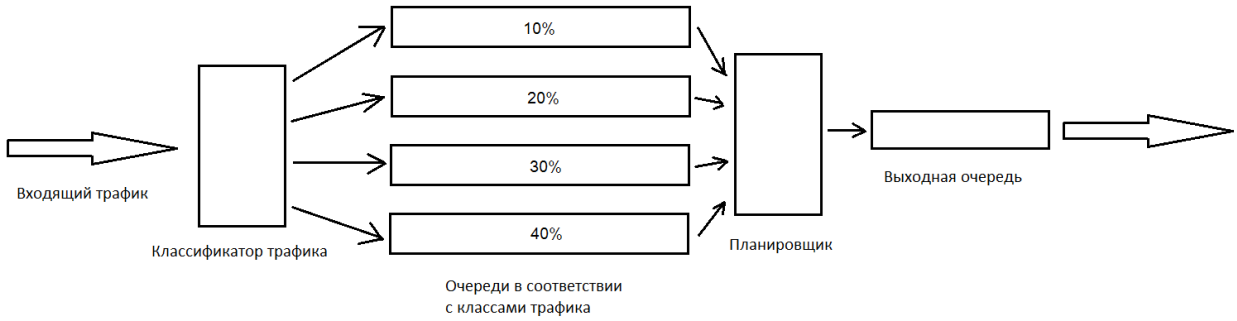

Рисунок 3 - Механизм работы метода настраиваемых очередей

На рисунке 3 показана схема работы механизма настраиваемых очередей. Она аналогична схеме приоритетной обработки очередей, за исключением процентного разделения пропускной способности на отдельные очереди. В данном случае имеется 4 очереди, то есть 4 класса трафика. Каждая очередь имеет свой вес: 10, 20, 30 и 40 процентов от максимальной пропускной способности выходного интерфейса. Если, цикл просмотра очередей (время, в течении которого планировщик работает с каждой очередью) равен 1с, а пропускная способность выходного интерфейса 100 Мбит/с, при цикличной обработке очередей первая очередь пропускает 10 Мбит, вторая 20 Мбит и так далее. Так каждый класс трафика получает гарантированную пропускную способность. Данный алгоритм применяется, например, в случае, когда высший приоритет имеет видео-трафик, который в свою очередь обладает большой интенсивностью. Если в случае перегрузки использовать обычный механизм приоритетных очередей, то трафик, имеющий более низкий приоритет, скорее всего, будет или частично потерян или будет иметь очень низкое качество обслуживания. Использование же механизма настраиваемых очередей позволяет дать определенную гарантированную пропускную способность для этого трафика. В этом случае целесообразно выделить для видео трафика вес больший, чем для других классов.

Взвешенные справедливые очереди (WFQ)

Механизм взвешенных справедливых очередей основан на сочетании механизма приоритетного обслуживания и механизма взвешенных настраиваемых очередей. В различном сетевом оборудовании механизм WFQ реализован по-разному и имеет различные возможности конфигурации. В большинстве случаев имеется одна независимая очередь, которая работает по механизму приоритетного обслуживания. Она всегда обслуживается в первую очередь до того момента, пока все пакеты из нее не будут извлечены. Как правило, данная очередь предназначена для служебных (системных) сообщений и сообщений некоторых приложений прикладного уровня, к которым предъявляются особые требования. Так как весь этот трафик имеет маленькую интенсивность, большая часть пропускной способности остается свободной для других очередей.Все остальные очереди обрабатываются по алгоритму взвешенного обслуживания, где каждой очереди, точно так же, присваивается свой вес.

Так же на некоторых моделях сетевого оборудования могут присутствовать дополнительные конфигурации и возможности реализации механизма WFQ. К примеру, в оборудовании фирмы «CISCOSYSTEMS» механизм взвешенных справедливых очередей делится на два вида:

- Flow-based WFQ (FWFQ) – основан на принципе «потоков».
- Class-based WFQ (CWFQ) – основан на принципе классов.

В случае Flow-based создается такое количество очередей, сколько типов трафика (потоков) реализовал классификатор. Каждому из множества потоков выделяется отдельная выходная очередь. В случае возникновения перегрузок всем этим очередям выделяется одинаковая пропускная способность.

Вариант основанный на классах имеет две разновидности. В первом случае класс трафика определяется по значению полей ToS. Во втором на основании такими параметрами, как номер входного порта или же номеру передающего хоста.

В итоге доступная пропускная способность «справедливо» распределяется, учитывая так же и значение поля ToS.

Справедливые очереди, базирующиеся на классах (CBWFQ)

Алгоритм CBWFQ так же основан на классах. Классы задаются непосредственно пользователем. Параметры, которыми характеризуется точно те же, что и в алгоритме WFQ. В данном случае появляется больше возможностей для перераспределения полосы пропускания между потоками. При установке класса может использоваться ACL или же номер входного интерфейса. Каждый класс так же соотносится с единственной очередью. Определенный процент полосы пропускания гарантируется лишь в случае перегрузки.

Алгоритм RED (Random early detection).

Во всех предыдущих алгоритмах отбрасывание производится по схеме «TailDrop». То есть отбрасываются пакеты, которым не хватает место в буферной памяти. То есть последние поступившие пакеты, что является не совсем рациональным использованием буферной памяти. Алгоритм RED основан на выборочном отбрасывании пакетов. Вероятность потери конкретного пакета в этом случае прямо пропорциональна пропускной способности. Пользователь в данном случае задает три параметра: min – минимальный размер очереди, выше которого алгоритм начинает выборочно отбрасывать пакеты. Max – это значение выше которого алгоритм не должен поднимать значение очереди, что не всегда удается, поэтому, существует третий параметр – burst – это максимальное количество пакетов, которое возможно поставить в очередь, когда превышено значение MAX. Алгоритм RED не предусматривает разделения на классы. Для этого были разработаны его модификации, такие как алгоритм WRED (Weightedrandomearlydetection (Взвешенное Произвольное Раннее Обнаружение)). WRED имеет возможность присваивать различным очередям разные пороговые значения. Таким образом,

для белее низких приоритетов могут быть установлены более низкие пороговые значения. Это позволяет защитить (уменьшить вероятность отбрасывания) пакетов с более высоким приоритетом, что очень важно в некоторых конкретных случаях.

Очереди с малой задержкой (LLQ)

Во многих случаях к трафику предъявляются строгие требования касаемо задержки. НапримерVoIP трафик или видео трафик. Алгоритм LLQ является совокупностью алгоритмов CBWFQ и PQ (приоритетной очередью). В этом случае все очереди ждут опустошения наиболее приоритетной. Единственный случай, в котором в высокоприоритетной очереди появится разница задержек, это момент ожидания передачи пакета из наименее приоритетной очереди, которая началась еще до получения пакета с наивысшим приоритетом.

3. Построение аналитической модели по обеспечению качества обслуживания в защищенной телекоммуникационной сети.

При построении любой мультисервисной защищенной сети (МСС) главной задачей является обеспечение требуемого для этой сети качества обслуживания (QoS). То есть сеть должна удовлетворять заданным параметрам уровня задержек, потерь пакетов и так далее. В процессе расчета показателей качества обслуживания нужно опираться на реальный характер поведения сетевого трафика. Так как сетевой трафик является по большей части разнородным, его следует моделировать не однородным потоком, а многомерной величиной.

В последнее время процесс развития телекоммуникационных сетей, и локальных сетей в частности стремительно набирает обороты. Развиваются как каналы передачи информации, так и средства обработки и коммутации. Однако даже с увеличением пропускной способности узлов и каналов передачи факт перегрузки остается одним из важнейших вопросов в обеспечении качества обслуживания. Так как процесс перегрузки может негативно отразится как на конечном пользователе, так и на самом оборудовании, устранению негативных последствий перегрузок, и их предотвращению уделяется особое внимание[28].

3.1 Построение архитектуры защищенной локальной сети.

Первым этапом работы является разработка архитектуры защищенной локальной сети с различными типамикурсирующего в ней трафика. Первым шагом построения защищенной сети является разработка политики безопасности данной сети. Под политикой безопасности будет пониматься документ, описывающий правила обеспечения безопасности информации и безопасности предприятия в общем, а так же правила поведения сотрудников организации при работе с ценной информацией[30]. Политика безопасности является основой построения как любой защищенной сети, так основным документом, регулирующим все аспекты информационной безопасности на

предприятии.Примерная структура политики безопасности организации приведена в приложении А.

Данная сеть является сетью структурного подразделения компании. Она имеет доступ в глобальную сеть Internet и являться сегментом виртуальной частной сети (VPN), состоящей из данной сети, сети центрального офиса компании, а так же других филиалов компании. Работает по принципу ЛВС-ЛВС. Использование технологий VPN позволяет значительно сэкономить финансы компании на оборудование выделенной линии между несколькими филиалами.

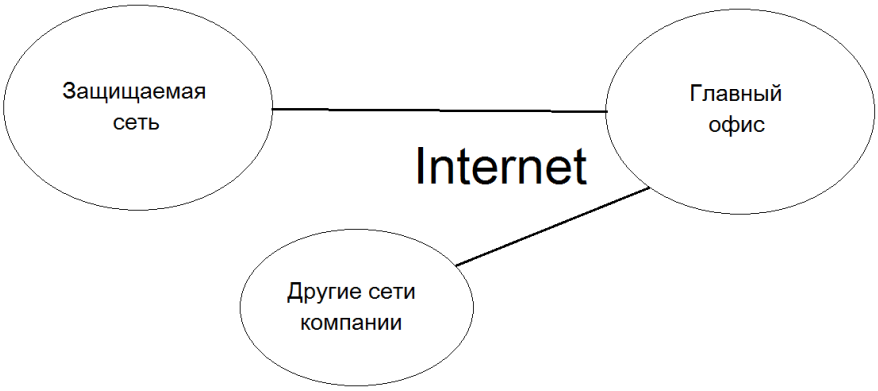

Рисунок 4 - Защищаемая сеть, как часть виртуальной частной сети

При использовании виртуальной частной сети (VPN) защищаемая локальная сеть может быть подвержена следующим угрозам безопасности:

- Возможность несанкционированного доступа к информации и полезным ресурсам данной сети путем неправомерного доступа в данную сеть.
- Возможность перехвата конфиденциальной информации в процессе ее передачи через открытую сеть Internet (технология VPN минимизирует эти риски).

Виртуальная сеть VPN создается при помощи формирования туннелей VPN - защищенных каналов связи, которые в свою очередь основаны на каналах связи общего пользования (открытых каналах связи).

При передаче информации в сети VPN для обеспечения безопасности выполняются следующие действия:

- Шифрование передаваемой информации с помощью криптографических алгоритмов и систем шифрования.
- Осуществление аутентификации, идентификации и авторизации обеих сторон сети VPN (в данном случае нашей корпоративной сети и сети центрального офиса компании)
- Осуществление проверки защищаемой информации на ее целостность и подлинность.

Все эти функции в защищаемой локальной сети выполняет шлюз безопасности VPN, представляющий из себя отдельное аппаратное устройство с внешним адресом относительно самой сети. Устройство имеет в себе встроенный блок, реализующий шифрование передаваемой информации. Так же безопасность передачи информации в момент ее передачи по открытой сети Internet достигается благодаря инкапсуляции и туннелирования входящих и исходящих пакетов. Другие сегменты виртуальной защищенной сети представляют из себяотдельных пользователей, подключенных с сети по схеме Клиент-ЛВС. Для их безопасного соединения с главным офисом используются VPN-серверы и VPN-клиенты. Схема построения защищенной виртуальной сети представлена на рисунке 5.

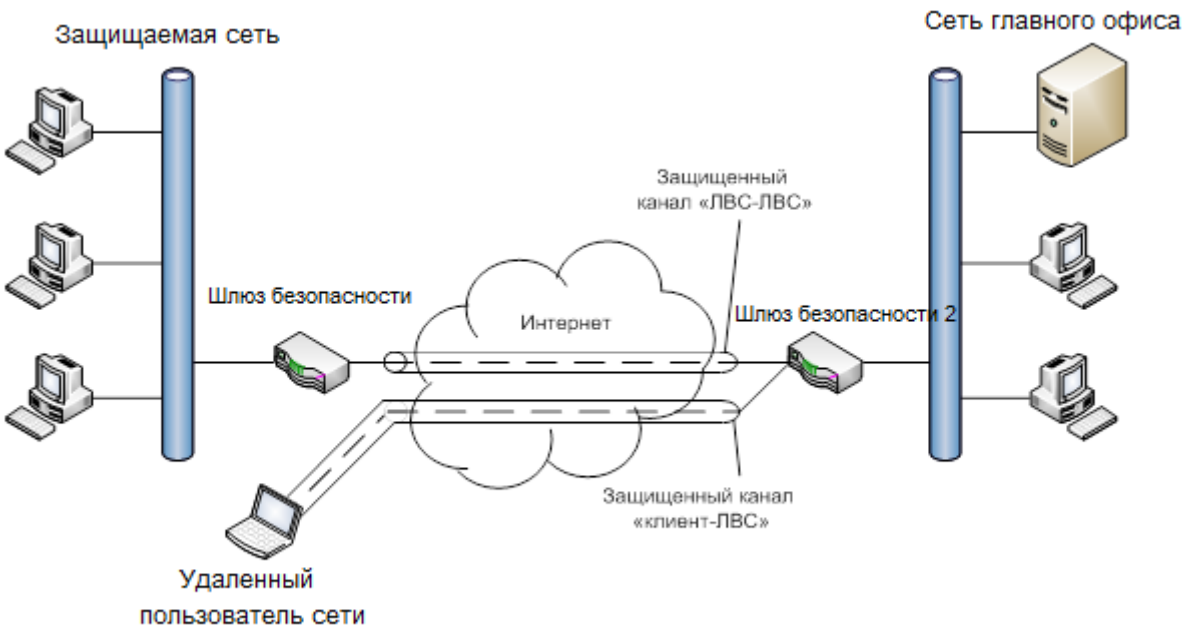

Рисунок 5 – Использование VPN для соединения двух локальных сетей

Виртуальную частную сеть возможно «проложить» как программно, так и с помощью аппаратных устройств. Сравнение основных характеристик нескольких аппаратных и программных реализаторовVPN приведено в приложении В.

В данной организации имеются общедоступные интернет ресурсы, размещенные на веб-серверах. Это значит, что к этим серверам предоставляется свободный доступ любых пользователей. Этот факт создает дополнительную брешь ссистеме безопасности, поскольку в этом случае злоумышленник может намного быстрее получить доступ к конфиденциальной информации, такой как пороли, базы данных, информация о сотрудниках и так далее. Поэтому следующим важным пунктом является использование демилитаризованной зоны (DMZ) в процессе построения архитектуры сети. Она представляет из себя сегмент сети, отделенный отзащищаемой локальной ее части. В ее состав входят сервера, хранящиеобщедоступную информацию. Демилитаризованная зона в данной сети создается посредствам двух межсетевых экранов. Этот подход, в отличии от схемы с одним фаерволом, является более безопасным. Работает данный принцип следующим образом. Первый межсетевой экран

(F1)контролирует соединение демилитаризованной зоны с внешней сетью, второй (F2) – со внутренней. При несанкционированном доступе к ресурсам внутренней сети, в этом случае, злоумышленнику придется обойти не одно, а два защитных устройства. Так же, межсетевые экраны, в данном случае, желательно, должны быть двух различных производителей. Например,F1 фирмы CISCO, а F2 фирмы ALTELL. Это обосновано тем, что в двух устройствах различных фирм меньше вероятность того, что в обоих этих устройствах будет одна и та же уязвимость. Недостатком такой архитектуры является большая стоимость, по сравнению со схемой, основанной на одном межсетевом экране. Схема построения DMZ показана на рисунке 6.

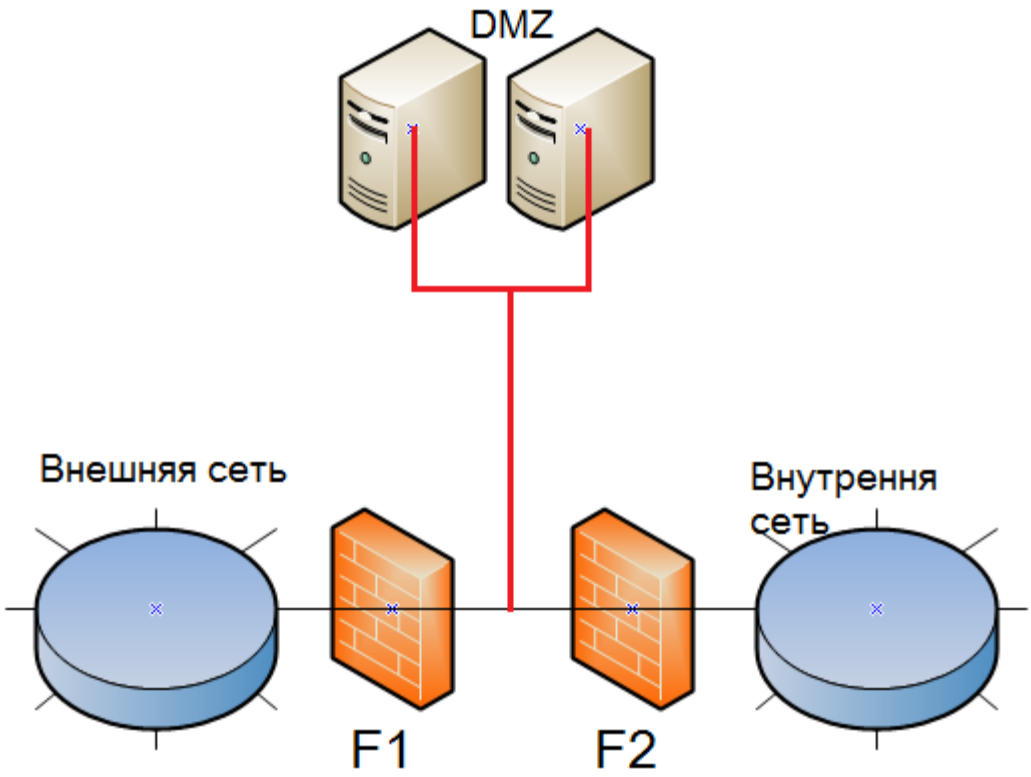

Рисунок 6 - Демилитаризованная зона

Следующим пунктом является использование механизмов трансляции сетевых адресов (NAT). Это повысит безопасность сети. NAT обезопасит сеть

от внешних атак. Функцию трансляции сетевых адресов будет выполнять один из фаерволовF1, в котором имеется блок, отвечающий за NAT.

Так же важным пунктом защиты локальной сети, является наличие в ней систем обнаружения и предотвращения атак (IDS и IPS). Обычно эти системы объединены. Системы обнаружения и предотвращения атак представляют из себя аппаратные устройства, способные выявлять сам факт несанкционированного или неавторизированного доступа в корпоративную сеть. Далее системы предотвращения атак выполняют следующие функции[6]:

- Информирование системного администратора о факте НСД.
- Обрыв соединения.
- Перенастройка межсетевого экрана с целью блокировки всех последующих действий злоумышленника.

Системы обнаружения и предотвращения сетевых атак могут размещаться как перед сетевыми экранами (снаружи), так и после них. Первый вариант применяется в случае, если интерес представляет весь подозрительный трафики все атаки, осуществляющиеся на данную сеть. Второй применяется в случае, когда интерес представляют только лишь атаки, которые преодолели межсетевые экраны. Перечень активных и пассивных действий систем обнаружения и предотвращения атак представлена в приложении Б. В данном случае, система обнаружения и предотвращения атаки размещается после обоих сетевых экранов. Схема подключения сетевойIDS показана на рисунке 6.

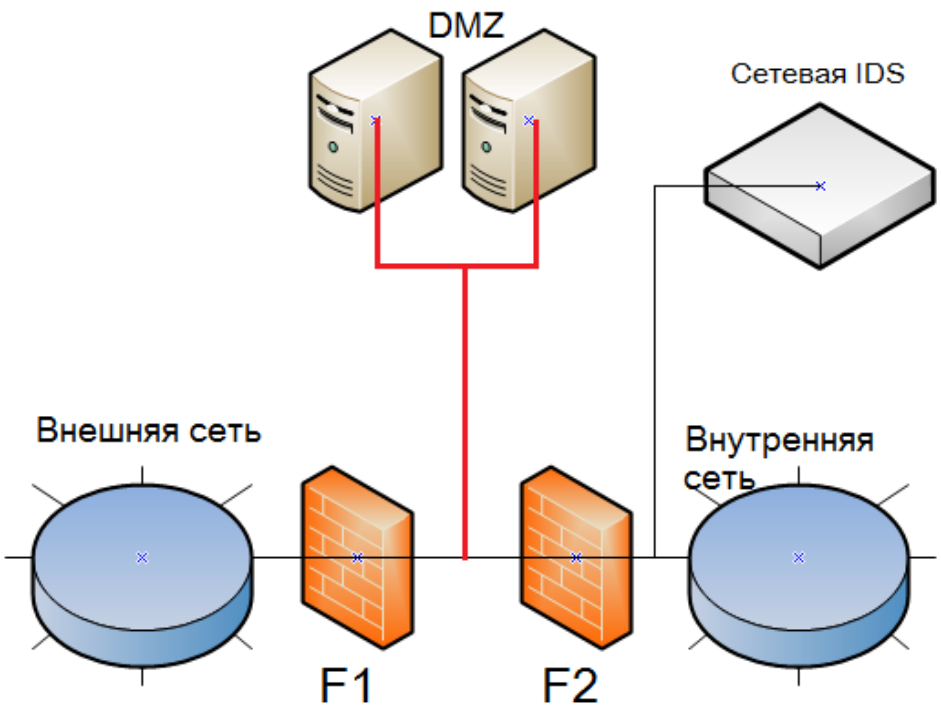

Рисунок 7 – Схема размещения в сети системы обнаружения и предотвращения атак

Так же непосредственную опасность представляет факт физического несанкционированного доступа к ресурсам корпоративной локальной сети. Поэтому очень важно обеспечить контроль доступа, как на территорию самой организации, так и к источникам конфиденциальной информации. Для обеспечения контроля лиц, контактирующих с КИ, используются системы контроля и управления доступом (СКУД). Каждый сотрудник при входе на территорию организации должен пройти идентификацию, путем сканирования уникального магнитного пропуска. Так же при начале работы с ПК, каждыйсотрудник должен авторизоваться с помощью уникального программно-аппаратного USB ключа, после чего он может преступать к дальнейшей работе. Кроме того физическая безопасность обеспечивается с помощью установленных на территории систем видео наблюдения.

Общая схема защищенной сети показана на рисунке 8. В ее состав входят следующие компоненты:

- Шлюз безопасности VPN (щ.б. VPN).
- Межсетевые экраны (F1 и F2).
- Демилитаризованная зона (DMZ), в которой находятся сервера (S1 и S2). S1 – веб-сервер, S2 – почтовый сервер.
- Коммутаторы (M1, M2, M3, M4, M5).
- Рабочие станции (C1, C2, C3, C4, C5).
- Iртелефоны (VoIP 1, VoIP2).

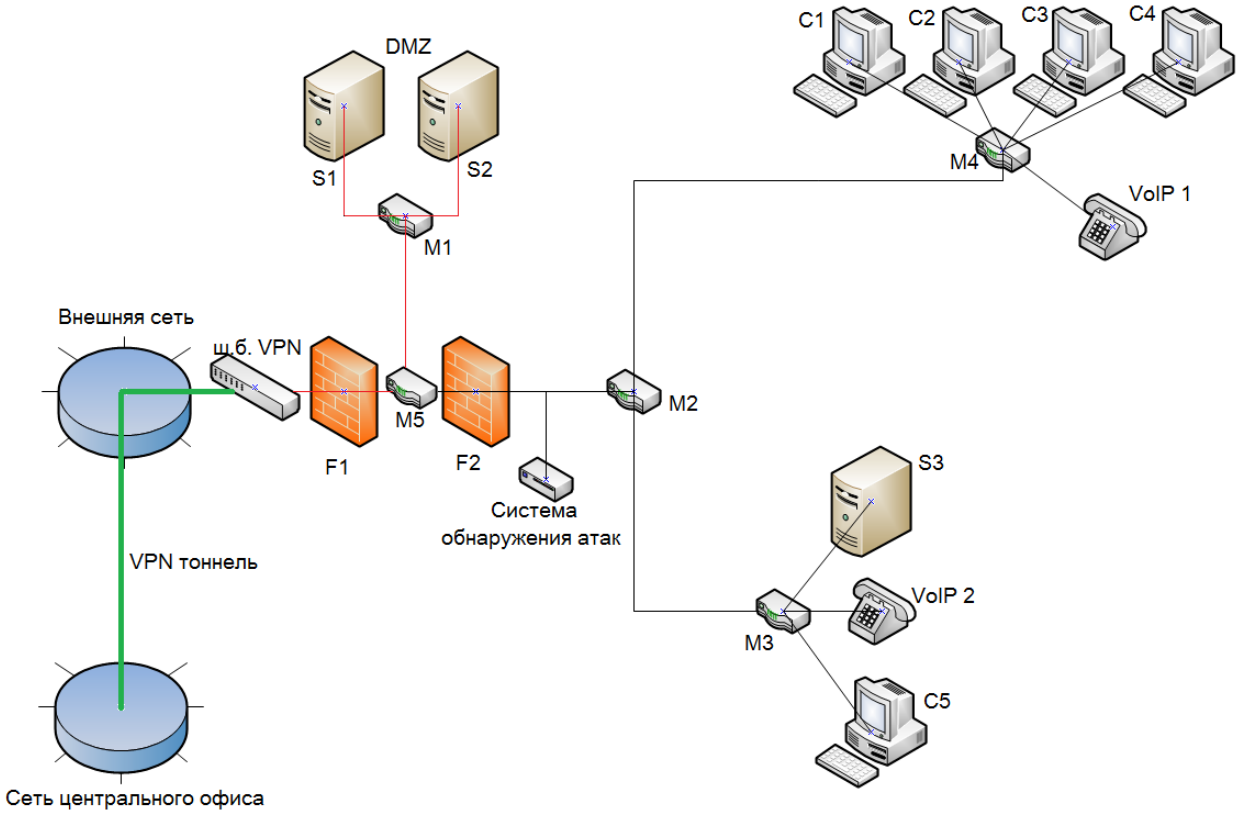

Рисунок 8 – Защищенная сеть

В данной сети трафик является разнородным. Каждый класс трафика обладает своими характеристиками. Изначально трафик делится на два класса, в соответствии с политикой приоритетности абонентов. В данном случае наивысший приоритет имеет сеть 2, в которой находится сервер, хранящий конфиденциальную информацию компании.

Приоритезацию этих двух сетей обеспечивает маршрутизатор M2. Для данных сетей он реализует дисциплину обслуживания в соответствии с механизмом обработки очередей PriorityQueuing (PQ). То есть, в случае возникновения перегрузки и появления очереди в маршрутизаторе M2, абсолютный приоритет будут иметь пакеты адресованные подсети 2. Это

обусловлено тем, что звонки с IP телефона этой сети гораздо важнее для политики компании, чем с телефона первой сети.

В свою очередь на маршрутизаторах M3 и M4 реализована политика CQ (взвешенные настраиваемые очереди). Данная политика включает в себя три очереди. Вес наиболее приоритетной составляет 50%, второй 30%, и наименее приоритетной 20% от пропускной способности выходного интерфейса маршрутизатора. В наиболее приоритетную очередь помещаются пакеты VOiP трафика и трафика видеоконференций, например протоколыRTSP, RTP и RTCP. Это обусловлено тем, что трафик видеоконференций и IP телефонии чувствителен к задержкам[29]. Так же его интенсивность тяжело рассчитать заранее. Схема работы данного механизма обработки очередей показана на рисунке 9. В приложении Г показаны сетевые ресурсы, необходимые для корректной работы средства видео и аудио связи на примере Skype[7].В общем виде, в данном случае трафик можно разделить на два класса: трафик чувствительный к задержкам (непрерывный) и «эластичный» (не чувствительный к задержкам).

Оставшиеся очереди настраиваются в зависимости от загруженности сети на данный момент.

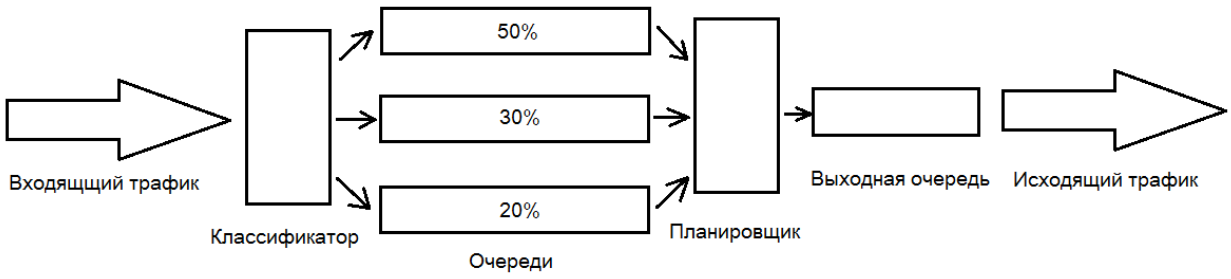

Рисунок 9 – Механизм взвешенных настраиваемых очередей в маршрутизаторах M3 и M4

При выборе оборудования для обеспечения безопасности конфиденциальной информации, в данном случае, нужно исходить из требуемых для данной сети ресурсов. Поскольку данная сеть является

корпоративной и не имеет большого числа пользователей, оборудование нужно выбирать соответственно.В качестве межсетевого экрана F2 может быть использован фаерволлCiscoASA5505 с максимальной пропускной способностью 150 Мбит/с. В качестве межсетевого экрана F1нужно выбирать более производительное оборудование, им может являться межсетевой экран D-linkDFL-1660,с максимальной пропускной способностью 1,2 Гбит/с. Он имеет уже встроенный реализаторVPN (350 Мбит/с) и предустановленный антивирус (225 Мбит/с).Так же данное оборудование имеет соответствующие сертификаты ФСТЭК. В качестве системы обнаружения и предотвращения атак может быть рекомендован программно-аппаратный комплекс «ПАК ViPNet IDS 1000»с максимальной производительностью 950 Мбит/с. Маршрутизатором М2 может выступать CISCOSF-300-24PP-K9-EU. Функции создания VPN тоннеля, так же, берет на себя межсетевой экран D-linkDFL-1660 с широкой конфигурацией настроек виртуальной частной сети.

3.2. Анализ влияния дисциплины обслуживания на производительность узла сети.

При исследовании методов обеспечения качества обслуживания главное внимание было уделено влиянию очередей на показатели передачи трафика. Принцип очередей в настоящее время применяется во всех сетях коммутации. Очереди подразумевают наличие в коммутационном устройстве буфера на входных и выходных его интерфейсах. На рисунке 10 представлены основные параметры, характеризующие принципы работы очередей.

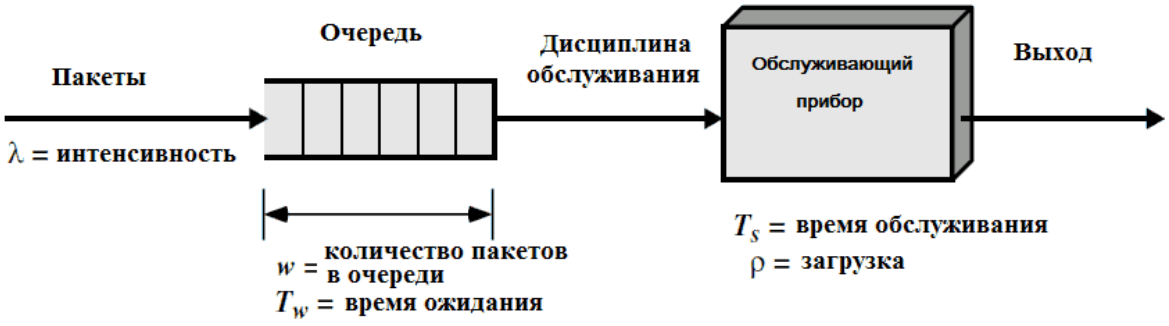

Рисунок 10 – параметры работы очередей

λ – средняя интенсивность поступления пакетов.

W – среднее число пакетов, ожидающих обслуживание.

T_w – среднее время ожидания обслуживания.

T_s - среднее время обслуживания пакетов обслуживающим прибором (интервал между моментом поступления пакета и завершением его обслуживания).

ρ – время, затрачиваемое прибором на обслуживание пакета.

T_r - Среднее время, которое пакет тратит в системе, т.е. время ожидания в очереди плюс время обслуживания сервером.

В данном случае предполагается, что длина очереди является бесконечной, это значит, что факт потери пакетов можно не рассматривать.

Основные элементы моделирования:

- Входящий простейший поток пакетов с интенсивностью λ (количество пакетов, поступающих на вход системы в единицу времени).
- Буферный накопитель, в котором образовывается очередь из пакетов.
- Обслуживающее устройство с загруженностью ρ.

Пакеты поступают на вход в произвольные моменты времени (случайное распределение). В случае, если буфер свободен, пакет передается на обслуживающее устройство. Если же буфер заполнен, то пакет попадает в очередь.

Моделирование влияния дисциплины обслуживания на производительность узла сети будет осуществляться в среде моделирования MatLab со встроенными блоками SimEvents. В данном случае будет рассмотрено две дисциплины обслуживания заявок: LIFO и FIFO. Параметром, характеризующим качество обслуживания, выступает пропускная способность узла коммутации. Модель системы массового обслуживания представлена на рисунке 11.

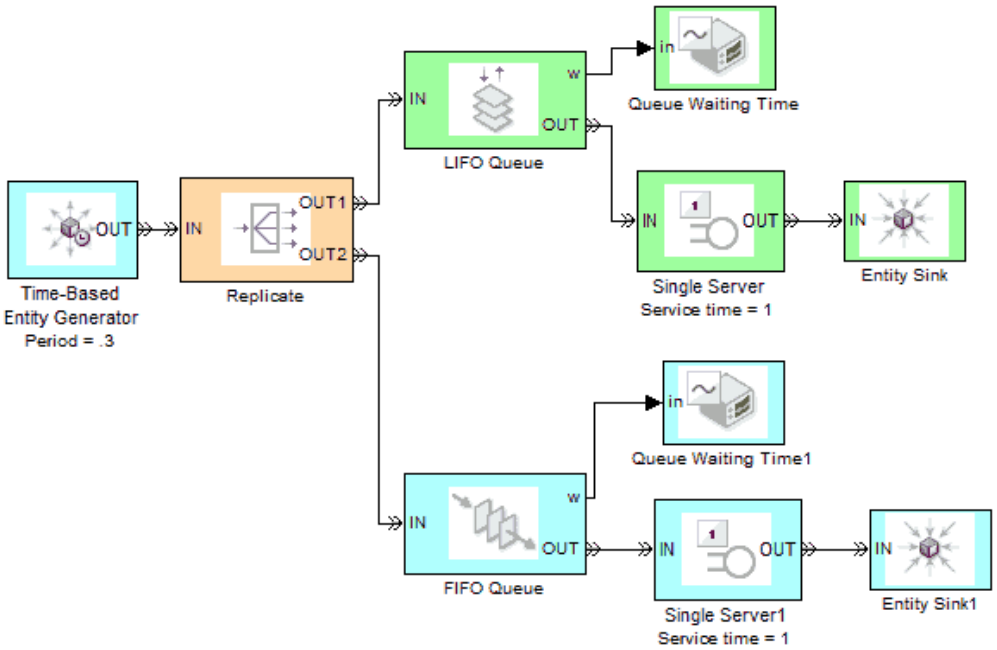

Рисунок 11 – Модель системы массового обслуживания

Блок Time-BasedEntityGeneratorвыполняетгенерациюпакетов. Период генерации пакетов был выбран 0,3 с. Все время моделирования было задано

равным 10 с. А время обслуживания пакетов в блоках реализующих ДО FIFOи LIFOбыло задано равным 1 с. Блок Replicate отвечает за разделение пакетов между двумя буферами, реализующими ДО. При этом емкость буферов по умолчанию была задана неограниченной. На рисунках 12 и 13 показаны результаты моделирования СМО с дисциплинами обслуживания LIFOи FIFO.

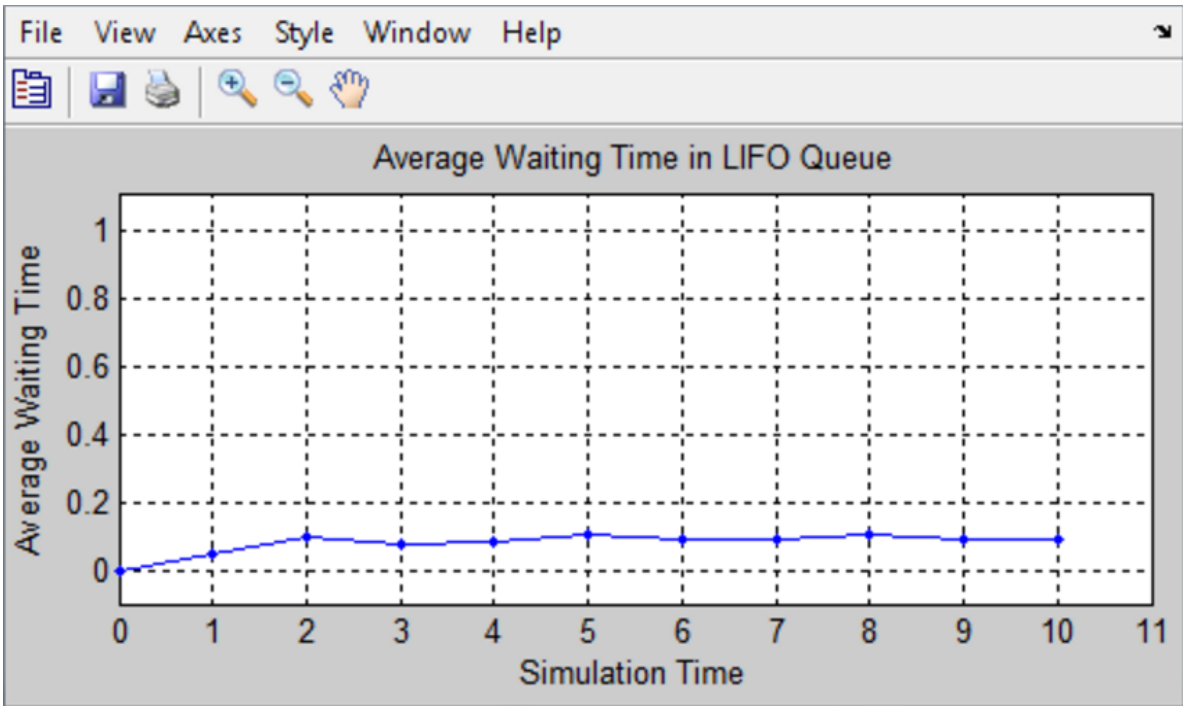

Рисунок 12 – Среднее время задержки пакетов в буфере LIFO

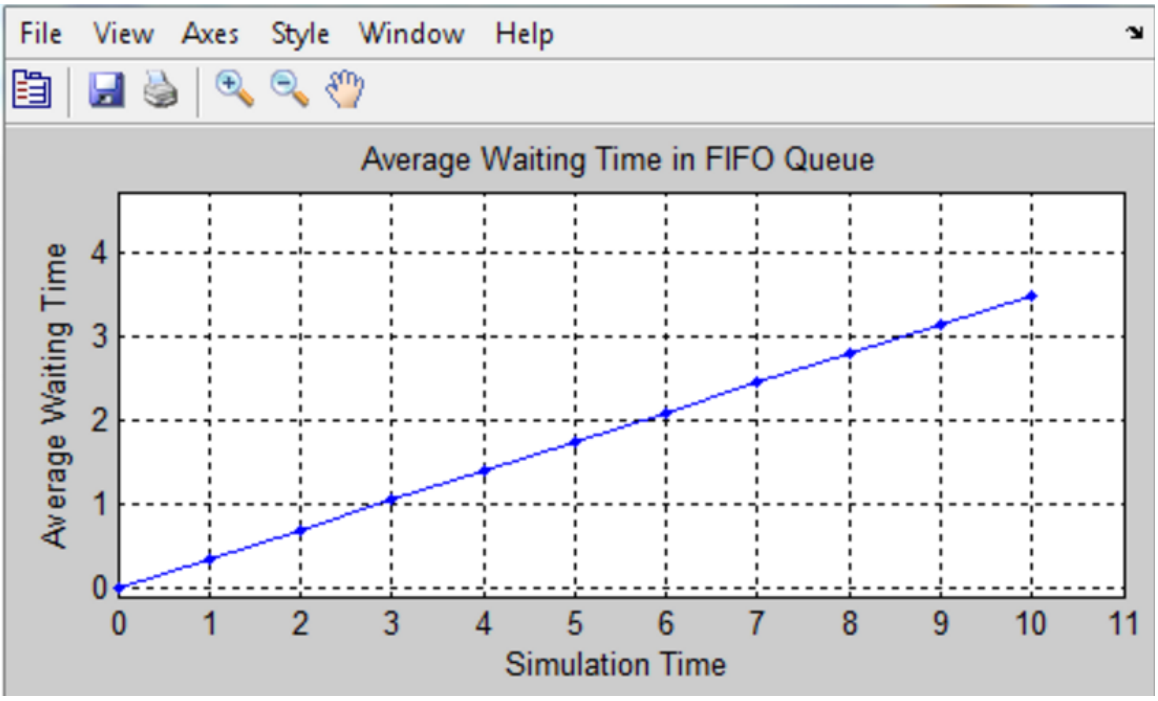

Рисунок 13 – Среднее время задержки пакетов в буфере FIFO

Исходя из результатов моделирования, можно сделать выводы о том, что при применении дисциплины обслуживания LIFO в СМО можно добиться повышения производительности устройства.

3.3. Разработка аналитической модели по обеспечению качества обслуживания в узле коммутации сети

Современные сети связи (сети связи следующего поколения) характеризуются различными видами трафика. Каждый из видов трафика имеет свои конкретные требования к ресурсам сети для обеспечения необходимого для него качества обслуживания. Таким образом в ССП или мультисервисных сетях необходимо наличие неких механизмов для обеспечения заданного качества обслуживания. Данные механизмы должны учитывать характер разнородного трафика. Для обеспечения заданного качества обслуживания, эти механизмы должны решать две основные задачи. Первая – классифицировать

входящий трафик, вторая – распределить ресурсы сети в соответствии с требованиями каждого типа трафика.

Механизм DiffServ является одним из наиболее распространенных механизмов обеспечения качества обслуживания в узле коммутации. Механизм его работы заключается в условном разделении трафика на три вида: чувствительный к задержкам (EF), чувствительный к потерям (AF) и трафик с не гарантированными показателями потерь и задержек, ему выделяется максимально возможное, на данный момент, качество обслуживания (BE).

Для начала нужно рассмотреть звено сети, в котором будут реализованы эти механизмы. Далее нужно определить характеристики звена сети, что будет реализовано с помощью построения аналитической модели этой системы.

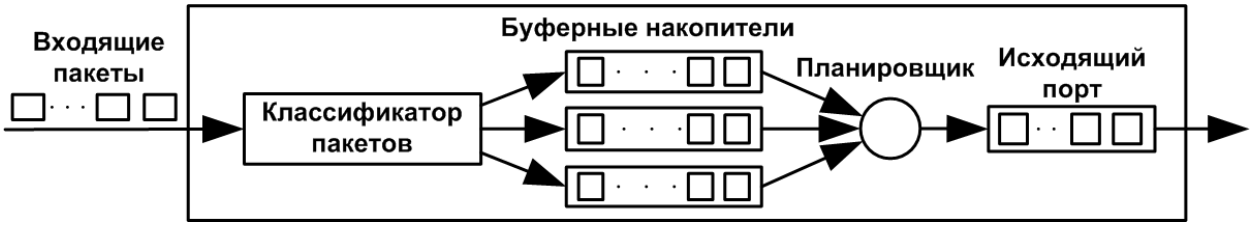

Рисунок 14 - Функциональная структура звена сети

Принцип функционирования звена сети следующий. После поступления пакетов на входной порт устройства они попадают в классификатор. В нем анализируются заголовки пакетов, и они размещаются по очередям (буферам) в зависимости от вида трафика. Затем используется алгоритм резервирования ресурсов в планировщике, что позволяет распределить пропускную способность устройства в соответствии с приоритетами трафика. Структура звена сети, обеспечивающего качество обслуживания, показана на рисунке 10. В данном случае будет уместно применить математические аппараты теории массового обслуживания для расчета ВВХ данной системы.

Расчет ВВХ функционирования узла коммутации.

Данное звено сети можно формально представить как сеть массового обслуживания. В данном случае планировщик будет работать по алгоритму Class-BasedWeightedFairQueuing (справедливое распределение ресурсов на

основе классов). Дисциплина обслуживания в данном случае заключается в обобщенном распределении процессорного времени (GeneralProcessorSharing – GPS). Таким образом, моделируемая система показана на рисунке 11.

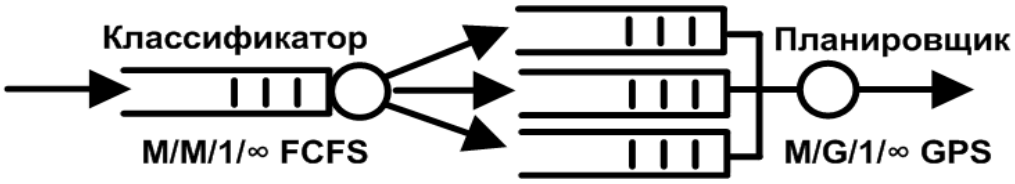

Рисунок 15 - Модель звена сети на основе СМО

В стандартных моделях систем массового обслуживания предполагается, что все запросы, которые поступают в систему, являются однородными (имеют одни и те же законы распределения времени обслуживания). Однако для аналитического описания работы механизмов QoS,нужна модель, в которой распределение времени обслуживания является неоднородным, так же как и важность данного запроса. В обоих случаях для описания потока можно использовать такие параметры, как интенсивность поступления заявок (λ) и μ (интенсивность обслуживания заявок).

1. Модель коммутатора типа $\vec{M}_r$/M/1/∞с относительными фиксированнымиприоритетами.

Началом будет анализ стандартных моделей из теории очередей и теории массового обслуживания, базирующихся на понятии простейшего потока и относительных фиксированных приоритетах. Данные модели являются стандартизированными и могут служить основой для более сложных моделей узлов коммутации (УК) [8].

1. В ней среднее время ожидания обслуживания пакета приоритета rравно [8, 9]:

$$Wr = \frac{\rho_R}{\mu*(1-\rho_R-1)*(1-\rho_R)} \quad (1)$$

Где $\rho_{R=}\Lambda_R/\mu$–общая нагрузка обслуживающего прибора. Приоритетне должен превышать r.

Λ_r – общая интенсивность поступления в обслуживающий прибор пакетов.Приоритет не должен превышать значение r.

Λ_R - общая интенсивность поступающих пакетов в прибор.

μ - интенсивность обслуживания коммутатором поступающих пакетов.

2. Средняя длина очереди, состоящей из пакетов приоритетаr в коммутаторе типа $\vec{M}_r$/M/1/∞, определяется следующими формулами [8,10]:

$$l_r = \begin{cases} L_r, \ r = 1 \\ L_r - L_{r-1}, r = \overline{2,R} \end{cases}, L_r = \sum_{m=1}^{\infty} m * P_{m+1}(r) \ (2)$$

Где$P_m(r)$ - распределение вероятностей состояний для коммутатора типа $\vec{M}_r$/M/1/∞[8].

В случае, когда$r = \overline{2,R}$, использование распределения вероятностей состояний определяет среднюю длину очереди r-го приоритета как разность между средней длинной очереди с общей нагрузкой ρ_r и средней длинной очереди с общей нагрузкой ρ_{r-1}. Для проверки вычислений может быть использована формула Литтла.

3. У буфера K есть максимальный объем. Вероятность того, что это объем будет превышен, приравнивается вероятности потери пакетов(согласно свойству эквивалентности систем с конечным и бесконечным буфером при малых нормах потерь). Рассчитывается исходя из распределения вероятности состояний как вероятность P_{k+1}[11]:

$$P_{k+1}(r) = \ \rho_R * (1 - \rho_r) * \rho_r^K, \rho_R < 1 (3)$$

2. Моделькоммутатора типа $\vec{G}_r$/G/1/∞ с относительными фиксированными приоритетами.

Для создания более сложных зависимостей для моделей коммутации $\vec{G}_r$/G/1/∞ используется метод, предложенный в диссертационной работе [8]. Данный метод основан на следующих факторах:

- Формулы для стандартизированных моделей УК типа $\vec{M}_r$/M/1/∞.
- Метод диффузионной аппроксимации.
- Метод инвариантов для систем обслуживания с приоритетами.

1. Средняя длина очереди из пакетов приоритетаr в УК типа $\vec{G}_r$/G/1/∞ вычисляется с помощью следующего выражения [11]:

$$l_r = \begin{cases} L_r,\ r = 1 \\ L_r - L_{r-1}, r = \overline{2,R} \end{cases},\ L_r = \Lambda_r * w_r^* * \frac{C_{a,r}^2 + C_{b,r}^2}{2} \qquad (4)$$

где w_r^* - среднее время ожидания начала обслуживания при входящей нагрузкеρ_r (без приоритетов) [8].

0=<ρ_r<1 – одно из условий метода диффузионной аппроксимации для обеспечения получения стационарных характеристик работы коммутатора.

$C_{a,r}^2$ - квадратичный коэффициент вариации времени поступления пакетов объединенного потока приоритета не выше r $(\overline{l,r})$. Определяется по закону сложения случайных величин.

$C_{b,r}^2$ - квадратичный коэффициент вариации времени обслуживания пакетов.

2. На основании (4) и формулы Литтла можно определить среднее время ожидания обслуживания пакетов приоритетаrв узле коммутации типа$\vec{G}_r$/G/1/∞:

$$W_r = \frac{l_r}{\lambda_r} \qquad (5)$$

При подстановке квадратичного коэффициента вариации распределения времени поступления пакетов ($C_{a,r}^2$=$C_{b,r}^2$=1 для экспоненциального распределения времени поступления и обслуживания) формулы (4) и (5) приравниваются к формулам (2) и (1). То естьформулы (4) и (5) согласуются со стандартизированнымиуравнениями, используемыми при работе со стандартными моделями теории очередей в массовом обслуживании (2) и (1).

3. Вероятность того, что максимальный заданный объем буфера будет превышен (вероятность потери пакетов приоритетаr) для коммутатора типа $\vec{G}_r$/G/1/∞ рассчитывается следующим выражением [9]:

$$P_{1+k} = \rho_R * (1 - \hat{\rho}_r) * \hat{\rho}_r^k \ , \qquad (6)$$

где $\hat{\rho}_r = \exp\left(-\frac{2*(1-\rho_r)}{C_{a,r}^2 * \rho_r + C_{b,r}^2}\right), \rho_R < 1 \qquad (7)$

3. Схожесть систем массового обслуживания с фиксированными приоритетами и СМО с динамическими приоритетами.

Общая формула среднего времени ожидания обслуживания пакетов приоритетаr для дисциплины обслуживания порядкаsузла типа $\vec{M}_r$/M/1/∞ [9]:

$$W_r^{(s)} = \frac{\frac{\Lambda_r}{(1-\rho_R)*\mu^2} - \sum_{i=r+1}^{R} \rho_i W_i \left(1 - \left(\frac{b_i}{b_r}\right)^{\frac{i}{s}}\right)}{1 - \sum_{i=1}^{r-1} \rho_i \left(1 - \left(\frac{b_r}{b_i}\right)^{\frac{i}{s}}\right)} \qquad (8)$$

где b_r - коэффициент, скорости нарастания приоритета для пакетов этих классов (b_1, $>b_2>$... $>b_r>0$).

Уравнение (8) является основным при анализе дисциплины обслуживания порядка s с наличием приоритетов. При s= 0 дисциплина обслуживания работает в порядке приоритетов, которые не меняются в течении времени – фиксированные приоритеты (ФП). При s=1 приоритеты в системе изменяются со временем линейно - динамическими приоритетами (ДП). При s=∞дисциплина обслуживания работает в порядке поступления (механизм обработки FIFO). Т.о., дисциплина обслуживания с динамическими приоритетами более обобщенная. В нее включается классс фиксированными относительными приоритетами.Так же соблюдены условия подобия в системах обслуживания с фиксированными и динамическими приоритетами (3-я теорема подобия)[10]:

1. Критерии подобия для сравниваемых явлений равны (попарно).

2. В системах происходят качественно одинаковые процессы (выполнение условий однозначности).

Коэффициенты подобия для узлов коммутации определяются следующим образом [10]:

$$C_r^w = \frac{W_r^{ДП}}{W_r^{ФП}}; \qquad (9)$$

$$C_r^L = \frac{L_r^{ДП}}{L_r^{ФП}}; \qquad C_r^{P_{k+1}} = \frac{P_{k+1}^{ДП}(r)}{P_{k+1}^{ФП}(r)} (10)$$

Исходя из того, что показатели работы узла коммутации L_r и $P_{k+1}(r)$ имеют линейную зависимость (2), следует:

$$C_r^L = C_r^{P_{k+1}} (11)$$

При работе с системой обслуживания с ДП, выражение, описывающее все показатели качества обслуживания, вывести невозможно. Но на основании теории подобия, возможно вывести выражения, описывающие качество функционирования (КФ) узла коммутации.

4. Модель УК типа $\vec{M}_r$/M/1/∞ с относительными динамическими приоритетами.

а) Среднее время ожидания обслуживания пакетов

приоритетаr в узле коммутации$\vec{M}_r$/M/1/∞ с ДП можно вычислить как:

$$W_r^{ДП} = \frac{\frac{\Lambda_r}{(1-\rho_R)*\mu^2} - \sum_{i=r+1}^{R} \rho_i W_i \left(1-\frac{b_r}{b_i}\right)}{1-\sum_{i=1}^{r-1} \rho_i \left(1-\frac{b_i}{b_r}\right)} \qquad (12)$$

2. Среднюю длину очереди пакетов приоритетаrможно рассчитать согласно формуле Литтла:

$$l_r^{ДП} = w_r^{ДП} * \lambda_r \qquad (13)$$

в) Вероятность того, что максимальный заданный объем буфера K будет превышен, можно принять за вероятность потери пакета:

$$P_{k+1}^{\text{ДП}}(r) = C_r^{P_{k+1}} * P_{k+1}^{\text{ФП}}(r) \qquad (14)$$

Где $C_r^{P_{k+1}} = \frac{P_{k+1}^{\text{ДП}}(r)}{P_{k+1}^{\text{ФП}}(r)}$ - коэффициент подобия системы обслуживания (при том, что ρ_r неизменна).

$P_{k+1}^{\text{ФП}}(r)$— вероятность того, что объем буфера K будет превышен. Для узла коммутации типа $\vec{M}_{\text{г}}$/M/1/∞с фиксированными приоритетами.

5. Модель узла типа $\vec{G}_{\text{г}}$/G/1/∞ с ДО на основе динамических приоритетов.

Исходя из метода диффузионной аппроксимации и закона сохранения накопленной в очереди работы можно вычислить среднюю длину очереди сρ_r (суммарная входящая нагрузка) для узла коммутации типа $\vec{G}_{\text{г}}$/G/1/∞ (дисциплина обслуживания – с динамическими приоритетами) [8]:

$$L_r^{ДП} = L_{r кл}^{ДП} * \frac{C_{a,r}^2 + C_{b,r}^2}{2} (15)$$

Где $L_{r\text{кл}}^{\text{ДП}}$ - средняя длинна очереди, в которой суммарная нагрузка = ρ_r.Узел коммутации типа $\vec{M}_{\text{г}}$/M/1/∞, считается, что входящий поток является простейшим, а дисциплина обслуживания – с динамическими приоритетами.

1. Средняя длинна очереди из пакетов приоритета r для узла коммутации типа $\vec{G}_{\text{г}}$/G/1/∞ вычисляется следующим образом:

$$L_r^{\text{ДП}} = \begin{cases} L_r^{\text{ДП}}, r = 1 \\ L_r^{\text{ДП}} - L_{r-1}^{\text{ДП}}, r = \overline{2, R}. \end{cases} (16)$$

2. Среднее время ожидания обслуживания пакета с приоритетом r, руководствуясь формулой Литтла, можно вычислить как:

$$W_r^{ДП} = \frac{l_r^{ПД}}{\lambda_r} (17)$$

3. Вероятность того, что максимальный заданный объем буфера K будет превышен, можно рассчитать по формуле (14) (исходя их теории подобия).

Таким образом, можно сделать следующие выводы. Основным способом обеспечения качества обслуживания в узле коммутации, в котором имеется приоритет одного трафика над другим, является факт управления самой дисциплиной обслуживания, исходя из суммарной входящей нагрузки пакетов с разными приоритетами. Это может быть обеспечено путем внедрения в узел коммутации таких функций, как мониторинг показателей качества обслуживания (уровень потери пакетов, задержка пакетов различных классов приоритета) и изменение ДОв реальном времени, исходя из уровня входящей нагрузки в узле коммутации.

В данном случае трафик делится на два типа: чувствительный к задержкам (непрерывный) и нечувствительный (эластичный). То есть можно выделить два класса приоритетов (r1 и r2). Для каждого из двух типов трафика существует предел допустимой задержки по времени (t1, t2).

1. В случае небольших нагрузок, когда суммарная нагрузка (ρ_R) не превышает первого порогового предела($\rho_{\text{пор1}}$), дисциплина обслуживания с фиксированными приоритетами обеспечивает все требуемые показатели качества обслуживания в УК для каждого из R приоритетных классов. В данном случае S=0, b1 и b2 – не используются.

2. В случае, когда суммарная входящая нагрузка (ρ_R) превышает пороговое значение ($\rho_{\text{пор1}}$), задержка (t2) так же превышает требуемое максимальное значение. В этом случае необходимо изменение дисциплины обслуживания на ДО с динамическими приоритетами. Это позволит избежать потери трафика приоритета r2 при обеспечении качества обслуживания трафика приоритета r1. В данном случае S=1 и b1,b2 – активны. Пакетам, поступающим в узел коммутации,присваиваются коэффициенты изменения приоритетных функций (b1, b2).

3. При последующем росте нагрузки (ρ_R) в узле коммутации осуществляется своевременное управление ДО с динамическими приоритетами. В результате среднее значение задержки не чувствительного

(эластичного) трафика не превышает порогового значения, то есть соответствует требуемому значению. В результате этого t1 возрастает. В свою очередь при дальнейшем росте суммарной нагрузки и ее превышении второго порогового значения ($\rho_{\text{пор2}}$), вновь производится перерасчет параметров. Это позволяет держать в пределах нормы среднее время пребывания пакетов приоритета r1. При этом задержка для пакетов приоритета r2 возрастает. После превышения второго порогового значения, при росте нагрузке в УК возможен факт отбрасывания пакетов приоритета r2 (эластичного трафика), что, в свою очередь, способствует обеспечению заданных показателей качества обслуживания для чувствительного к задержкам трафика. Принцип управления дисциплиной обслуживания в зависимости от суммарной входной нагрузки показан на рисунке 10.

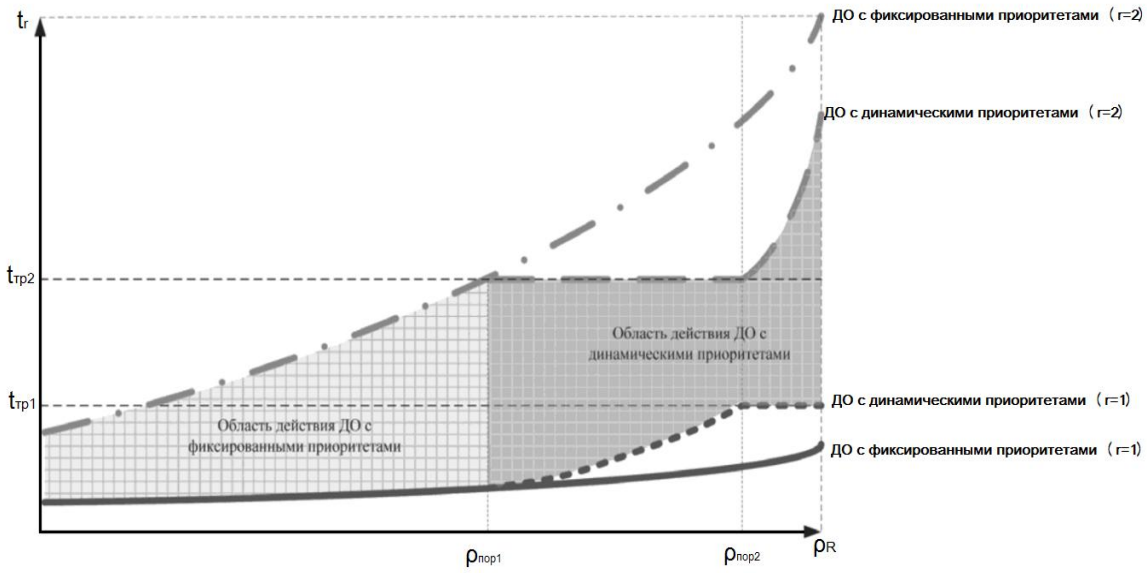

Рисунок 16 - Управление дисциплиной обслуживания, основанное на зависимости среднего времени задержки в узле коммутации от суммарной входной нагрузки

4. Обеспечение безопасности жизнедеятельности при работе персонала

Так как данная выпускная квалификационная работа нацелена на разработку модели по обеспечению качества обслуживания в ЗТКС, то в качестве объекта исследования будет рассмотрена сложная телекоммуникационная система, которая предполагает наличие большого числа пользователей. В свою очередь в состав данной системы будет входить множество структур передачи информации, которые предполагают использование специально предназначенного оборудования, такого как: Сервера, ПК, разнохарактерные каналы связи, коммутационное оборудование и так далее.

Исходя из вышеизложенного, на персонал, который будет участвовать при реализации модели, а также взаимодействовать в дальнейшем с фактически реализованной моделью, могут воздействовать следующие факторы, способные нанести вред жизни и здоровью человека, а именно [26]:

1. Физические факторы:

- Возникает угроза пожара, поскольку в рабочей зоне находятся электроприборы, использование которых повышает температуру поверхности оборудования и может вызвать перегрев;

- Возникает угроза поражения электрическим током, так как может возникнуть повышенное значение напряжения электрической цепи, замыкание которой может пройти через тело работника;
- Возникает угроза повреждения конечностей в связи с наличием подвижных частей производственного оборудования;
- Угроза нарушения рабочего микроклимата (повышенная/ пониженная влажность и подвижность воздуха, искусственное освещение и недостаток естественного света, повышенный уровень шума, запылённость воздуха, повышенный уровень электромагнитных излучений).

2. Химические факторы (вредное воздействие токсичных и раздражающих веществ при контакте с кожным покровом человека и слизистыми оболочками);

3. Психофизиологические факторы[16]:

- Физические перегрузки;
- Нервно-психические перегрузки (умственное перенапряжение, монотонность труда, эмоциональные перегрузки).

Таким образом, в данной главе необходимо рассмотреть следующее:

- Требования к организации и оборудованию рабочего места;
- Обеспечение электробезопасности и пожарной безопасности;
- Правила работы с ПК;
- Эргономика взаимодействия человек-система.

4.1. Обеспечение организации и оборудования безопасного рабочего места

Под рабочим местом понимается структурная часть производственного пространства, в которой субъект труда взаимосвязан с размещёнными средствами и предметом труда для осуществления единичных процессов труда в соответствии с целевой функцией получения результатов труда. [17]

В РФ требования к организации рабочего места определяются в документах:

- Трудовой кодекс РФ;
- Нормативно-правовые акты субъектов РФ;
- Государственными и международными стандартами;
- Трудовым договором.

Общие эргономические требования определены в стандартах ГОСТ 12.2.032-78 и ГОСТ 12.2.033-78, регламентирующих состояние рабочего места при работе в положении сидя и стоя, таких как [18]-[19]:

- Расположение всех элементов рабочего места в соответствии с физиологическим и психологическим требованиям, в зависимости от работы, выполняемой сотрудником;
- Конструкцией производственного оборудования в пределах зоны досягаемости.

Правила и условия, которые должны быть соблюдены на рабочем месте для предотвращения неблагоприятного воздействия микроклимата и освещения рабочих мест и производственных помещений на здоровье и жизнь персонала излагаются в СанПиН 2.2.4.548-96. С оптимальными параметрами рабочих помещений можно ознакомиться в таблице 1, где приведены оптимальные соотношения микроклиматических параметров для разных категорий работ и времени года.

Таблица 1 – Оптимальные величины показателей микроклимата [15], [20]

Период года	Категория работ по уровню энергозатрат, Вт	Температура воздуха, ^{o}C	Температура поверхностей, ^{o}C	Относительная влажность воздуха, %	Скорость движения воздуха, м/с
Холодный	Ia (до 139)	22-24	21-25	60-40	0,1
	Iб (140-174)	21-23	20-24	60-40	0,1
	IIa (175-232)	19-21	18-22	60-40	0,2
	IIб (233-290)	17-19	16-20	60-40	0,2
	III (более 290)	16-18	15-19	60-40	0,3
Теплый	Ia (до 139)	23-25	22-26	60-40	0,1
	Iб (140-174)	22-24	21-25	60-40	0,1

	IIа (175-232)	20-22	19-23	60-40	0,2
	IIб (233-290)	19-21	18-22	60-40	0,2
	III (более 290)	18-20	17-21	60-40	0,3

Так как большинство информации, воспринимаемой человеком, происходит посредством зрительного восприятия, то важным элементом становится оснащение рабочего места правильно спроектированным освещением. Более того, неправильное освещение рабочих мест увеличивает риск получения травмы или несчастных случаев. На данный момент используются следующие виды освещения:

- Естественное – обязательно для помещений, в котором находится рабочий персонал;
- Искусственное – используется в основном в тёмное время суток. Бывает общее – если помещение освещено равномерно, и локализованное, в обратном случае;
- Совмещённое освещение. Освещённость на поверхности стола в зоне размещения документа должна быть в пределах от 300 до 500 лк. [21], [22];
- Аварийное освещение – в случае отключения общего. Должно позволять вести наблюдение за работой при незапланированном отключении рабочего освещения. Оно должно быть не менее 2 лк в помещении и 1 лк на территории предприятия. Минимальная освещённость эвакуационного освещения на полу проходов и на ступенях лестниц в помещении – 0,5 лк, а на улице – 0,2 лк. [21], [22]

Освещение рабочего места должно создавать максимально комфортные условия для деятельности, а также должно наносить минимальный вред окружающей среде. Нарушение норм освещения ведёт к снижению работоспособности и ухудшению здоровья персонала. Для поддержания оптимальных условий труда необходимо заменять перегоревшие лампы и производить своевременную уборку светильников и окон.

4.2. Обеспечение пожарной безопасности

Под пожарной безопасностью понимается состояние защищённости личности, имущества, общества и государства от пожаров. Пожарная организация объекта должна обеспечиваться системами предотвращения пожара и противопожарной защиты, а также организационно-техническими мероприятиями. Системы безопасности характеризуются уровнем обеспечения пожарной безопасности людей и материальных ценностей, экономическими критериями эффективности данных систем для материальных ценностей с учётом всех стадий жизненного цикла объектов и выполнять одну из следующих задач [13]:

- Исключать возникновение пожара;
- Обеспечивать пожарную безопасность людей;
- Обеспечивать пожарную безопасность материальных ценностей;
- Обеспечивать пожарную безопасность людей и материальных ценностей одновременно.

Достижению пожарной безопасности способствуют:

- Нормативно-правовое регулирование, осуществление и организация мер пожарной безопасности;
- Организация деятельности пожарной охраны и организация научно-технического обеспечения пожарной безопасности;
- Разделение прав, обязанностей и ответственности пожарной безопасности;
- Обеспечение безопасных условий быстровоспламеняющимся предметам;
- Переход на иные материалы, отвечающие стандартам пожарной безопасности;
- Выполнение работ и услуг в области пожарной безопасности, использование и обновление соответствующей пожарно-технической продукции;

- Организация противопожарной пропаганды, информационное обеспечение и обучение персонала мерам пожарной безопасности;
- Лицензирование деятельности в области пожарной безопасности и подтверждение соответствия продукции и услуг в области пожарной безопасности.

Таким образом, для обеспечения безопасных пожарных условий необходимо максимально исключить условия образования горящей среды на рабочем месте посредством изоляции от источников возгорания при помощи специализированного пожарного оборудования. Также необходимо проводить своевременное обучение и переобучение персонала мерам пожарной безопасности, проводить учения и обеспечивать всех работников средствами защиты от пожара.

4.3. Обеспечение электробезопасности

Электрическая безопасность – это система организационных мероприятий и технических средств, предотвращающих опасное воздействие и угрозу жизни на персонал от электрического тока, электромагнитного поля и статического электричества. Электробезопасность включает в себя следующие мероприятия:

- Правовые;
- Социально-экономические;
- Организационно-технические;
- Санитарно-гигиенические;
- Лечебно-профилактические.

Под методами защиты понимается ряд мероприятий, которые снижают вероятность получения травм или повреждений при контакте с электрооборудованием. Достижению электробезопасности способствуют [14]:

- Создание нормативно-правовой базы по регулированию и организации мер безопасности поражения электричества;

- Проектирование электросистем квалифицированным лицом в соответствии с регламентами и документацией, при условии полного оснащения необходимым оборудованием и материалами;
- Создание защитных изоляционных конструкций (использование сверхнизких напряжений при электроснабжении объектов повышенной влажности, заземление, электрическое разделение сетей, обеспечение недоступности к токоведущим частям);
- Оснащение помещения специальными обозначениями по предупреждению электрического поражения;
- Проведение профилактических работ с персоналом, обучение безопасному взаимодействию с электроприборами, а также обучение правилам реагирования и оказания первой помощи при поражении электрическим током.

Электробезопасность регламентируется правовой и технической документацией, наличие которой является обязательным при взаимодействии персонала с электроприборами и сетями. Основы электробезопасности являются обязательными для лиц, которые обслуживают, либо используют в своей деятельности электроустановки и электроприборы.

4.4. Обеспечение безопасности при работе с ПК

Правила работы персонала с ПК подразумевают правильное и безопасное использование машин и оборудования во избежание получения травм и увечий.

К работе могут быть допущен лишь тот персонал, который прошёл специальное обучение безопасным методам использования, вводный и первичный инструктаж на рабочем месте. В период эксплуатации ПК на работника могут воздействовать следующие факторы, которые могут вызвать различные изменения в организме [24]:

- Повышенный уровень электромагнитных излучений;
- Повышенный уровень статического электричества;
- Пониженная ионизация воздуха;
- Статические физические перегрузки;

- Перенапряжение зрительных анализаторов.

Правилами установлены нормы, соблюдение которых не вызовет разрушающее воздействие на здоровье и жизнь персонала, а именно [23]:

- Требования к помещениям для работы с ПК (Площадь на одно рабочее место пользователей ПЭВМ на базе электроннолучевой трубки (ЭЛТ) должна составлять не менее 6 м2);
- Требования к ПК (регулирование положения ПК, настройки контрастности, соответствие нормам допустимого значения излучения);
- Требования к микроклимату, содержанию аэроионов и вредных химических веществ в воздухе при работе с ПК (влажность воздуха, температура должны соответствовать типу помещения);
- Требования к уровню шума и вибрации, освещению (уровни шума на рабочих местах не должны превышать предельно допустимых значений, установленных для данных видов работ в соответствии с действующими санитарно-эпидемиологическими нормативами).

Таким образом, в рамках работы на ПК необходимо обеспечить все аспекты максимально безвредного взаимодействия человека и оборудования. Соблюдение норм и правил не приведёт к изменениям здоровья человека, не сможет вызвать иных вредных факторов, опасных для общества, не нарушит электробезопасность помещения и пожарную безопасность, а обеспечит оптимальные условия труда.

4.5. Эргономика взаимодействия человек-система

Растущий технологический прогресс ставит вопрос разработки таких интерактивных систем, которые будут направлены на создание оптимальных и пригодных к использованию полезных систем с учётом особенностей конечных пользователей этих систем, их потребностей, использую основы эргометрических принципов. Речь идёт о человеко-ориентированном проектировании, которое позволяет увеличить результативность, эффективность, доступность и устойчивость систем, удовлетворённость

пользователя и производительность его труда, а также предотвращает неблагоприятное влияние использования систем на здоровье и безопасность человека. Использование человеко-ориентированного проектирования при проектировании и модернизации программного и аппаратного обеспечения излагается с ГОСТ Р ИСО 9241-210. Данный стандарт позволяет понять роль человеческого фактора и эргономики в процессе проектирования в целом.

Разработанные системы с использованием человеко-ориентированных методов повышают качество системы в целом за счёт [25]:

- Увеличения производительности труда;
- Упрощения понимания и использования процессов (снижение затрат на обучение и переквалификацию персонала);
- Повышения доступности использования для широкого круга пользователей;
- Учёта пользовательского опыта;
- Снижения уровня стресса и дискомфорта;
- Обеспечения конкурентного преимущества;
- Достижения поставленных целей и устойчивого развития.

Использование человеко-ориентированного подхода сокращает издержки производства, увеличивает вероятность успешного завершения проекта, снижает риски потерь и несоответствия желательным требованиям.

Таким образом, в данной главе были рассмотрены основные требования, соблюдение которых на рабочих местах приведёт к росту продуктивности работы персонала, их физическому и психоэмоциональному здоровью при выполнении своих должностных обязанностей.

ЗАКЛЮЧЕНИЕ

В условиях наличия в локальной корпоративной сети конфиденциальной информации, сеть должна быть защищена путем специальныхсредств обеспечения безопасности. Данные средства напрямую влияют на вероятностно временные характеристики (ВВХ) доставки пакетов. Встает вопрос обеспечения качества обслуживания в данной сети, не смотря на наличие в ней различных дополнительных средств обеспечения конфиденциальности, целостности и доступности информации. Качество обслуживания, в данном случае, обеспечивается путем приоритезации сетевого трафика, в зависимости от степени важности передаваемой информации, и ее чувствительности к задержкам.

В ходе выполнения выпускной квалификационной работы были достигнуты следующие цели: построена архитектура защищенной корпоративной сети, в которой обеспечена конфиденциальность и целостность информации, как в рамках ее нахождения в самой защищенной сети, так и при ее передаче по открытым каналам связи (при обмене информацией с центральным офисом данной компании). Разработана аналитическая модель по обеспечению качества обслуживания в защищенной телекоммуникационной сети. Так же были предложены практические рекомендации по выбору активного сетевого оборудования для обеспечения безопасности конфиденциальной информации в данной сети и предложен подход к учету

влияния средств защиты на вероятностно-временные характеристики передачи трафика.

Так же была построена аналитическая модель по обеспечению качества обслуживания основанная на управлении дисциплиной обслуживания, в зависимости от суммарной входящей нагрузки в узле коммутации. В ней трафик делится на два приоритетных класса, в зависимости от его чувствительности к задержкам. На практике чаще всего используется ДОс относительными фиксированными приоритетами, за счет ее крайней эффективности при ограничении пропускной способности, простоты ее реализации и относительного быстродействия. Минусом дисциплины обслуживания с относительными фиксированными приоритетами является факт того, что при крайне высоком уровне нагрузки, низкоприоритетный трафик может теряться (дискриминироваться). В свою очередь дисциплина обслуживания с относительными динамическими приоритетами (ДП) не допускает факт отбрасывание трафика более низкого приоритета, что является во многих случаях большим плюсом. Однако,ДО с ДП требует от узла коммутации увеличения его программно-аппаратных вычислительных ресурсом, что в свою очередь, требует дополнительных затрат со стороны заказчика.

Так же были рассмотрены основные требования касаемо безопасности жизнедеятельности рабочего персонала при работе с защищенной сетью. Соблюдение данных требований на рабочих местах должно привести к росту продуктивности работы персонала, а так же к обеспечению эмоционального и физического здоровья персонала.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Доктрина информационной безопасности Российской федерацииURL: http://www.scrf.gov.ru/documents/6/5.html

2. Информационная безопасность Российской федерацииURL: https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C

3. Сети связи специального назначения URL: http://www.consultant.ru/document/cons_doc_LAW_43224/612d262845b1bd015cb4bafec69732641a9778f7/

4.Качество обслуживанияURL: http://www.cisco.com

5. приоритетное обслуживание URL:http://www.cisco.com/cisco/web/support/RU/9/97/97327_tech_tk652_tk698_technologies_white_paper09186a00800d6b73.html

6. Функции выполняемые системами обнаружения и предотвращения атак URL: https://it-sektor.ru/politika-bezopasnosti.html

7. Сетевые ресурсы, необходимые для корректной работы Skype URL:https://lifehacker.ru/2014/08/26/skolko-trafika-sedaet-skype/

8. Сычев К.И. Модели и методы исследования процессов функционирования и оптимизации построения сетей связи следующего поколения (NextGenerationNetwork). - М.:2009.-378с.

9. Клейнрок Л. Вычислительные системы с очередями. - М.: Мир, 1979. - 600 с.

10. Гухман А.А. Введение в теорию подобия. - М.: Высшая школа, 1973. - 295 с.

11. Гнеденко Б.В., Коваленко И.Н. Введение в теорию массового обслуживания. – М.: ЛКИ, 2013. – 400с.

12. Кучерявый Е.А. Управление трафиком и качество обслуживания в сети Интернет. –М.: Наука и техника, 2004. -335с

13. ГОСТ 12.1.004-91 Пожарная безопасность. Общие требования. Введ. 01.07.1992. – М. :Стандартинформ, 2006. – 126 с.;

14. ГОСТ Р 12.1.019-2009 Электробезопасность. Общие требования и номенклатура видов защиты. Введ. 01.01.2009. – М. :Стандартинформ, 2010. – 28 с.;

15. СанПиН 2.2.4.548-96 Гигиенические требования к микроклимату производственных помещений, Введ. 01. 10. 1996. – М. : Минздрав России, 1997. – 16 с.;

16. Сергеев А.Г., Баландина Е.А., Баландина В.В. Менеджмент и сертификация качества охраны труда на предприятии, СПб.: Логос, 2005. - 256с.

17. Подымалов Н. Проблемы повышения качества производства // Плановое хозяйство : Издание Госплана СССР. — М.: Госплан СССР, 1991. — № 1. — С. 123.;

18. ГОСТ 12.2.032-78 Система стандартов безопасности труда. Рабочее место при выполнении работ сидя. Общие эргономические требования. Введ. 01.01.2009. – М. :Стандартинформ, 2010. – 9 с.;

19. ГОСТ 12.2.032-78 Система стандартов безопасности труда. Рабочее место при выполнении работ стоя. Общие эргономические требования. Введ. 01.01.2009. – М. :Стандартинформ, 2010. – 9 с.;

20. СанПиН 2.2.4.548-96 Гигиенические требования к микроклимату производственных помещений, Введ. 01. 10. 1996. – М. : Минздрав России, 1997. – 16 с.;

21. СанПиН 2.2.1/2.1.1. 1278-03 Гигиенические требования к естественному, искусственному и совмещенному освещению жилых и общественных зданий. Введ. 15.06.2003. – М. : Минздрав России, 2010. – 26 с.;

22. СНиП П-4-79 Естественное и искусственное освещение. М.:Стройиздат, 1980. -48 с.;

22. СанПиН 2.2.2/2.4.1340-03 "Гигиенические требования к персональным электронно-вычислительным машинам и организации работы";

24. Типовая инструкция по охране труда при работе на персональном компьютере ТОИ Р-45-084-01;

25. ГОСТ Р ИСО 9241-210-2012 Эргономика взаимодействия человек-система. Человеко-ориентированное проектирование интерактивных систем. М: Стандартинформ, 2013. -36с.;

26. ГОСТ 12.3.002-2014 Система стандартов безопасности труда. Процессы производственные. Общие требования безопасности. Введ. 01.07.2016. – М. :Стандартинформ, 2016. – 10 с.

27. Специальные требования и рекомендации по технической защите конфиденциальной информацииURL: http://www.rfcmd.ru/sphider/docs/InfoSec/RD_FSTEK_requirements.htm

28. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы (4-е издание), СПб.: Питер, 2010. - 943 с.

29. Бронштейн О.И., Духовный И.М. Модели приоритетного обслуживания в информационно-вычислительных системах. М.: Наука, 1976.-220 с.

30. Политика информационной безопасности URL: https://habrahabr.ru/post/174489/

31. Крухмалев В. В., Гордиенко В. Н., Моченов А. Д. Основы построения телекоммуникационных систем и сетей. М.: Горячая линия – Телеком, 2004. – 424 с.

ПРИЛОЖЕНИЕ А

Структура политики безопасности предприятия

1. Общие положения.
   1.1. Назначение документа.
   1.2. Основания для разработки документа.
   1.3. Основные определения.
2. Идентификация системы.
   2.1. Идентификатор и имя системы.
   2.2. Ответственные подразделения.
   2.3. Режим функционирования системы.
   2.4. Описание и цели системы.
   2.5. Цели и задачи ПБ.
   2.6. Системная среда.
      2.6.1. Физическая организация системы.
      2.6.2. Логическая организация системы.
   2.7. Реализованные сервисы системы.
   2.8. Общие правила, принятые в системе.
   2.9. Общее описание важности информации.
3. Средства управления.
   3.1. Оценка рисков и управление.
   3.2. Экспертиза СЗИ.
   3.3. Правила поведения, должностные обязанности и ответственность.
   3.4. Планирование безопасности.
   3.5. Разрешение на ввод компонента в строй.
   3.6. Порядок подключения подсетей подразделения к сетям общего пользования.
4. Функциональные средства.
   4.1. Защита персонала.
   4.2. Управление работой и вводом-выводом.
   4.3. Планирование непрерывной работы.
   4.4. Средства поддержки программных приложений.
   4.5. Средства обеспечения целостности информации.

4.6. Документирование.
4.7. Осведомленность и обучение специалистов.
4.8. Ответные действия в случаях возникновения происшествий.
5. Технические средства.
5.1. Требования к процедурам идентификации и аутентификации.
5.2. Требования к системам контроля и разграничения доступа.
5.3. Требования к системам регистрации сетевых событий.

ПРИЛОЖЕНИЕ Б

Таблица Б.1 – Пассивные и активные действия систем обнаружения и предотвращения атак

Политика	Пассивные действия	Активные действия
Обнаружение атак	Ведение журналов Ведение доп. Журналов	Нет
Предотвращение атак	Ведение журналов Уведомления о факте НСД	Закрытие соединения, завершение процесса, перенастройка маршрутизатора/межсетевого экрана.
Обнаружение нарушений политики	Ведение журналов, уведомление сис. Адм.	нет
Принудительное использование политик	Ведение журналов, уведомление сис. Адм.	Закрытие соединения, перенастройка оборудования
Принудительное использование политик соединения	Ведение журналов, уведомление сис. Адм.	Закрытие соединения. Возможно перенастройка маршрутизатора или межсетевого экрана
Сбор доказательств	Ведение журналов Ведение дополнительных журналов Уведомление	Обманные действия. Возможно закрытие соединения

ПРИЛОЖЕНИЕ В

Таблица В.1 - Сравнение основных характеристик нескольких аппаратных и программных устройств VPN

№ П/П	Параметр	Windows NT и 2000	Cisco IOS 12.x	CheckPoint FW-1	КК «ШИП»	Застава 2.5
1	Производство	США	США	Израиль	Россия	Россия
2	Протокол для туннелирования	PPTP, IPSec	L2TP, IPSec	IPSec	SKIP	SKIP
3	Способ реализации	Программный	Программный	Программный	Программно-аппаратный	Программный
4	Поддерживаемые платформы	Intel	Cisco	Intel, SunSPARC, HP	Intel	Intel, SunSPARC
5	Операционные системы	Реализуется на Windows	IOS 12.x	Windows 95, 98, 2000, NT, Soliaris, Linus, HP-UX	FreeBSD	Windows 95, 98, 2000, NT, Soliaris
6	Аутентификация и проверка целостности пакетов	Только проверка целостности	Да	Да	Да	Да
7	Поддержка внеш. устр-в аутентификации	Да	Нет	Да	Да	Да

8	Функция центрального администрирования VPN	Да	Да	Да	Нет	Да
9	Криптоалгоритмы	DES, 3DES	DES, 3DES	DES, 3DES, CAST, IDEA	ГОСТ 28147-89	ГОСТ 28147-89, ВЕСТА-2М, DES, 3DES
10	Длина ключа (бит)	168	168	168	256	256
11	Ведение журнала	Да	Да	Да	Да	Да
12	Макс. Производительность (Мб/с)	Зависит от аппаратной платформы	250	Зависит от аппаратной платформы	8	Зависит от аппаратной платформы
13	Поддержка внешних средств защиты от НСД	Да	Нет	Да	Да	Да

ПРИЛОЖЕНИЕ Г

Таблица Г.1 - Сетевые ресурсы, необходимые для корректной работы средства видео и аудио связи Skype

Вид звонка	Рекомендуемые требования к входящей / исходящей скорости Интернета	Расход трафика в час
Вызов абонента	100 Кбит/с / 100 Кбит/с	90 Мбайт
Видеосвязь /демонстрация экрана	300 Кбит/с / 300 Кбит/с	270 Мбайт
Видеосвязь (высокое качество)	500 Кбит/с / 500 Кбит/с	450 Мбайт
Видеосвязь (в формате HD)	1,5 Мбит/с / 1,5 Мбит/с	1,35 Гбайт
Групповая видеосвязь (3 участника)	2 Мбит/с / 512 Кбит/с	1,15 Гбайт
Групповая видеосвязь (5 участников)	4 Мбит/с / 512 Кбит/с	2,07 Гбайт
Групповая видеосвязь (более 7 участников)	8 Мбит/с / 512 Кбит/с	3,91 Гбайт