Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ»

Кафедра «Телекоммуникационные системы»
Специальность 6М071900 «Радиотехника, электроника и телекоммуникации»

ДОПУЩЕН К ЗАЩИТЕ
Зав. кафедрой
к.т.н., Шагиахметов Д.Р.
(ученая степень, звание, ФИО) (подпись)
«_____» _____ 2014 г.

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ
пояснительная записка

на тему: «Исследование особенностей построения виртуальной корпоративной сети связи»

Магистрантка Ахметжанова К.Б (подпись) группа НПМ-12-01
(Ф.И.О.)

Руководитель к.х.н (подпись) Кудинова В.А
(ученая степень, звание) (Ф.И.О.)

Рецензент _____ _____ _____
(ученая степень, звание) (подпись) (Ф.И.О.)

Консультант по ВТ к.х.н., ст.преп. (подпись) Данько Е.Т.
(ученая степень, звание) (Ф.И.О.)

Нормоконтроль к.х.н., ст.преп (подпись) Кудинова В.С.
(ученая степень, звание) (Ф.И.О.)

Алматы, 2014

Некоммеческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ»

Факультет «Радиотехники, электроники и связи»
Специальность 6М071900 «Радиотехники, электроники и телекоммуникации»
Кафедра «Телекоммуникационных систем»

ЗАДАНИЕ
на выполнение магистерской диссертации

Магистрантке Ахметжановой Куралай Бауыржановне
(фамилия, имя, отчество)

Тема диссертации: «Исследование особенностей построение виртуальной корпоративной сети связи»
утверждена Ученым советом университета № 142 от «30» октября 2013 года
Срок сдачи законченной диссертации «25» мая 2014 года
Цель диссертационной работы Рассмотреть особенности построения банковских виртуальных корпоративных сетей.
Перечень подлежащих разработке в магистерской диссертации вопросов или краткое содержание магистерской диссертации:
1) Исследование особенностей функционирования банковских территориально-распределенных систем;
2) Исследование принципов организации архитектуры банковской сети и обеспечения безопасности банковской системы;
3) Провести моделирование расчета характеристик корпоративной сети;

Перечень графического материала (с точным указанием обязательных чертежей):

Рисунок 1 – VPN позволяет проложить защищенные каналы через открытые сети и Internet

Рисунок 2 – Сегментация внутренних сетей банка с помощью VPN

Рисунок 3 – Задачи по обеспечению безопасности информационного взаимодействия

Рисунок 4 – Построение виртуальной частной сети на основе Интернет

Рисунок 5 – Виртуальная частная сеть с удаленным доступом(Remote Access VPN)

Рисунок 6 - Внутрикорпоративная сеть (Intranet VPN)

Рекомендуемая основная литература:

Браун С. Виртуальные частные сети. — М.: Лори, 2001. — 508 с.

1. Тихонов В.И. Статистическая радиотехника. - Изд. 2-е, перераб. и доп. - М.: Радио и связь. 1982. - 624с.
2. Феер К. Беспроводная цифровая связь, пер. с англ. / Под ред. В.И. Журавлева. М. Радио и связь, 2000.-262с.
3. Френке Л. Теория сигналов. Пер. с англ. — М.: Сов. радио, 1974. — 344с.
4. Шахнович И. Современные технологии беспроводной связи. М.: Техносфера, 2004.- 168с.

ГРАФИК
подготовки магистерской диссертации

Наименование разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю	Примечание
1 Информационный обзор согласно темы диссертации	04.11.2012	
2 Разработка математической модели с учетом электромагнитной совместимости	12.03.2013	
3 Создание модели для проведения эксперимента на базе программы Netcracker	11.10.2013	
4 Экспериментальное исследование повышение эффективности канала связи	13.02.2014	
5 Анализ полученных экспериментальных и расчетных данных	07.04.2014	
6 Оформление диссертационной работы	25.05.2014	

Дата выдачи задания 05.09.2012 г.

Заведующий кафедрой _____ Шагиахметов Д.Р.
(подпись) (Ф.И.О.)

Руководитель диссертации _____ Кудинова В.А
(подпись) (Ф.И.О.)

Задание приняла к исполнению
магистрантка _____ Ахметжанова К.Б
(подпись) (Ф.И.О.)

Аңдатпа

Бұл диссертациялық жұмыста ВПН технологиясын қолдану арқылы, құрылған корпоративті банктер жүйелерін зерттеу әдістері және шешімдері қарастырылған.

Бірінші бастамада, қаншалықты ВПН әдісі банктік жүйелер жасауға мүмкіндік беретіні қарастырылған.

Ал екінші бастамада, банктік жүйе және оның тиімділігін байқау үшін математикалық қалыптың банктік кешені әзірленген.

Ал диссертациялық жұмыстың үшінші бастамасында, математикалық қалыптың мүмкіндігі мен оның практикалық мақсатта қаншалықты оңай шешімін табуға болатыны, эксперименттті түрде зерттелініп анықталған.

Аннотация

Данная диссертационная работа посвящена разработке методов и средств анализа корпоративных банковских сетей, построенных с применением технологии VPN. В первой главе проведен анализ возможностей и методов применения VPN- технологии при создании банковских сетей.

Во второй главе разработан комплекс математических моделей для расчета характеристик банковской сети и оценки эффективности ее функционирования.

В третьей главе диссертационной работы проведены экспериментальные исследования для оценки качества математических моделей и возможности их применения при решении практических задач.

Abstract

This thesis is devoted to the development of methods and tools for analyzing corporate banking networks built using the technology of VPN. In the first chapter the analysis capabilities and methods of application of VPN-technology to create banking networks.

The second chapter has developed a set of mathematical models to calculate the characteristics of the banking network and evaluate the effectiveness of its functioning.

In the third chapter of the thesis experimental studies to assess the quality of mathematical models and their possible application in solving practical problems.

Содержание

Введение

Нынешние территориально-распределенные корпоративные вычислительные сети являются важной составной частью систем управления различными предприятиями и учреждениями, от эффективности их работы существенно зависит эффективность деятельности предприятия.

Быстрое развитие IP-сетей (прежде всего Интернет) породило новую тенденцию — использование для построения глобальных корпоративных связей более дешевого и более доступного (по сравнению с выделенными каналами) транспорта пакетных сетей общего пользования (публичные сети).

Однако такое заманчивое и дешевое решение — передача корпоративных данных через публичную сеть, например Интернет, часто представляет угрозу для безопасности сети предприятия, что особенно важно для банковских систем. Кроме того, для корпоративных сетей важное значение имеет качество обслуживания пользователей, предоставление заданного набора услуг и гарантий, что не всегда просто обеспечить в публичных сетях.

Для решения этих проблем может быть использована технология виртуальных частных сетей VPN (Virtual Private Network). Эта технология позволяет превратить соединения в пакетных сетях общего пользования в защищенные каналы с гарантированной полосой пропускания, обеспечивая безопасность и широкий спектр сервисов при приемлемой стоимости устанавливаемых соединений. Поэтому данная технология востребована многими предприятиями и организациями, не имеющими собственных сетевых ресурсов, прежде всего банковскими организациями ввиду ее экономичности, доступности и безопасности.

Отличительными особенностями крупных территориально-распределенных корпоративных сетей являются: применение глобальных связей и объединение отдельных локальных сетей филиалов предприятия и компьютеров его удаленных сотрудников с центральной локальной сетью; обслуживание большого количества разнородных пользователей. Все эти особенности также обусловливают целесообразность разработки сетей с использованием технологии VPN, позволяющей сочетать требования безопасности к предоставляемым сервисам системы. Однако, для ее эффективного применения требуется решение ряда специальных задач, связанных с выбором структуры сети, организацией работы пользователей и сетей, обеспечением требуемого уровня защиты данных и требуемых характеристик передачи и обработки информации.

К настоящему времени имеется достаточно богатый практический опыт создания крупных корпоративных сетей на базе технологии VPN, однако требуются теоретические обоснования предлагаемых решений. Как правило, в каждом конкретном случае необходимы свои оригинальные решения, обусловленные спецификой сети и корпорации, особенно банка, которые нужно оценить с применением достаточно универсальных методов и моделей.

1 Банковские территориально-распределенные сети

Повсеместное использование информационных технологий (ИТ) стало в настоящее время объективной необходимостью. Спектр областей, в которых применяются информационные технологии, чрезвычайно широк. Одной из сфер, где их значение было традиционно велико с момента начала их бурного развития, является финансовая сфера [2]. При этом важное место занимают банковские системы и создаваемые для обеспечения их работы банковские сети.

1.1 Задачи банковских систем

Можно с уверенностью утверждать, что процесс информатизации банковской деятельности продолжится и в обозримой перспективе. Основными тенденциями станут повышениекачества и надежности предлагаемых продуктов и услуг, увеличение скорости существления расчетных операций, организация удаленного электронного доступа клиентов к банковским продуктам. Эти факторы связаны, прежде всего, со стремлением банков к достижению конкурентных преимуществ на финансовых рынках.

Вследствие применения банковских информационных технологий стало возможным решение следующих задач в создаваемых и развивающихся банковских системах:

- качественное расширение рынка продуктов и услуг,
- охват большей доли рынка посредством использования банкоматов, электронных расчетных систем,
- использование Интернет-технологий,
- оперативный доступ клиентов к информации.

Все это и в дальнейшем будет способствовать активному внедрению в банковскую практику самых последних достижений в области вычислительной техники, сетевых и информационных технологий, методов защиты информации и обработки данных [2, 6, 7].

1.2 Организация работы банковской системы

В настоящее время расходы на ИТ-решения как никогда высоки. По статистическим данным, на закупку и внедрение ИТ-решений банки выделяют не менее 5% годовой сметы расходов. Но суммы затрат во многом зависят от того, какие именно информационные проекты ведет банк, какую рыночную нишу он занимает и какие новые услуги собирается внедрять. В частности, ИТ-бюджеты банков, ведущих агрессивную политику на рынке, могут достигать

35% от общих затрат. Все это приводит к резкому росту значения ИТ-области, которая становится одной из самых затратных и одновременно высокорискованных областей в банковской деятельности.

За последнее время значительно возросло значение новых банковских услуг, предоставляемых клиентам посредством Интернет-технологий [40]. Учитывая повсеместное использование банками систем электронной связи и постепенный переход к безбумаясной технологии обмена информацией, можно судить о важности этого направления для банков. Данная проблема также актуальна для крупных банков, работающих в режиме онлайн с филиалами. Многие разработчики информационных систем включают средства защиты информации в собственные программные продукты. Помимо этого существуют различные средства независимых разработчиков, осуществляющие защиту передаваемой информации от несанкционированного просмотра и изменения при передаче. Это является важным, т.к. филиальная сеть в большинстве случаев построена на общественной сети [38, 66, 73].

1.3 Обслуживание пользователей

Для повышения качества и оперативности обслуживания пользователей очевидна необходимость создания банковской территориально-распределенной вычислительной сети, позволяющей обеспечивать доступ удаленных пользователей и сетей, обрабатывать все возрастающие информационные потоки. Немаловажно и то, что банки обладают достаточными финансовыми возможностями. Однако, вкладывая средства в программное обеспечение, компьютерное и телекоммуникационное оборудование и создание базы для перехода к новым вычислительным платформам, банки стремятся к удешевлению и ускорению своей рутинной работы. При этом одна из основных задач при создании сети интеграция унаследованных систем в распределенную архитектуру территориально-распределенных сетей [35, 123, 124].

В банковской деятельности, широко используются базы данных на основе модели "клиент-сервер" (ОС Unix и БД Oracle); средства межсетевого взаимодействия для межбанковских расчетов; службы расчетов, целиком ориентированных на Internet, или, так называемые, виртуальные банки; банковские экспертно-аналитические системы, использующие принципы искусственного интеллекта и многое другое.

Банковские системы и сети обычно реализуются по модульному принципу [49]. Широко используются специализированные мощные или универсальные компьютеры, объединяющие несколько ЛВС, применяется межсетевой обмен и удаленный доступ к ресурсам центрального офиса банка для выполнения операций "электронных платежей".

На первый план при построении такой сети выходят качество обслуживания клиентов, предоставление требуемого перечня необходимых

услуг и снижение задержек при использовании территориально- распределенной сети.

1.4 Характеристики и функции банковской сети

Среди основных функций банковских систем, которые реализуются в рамках создания защищенной территориально-распределенной корпоративной сети, можно выделить следующие:

- автоматизация всех ежедневных внутрибанковских операций, ведение бухгалтерии и составление сводных отчетов;
- связь с филиалами и иногородними отделениями;
- автоматизированное взаимодействие с клиентами (так называемые системы "банк-клиент");
- анализ всей деятельности банка и выбор оптимальных в данной ситуации решений;
- автоматизация розничных операций — применение банкоматов и кредитных карточек;
- проведение межбанковских расчетов;
- автоматизация работы банка на рынке ценных бумаг.

Таким образом, любая банковская корпоративная сеть представляет собой сложный комплекс, объединяющий сотни отдельных компьютеров, ЛВС и ГВС, структурированный для выполнения перечисленных функций. Целью создания банковской территориально-распределенной сети является обеспечение персонала и клиентов необходимыми видами услуг, при условии, что расходы на создание и эксплуатацию не превышают доходов от внедрения сети [61].

Для выбора наиболее удачного решения необходимо учитывать следующие факторы: стоимость, возможность масштабирования, возможность использования существующих ресурсов, наличие системы защиты информации, надежность системы, наличие средств восстановления при сбоях, возможность работы в режиме реального времени. Этому посвящена дальнейшая работа.

1.5 Архитектура банковской сети

Корпоративная сеть банка представляет собой частный случай корпоративной сети крупной компании. Однако специфика банковской деятельности предъявляет жесткие требования к системам защиты информации в компьютерных сетях банка. Не менее важную роль при построении корпоративной, территориально-распределенной банковской сети играет необходимость обеспечения безотказной и бесперебойной работы, поскольку даже кратковременный сбой в ее работе может привести к значительным

убыткам [104, 148, 153, 154, 155]. Кроме того, требуется обеспечить быструю и надежную передачу большого объема данных, поскольку многие прикладные банковские программы должны работать в режиме реального времени.

1.6 Структура банковской сети

Можно выделить следующие основные структурные особенности корпоративной сети банка:

- сеть объединяет в структурированную и управляемую замкнутую систему все принадлежащие компании (банку) информационные устройства: отдельные компьютеры, локальные и удаленные вычислительные сети, хост-серверы, рабочие станции, телефоны, факсы, офисные АТС, сети банкоматов, онлайновые терминалы;
- в сети обеспечивается надежность ее функционирования и мощные системы защиты информации, гарантируется безотказная работа системы, как при ошибках персонала, так и в случае попытки несанкционированного доступа;
- существует отлаженная система связи между банковскими отделениями разного уровня (как с городскими отделениями, так и с иногородними филиалами).-

В связи с современными тенденциями развития банковских услуг (например, обслуживание по телефону, круглосуточный доступ к банкоматам и онлайновым терминалам, развитие сетей быстродействующих платежных терминалов в торговых точках, круглосуточные операции с акциями клиентов) появляется потребность в специфичных для банков телекоммуникационных решениях. Существенную роль приобретает организация оперативного, надежного и безопасного доступа удаленного клиента к современным банковским услугам.

Факторы, влияющие на выбор технологии передачи информации, носят экономический, географический и политический характер и связаны, в первую очередь, с политикой национальных телекоммуникационных компаний.

В общем случае корпоративная сеть банка может быть построена на самых различных каналах связи — от выделенных линий (аналоговых и цифровых) до коммутируемых цифровых E1 и Fractional El, в том числе, и на оптоволоконных, спутниковых, радио и микроволновых каналах, и на основе разнообразных протоколов и технологий ISDN, X.25, Frame Relay и ATM [92, 93].

Касаясь вопроса предпочтительной архитектуры банковской сети, можно отметить, что наиболее распространенной в европейских странах и актуальной на сегодня для банков является топология "звезда", простая или многоуровневая, с главным офисом в центре, соединенным с региональными отделениями. Преобладание этой топологии определяется следующими факторами:

- прежде всего, самой структурой банковских организаций (наличием региональных отделений и большим объемом передаваемой между ними информации);

- высокой стоимостью аренды каналов связи. Нужно иметь в виду, что обычно при организации связи с удаленными отделениями практически не используются коммутируемые телефонные каналы. Здесь необходимы высокоскоростные и надежные линии связи [62, 112, 121].

В странах Восточной Европы и СНГ в пользу применения топологии "звезда" действует дополнительный фактор — недостаточно развитая инфраструктура телекоммуникаций и связанные с этим трудности в получении банком большого числа каналов связи. В этих условиях особенно важным становится внедрение экономичных решений, существующих на мировом рынке, а иногда и специально доработанных для соответствия условиям развивающихся стран.

В общем случае, когда возникает необходимость связывать региональные офисы друг с другом напрямую, приобретает актуальность топология "каждый с каждым". По своей сути эта топология отличается повышенной надежностью и отсутствием перегрузок. Практически могут быть реализованы многочисленные смешанные варианты топологий, как в случае "децентрализованного главного офиса", когда различные отделы центрального офиса банка — расчетный, кредитный, аналитический, технический или любой другой — находятся в разных зданиях.

В некоторых европейских странах существуют общенациональные конфигурации, когда корпоративные сети отдельных банков образуют "суперзвезду" с межбанковским расчетным центром в качестве вершины телекоммуникационной банковской иерархии. Этот вопрос напрямую связан с выбором системы межбанковских взаиморасчетов и будет рассмотрен ниже.

Использование интегрированной передачи данных:

Рассмотрим, в качестве примера, решения компании RAD Data Communications, традиционно ориентированной на европейский рынок.

Основная современная тенденция развития банковских сетей в Европе, как и корпоративных сетей вообще — переход к интегрированной передаче данных и речи (по экспертным оценкам, интегрированный трафик в 1996 г. составил 72% от общего — против 22% в 1989 г.). Данные, голос (телефонные разговоры), факсы и видеоинформация передаются по одному и тому же каналу, что обеспечивает многократное снижение расходов на аренду каналов или их прокладку. Здесь важную роль играют сети ATM.

Технически это осуществляется путем мультиплексирования, интегрированной передачи и последующего демультиплексирования отдельных информационных потоков. Различные классы мультиплексоров позволяют интегрировать информационные потоки различной величины, поступающие как от маленьких удаленных отделений, так и от крупных региональных офисов по каналам от 9,6 Кбит/с до 2,048 Мбит/с и выше. В конкретных приложениях возможно применение дополнительных встроенных в мультиплексоры

механизмов, повышающих эффективность использования полосы пропускания канала связи. Мультиплексоры с опцией Day/Night Configuration работают с учетом разницы в характере дневного и ночного трафика (больше каналов голоса — днем, а каналов данных — ночью). Адаптивные мультиплексоры отводят всю полосу речевого канала под передачу данных, если речевой трафик отсутствует, Механизм динамичного разделения полосы пропускания по каналам повышает эффективность путем отслеживания состояния каналов: полоса пропускания распределяется по "активным" каналам по мере необходимости. Далее, благодаря специальной технологии silence suppression, во время пауз в телефонных разговорах передаются другие потоки данных, голос, факсы и трафик LAN.

В результате использования интегрированной передачи очевидна существенная экономия в использовании самого дорогостоящего ресурса сети — каналов связи.

Дополнительные выгоды дает одновременное с интеграцией уплотнение информации, в первую очередь, речи. Например, одна из самых современных технологий компрессии голоса MP-MLQ, впервые реализованная в мультиплексорах компании RAD Data Communications, позволяет практически без потери качества звучания речи одновременно передавать до 13 телефонных разговоров по одному стандартному каналу связи 64 Кбит/с.

Применение интегрированной передачи информационных потоков позволяет обеспечить каждое рабочее место полным комплексом информационных услуг при оправданных расходах на их поддержание. Кроме того, телефонные разговоры между региональными отделениями превращаются во внутрифирменные, что обеспечивает лучший контроль и безопасность.

VPN решает проблему контроля на всей протяженности канала. Более того, отпадает необходимость в собственных каналах. Например, можно подключить в каждом городе локальные сети филиалов банка к местному провайдеру Internet. Затем установить на пограничном с Internet компьютере каждого филиала программное обеспечение, выполняющее шифрование проходящей информации. Задача решена. Важно, чтобы VPN позволяла установить соответствующее программное обеспечение на отдельные компьютеры сотрудников, имеющих право доступа к вашим локальным сетям из дома или из гостиничного номера в командировке. На рисунке 1 схематично представлена сеть VPN, позволяющая создать защищенные каналы через общественные (публичные) компьютерные сети.

Таким образом, можно получить свою собственную защищенную сеть (VPN), образующую жесткий непроницаемый периметр и наложенную на доступный всем Internet или любые другие сети. В локальную сеть каждого филиала смогут войти только защищенные и аутентифицированные пакеты от других участников VPN. Эти пакеты, будут дешифроваться на выходе из "труб" и подаваться вышестоящим приложениям в первозданном виде.

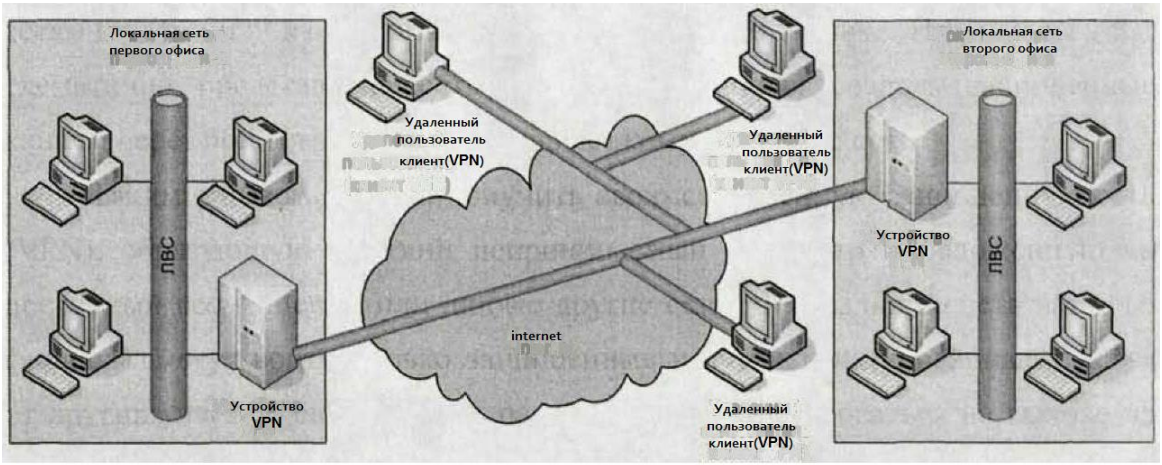

Рисунок 1 - VPN позволяет проложить защищенные каналы через открытые сети и Internet

Необходимо отметить, что технология VPN является не только способом защиты информации на внешних сетях. С потребительской точки зрения — это средство для создания дешевых, но надежно защищенных каналов через открытые сети и Internet.

Внутренняя задача. Присущий VPN эффект "защищенных труб" многие организации с успехом применяют и на внутренних сетях. Используемые сейчас локальные сети Ethernet работают по принципу "широковещания", посылая информацию по всем компьютерам сети, даже если она предназначена только для компьютеров кредитного отдела. VPN позволяет разделить информационные потоки различных подразделений банка. При этом новая сегментация будет отражать только структуру бизнес- процессов и не будет зависеть от конкретной топологии внутренних локальных сетей.

На рисунке 2 показана возможная схема реализации такого подхода. С помощью VPN созданы три логически разделенные виртуальные сети.

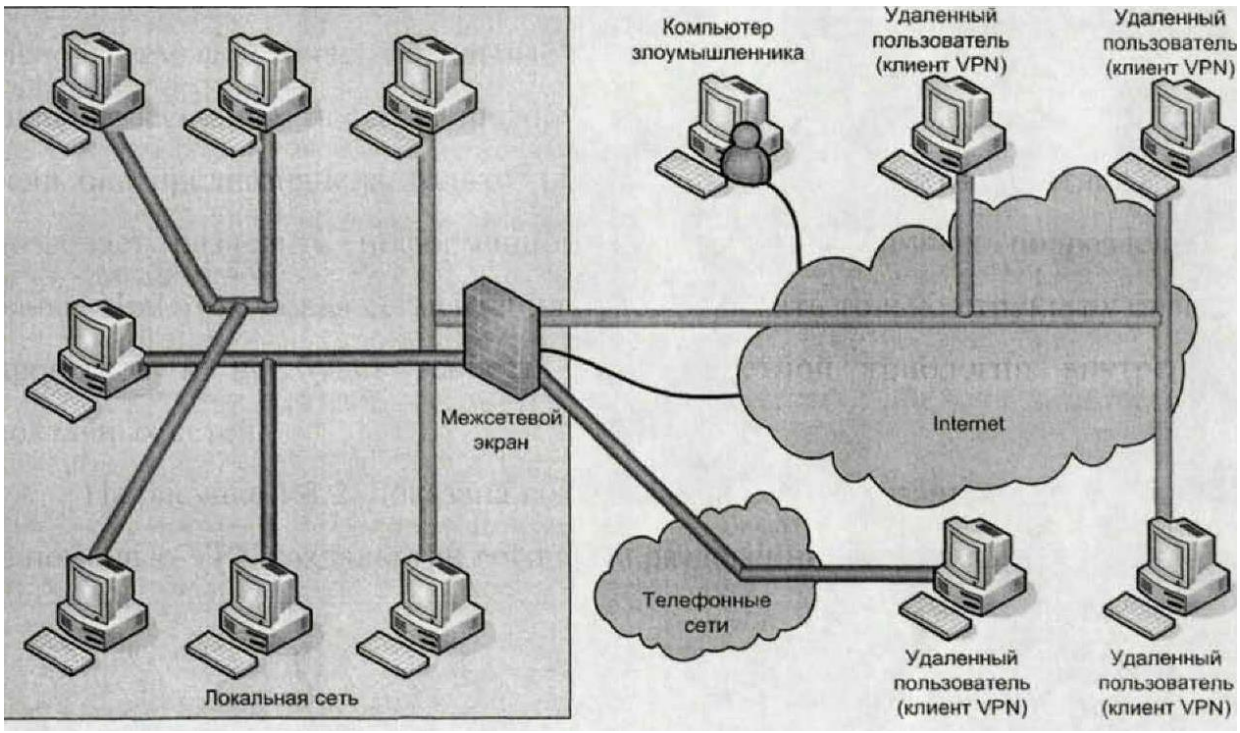

Рисунок 2 - Сегментация внутренних сетей банка с помощью VPN

Первая VPN включает 4 компьютера и находится целиком в локальной сети предприятия. Это VPN кредитного отдела. Вторая частично выходит во внешние сети, обеспечивая доступ к экстранет-серверу оператору из локальной сети и трем клиентам банка, подключенным через Internet. Третья VPN обеспечивает директору защищенный доступ из дома к своему рабочему компьютеру и компьютеру секретаря через модемный вход сервера доступа.

Все пользователи перечисленных VPN могут быть уверены, что их конфиденциальная информация доступна строго заданному кругу участников взаимодействия независимо от их местонахождения (внутри или снаружи стен банка) и способа доступа к сети.

Необходимая степень защиты. Основной задачей VPN является шифрование трафика, надежность которого определяется двумя функциональными характеристиками.

Первая заключается в стойкости используемых алгоритмов. Наиболее надежная защита строится только на проверенных временем и специалистами алгоритмах, утвержденных в многочисленных международных, государственных и отраслевых стандартах. Исключительно опасно полагаться на системы, надежность которых базируется только на том, что их авторы никогда не раскрывают сути и кода своих алгоритмов. В современной криптографии вся секретная часть защиты спрятана не в знании кода алгоритма, а в наличии ключа — длинного случайного числа, поданного на "вход" алгоритма вместе с защищаемыми данными.

Вторая характеристика — длина ключа, на котором производится шифрование. Не вдаваясь в подробности, отметим, что минимально разумной длиной ключа на данный момент считается 128 бит.

К сожалению, огромное количество зарубежных систем защиты предлагают шифрацию очень надежными алгоритмами (например, DES — американским государственным стандартом) на совершенно неприемлемой длине ключа — 40 или 56 бит, что позволит легко вскрывать вашу информацию [52, 156, 165, 167]. Надо отдать должно стандартам, осуществляющим надежную защиту данных на очень длинных ключах — это государственный стандарт ГОСТ 28147-89 (ключ 256 бит) и отраслевой стандарт газовой промышленности ВЕСТА (ключ 512 бит). Вы можете смело доверять криптосистемам, работающим на этих алгоритмах.

1.7 Задачи анализа банковской сети

Принципы и правила построения банковских сетей широко описаны в литературе, в частности — использование технологии VPN при создании территориально-распределенных корпоративных сетей. При этом практически все разработчики и администраторы сети сталкиваются с рядом задач, отмеченных выше, решение которых требует учета конкретных особенностей сети, банковской системы, корпоративных правил. Подобные задачи не имеют стандартных решений, и для их решения требуется проводить анализ условий работы сети. Однако, возможны достаточно общие подходы даже к решению таких задач. Здесь выделены две общие для многих банковских сетей задачи, которые обязательно нужно решать при создании банковских сетей. Ниже представлены общие постановки этих задач, определяющие возможности и критерии качества их решения.

Первая задача - это обеспечение бесперебойной работы банковской сети в режиме «non-stop». При этом наиболее часто возникает задача борьбы с отказами оборудования, в частности борьба с отказами и сбоями серверов.

В таких критических системах возможны несколько путей решения задачи, среди которых наиболее распространенными являются: создание резервов серверного оборудования для каждого значимого сервера во всех отделениях (подразделениях); - управление потоками данных (запросов) путем перенаправления потоков данных с отказавших серверов на другие, работающие сервера.

Вторая задача - это оценка загрузки VPN-каналов и формирование требований к качеству связи. Задача возникает потому, что в большинстве случаев, банками используются каналы, которые не являются их собственностью, а арендуются (арендованные каналы связи). Обычно, при использовании таких каналов, заключается договор с провайдером, в котором определяется перечень услуг, предоставляемых провайдером, и перечень

характеристик связи, которые провайдер должен обеспечивать. За каждую услугу и значение каждой характеристики банк должен платить, размер оплаты зависит от его потребностей и запросов провайдера. При этом с провайдером должны быть выстроены договорные отношения об оплате и тарифах, с тем, чтобы обеспечить заданный уровень услуг, но тогда банку необходимо обоснованно выбирать требования к качеству услуг, чтобы избежать необоснованных затрат. Особенность задачи в том, что помимо загрузки общедоступных Интернет-каналов, передаваемой банком информацией («полезные» потоки данных), в этих же каналах связи присутствуют "боковые" потоки данных (боковая информация) от других пользователей Интернет, которые не зависят от работы банка. В результате загрузка канала провайдера, определяется интенсивностью полезного потока и интенсивность "бокового" потока. Это необходимо учитывать при выборе параметров обслуживания, т.к. характеристики канала могут ухудшаться из- за "бокового" потока. Статистика параметров "бокового" потока должна собираться и оцениваться путем мониторинга, для принятия правильных решений при заключении договора с провайдером.

Перечисленные задачи характерны для многих банков и компаний. Однако их решение сопряжено с необходимостью проведения предварительного анализа, позволяющего оценивать достоинства различных вариантов и выбирать из них более предпочтительный.

Так, решение первой задачи путем резервирования достаточно часто применяется на практике, однако требует значительных затрат на приобретение и обслуживание резервного оборудования, которое может быть не задействовано и приносить убытки. Поэтому необходимо обосновать целесообразность резервирования определенного количества серверов.

В общем случае при использовании резервирования серверов задача может быть сформулирована следующим образом. Пусть в системе имеется N основных серверов. Для обеспечения бесперебойной работы системы используется $0 \le M \le N$ резервных. Выход из строя основного сервера, который не имеет резервного, приводит к затратам (потерям), величина которых равна Величина затрат на резервирование основного сервера — g. Вероятность отказа основного сервера — 0 < p < 1. Общие затраты на эксплуатацию системы — $S(N, M, p, s, g)$ складываются из затрат на резервирование и затрат, связанных с потерями при выходе из строя основных серверов, не имеющих резерва.

Требуется определить число резервных серверов - M*, чтобы либо минимизировать общие затраты на эксплуатацию системы, т.е. чтобы для любого $M \neq M^*$, выполнялось неравенство:

$$S(N, M^*, p, s, g) \le S(N, M, p, s, g) \text{ (задача оптимизации),} \qquad (1.3.1)$$

либо для заданного значения $0 < S^* < \infty$ выполнялось неравенство:

$S(N, M^*, p, s, g) \leq$ S***** (задача поиска приемлемого решения). (1.3.2)

Решение путем управления потоками данных менее затратно, но также требует проведения исследований, для оценки различных вариантов управления. При этом необходимо найти такое управление потоками данных, которое обеспечивает приемлемую загрузку серверов и каналов связи, а также время исполнения запросов пользователей. В общем случае задача может быть сформулирована следующим образом. Пусть в системе имеется N основных серверов. Вероятность отказа основного сервера — 0 < p < 1**.** При отказе сервера номер i его функции выполняет сервер номер j. При этом потоки данных, передаваемых на сервер i, перенаправляются на сервер j, а потоки данных, следующих от сервера i, следуют от сервера j по тем же адресам. Общие затраты при изменении направлений потоков - $H(N, p, i, j)$ связаны с изменением нагрузки на каналы связи, нагрузки сервера j и временем исполнения запросов, адресованных на сервер i. Требуется определить номер сервера j, так, чтобы либо, для любого $k \neq j$ выполнялось неравенство:

$H(N,p,i,j) \leq H(N,p,i,k)$(задача оптимального выбора), (1.3.3)

либо, для заданного $0 < H^* < \infty$, выполнялось неравенство:

$H(N,p,i,j) \leq H^*$ (задача поиска приемлемого решения) (1.3.4)

Решение второй задачи требует оценки и анализа затрат банка на поддержку требуемого качества услуг (сервисов). В общем случае задача может быть сформулирована следующим образом.

Задано число (набор) услуг VPN-провайдера — I, что соответствует числу типов потоков данных, передаваемых банком по каналам связи провайдера.

Задана структура корпоративной банковской сети. Заданы тарифы за обеспечение заданных параметров этих услуг – $\alpha = (\alpha_1(\gamma_1), \alpha_2(\gamma_2), ..., \alpha_1(\gamma_1))$, где $0 < \alpha_i(\gamma_i) < \infty$, (i=1,2, ...,I).

Заданы средние величины параметров "бокового" трафика - по каждому типу - $\lambda = (\lambda_1, \lambda_2, ..., \lambda_i)$**,** где $0 \leq \lambda_1 < \infty$**,** (i=1**,2,** ...,I).

Величина затрат банка на получение требуемого набора услуг заданного качества - $A(I, \alpha, \gamma, \lambda)$, здесь $\gamma = (\gamma_1, \gamma_2, ..., \gamma_I)$, где $0 \leq \gamma_i < \infty$, (i =1,2, ..., I) параметры потоков данных различных типов, передаваемых банком по VPN каналам провайдера.

Требуется:

- определить параметры передаваемых банком по VPN каналам потоков данных, которые требуют обеспечения услуг - $\gamma = (\gamma_1, \gamma_2, ..., \gamma_I) >$ где

$0 \leq \gamma_i < \infty$, (i =1,2,..., I) (анализ структуры банковской сети);

- определить значения параметров услуг провайдера и соответствующие тарифы $(\alpha^* = (\alpha_1^*(\gamma_1), \alpha_2^*(\gamma_2), ..., \alpha_I^*(\gamma_I)))$ так, чтобы затраты банка не превышали заданной величины А*:

$$A(I, \alpha^*, \gamma, \lambda) < A^* \text{ (задача поиска приемлемого решения). (1.3.5)}$$

Таким образом, для решения перечисленных задач и выбора приемлемых (может быть оптимальных) вариантов их решения требуется количественная оценка различных вариантов их решения, что возможно при наличии соответствующих средств анализа.

Разработке таких средств и правил их применения будут посвящены последующие разделы диссертационной работы.

Для решения поставленных в первой главе задач необходимо исследовать работу банковской сети, построенной с использованием VPN- технологий, определить специфику виртуальных частных сетей (VPN). Поэтому в этой главе будут представлены основные принципы построения и практической реализации виртуальных частных сетей. Представлены систематизированные сведения об архитектуре и технической реализации VPN, способы обеспечения качества предоставляемых услуг и безопасности передачи информации. Приведены наиболее распространенные на практике и исследованные в литературе методы построения территориально- распределенных корпоративных сетей с использованием технологии VPN. Рассмотрены задачи, возникающие при создании сети, и определены основные направления дальнейших исследований [21, 27, 90].

2 Методы и средства построения корпоративных виртуальных сетей

Для решения поставленных в первой главе задач необходимо исследовать работу банковской сети, построенной с использованием VPN- технологий, определить специфику виртуальных частных сетей (VPN). Поэтому в этой главе будут представлены основные принципы построения и практической реализации виртуальных частных сетей. Представлены систематизированные сведения об архитектуре и технической реализации VPN, способы обеспечения качества предоставляемых услуг и безопасности передачи информации. Приведены наиболее распространенные на практике и исследованные в литературе методы построения территориально- распределенных корпоративных сетей с использованием технологии VPN. Рассмотрены задачи, возникающие при создании сети, и определены основные направления дальнейших исследований [21, 27, 90].

2.1 Назначение виртуальных сетей

Стремительное развитие Интернет, которое наблюдается в течение последних лет, открывает любому владельцу компьютера доступ к неограниченным ресурсам информации. В связи с этим возможность индивидуального и коллективного доступа к корпоративной сети практически в любое время быстро превращается в неизменное требование делового мира. Стремясь к укреплению сотрудничества с партнерами и поставщиками, компании открывают для них отдельные сегменты своих сетей, благодаря чему сокращается время, затрачиваемое на внедрение новой продукции, и повышается качество обслуживания клиентов [108, 109, 110].

VPN — это объединение удаленных локальных сетей или отдельных рабочих мест с использованием специальных аппаратных или программных устройств, осуществляющих информационную защиту транзитного трафика и его туннелирование поверх публичных сетей с пакетной передачей [92].

Безопасность информационного взаимодействия локальных сетей и отдельных компьютеров через открытые публичные пакетные сети, например через Интернет, требует качественного решения двух базовых задач:

- защиты подключенных к публичным каналам связи локальных сетей и отдельных компьютеров от несанкционированных действий со стороны внешней среды.

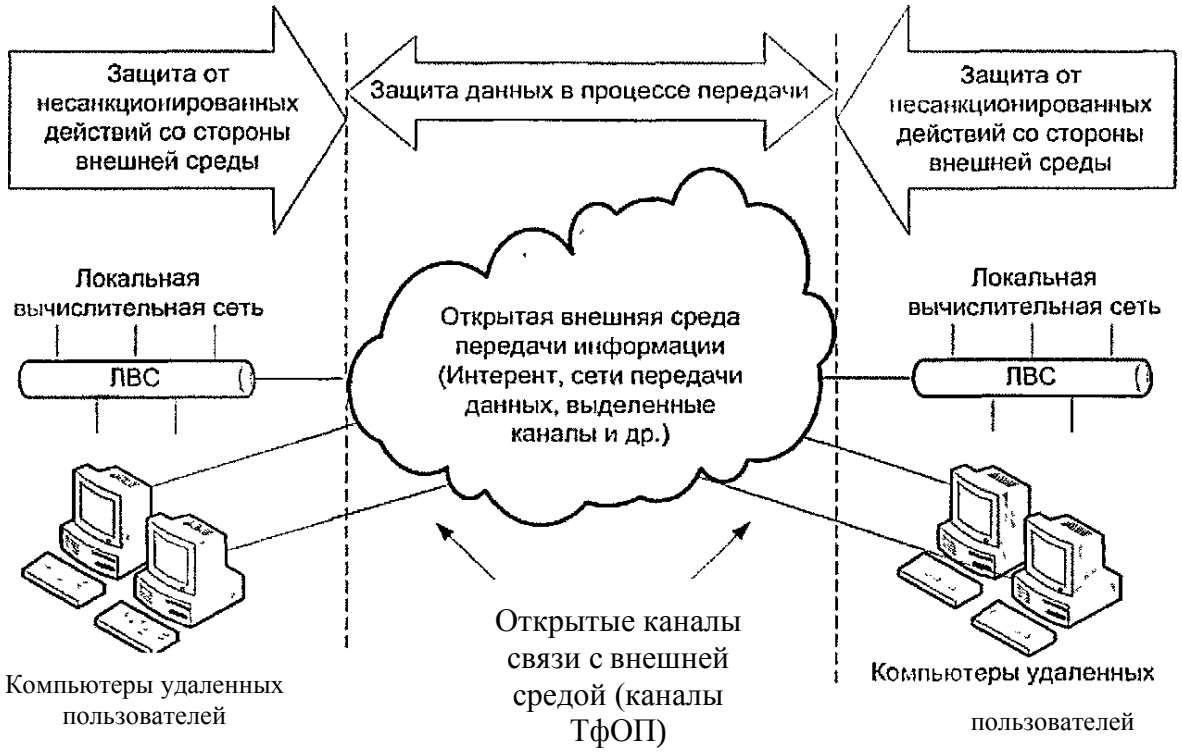

Рисунок 4 - Задачи по обеспечению безопасности информационного взаимодействия

Обеспечение соответствующего уровня безопасности обмена информацией может достигаться за счет комплексного использования организационных, технических, аппаратно-программных и криптографических средств защиты, а также осуществления непрерывного контроля за эффективностью реализованных мер по обеспечению информационной безопасности.

Комплекс защитных мер должен предусматривать [63]:

- предотвращение утечки, утраты и подделки информации;
- предотвращение угрозы информационной безопасности личности, общества, государства;
- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации.

Применение этих мер позволит решить проблему максимально защищенной работы любых пользователей через публичную телекоммуникационную сеть и безопасного подключения к ней органов государственной власти, бюджетных организаций, пунктов коллективного доступа и коммерческих пользователей [63].

Открытую внешнюю среду передачи информации можно разделить на среду скоростной передачи данных, в качестве которой может использоваться выделенная 1Р-сеть или Интернет, а также более медленные общедоступные каналы связи, в качестве которых чаще всего применяют каналы телефонной сети. Наиболее простым способом объединения локальных сетей и удаленных

компьютеров является объединение на основе глобальной сети Интернет (рисунок 4).

Организация виртуальных сетей на основе Интернета обладает рядом преимуществ:

- обеспечивает масштабируемую поддержку удаленного доступа к ресурсам локальной сети, позволяя мобильным пользователям связываться по местным телефонным линиям с поставщиками услуг Интернета и таким образом входить в свою корпоративную сеть; - при организации удаленного доступа пользователей к локальной сети исключается необходимость в наличии модемных пулов, а трафиком дистанционного доступа можно управлять точно так же, как любым другим трафиком Интернета;
- сокращаются расходы на информационный обмен через открытую внешнюю среду.

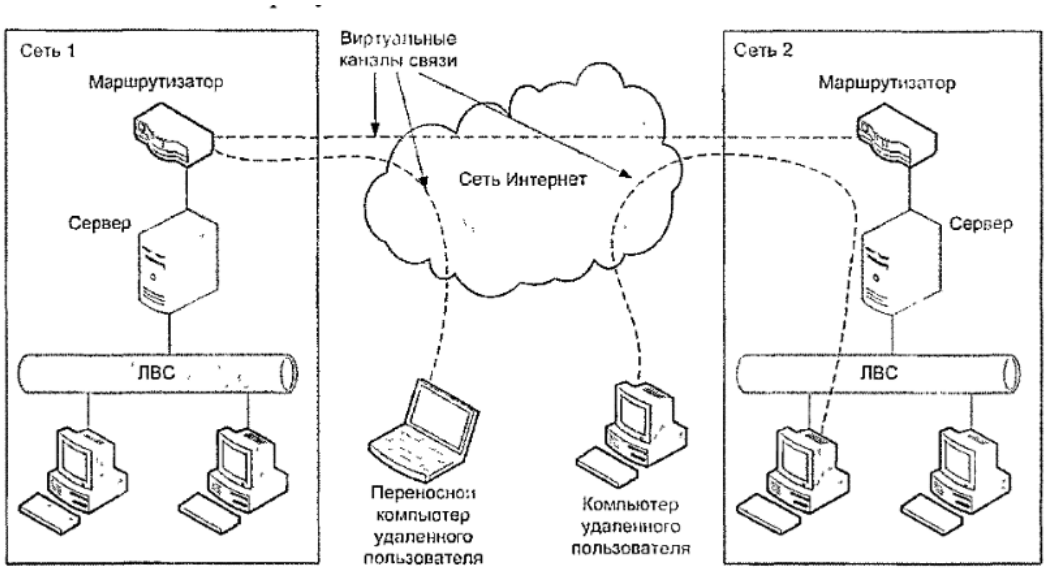

Рисунок 4 - Построение виртуальной частной сети на основе Интернет

Однако гарантированное качество обслуживания для потоков пользовательских данных, а также защиту их от возможного несанкционированного доступа или разрушения в полной мере могут обеспечить только выделенные IP-сети, а также сети ATM или Frame Relay, принадлежащие отдельным провайдерам. Использование публичных сетей ATM или Frame Relay в качестве основы для VPN имеет одно несомненное преимущество по сравнению с Интернетом, а именно встроенную поддержку качества транспортного обслуживания. Однако повсеместная распространенность сетей на базе протокола IP, их универсальность и экономичность делает эти сети более привлекательной основой создания VPN для большинства предприятий и организаций. К тому же в выделенных IP-сетях начинают широко внедряться такие протоколы и технологии управления качеством обслуживания (QoS, Quality of Service), как RSVP, DiffServ и MPLS [42, 90].

2.2 Услуги VPN

На базе технологии VPN могут быть реализованы четыре основных вида услуг [27].

1. Виртуальная частная сеть с удаленным доступом (Remote Access VPN) (рис. 4) позволяет реализовать защищенное взаимодействие между сегментом корпоративной сети (центральным офисом или филиалом компании) и удаленным пользователем, который подключается к корпоративным ресурсам. Удаленный пользователь, как правило, не имеет статического IP-адреса и подключается к защищаемому ресурсу не через выделенное устройство VPN, а напрямую с собственного компьютера, где и устанавливается программное обеспечение, реализующее функции клиента.

Эти функции включают хостинг и управление, хостинг пользовательской базы данных (сервер RADIUS), а также поддержку безопасности с помощью межсетевых экранов и шифрования.

2. Внутрикорпоративная виртуальная частная сеть, интранет (Intranet) VPN позволяет объединить в единую защищенную сеть несколько распределенных филиалов одной организации, взаимодействующих по открытым каналам связи операторской IP-сети (рис.5).

Именно этот вариант получил наиболее широкое распространение во всем мире. Интранет VPN позволяет организации устанавливать связь между филиалами компании через выделенную IP-сеть или Интернет.

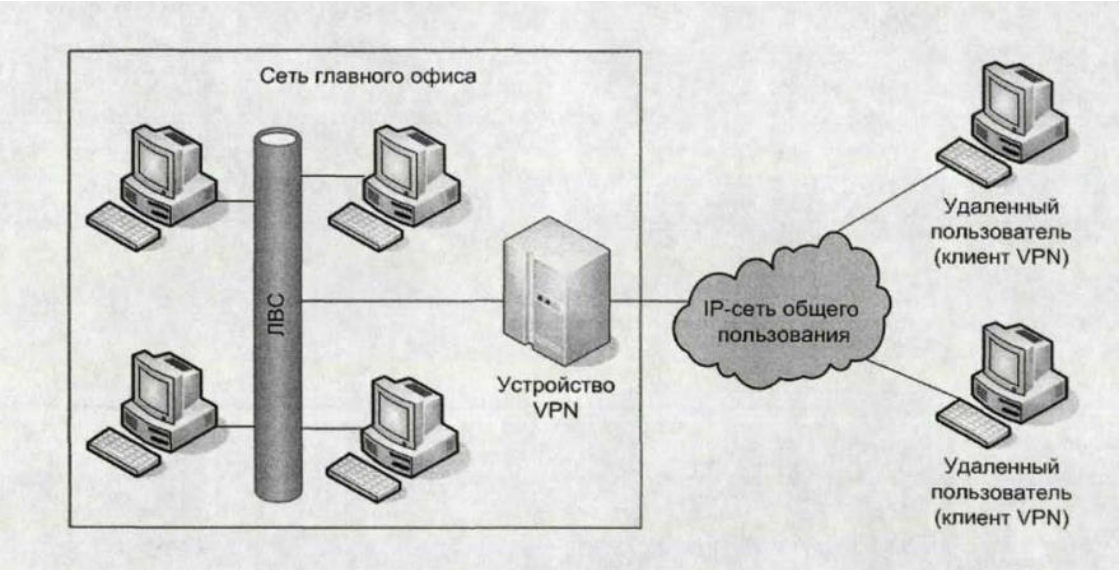

Рисунок 5 – Виртуальная частная сеть с удаленным доступом(Remote Access VPN)

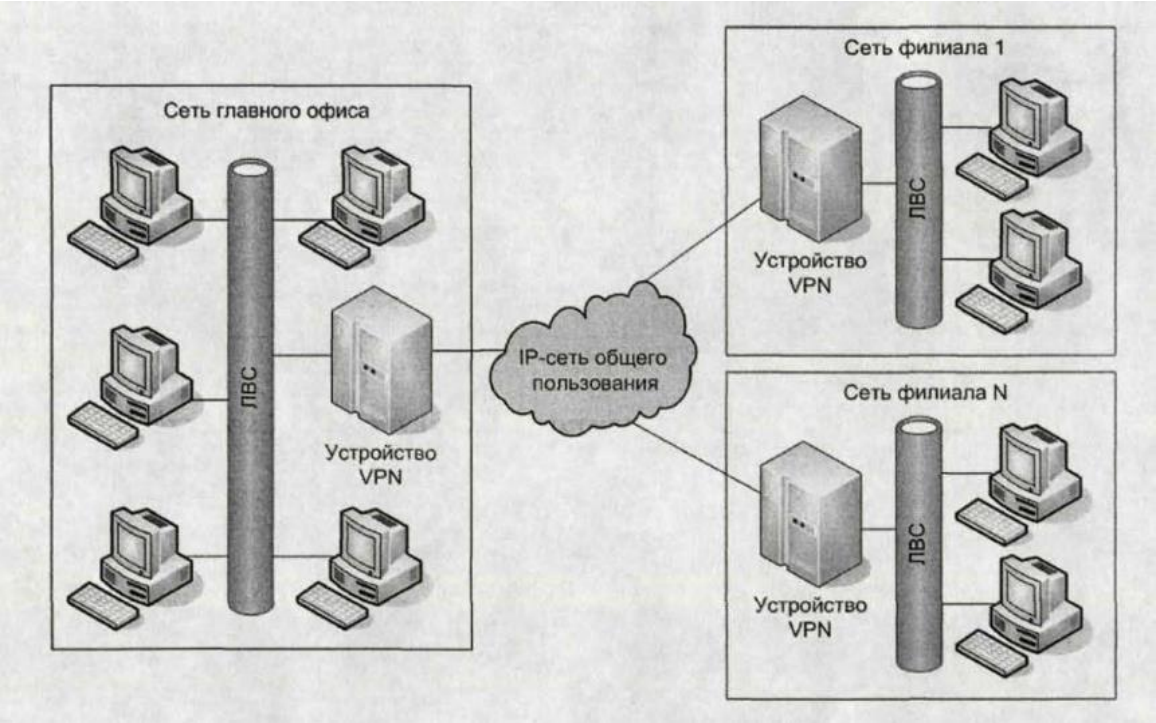

Рисунок 6 – Внутрикорпоративная сеть (Intranet VPN)

Эта технология использует методы IP-туннелирования, такие как GRE (Generic Router Encapsulation), L2TP (протокол туннелирования на Уровне 2) или IPSec (IP Security). Эти туннели устанавливаются между офисными маршрутизаторами для создания виртуальных частных соединений между офисами по принципу «от точки до точки». Для повышения уровня безопасности данные в виртуальном канале могут шифроваться.

3. Межкорпоративная сеть, экстранет (Extranet) VPN является услугой, которая обеспечивает прямой доступ из сети одной компании к сети другой компании и, таким образом, способствует повышению надежности связи, поддерживаемой в ходе делового сотрудничества.

Сети «экстранет VPN» в целом похожи на внутрикорпоративные виртуальные частные сети с той лишь разницей, что взаимодействуют через публичную IP-сеть разных компаний (рисунок 7). В этом случае проблема защиты информации является более острой. Когда несколько компаний принимают решение работать вместе и открывают друг для друга свои сети, они должны позаботиться о том, чтобы их новые партнеры имели доступ только к определенной информации. Таким образом, пользователь может иметь единый канал доступа, удовлетворяющий все его потребности в связи, как общедоступной, так и частной, включая голосовую. С помощью технологии «голос поверх IP» (VoIP) голосовые сообщения могут передавать между офисами по частным виртуальным сетям, а доступ к ТфОП может осуществляться через шлюзы, предоставляемые сервис-провайдером.

4. VPN «Клиент-сервер» (Client/Server VPN) обеспечивает защиту передаваемых данных между двумя удаленными узлами (не сетями) одной корпоративной сети (рис.8). Особенность данного варианта состоит в том, что VPN строится между узлами, находящимися, как правило, в одном сегменте сети, например между рабочей станцией и сервером. Такая необходимость очень часто возникает в тех случаях, когда необходимо создать в одной физической сети несколько логических сетей.

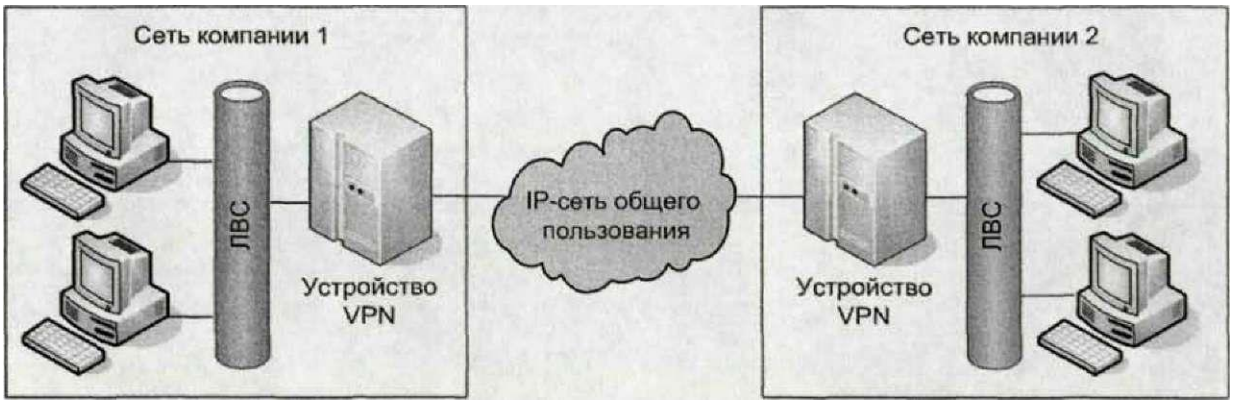

Рисунок 7 - Межкорпоративная сеть (Extranet VPN)

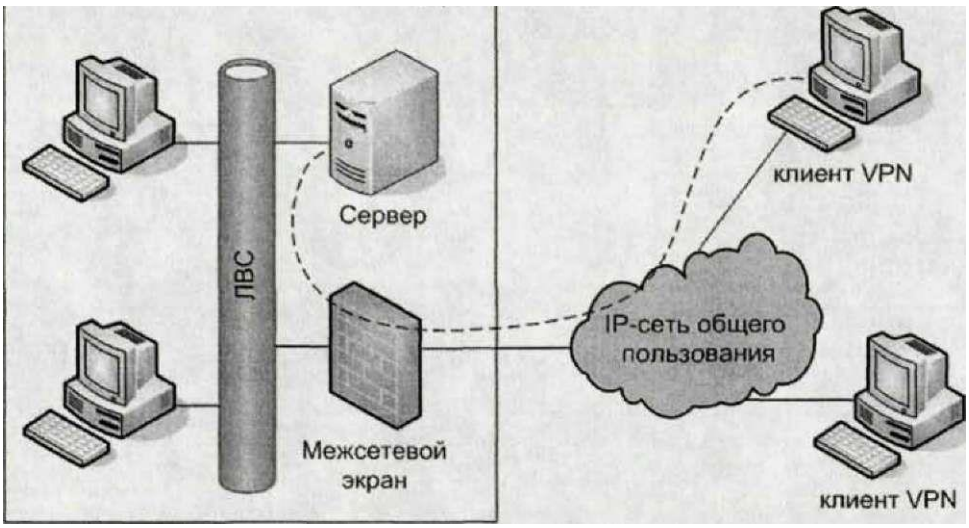

Рисунок 8 - VPN «Клиент-сервер» (Client/Server VPN)

По мнению многих специалистов, VPN входит в тройку важнейших технологий, которые предприятия собираются использовать в ближайшем будущем. Значимость этой технологии для любых предприятий, а тем более для бюджетных организаций, обусловлена прежде всего экономическим выгодами, которые связаны с ее внедрением. По оценке компании Infonetics Research, при

использовании VPN компания может сэкономить от 20 до 40% средств при связи «сеть-сеть» и от 60 до 80% — при подключении удаленных пользователей.

Анализ доходов зарубежных сервис-провайдеров и расходов корпоративных заказчиков, связанных с технологией VPN, показывает их значительный рост в последние годы [157].

В отчете компании Infonetics [95] отмечается широкое признание и распространение технологии MPLS среди сервис-провайдеров, которые рассматривают эту технологию в качестве основы для поддержки услуг VPN. Так, 83% респондентов планируют с помощью MPLS развернуть виртуальные частные сети.

2.3. Варианты технической реализации

Существует несколько вариантов технической реализации VPN. Основными критериями выбора того или иного решения являются производительность средств построения VPN и, конечно, их стоимость. Для создания виртуальной частной сети могут использоваться аппаратные, программные средства или их комбинация. Обычно аппаратные средства являются не только более производительными, но и более дорогостоящими.

Аппаратные методы шифрования обеспечивают более высокий уровень безопасности, чем программные, поскольку могут поддерживать ключи большей разрядности без увеличения задержки при передаче данных. Кроме того, аппаратные средства обеспечивают лучшую масштабируемость. Однако программные средства также имеют ряд преимуществ, главное из которых меньшая стоимость. Ниже дается анализ основных вариантов технической реализации VPN [27, 21, 90].

Многие существующие реализации YPN основаны на использовании межсетевых экранов (МЭ) (англоязычный термин Firewall — «брандмауэр», или «пожарная стена») с дополнительными функциями поддержки VPN, когда устанавливается шифрованное соединение через публичную IP-сеть (например, Интернет) с другим МЭ или клиёнтами VPN.

Межсетевые экраны реализуют механизмы контроля доступа из внешней сети к внутренней путем фильтрации всего входящего и исходящего трафика, пропуская только авторизованные данные. Большинство межсетевых экранов поддерживают туннелирование и шифрование данных. В этом случае к программному обеспечению собственно межсетевого экрана добавляется модуль шифрования.

Другим способом построения VPN является применение маршрутизаторов для создания защищенных каналов. Так как вся информация, исходящая из локальной сети, проходит через маршрутизатор, целесообразно возложить на этот маршрутизатор и задачи шифрования.

Данный метод построения виртуальной сети наиболее целесообразно использовать в организациях, имеющих разветвленную сеть филиалов. VPN на базе программного обеспечения

Следующим подходом к построению YPN являются полностью программные решения. При реализации такого подхода используется специализированное программное обеспечение, которое работает на выделенном компьютере и, в большинстве случаев, выполняет роль proxy- сервера. Компьютер с таким программным обеспечением может быть расположен за межсетевым экраном. VPN на базе сетевой ОС

Построение виртуальных частных сетей на базе операционной системы является достаточно удобным и относительно дешевым средством создания инфраструктуры защищенных каналов. Наибольшее распространение среди операционных систем, которые позволяют построить VPN штатными средствами самой операционной системы, получили Windows и UNIX.

К недостаткам в целом метода организации виртуальных частных сетей на базе операционной системы следует отнести недостаточную защищенность операционных систем с точки зрения обеспечения безопасности, особенно это актуально для продукции компании Microsoft. VPN на базе специализированных аппаратных средств

Вариант построения VPN на базе специальных устройств может быть использован в сетях, требующих высокой производительности по шифрованию трафика. Обычно в качестве специальных средств выступают VPN-шлюзы, реализованные в виде отдельных аппаратных устройств. Сравнение вариантов технической реализации VPN

2.4 Варианты расположения VPN-устройств в сети

При практической реализации VPN одной из главных задач является определение оптимального расположения VPN-устройств относительно других устройств защиты сети. Как правило, при построении VPN администратор сталкивается с тем, что для обеспечения безопасности корпоративной сети уже используется какое-либо защитное устройство (чаще всего это межсетевой экран или фильтрующий маршрутизатор, выполняющий эту функцию). В этом случае возникает задача размещения межсетевого экрана и VPN-шлюза. Совмещение функций межсетевого экрана и VPN-шлюза эту проблему снимает, но только частично. Во-первых, эта тенденция не абсолютна и имеет противников, а во-вторых, на сегодняшний день уже выпущено и продолжает выпускаться большое количество VPN-шлюзов без функций межсетевого экрана и межсетевых экранов без функций VPN-шлюзов.

При выборе варианта взаимного расположения VPN-шлюза и межсетевого экрана необходимо учитывать ряд факторов. Во-первых, межсетевой экран не может контролировать сетевой доступ на основании зашифрованных пакетов.

Во-вторых, VPN-шлюз сам требует защиты от угроз из сети общего пользования. В-третьих, конфигурация связей, образованная шлюзом и межсетевым экраном, может повлиять на надежность соединения корпоративной сети с IP-сетью общего пользования.

Ниже приведены варианты взаимного расположения VPN-шлюза и межсетевого экрана, которые наиболее часто используются на практике [90].
Размещение шлюза перед межсетевым экраном

При размещении шлюза перед межсетевым экраном через шлюз приходится передавать весь трафик: как открытый, так и зашифрованный. В этом случае межсетевой экран загружен обработкой всего трафика, причем фильтрация изначально зашифрованных данных выполняется после их дешифрирования шлюзом. Недостаток такой схемы — открытость шлюза для всех атак со стороны сети общего пользования.

Размещение шлюза позади межсетевого экрана

При размещении шлюза позади межсетевого экрана он защищается последним от атак. Однако при этом администратор корпоративной сети должен сконфигурировать межсетевой экран таким образом, чтобы он пропускал пакеты, несущие зашифрованный трафик.

Такая реализация привлекательна тем, что позволяет консолидировать администрирование и управление сетевыми компонентами. Однако в одном устройстве обычно трудно совмещать операции маршрутизации, защиты информации, управления доступом и регистрации событий. Поэтому в настоящее время гораздо эффективней выполнять функции VPN раздельно.
Раздельное подключение шлюза и межсетевого экрана

В этом случае и шлюз, и сетевой экран имеют собственную связь с IP-сетью общего пользования. При этом шлюз обрабатывает только зашифрованный трафик, который после расшифровки попадает в межсетевой экран и обрабатывается там в соответствии с существующей политикой безопасности предприятия. Таким образом, шлюз и межсетевой экран объединяют усилия по защите корпоративной сети, а надежность связи с сетью общего пользования повышается за счет существования двух независимых каналов (хотя отказ межсетевого экрана по-прежнему приведет к отказу связи с корпоративной сетью). Во многих отношениях этот вариант является предпочтительным .Подключение шлюза параллельно межсетевому экрану

Чаще всего производители VPN-продуктов предлагают использовать два соединения с сетью общего пользования — одно для межсетевого экрана, а другое для шлюза VPN . Эта архитектура потенциально более опасна по сравнению с предыдущими: во всех ранее рассмотренных схемах трафик всегда обрабатывается и межсетевым экраном, и VPN-шлюзом, либо последовательно, либо одновременно. В данном же случае корпоративную сеть отделяет от сети общего пользования только одно устройство — либо шлюз, либо межсетевой экран, которые обрабатывают трафик независимо, и их защитные функции не объединяются. Хотя надежность данной схемы довольно высокая, поскольку

корпоративная сеть связана с ГР-сетью общего пользования двумя независимыми каналами.

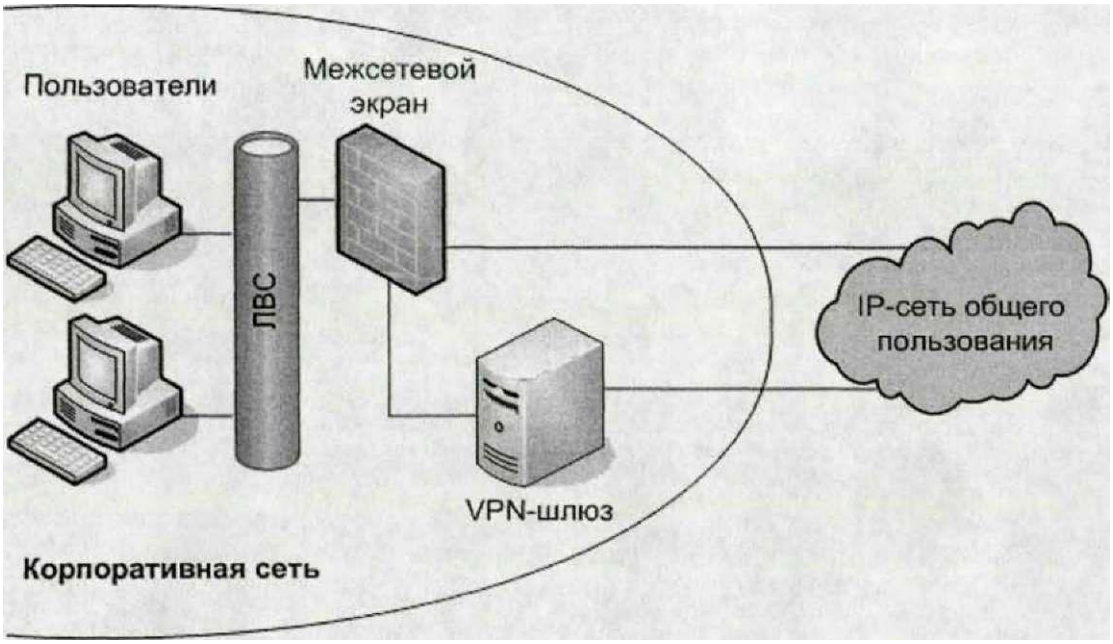

Рисунок 8 - Раздельное подключение шлюза и межсетевого экрана

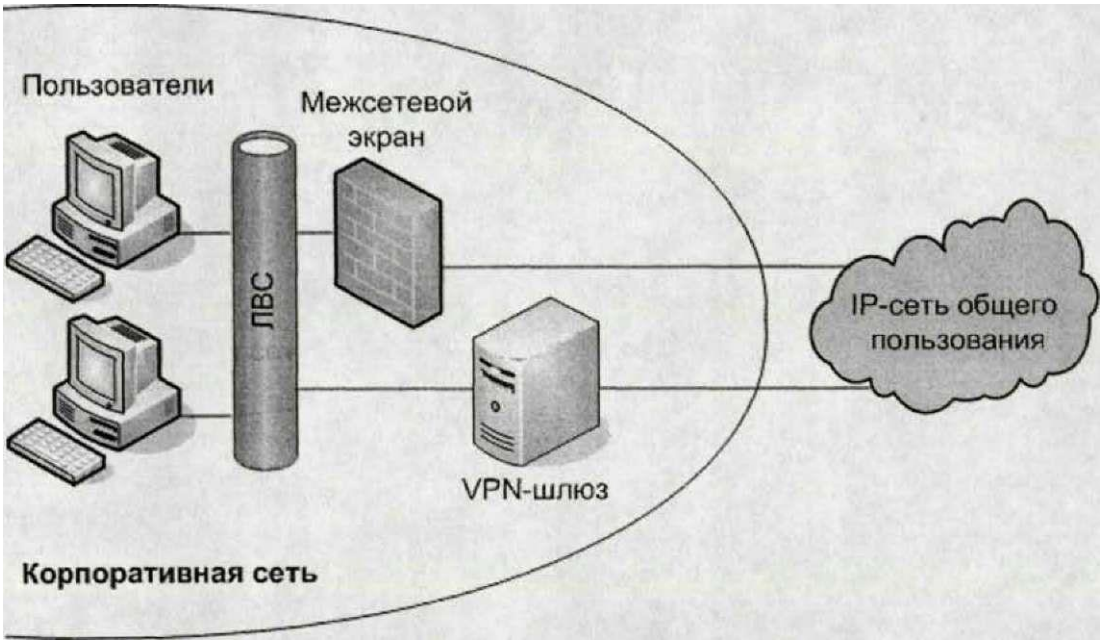

Рисунок 9 - Вариант размещения шлюза параллельно межсетевому экрану

2.5 Базовые технологии обеспечения качества услуг

Поддержка заданного качества обслуживания (QoS — Quality of Service) является одной из главных задач при внедрении виртуальных частных сетей. Однако решение данной задачи представляется весьма сложным, особенно если необходимо обеспечивать заданное качество обслуживания в Интернете. В глобальной сети работает множество провайдеров, которым трудно договориться между собой о координации совместных усилий для обеспечения сквозного качества обслуживания. Поэтому гарантированное качество обслуживания в сетях VPN может быть реализовано в пределах одного или нескольких провайдеров, между которыми существует определенная договоренность в данном направлении.

2.6 Обеспечение качества обслуживания на базе протокола RSVP

Одним из средств обеспечения качества в IP-сетях является использование протокола резервирования ресурсов (Resource Reservation Protocol, RSVP), рекомендованного комитетом IETF. С помощью протокола RSVP можно обеспечить в сети гарантированное качество обслуживания при передаче видео- и аудиосигналов. Протокол RSVP обеспечивает QoS за счет эмуляции выделенных каналов (резервирования требуемой полосы пропускания) в IP-сетях для каждого вызова [27, 93].

RSVP является протоколом сигнализации, который обеспечивает резервирование сетевых ресурсов и управление ими с целью предоставления интегрированных сервисов. Используя RSVP, отправитель периодически информирует получателя о требуемом объеме сетевых ресурсов .

Одна из интересных особенностей RSVP заключается в том, что запросы на резервирование ресурсов направляются только от получателей данных в сторону отправителей, а не наоборот. Такой подход обусловлен тем, что лишь устройство-получатель знает, с какой скоростью оно должно получать данные, чтобы надежно декодировать аудио- или видеосигналы. Другая уникальная особенность RSVP состоит в том, что резервирование проводится лишь для одного направления.

Недостатком протокола RSVP является то, что полоса пропускания, выделяемая источнику информации, при снижении активности источника не может быть использована для передачи другой информации. Поскольку для реализации QoS протокол RSVP требует резервирования ресурсов или каналов связи, небрежные или безответственные пользователи могут захватить ресурсы сети, инициируя несколько сеансов QoS подряд.

RSVP имеет весьма хорошие перспективы на корпоративном уровне, где администратор имеет возможность определить, какие параметры маршрутизатор будет использовать для обслуживания запросов о предоставлении QoS. В глобальных сетях маршрутизаторы вовсе не обязательно находятся под той же юрисдикцией, что и хосты, и приложения, производящие запросы, что осложняет гарантирование QoS.

Поддержка заданного качества обслуживания (QoS — Quality of Service) является одной из главных задач при внедрении виртуальных частных сетей. Однако решение данной задачи представляется весьма сложным, особенно если необходимо обеспечивать заданное качество обслуживания в Интернете. В глобальной сети работает множество провайдеров, которым трудно договориться между собой о координации совместных усилий для обеспечения сквозного качества обслуживания. Поэтому гарантированное качество обслуживания в сетях VPN может быть реализовано в пределах одного или нескольких провайдеров, между которыми существует определенная договоренность в данном направлении.

2.7 Обеспечение качества на базе технологии MPLS

Виртуальные частные сети на основе технологии коммутации по меткам MPLS (Multi Protocol Label Switching) получают все большее распространение. Количество отечественных провайдеров услуг, предлагающих своим клиентам воспользоваться данным видом сервиса для экономичного построения сетей интранет и экстранет, постоянно увеличивается. От других способов построения виртуальных частных сетей MPLS VPN выгодно отличает высокая масштабируемость, возможность автоматического конфигурирования и естественная интеграция с другими сервисами IP, которые сегодня поддерживаются любым провайдером: доступ к Интернету, Web и почтовые службы, хостинг [88, 160, 161].

Основные компоненты, участвующие в построении виртуальной частной сети на базе технологии MPLS, представлены на рис. 9.

В общем случае у каждого клиента может быть несколько территориально обособленных IP-сетей, каждая из которых может включать несколько подсетей, связанных маршрутизаторами. Такие территориально- изолированные «островки» корпоративной сети принято называть конечными точками VPN. Конечные точки, принадлежащие одному клиенту, обмениваются IP-пакетами через сеть провайдера и образуют виртуальную частную сеть этого клиента [96, 169, 170]. Для обмена маршрутной информацией в пределах конечной точки узлы пользуются внутренним протоколом маршрутизации (Interior Gateway Protocol, IGP), область действия которого ограничена автономной системой RIP, OSPF или IS-1

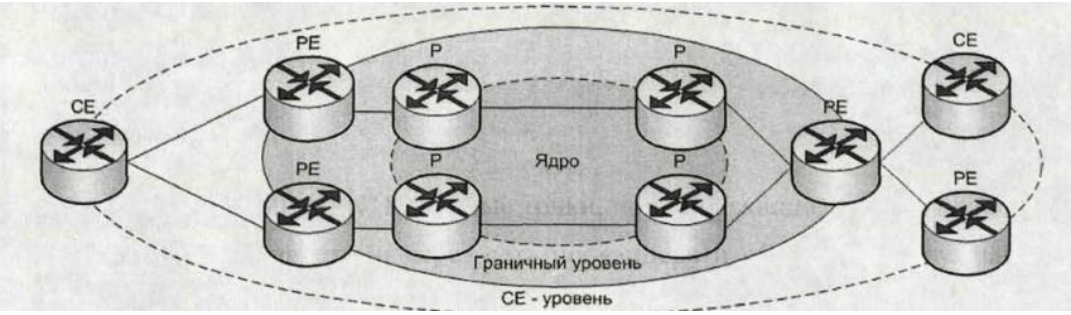

Рисунок 10 - Компоненты MPLS VPN

Маршрутизатор, с помощью которого клиент подключается к магистрали провайдера, называется пограничным маршрутизатором пользователя (Customer Edge router, CE). Будучи компонентом сети пользователя, CE ничего не «знает» о существовании VPN, Он может быть соединен с магистральной сетью провайдера несколькими каналами. Магистральная сеть провайдера является сетью MPLS, где пакеты IP продвигаются на основе не IP-адресов, а локальных меток. Эта метка содержит информацию о требуемом для каждого пакета уровне QoS.

Сеть MPLS состоит из маршрутизаторов с коммутацией по меткам (Label Switch Router, LSR), которые направляют трафик по предварительно проложенным путям с коммутацией по меткам (Label Switching Path, LSP) в соответствии со значениями меток. Устройство LSR — это своеобразный гибрид IP-маршрутизатора и коммутатора, при этом от IP-маршрутизатора берется способность определять топологию сети с помощью протоколов маршрутизации и выбирать рациональные пути следования трафика, а от коммутатора техника продвижения пакетов с использованием меток и локальных таблиц коммутации. Устройства LSR для краткости часто называют просто маршрутизаторами, так как они с таким же успехом способны маршрутизировать пакеты на основе IP-адреса, если поддержка MPLS отключена.

Маршрутизаторы PE являются функционально более сложными, чем маршрутизаторы провайдера. На них возлагаются главные задачи по поддержке VPN, а именно разграничение маршрутов и данных, поступающих от разных клиентов. Маршрутизаторы PE служат также оконечными точками путей LSP между конечными точками пользователей, и именно PE назначает метку пакету IP для его транзита через внутреннюю сеть маршрутизаторов P.

3 Математические модели анализа корпоративных виртуальных частных сетей

В этой главе приводятся результаты обзора и разработки математических моделей для оценки и расчета параметров системы резервирования серверов, характеристик передачи данных по каналам связи VPN-провайдеров.

Сформулированы основные принципы анализа структуры. Решены задачи описания структуры и вычисления характеристик структуры: интенсивностей потоков данных между узлами сети, нагрузка на узлы и структурообразующее оборудование сети.

3.1 Описание и расчет характеристик структуры корпоративной сети, построенной по технологии VPN

Приведенные перед этим результаты математического моделирования описывают структуру сети формально, без учета требований приложений и клиентов. Полученные результаты имеют достаточно узкую направленность, обеспечивая расчет характеристик отдельных элементов сети (двухточечные каналы связи, соединения, одиночные серверы) отсутствует возможность получения комплексных результатов для всей сети в целом. В связи с этим необходимы новые подходы к анализу сети. Одним из таких подходов является подход, основанный на том, что приложения, реализуемые в сети, определяют всю ее работу и поэтому анализ сети необходимо начинать с анализа взаимодействия приложений. Это во многом справедливо, поскольку именно приложения являются источниками и потребителями передаваемой в сети информации, формируя потоки данных в каналах связи. От размещения приложений по узлам сети и взаимодействия приложений зависят параметры потоков данных, загрузка каналов связи и сетевого оборудования. Из этого следует, что необходимо анализ работы приложений совмещать с анализом структуры сети.

Кроме того, особенность банковской системы состоит в том, что нужно обеспечить качество обслуживания клиентов банка, поэтому важно ориентировать сеть на решение конкретных прикладных задач.

Пусть число задач в системе обозначим L. Каждая задача состоит из нескольких приложений. Под приложением будем понимать программу, которая запускается пользователем при решении задачи, программа может быть как специальной, так и общесистемной, предназначенной для выполнения стандартных процедур, которые также требуются при решении задачи.

В каждой сети имеются хранилища данных (базы данных); их число в сети — R. Число узлов сети — M, количество пользователей сети — N. В системе функционирует D различных приложений.

Каждая задача k характеризуется следующим набором параметров: $S_k = \{p_k, d_k, \mathrm{u}_k\}$, (k= 1,2,...,L.)

(Здесь, в отличие от работы [74] не используется матрица, задающая последовательность запуска приложений при решении задач, поскольку эти данные не требуются в нашем случае.)

Вектор $p_{k1} = (p_{k1}, p_{k2}, ..., p_{kD})$ определяет приложения, которые исполняются при выполнении задачи k, при этом $p_{ki} = 1$, если приложение номер i выполняется при решении задачи *k.* и $p_{ki} = 0$, если приложение номер i не выполняется при решении задачи k (i= 1, 2,...,D; k = 1, 2,... **,**L). Векторы $p_{k1} = (p_{k1}, p_{k2}, ..., p_{kD})$ составляют матрицу $P = \|p_{ki}\|$, задающую связи между всеми задачами системы и всеми приложениями.

Вектор $d_{ki} = (d_{k1}, d_{k2}, ..., d_{kR})$ определяет базы данных, которые используются при выполнении задачи k, при этом $d_{ki} = 1$, если база данных номер i используется при решении задачи k, и $d_{ki} = 0$, если база данных номер I не используется при решении задачи k (i= 1, 2,..., R; k = 1, 2,... , L)**.**

Для всех элементов вектора d_k должно выполняться условие: $\sum_{i=1}^{R} d_{ki} \geq 0$ означающее, что при решении задачи номер k может не использоваться ни одной базы данных. Из векторов $d_{ki} = (d_{k1}, d_{k2}, ..., d_{kR})$ составляется матрица $D = \|d_{ki}\|$ задающая связи между задачами системы и базами данных.

Вектор $u_k = (u_{k1}, u_{k2}, ..., u_{kN})$ определяет множество пользователей системы, которым требуется запускать задачу ***k,*** при этом $u_{kj} = 1$, если пользователь j запускает задачу k, и $u_{kj} = 0$, если пользователь j не запускает задачу $k (j = 1, 2, ..., N; k = 1, 2, ..., L)$**.**

Векторы $u_k = (u_{k1}, u_{k2}, ..., u_{kN})$ составляют матрицу $U = \|u_{ki}\|$ определяющую потребности пользователей системы в запуске задачи.

Каждый i пользователь характеризуется интенсивностью потока запросов на запуск задач в системе — $\lambda_{ij} \geq 0 (j = 1, 2, ..., N; k = 1, 2, ..., L)$. Здесь λ_{ij} — интенсивность потока запросов от пользователя номер i на запуск задачи номер j. Множество интенсивностей потоков запросов от пользователей на запуск задач будем задавать матрицей $\Lambda = \|\lambda_{ij}\|$. Очевидно, что $\lambda_{ij} = 0$, если $u_{ij} = 0$ т.е. интенсивность потока запросов на запуск задачи номер j от пользователя номер i равна нулю, если этот пользователь не запускает данную задачу.

Приложение номер *т,* используемое при решении задачи номер *k* характеризуется набором: $A_{km} = \{v_{km}, b_{km}\}$, *(k* = 1,2,...,*L; т* = 1,2,...,D)
Здесь вектор $v_{km} = \{v_{km1}, v_{km2}, ..., v_{kmR}\}$ определяет объемы данных,
которыми обменивается приложение *т* с базами данных за один сеанс решения задачи *k,* так $v_{kmr} \geq 0$ — объем данных, которыми обменивается приложение т с базой данных r. Векторы $v_{km} = \{v_{km1}, v_{km2}, ..., v_{kmR}\}$ составляют матрицы $V_k = \|v_{kmr}\|$ *(m* = 1,2,...,D*; r* = 1,2,...,R)задающие объемы передаваемых данных между приложениями и базами данных.

Вектор $b_{km} = \{b_{km1}, b_{km2}, ..., b_{kmD})$ определяет объемы данных, которыми обменивается приложение номер r с другими приложениями при своей работе при решении задачи номер k, так $b_{kmj} \geq 0$ объем данных, которыми обменивается приложение m с приложением j. Векторы $b_{km} = \{b_{km1}, b_{km2}, ..., b_{kmD})$ составляют матрицы $B_k = \|b_{kmd}\|$, (m = 1,2,...,D; d-1,2,...,D)), задающие объемы передаваемых данных между приложениями при решении задач.

Интенсивности и объемы потоков данных в сети корпоративной системы определяются интенсивностями запуска задач пользователями и запускаемыми при этом приложениями. Здесь условимся, что объем передаваемых по сети данных задается в установленных единицах, например, байтах.

Размещение приложений по узлам сети задается матрицей

$$G = \|g_{ij}\| \qquad (3.2.1)$$

где $g_{ij} = 1$, если приложение i установлено на узле j и $g_{ij} = 0$, если приложение i не установлено на узле j (i = 1, 2,..., D;j=1, 2,..., M).

При формировании структуры сети производится также и распределение пользователей между узлами. Т.е. за каждым пользователем системы закрепляется узел сети, что соответствует закреплению за пользователем конкретной рабочей станции

Подключение пользователей к узлам задается матрицей:

$$H = \|h_{ij}\| \qquad (3.2.2)$$

где $h_{ij} = 1$ если пользователь i подключен к узлу j и $h_{ij} = 0$, если пользователь j не подключен к узлу i (i= 1,2,..., N;j= 1,2,.., M).

Распределение баз данных по узлам сети задается матрицей $S = \|s_{rm}\|$, где $s_{rm} = 1$, если база данных номер r размещена на узле т, и $s_{rm} = 0$, если база данных номер r не размещена в узле сети т, (r = 1,2,..., R; т = 1, 2,..., M).

Распределенную базу данных будем рассматривать, в соответствии с 3.1.3, как совокупность отдельных баз данных, но в данном случае каждую базу данных удобно рассматривать как приложение.

Далее в качестве примера, приведено описание информационной структуры для случая решения трех задач (задача 1,задача 2 и задача 3).

Считаем, что число пользователей системы N = 4, число узлов M = 7, число приложений D= 5, число баз данных R = 2. При этом одна база номер 2 используется двумя задачами.

Пользователь 3 задачи не запускает.

Задача 1: $S_1 = \{p_1, d_1, u_1\}$ где, p_1 = (1,1,0,0,0), d_1 = (0,1) , u_1 = (1,0,0,0),

Задача 2: $S_2 = \{p_2, d_2, u_2\}$, где p_2 = (0,0,0,1,1), d_2 = (1,1), u_2 =(0,0,0,1),

Задача 3: $S_3 = \{p_3, d_3, u_3\}$, где p_3 =(0,0,1,0,0), d_3 =(1,0), u_3 =(0,1,0,0),

На рисунке 3.2.1 приведена информационная структура системы, соответствующей заданному описанию.

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}, G = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$S = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, P = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}, U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}, D = \begin{pmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

3.2 Расчет параметров потоков данных

Используя введенные средства описания (определения, задания) информационной структуры сети в виде набора данных, можно определить параметры потоков данных между узлами сети.

Значения элементов матрицы Λ определяются спецификой работы пользователей корпоративной системы, и будем считать их известными.

Очевидно, что потоки запросов пользователей сначала поступают на те узлы сети, к которым прикреплены пользователи. Закрепление пользователей за узлами задается матрицей H, определенной ранее.

Интенсивность потока запросов на запуск задачи определяет и интенсивности запуска приложений, которые используются этой задачей.

Суммарная интенсивность потока запросов на запуск задачи *k:*

$$\lambda_k = \sum_{i=1}^{N} \lambda_{ik} \text{ , } (k=1,2,\ldots,L) \qquad (3.2.3)$$

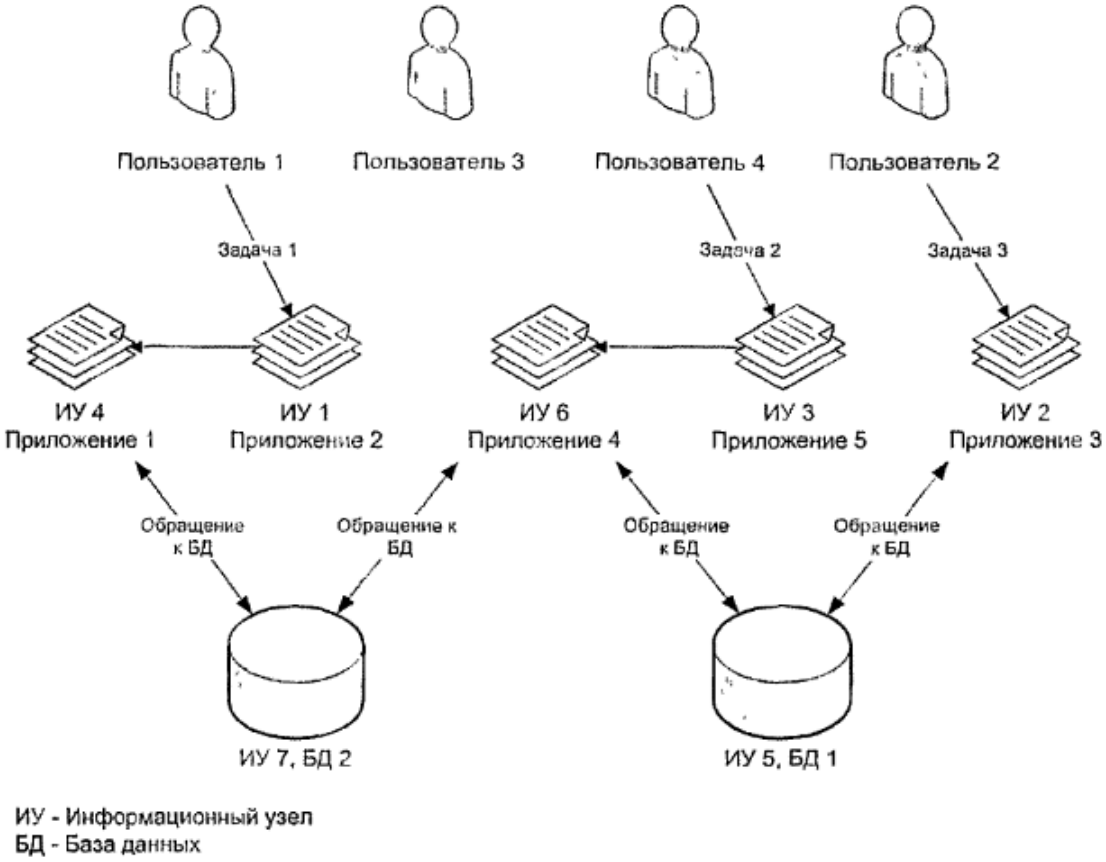

Рисунок 11 – Информационная структура системы

Вектор интенсивностей запуска задач в системе — $\lambda = (\lambda_1, \lambda_2, ..., \lambda_L)$ вычисляется по формуле: $\lambda = \mathrm{e}_N \Lambda$, где e_N единичный вектор размерности *N*.

Вектор γ определяет интенсивности запуска приложений в системе (в корпоративной сети системы) $\gamma = (\gamma_1, \gamma_2, ..., \gamma_D) : \gamma = \lambda P$,

$$\gamma_j = \sum_{k=1}^{L} \lambda_k p_{kj} \ , \qquad (3.2.4)$$

что означает суммарную интенсивность запуска приложения номер у всеми задачами, решаемыми системой.

$\mathrm{Z}_k = \left\| z_{kij} \right\|$ матрица, где элемент z_{kij} равен суммарному объему данных, передаваемому между узлами сети i и j при решении задачи *k*. Тогда:

$$z_{kij} = \sum_{r}^{D} g_{ri} p_{kr} (\sum_{m=1}^{D} g_{mj} p_{km} b_{rm}) + \left[\sum_{r}^{D} g_{ri} p_{kr} (\sum_{m=1}^{R} s_{mj} d_{km} v_{rm}) \right]$$

(k = 1,2,…,L, i = 1,2,..., M; j = 1,2,.,M)

Матрица интенсивностей потоков данных между узлами, сети при решении задачи k вычисляются по формуле: $A_k = \lambda_k Z_k, (k = 1, 2, ..., L)$ $\mathrm{A}_k = \left\| \alpha_{kij} \right\|$, где

$\alpha_{kij} = \lambda_k z_{kij}$, $(i = 1,2,...,\mathrm{M};\ \mathrm{j} = 1,2,....\mathrm{M})$. α_{kij} — суммарная интенсивность потоков данных между узлами i и j при решении задачи k.

Формула для вычисления интенсивности потока запросов на запуск приложения y, установленного на узле i: $\beta_{ji} = \gamma_j g_{ji}$. (j=1,2,..., D; i= 1,2,..., M.). В матричной форме: $B^* = \|\beta_{ij}\| = \Gamma_{dg} G$, где $\Gamma_{dg} = \|\gamma_{ij}^*\|$-диагональное матрица ,у которой $\gamma_{ij}^* = \gamma_i$ и $\gamma_{ij}^* = 0$, если $i \neq j$,(j=1,2,…,D;i=1,2,…,D),матрица G определяется в (3.2.1)

Если нужно вычислить интенсивность потока запросов на запуск приложения номер у на узле / только от задачи к, то можно воспользоваться формулой: $\beta_{kji} = \lambda_k g_{ji} p_{kj}.(k = 1,2,...,L;\ j = 1,2,...,D;\ i = 1,2,...,M)$

Если на узле i установлена база данных (хранилище данных), то можно определить интенсивность потока запросов от приложений к базе данных у при решении задачи k: $\varphi_{kij} = \lambda_k s_{ji} d_{kj}, (k = 1,2,...,L;\ j = 1,2,...,\mathrm{R};\ \mathrm{i} = 1,2,...,\mathrm{M}.)$

Формула для вычисления суммарной интенсивности потока запросов к базе данных номер у, установленной на узле номер / при решении всех задач:

$$\varphi_{ji} = \sum_{k=1}^{L} \lambda_k s_{ji} d_{kj} = \sum_{k=1}^{L} \varphi_{kji}, (\ j = 1,2,...,\mathrm{R};\ \mathrm{i} = 1,2,...,\mathrm{M}.)$$

Здесь, если $\varphi_{ji} = 0$, то на узле i не установлена база данных номер j.Величины φ_{ji}, составляют матрицу $\Phi = \|\varphi_{ji}\|$

При проведении расчетов предусмотрены случаи, когда на одном узле установлено несколько приложений или несколько баз данных. Тогда суммарная интенсивность потока запросов на запуск приложений, установленных на узле i вычисляется по формуле: $\beta_i = \sum_{j=1}^{D} \beta_{ji}$, а суммарная интенсивность потока запросов к базам данных, установленным на узле i, вычисляется по формуле: $\varphi_i = \sum_{j=1}^{R} \varphi_{ji}$.

Для приведенного в предыдущем разделе примера информационной структуры (рисунок 12) проведем расчеты параметров потоков данных. Пусть матрица интенсивностей запросов пользователей на запуск задач имеет вид: $\Lambda = \begin{bmatrix} 10 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 20 \\ 0 & 5 & 0 \end{bmatrix}$.Здесь единицей считаем один час . Имеем :

$\lambda = (10,5.20).\gamma = \lambda P = (10,10,5,20,20)$.

$$Z_1 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 10 & 0 & 0 & 0 & 0 & 0 & 100 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad Z_3 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 50 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$A_1 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 100 & 0 & 0 & 0 & 0 & 0 & 1000 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad A_2 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 50 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 50 & 0 & 500 & 0 & 150 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$A = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 200 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 50 & 0 \\ 100 & 0 & 0 & 0 & 0 & 0 & 1000 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 50 & 0 & 500 & 0 & 150 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad A_3 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 200 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$B^* = \begin{bmatrix} 0 & 0 & 0 & 10 & 0 & 0 & 0 \\ 10 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 20 & 0 \\ 0 & 0 & 20 & 0 & 0 & 0 & 0 \end{bmatrix} \quad Z_2 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 10 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 10 & 0 & 100 & 0 & 30 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\Phi = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

3.3 Расчет параметров потоков данных для сетей на основе технологии VPN

Применение технологии VPN при создании корпоративных сетей, как отмечалось выше, требует привлечения провайдеров, для подключения к общедоступной или ведомственной среде передачи данных. Поскольку услуги провайдеров требуют оплаты, размеры которой зависят от передаваемого трафика и условий предоставления услуг связи (например, QoS), то необходимо иметь возможность вычислять параметры потоков данных, передаваемых по каналам провайдеров [74, 93, 106].
В связи с этим возникает потребность в разработке методов и моделей для расчета параметров потоков данных в корпоративных сетях с заданной структурой.

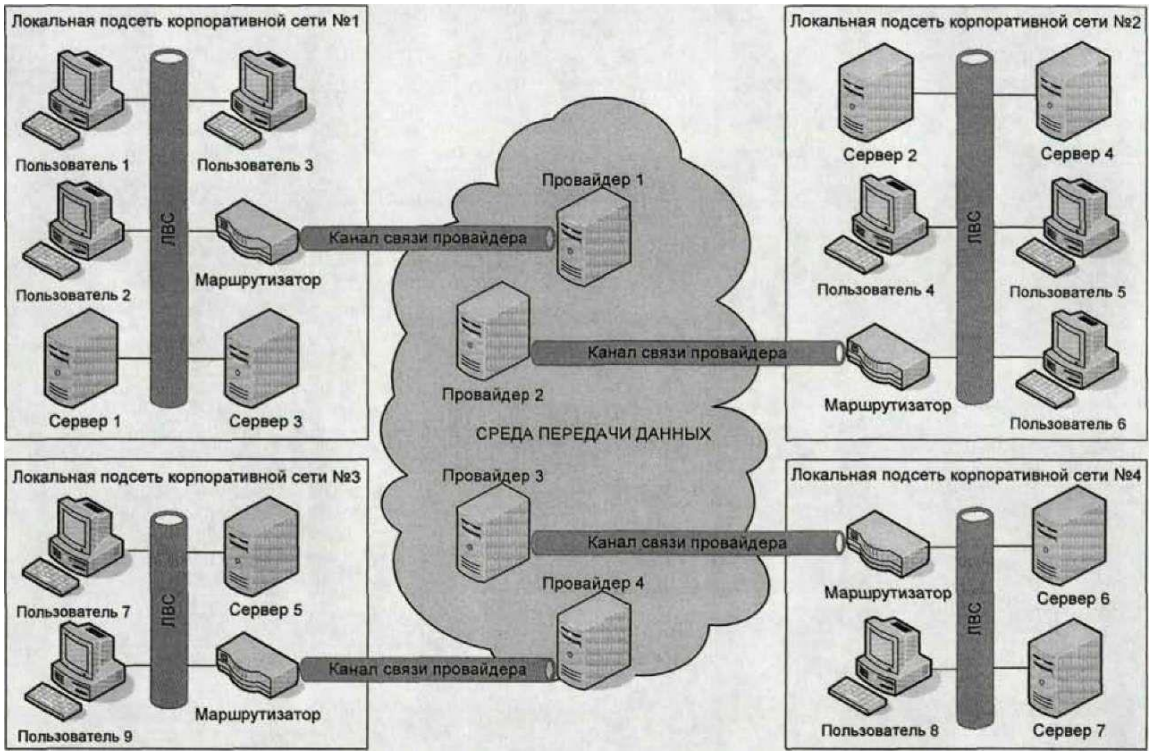

Рисунок 12 - Структура корпоративной VPN сети

Как видно из рисунка 12 корпоративная сеть состоит из локальных подсетей, объединенных через каналы связи провайдеров, обеспечивающих доступ к внешней среде передачи данных.

Пусть распределение узлов корпоративной сети между локальными подсетями задается матрицей : $Y = \|y_{ij}\|, (i = 1,2,...,M;\ j = 1,2,...,\mathrm{KV})$ где

$y_{ij} = 1$, если узел i корпоративной сети, входит в состав локальной подсети

корпоративной сети; $y_{ij} = 0$, если узел i корпоративной сети, не входит в состав локальной подсети j корпоративной сети; KV — число локальных подсетей корпоративной сети, связанных между собой через внешнюю среду передачи данных.

Используя приведенные выше результаты, в [74] получена формула для вычисления матрицы: $V = \|v_{mn}\|, (m = 1,2,...,KV; n = 1,2,...,KV)$, где v_{mn} — суммарная интенсивность потоков данных передаваемых от подсети номер *т* к подсети *n;* v_{kmn} — суммарная интенсивность потоков данных внутри подсети *т.* Матрица V вычисляется по формуле:

$$\mathrm{V} = (\mathrm{Y})^T A(Y) \qquad (3.2.8)$$

По аналогии с полученными выше результатами вычисляются матрицы $V_k = \|v_{kmn}\| = (\mathrm{Y})^T A_k(Y)$, *(к* = 1,2,..,*L; т = 1,2,…, KV; n* = 1,2,..., *KV*), где v_{kmn} — суммарная интенсивность потоков данных задачи *к,* передаваемых от подсети *т* к подсети *n;* v_{kmn} — суммарная интенсивность потоков данных задачи *к* внутри подсети *т.*

Суммарная интенсивность потока данных, передаваемого по каналу связи провайдера, обслуживающего локальную подсеть *т:*

$$\gamma_m = \sum_{\substack{j=1 \\ j \neq m}}^{KV} v_{jm} + v_{mj}, (m = 1,2,...,KV) \qquad (3.2.9)$$

Суммарная интенсивность потока данных задачи *к,* передаваемого по каналу связи провайдера, обслуживающего локальную подсеть т:

$$\gamma_{km} = \sum_{\substack{j=1 \\ j \neq m}}^{KV} v_{kjm} + v_{kmj}, (m = 1,2,...,KV) \qquad (3.2.10)$$

Здесь необходимость выделения потоков данных различных задач обусловлена тем, что для различных задач могут потребоваться различные параметры каналов связи, например, при заключении договоров о качестве обслуживания (QoS).

Таким образом, имеются все необходимые формулы для вычисления нагрузки на каналы связи провайдеров.

4 Экспериментальная часть

Виртуальные корпоративные сети (VPN) обеспечивают безопасную и надежную связь между узлами заказчика. С увеличением количества и размера виртуальных частных сетей поставщикам необходимо использовать эффективные методы построения сети VPN [1].

Глобальная VPN дает возможность подключения в любой точке мира. Архитектура VPN поддерживает надежный механизм аутентификации для обеспечения легкого доступа к внутренней сети из любого места с помощью любых доступных средств массовой информации, включая аналоговые модемы, ISDN, кабельные модемы, DSL и беспроводную [2].

Корпоративные сети используют технологию MPLS для соединения географически удаленных мест. Принцип прямого подключения этой технологии заключается в использовании таблиц маршрутизации провайдера [3].

На настоящий момент действующая сеть не отвечает требованиям корпоративной сети по следующим причинам : по истечении времени штат компании увеличивается и , возникает потребность в увеличении количества номеров телефонов, так как новые сотрудники потребуют установки новых номеров телефонов. Производственный процесс также потребует подключения дополнительных номеров. В связи с этим руководителям приходится расширять и модернизировать существующую сеть [4].

В работе исследуется трафик корпоративной сети для построения виртуальной корпоративной сети связи.

На рисунке 13 показана схема существующей корпоративной сети.

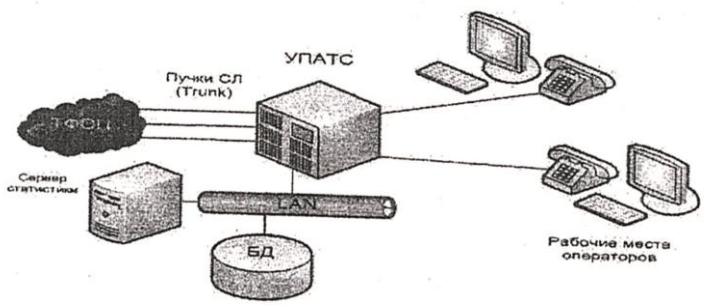

Рисунок 13- Схема действующей корпоративной сети [5]

Была разработана имитационная модель расширения данной сети с помощью программы NetCracker и сняты зависимости изменения трафика при передаче информации по различным маршрутам в виртуальной сети. Результаты экспериментов представлены в таблицах 1,2,3.

На рисунке 13 показана схема разработанной имитационной модели расширенной корпоративной сети на основе пакета программы NetCracker.

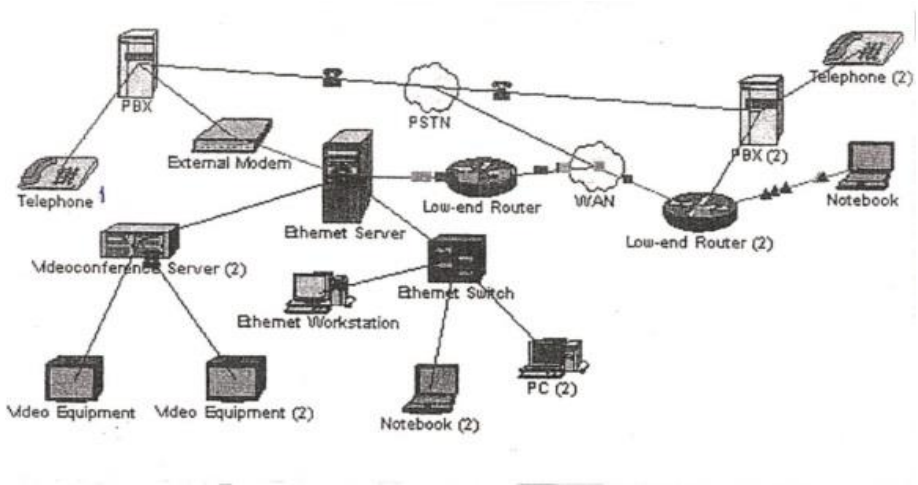

Рисунок 14 - Схема спроектированной имитационной модели расширенной корпоративной сети на базе пакета программы NetCracker.

В таблице 1 представлено прохождение трафика от телефона 1 до телефона 2

Т а б л и ц а 1- Прохождение трафика от телефона 1 до телефона 2

Номер эксперимента (№)	Знач. траф. (бит)	Знач. траф. (бит)	Знач. траф. (бит)	Знач. траф. (бит)	Знач. траф. (бит)	Знач. траф. (бит)	Знач. траф. (бит)	Знач. траф. (бит)	Знач. траф. (бит)	Знач. Траф. (бит)
1	990,7	990,5	990,4	980	970,8	970,4	970,4	970,2	970,2	970,1
2	988,8	988,4	991,7	977,7	968,6	968,5	968,3	967,8	967,8	967,4
3	991,3	990,9	990,8	981,7	971,9	971,7	970,9	970,8	969,9	969,8
Мат.ожид траф.	990,27	989,93	990,97	979,80	970,43	970,20	969,87	969,60	969,30	969,10
Средне-квадрат. отклон.	0,57	0,60	0,15	1,34	0,94	0,86	0,63	0,84	0,57	0,73

Из таблицы 1 видно, что величина телефонного трафика уменьшилось всего на примерно на 2 процента за счет затухания при прохождении двух PBX.

На рисунке 15 приведен график зависимости распределения величины математического ожидания трафика и доверительный интервал, в результате имитации его прохождения от телефона 1 до телефона 2.

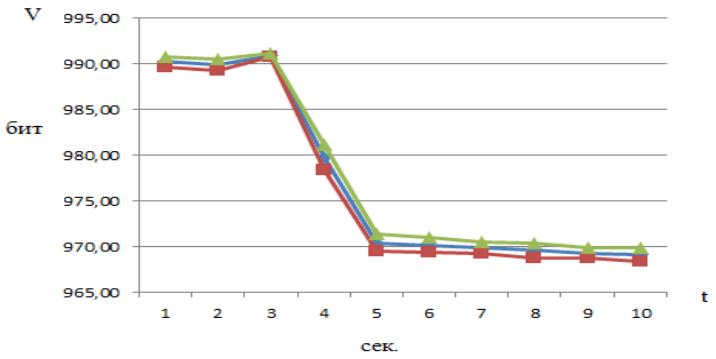

Рисунок 15 – Зависимость математического ожидания трафика от времени моделирования и доверительный интервал при прохождении сигнала от телефона 1 до телефона 2 через две РВХ

Из рисунка 3 видно, что математическое ожидание трафика падает примерно на 2 процента.

В таблице 2 представлено прохождение трафика от удаленного абонента (ноутбук) до маршрутизатора 2.

Т а б л и ц а 2 - Прохождении трафика от удаленного абонента (ноутбук) до маршрутизатора 2

Номер эксперимента (№)	Знач. траф. (бит)	Знач. траф. (бит)	Знач. трф. (бит)	Знач. траф. (бит)	Знач. траф. (бит)	Знач. траф. (бит)	Знач. траф. (бит)	Знач. траф. (бит)	Знач. траф. (бит)	Знач. траф. (бит)
1	996,4	994,5	994,3	990,2	895,6	894,5	894,6	893,8	893,7	893,7
2	992,3	990,5	988,4	987,3	889,5	889,5	888,4	888,3	888,3	888,1
3	998,2	998,3	995,3	992,2	895,5	895,3	894,6	894,5	893,9	893,8
Мат. ожид.	995,63	994,43	992,67	989,90	893,53	893,10	892,53	892,20	891,97	891,87
Средне-квад. откл.	3,05	5,07	4,63	2,02	4,07	3,29	4,27	3,84	3,36	3,55

Из таблицы 2 видно, что величина трафика падает примерно на 9-10 процентов за счет прохождения маршрутизатора 1.

На рисунке 16 приведен график зависимости распределения величины математического ожидания трафика и доверительный интервал, в результате имитации его прохождения пути от удаленного абонента (ноутбука) до маршрутизатора 2.

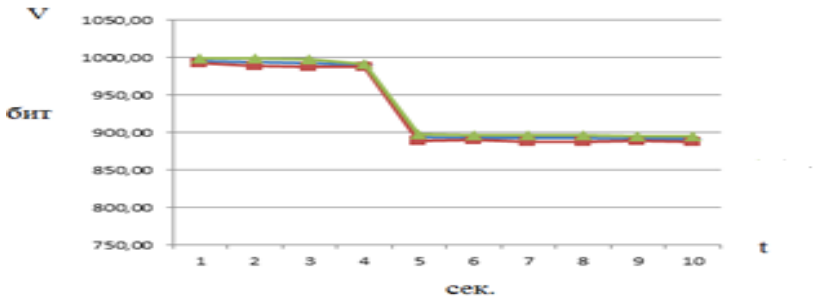

Рисунок 16 – Зависимость математического ожидания трафика от времени моделирования и доверительный интервал при прохождении пути от удаленного абонента (ноутбука) до маршрутизатора 2.

Из рисунка 16 видно, что при прохождении трассы по передаче данных от удаленного абонента до маршрутизатора 2,величина математического ожидания трафика падает примерно на 9-10 процентов за счет прохождения маршрутизатора 1.

В таблице 3 представлено прохождение трафика после WAN перед ноутбуком после Ethernet Switch.

Т а б л и ц а 3 - Прохождение трафика после WAN перед ноутбуком после Ethernet Switch

Номер эксперимента (№)	Знач. трафика (бит)	Знач. трафика (бит)	Знач. трафика (бит)	Знач. трафика (бит)	Знач. трафика (бит)	Знач. трафика (бит)	Знач. трафика (бит)	Знач. трафика (бит)	Знач. трафика (бит)	Знач. трафика (бит)
1	998,3	998,2	997,8	997,4	750,7	690,7	553,9	553,5	551,9	550,6
2	995,3	994,5	993,9	992,3	753,4	691,4	553,7	552,1	551,5	550,9
3	999,2	998,3	998,3	998,2	752,8	687,9	554,8	556,9	553,8	550,5
Мат. ожид.	997,6	997	996,67	995,97	752,3	690	554,13	554,17	552,4	550,67
Среднеквад рат. откл.	1,4	1,6	1,9	3,4	0,7	1,1	0,1	2,0	0,5	0,0

Из таблицы 3 видно, что величина трафика падает примерно на 45%.

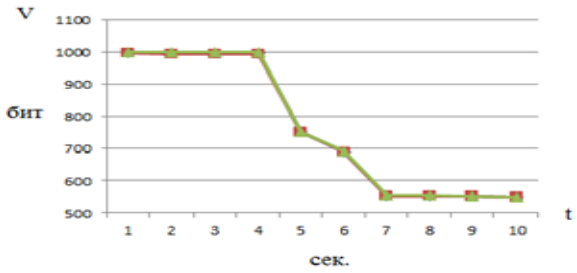

Рисунок 17 – Зависимость математического ожидания трафика от времени моделирования при прохождении пути после WAN и перед ноутбуком после Ethernet Switch.

Из рисунка 17 видно, что основное уменьшение трафика происходит при прохождении трассы через второй маршрутизатор слева от удаленного абонента(ноутбук) через WAN в сторону ЛВС.

Заключение

По результатам проведенных исследований и практического применения разработанных моделей в реальной системе можно сделать следующие выводы:

1. Проведенный анализ специфики работы банковских информационных систем и сетей, предназначенных для их обслуживания, показал, что для построения корпоративной банковской сети целесообразно применять технологию виртуальных частных сетей (VPN), которая позволяет обеспечить выполнение основных требований по безопасности и качеству обслуживания клиентов и приложений.

2. Анализ современного состояния и направлении развития VPN-технологии позволил сделать вывод о перспективности ее применения при создании банковских сетей нового поколения, при этом выделены основные задачи, требующие решения при создании сети.

3. Разработан комплекс математических моделей для решения задачи обеспечения бесперебойной работы банковской системы (сети), позволяющий определить оптимальные или допустимые параметры резервирования и управления потоками данных на серверы, обеспечивающие оптимальный либо заданный уровень затрат.

4. Разработан комплекс математических моделей, позволяющих определить допустимые параметры качества обслуживания потоков данных в каналах провайдеров с учетом параметров «бокового» трафика, свойственного публичным сетям передачи данных. Модели дают возможность выбирать провайдеров связи и обосновывать размер платы за их услуги.

В результате проведенных исследований созданы основы методики анализа внутренней сетевой среды и публичной сети, используемых при создании корпоративной банковской сети, позволяющие получать количественные оценки характеристик сети и определить пути повышения эффективности использования технологий VPN, что способствует увеличению общей конкурентоспособности всего предприятия.

Полученные в работе результаты могут быть использованы на этапах создания (проектирования), модернизации и текущего администрирования корпоративной банковской сети, построенной с применением технологии VPN.

Список литературы

1. Абиссов Ю.А., Трекущенко П.И. Повышение эффективности скорости передачи данных в сетях с коммутацией сообщений // Техника средств связи, сер. ТПС. 1982. Вып.2(5). — С. 35-41.
2. Абрамов А.В. Новое в финансовой индустрии: информатизация банковских технологий. — СПБ: Питер, 1997.
3. Абуталиев Ф.Б., Саидахмедов Ш.Х. Аналитическая модель тракта передачи данных для сети коммутации пакетов. — В кн.: Вычислительные сети коммутации пакетов: Тез.докл. Всес. конф. — Рига: Зпнатне, 1979, с. 162-166.
4. Абуталиев Ф.Б., Саидахмедов Ш.Х. Об одном аналитическом методе оценки коммутации пакетов в сетях // Изв. УзССР, сер. техн. наук. 1978. №5. — С. 8-11.
5. Аветов Ю.В., Головин Ю.А. Формализация и оценка эффективности протокола Х.25/2. — Методические материалы и документация по пакетам прикладных программ, 1983, вып.24. Рекомендация МККТТ Х.25 и ее применение в информационно-вычислительных сетях. 4.1. Опыт применения рекомендации Х.25, с. 146-159.
6. Автоматизированные банковские системы. / Демин В.С. и др.— М.: Менатеп—Информ, 1997. — 260с.
7. Англицкин И.К. Состояние и перспективы информационного обеспечения российских банков. // Финансы и кредит. — 2006. — №8 (176) — С. 20-23.
8. Аджиев В.В. Мифы о безопасности программного обеспечения: уроки знаменитых катастроф. // Открытые системы. ■—- М.:, 1998. №6. — С. 13-15.
9. Аллен Д. Следующая волна VPN на базе IP // LAN. 2001. № 3. — С. 86-95.
10. Байбулатов Р.Б., Бедова Л.Ю., Иванушкина Л.И. Оценка времени передачи сообщения методом дейтаграмм в вычислительной сети // Проблемы МСНТИУМЦНТИ. 1991. № 2. — С. 68-70.
11. Барабанов С., Коростелин А., Крюков С. Компьютерные сети: вчера, сегодня, завтра// КомпьютерПресс. 1997. № 2. — С. 152-162
12. Барабанов С, Коростелин А., Крюков С. Компьютерные сети: вчера, сегодня, завтра//КомпьютерПресс. 1997. № 3. — С. 158-162.
13. Башарин Г.П., Богуславский Л.Б., Самуилов К.Е. О методах расчета пропускной способности сетей связи ЭВМ // Итоги науки и техники, сер. Электросвязь. 1993, Т. 13. — С. 32-106.
14. Башарин Г.П., Бочаров П.П., Коган Я.А. Анализ очередей в вычислительных сетях. Теория и методы расчета. — М.: Наука. Гл. ред. физ.— мат. лит., 1992. - 336 с.
15. Башарин Т.П., Кокотушкин В.А., Наумов В.А. О методе эквивалентных замен расчета фрагментов сетей связи для ЦВМ // Изв.АН СССР. Техническая кибернетика. 1989. № 6. — С. 92-99.

16. Башарин Г.П., Куренков Б.Е. Исследование одной системы массового обслуживания с дискретным временем // Изв.АН СССР. Техническая кибернетика. ■— 1993. — № 6. — С. 26-30.

17. Беллман Р., Дрейфус С. Прикладные задачи динамического программирования. — М.: Наука, 1965.

18. Белов В.В., Пылькин А.Н. Оценка эффективности протоколов управления информационным каналом при зависимых искажениях пакетов. — В кн.: Вычислительные сети коммутации пакетов: Тез.докл. 3 Всес.конф. — Рига: Институт электроники и вычислительной техники АН Латв.ССР, 1983, т. 1,с. 16-18.

19. Белов С. Практика построения ведомственных сетей frame relay в России // Сети. 1997. № 5. — С. 48-52.

20. Бертсекас Д., Галлагер Р. Сети передачи данных. — М.: Мир, 1989. —544 с.

21. Бирюков В.В., Ващилин Э.П., Полянский С.Н. Оценка эффективности процедуры HDLC. — В кн.: Вычислительные сети коммутации пакетов: Тез.докл. 3 Всес.конф. — Рига: Институт Электроники и вычислительной техники АН Латв.ССР, 1983, т.. 1, с. 81-85.

22. Бирюков В.В., Ващилин Э.П. Динамическая адаптация параметров процедуры управления звеном передачи данных. — В кн.: Информационно-вычислительные сети ЭВМ: Материалы семинара. - М.: Моск. дом науч.-— техн. пропаганды, 1980. с. 136-142.

23. Богуславский Л.Б. Управление потоками данных в сетях ЭВМ. — М.: Энергоатомиздат, 1984.- 168с.

24. Богуславский Л.Б., Геленбе Е. Аналитические модели процедур управления звеном передачи данных сетей ЭВМ с коммутацией пакетов // Автоматика и телемеханика. — 1990. — № 7. — С. 181-192.

25. Богуславский Л.Б., Кучеров В.П., Столяр А.Л. Сравнительный анализ протоколов HDLC и DDCMP. — В кн.: X Всес. шк.—сем. по вычислительным сетям: Тез.докл. — М. — Тбилиси, 1985, ч.3, с. 123-128.

26. Боровихин Е.А., Коротаев И.А. Анализ функционирования и оптимизация протокола HDLC // Автоматика и вычислительная техника. — 1993.—№2.—С .47-51.

27. Браун С. Виртуальные частные сети. — М.: Лори, 2001. — 508 с.

28. Брандмауэр OfficeConnect Internet Firewall [Электронный ресурс]. Режим доступа: http://www.3com.ru/products/firewalls/oc—firewall/400546.pdf, свободный. — Загл. с экрана.

29. Бройтман Д. Микроархитектура процессора P6 // Монитор. — 1995.—№3.—С. 6-11.

30. Бройтман Д. Процессор P6: Общий обзор // Монитор. — 1995. — №5.—С. 8-12.

31. Бутримеико А.В. Разработка и эксплуатация сетей ЭВМ. — М.: Финансы и статистика, 1998. — 256 с.

32. Валях Е. Последовательно-параллельные вычисления. М.: Мир, 1995.—456 с.

33. Васильев В. Управление информационными потоками в системах поддержки принятия решения // Компьютеры + Программы. —1996.—№5.— С. 9-13

34. Вейцман К. Распределенные системы мини- и микро-ЭВМ. — М.: Финансы и статистика, 1993. - 382 с.

35. Вишневский В.М. Теоретические основы проектирования компьютерных сетей. —М.: Техносфера, 2003. — 512 с.

36. Волобуев В. Малевский П. Удаленный доступ по каналам ISDN // КомпьютерПресс. —1996. — № 5. - С. 119-123

37. Волобуев В. Технология ISDN в информационных сетях // Сети. — 1997. —*№4*. _*с*. 14-24.

38. Воронин А., Курилов О. Организация услуг VPN на базе операторских сетей // Технологии и средства связи / Ежегодный отраслевой каталог. — 2002. — С. 68-73.

39. Вычислительные сети и сетевые протоколы. / Д.Девис, Д. Барбер, У .Прайс, С.Соломонидес. — М.: Мир, 1996. — 563 с.

40. Гайкович Ю.В, Першин А.С. Безопасность электронных банковских систем. — М: Единая Европа, 1994 г.

41. Гвоздев И. М., Зайчиков В. К, Мошак Н. К, Пеленицын М. Б., Селезнев С. П., Шепелявый Д. А. Отечественные средства построения для виртуальных частных сетей // Сети и системы связи. 1999. № 12. С. 24-28.

42. Гольдштейн А.Б., Гольдштейн Б.С. Технология и протоколы MPLS. — СПб.: БХВ—Санкт-Петербург, 2005. — 304 с.

43. ГОСТ 26113-84. Процедуры управления звеном передачи данных. Элементы балансных процедур при одновременной двусторонней передаче информации и защиты от ошибок.

44. Даффи Д. Поддержка качества в виртуальных сетях // Сети. — 2001. —№09. —С. 21-29.

45. Денисова Т.Б. Надежность и безопасность услуги VPN // Электросвязь. — 2005. — № 9. — С. 20-22.

46. Джонсон Дж., Распределенные системы в многофилиальной структуре // PC Magazine/Russian Edition. — 1998 г. — №10. — С. 18-21.

47. Дрожжинов В.И., Мямлин А.Н. Сети коммутации пакетов с интерфейсом X.25. — Методические материалы и документация по пакетам прикладных программ, 1983, вып.24. Рекомендация МККТТ X.25 и ее применение в информационно-вычислительных сетях. 4.1. Опыт применения рекомендации X.25, с. 5-42.

48. Запечников СВ., Милославская Н.Г., Толстой А.И. Основы построения виртуальных частных сетей: Учебн. пособие для вузов. — М.: Горячая линия—Телеком, 2003. — 249 с.

49. Заратуйченко О.В. Концепции построения и реализации информационных систем в банках. — СУБД, 1996. — №4.

50. Захаров Г.П., **JIoxmotko** В.В. Оптимизация структуры сетей передачи данных с коммутацией пакетов. —- М., 1981. — 64 с. (Препринт/Научный совет по проблеме "Кибернетика" АН СССР).

51. Захватов М.А. Вопросы безопасности в MPLS сетях // Документальная электросвязь. — 2004. — № 13. — С.76-78.

52. Зима В., Молдовян А., Молдовян Н. Введение в защищенные виртуальные сети [Электронный ресурс]. Режим доступа: http://www.cobra.ru/ru/articles/p—vvzvs.html, свободный. - Загл. с экрана.

53. Зоркальцев А.В. Выбор оптимальной ширины окна сети ЭВМ с коммутацией пакетов // Автоматика и вычислительная техника. — 1984. — №5. — С. 8-13.

54. Зоркальцев А.В., Назаров А.А. Асимптотический анализ задержки эшелона кадров в информационном канале сети ЭВМ с коммутацией пакетов // Автоматика и вычислительная техника. — 1986. — №5. —С. 19-25.

55. Ивановский В.Б. Аналитическое моделирование приоритетных узлов синхронных информационно-вычислительных сетей // Автоматика и вычислительная техника. — 1999. — № 6. — С. 51-56.

56. Ивановский В.Б. Метод эквивалентных замен расчета узлов дискретных сетей связи // Автоматика и вычислительная техника. —1999.— №5.—С. 58-65.

57. Ивановский В.Б. О дискретных приоритетных системах обслуживания // Автоматика и телемеханика. — 1997. — № 4. — С. 37-44.

58. Ивановский В.Б. О свойствах выходных потоков в дискретных системах массового обслуживания // Автоматика и телемеханика. —1994.— №11.—С. 32-39.

59. Ивановский В.Б. Операционный анализ сетей связи с блокировками // Автоматика и вычислительная техника. — 1998. — № 3. — С. 32-38.

60. Иносэ Х., Сайто Т. Теоретические аспекты анализа и синтеза сетей пакетной связи. — ТИИЭР. — 1998. — Т. 66. — № 11. — С. 139-155.

61. Информационные подразделения в коммерческих структурах: как выжить и преуспеть. / Линьков И.И. и др.— М.: НИТ, 1998 г. — 543 с.

62. Информация администрации сети RSNet [Электронный ресурс]. Режим доступа: http://www.gov.ru/main/page5.html, свободный. - Загл. с экрана.

63. Ишкин В.Х. Единая сеть электросвязи и телемеханики электроэнергетики на период до 2015 г. Состояние и развитие // Мир связи. Connect! —1999. —№ 11. —С. 48-50.

64. Каталог сетевых продуктов // LAN Русское издание. Журнал сетевых решений. — 1996. — Т. 2. — С. 9-240

65. Клейнрок Л. Вычислительные системы с очередями. Пер. с англ. Под ред. Б.С. Цыбакова. — М.: Мир. 1979. — 600 с.

66. Компьютеризация банковской деятельности. / Титоренко Г.А. и др. — М.: Финстатинформ, 1997 г. - 208 с.

67. Кормен Т. Х., Лейзерсон Ч. И., Ривест Р. Л., Штайн К. Алгоритмы: построение и анализ / 2—е издание. — М.: Вильяме, 2005. — 1296 с.

68. Корпоративные территориальные сети связи. Выпуск 3. Под ред. М.Б. Купермана. — М.: Информсвязь, 1997. - С.55-65.

69. Кофман А., Анри-Лабордер А. Методы и модели исследования операций. — М.: Мир, 1977. — 432 с.

70. Кристофидес Н. Теория графов. Алгоритмический подход. — М.: Мир, 1978. —432 с.

71. Крылов В.В., Самохвалова С.С. Теория телетрафика и ее приложения: Учебн. пособие. — СПб.: BHV, 2005. — 288 с.

72. Ланкастер П. Теория матриц. Пер. с англ., — М.: Наука, 1978. — 280 с.

73. Леонов С. Реальная виртуальность [Электронный ресурс]. Режим доступа: http://www.computerra.ru/offline/1998/237/1149, свободный. - Загл. с экрана.

74. Леохин Ю.Л. Анализ информационной структуры корпоративной сети//Известия высших учебных заведений. Поволжский регион. Технические науки, — 2008, — № 4, — стр. 27-40.

75. Леохин Ю.Л. Анализ технической структуры корпоративной сети//Известия высших учебных заведений. Поволжский регион. Технические науки, — 2009, — № 1.

76. Лукацкий А. Атаки на VPN [Электронный ресурс]. Режим доступа: http://www.bugtraq.ru/library/crypto/vpn3.html, свободный. - Загл. с экрана.

77. Лясковский Ю. Построение территориальных сетей с интеграцией услуг // КомпьютерПресс. — 1997. — № 8. — С. 245-250.

78. Майника Э. Алгоритмы оптимизации на сетях и графах. — М.: Мир, 1981.

79. Макстеник М. Сравнение сетевых архитектур // Сети. — 1997. — №2.—С. 14-28

80. Мартин Дж. Системный анализ передачи данных. — М.: Мир, 1975,т.1,т.2,—256с.,432с.

81. Махметов Г. Реализация IPsec в свободно распространяемых UNIX [Электронный ресурс]. Режим доступа: http://vvww.compress.ru/Temp/ 702/index.htm, свободный. - Загл. с экрана.

82. Медведев Г.А. Характеристики случайных процессов в ЛВС с маркерным доступом и несимметричной нагрузкой // Автоматика и вычислительная техника. — 1995. — № 4. — С. 67-80.

83. Медведев Г.А. Характеристики случайных процессов в ЛВС со случайным доступом и несимметричной нагрузкой // Автоматика и вычислительная техника. —1994. — № 3. — С. 40-48

84. Медведев Г.А., Решетникова Н.Д., Розов М.М. Приближенный метод расчета характеристик передачи пакетов в информационно-вычислительной сети с гибридной коммутацией // Автоматика и вычислительная техника. — 1989. — № 1. — С. 42-47.

85. Межсетевой экран PIX Firewall [Электронный ресурс]. Режим доступа: http://www.cisco.com/global/RU/win/products/sec_pix.shtml, свободный. - Загл. с экрана.

86. Мизин И.А., Богатырев В.А., Кулешов А.П. Сети коммутации пакетов. — М.: Радио и связь, 1986. - 408 с.

87. Михалевич И.Ф., Сычев К.И., Лузин В.Ю. Оптимизация пропускной способности корпоративных сетей связи // Электросвязь. — 2003. —№10. —С. 36-39.

88. Мишин А.И. Леус В.А. Асинхронно-локальные системы и среды. —Новосибирск: Институт математики СО РАН СССР, 1991. - 179 с.

89. Моисеев Н.Н., Иванилов Ю.П., Столярова Е.М. Методы оптимизации. •—М.: Наука, 1978. — 352 с.

90. Нуштаев А.В., Росляков А.В. Алгоритмы построения отказоустойчивых виртуальных частных сетей // Доклады 60-й научной сессии, посвященной Дню Радио. — М., 2005. — С. 54-57.

91. Олвейн В. Структура и реализация современной технологии MPLS.: Пер. с англ. — М.: Изд. дом «Вильяме», 2004. — 480 с.

92. Олифер В.Г., Олнфер Н.А. Компьютерные сети. Принципы, технологии, протоколы. — СПб.: Издательство «Питер», 1999. — 672 с.

93. Олифер В.Г., Олифер Н.А. Новые технологии и оборудование IP-сетей. СПб.: БХВ-Санкт-Петербург, 2000. - 512 с.

94. Оре О. Теория графов. — М.: Наука, 1968. — 336 с.

95. Паппалардо Д. Виртуальная реальность? // Сети. 1999. № 05-06. — С. 54-61.

96. Паршенков Н.Я., Кольцов А.Н. Влияние величины таймаута на пропускную способность информационного канала при использовании процедуры LAPB. — В кн.: 10 Всес. шк.—сем. по вычислительным сетям: Тез. докл. —М.:—Тбилиси, 1985, ч.2, с. 273-278.

97. Первый кирпич в стене VPN. Обзор устройств VPN начального уровня [Электронный ресурс]. Режим доступа: http://www.ixbt.com/comm/vpnl. shtml, свободный. - Загл. с экрана.

98. Построение виртуальных частных сетей (VPN) на базе технологии MPLS. — М.: Cisco Systems, 2001. — 48 с.

99. Прокопьев Н. Теория и практика: VPN стандартными средствами Windows 2000 [Электронный ресурс]. Режим доступа: http://i2r. rusfund.r/static/385/out_10155.shtml, свободный. - Загл. с экрана.

100. Протоколы и методы управления в сетях передачи данных / Под ред. Ф.Ф.Куо. — М.: Радио и связь, 1985. - 480 с.

101. Размахаев С HTTP — протокол передачи гипертекстов // КомпьютерПресс. —1997. — № 7. — С 174-180.

102. Райзер М. Оценка характеристик систем передачи данных // ТИИ—ЭР. — 1982. — Т.70. — № 2. — С. 28-59.

103. Растригин JI.A., Эрмуйжа А.А. Агрегатная модель протокола с адаптацией длины кадра // Автоматика и вычислительная техника. —1984.— №2.—С. 11-15.

104. Рекомендация МККТТ X.25 и ее применение в информационно-вычислительных сетях. 4.2. Описание рекомендации X.25. — Методические материалы и документация по пакетам прикладных программ, — 1983, — 24. — 147с.

105. Репин М. Виртуальные частные сети и IPsec [Электронный ресурс]. Режим доступа: http://www.nortelnetworks.ru/press/press/repin.html, свободный. - Загл. с экрана.

106. Ретана А., Слайс Д., Уайт Р. Принципы проектирования корпоративных IP—сетей.: Пер. с англ. — М.: Издательский дом «Вильяме», 2002. —368 с.

107. Росляков А.В. Виртуальные частные сети. Основы построения и применения. — М.: Эко—Трэндз, 2006. — 304 е.: ил.

108. Росляков А.В. Классификация потоковых моделей VPN // Шестая Международная научно-техническая конференция «Проблемы техники и технологии телекоммуникаций». — Уфа, 2005. — С. 34-35.

109. Росляков А.В. Оптимальное распределение сетевых ресурсов для реализации виртуальных частных сетей // Труды учебных заведений связи — СПб., СПбГУТ, 2004. — С. 65-74.

110. Росляков А.В. Отличительные особенности телекоммуникационной сети для государственных нужд // Телекоммуникационное поле регионов. — 2005. — № 1. — С. 10-13.

111. Росляков А.В. Построение виртуальных частных сетей на базе потоковой модели // 7-я Международная конференция «Цифровая обработка сигналов и ее применение» (DSPA—2005): Тез. докл. — М., 2005. С. 136-139.

112. Росляков А.В. Системное проектирование интегрированной телекоммуникационной инфраструктуры // Труды Российского научно-технического общества радиоэлектроники, электроники и связи имени А.С. Попова. Серия: Научная сессия, посвященная Дню радио.— М.: Радио и связь, 2004. — Вып. LIX—1 — С. 39-41.

113. Росляков А.В., Нуштаев А.В. Анализ возможности применения технологии VPN для ФЦП «Электронная Россия» // XI Российская научная конференция профессорско-преподавательского состава ПГАТИ: Тез. докл. — Самара, 2004. — С. 60-61.

114. Сарыпбеков Ж.С. Вычислительные системы и сети: архитектура, проблемы и перспективы. —Алма-Ата: КазНИИНКИ, 1991. — 136 с.

115. Сериков И. Виртуальные частные сети [Электронный ресурс]. Режим доступа: http://www.pcmag.ru/archive/9905/ 059932.asp, свободный. - Загл. с экрана.

116. Сидтиков А.Х. Повышение экономической эффективности при планировании региональной информационной сети // Тезисы докладов Всероссийской научной конференции «Relarn-99». — Самара, 1999. С. 35.

117. Скляревич А.Н. Определение характеристик производительности канала при двухсторонней совместимой во времени пересылке нескольких больших массивов // Автоматика и вычислительная техника. —1989.—№4.— С. 13-20.

118. Скляревич А.Н. Оценка производительности информационного канала при односторонней передаче с возможными ошибками поступающего пуассоновского потока кадров // Автоматика и вычислительная техника. — 1989. —№5. —С. 46-50.

119. Скляревич А.Н. Характеристики времени передачи заданного объема информации по сетевому каналу при возможности сбоев // Автоматика и вычислительная техника. —1986. — № 3. — С. 38-44

120. Скляревич И.К. Оптимальный размер диалогового блока, передаваемого по сеансовому соединению // Автоматика и вычислительная техника. - 1989. - № 4. - С. 49-55.

121. Скляревич И.К. Условия рациональности сегментирования пакетной коммутации // Автоматика и вычислительная техника. — 1989. — №6.—С. 15-22.

122. Соболев Д.В. Защищенная телекоммуникационная сеть оператора связи на базе технологии IP-MPLS для построения корпоративной сети сетях // Документальная электросвязь. — 2004. — № 13. — С. 82-84.

123. Стандарты по локальным вычислительным сетям: Справочник / В.К.Щербо, В.М.Киреичев, С.И.Самойленко; Под ред. С.И.Самойленко. — М.: Радио и связь, 1990. — 304 с.

124. Столлингс В., Компьютерные системы передачи данных. •— Изд. д. Вильяме, 2002. — 928 с.

125. Танненбаум Э., М. Ван Стен. Распределенные системы. Принципы и парадигмы. — СПб.: Питер, 2003. — 877 с.

126. Типовые решения по организации виртуальных частных сетей [Электронный ресурс]. Режим доступа: http://www.incap.ru/Incap/idp/bd/netsupport/typical/vpn.html, свободный. - Загл. с экрана.

127. Тушнолобов И.Б., Урусов Д.П., Ярцев В.И. Распределенные сети. — СПб.: Питер, 1998.

128. Умрихин Ю.Д. Оптимизация сложных информационных систем. — М.: Минрадиопром, 1983.—125 с.

129. Фиско Р., Пьемонт М., Карни Д. и др. Идеальные компоненты // PC Magazine/RE. — 1996. — № 10. — С. 56-93.

130. Ху Т. Целочисленное программирование и потоки в сетях. — М.: Мир, 1977. Беллман Р., Дрейфус С. Прикладные задачи динамического программирования. — М.: Наука, 1965.

131. Чернат А.П. Процедуры линейного управления, используемые в коммутационном процессоре. —В кн.: Вопросы построения сетей ЭВМ и ВЦ коллективного пользования. — Киев: ИК АН УССР, 1978, с. 20-29.

132. Шарейко Л.А., Чебанюк А.В., Подгурскин А.И. Повышение пропускной способности протоколов управления каналом передачи данных.

— В кн.: Вычислительные сети коммутации пакетов: Тез.докл. III Всес.конф. — Рига: Институт электроники и вычислительной техники АН Латв.ССР, 1983, т.1, с. 118-122.

133. ШарейкоЛ.А., Петрунин В.С. Модель оценки временных задержек в распределенных сетях коммутации пакетов. — В кн.: XVI Всесоюзная школа-семинар по вычислительным сетям: Тез.докл. — М.: Винница, 1991, т.З, с. 87-92.

134. Шварц М. Сети связи: Протоколы, моделирование и анализ: в 2-х ч. 4.1. •—-М.: Наука. Гл. ред. физ.—мат. лит., 1992. - 336 с.

135. Шварц М. Сети ЭВМ. Анализ и проектирование. — М.: Радио и связь, 1997.-336 с.

136. Шереметьев А. Отказоустойчивые дисковые массивы // КомпьютерПресс. —1997. — № 7. — С. 40-47.

137. Шестаков М. Частные сети передачи данных: подходы и методы построения // КомпьютерПресс. -— 1996. — № 8. — С. 83-86.

138. Шестаков М. Частные сети передачи данных: подходы и методы построения // КомпьютерПресс. —1996. — № 10. — С. 79-82.

139. Шестаков М. Частные сети передачи данных: подходы и методы построения // КомпьютерПресс. —1996. — № 9. — С. 128-133.

140. Шнепс М.А. Системы распределения информации. Методы расчета. — М.: Связь, 1979. — 344 с.

141. Шэнк Д.Д. Технология клиент/сервер и ее приложения. — М.: Издательство "ЛОРИ", 1995,—418с.

142. Якубайтис Э.А. Информационно-вычислительные сети. — М.: Финансы и статистика, 1984. —232 с.

143. Altiok T. Approximate analysis of exponential tandem queues with blocking. — Eur. Journ. of Oper. Res. — 1998. — Vol. 11. — № 4. — P. 390-398

144. Azuma M., Ebihara Y., Ikeda K. Study on the throughput limits over the HDLC Protocol. — Journ. of Inform. Process. — 1998. — Vol. 5. — № 3. — P. 155-161.

145. Bux W., Kummerle K., Truong H.L. Balanced HDLC Procedures: A Performance Analysis // IEEE Trans, on Commun. — 1997. — Vol. COM—28. — № 11.—P. 1889-1898.

146. Bux W., Kummerle K., Truong H.L. Data Link—Control Performance: Results Comparing HDLC Operational Modes. — Comput. Networks. —1997. — Vol. 6.—№1.—P. 37-51

147. Caseau P., Pujolle G. Throughput Capacity of a Sequence of Quenes with Blocking due to Finite Waiting Room // IEEE Trans, on Software Eng. — 1989.—Vol. SE—5. —№6.—P. 631-642.

148. Chu W.W. Optimal Message Block Size for Computer Communications with Error Detection and Retransmission Strategies // IEEE Trans, on Commun. — 1999. — Vol. COM—22. — № 10. — P. 1516-1525.

149. Cinkler T., Maliosz M. Configuration of Protected Virtual Private Networks // Design Of Reliable Communication Networks, DRCN. — Budapest, Hungary, 2001.

150. Duffield N.G., Gay aim P., Greenberg A., Mishra P., Ramakrishnan K.K., van der Merwe J.E. Resource management with hoses: point-to-cloud services for virtual private networks // IEEE/ACM Transactions on Networking. — 2002. — V. 10, №5. —P. 679-692.

151. Duffield N.G., Goyalm P., Greenberg A., Mishra P., Ramakrishnan K.K., van der Merwe J.E. A flexible model for resource management in virtual private networks // Proceedings of ACM SIGCOMM. — 1999. — P. 95-108.

152. Easton M.C. Batch Throughput Efficiency of ADCCP/HDLC/SDLC Selective Reject Protocols // IEEE Trans, on Commun. —1995. — Vol. COM—28. —№2. —P. 187-195.

153. Eisenbrand F., Grandoni F. An improved approximation algorithm for virtual private network design // ACM-SIAM Symposium on Discrete Algorithms. — 2005.—P. 928-932.

154. Eisenbrand F., Grandoni F., Oriolo G., Skutella M. New approaches for virtual private network design // International Colloquium on Automata, Languages and Programming. — 2005. —P. 1151-1162.

155. Gupta A., Kleinberg J., Kumar A., Rastogi R., Yener B. Provisioning a virtual private network: a network design problem for multicommodity flow // Proceedings of ACM STOC. — 2001. — P. 389-398.

156. Gupta A., Kumar A., Rastogi R. Traveling with a Pez dispenser (or, routing issues in MPLS) // In 42nd IEEE Symposium on Foundations of Computer Science. — Las Vegas, NV, 2001. —P. 148-157.

157. Hota C, Jha S.K., Raghurama G. Restoration of Virtual Private Networks with QoS Guarantees in the Pipe Model // Proceedings in Distributed Computing IWDC. — Kol-kata, India, 2004. — P. 289-302.

158. IP VPNs for Service Providers: The Foundation for Profitable [Электронный ресурс]. Режим доступа: http://www.cisco.com/en/US/ netsol/ns341/, свободный. — Загл. с экрана.

159. Irland M.I., Pujolle G. Comparison of Two Packet-Retransmission Techniques // IEEE Trans, on Inform. Theory, 1998. — vol. IT-26. — №1. — P.92-97

160. Johnson T. Packet switching services and the data communication user. Pt. I. — London: Ovum, 1976. — 153 p.

161. Kar K, Kodialam M., Lakshman T.V. Minimum interference routing of bandwidth guaranteed tunnels with MPLS traffic engineering applications // IEEE J. Selected Areas in Communications. — 2000. — V. 18, № 12. — P. 2566—2579.

162. Ахметжанова К.Б., Кудинова В.С. «Исследование построения виртуальной корпоративной сети связи» // Сборник материалов конференции. АУЭС. -2013.- С.13-18.

Приложение А
Текст программы моделирования системы массового обслуживания

```
GENERATE 8,4 ;генерация транзактов
QUEUE QRAM ;вход в накопитель
QUEUE QN ;вход в очередь к основному каналу
SEIZE OSKANAL ;занять основной канал
DEPART QN ;покинуть очередь к основному каналу
ADVANCE 7,3 ;задержка на обработку
RELEASE OSKANAL ;освободить основной канал
DEPART QRAM ;покинуть накопитель
OUT TERMINATE ;вывод транзактов из модели
GENERATE 170,30,,,1 ;генерация «сбойных» транзактов
PREEMPT OSKANAL,PR,OUT ;захват основного канала
SPLIT 1,REZ ;передача копии транзакта в резервный канал
ADVANCE 20,7 ;задержка на восстановление основного канала
RETURN OSKANAL ;освободить основной канал
TRANSFER ,OUT ;переслать транзакт на блок TERMINATE
REZ QUEUE 1 ;занять очередь
ADVANCE 1,1 ;задержка на запуск резервного канала
DEPART 1 ;покинуть очередь
QUEUE 2 ;вход очередь к резервному каналу
SEIZE RKANAL ;занять резервный канал
DEPART 2 ;покинуть очередь к резервному каналу
ADVANCE 7,3 ;задержка на обработку
RELEASE RKANAL ;освободить резервный канал
TRANSFER ,OUT ; переслать транзакт на блок TERMINATE
;сегмент таймера
GENERATE 7200 ;генерация транзактов через 7200 с
TERMINATE 1 ;вывод транзакта из модели и уменьшение значения счетчика на единицу
START 1 ;установка начального значения счетчика в еденицу
```

Приложение Б
Листинг программы

```
START TIME END TIME BLOCKS FACILITIES STORAGES
0.0   7200.000 28 2 0
      NAME VALUE
      OSKANAL 10002.000
      OUT 10.000
      QN 10001.000
      QRAM 10000.000
      REZ 17.000
      RKANAL 10003.000

LABEL LOC BLOCK TYPE ENTRY COUNT CURRENT COUNT RETRY
1 GENERATE 894 0 0
2 QUEUE 894 0 0
3 QUEUE 894 2 0
4 SEIZE 892 0 0
5 DEPART 892 0 0
6 ADVANCE 892 1 0
7 RELEASE 853 0 0
8 DEPART 853 0 0
OUT 9 TERMINATE 975 0 0
10 GENERATE 42 0 0
11 PREEMPT 42 0 0
12 SPLIT 42 0 0
13 ADVANCE 42 0 0
14 RETURN 42 0 0
15 TRANSFER 42 0 0
REZ 16 QUEUE 42 0 0
17 ADVANCE 42 0 0
18 DEPART 42 0 0
19 QUEUE 42 0 0
20 SEIZE 42 0 0
21 DEPART 42 0 0
22 ADVANCE 42 0 0
23 RELEASE 42 0 0
24 TRANSFER 42 0 0
25 GENERATE 1 0 0
26 TERMINATE 1 0 0

FACILITY ENTRIES UTIL. AVE. TIME AVAIL. OWNER PEND INTER RETRY DELAY
OSKANAL 934 0.954 7.357 1 978 0 0 2 0
RKANAL 42 0.039 6.703 1 0 0 0 0 0

QUEUE MAX CONT. ENTRY ENTRY(0) AVE.CONT. AVE.TIME AVE.(-0) RETRY
1 1 0 42 0 0.006 1.031 1.031 0
2 1 0 42 42 0.000 0.000 0.000 0
QRAM 43 41 894 0 21.064 169.645 169.645 0
QN 6 2 894 126 1.350 10.871 12.654 0

FEC XN PRI BDT ASSEM CURRENT NEXT PARAMETER VALUE
981 0 7201.562 981 0 1
978 0 7205.764 978 7 8
974 1 7323.492 974 0 11
982 0 14400.000 982 0 27
```