НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

На правах рукописи

ПОЛЯКОВ Кирилл Александрович

МЕТОДЫ ОЦЕНКИ АППАРАТУРНОЙ НАДЕЖНОСТИ И ЗАЩИТЫ КОММЕРЧЕСКОЙ ИНФОРМАЦИИ ЭЛЕКТРОННОЙ ТОРГОВОЙ ПЛОЩАДКИ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

Специальность 05.12.13 – Системы, сети и устройства телекоммуникаций

Диссертация

на соискание ученой степени кандидата технических наук

Научный руководитель
Доктор технических наук, профессор
Жданов В.С.

Научный консультант
доктор технических наук, доцент
Сафонова И.Е.

Москва 2014

Оглавление

Тема: «МЕТОДЫ ОЦЕНКИ АППАРАТУРНОЙ НАДЕЖНОСТИ И ЗАЩИТЫ КОММЕРЧЕСКОЙ ИНФОРМАЦИИ ЭЛЕКТРОННОЙ ТОРГОВОЙ ПЛОЩАДКИ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ»

ВВЕДЕНИЕ

Актуальность. Развитие телекоммуникационных технологий меняет подход к проектированию, построению и модернизации большинства корпоративных систем и сетей, которые становятся более сложными и масштабными с точки зрения их инфраструктуры, функциональности и используемых сервисов. К этому классу относятся современные системы электронных торгов – электронные торговые площадки (ЭТП), программно-аппаратная реализация которых опирается на современные информационные и телекоммуникационные технологии. Они решают задачи по безопасной и бесперебойной передаче и обработке информации, содержащей коммерческую (а в некоторых случаях - государственную) тайну. Качество и эффективность систем этого класса во многом определяются как их аппаратурной надежностью, так и надежностью программных средств защиты информации: проблема обеспечения надежности телекоммуникационных систем и сетей, являющихся ядром систем электронных торгов, остается актуальной. Требуют дальнейшего изучения и развития методы оценки надежности устройств, критичных к задержке результатов вычислений [1, 6, 10]. Актуальными являются вопросы защиты коммерческой информации ЭТП: системы электронной торговли должны гарантировать юридически значимый документооборот, т.е. обеспечить аутентификацию, целостность информации и неотрекаемость. Необходимо отметить, что ЭТП и электронные торги появились в РФ в начале 2000 годов, но действительно развитие данных сервисов началось только в 2009 году, когда крупные корпорации и госкомпании начали подготовку к выполнению поручения правительства по сокращению издержек на 10% в год в течение 3 лет. Далее появился Федеральный закон Российской Федерации от 18 июля 2011 г. N 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц», обязывающий более 20000 компаний проводить свои закупки в электронной

форме [2, 52, 61]. При увеличении интереса к ЭТП и, как следствие, потока клиентов увеличивались и совершенствовались функциональные возможности ЭТП.

Следовательно, актуальной научной задачей является разработка и развитие методов обеспечения надежной передачи, обработки и защиты коммерческой информации ЭТП в телекоммуникационных сетях с целью улучшения их технических характеристик и повышения эффективности функционирования.

В процессе решения поставленной научной задачи автор в своих исследованиях опирался на труды российских и зарубежных ученых, которые внесли существенный вклад в развитие телекоммуникационных сетей – Л.Клейнрок, А.Гарсиа-Диас, В.М.Вишневский, А.И.Русаков, А.Н.Назаров, Ю.В.Семенов, В.Столлингс, Г.П.Башарин, Г.Хелд, Д.Филлипс, И.А.Мизин, О.И.Бронштейн, С.Фейт, Эд.Уилсон и другие ученые.

Проводимые исследования актуальны как в настоящее время, так и на обозримую перспективу развития телекоммуникационных систем и сетей.

Цель и задачи исследований заключается в повышении эффективности процессов проектирования, функционирования и развития телекоммуникационных систем и сетей, используемых в электронной коммерции, за счет разработки новых методов, моделей и алгоритмов оценки надежности и защиты коммерческой информации электронных торговых площадок.

Для достижения поставленной цели потребовалось решение следующих задачи:

1) исследовать особенности использования телекоммуникационных сетей в электронной коммерции и определить критерии эффективности их работы и провести анализ методов и средств обеспечения аппаратурной надежности и информационной безопасности в телекоммуникационных системах

электронной коммерции;

2) разработать графовую модель оценки аппаратурной надежности телекоммуникационных сетей электронной коммерции и алгоритм ее анализа;

3) разработать метод оценки надежности устройств телекоммуникационных систем и сетей, критичных к задержке результатов вычислений;

4) разработать алгоритм резервирования устройств корпоративной телекоммуникационной сети электронной коммерции и ЭТП;

5) разработать метод поэтапного подписания документов электронной подписью для электронной торговой площадки, включающий методику проверки сертификатов и процедуру принятия решения об участии пользователя в электронных торгах;

6) разработать программное обеспечение, реализующее предложенные методы, алгоритмы и модели.

Объект исследования - корпоративные телекоммуникационные сети электронной коммерции.

Предмет исследования - методы и модели оценки и расчета аппаратурной надежности сетей и защиты коммерческой информации ЭТП в телекоммуникационных сетях электронной коммерции.

Методы исследования - методы теории сложных систем, систем и сетей массового обслуживания, теория графов, методы математического моделирования, принятия решений и оптимизации, теория вероятности.

Научная новизна работы заключается в том, что разработаны:

1) метод оценки надежности устройств телекоммуникационных сетей электронной коммерции, критичных к задержке результатов вычислений, позволяющий прогнозировать вероятность выхода из строя узла/элемента сети и ЭТП, как при обслуживании заявок электронной торговой площадки, так и в свободном состоянии;

2) графовая модель оценки аппаратурной надежности и алгоритм ее анализа, позволяющие проверять правильность проектных решений и применять меры по повышению надежности сетей; проводить оптимизацию аппаратурной надежности и многоуровневое моделирование с учетом специфики работы сетевых устройств; прогнозировать стратегию модернизации и развития корпоративных сетей электронной коммерции;

3) алгоритм резервирования элементов телекоммуникационной сети электронной коммерции и элементов ЭТП, который в отличие от уже существующих позволяет эффективно реализовать резервирование, обеспечив не только заданные показатели надежности, но и добиться этого как можно более экономично с наименьшими суммарными затратами на резервные элементы, т.е. при заданных ресурсных ограничениях достичь максимально возможной аппаратурной надежности всей сети;

4) эффективный метод поэтапного подписания документов электронной подписью для ЭТП, который в отличие от уже существующих, включает

- методику проверки сертификатов, позволяющую проводить проверку сертификатов сразу по 5 позициям (имеющиеся аналоги проводят проверку только по 1 или 2 позициям),

- процедуру принятия решения об участии пользователя в электронных торгах, позволяющую провести декомпозицию и анализ проблемы оценки альтернативных решений в конкретной ситуации.

Практическая значимость работы состоит:

- в создании программного обеспечения системы оценки надежной передачи и защиты информации электронной торговой площадки в телекоммуникационных сетях электронной коммерции;
- в разработке методических материалов по моделированию телекоммуникационных сетей, расчета их надежности и защиты информации;

- в возможности использования разработанного математического аппарата для современных автоматизированных систем электронных торгов;

Основные научные положения, выносимые на защиту

1) метод оценки надежности устройств телекоммуникационных сетей электронной коммерции, критичных к задержке результатов вычислений;

2) графовая модель оценки аппаратурной надежности и алгоритм ее анализа;

3) алгоритм резервирования устройств телекоммуникационной сети электронной коммерции и ЭТП;

4) метод поэтапного подписания документов ЭП для электронной торговой площадки.

Реализация результатов диссертационной работы.

Основные результаты исследований использовались:

- на электронной торговой площадке ООО «Аукционный Конкурсный Дом» (www.a-k-d.ru), являющейся официальной электронной торговой площадкой Госкорпорации «Росатом», торги на которой проводят такие предприятия как ФГУП «Атомфлот», Международный аэропорт Домодедово и ряд других, что позволило эффективно оптимизировать телекоммуникационную сеть предприятия АКД с учетом решаемых задач и улучшить технические характеристики сети более чем на 30%;

- в учебном процессе кафедры вычислительные системы и сети МИЭМ НИУ ВШЭ при преподавании дисциплин «Теоретические основы построения вычислительных систем и сетей», «Проектирование систем и сетей» и «Моделирование компьютерных сетей и телекоммуникационных систем».

Апробация работы. Основные положения и результаты работы опубликованы в рецензируемых научно-технических журналах, докладывались и обсуждались:

- на Юбилейной X Международной научно-практической конференции

«Инновации на основе информационных и коммуникационных технологий» (ИНФО-2013), Сочи;

- на международной научно-технической конференции «International conference in informatization and telecommunication», Ruen (France), 2011;
- на 17-й международной конференции «Распределенные компьютерные и коммуникационные сети; управление, вычисление, связь», (DCCN-2013) Москва;
- на научном семинаре кафедры «Вычислительные системы и сети» МИЭМ НИУ ВШЭ.

Достоверность научных результатов подтверждается:

- данными об успешном практическом применении результатов диссертации;
- корректностью выводов математических зависимостей для расчета надежности сетей;
- полученные научные результаты обеспечены математическими доказательствами или экспериментальной проверкой, а также согласованы с имеющимися результатами других авторов, опубликованными в отечественной и зарубежной литературе.

Приоритет практических решений подтвержден авторскими свидетельствами о государственной регистрации программ для ЭВМ.

Объем и структура диссертации

Диссертация состоит из введения, четырех глав, заключения, списка литературы из 105 наименований и приложения, содержит 16 рисунков и 6 таблиц. Основной текст диссертации изложен на 110 страницах.

В первой главе проведен анализ состояния и перспектив развития телекоммуникационных сетей. Показано, что электронная коммерция характеризуется разносторонностью и объединяет множество коммуникационных технологий. Приведены функции, возможности и

преимущества работы на ЭТП для заказчика и для компании, представлены примеры федеральных и коммерческих торговых площадок. Проанализированы существующие способы обеспечение надежности функционирования автоматизированных систем электронных торгов.

Проанализированы особенности использования телекоммуникационных сетей в электронной коммерции. Показано, что для оценки надежности сетей необходимо выбрать частные аспекты – аппаратурную (элементарную) и функциональную (структурную) надёжности.

Проведен анализ методов и средств обеспечения информационной безопасности в телекоммуникационных сетях электронной коммерции. Исследованы методы и модели оценки надежности таких сетей. Определены требования, предъявляемые к моделям. Исследованы современные системы оценки надежности и защиты информации, как Российские, так и зарубежные. Дана формализация постановки задачи.

Во второй главе описаны методы и модели оценки аппаратурной надежности телекоммуникационной сети - как сложной иерархической системы.

Исследованы особенности математических моделей расчета надежности телекоммуникационных сетей. Эти модели имеют дело с вероятностными процессами и используют в качестве исходных данных достаточно недостоверную статистику, а иногда эта статистика вообще отсутствует.

Представлен разработанный метод оценки надежности устройств телекоммуникационных сетей электронной коммерции, критичных к задержке результатов вычислений.

Приводится описание разработанного алгоритма резервирования устройств корпоративной телекоммуникационной сети электронной коммерции. Алгоритм основан на методе наискорейшего покоординатного

спуска, а процесс создания резервированной системы, т.е. какого-либо участка (или элемента) сети представляется в виде многошагового процесса.

Представлены разработанные графовая модель оценки аппаратурной надежности телекоммуникационной электронной коммерции сети и алгоритм ее анализа.

В третьей главе исследованы средства и методы защиты информации ЭТП в телекоммуникационных сетях электронной коммерции, а также требования к классу защищенности 1Г для автоматизированной системы электронной торговой площадки.

Представлены схемы построения электронной подписи, проанализированы их особенности. Исследованы преимущества использования хэш-функций в схемах электронной подписи для зашиты коммерческой информации ЭТП.

Представлен разработанный метод поэтапного подписания документов ЭП для электронной торговой площадки, который содержит 8 основных этапов: подготовка данных; получение комплекта ЭП; подготовка к работе с ЭП; проверка данных; проверка сертификатов оператором ЭТП; использование ЭП; проверка ЭП, принятие решения об участии пользователя в электронных торгах. Метод базируется на современных ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012. Обосновано применение ГОСТ Р 34.11-2012 в схеме ЭП.

Дано описание разработанной методики проверки сертификатов, которая является уникальной и позволяет проводить проверку сертификатов сразу по 5 позициям: проверка сроков действия пользовательского сертификата, сроков действия корневого сертификата, наличие соответствующего корневого сертификата в базе, проверка в списках отозванных, соответствия пользователя и сертификата.

Представлена разработанная процедура принятия решения ЛПР об участии пользователя в электронных торгах. Анализ существующих подходов

к решению этой задачи показал целесообразность принятия решения на базе экспертных процедур, где наиболее эффективным является метод анализа иерархий.

В четвертой главе представлены экспериментальные результаты реализации методов, алгоритмов и моделей, предложенных в главах 1 - 3 диссертационной работы. Приводится описание разработанной системы оценки надежной передачи и защиты информации ЭТП в телекоммуникационных сетях электронной коммерции. Сформулированы требования, предъявляемые к программному обеспечению разработанной системы. Продемонстрированы основные этапы ее функционирования. Обосновано практическое применение, разработанного математического аппарата в автоматизированных системах электронных торгов.

В заключении сформулированы основные выводы по диссертационной работе в целом.

В приложении приводятся акты использования результатов диссертационной работы.

Публикации. Основные положения диссертационной работы отражены в 8 публикациях, в том числе: в 3 статьях, опубликованных в журналах, входящих в перечень ВАК России, 5 статьях в других рецензируемых изданиях, 3 доклада в трудах международных конференций, зарегистрировано 2 объекта интеллектуальной собственности.

Личное участие автора в полученных результатах

Работа явилась обобщением результатов исследования автора в период с 2010 года по настоящее время и выполнена в МИЭМ НИУ ВШЭ на кафедре «Вычислительные системы и сети». Представленные результаты исследований получены лично автором. В работах, опубликованных в соавторстве, соискателю принадлежит ведущая роль при постановке задачи, разработки метода ее решения и обобщении полученных результатов.

ГЛАВА 1. ПОСТАНОВКА ЗАДАЧИ НАДЕЖНОЙ ПЕРЕДАЧИ И ЗАЩИТЫ ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

1.1. Надежность – как один из критериев оценки качества телекоммуникационных сетей

К телекоммуникационным сетям относятся [4, 13, 20]: компьютерные и телефонные сети, радиосети, телевизионные сети. Анализ теоретических и экспериментальных исследований [2, 18, 20, 59, 87, 89, 90, 97, 98] позволяет выделить основные критерии оценки качества (критерии эффективности работы) телекоммуникационных сетей – это производительность, надежность, безопасность, расширяемость, масштабируемость, прозрачность, поддержка разных видов трафика, управляемость, совместимость. Иногда в понятие «качество обслуживания» сети включают только две важные характеристики – это производительность и надежность. На рис. 1.1 представлен пример телекоммуникационной сети.

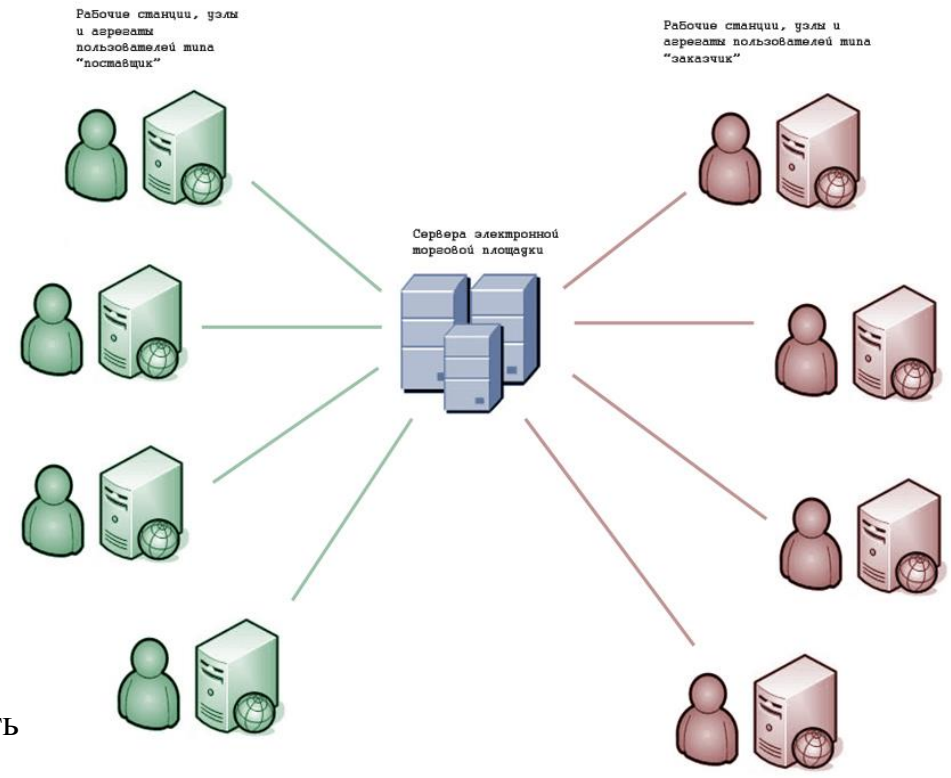

Рис.1.1 – Телекоммуникационная сеть

При анализе надежности и безопасности сетей следует выделять такие показатели как: вероятность отказа, среднее время наработки на отказ, интенсивность отказов, коэффициент готовности, сохранность данных и защита их от искажений, согласованность (непротиворечивость) данных, вероятность доставки пакета узлу назначения без искажений, вероятность потери пакета, вероятность искажения отдельного бита передаваемых данных, отношение потерянных пакетов к доставленным, безопасность или способность системы защитить данные от несанкционированного доступа, отказоустойчивость.

Для оценки надежности сетей необходимо выделить частные аспекты – аппаратурную (элементарную) и функциональную (структурную) надёжность, соответствующие методы их оценки, и рассмотреть методические вопросы надежности с учетом *QoS*, рекомендации МСЭ-Т G.602, G.821 ITU-T, ГОСТ27.003 - 83, ГОСТ 27.410 - 83, ГОСТ 27.002 - 83, ГОСТ 27.003-83 и других [17, 22, 23, 59, 71, 91]. Элементарная надежность – это свойство, присущее элементу сети связи, сохранять работоспособность с качеством не хуже заданного на некотором интервале времени. Структурная надежность – свойство сети обеспечивать связность пользователей с качеством не хуже заданного на некотором интервале времени.

Для оценки надежности применяются следующие основные характеристики: готовность, безопасность и отказоустойчивость. Надежность телекоммуникационных сетей во многом определяется надежностью сегментов физической среды передачи для каналов связи и надежностью сетевого оборудования. С помощью одного показателя надёжность такого сложного и многогранного объекта, как телекоммуникационные сети, полностью охарактеризовать невозможно, поэтому для более полной характеристики необходимо определение целого набора параметров надёжности [22, 33, 60, 66]. Как известно, недостаточно определить надежность на качественном уровне, необходимо оценивать надежность количественно и сравнивать различные объекты по их надежности. С этой целью вводятся показатели и критерии надежности. Показатель надежности - количественная характеристика одного или нескольких единичных свойств, определяющих надежность объекта. Различают единичные и комплексные показатели

надежности [33, 59, 81]. Комплексные показатели характеризуют несколько единичных свойств.

Для характеристики качества функционирования сетей и устройств в теории надежности разработаны набор интервальных, интегральных и точечных *показателей надежности,* а также методы их расчета.

Каждый объект характеризуется вектором единичных и комплексных показателей. Поскольку при сравнении вариантов один из них может быть лучше альтернативного варианта по одному показателю и хуже по другому, то среди показателей выбирают тот, который в конкретных условиях наилучшим образом отражает свойство надежности, и именно его выбирают в качестве критерия надежности.

Существуют следующие критерии оценки надежности устройств телекоммуникационных сетей: ремонтопригодность, гарантийный срок эксплуатации, коэффициент готовности, коэффициент простоя и т. д.. Правило, выбор показателя диктуется либо принятым в отрасли стандартом, либо непосредственно потребителем [59, 66].

В таблице 1.1 представлена классификация систем по уровню надежности [59, 69].

Таблица 1.1.

Коэффициент готовности	**Типы систем**	
0,99	Обычная	Conventional
0,999	Высокой надежности	Highavailability
0,9999	Отказоустойчивая	Faultresilient
0,99999	Безотказная	Faulttolerant

1.2. Особенности использования телекоммуникационных сетей в электронной коммерции

Для телекоммуникационных сетей корпораций, занимающихся электронной коммерцией (корпоративных телекоммуникационных сетей) характерны свои особенности. Организационная структура такой корпорации такова, что отдельные функции распределяются горизонтально между его

подразделениями, а иерархические взаимоотношения ослаблены. В современных западных исследованиях, посвященных информационному обществу, сетевые корпорации называются также «организация с модульной структурой» или «динамическая сетевая организация» [12, 15, 21, 39, 66, 74]. Согласование действий подразделений в корпорациях данного типа осуществляется головным офисом через Интернет, но при этом отличительными особенностями являются самоорганизующиеся процессы и децентрализованное управление; количество внутренних иерархических уровней в сетевых корпорациях невелико. Процесс создания сети в этом случае существенно упрощается, поскольку отпадает необходимость в разработке интеграционного проекта, так как отдельные подразделения могут создавать собственные подсистемы, используя свои локальные сети и серверы, не связывая их с другими подразделениями, а затем могут подключаться к единой системе корпорации. Особенности построения таких сетей [9, 58, 61, 66, 74]:

- совершенствование методов доступа в Интернет;
- перенос интернет-сервисов на мобильные терминалы (в том числе на сотовые телефоны), многие зарубежные банки активно внедряют мобильные торговые платформы, оптимизированные для iPad, iPhone и прочих устройств, перспективно развитие аналогичных мобильных банковских платформ и в России;
- создание и распространение более удобных интернет-стандартов;
- используются высокоскоростные технологии передачи информации и различные комбинации каналов связи;
- предусматривается интеграция сети с другими телекоммуникационными системами, а также создание резервных каналов связи и дублирование всех основных компонентов систем, что обеспечивает высокую производительность, надежность и отказоустойчивость сети, а также способность к дальнейшему развитию;
- объединение десятков тысяч компьютеров, размещенных в различных странах и городах;
- повышенные требования к надежности передачи и защите информации в таких сетях.

Среди требований к проведению коммерческих операций следует выделить: конфиденциальность, целостность, аутентификация, авторизация, гарантии и сохранение тайны. Первые 4-е требования можно обеспечить техническими средствами, выполнение последних 2-х зависит от технических средств и от ответственности отдельных лиц и организаций, а также от соблюдения законов.

1.3. Автоматизированные системы электронных торгов

1.3.1. Электронная торговая площадка

Аппаратно-программной основой электронной коммерции являются телекоммуникационные системы и сети, глобальная сеть Интернет, коммерческие и корпоративные сети, информационные и телекоммуникационные технологии [61, 73, 93 - 94].

Системы электронных торгов представляют собой программные и технологические решения, предназначенные для автоматизации процедур подготовки и проведения электронных аукционов и других видов конкурентных закупок. Самой распространенной, простой и удобной формой применения систем электронной торговли являются электронные торговые площадки (ЭТП). Большое значение в развитии электронных торговых площадок имеет формирование законодательной базы государственных закупок. Системы электронных торгов постепенно будут переходить с уровня ЭТП на уровень полномасштабных систем управления торгово-закупочной детальностью с использованием телекоммуникационных сетей. ЭТП – это комплекс информационных и технических средств, обеспечивающий взаимодействие заказчика с поставщиком через телекоммуникационные каналы на всех этапах при заключении сделки [21, 44, 52, 66, 92].

Функции ЭТП включают: информационную функцию, обеспечивающую доступ к перечню организаций на ЭТП и получить информацию по интересующей организации; функцию маркетинга; рекламную функцию; торговую функцию; аналитическую функцию, позволяющую проводить сравнительный анализ различных показателей деятельности организаций;

функцию защиты информации, обеспечивающую безопасный электронный документооборот, построенный с использованием сертифицированных средств криптографической защиты информации.

Преимущества работы на ЭТП для заказчика и для компании заключаются в следующем: большая экономия рабочего времени; экономия денег на организации и проведении закупок; прозрачность процесса закупок; честная конкуренция; участие в торгах возможно «из любой точки мира, не выходя из офиса»; доступность для представителей любого бизнеса - цена и условия лота ничем не ограничены.

Для работы на электронной торговой площадке Организация - участник размещения заказа должна иметь средства электронной подписи (ЭП), выданные удостоверяющим центром, прошедшем авторизацию и заключившим соглашение с оператором электронной площадки, отобранным для проведения аукционов при размещении государственного заказа [7, 62, 66].

Существуют следующие ЭТП предназначенные:

1) для размещения государственного заказа;

2) для коммерческих заказчиков – специализированные и многопрофильные.

Среди федеральных торговых площадок можно выделить:

- Электронная площадка ЗАО «Сбербанк - АСТ», предназначена для размещения заказов для государственных и муниципальных нужд.
- ОАО «Единая электронная торговая площадка» было создано в качестве специализированной компании для проведения электронных аукционов для заказчиков г. Москвы и развития ЭТ в государственном секторе в целом.
- ООО «РТС-Тендер» является организацией в рамках Группы РТС электронных аукционов для осуществления государственных, муниципальных и корпоративных закупок.
- Электронные торги АГЗРТ zakazrf.ru, предназначена для размещения заказов для государственных и муниципальных нужд.

- Электронная торговая площадка ММВБ «Госзакупки», предназначена для размещения заказов для государственных и муниципальных нужд.

Среди коммерческих торговых площадок можно выделить:

- АКД – электронная торговая площадка, разработанная в 2009 году для проведения всех видов электронных закупок (в том числе по ФЗ №223-ФЗ) и процедур на продажу.

- SETonline - Оператором системы электронных торгов SETonline является ООО «СЭТОНЛАЙН», созданное в партнерстве с компанией NAUMEN. Оказание комплекса услуг по организации закупочной деятельности предприятий в соответствии с требованиями ФЗ №223-ФЗ от 18.07.2011. Внедрение автоматизированных систем управление закупками предприятия на базе NAUMEN GPMS для государственных и коммерческих заказчиков.
- Торговый портал «Фабрикант» - российская Межотраслевая Система Электронных Торгов, позволяющая проводить полный комплекс конкурентных торгово-закупочных процедур по продаже или покупке продукции, работ и услуг в рамках корпоративных закупок предприятий и организаций.

1.3.2. Обеспечение надежности функционирования телекоммуникационных систем электронных торгов

Для построения надежных телекоммуникационных сетей (ТКС) и систем можно использовать различные виды обеспечения: экономическое; временн*о*е; организационное; структурное; технологическое; эксплуатационное; социальное; алгоритмическое [23, 34, 35, 63].

Для обеспечения надежности технических средств чаще всего производится:

● резервирование (дублирование) технических средств (компьютеров и их компонентов, сегментов сетей и т. д.);

● использование стандартных протоколов работы устройств ТКС;

● применение специализированных технических средств защиты информации.

Средствами защиты информации телекоммуникационных систем, в том числе систем электронных торгов являются технические, криптографические, программные и другие средства, предназначенное для защиты информации, средства, в котором оно реализовано, а также средство контроля эффективности защиты информации. Средства защиты информации делятся на: физические, аппаратные, программные, криптографические, и комбинированные. Подробно стандарты информационной безопасности для телекоммуникационных систем представлены в главе 3 данной работы.

1.3.3. Анализ методов и средств обеспечения аппаратурной надежности и информационной безопасности в телекоммуникационных сетях электронной коммерции

Повышение надежности заключается в предотвращении неисправностей, отказов и сбоев. Основным способом повышения готовности является избыточность, на основе которой реализуются различные варианты отказоустойчивых архитектур.

Для коммерческих предприятий безопасность является экономической категорией. В настоящее время разрабатываются комплексные подходы к информационной безопасности предприятия. Создаются концепции (политики) безопасности предприятия [8, 11, 25, 38, 40, 45]. В сети уязвимым являются сетевые протоколы и устройства, образующие сеть, ОС, базы данных и приложения. Методы и средства обеспечения надежности и информационной безопасности в телекоммуникационных сетях разделяются на организационные и программно-технические.

1. Организационные методы: управление персоналом, физическая защита, поддержание работоспособности, планирование восстановительных работ.

2. Программно-технические методы. Среди современных программно-технических методов повышения безопасности информации в телекоммуникационных сетях электронной коммерции можно выделить: правильная конфигурация узлов сети; рациональное применение методов резервирования; при проектировании сети нужно использовать элементы, обеспечивающие безопасность; использование отказоустойчивых компьютеров с отказоустойчивыми аппаратными компонентами; кластеризация компьютеров (обеспечивают коэффициент готовности до 0,999-high availability); дуплексированне и зеркальное отображение дисков (diskmirroring); автоматическое подключение (auto-reconnection); дублирование файловой системы; отслеживание транзакций (transactiontracking); использование межсетевых экранов и брандмауэров; идентификация и аутентификация; разграничение доступа; протоколирование и аудит; криптографическое преобразование данных.

1.4. Исследование методов и моделей оценки надежности корпоративных телекоммуникационных сетей

Проблема сетевой надежности исследуется достаточно давно. Точного решения даже для сетей ограниченного размера эта задача не имеет, но можно произвести оценку надежности сверху и снизу, но даже это требует достаточно сложных расчетов. Поэтому из-за сложности прямых вычислений многие исследователи ограничиваются лишь оценкой возможных границ надежности [47, 79, 81].

- Так как сети являются сильно связными структурами, то расчет их надежности *строго аналитическими методами* затруднен [3, 36, 40, 80]. Единственным *численным методом расчета надежности сильно связанных сетей является метод полного перебора*, который, даже с привлечением быстродействующих ЭВМ, не позволяет анализировать сети, содержащие более 50 случайных компонент, поэтому часто применяют *метод частичного перебора* [28].
- Иногда на практике надежность и распределения надежности определяются *эмпирически* [79, 81]

- Среди *методов вероятностного анализа сетей* используются *алгоритмические* и *логико-вероятностные методы* [24, 37, 56, 59, 79].

Из-за отсутствия приемлемой модели механизма потерь в сети и присущей сложности расчета используются *время-зависимые модели с дискретной вероятностью* [24, 46, 49].

- *Алгоритмы точного вычисления мер надежности* [79, 81]. Можно выделить следующие алгоритмы точного вычисления мер надежности: точные алгоритмы с экспоненциальным временем для общих сетей, и точные алгоритмы с полиномиальным временем для ограниченного класса сетей.
- *Методы структурной надежности сетей.* При исследовании структурной надежности сетей применяются следующие методы [79, 80]: точный метод анализа структурной надежности; приближенные методы - статистической оценки, разложения, двухсторонней оценки, метод сечений или совокупности путей.
- *Модели безотказности элемента. Экспоненциальное (показательное) распределение. Распределение Вейбулла. Усеченное нормальное распределение* [66, 59, 79].
- Простым и легко реализуемым методом повышения аппаратурной надежности корпоративных телекоммуникационных сетей является *резервирование.* Резервирование - это повышения надежности системы с помощью применения дополнительных средств. Существуют следующие виды резервирования: структурное, функциональное, временное, информационное (более подробно этот вопрос рассмотрен в главе 3 данной работы).

Существуют и другие методы и модели, используемых при решении задач обеспечения аппаратурной надежности сетей. Все эти методы и модели имеют свои преимущества и недостатки, что вызывает определенные ограничения на их применение при проектировании специализированных корпоративных телекоммуникационных сетей. Следовательно, разработка новых моделей и алгоритмов расчета аппаратурной надежности устройств таких сетей, с учетом имеющихся наработок в этой области, является актуальной научной задачей.

К моделям сетей предъявляются следующие основные требования – это

универсальность, точность, адекватность и экономичность [72, 75, 106]. Кроме того, при расчете аппаратурной надежности корпоративных телекоммуникационных сетей следует учитывать и целый ряд требований к моделям таких сетей и их элементов: экономичность, наглядность; обладать вычислимостью, т.е. возможностью исследования качественных и количественных закономерностей функционирования сети; алгоритмизуемость - возможность разработки алгоритмов и программы, реализующей модель на ЭВМ, причем алгоритм решения задачи на ЭВМ связан.

1.5. Анализ современных систем оценки надежности и защиты информации

1.5.1. Программные комплексы для расчета надежности

В России и за рубежом проблемой оценки надежности систем, сетей и средств вычислительной техники занималось значительное количество научно-технологических центров и оргазиций, результатом их деятельности стало создание программно-инструментальных комплексов. Однако, большинство таких систем довольно сложные и дорогие [59, 79, 82, 86, 99].

Среди современных программных средств, предназначенные для анализа и расчета надежности, готовности и ремонтопригодности можно выделить отечественные и зарубежные системы: АРБИТР, АРМ Надежности, АСОНИКА-К, AnyGraph, CRISS, AggreGateNetworkManager, BlockSim, ITEMSoftware, ReliabilityWorkbench, Windchill.

Например, AnyGraphсоздана для упрощения разработки системных моделей используемых при расчете надежности сложных технических систем и их анализ. Теоретической основой программного обеспечения (ПО) AnyGraph являются логико-вероятностные методы (ЛВМ) моделирования. Базовой концепцией ПО является представление модели как набора взаимодействующих между собой узлов (технических элементов) и логических связей между ними. Построенная с помощью графического редактора ПО AnyGraph модель имеет высокую наглядность.

Система AggreGateNetworkManager осуществляет мониторинг элементов сети. Проверяется показатель доступности, характеризующий основное

состояние контролируемого элемента сети при помощи стандартных процедур, таких как пинг сетевого устройства или соединение с сервисом через указанный порт. Мониторинг работоспособности сетевого элемента заключается в комплексной проверке, гарантирующей, что управляемый элемент не «работает должным образом».

1.5.2. Системы защиты информации

На рынке защиты информации предлагается много отдельных инженерно-технических, программно-аппаратных, криптографических средств защиты информации [5, 16, 54, 83, 102].

- Разработка фирмы «ИМПУЛЬС-ИВЦ» - программа «ИМПУЛЬС. Программный продукт позволяет предотвратить утечки конфиденциальных данных из информационной системы организации. Результат - выявление фактов нарушения конфиденциальности; консолидация собранной информации в централизованном хранилище данных; формирование статистической отчетности с возможностью группировки по различным параметрам, для выявления случаев нарушения установленных правил работы в сети организации; выявление случаев нецелевого использования, фактов изменения пользователями, установки или удаления ими программного обеспечения.
- Разработки компания Zecurion — ведущий российский разработчик DLP-систем для защиты от утечек информации. Например, ZecurionZgate анализирует все данные, передаваемые сотрудниками за пределы локальной сети, и блокирует утечки конфиденциальной информации через корпоративную почту, социальные сети, форумы, интернет-пейджеры, веб-почту, FTP-ресурсы.
- Система защиты информации SecretNet, разработанная ЗАО НИП «Информзащита», имеет широкие возможности по управлению полномочиями

пользователей, существенно дополняя возможности замка «Соболь» по защите от НСД.

- SecretDisk фирмы «Аладдин» создает в компьютере «секретные» логические диски, при сохранении информации на которых она автоматически шифруется в «прозрачном» режиме. Чтобы получить доступ к такому диску, необходимо подключить электронный ключ и набрать пароль.
- Государственные организации успешно применяют средства защиты информации компании «Код Безопасности». Эти разработки обладают всеми необходимыми сертификатами (ФСБ и ФСТЭК России), чтобы обеспечить защиту и сделать возможной аттестацию автоматизированных систем любой категории: защита конфиденциальной информации, защита персональных данных, защита государственной тайны. Например, продукт – vGate – позволяет государственным организациям внедрять современные технологии виртуализации в системах, обрабатывающих информацию ограниченного доступа, и тестировать их по требованиям ФСТЭК России.
- КриптоПро CSP — криптографический проект компании «Крипто-Про».
- Крипто-КОМ — криптографический проект компании ЗАО «Сигнал-КОМ».

И многие другие.

1.6. Формализация постановки задачи

В формализованном виде решение научной задачи, представляет собой тройку:

$$Z_{задача} = <X_{сеть}, F_{метод}, Y^{ND}>. \quad (1.1)$$

где $X_{сеть}$ - объект исследования, Y^{ND}- требуемый научный результат, $F_{метод}$ - методы исследования.

Объектом исследования являются корпоративные телекоммуникационные сети, используемые в электронной коммерции. Объект исследования это множество:

$$X_{сеть} = \{ M_{СЕТИ}, K, X_{pr}, OGR \}, \quad (1.2)$$

где $M_{СЕТИ}$ – модель сети расчета аппаратурной надежности; K - критерии эффективности работы телекоммуникационных сетей (см.п.1.1 данной главы); X_{pr} - параметры сети; OGR – ограничения, указанные в ТЗ на разработку для каждой конкретной сети.

Свойства параметров: независимость, допустимость, ограниченность. Единицы измерения X_{pr} - стандартные (система СИ), а также булевые и безразмерные величины.

Предметом исследования являются методы и модели оценки и оптимизации аппаратурной надежности сетей и защиты коммерческой информации ЭТП в сетях телекоммуникаций.

Методы исследования $F^*_{метод}$ определяются сущностью поставленных теоретических и практических задач.

Требуемый научный результат Y^{ND} – это выходные параметры, при которых обеспечивается надежная передача и защита коммерческой информации ЭТП в телекоммуникационных сетях. Формула обеспечения надежной передачи и защиты коммерческой информации электронной торговой площадки в телекоммуникационных сетях представляется следующим образом:

Методы обеспечения надежности телекоммуникационной сети электронной коммерции + Методы обеспечения защиты коммерческой информации ⇒ Надежная передача и защита коммерческой информации ЭТП

Скорость канала передачи данных, предоставленного для доступа в Интернет, должна быть не менее 1 Гбит/с; на физическом уровне указанный канал связи должен обеспечивать средний показатель безотказной передачи данных не хуже девяноста девяти целых девяносто пяти сотых процента 99,95% в течение непрерывного 24-х часового периода, а вероятность ошибки одиночного символа в канале не превышает $1x10^{-10}$. Критерии, по которым

предоставленный канал считается действующим или недействующим, соответствуют Рек. G.821 ITU-T. Модели и алгоритмы расчета аппаратурной надежности телекоммуникационных сетей электронной коммерции представлены в главе 2. ТКС Оператора должна соответствовать требованиям Руководящего документа Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» исходя из того, что класс защищенности ТКС не может быть менее уровня «1Г». Стандарты информационной безопасности и методы защиты коммерческой информации представлены в главе 3 диссертационной работы.

Схема решения поставленной научной задачи представлена на рис. 1.2.

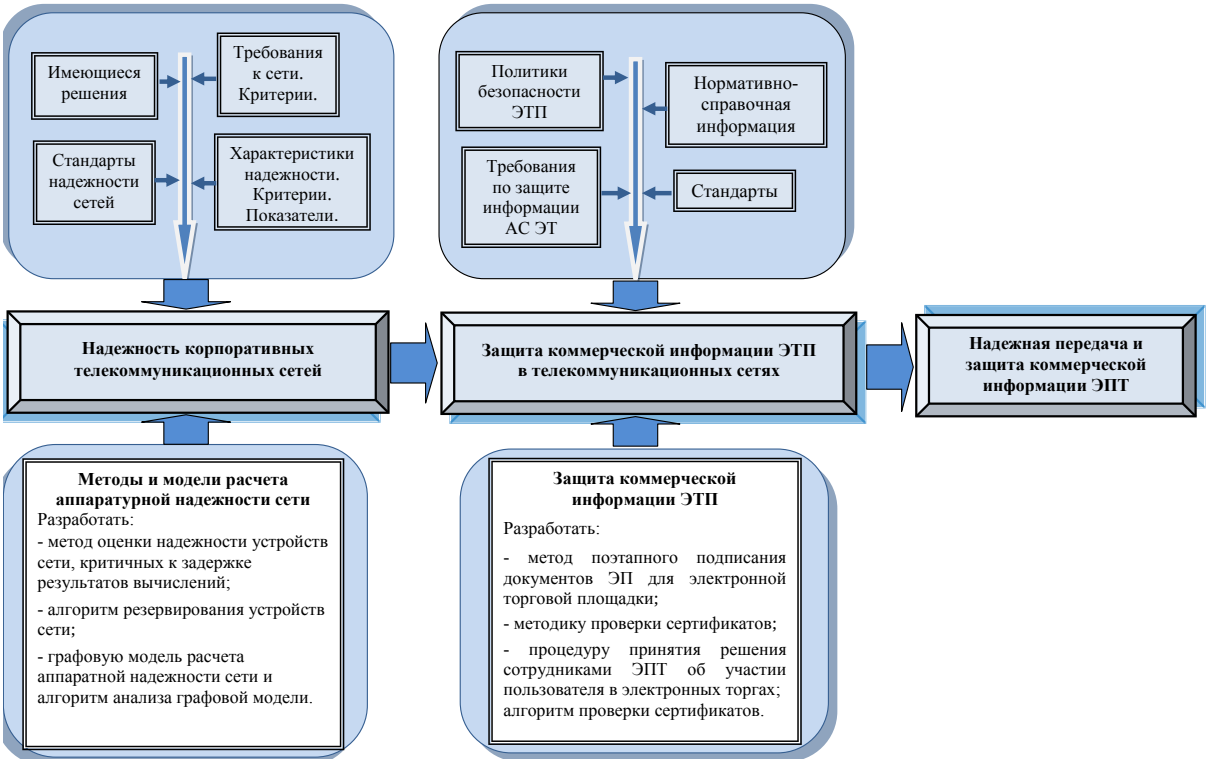

Рис.1.2 – Схема решение поставленной научной задачи

Проведенное исследование позволяет сделать вывод о том, что расчет аппаратурной надежности корпоративных телекоммуникационных сетей

целесообразно проводить с помощью процедуры декомпозиции. В диссертационной работе рассматривается аппаратурная (элементарная) надежность корпоративных телекоммуникационных сетей.

Между показателями производительности и надежности сети существует тесная связь. Ненадежная работа сети часто приводит к снижению ее производительности. Это объясняется тем, что сбои и отказы каналов связи и коммуникационного оборудования приводят к потере или искажению некоторой части информации, в результате чего коммуникационные протоколы вынуждены организовывать повторную передачу данных.

ВЫВОДЫ К ГЛАВЕ 1

1. Электронная коммерция объединяет множество коммуникационных технологий. Самой распространенной, простой и удобной формой применения систем электронной торговли являются электронные торговые площадки (ЭТП). Рассмотрены функции, возможности и преимущества работы на ЭТП для заказчика и для компании, представлены примеры федеральных и коммерческих торговых площадок. Проанализированы существующие способы обеспечение надежности функционирования телекоммуникационных систем электронных торгов. Показано, что системы электронных торгов переходят с уровня электронных торговых площадок на уровень полномасштабных систем управления торгово-закупочной детальностью с использованием телекоммуникационных сетей, следовательно, основой электронной коммерции являются телекоммуникационные сети.

2. Проанализированы особенности использования телекоммуникационных сетей в электронной коммерции. Приведены основные критерии эффективности работы сетей. Показано, что к таким сетям предъявляются повышенные требования к надежности передачи и защите информации. Исследованы источники ненадежности сетей. Определены характеристики, показатели и критерии аппаратурной надежности телекоммуникационных сетей электронной коммерции. Показано, что для

оценки надежности сетей необходимо выбрать частные аспекты – аппаратурную (элементарную) и функциональную (структурную) надёжности.

3. Проведен анализ методов и средств обеспечения информационной безопасности в телекоммуникационных сетях электронной коммерции. Исследованы методы и модели оценки надежности таких сетей. Определены требования, предъявляемые к моделям – это универсальность, точность, адекватность, экономичность, экономичность, наглядность, вычислимость, алгоритмизуемость. Проведенное исследование показало, что методы и модели имеют свои достоинства и недостатки, что вызывает определенные ограничения на их применение при проектировании специализированных корпоративных телекоммуникационных сетей. Следовательно, разработка новых моделей и алгоритмов расчета аппаратурной надежности устройств таких сетей, с учетом имеющихся наработок в этой области, является актуальной научной задачей.

4. Проанализированы и исследованы современные системы оценки надежности и защиты информации, как российские, так и зарубежные. Как показало исследование, большинство таких систем являются сложными и дорогостоящими.

5. Дана формализация постановки задачи. Представлена формула обеспечения надежной передачи и защиты коммерческой информации электронной торговой площадки в телекоммуникационных сетях, которая включает методы и модели обеспечения надежности телекоммуникационной сети электронной коммерции и методы обеспечения защиты коммерческой информации.

ГЛАВА 2. МЕТОДЫ И МОДЕЛИ ОЦЕНКИ АППАРАТУРНОЙ НАДЕЖНОСТИ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ КАК СЛОЖНОЙ ИЕРАРХИЧЕСКОЙ СИСТЕМЫ

2.1. Вероятность безотказной работы сетевых элементов

В настоящее время проблема надежности сетей становится все более актуальной. Первые разработки в области систем повышенной аппаратурной надежности проводились для сетей, где отказ мог повлечь катастрофы, например при управлении ядерными реакторами и оборонными комплексами. В ряде промышленных отраслей с экономической точки зрения также становится выгодно применять сети повышенной аппаратурной надежности.

С ростом масштабов корпоративных телекоммуникационных сетей резко увеличилось количество узлов, работающих без постоянного присутствия персонала [65, 68, 70]. В таких условиях вероятность отказа узла и линейного тракта становятся соизмеримыми, а локализация неисправного узла является весьма проблематичной, при этом причиной отказа узлов может быть выход из строя блоков питания сетевого оборудования.

Аппаратурная сетевая надежность содержит ряд аспектов, касающихся проектирования и анализа сетей и зависит от случайных отказов сетевых элементов. Аппаратурная надежность телекоммуникационной сети, как и всякой системы, определяется надежностью составляющих ее элементов, поэтому следует оценивать надежность телекоммуникационной корпоративной сети – как сложной иерархической системы. Здесь элементом может считаться сервер, рабочая станция, оборудование ЭТП, терминал, канал связи и т.д.. В то же время, рассматривая функционирование рабочей станции, можно выделить процессор, устройства ввода/вывода, различные интерфейсы.

Расчеты надежности необходимо производить на стадии технического проектирования, когда уже более детально известны состав сети, ее структура и принципы функционирования, позволяющие проверить правильность принятых проектных решений, найти «слабые места» и выработать

определенные рекомендации по повышению надежности и эффективности ее функционирования.

Особенностью математических моделей надежности сетей является то, что эти модели имеют дело с вероятностными процессами и используют в качестве исходных данных достаточно недостоверную статистику, а иногда эта статистика вообще отсутствует. Первое относится, как правило, к данным по надежности, а второе – к информации о потоках в сетях, об интенсивности межабонентской связи, о параметрах пропускной способности, надежности передачи и т.д. Создание математических моделей направлено на количественную оценку уровня надежности и эффективности функционирования сетей. Если не всегда можно с полным основанием доверять абсолютным значениям вычисленных априорно или оцененных статически тех или иных показателей надежности, то для сравнительного анализа надежности различных вариантов построения или использования сетей, математические методы расчета надежности могут быть очень важны [68, 81, 95]. Расчеты аппаратурной надежности приносят большую пользу на ранних этапах проектирования, когда возникает вопрос о сравнении различных возможных вариантов построения корпоративной сети. Расчетные методы определения надежности дают возможность обоснованно планировать и прогнозировать стратегию модернизации и развития сети.

Вероятность безотказной работы какого-либо элемента телекоммуникационной сети можно записать в виде

$$P_T(x) = P_1(y_1)P_1(y_2 \mid y_1)...P_m(y_m,..., y_{m-1}), \qquad (2.1)$$

где $P_j(y_j)$- безусловная вероятность выполнения *j*-го условия работоспособности; *x* – входные параметры; *y* – выходные параметры элемента сети; $P_T(y_k \mid y_1,...., y_{k-1})$ - условная вероятность выполнения *к*-го условия работоспособности [95, 101].

Вероятность $P_T(X)$ также можно представить как математическое ожидание некоторого функционала, для выходных параметров*Y*(*X*) на заданном интервале времени функционирования элемента *T*с учетом*Y(x(t))* - номинальных значений его выходных параметров [78, 95].

Обозначим через Y_{jmin} минимальное значение j-го выходного параметра элемента на интервале времени [0, T]*:*

$$Y_{j\min} = \min_{t\in[0,T]} Y_j(x(t)), \qquad j = 1,\ldots, n \tag{2.2}$$

Величина Y_{jmin} является случайной с плотностью распределения $\Phi_j(Y)$ [95], которая в общем случае определяется номинальными значениями параметров элементов, законами распределения этих параметров во времени, видом функциональной зависимости $Y_j(x(t))$ и величиной интервала времени.

Совокупность номинальных значений параметров элементов сети представляет допустимое решение, если соответствующий вектор принадлежит области допустимой вариации его параметров. Вследствие действия различных дестабилизирующих факторов (износ, температура, влажность и т.д.) реальные значения параметров сетевых элементов отличаются от номинальных (расчетных). Это характерно для специальных сетей. При эксплуатации эти отклонения определяются условиями работы. Поскольку значения параметров элементов сети являются случайными, то условия их работоспособности могут выполняться не абсолютно, а с той или иной вероятностью [24, 43, 95].

Тогда вероятность выполнения j-го условия работоспособности элемента сети можно записать в виде:

$$P_j(y_j(x)) = \int_{a_j}^{a_m} \Phi_j(y)dy, \tag{2.3}$$

где $\Phi_j(y)$ - плотность распределения величины Y_j; $(a_1,\ldots,a_m)$ область работоспособности [43, 95].

Вероятность безотказной работы i-го элемента сети

$$P_{Ti} = \prod_{j=1}^{H} P_j(y_j(x)) \tag{2.4}$$

Для локальных критериев аппаратурной надежности телекоммуникационной сети, среди которых существуют противоречивые и несводимые один к другому, условия работоспособности элементов определяются с помощью неравенства:

$$y_j(x+\Delta x) \geq y_j(x), \qquad j=1,\ldots,m\,. \tag{2.5}$$

Случайные величины Y_j могут представлять собой значения выходных параметров элементов в момент времени t=0. Введение случайных величин при определении параметрической надежности (это вероятность безотказной работы элемента по постепенным отказам на заданном интервале времени $[0,T]$) дает возможность перейти от рассмотрения случайных функций (процессов) к рассмотрению случайных величинY_j и существенно упростить проблему оптимизации параметрической надежности и ее решение, за счет возможности унифицировать запись и способ вычисления показателей надежности.

Коэффициент аппаратурной готовности сети можно вычислить по формуле:

$$K_{\text{гот}} = \prod_{i=1}^{H} P_{Ti}\,, \tag{2.6}$$

где H- число элементов сети (с учетом необходимой степени детализации сетевых элементов в каждом конкретном случае); P_{Ti} - вероятность того, что i-й элемент сети находится в рабочем состоянии.

2.2. Оценка надежности устройств сети, критичных к задержке результатов вычислений

К настоящему времени остаются недостаточно изученными методы оценки надежности устройств, критичных к задержке результатов вычислений. Это проявляется в недопустимости ожидания запросов в очереди и невозможности возобновления вычислительного процесса после возникновения отказов. Решение подобных задач является актуальным для корпоративных телекоммуникационных сетей электронной коммерции.

Пусть устройство, например сервер, или любой другой узел/элемент сети (ЭТП) может выходить из строя либо при обслуживании заявок, либо в

свободном состоянии, либо как в том, так и в другом состоянии. Во многих случаях согласование с реальной ситуацией дает предположение о том, что устройство выходит из строя случайно за время *t*. Это может вызвать крайне нежелательные последствия для функционирования электронно-торговой площадки при использовании телекоммуникационных сетей в электронной коммерции.

Предположим, что такой элемент сети может выйти из строя только тогда, когда он не занято обслуживанием заявок. Если в момент *t* закончился его период занятости и до момента $t+\Delta t$ другие заявки не поступили, то за это время устройство может выйти из строя с вероятностью [77, 78, 95]: $P_0(t) = \int_0^{t+\Delta t} s(t)dt$, где *s* – состояние аппаратурной неисправности (отказа) устройства.

Время восстановления можно предположить случайной величиной с функцией распределения $R_0(t)$ и конечным математическим ожиданием для случайного процесса $s(t) = \{l(t), \gamma(t)\}$. Первая компонента этого процесса *l(t)* может принимать только два значения: 0 и 1. Если *l(t)=0*, то в момент *t* узел (устройство) находится в исправном состоянии. Если же в момент *t* он находится в неисправном состоянии или занят обслуживанием требования, то *l(t)*=1.

Вторая компонента *γ(t)* имеет различный физический смысл в зависимости от того, равна первая компонента 0или 1. В первом случае γ(*t)* это время с момента *t* до момента выхода бы из строя, если после *t* поток заявок прекратится; во втором случае *γ(t)* - время с момента *t* до того момента, когда устройство начнет обслуживание заявок, если бы они поступили в момент *t.*

Обозначим:

$$F_i(x,t) = \sum_{i=0}^{n} f(s_i(t)), \qquad F_i(x) = \lim_{t\to\infty} F_i(x,t). \tag{2.7}$$

Случайный процесс *s*(*t)* обладает эргодическим распределением [77, 95] и $F_i(x)$ удовлетворяют системе интегро-дифференциальных уравнений:

$$F_0(x,t) - F_0(x) + F_0(x)F_0(x,t) = P_0(t), \tag{2.8}$$

$$F_i(x,t) - F_i(x) + \int_0^{t+\Delta t} F_0(x,t)dF_0(x) + R_0(t)F_0(x,t) = P_i(t), \qquad (2.9)$$

с дополнительным условием

$$F_0(\infty) + F_i(\infty) = 1, \qquad F_0(0) = F_i(0) = 0. \qquad (2.10)$$

Примем, что t_0 - момент окончания некоторого периода занятости и T - длительность следующего периода занятости (под периодом занятости следует понимать такой интервал времени, в начале и в конце которого $l(t)=0$, а для всех t из этого интервала $l(t)\neq 0$).

Возможны два взаимно исключающих друг друга случая:

1) после момента t_0 поступит заявка, причем устройство до этого еще не выйдет из строя;

2) устройство выйдет из строя раньше, чем поступит заявка.

Вероятности, с которыми осуществится первый и второй случаи, равны соответственно:

$$\int_0^{t+\Delta t} e^{-t}[1 - P_0(t)]dt \quad \text{и} \quad \int_0^{t+\Delta t} e^{-t} P_0(t)dt. \qquad (2.11)$$

Следовательно,

$$MO = \int_0^{t+\Delta t} e^{-t}[1 - P_0(t)]dtMO_1, \qquad (2.12)$$

$$MO = \int_0^{t+\Delta t} e^{-t} P_0(t)dtMO_2, \qquad (2.14)$$

где MO - математическое ожидание при условии, что осуществился 1-й или 2-й случай (i=1 или 2).

MO_1 совпадает с математическим ожиданием периода занятости, в котором устройство находится в рабочем состоянии:

$$MO_1 = \frac{T}{1-\rho}, \qquad (2.15)$$

где ρ - загрузка этого узла, которую можно определить, как показано в работах [78, 95].

Величина MO_2 равна

$$MO_2 = \sum_{n=0}^{\infty} p_n MO_n \ , \tag{2.16}$$

где p_n - вероятность того, что за время восстановления поступит ровно n заявок, MO_n равно сумме математического ожидания времени восстановления и математического ожидания n периодов занятости для устройства, не выходящего из строя.

Таким образом:

$$\begin{aligned} MO_2 &= \sum_{n=0}^{\infty}(t_0 + \frac{nT}{1-\rho}) \int_0^{t+\Delta t} \frac{t^n}{n!} e^{-t} dR_0(t) = \int_0^{t+\Delta t} (\sum_{n=0}^{\infty}(t_0 + \frac{nT}{1-\rho}) \frac{t^n}{n!}) e^{-t} dR_0(t) = \\ &= \int_0^{t+\Delta t} (t_0 e^t + \frac{T}{1-\rho}) e^{-t} dR_0(t) = \int_0^{t+\Delta t} (T + \frac{T}{1-\rho}) dR_0(t) = t_0(1 + \frac{\rho}{1-\rho}) = \frac{t_0}{1-\rho} \end{aligned} \tag{2.17}$$

Окончательно можно получить:

$$MO = \frac{T}{1-\rho} + \frac{t_0 - T}{1-\rho} \int_0^{t+\Delta t} e^{-t} P_0(t) dt \le \frac{1}{1-\rho} \max(T, t_0) < \infty . \tag{2.18}$$

Процесс *s(t)* является регенерирующим процессом [95], моментами регенерации этого процесса будут те моменты времени t_n, когда $l(t_n\text{-}0)$=l, $l(t_n\text{+}0)$=0. Интервал $t_{n+1}\text{-}t_n$ между двумя последовательными моментами регенерации складывается из времени до первого отказа или поступления заявки (в зависимости от того, что произойдет раньше) и последующего периода занятости. Значит,

$$MO_n = \int_0^{\infty} e^{-t}(1 - P_0(t)) dt + \frac{T}{1-\rho} + \frac{t_0 + T}{1-\rho} \int_0^{\infty} e^{-t} P_0(t) dt < \infty . \tag{2.19}$$

Это условия применимости эргодической теоремы для регенерирующих процессов и, следовательно, можно заключить, что случайный процесс *s(t)* обладает эргодическим распределением [77, 95]. Эргодическое распределение удовлетворяет системе интегро-дифференциальных уравнений (2.8) - (2.9) с условиями (2.10).

Для процесса $s(t)=\{l(t), \gamma(t)\}$ характерны следующие свойства [95]:

- вторая компонента $\gamma(t)$ непрерывно убывает со скоростью, равной 1 ($\gamma(t)$ всегда означает время с момента t до момента окончания некоторого события); когда период занятости заканчивается, то $\gamma(t)$ принимает значение, равное времени до следующего отказа (неисправности);
- для первой компоненты процесса $s(t)$ закон ее изменения определяется из этой случайной величины.

Следовательно, что если x - точка, в которой функции $F_0(x)$, $F_i(x)$, $F_i(x,t)$, $F_0(x,t)$, $P_0(t)$ и $R_0(t)$ имеют производные, то справедливы формулы [77, 95]:

$$F_0(t) = (F_0(x) - F_0(x,t))(1 - P_0(t)) + F_0(x,t)P_0(t) + P(t), \qquad (2.20)$$

$$F_i(t) = (F_i(x) - F_i(x,t))(1 - P_0(t)) + t\int_0^{t+\Delta t} F_i(x,t)dF_i(t) + P_0(t)R_0(t) + F_0(\infty)P(t) + P(t)$$

переходящие при $t \to 0$ в уравнения (2.8) и (2.9).

Когда устройство предполагался абсолютно надежным, устанавливается абсолютная непрерывность функций $F_0(t)$ и$F_i(t)$ и значит, выведенные уравнения можно решать, используя обычные правила для преобразования Лапласа [95].

Необходимо ввести следующие обозначения:

$$\Phi_i(s) = \int_0^{\infty} e^{-t} F_i(t)dt, \qquad (i = 1,2);$$

$$\Delta_0(s) = \int_0^{\infty} e^{-t} P_0(t)dt; \qquad P_0(s) = \int_0^{\infty} e^{-t} dR_0(t); \qquad q(s) = \int_0^{\infty} e^{-t} dF_0(t),$$

Применив к обеим частям уравнений (2.8) и (2.9) преобразование Лапласа, получим:

$$\Phi_0(s)(1 - \frac{T}{P_0(s_i)}) + F_i(t)\frac{\Delta_0(s_i)}{h(s_i)} = \frac{F_0(t)}{P_0(s_i)}, \qquad (2.21)$$

$$\Phi_i(s)\left(1 - \frac{T}{P_0(s_i)} + \frac{h(s_i)}{\Delta_0(s_i)}\right) + F_i(t)\frac{P_0(s_i)}{h(s_i)} + F_0(\infty)\frac{h(s_i)}{\Delta_0(s_i)} = \frac{F_0(t)}{\Delta_0(s_i)}, \qquad (2.22)$$

или

$$\Phi_0(s) = \frac{F_0(t) - F_i(t)\Delta_0(s_i)}{1 - P_0(s_i)}, \qquad (2.23)$$

$$\Phi_i(s) = \frac{F_i(t) - F_0(t)h(s_i) - F_0(\infty)\Delta_0(s_i)}{P_0(s_i) - (1 - P_0(s_i))}. \quad (2.24)$$

Уравнения (2.23) - (2.24) определяются преобразованиями Лапласа-Стилтьеса функций $F_0(t)$ и $F_i(t)$. Левая часть равенства (2.12) определяет аналитическую функцию в полуплоскости $Re\{s_i\}>0$ [95]. Следовательно, в точке, где знаменатель правой части этого равенства обращается в нуль, должен обратиться в нуль и числитель. Отсюда справедливо соотношение

$$F_0(t) = \Delta_0(s_i)F_i(t). \quad (2.25)$$

Левая часть равенства (2.24) ограничена при $Re\{s_i\}>0$. Знаменатель правой части при $s_i=0$ обращается в нуль. Условие равенства нулю в этой точке для числителя правой части:

$$F_i(t) - F_0(t) = \Delta_0(s_i)F_0(\infty). \quad (2.26)$$

Из уравнений (2.25) и (2.26) можно выразить $F_0(t)$ и $F_i(t)$ через одну неизвестную постоянную $F_0(\infty)$: $F_0(t) = \frac{\Delta_0(s_i)F_0(\infty)}{1-\Delta_0(s_i)}$; $F_i(t) = \frac{F_0(\infty)}{1-\Delta_0(s_i)}$.

Подставив эти соотношения в (2.23) и (2.24):

$$\Phi_0(s) = \frac{q(s)(\Delta_0(s) - \Delta_0(s))F_0(\infty)}{q(s)(1-\Delta_0(s))}, \quad (2.27)$$

$$\Phi_i(s) = q(s_i)\frac{1 - q(s_i) + \Delta_0(s_i)(q(s_i) - P_0(s_i))}{(q(s_i)(1-\Delta_0(s_i)))(1-\Delta_0(s_i))}F_0(\infty). \quad (2.28)$$

При условии (2.10), из которого следует, что $\Phi_0(0)+\Phi_i(0)=1$, в окрестности нуля преобразования Лапласа-Стилтьеса распределения $R_0(t)$ допускают разложение $q(s_i) = 1 - T + \Delta_0(s_i)$, $P_0(s_i) = 1 - t_0 + \Delta_0(s_i)$. Если подставить эти соотношения в два равенства и перейти к пределу при$s\to 0$, то:

$$\Phi_0(0) = F_0(\infty), \quad \Phi_i(0) = \frac{T + \Delta_0(s_i)(t_0 - T)}{(1-\rho)(1-\Delta_0(s_i))}F_0(\infty), \quad (2.29)$$

Из условия (2.10) следует равенство

$$\left(1+\frac{T+\Delta_0(s_i)(t_0-T)}{(1-\rho)(1-\Delta_0(s_i))}\right)F_0(\infty)=1 \text{ или } F_0(\infty)=\frac{(1-\rho)(1-\Delta_0(s_i))}{1-\Delta_0(s_i)(1-t_0)}. \quad (2.30)$$

Окончательно подстановка в формулы (2.27) и (2.28) дает:

$$\Phi_0(s)=\frac{(1-\rho)(\Delta_0(s_i)-\Delta_0(s_i))}{T(1-\Delta_0(s_i)(1-t_0))}, \quad (2.31)$$

$$\Phi_i(s)=\frac{(1-\rho)(1-q(s_i)+\Delta_0(s_i)(q(s_i)-P_0(s_i)))}{T(1-q(s_i))(1-\Delta_0(s_i)(1-t_0))}. \quad (2.32)$$

Таким образом, найден вид преобразований Лапласа - Стилтьеса распределения случайного процесса *s(t).*

Следовательно

$$\Phi(s)=\Phi_0(s)+\Phi_i(s). \quad (2.33)$$

Если во время обслуживания заявок пользователей рассматриваемый сетевой элемент (устройство) может выйти из строя за время t. В момент t_0 началось обслуживание заявок. Через Δt можно обозначить время от момента t_0 до того момента, когда оно будет способно к обслуживанию следующей заявки. Время Δt может состоять из времени обслуживания заявок, поступивших на обслуживание в момент t_0; если же устройство за это время вышло из строя n раз, то Δt будет состоять из времени обслуживания и n времени его восстановления. Время восстановления является случайной величиной с функцией распределения $R_1(t)$. Тогда формула вероятности того, что оно будет неисправно:

$$P_0(t)=\sum_{n=0}^{\infty}\int_0^{t_0+\Delta t} R_1^{(n)}(t_0+\Delta t)R_1(t)\frac{(f(s))^n}{n!}e^{-t}, \quad (2.34)$$

где $R_1^{(n)}(t_0+\Delta t)$ - функция распределения суммы n независимых случайных величин.

Если под временем обслуживания понимать случайную величину *T'*, то время ожидания произвольной заявки будет определяться формулами (2.31) -

(2.32), в которых q(s) заменена преобразованием Лапласа-Стилтьеса $q_{T'}(s)$ случайной величины T', тогда

$$q_{T'}(s) = \int_0^{\infty} e^{-T'} dF_0(T') \{ \sum_{n=0}^{\infty} \int_0^{t_0+\Delta t} R_1^{(n)}(t_0 + \Delta t) R_1(t) \frac{(f(s))^n}{n!} e^{-t} \} dt . \quad (2.35)$$

Для условия, при котором, случайный процесс $s(t)$ обладает эргодическим распределением необходимо вычислить математическое ожидание случайной величины T:

$$MO = (1 - \frac{T}{1-\rho}) + \frac{t_0 - T'}{1-\rho} \int_0^{t_0+\Delta t} e^{-T'} P_0(t) dt + \frac{1}{1-\rho} . \quad (2.36)$$

Условием эргодичности процесса $\bar{s}(t)$ является неравенство [78, 95]:

$$\int_0^{t_0+\Delta t} e^{-T'} (1 - P_0(t)) dt + \frac{t_0 - T'}{1-\rho} q_{T'}(s_i) \le \int_0^{\infty} e^{-T'} (1 - P_0(t)) dt + \Phi(s) . \quad (2.37)$$

Следовательно, при некоторых значениях параметров процесс, обладающий эргодическим распределением при абсолютно надежном устройстве, теряет это свойство, когда оно подвержено случайным (или неслучайным) поломкам. Разработанный метод расчета надежности устройств телекоммуникационных сетей электронной коммерции, критичных к задержке результатов вычислений, позволяет определить и прогнозировать вероятность выхода из строя узла/элемента сети (а также и ЭТП), как при обслуживании заявок электронной торговой площадки, так и в свободном состоянии. С учетом этого необходимо обеспечить надежную передачу коммерческой информации ЭТП по телекоммуникационным сетям, применив еще более существенные меры по повышению надежности сетей, например дополнительное резервирование, которое должно быть оптимальным (рациональным).

2.4. Алгоритм резервирования устройств сети

Одним из эффективных и достаточно просто реализуемых методов

повышения аппаратурной надежности корпоративных телекоммуникационных сетей, и в том числе для сетей электронной коммерции, является резервирование/дублирование или избыточность. Существует множество работ отечественных и зарубежных авторов, посвященных этой проблеме [68, 73, 81, 95]. Резерв может находиться в таком же режиме, что и основные элементы, а может находиться в запасе. В первом случае говорят о нагруженном, а во втором – о ненагруженном резерве. Существует и промежуточный случай – облегченный резерв [68, 95]. Резервирование является простым и эффективным методом повышения аппаратурной надежности телекоммуникационной сети, но не всегда оптимальным (рациональным). Например, дублирующий маршрутизатор остается пассивным до выхода основного из строя, но это не дешевое решение [68].

Следовательно, при резервировании, возникает задача не только обеспечить заданные показатели надежности, но и добиться этого как можно более экономично, с наименьшими суммарными затратами на резервные элементы, либо при заданных ресурсных ограничениях достичь максимально возможной аппаратурной надежности всей сети [81, 95]. Обычно для этого удается выделить одну наиболее важную характеристику надежности, которую для краткости можно назвать «стоимостью» вне зависимости от ее физической сущности, но на практике чаще своего встречаются ситуации, когда ограничения накладываются по нескольким ресурсам [68, 95].

Выделяют несколько видов резервирования: структурное, временное, информационное, функциональное и другие.

Для случая, когда показатель аппаратурной надежности телекоммуникационной сети выражается в виде произведения соответствующих показателей надежности отдельных резервных групп (элементов) можно записать:

$$P(x_1, x_2, ..., x_m) = \prod_{1 \le i \le m} P_i(x_i), \qquad (2.38)$$

где $P_i(x_i)$ - вероятность безотказной работы i-й резервной группы при наличии резерва x_i.

Если аппаратурная надежность сети высока, то

$$ND(x_1, x_2,..., x_m) << 1. \qquad (2.39)$$

Обычно в задачах резервирования предполагается, что стоимость резервов для сети в целом, $C(x_1, x_2,..., x_m)$ определяется как

$$nC(x_1, x_2,..., x_m) = \sum_{1 \le i \le m} C_i(x_i). \qquad (2.40)$$

Стоимость резерва *i*-й резервной группы:

$$C(x_i) = c_i x_i, \qquad (2.41)$$

где c_i – стоимость одного элемента *i*-го типа.

При этом возможны постановки двух следующих условий резервирования [68, 95].

1. Раздельным резервированием части сети, состоящей из *m* резервных групп, добиться того, чтобы показатель надежности был не, менее заданного ND_0 при минимально возможной стоимости резерва в целом:

$$\min_x \{C(x_1, x_2,..., x_m) \mid P(x_1, x_2,..., x_m) \ge ND_0 \qquad (2.42)$$

2. Раздельным резервированием части сети, состоящей из *m* резервных групп, добиться того, чтобы при максимально возможном показателе надежности стоимость всего резерва не превысила заданного значения C_0 [68, 95]:

$$\min_x \{P(x_1, x_2,..., x_m) \mid C(x_1, x_2,..., x_m)\} \ge C_0 \qquad (2.43)$$

Как правило, исходные данные задачи оптимизации аппаратурной надежности сетевых элементов не отличаются точностью и достоверностью, поэтому использование строгих методов дискретной оптимизации является с практической точки зрения некорректным. Здесь оправданно применение приближенных алгоритмов, например, метода наискорейшего

покоординатного спуска [28]. В [95] и других известных работах предложены методы оптимизации надежности резервирования такие как - метод динамического программирования, метод универсальных производящих функций и т.д. Однако, для всех этих методов характерно, что каждый элемент характеризуется обязательным возрастанием показателя надежности при росте суммарных затрат.

Процесс создания оптимальной резервированной системы, т.е. какого-либо участка (или элемента) сети можно представить в виде многошагового процесса. На первом шаге определяется такая подсистема, добавление к которой одного резервного элемента дает наибольший «удельный» выигрыш в приросте показателя аппаратурной надежности сети в целом. На втором шаге определяется следующая подсистема (включая и ту, к которой только что был добавлен резервный элемент), которая характеризуется тем, что добавление к ней одного резервного элемента дает опять наибольшее относительное приращение результирующего показателя надежности. Аналогичным образом процесс построения оптимальной системы продолжается далее [68].

Можно допустить, что на некотором N-м шаге построенного таким образом процесса каждая i-я подсистема уже имеет по $x_i^{(N)}$ резервов, и на каждом шаге построения добавлялся последовательно по одному элементу, тогда

$$N = \sum_{i}^{n} x_i^{(N)}. \tag{2.44}$$

Различные показатели аппаратурной надежности, полученные после проведения N-го шага описанного процесса, можно обозначить верхним индексом N. Для шага N результирующий показатель надежности определяется как:

$$P^{(N)} = P(X^{(N)}) = P(x_i^{(N)},..., x_n^{(N)}) = \prod_{i=1}^{n} P_i(x_i^{(N)}), \tag{2.45}$$

а суммарная стоимость резервных элементов

$$C^{(N)} = C(X^{(N)}) = C(x_i^{(N)},..., x_n^{(N)}) = \prod_{i=1}^{n} c_i x_i^{(N)}, \tag{2.46}$$

В соответствии с алгоритмом наискорейшего покоординатного спуска для выбора направления движения на (N+1)-м шаге процесса следует найти

$$ND^{(N+1)} = \max ND_i^N(x_i^{(N)}) = \max \frac{P(X_i^{(N)}, x_i^{(N)}+1) - P(X^{(N)})}{C(X_i^{(N)}, x_i^{(N)}+1) - C(X^{(N)})}, \qquad (2.47)$$

где X_i есть вектор X без компоненты x_i.

Предварительно можно выразить:

$$P(X_i^{(N)}, x_i^{(N)}+1) = \frac{P(x_i^{(N)}+1)}{P(x^{(N)})} P_i(X^{(N)}),\ C(X_i^{(N)}, x_i^{(N)}+1) = c_i C(X^{(N)}) \quad (2.48)$$

Отсюда

$$\begin{aligned} ND^{(N+1)} &= \max_{1\le i\le n} ND_i^{(N)}(x_i^{(N)}) = \max_{1\le i\le n} \frac{1}{c_i}\left[\frac{P_i(x_i^{(N)}+1)}{P_i(x_i^{(N)})} P_i(X^{(N)}) - P_i(X_i^{(N)})\right] = \\ P(X^{(N)}) &\max_{1\le i\le n} \frac{P_i(x_i^{(N)}+1) - P_i(x_i^{(N)})}{c_i P_i(x_i^{(N)})} = P(X^{(N)}) \max_{1\le i\le n} ND_i^{(N)}(x_i^{(N)}), \end{aligned} \qquad (2.49)$$

где $ND_i^{(N)}(x_i^{(N)}) = \frac{P_i(x_i^{(N)}+1) - P_i(x_i^{(N)})}{c_i P_i(x_i^{(N)})}$.

Поскольку $P(X^{(N)})$ входит во все величины $ND_i^{(N)}(x_i^{(N)})$ и не влияет на нахождение направления движения, то можно упростить вычислительные процедуры, связанные с проведением процесса построения оптимальной системы, т.е. сети – как высоконадежной системы [68]. Содержание процесса не изменится, если на (N+1)-м шаге процедуры двигаться в направлении

$$ND^{(N+1)} = \max_{1\le i\le n} ND_i^{(N)}(x_i^{(N)}). \qquad (2.50)$$

С учетом (2.38) – (2.50) алгоритм резервирования устройств сети может быть записан следующим образом:

1 шаг. Вычислить $ND_i^{(0)}(x_i) = \frac{1}{c_i P_i(x_i^{(0)})}[P_i(x_i^{(0)}+1) - P_i(x_i^{(0)})]$, причем $x_i^{(0)} = 0$ для i=1,2,...,n.

2 шаг. Выбрать наибольшую из величин $ND_i^{(0)}$: $ND^{(1)} = ND_{k_0}^{(0)}(x_{k_0}^{(0)}) = \max_{1\le i\le n} ND_{k_0}^{(0)}(x_{k_0}^{(0)})$

3 шаг. Найти $x_{k_0}^{(1)} = x_{k_0}^{(0)} + 1$.

4 шаг. Остальные $x_i^{(1)}$ для $i \ne k_0$ получить увеличением на единицу верхнего индекса: $x_i^{(1)} = x_i^{(0)} + 0$.

5 шаг. В результате построить новый вектор состава системы $X^{(1)} = (X_{k_0}^{(0)}, x_{k_0}^{(1)})$.

6 шаг. Вычислить новое значение $ND_{k_0}^{(1)}(x_{k_0}) = \frac{1}{c_{k_0} P_{k_0}(x_{k_0}^{(1)})}[P_{k_0}(x_{k_0}^{(1)} + 1) - P_{k_0}(x_{k_0}^{(1)})]$.

7 шаг. Остальные $ND_i^{(1)}(x_i^{(1)})$ для $i \neq k_0$ получить увеличением на единицу верхнего индекса: $ND_i^{(1)}(x_i^{(1)}) = ND_i^{(0)}(x_i^{(0)})$.

8 шаг. Если $i \neq k_0$, то процесс повторить, начиная с 1 шага, иначе переход к шагу 9.

9 шаг. Окончание работы алгоритма.

Для выполнения первого условия необходимо вести контроль значения $P(X^{(k)})$, получающегося на каждом *k*-м шаге. Этот процесс прекращается на шаге *N*, когда $P(X^{(N-1)}) < ND_0 \le P(X^{(N)})$. При этом принимается, что вектор состава системы $X^{(N)}$ является искомым. Для выполнения второго условия необходимо вести контроль значения $C(X^{(k)})$, получающегося на каждом *k-м* шаге. Процесс прекращается на шаге *N*, когда $C(X^{(N-1)}) < C_0 \le C(X^{(N)})$. Принимается, что вектор состава системы $X^{(N-1)}$ является искомым.

Следует отметить, что разработанный алгоритм резервирования устройств сети проверен на большом числе практических примеров и показал свою эффективность [68]. Этот алгоритм, в отличие от уже существующих, оказался одним из самых безотказных, требует значительно меньше вычислительных ресурсов и позволяет за небольшое число шагов получать удовлетворительные результаты.

2.5. Графовая модель оценки аппаратурной надежности телекоммуникационной сети

2.5.1. Разработка графовой модели

Математическую модель для расчета аппаратурной (физической) надежности корпоративной телекоммуникационной сети электронной коммерции можно представить в виде ориентированного графа Граф *G*=(*E*,*L*) (рисунок 2.1), где вершины графа это физические элементы сети – узлы и

каналы связи (оборудование), а дуги – это иерархические связи этих элементов [69].

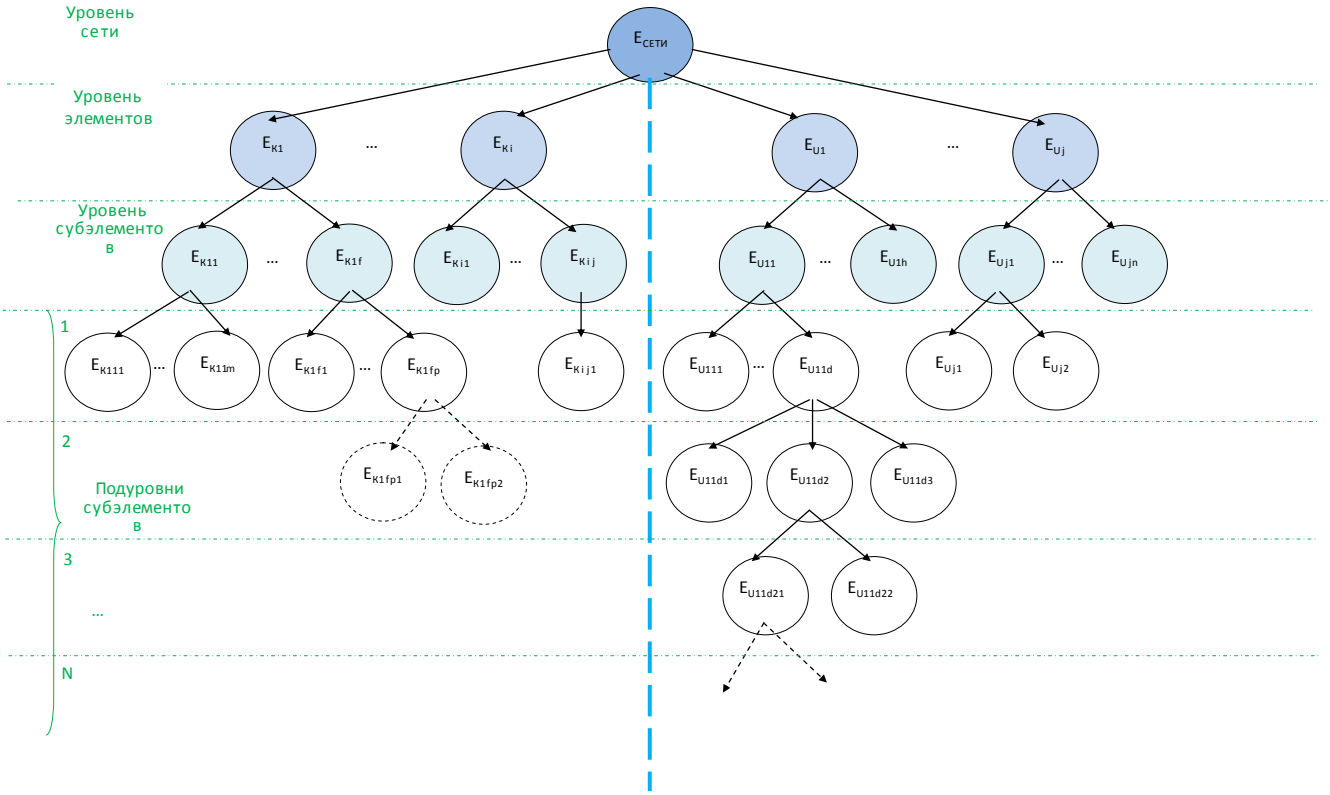

Рис. 2.1 – Графовая модель расчета аппаратурной надежности корпоративной телекоммуникационной сети

Графовая модель имеет три основных уровня:

1 – уровень сети (все устройства сети). Аппаратурная надежность сети, как и всякой системы, определяется надежностью составляющих ее элементов.

2 – уровень элементов сети (узлы – устройства и физические каналы связи). Здесь элементом является сервер, рабочая станция, терминал, канал связи и т.д.., например это рабочая стация.

3 - уровень субэлементов. Так при рассмотрении функционирование рабочей станции, можно выделить процессор, устройства ввода/вывода и т.д.

Уровень субэлементов содержит множество подуровней 1, 2, …, *N*, на которых более детально анализируется аппаратурная надежность составляющих элементов. Для рабочей станции это может быть, например, устройства ввод/вывода. Далее на следующем подуровне происходит

дальнейшая детализации элемента и его составляющих частей. Как показано в главе 1, степень детализации элемента сети в каждом конкретном случае определяется целью исследования и характером выбранного показателя надежности.

Например: множество элементов сети $E_{СЕТИ}=\{E_{K1},\ldots, E_{Ki}; E_{U1},\ldots, E_{Uj}\}$, т.е.

$$\{E_{K1},\ldots, E_{Ki}\}\subseteq E_{СЕТИ} \text{ и} \{E_{U1},\ldots, E_{Uj}\}\subseteq E_{СЕТИ}$$

В свою очередь $E_{K1}=\{E_{K11},\ldots,E_{K1f}\},\ldots, E_{Ki}=\{E_{Ki},\ldots,E_{Ki}\}$, причем

$E_{K11}=\{E_{K111},\ldots,E_{K11m}\}$, …, $E_{K1f}=\{E_{K1f1},\ldots, E_{K1fp}\},\ldots, E_{Ki}=\{E_{Ki1}\}$, и т.д.

$E_{U1}=\{E_{U11},\ldots, E_{U1h}\},\ldots, E_{Uj}=\{E_{Uj1},\ldots, E_{Ujn}\}$, причем

$E_{U11}=\{E_{U111},\ldots, E_{U11d}\}$, …, далее

$E_{U11d}=\{E_{U11d1},E_{U11d2}, E_{U11d3}\},\ldots$

На следующем подуровне $E_{U11d2}=\{E_{U11d21}, E_{U11d22}\}$ и так далее.

Таким образом, расчет аппаратурной надежности корпоративной телекоммуникационной сети проводится с помощью процедуры декомпозиции.

2.5.2. Анализ графовой модели

Алгоритм анализа графовой модели телекоммуникационной сети включает следующие основные шаги.

1 шаг. Ввод данных (виды оборудования, число устройств, виды устройств (с учетом степени детализации), Т - анализируемый период времени; задание показателя надежности для элементов сети, где P_E - значение вероятности;)

2 шаг. Анализ вводимых данных.

3 шаг. Формирование графовой модели сети $G=(E,L)$ на основании вводимых данных.

3.1. Определение множества вершин и дуг графа $G=(E,L)$.

3.2. Выбор уровней и подуровней графовой модели сети:

1 – уровень сети.

2 – уровень элементов сети.

3 – уровень субэлементов: подуровни 1, 2, …, N.

3.3. Формирование множества вершин $E_{СЕТИ}$ графа$G=(E,L)$, причем,

$E^{э}_{K} \cup E^{э}_{U} \cup E^{сэ}_{K} \cup E^{сэ}_{U} \cup E^{псэ}_{K} \cup E^{псэ}_{U} = E_{СЕТИ}$.

- в начальном состоянии множества вершин

$E^{э}_{K} = \varnothing$, $E^{э}_{U} = \varnothing$, $E^{сэ}_{K} = \varnothing$, $E^{сэ}_{U} = \varnothing$, $E^{псэ}_{K} = \varnothing$, $E^{псэ}_{U} = \varnothing$.

- выбор неотмеченной вершины;

- на 1-м уровне: вершина E_{Ki} отмечается и включается в множество вершин $E^{э}_{K}$, вершина E_{Uj}отмечается и включается в множество $E^{э}_{U}$;

- на 2-м уровне: вершина E_{Kif}отмечается и включается в множество вершин $E^{сэ}_{K}$, вершина E_{Ujm}отмечается и включается в множество $E^{сэ}_{U}$;

- на 3-м уровне для каждого из подуровней: вершины E_{Kifn}и E_{Ujmn}отмечаются и включаются в соответствующие множества $E^{псэ}_{K}$ и $E_{U}{}^{псэ}$.

- формирование завершается после просмотра всех необходимых вершин графа *G*.

3.4. Определение вершины входа $E^{вх} \in E$ и вершины выхода $E^{вых} \in E$ графа $G=(E,L)$.

3.5. Построение пути между $E^{вх}$ и вершины выхода $E^{вых}$ графа$G=(E,L)$.

4 шаг. Выделение подграфов $G_k = (E_k, L_k)$ и $G_u = (E_u, L_u)$ графа $G=(E,L)$, где $k=1,2,\ldots$, и $u=1,2,\ldots$. На рис.2.2 представлен пример подграфа графа *G=(E,L)*.

4.1. Определение множества необходимых элементов сети, на основании которого осуществляется выделение подграфа $G_k = (E_k, L_k)$ и $G_u = (E_u, L_u)$.

4.2. Формирование подмножеств вершин $E^{э}_{Ki}$ и $E^{э}_{Uj}$ – элементов, $E^{сэ}_{Ki}$, $E^{сэ}_{Uj}$ – субэлементов, $E^{псэ}_{Ki}$, $E^{псэ}_{Uj}$ – подуровней субэлементов для подграфов $G_k = (E_k, L_k)$ и $G_u = (E_u, L_u)$.

4.3. Определение вершин входа $E^{вх}_{k} \in E_k$ и выхода $E^{вых}_{k} \in E_k$ для подграфа $G_k = (E_k, L_k)$.

4.4. Определение вершин входа $E^{вх}_{u} \in E_u$ и выхода $E^{вых}_{u} \in E_u$ для подграфа $G_u = (E_u, L_u)$.

4.5. Построение пути между вершинами $E^{вх}_{k}$ и $E^{вых}_{k}$, а также между вершинами $E^{вх}_{u}$ и $E^{вых}_{u}$.

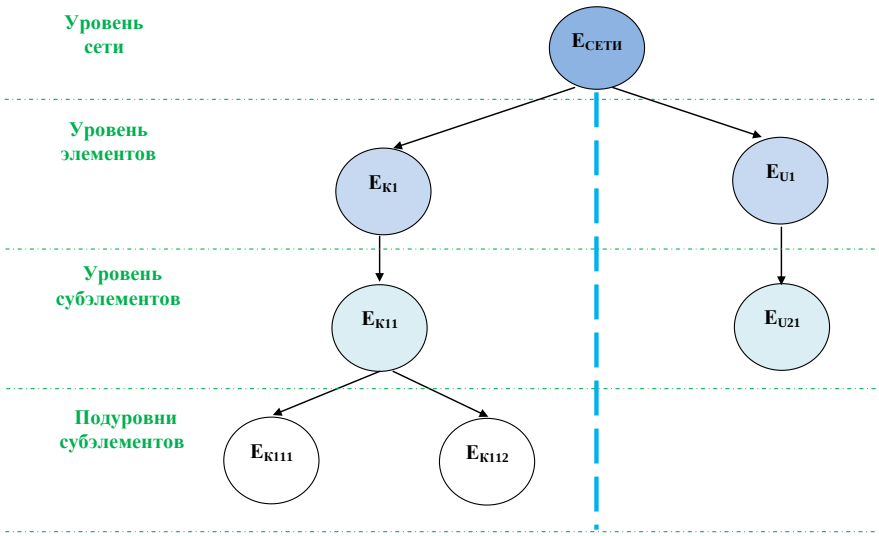

Рис. 2.2 Пример подграфа графа$G=(E,L)$.

5 шаг. Анализ подграфов $G_k=(E_k,L_k)$ и $G_u=(E_u,L_u)$.

5.1. Для графа $G=(E,L)$ каждый из выделенных подграфов состоит из K и U элементов сети, каждый из элементов выполняет функции $F_i=\{f_1,f_2,\ldots,f_n\}$ и может находиться в одном из состояний:

– s_1 – полной работоспособности (с возможностью выполнения всех функций $\{f_1,f_2,\ldots,f_n\}$),

– s_2 –частичной работоспособности (с потерей способности выполнения части первоначально реализуемых функций),

– s_3 – полного отказа.

5.2.Табличное представление подграфов $G_k=(E_k,L_k)$ и $G_u=(E_u,L_u)$. С целью сокращения объема занимаемой памяти целесообразно представить подграфы таблицами, где номер строки таблицы – это номер вершины, а содержимое строки определяют связи этой вершины с другими вершинами.

5.3. Расчет вероятности безотказной работы устройств сети

- Расчет вероятности безотказной работы устройств сети по формулам (2.1)- (2.5).

- Расчет надежности устройств сети, критичных к задержке результатов вычислений. (2.7)-(2.37):

- оценка отказа устройства в свободном состоянии. (2.7)-(2.33).

- оценка отказа устройства во время обслуживания заявок пользователей (2.34)-(2.37).

5.3. Для каждой таблицы строится матрица $\|\varphi_{ij}\|_{n\times m}$, элемент которой – это элемент оборудования: в исходном состоянии все φ_{ij}=1, если *j*-й способен выполнить функцию f_i, то φ_{ij}=1, иначе φ_{ij}=0, т.е. таблицы характеризуются матрицами состояний элементов сети.

5.4. Выделение σ-й выборки элементов и определение *l*-диагонали матрицы $\|\varphi_{ij}\|_{n\times m}$:

- выбор $\varphi(i,\sigma)$ последовательности из *l* элементов *i*-й строки матрицы $\|\varphi_{ij}\|_{n\times m}$ соответствующих σ-й выборке элементов

$$\varphi(1,\sigma),\ \varphi(2,\sigma),\ \ldots,\varphi(n,\sigma), \qquad (2.51)$$

σ-я выборка включает *n* элементов по *l*с каждой строки, без повторения столбцов расположения выбранных элементов (последовательность (2.51) является *l*-диагональю матрицы $\|\varphi_{ij}\|_{n\times m}$);

- вычисление *l*-диагонального произведения матрицы $\|\varphi_{ij}\|_{n\times m}$ (произведение $\varphi^*(1,\sigma),\varphi(2,\sigma),\ldots,\varphi(n,\sigma)$);

- суммирование по всем выборкам последовательностей элементов (2.51) матрицы:

$$\sum_{\sigma}\varphi^*(1,\sigma),(2,\sigma),\ldots,(n,\sigma) \qquad , \qquad (2.52)$$

где $\varphi^*(1,\sigma)$ - произведение *l* элементов *i*-й строки матрицы $\|\varphi_{ij}\|_{n\times m}$, соответствующих σ-й выборке.

5.5. Анализ условий работоспособности элементов сети. *l*-диагональ матрицы $\|\varphi_{ij}\|_{n\times m}$ положительна, если соответствующее ей *l* -диагональное произведение равно единице. Элементы сети работоспособны, если существует положительная*l*-диагональ матрицы $\|\varphi_{ij}\|_{n\times m}$ (для бинарной матрицы равно 1).

- Если $\sum_{\sigma}\varphi^*(1,\sigma),(2,\sigma),\ldots,(n,\sigma)=1,$ (2.53)

то сеть работоспособна (обеспечивает требуемое качество обслуживания).

- Если $\sum_{\sigma} \varphi^*(1,\sigma),(2,\sigma),\ldots,(n,\sigma)=0,$ (2.54)

то сеть не работоспособна.

- Переход элемента подматрицы из 1 в 0 отражает отказ соответствующих элементов сети, переход элемента подматрицы из 0 в 1 показывает возможность восстановления работоспособности (рассматриваемое сечение является минимальным).

- При оценке надежности оборудования исследуемых подсетей (участков сети) необходимо учитывать пересекаемость оборудования задействованного при выполнении функций $F_i=\{f_1, f_2,\ldots,f_n\}$. Для этого выделяется некоторое общее оборудование, отказ которого связан с выходом из строя всего участка, и оборудование, отказ которого приводит к потере только соответствующих функций F_i; предположим, что потеря различных функций равновероятна.

- Условия (2.53 и 2.54) позволяют оценить число работоспособных состояний части (или всей) сети в зависимости от суммарного числа $0<k<n$ функций $\{f_1,f_2,\ldots,f_n\}$. Каждое состояние соответствует варианту расположения (комбинации)k нулей в матрице $\|\varphi_{ij}\|_{n\times m}$, а с учетом пересечения оборудования k может состоять из $k_d,\ldots,k_g,\ldots,k_m$.

- При $k\geq n$ все элементы сети не работоспособны, при $0<k<n$ отказ всех элементов минимального сечения, отображаемого в матрице $\|\varphi_{ij}\|_{n\times m}$ невозможен, следовательно, все C_n^k состояний системы (для каждого k) могут быть работоспособны.

- Определение числа работоспособных состояний:

$$N_k = C_n^k - \sum_{s=1}^{n} b(s_i,k_g), \qquad (2.55)$$

где $b(s_i,k_g)$ - число комбинаций, соответствующих отказу элементов минимального сечения, отображаемого в матрице $\|\varphi_{ij}\|_{n\times m}$

Формула (2.55) дает нижнюю оценку числа работоспособных состояний системы, так как при суммировании в (2.55) возможен многократный учет состояний с отказом элементов двух или большего числа минимальных сечений. Погрешность приближения (2.55) возрастает при больших k (ввод и сравнение с допустимым значением погрешности).

5.6. Для элементов сети большинство условий работоспособности имеют конфликтный характер - увеличение значений одних запасов работоспособности влечет за собой уменьшение других. В этих условиях решение задачи находится на вершине конфликтных запасов работоспособности [69, 95]. Следовательно, вероятность безотказной работы какого-либо устройства сети в первую очередь будет определяться наименьшей из вероятностей удовлетворения отдельных условий работоспособности. По заданным значениям P_E (а, также, при вычислении $K_{\text{готз}}$) оценивается возможность обеспечения аппаратурной надежности:

- если $P_{Ti} < P_E$ и $K_{\text{гот}} < K_{\text{готз}}$, (2.56)

то требуемая вероятность неприемлема, данное оборудование для сети выбрано неудачно с точки зрения аппаратурной надежности всей сети, и требуются меры по достижению необходимой вероятности, например такие как замена оборудования, дублирование и т.д., переход к шагу 6.

- если $P_{Ti} \le P_E$ и $K_{\text{готз}} \le K_{\text{гот}}$, (2.57)

то оборудование выбрано удачно, и можно (если это необходимо) провести оптимизацию по критерию стоимости [69], переход к шагу 7.

6 шаг. Резервирования устройств сети с помощью разработанного алгоритма, представленного в п.п.2.4 данной главы. Переход к шагу 3.

6.1. Выполняются расчет надежности и оценка полученных результатов вычислений с заданными (необходимыми).

6.2. Проверка условий (2.56) и (2.57):

- если выполняются условия (2.56), то переход к шагу 3;
- если выполняются условия (2.57), то переход к шагу 7.

7 шаг. Окончание работы алгоритма.

Следует отметить, что при решении задач оптимизации аппаратурной надежности сети можно использовать в качестве целевой функции вероятность безотказной работы устройств, минимальный запас работоспособности устройств и критерий гарантированного запаса работоспособности, так как именно эти критерии надежности наилучшим образом позволяют проводить эффективную оптимизацию параметрической надежности сети и обеспечивают заданную надежность при заданных затратах [69, 95, 101].

Разработанные графовая модель оценки аппаратурной надежности корпоративной телекоммуникационной сети и алгоритм анализа графовой модели обеспечивают многоуровневое моделирование и позволяют учитывать специфику работы устройств разных уровней. С их помощью можно обоснованно прогнозировать стратегию модернизации и развития сети. Проведенная экспериментальная проверка показала, что точность результатов является достаточной для оценки надежности сети, а показатели надежности соответствуют международным стандартам, определенным в рекомендации МСЭ-Т G.602 [69]. Результаты экспериментальной проверки разработанных методов, моделей и алгоритмов представлены в главе 4 диссертационной работы.

ВЫВОДЫ К ГЛАВЕ 2

1. Проанализированы особенности математических моделей расчета надежности телекоммуникационных сетей. Эти модели имеют дело с вероятностными процессами и используют в качестве исходных данных достаточно недостоверную статистику, а иногда эта статистика вообще отсутствует (первое относится, как правило, к данным по надежности, а второе – к информации о потоках в сетях, об интенсивности межабонентской связи, о параметрах пропускной способности, надежности передачи и т.д.).

2. Разработан метод оценки надежности устройств телекоммуникационных сетей электронной коммерции, критичных к задержке результатов вычислений, позволяющий определить и прогнозировать вероятность выхода из строя узла/элемента сети (ЭТП), как при обслуживании заявок электронной торговой площадки, так и в свободном состоянии.

3. Разработан алгоритм резервирования устройств корпоративной телекоммуникационной сети электронной коммерции, который в отличие от уже существующих требует значительно меньше вычислительных ресурсов (примерно в 1,5 раза), и позволяет за небольшое число шагов получать удовлетворительные результаты. Алгоритм основан на методе наискорейшего покоординатного спуска, а процесс создания оптимальной резервированной системы, т.е. какого-либо участка (или элемента) сети представляется в виде многошагового процесса. На первом шаге определяется такая подсистема,

добавление к которой одного резервного элемента дает наибольший «удельный» выигрыш в приросте показателя аппаратурной надежности сети в целом. На втором шаге определяется следующая подсистема (включая и ту, к которой был добавлен резервный элемент), характеризующаяся тем, что добавление к ней одного резервного элемента дает опять наибольшее относительное приращение результирующего показателя надежности. Аналогичным образом процесс построения оптимальной системы продолжается далее.

Разработанный алгоритм позволяет эффективно реализовать резервирование элементов сети и ЭТП, обеспечив не только заданные показатели надежности, но и добиться этого как можно более экономично, с наименьшими суммарными затратами на резервные элементы, либо при заданных ресурсных ограничениях достичь максимально возможной аппаратурной надежности всей сети. Алгоритм проверен на большом числе практических примеров и показал свою эффективность (АКД).

4. Разработаны графовая модель оценки аппаратурной надежности телекоммуникационной электронной коммерции сети и алгоритм ее анализа, позволяющие:

- проверять правильность проектных решений, находить «слабые места» и применять существенные меры по повышению надежности сетей, а также эффективности их функционирования, обеспечивая необходимую надежность передачи коммерческой информации ЭТП по телекоммуникационным сетям,

- проводить оптимизацию аппаратурной надежности для широко спектра сетей

- проводить многоуровневое моделирование с учетом специфики работы сетевых устройств разных уровней,

- прогнозировать стратегию модернизации и развития корпоративной сети электронной коммерции.

ГЛАВА 3. МЕТОДЫ ЗАЩИТА КОММЕРЧЕСКОЙ ИНФОРМАЦИИ ЭТП В КОРПОРАТИВНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

3.1. Стандарты информационной безопасности

В настоящее время существует множество международных и отечественных наработок в области безопасности и защиты информации [28 – 32, 53, 103].

Имеются следующие основополагающие документы в области информационной безопасности: «Оранжевая книга» (критерии оценки безопасности компьютерных систем" - Trusted Computer System Evaluation Criteria -TCSEC); стандарты «Радужная серия», Гармонизированные критерии Европейских стран (ITSEC), Рекомендации X.800; Концепция защиты от НСД Госкомтехкомиссии при Президенте Российской Федерации.

В качестве примера также можно привести Международный стандарт информационной безопасности ISO/IEC 15408, известный как «CommonCriteria» - «Критерии оценки безопасности информационных технологий».

Среди стандартов по безопасности информационных технологий в РФ можно выделить ряд документов [28-32], регламентирующих защиту взаимосвязи открытых систем, а также нормативные документы по средствам, системам и критериям оценки защищенности средств вычислительной техники и автоматизированных систем: ГОСТ Р ИСО 7498-2-99, ГОСТ Р ИСО/МЭК 9594-8-98, ГОСТ Р ИСО/МЭК 9594-9-95, ГОСТ Р 50739-95, ГОСТ 28147-89, ГОСТ Р 34.10-94, ГОСТ Р 34.11-94 и т.д.

В Internet существует целый ряд комитетов, которые занимаются стандартизацией интернет-технологий. Это организации, составляют основную часть Рабочей группы инженеров Интернета – InternetEngineeringTaskForce, IETF [40, 53]. Можно также выделить OMG (Object Management Group), VRML (Virtual Reality Markup Language) Forum и Java Development Connection [25, 53]. В качестве средств обеспечения безопасности в Internet имеются протоколы защищенной передачи данных – а именно SSL (TLS), SET, IPv.6 [25, 40, 53].

3.2. Требования к классу защищенности 1Г для автоматизированной системы электронной торговой площадки

АС Оператора должна соответствовать требованиям Руководящего документа Гостехкомиссии «Автоматизированные системы. Защита от несанкционированного доступа к информации. Руководящий документ устанавливает классификацию автоматизированных систем, подлежащих защите от несанкционированного доступа к информации, и требования по защите информации в автоматизированных систем (АС) различных классов [51, 59, 81]. Документ разработан в дополнение ГОСТ 34.003-90, ГОСТ 34.601-90, РД 50-680-88, РД 50-34.680-90 и других документов. Предполагается деление АС на соответствующие классы по условиям их функционирования с точки зрения защиты информации необходимо в целях разработки и применения обоснованных мер по достижению требуемого уровня защиты информации, классы подразделяются на группы. Первая группа включает многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Группа содержит пять классов - 1Д, 1Г, 1В, 1Б и 1А. К этой группе относится и АС оператора ЭТП, а именно к классу 1Г (см. требования п.п. главы 1 данной работы).

В общем случае, комплекс программно-технических средств и организационных решений по защите информации от несанкционированного доступа (НСД) реализуется в рамках системы защиты информации от НСД (СЗИ НСД), условно состоящей из следующих четырех подсистем: - управления доступом; регистрации и учета; криптографической; обеспечения целостности (таблица 3.1). В таблице используются обозначения: «-» - нет требований, «+» - есть требования к данному классу; СЗИ - система защиты информации; СЗИ НСД - система защиты информации от несанкционированного доступа.

Таблица 3.1.

Подсистемы и требования	Класс 1Г
1. Подсистема управления доступом	

1.1. Идентификация, проверка подлинности и контроль доступа субъектов:	
в систему	+
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	+
к программам	+
к томам, каталогам, файлам, записям, полям записей	+
1.2. Управление потоками информации	-
2. Подсистема регистрации и учета	
2.1. Регистрация и учет:	
входа (выхода) субъектов доступа в (из) систему (узел сети)	+
выдачи печатных (графических) выходных документов	+
запуска (завершения) программ и процессов (заданий, задач)	+
доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи	+
доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей	+
изменения полномочий субъектов доступа	-
создаваемых защищаемых объектов доступа	-
2.2. Учет носителей информации	+
2.3. Очистка освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	+
2.4. Сигнализация попыток нарушения защиты	-
3. Криптографическая подсистема	
3.1. Шифрование конфиденциальной информации	-
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах	-
3.3. Использование аттестованных (сертифицированных) криптографических средств	-
4. Подсистема обеспечения целостности	
4.1. Обеспечение целостности программных средств и обрабатываемой информации	+
4.2. Физическая охрана средств вычислительной техники и носителей информации	+
4.3. Наличие администратора (службы) защиты информации в АС	-
4.4. Периодическое тестирование СЗИ НСД	+
4.5. Наличие средств восстановления СЗИ НСД	+
4.6. Использование сертифицированных средств защиты	-

3.3. Средства защиты информации электронной торговой площадки в телекоммуникационных сетях

В телекоммуникационных сетях электронной коммерции системы электронной торговли должны гарантировать юридически значимый

документооборот, т.е. обеспечить: аутентификацию, целостность информации и неотрекаемость. Для обеспечения юридически значимого документооборота используется Электронная Подпись (ЭП).

3.3.1. Криптографические хэш-функции

На сегодняшний день имеется множество алгоритмов хэширования с различными свойствами, такими как разрядность, вычислительная сложность, криптостойкость и т.д. [25, 31, 32, 51]. Хэш-функция *H* считается криптографически стойкой, если удовлетворяет 3 основным требованиям: необратимость, стойкость к коллизиям первого рода, стойкость к коллизиям второго рода [25, 51]. Эти требования не являются независимыми. Хэш-функция из *n*-бит считается криптостойкой, если вычислительная сложность нахождения коллизий для нее близка к $2^{n/2}$.

Хэширование часто используется в алгоритмах электронной подписи, где шифруется не само сообщение, а его хэш-код, что уменьшает время вычисления, а также повышает криптостойкость. Во многих случаев вместо паролей хранятся значения их хэш-кодов [25, 55].

Российский стандарт ГОСТ Р 34.11-94 основан на блочном алгоритме шифрования ГОСТ 28147-89 [32]. Его недостатки ГОСТ Р 34.11–94: в отличие от SHA-2 и SHA-3, ГОСТ 34.11-94 не предусматривал возможности вариации длины выходного хэша (это необходимо для встроенных реализаций с ограниченными ресурсами); у хэш-функции ГОСТ Р 34.11–94 не самые быстрые программные решения; неопределенность с S-блоками.

Российский стандарт ГОСТР 34.11-2012 разработан в качестве замены ГОСТ Р 34.11–94 [31]. Стандарт определяет алгоритм и процедуру вычисления хэш-функции для последовательности символов. Разработка вызвана потребностью в создании хэш-функции, соответствующей современным требованиям к криптографической стойкости и требованиям стандарта ГОСТ Р 34.10-2012 к электронной подписи – «Стрибог».

Определенная в стандарте функция хэширования используется при реализации систем электронной подписи на базе ассиметричного криптографического алгоритма. Стандарт связан с международными - ИСО

2382–2, ИСО/МЭК 9796, серий ИСО/МЭК 14888 и ИСО/МЭК 10118. ГОСТ Р 34.11-2012, определяет две функции хэширования с длинами хэш-кода n=256 бит и n=512 бит.

Согласно ГОСТ Р 34.11-2012, при вычислении хэш-функции проводятся следующие операции: покомпонентного сложения по модулю 2 векторов и конкатенация векторов, отображения, биективного отображения, произведения отображений, операции сложения в кольце, где Z_{2^n} - кольцо вычетов по модулю 2^n. Используются: инициализационные векторы; итерационные константы, нелинейные биективные преобразования множества двоичных векторов, заданные подстановкой; перестановка байт и линейное преобразование множества двоичных векторов. Главным отличием Стрибог от ГОСТ Р 34.11-94 является функция сжатия [31]. Преимущества ГОСТ Р 34.11-2012: в ГОСТ Р 34.11-2012 четко заданы значения «итерационных констант»; структура алгоритма нового стандарта позволяет проще разделить его вычисление на несколько потоков; по результатам проведенного в МИЭМ НИУ ВШЭ исследования, производительность нового алгоритма примерно в 1,5 раза выше, чем предыдущего (на некоторых реализациях).

3.3.2 Управление криптографическими ключами

Управление ключами – это информационный процесс, реализующий следующие три основные функции: генерацию, хранение и распределение ключей. Для получения ключей используются аппаратные и программные средства генерации случайных значений ключей [25, 40, 51, 102].

Закрытый ключ известен только клиенту электронной торговой площадки. ЭТП имеет только публичный ключ, позволяющий ему определить правильность ЭП, создаваемой с помощью закрытого ключа. Без закрытого ключа никто не может создать документ с подписью данного клиента. Закрытый ключ является уязвимым компонентом всей криптосистемы ЭП. В настоящее время используются следующие устройства хранения закрытого ключа: смарт-карты, USB-носители, таблетки Touch-Memory и другие [40, 51, 55]. Существуют криптопроцессоры, необходимы для защищенного хранения и

использования криптографических ключей, сертификатов, файлов и для работы с ЭП. Разработана спецификация TrustedPlatformModule (TPM), описывающая криптопроцессор, в котором хранятся криптографические ключи [40, 51, 55, 104].

Распределение ключей - самый ответственный процесс в управлении ключами, реализуется двумя способами: использованием одного или нескольких центров распределения ключей; прямым обменом сеансовыми ключами между пользователями сети.

Важной проблемой всей криптографии с открытым ключом, в том числе и систем ЭТП, является управление открытыми ключами [40, 55]. Задача защиты ключей от подмены решается с помощью сертификатов.

Сертификат открытого ключа – электронный документ, который удостоверяет владельца пары ключей. Сертификат публичного ключа регистрируется в Центре Сертификации (государственном, частном или банковском), что обеспечивает определение принадлежности данной пары ключей конкретному юридическому или физическому лицу и срока действия данной пары ключей. Обычно, исходя из политики безопасности, желательно пересоздание пары ключей каждый год.

Для использования ЭП необходим Удостоверяющий центр (УЦ), который подтвердит, что сертификат выдан именно тому лицу, которое его применяет. Он заверяет сертификаты своей подписью, хранит базы сертификатов с открытыми ключами и обеспечивает к ним доступ, а также позволяет проверить их подлинность.

Правовую основу ЭП обеспечил Федеральный закон 1-ФЗ «Об электронно-цифровой подписи»»[64 – 65, 96].

3.3.3. Электронная подпись

Электронная подпись (ЭП) или *электронная цифровая подпись (ЭЦП)* – это строка бит, полученная в результате процесса формирования подписи, которая может иметь внутреннюю структуру, зависящую от конкретного механизма формирования подписи [25, 40, 55].

ЭП является реквизитом электронного документа, который позволяет установить принадлежность подписи владельцу сертификата ключа ЭП и определить отсутствие искажения электронной информации в документе с момента формирования ЭП. Значение этого реквизита получается после криптографического преобразования информации с использованием закрытого ключа ЭП. При организации защищенного канала связи с владельцем ЭП используется открытый ключ [40, 51, 55].

Защита ключей от подмены осуществляется с помощью сертификатов. Согласно ст. 2 Федерального Закона от 06.04.2011 «Об электронной подписи» № 63-ФЗ, сертификат открытого ключа - это цифровой или бумажный документ, подтверждающий соответствие между открытым ключом и информацией, идентифицирующей владельца ключа [96]. Сертификат содержит информацию о владельце, сведения об открытом ключе, его назначении и применении, название центра сертификации и т. д.

Модели организации сертификатов [64, 65, 82, 104]:

1) централизованная, реализующаяся на основе «сетей доверия» (здесь путем перекрестного подписания сертификатов знакомых и доверенных людей каждым пользователем строится так называемая «сеть доверия»);

2) децентрализованная (здесь используются центры сертификации, поддерживаемые доверенными организациями).

Центр сертификации формирует закрытый ключ, собственный сертификат, сертификаты конечных пользователей и удостоверяет их аутентичность своей ЭП, проводит отзыв истекших и скомпрометированных сертификатов и ведет базы выданных и отозванных сертификатов.

В России в 1994г. разработан первый российский стандарт ЭЦП - ГОСТ Р 34.10-94 [30]. В 2002 году с целью обеспечения большей криптостойкости алгоритма, взамен этого ГОСТа был введен ГОСТ Р 34.10-2001 [51, 55]. В соответствии с этим стандартом, термины «электронная цифровая подпись» и «цифровая подпись» являются синонимами, с 01.06.12 термин «электронно-цифровая подпись» заменен на – «электронная подпись». 01.01.13 года ГОСТ Р 34.10-2001 заменен на ГОСТ Р 34.10-2012 [29].

Федеральный закон РФ от 06.04.11 г. № 63-ФЗ устанавливает следующие виды ЭП: простая электронная подпись, усиленная неквалифицированная подпись, усиленная квалифицированная.

С 01.01.13 года гражданам РФ выдается универсальная электронная карта, в которую встроена усиленная квалифицированная ЭП.

Как правило, подписываемые документы имеют переменный и/или большой объем, поэтому ЭП ставится не на сам документ, а не его хэш. Для вычисления хэша используются криптографические хэш-функции, это является гарантией обнаружения изменений документа при проверке подписи. Использование хэш-функции не обязательно при ЭП, а сама хэш-функция не является частью алгоритма ЭП, поэтому можно использовать любую надежную хэш-функция или совсем ее не использоваться.

Применение ЭП имеет смысл, если при вычислении легитимной подписи без знания закрытого ключа процесс становится вычислительно сложным.

Таким образом, при формировании политики безопасности и системы оценок эффективности, а также при проведении комплексных испытаний защищенности следует пользоваться положениями ISO 15408 («CommonCriteria»). Для реализации и оценки технического совершенства систем шифрования и электронной подписи предназначены соответствующие ГОСТы. Если нужно защитить канал обмена произвольной информацией, то целесообразно использовать протокол TLS. При необходимости обеспечения безопасности финансовых транзакций можно использовать стандарт SET *(Secure Electronic Transaction)* , включающий в себя протоколы защиты каналов в качестве одного из стандартов более низкого уровня.

3.4. Метод поэтапного подписания документов ЭП для электронной торговой площадки

В основу метода поэтапного подписания документов для электронной торговой площадки положены существующие стандарты, например ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012, при этом учитывались современные изменения и дополнения. При написании этой главы использованы обозначения, согласно соответствующим стандартам [29 - 32].

Разработанный метод поэтапного подписания документов ЭП для электронной торговой площадки содержит основные этапы:

0 этап. Подготовка данных.

1 этап. Получение комплекта ЭП.

2 этап. Подготовка к работе с ЭП.

3 этап. Проверка данных.

4 этап. Проверка сертификатов оператором ЭТП.

5 этап. Использование ЭП.

6 этап. Проверка.

7 этап. Процедура принятия решения лицом, принимающим решение - ЛПР (это сотрудники ЭТП) об участии пользователя в электронных торгах на ЭТП.

0 этап. Подготовка данных.

1. Подготовка исходных данных для ЭП.

Определение параметров схемы ЭП. Параметр схемы ЭП – это элемент данных, общий для всех субъектов схемы ЭП, известный или доступный всем этим субъектам.

Параметры ЭП по ГОСТ Р 34.10-2012 [29]:

– p - модуль эллиптической кривой [19, 42, 84];

– эллиптическая кривая E, задаваемая инвариантом J(E) или коэффициентами $a,b \in F_p$;

– целое число m – порядок группы точек E [85, 88];

– q - порядок циклической подгруппы группы точек E [29, 85, 88];

– точка $P \neq 0$ кривой E, с координатами (x_p, y_p), причем $qP=0$ (0 – это нулевая точка);

– хэш–функция $h(\text{-}): V^* \to V_l$ (где V^* – множество всех двоичных векторов произвольной конечной длины, V_j – множество всех двоичных векторов длиной l бит).

2. Выбор требований к параметрам ЭП согласно ГОСТ Р 34.10-2012(в стандарте предусмотрена возможность выбора одного из двух вариантов требований к параметрам):

– выполнение условия $p^t \neq 1 (\mathrm{mod}\, q)$, для всех целых t = 1, 2, … B, где B=31, если $2^{254}<q<2^{256}$, и B = 131, если $2^{508}<q< 2^{512}$;

– выполнение $m \neq p$;

– инвариант кривой должен удовлетворять условию $J(E) \neq 0{,}1728$.

3. Документы к заявке:

1) устав.док.;

2) договор.зип.;

3) системная заявка:

- информация о пользователе,

- список документов и их хэш сумма $M=\{M_1, M_2, M_3\}$,

где M – множество документов к заявке, M_1 - устав.док., M_2 - договор.зип., M_3 - системная заявка.

$M_3=\{M_{3p}, M_{3d}\}$,

где M_{3p}, - информация о пользователе, M_{3d}- список документов и их хэш сумма, которая определяется ГОСТ Р 34.11-2012 для ЭП).

$M_{3d}=\{M_{3d1},\ldots,M_{3dg}\}$.

- Вычисление хэш-суммы *H(M)* (или $\bar{h} = h(M)$ документов M согласно [31], которая отображает M в хэш-код *H(M)*:

$$H : V^* \to V_n, \tag{3.1}$$

где V^* - множество всех двоичных векторов-строк конечной размерности, включая пустую строку; V_n - множество всех n-мерных двоичных векторов, n – целое неотрицательное число.

Исходные данные: M – документы, подлежащие хэшированию, IV – инициализационный вектор хэширования, где $IV \in V_{512}$.

– присвоение начальных значений для текущих величин.

– если $|M|< 512$, то осуществляется переход к п.3, иначе вычисляется подвектор $M_i \in V_{512}$ для M:

$$M = M' || M_i \text{ и } M \in V^*, |M|<2^{512}. \tag{3.2}$$

Значение хэш-функции M вычисляется с помощью итерационной процедуры. На каждой итерации вычисления хэш-функции используется функция сжатия [31]:

$$g_N : V_{512} \times V_{512} \to V_{512}, \quad N \in V_{512}, \qquad (3.3)$$

где V_n - множество всех n-мерных двоичных векторов (n - целое неотрицательное число).

– определяется значение величины h:

$$h=H(M), \qquad (3.4)$$

которое и является значением функции хэширования $H(M)$.

1 этап. Получение комплекта ЭП.

1.1.Генерация ключей, т.е. генерация псевдослучайного целого числа k: $0<k<q$.Клиенту ЭП необходимо иметь ключ подписи и ключ проверки подписи.

1.2. Исходные данные для формирования ЭП:

d - ключ подписи (целое число, $0<d<q$;) - элемент секретных данных, специфичный для клиента и используемый только им в процессе формирования подписи; M - подписываемый документ, $M \in V^*$.

Результат:

ζ – ЭП документа M.

Вычислить:

1) α (целое число), двоичным представлением которого является вектор $\bar{h}$, где $\bar{h} = h(M)$; $e \equiv \alpha (\mathrm{mod}\ q)$; если e= 0, то e=1.

2) точку эллиптической кривой $C=kP$, $r \equiv x_c (\mathrm{mod}\ q)$, x_c– x-координата точки С, если r=0, то переход к п.1.1 этапа 1 [19, 42, 84].

3) $s \equiv (rd + ke)(\mathrm{mod}\ q)$, если s=0, то - к п.1.1 этапа 1.

4) $\bar{r}$ и $\bar{s}$ (двоичные векторы), определение ЭП $\zeta = (\bar{r} \| \bar{s})$ как конкатенации двух двоичных векторов.

1.3.КриптоПРОCSP (криптопровайдер).

1.4. Выпуск сертификата .crt/.cer (публичный)

1.5. Запись на носитель USB закрытого ключа (должен быть не экспортируемым).

1.6. Аккредитация на ЭТП:

- УЦ Контур (удостоверяющий центр),
- УЦ Тензор,
- УЦ Гарант электронный экспресс.

2 этап. Подготовка к работе с ЭП.

2.1. Настройка IE браузера.

2.2. Установка библиотеки capicom от Microsoft.

2.3. Загрузка своего сертификата на ЭТП:

$cert^{p}_{pi}$:= $cert_{pi}$.crt/.cer,

где p_i - клиент i, $cert^{p}_{pi}$ – публичный сертификат клиента p_i.

$cert_{pi}$.crt/.cer$\Rightarrow$ЭТП.

3 этап.Проверка данных.

3.1. Присвоение СА клиенту p_i идентификатора ID: p_i:=ID_i, где СА (certificationauthority) - удостоверяющий центр, или УЦ, ID_i - идентификатор клиента i.

3.2. Проверка личного сертификата клиента - $cert^{l}_{pi}$ (ID_i) в БД корневых сертификатов - $dBcert_{RC}$(thedatabaserootcertificates) СА.

Если (ID_i)$cert^{l}_{pi} \in dBcert_{RC}$, то переход к 4 этапу, иначе – на окончание работы.

4 этап. Проверка $cert^{l}_{pi}$ **оператором ЭТП.**

$$PR=\{pr_1,\ldots,pr_2,\ldots,pr_j,\ldots,pr_N\}, \quad (3.5)$$

где PR - Множество параметров (сертификата), которые проходят проверку оператором ЭТП; pr_j – параметры (позиции сертификата клиента): pr_1 - название компании, pr_2 - ИНН, и другие.

Если $pr_j \in cert^{l}_{pi}$, j=1,2,…,N, то занесение в БД используемых сертификатов:

$$ID_i = cert^{l}_{pi}.cer, \text{ или } (cert_{pi})Сертификат.cer \in dBcert_{US}, \quad (3.6)$$

где $dBcert_{US}$ – БД используемых сертификатов.

Переход к 5 этапу, иначе – на окончание работы.

5 этап. Использование ЭП.

5.1. Использование ζ для подписания документов на ЭТП.

Документ.pdf+ ЭЦП.sig (3.7)

или M. pdf+ζ .sig.

5.2. Проверка ЭП.

Исходные данные: ζ - ЭП, M - документ, Q - ключ проверки ЭП, т.е. точка эллиптической кривой с координатами (xq,yq), где $dP=Q$ - это элемент данных, связанный с ключом подписи и используемый проверяющей стороной в процессе проверки

Результат: свидетельство - элемент данных, представляющий соответствующее доказательство достоверности или недостоверности ЭП.

Вычислить:

1) по ЭП - вычисление целых чисел r и s; если $0<r<q$ и $0<s<q$, то переход к п.1.1 этапа 1., иначе ЭП - неверна.

2) α, двоичным представлением которого является вектор $\bar{h}$;

определение $e \equiv \alpha (\mathrm{mod}\ q)$; если $e=0$, то $e=1$.

3) $v \equiv e^{-1} (\mathrm{mod}\ q)$; $z_1 \equiv sv \bmod q$; $z_2 \equiv -rv \bmod q$.

4) точку эллиптической кривой $C=z_1P+z_2Q$, определение $R \equiv x_c \bmod q$,

(x_cx – координата точки C) [19, 42, 84].

5) если $R=r$, то ЭП принимается, иначе - ЭП неверна.

Криптостойкость ЭП опирается на стойкость хэш-функции и на стойкость самого алгоритма шифрования. Стойкость алгоритма шифрования основывается на дискретном логарифмировании в группе точек эллиптической кривой [19, 42, 84].

6 этап. Проверка. Этот этап, основанный на разработанной методике проверки сертификатов.

6.1. Определение необходимых позиций:

$$PZ=\{pz_1, pz_2, pz_3, pz_4, pz_5\}, \quad (3.8)$$

где PZ - множество всех проверяемых позиций сертификата, pz_1 - сроки действия пользовательского сертификата, pz_2 – сроки действия корневого сертификата, pz_3 – наличие соответствующего корневого сертификата в базе, pz_4, - наличие в списках отозванных,pz_5 – соответствие пользователя и сертификата.

Позиции проверки – это безразмерные (булевы) величины, причем для каждой позиции:

$$pz_i = \begin{cases} 1 - \textbf{результат проверки положительный} \\ 0 - \textbf{отрицательный результат проверки} \end{cases} \quad (3.9)$$

Ввод pz_i для проверки, где j=1,…,5.

6.2. Методика проверки.

1. Сроки действия пользовательского сертификата.

t^l_1 – начало действия $cert^l_{pi}$, t^l_2 – окончание действия $cert^l_{pi}$, $[T^l_1, T^l_2]$ – реальный период времени действия сертификатов.

$t^l_1 \subseteq cert^l_{pi}.cer$; $t^l_2 \subseteq cert^l_{pi}.cer$;

Если $t^l_1 \in [T^l_1, T^l_2]$ и $t^l_2 \in [T^l_1, T^l_2]$,

то pz_1= 1и переход к п.2,

иначе – pz_1=0 и переход к п.6.

2. Сроки действия корневого сертификата.

t^k_1 – начало действия корневого сертификата, t^k_2 – окончание действия корневого сертификата, $[T^k_1, T^k_2]$ - реальный временной период действия сертификата.

$t^k_1 \subseteq cert^k_{pi}.cer$; $t^k_2 \subseteq cert^k_{pi}.cer$;

Если $t^k_1 \in [T^k_1, T^k_2]$ и $t^k_2 \in [T^k_1, T^k_2]$,

то pz_2=1, переход к п.3,

иначе pz_2=0 – переход к п.6.

3. Наличие соответствующего корневого сертификата в базе – $dBcert_{RC}$:

Если $cert^k_{pi}.cer \in dBcert_{RC}$,

то pz_3=1 и переход к п.4,

иначе pz_3=0 – переход к п.6.

4. Проверка в списках отозванных УЦ сертификатов

УЦ публикует списки отозванных сертификатов - CertificateRevocationList(CRL):

$dBcert_{CRL} \in CA$.

Если $cert^k_{pi}.cer \in dBcert_{CRL}$

и $cert^l_{pi}.cer \in dBcert_{CRL}$,

то pz_4=1, переход к п.5,

иначе pz_3=0 – переход к п.6.

5. Соответствие пользователя и сертификата.

Анализ БД используемых сертификатов $dBcert_{US}$:

Клиент ID333=Сертификат.cer;

Если $p_i \in ID_i$, и

если $ID_i \in cert^l_{pi}.cer$, и

если $ID_i \in dBcert_{US}$, и

если $cert^l_{pi}.cer \in dBcert_{US}$, то pz_5=1, переход к п.6, иначе pz_5=0 переход к п.7.

6. Результат проверки. *PZ** - результат проверки всех позиций множества *PZ*.

Вычислить $PZ^* = \prod_{i=1}^{5} pz_i$, (3.10)

если *PZ** = 1, то сертификат прошел проверку – переход к п.7,

если *PZ**=0, то сертификат не действительный – переход к 1 этапу

7. Окончание проверки.

7 этап. Процедура принятия решения ЛПР - лицом, принимающим решение (сотрудники ЭТП) об участии пользователя в электронных торгах представлена в п.3.5 данной главы.

3.5. Процедура принятия решения сотрудниками ЭТП об участии пользователя в электронных торгах

Процедура принятия решения об участии пользователя в электронных торгах на ЭТП проводится ЛПР - лицом, принимающим решение - это сотрудники электронной торговой площадки. Здесь выбор решения может осуществляться как в условиях определенности, так и в условиях неопределенности исходной информации. Для этого необходимо провести анализ методов оценки альтернативных вариантов решений, позволяющих количественно оценить их эффективность. При выборе решения сотрудниками ЭТП требуется применение специфических приемов и методов, предполагающих использование их интуиции и опыта работы. Получаемые альтернативные варианты решений допускают упорядочение по некоторым аспектам. Здесь важным является получение оценок рассматриваемых альтернатив, при котором каждому решению ставится в соответствие совокупность чисел (вектор значений критериев качества решений) [65, 48, 57]. Задачи оценивания чаще всего решаются экспертными методами. Методы экспертных оценок подробно представлены в таких работах как [48, 57, 100, 105]. Среди существующих методов можно выделить метод шкалирования, методы ранжирования альтернатив, метод минимального расстояния и т.д. [48, 57, 100]. Следует отметить, что методы непосредственной ранжировки достаточно трудны для экспертов, поскольку им приходится одновременно оценивать ряд альтернатив, присваивая каждой определенное место (ранг) в ряду ранжировки. Более приемлемым является использование экспертами механизма попарных сравнений [48, 57, 100]. При попарном сравнении альтернатив используется аппарат бинарных отношений.

Метод анализа иерархий является систематической процедурой для иерархического представления элементов, определяющих суть любой

проблемы, и в частности проблемы выбора решения сотрудником ЭТП о допуске к участию пользователей в электронных торгах на ЭТП [64, 65].

Использование метода анализа иерархий в рассматриваемой задаче имеет следующие преимущества:

- метод дает возможность провести декомпозицию и анализ проблемы оценивания альтернативных решений в конкретной ситуации;

- позволяет учитывать предпочтения ЛПР на множестве критериев и требуется только определить важность критерия путем попарного сравнения;

- иерархическое представление дает ЛПР простую для понимания картину влияния изменения приоритетов на верхних уровнях на приоритеты элементов нижних уровней;

- метод достаточно хорошо автоматизируется.

Существует несколько видов иерархий [48, 57, 76, 105]. Для процедуры принятия решения ЛПР об участии пользователя в электронных торгах на ЭТП наиболее приемлемыми являются доминантные иерархии.

В решаемой задаче имеется набор альтернатив A_1, A_2, …,A_n и множество критериев оценки альтернатив K_1,K_2,…,K_m. Задача состоит в том, чтобы выбрать наиболее рациональное решение в конкретной ситуации с точки зрения ЛПР.

Альтернативные действия ЛПР:

- A_1– допустить к торгам,
- A_2 – не допустить,
- A_3 – еще раз проверить надежность сети, канала связи, оборудования ЭТП.

Множество критериев оценки альтернатив $K = \{K_1, K_2, \ldots, K_m\}$ включает: сертификаты, позиции сертификатов, информация о пользователе, список документов, хэш-сумму документов.

Процедура принятия решения ЛПР об участии пользователя в электронных торгах на ЭТП включает 8 шагов.

1. Методом попарных сравнений необходимо оценить важность критериев. На данном шаге необходимо участие ЛПР: используя заданную шкалу градации качества, он должен сравнить попарно все критерии.

Если критерий K_i предпочтительнее K_j, то K_{ij} = 1, иначе K_{ij} = -1, при эквивалентности K_{ij} = 0:

$$K_{ij} = \begin{cases} 1, \textit{если } K_i > K_j; \\ 0, \textit{если } K_i \sim K_j; \\ -1, \textit{если } K_i < K_j. \end{cases} \quad (3.11)$$

2. Сравнение критериев попарно и получение матрицы:

	K_1	…	K_i	…	K_m
K_1	K_{11}	…	K_{1i}	…	K_{1m}
…	…	…	…	…	…
K_j	K_{j1}	…	K_{ji}	…	K_{jm}
…	…	…	…	…	…
K_k	K_{k1}	…	K_{ki}	…	K_{lm}

(3.12)

3. Вычисление весов критериев:

$$W_i = \sqrt[m]{K_{i1}...K_{im}} \quad (3.13)$$

$$|W_i| = \sqrt[m]{\prod_{i=1}^{m} K_{im}} \quad (3.14)$$

$$\overline{W_i} = \frac{W_i}{\sum_{i=1}^{m} W_i} \quad (3.15)$$

4. Сравнение важности альтернатив по критериям, которое проводится при фиксации каждого из критериев [170].

K_i	A_i		A_3
A_1	y_{11}	…	y_{13}
…	…	…	…
A_3	y_{31}	…	y_{33}

(3.16)

5. Вычисление весов альтернатив по каждому критерию:

$$V_i(K_i) = \sqrt[n]{\prod_{r=1}^{n} y_{i`r}}\ , \tag{3.17}$$

$$\overline{V}_i(K_i) = \frac{V_i(K_i)}{\sum_{i=1}^{n} V_i(K_i)}\ . \tag{3.18}$$

6. Получение матрицы весов альтернатив по каждому критерию.

	A_1	A_2	A_3
	–	–	–
K_1	$V_1(K_1)$	$V_2(K_1)$	$V_3(K_1)$
...	…	…	…
	–	–	–
K_m	$V_1(K_m)$	$V_2(K_m)$	$V_n(K_m)$

(3.19)

7. Вычисление функции ценности для каждой альтернативы.

$$F_i = \sum_{i=1}^{m} \overline{V}_i(K_i)\overline{W}_i\ . \tag{3.20}$$

8. Выбор альтернативы A_i (действия) по функции ценности.

При использовании метода попарных сравнений каждому эксперту приходится выполнять число сравнений альтернатив, определяемое числом сочетаний из n по 2: C_n^2, т.е. сравнивать альтернативы между собой. Получаемая при этом матрица отражает его систему предпочтений. В отдельных случаях предпочтения эксперта могут содержать циклические участки, когда предпочтения эксперта не определяются однозначно. Если матрицу предпочтений эксперта изобразить графом, то в графе при обходе по ориентированным дугам в том случае появляются замкнутые контуры [48, 101]. В такой ситуации метод ранжировки не дает возможность определения рангов, отражающих систему предпочтений эксперта. Поэтому, перед вычислением суммарной матрицы предпочтений экспертов ее проверяют на отсутствие циклов, т.е. на ацикличность.

Следует отметить, что все операции, которые проводит эксперт ЭТП (шаги 1 – 8) относятся к классу нормально-допустимых по сложности [48, 57].

Таким образом, предложен и обоснован эффективный метод поэтапного подписания документов ЭП для ЭТП, который содержит 8 основных этапов. В отличие от существующих метод основан на современных ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012, позволяет проводить проверку сертификатов сразу по 5 позициям, имеющиеся аналоги проводят проверку только по 1 или 2 позициям.

ВЫВОДЫ К ГЛАВЕ 3

1. Проведены анализ и исследование средства и методов защиты информации ЭТП в телекоммуникационных сетях электронной коммерции. Показано, что в таких сетях системы электронной торговли должны гарантировать юридически значимый документооборот, т.е. обеспечить: аутентификацию, целостность информации и неотрекаемость. Представлены требования к классу защищенности 1Г для автоматизированной системы электронной торговой площадки.

2. Исследованы преимущества использования хэш-функций в схемах электронной подписи для зашиты коммерческой информации ЭТП в телекоммуникационных сетях. Обосновано применение ГОСТ Р 34.11-2012 в схеме ЭП – подписываемые документы ЭТП часто имеют большой объем, поэтому электронная подпись ставится не на сам документ, а на его хэш, следовательно, целесообразно использовать хэш-функцию для защиты информации ЭТП в телекоммуникационных сетях электронной коммерции. При этом производительность нового алгоритма по ГОСТ Р 34.11-2012 для схемы ЭП примерно в 1,5 раза выше, чем предыдущего стандарта для некоторых реализаций.

3. Разработан эффективный метод поэтапного подписания документов ЭП для электронной торговой площадки, который содержит 8 основных этапов: подготовка данных; получение комплекта ЭП; подготовка к работе с ЭП; проверка данных; проверка сертификатов оператором ЭТП; использование ЭП; проверка ЭП, принятие решения об участии пользователя в электронных торгах. Метод основан на современных ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012.

4. Разработана методика проверки сертификатов, которая является уникальной и позволяет проводить проверку сертификатов сразу по 5 позициям. Это - проверка сроков действия пользовательского сертификата, сроков действия корневого сертификата, наличие соответствующего корневого сертификата в базе, проверка в списках отозванных, соответствия пользователя и сертификата. Имеющиеся аналоги проводят проверку только по 1 или 2 позициям. Следовательно, разработанная процедура позволяет более, чем в 2 раза повысить эффективность защиты коммерческой информации ЭТП в телекоммуникационных сетях.

5. Разработана процедура принятия решения ЛПР об участии пользователя в электронных торгах. Анализ существующих подходов к решению этой задачи показал целесообразность принятия решения на базе экспертных процедур, где наиболее эффективным является метод анализа иерархий, так как:

- метод дает возможность провести декомпозицию и анализ проблемы оценивания альтернативных решений в конкретной ситуации;

- позволяет учитывать предпочтения ЛПР на множестве критериев и требуется только определить важность критерия путем попарного сравнения;

- иерархическое представление дает ЛПР простую для понимания картину влияния изменения приоритетов на верхних уровнях на приоритеты элементов нижних уровней.

ГЛАВА 4. ЭКСПЕРИМЕНТАЛЬНАЯ ПРОВЕРКА МЕТОДОВ ОБЕСПЕЧЕНИЯ НАДЕЖНОЙ ПЕРЕДАЧИ И ЗАЩИТЫ КОММЕРЧЕСКОЙ ИНФОРМАЦИИ ЭТП В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

В данной главе приведены экспериментальные результаты реализации методов, моделей и алгоритмов, разработанных во второй и третьей главах диссертационной работы. Представлено созданное на основе разработанного математического аппарата программное обеспечение системы оценки надежной передачи и защиты информации электронной торговой площадки в телекоммуникационных сетях электронной коммерции.

4.1. Структура компании «Аукционный Конкурсный Дом»

Аукционный Конкурсный Дом (АКД) - компания, оказывающая широкий спектр юридических, консалтинговых и правовых услуг в области электронных торгов и является одним из лидеров в Российской Федерации по количеству проведенных аукционов по закупкам товаров, работ и услуг для государственных и муниципальных нужд [62, 64, 67]. Функциональная структура компании представлена на рис. 4.1.

Основные виды деятельности АКД:

1) организация и проведения торгов в форме аукционов и конкурсов разного уровня сложности и ответственности (проведение торгов в электронной форме, конкурсов по подбору инвесторов, аукционов по реализации имущества и т.д.);

2) осуществление функций официальной отраслевой электронной торговой площадки Государственной корпорации «Росатом».

Информация о торгах доводится до заинтересованных участников автоматически посредством рассылки электронных писем. Автоматическое формирование отчета о проведенных торгах производится одним нажатием кнопки. Допуск участников в торги осуществляет заказчик торгов в своем

личном кабинете на автоматизированной площадке. В момент торгов участники (поставщики) не видят названия своих конкурентов.

Использование электронной подписи (ЭП) регулируется устоявшейся нормативно правовой базой; при ее создании применяются только сертифицированное программное обеспечение [63 - 64].

Рис. 4.1 – Структура АКД

Для обеспечения надежной передачи по сети и защиты коммерческой информации при проведении торгов на ЭТП «Аукционный Конкурсный Дом» применяются специально разработанные методы, модели и алгоритмы, подробное описание которых приводятся в главах 2 – 3 диссертационной работы.

4.2 Результаты экспериментального исследования разработанного математического аппарата

Эксперименты проводились на сетях АКД. Целью этого исследования является экспериментальное подтверждение разработанного математического аппарата.

На рис. 4.3 представлена вероятность безотказной работы элементов телекоммуникационной сети электронной коммерции (АКД) за период времени T, измеряемый в годах:

- график 1 соответствует этапу проектирования сети без предварительного расчета аппаратурной надежности и использования оптимального (рационального) резервирования сетевых устройств;
- график 2 – та же функция за аналогичный период времени, но после предварительного расчета надежности с применением разработанного алгоритма резервирования устройств сети;

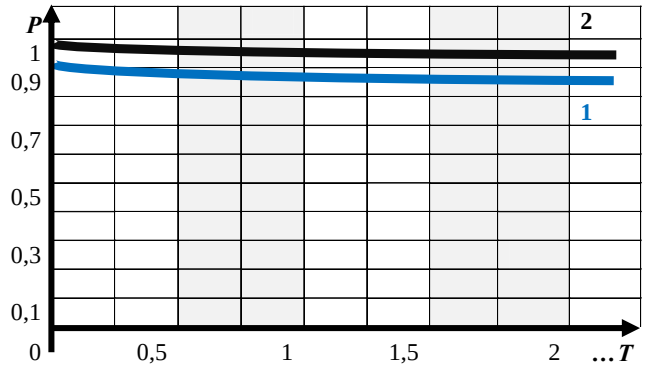

Рис. 4.3 – Вероятность безотказной работы сети до и после резервирования устройств

Приведенные результаты показывают, что вероятность безотказной работы корпоративной телекоммуникационной сети электронной коммерции в результате использовании резервирования устройств, основанного на разработанном алгоритме, повысилась до 0,9998, т.е. сеть перешла из разряда высоконадежной в разряд отказоустойчивой (см. п.1.4.2 главы 1).

В таблице 4.1 представлены значения среднего показателя безотказной передачи данных по физическому каналу связи для доступа в сеть Интернет при скорости 1 Гбит/с в течение интервала времени *T*, разделенного на периоды по 24 часа для сети АКД.

Подробно требования к каналу связи сформулированы в п. 1.7 главы 1 данной работы. Критерии, по которым предоставленный канал считается действующим или недействующим, соответствуют Рек. G.821 ITU-T.

Таблица 4.1

Средний показатель безотказной передачи данных

	Средний показатель безотказной передачи данных (в %)
t_1	99,965
t_2	99,974
t_3	99,967
t_4	99,976
t_5	99,968
t_6	99,978
t_7	99,969
t_8	99,967
t_9	99,963
t_{10}	99,971
t_{11}	99,977
t_{12}	99,978
t_{13}	99,981
t_{14}	99,982
t_{15}	99,973
t_{16}	99,971
t_{17}	99,969
t_{18}	99,972
…	…
t_L	99,975

Как видно из таблицы, канал связи на физическом уровне обеспечивает средний показатель безотказной передачи данных от 99,965% до 99,991% в течение непрерывного 24-х часового периода при скорости передачи 1 Гбит/с. В требованиях к каналу связи указывается (см.п.1.7 главы 1), что на физическом уровне этот показатель должен быть не менее 99,95% в течение 24-х часов.

В таблице 4.2 представлено сравнение экспериментальных и расчетных данных (глава 2 данной работы) при оценке аппаратурной надежности сети АКД. Данные представлены за период наблюдения t, состоящий из временных интервалов $t_1 < t_i < t_N$.

Таблица 4.2

Вероятность безотказной работы элементов сети

	Экспериментальные данные	Расчетные данные (формулы 2.1-2.5)
t_1	0,99984	0,99983
t_2	0,99981	0,99980
t_3	0,99982	0,99981
t_4	0,99983	0,99982
t_5	0,99981	0,99980
t_6	0,99984	0,99984
t_7	0,99983	0,99982
…	…	…
t_N	0,99982	0,99981

Из таблицы следует, что разница между экспериментальными и расчетными данными составляет не более $\Delta P(t_j)$=0,00001.

В таблице 4.3 представлены значения параметров качества обслуживания при передаче мультимедийного трафика АКД, полученные при использовании разработанных методов и моделей для расчета надежности (п.п. главы 2,3).

Таблица 4.3

Значения параметров QoS при передаче трафика

Тип сервиса	**Параметры качества обслуживания**			
	Допустимые значения, согласно МСЭ-Т		**Полученные значения**	
	Вероятность отказа элемента	**Вероятность потери данных**	**Вероятность отказа элемента**	**Вероятность потери данных**
IP-телефония	10^{-3}	10^{-3}	$1x10^{-3}$	$1x10^{-3}$

Видеоконференция	10^{-3}	10^{-3}	$1x10^{-3}$	$1x10^{-3}$
Цифровое видео по запросу	10^{-3}	10^{-3}	$1x10^{-3}$	$1x10^{-4}$
Передача данных	10^{-6}	10^{-6}	$1x10^{-6}$	$1x10^{-6\text{-}10}$
Телевизионное вещание	10^{-8}	10^{-8}	$0{,}5x10^{-8}$	$0{,}2x10^{-8}$

Полученные значения для вероятности отказа элемента и вероятности потери данных соответствуют допустимым значениям, согласно существующим стандартам (см. п.1.1 первой главы диссертационной работы).

На рис.4.4 схематично представлено повышение эффективности функционирования сети и ЭТП за счет применения предложенного теоретического аппарата, где график 1 – это эффективность функционирования до применения разработанных методов, алгоритмов и моделей; график 2 – результат их применения.

Здесь следует отметить, что эффективность функционирования является интегральным критерием $K_Э$:

$$K_Э(0,T) = \max \int_{t=0}^{T} K_Э(t)dt ,$$

при

$$X = \{x_i\}, i = 1,...,m ,$$

где X – множество всех параметров, от которых зависит эффективность; T - период времени функционирования ЭТП

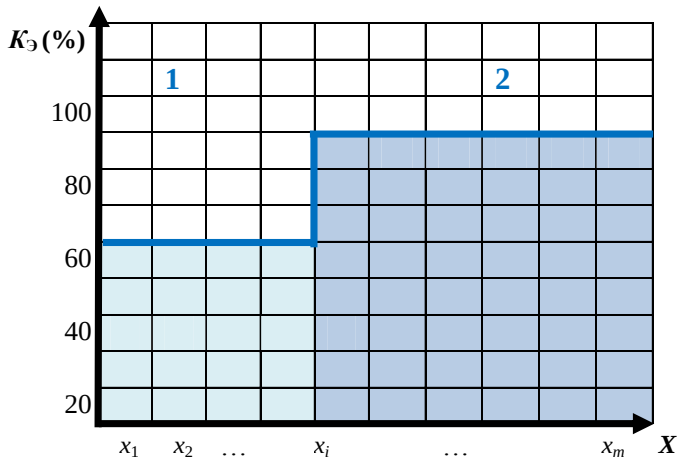

Рис. 4.4 – Повышение эффективности функционирования сети АКД/ЭТП

Критерий $К_Э$ включает (помимо показателей надежности и безопасности) и такой частный критерий как - «темп удвоения капитала», который выражается скалярной функцией времени и может быть как прогнозным (вычисляется путем математического моделирования), так и оперативным (непосредственно измеряется). На основании этого критерия оценивают стратегические и оперативные решения, например: стоит ли разрабатывать свою систему или лучше закупить предлагаемую на рынке; как формировать тарифы; в каком направлении развивать состав услуг; целесообразно ли интегрироваться с ведомственными сетями телекоммуникации и т.д.

Как видно из рисунка 4.4, эффективность функционирования сети и ЭТП за счет применения предложенного теоретического аппарата можно повысить более чем на 30%.

4.3 Программное обеспечение системы оценки надежной передачи и защиты информации ЭТП в телекоммуникационных сетях электронной коммерции

4.3.1 Состав и технические характеристики системы

В главе 1 данной работы представлена формула обеспечения надежной передачи и защиты коммерческой информации электронной торговой площадки в телекоммуникационных сетях. Согласно этой формуле разработано программное обеспечение (ПО) системы для оценки надежной передачи и защиты коммерческой информации ЭТП в телекоммуникационных сетях электронной коммерции, которое состоит из 2-х основных частей: 1-я часть – это расчет аппаратурной надежности сети; 2-я часть – обеспечение защиты коммерческой информации.

Разработанная система состоит из 4-х основных модулей:

1) ввода исходных данных;

2) расчета аппаратурной надежности сети (элементов сети, включая оборудование ЭТП);

3) защиты коммерческой информации ЭТП;

4) формирования и анализа полученных результатов для проведения торгов на ЭТП.

Реализуется ПО системы оценки надежной передачи и защиты коммерческой информации ЭТП в телекоммуникационных сетях электронной коммерции четырьмя пакетами программ:

1) пакет программ расчета и оценки аппаратурной надежности сети и оборудования ЭТП;

2) пакет программ организации управления модулями;

3) «Электронный аукцион A-K-D» // Свидетельство об официальной регистрации программ для ЭВМ № 2008613055 от 26.06.2008. – Москва. – Федеральная служба по интеллектуальной собственности, патентам и товарным знакам;

4) «Электронная торговая площадка a-k-d» // Программа для ЭВМ № 2011614170 от 27.05.2011. – Москва. – Федеральная служба по интеллектуальной собственности, патентам и товарным знакам.

Технические характеристики системы

Для работы с системой электронной торговой площадки «WWW.A-K-D.RU» необходимо выполнение следующих аппаратных и программных требований:

- ПК с операционной системой Microsoft Windows 2000 или более поздней версии (Windows XP, WindowsServer 2003, WindowsVista), оснащённый ОЗУ (оперативное запоминающее устройство) в объёме не менее рекомендованного Microsoft для установленной операционной системы.

- разрешение экрана не ниже 1024x768 точек;

- канал Интернет не менее 50 кбит/с;

- браузер MS Internet Explorer версии 6.0 и выше с включенной поддержкой файлов Cookies, JavaScript, Flash и разрешение на всплывающие окна;

- Microsoft Office 2003 - для просмотра размещенных на сайте электронной торговой площадки «WWW.A-K-D.RU» документов;

- персональный электронный почтовый ящик и почтовый клиент с возможностью просмотра писем в формате HTML;

- отсутствие ограничений на сервере организации Клиента по объему скачивания и отправки файлов на сайты зоны a-k-d.ru;

- отсутствие ограничения на скачивание и загрузку файлов с расширениями «doc» с/на сервер(а) http://www.a-k-d.ru.

4.3.2 Функционирование системы

Программное обеспечение системы позволяет контролировать процессы на различных этапах; при этом используется следующие типы данных: вводимые пользователем и справочные данные. Система имеет подсистему помощи и способна помочь пользователю, предоставив перечень необходимых действий и решений.

Модуль расчета аппаратурной надежности сети (элементов сети, включая оборудование ЭТП) базируется на разработанных методах, моделях и алгоритмах – это:

- модели расчета вероятности безотказной работы сетевых элементов;
- алгоритм резервирования устройств сети и оборудования ЭТП;
- графовая модель оценки аппаратурной надежности телекоммуникационной сети электронной коммерции и алгоритм ее анализа;
- метод оценки надежности устройств телекоммуникационных сетей электронной коммерции, критичных к задержке результатов вычислений.

На рис. 4.5 представлен фрагмент работы системы (расчет аппаратурной надежности сети).

При расчете аппаратурной надежности имеется возможность импортировать планы помещений, при этом, исходный план разделяется на участки, где каждый подплан раскрывает следующий участок детализации. Кроме этого, есть возможность отобразить схемы логических и физических связей корпоративной телекоммуникационной сети электронной коммерции.

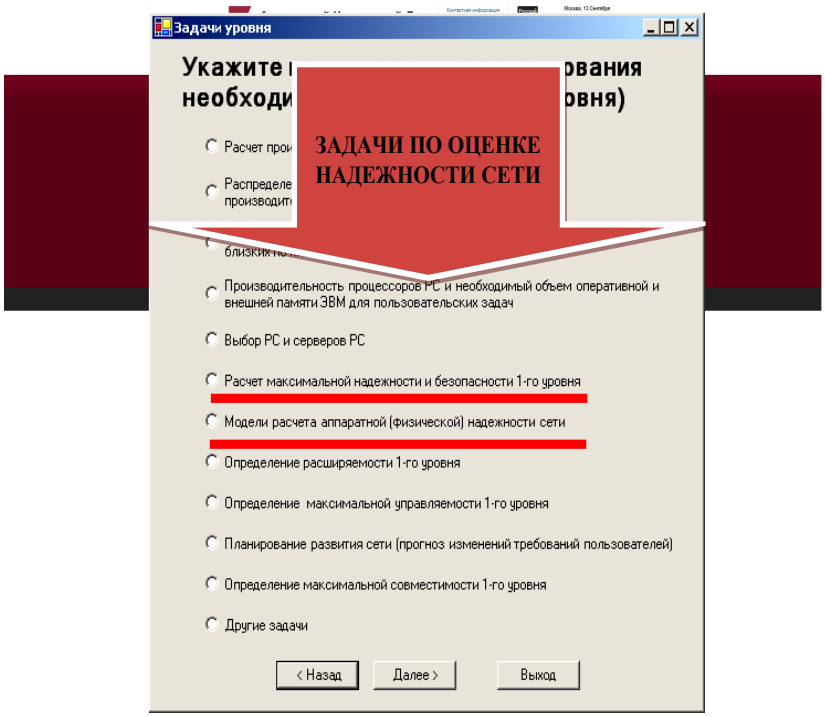

Рис. 4.5 – Выбор задач расчета надежности

Система предоставляет документацию по сети, включающую информацию об изменениях, а также позволяет создавать описание работ и другие отчеты [22, 44, 50]. Система оперирует интеллектуальными объектами, каждый из которых точно описывает представляемое им устройство или среду.

Модуль защиты коммерческой информации ЭТП базируется на следующих результатах, полученных в работе:

- методе поэтапного подписания документов ЭП для ЭТП, основанного, например на ГОСТ Р 34.11-2012, ГОСТ Р 34.10-2012 и др., с учетом современных изменений и дополнений;
- методике проверки сертификатов, проводимой сразу по 5 позициям.

При этом учитываются:

- оценочные стандарты и технические спецификации информационной безопасности;
- стандарты безопасности в сети Internet;

- требования к классу защищенности 1Г для автоматизированной системы ЭТП;
- существующие современные средства защиты информации ЭТП в телекоммуникационных сетях электронной коммерции.

На рис. 4.6 представлена информация для заказчиков и участников, о том, как стать пользователем системы ЭТП.

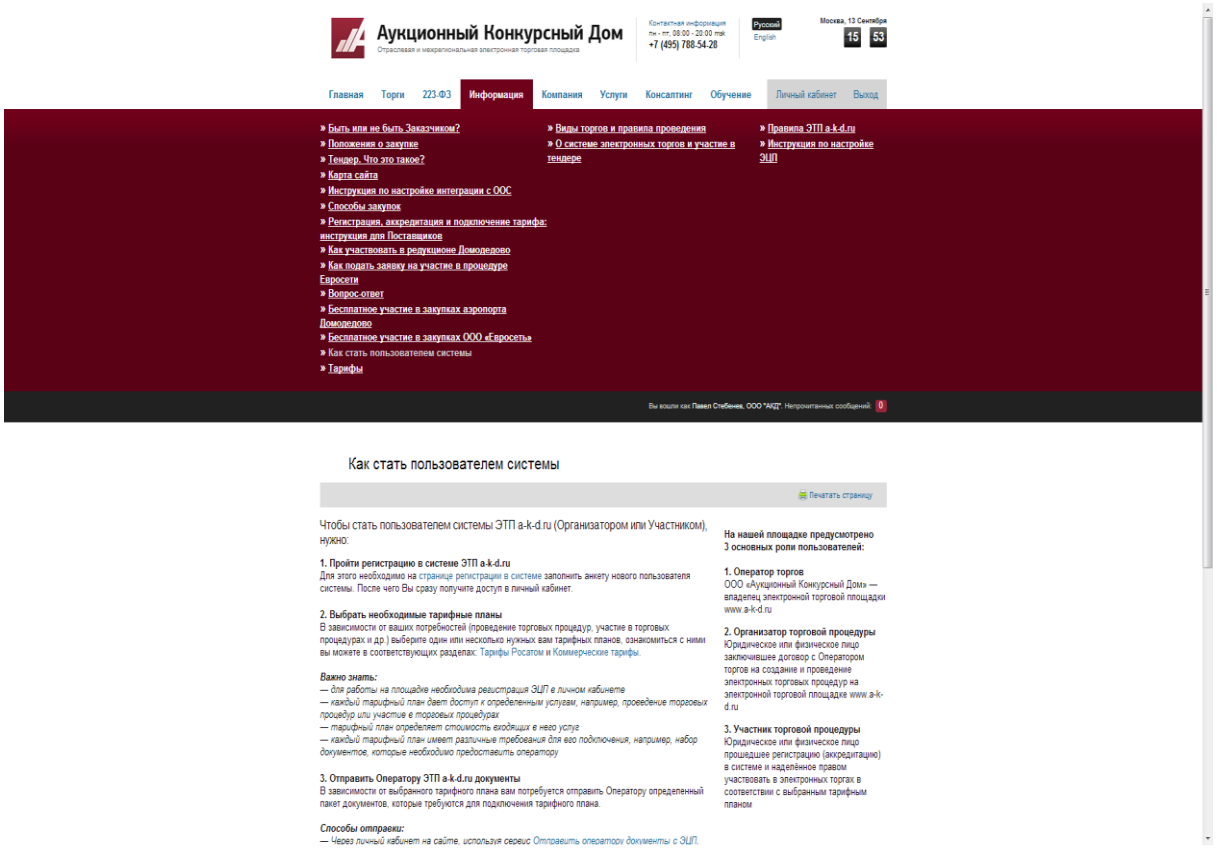

Рис. 4.6 – Информация о системе

Для работы с электронной подписью на ЭТП нужно произвести следующие действия.

В УЦ клиенту (пользователю) необходимо приобрести: сертификат ключа ЭП, носитель ключа ЭП – USB-носитель (eToken/RuToken) или дискета, программу КриптоПро CSP.

На рис. 4.7 представлена инструкция по настройке электронной подписи.

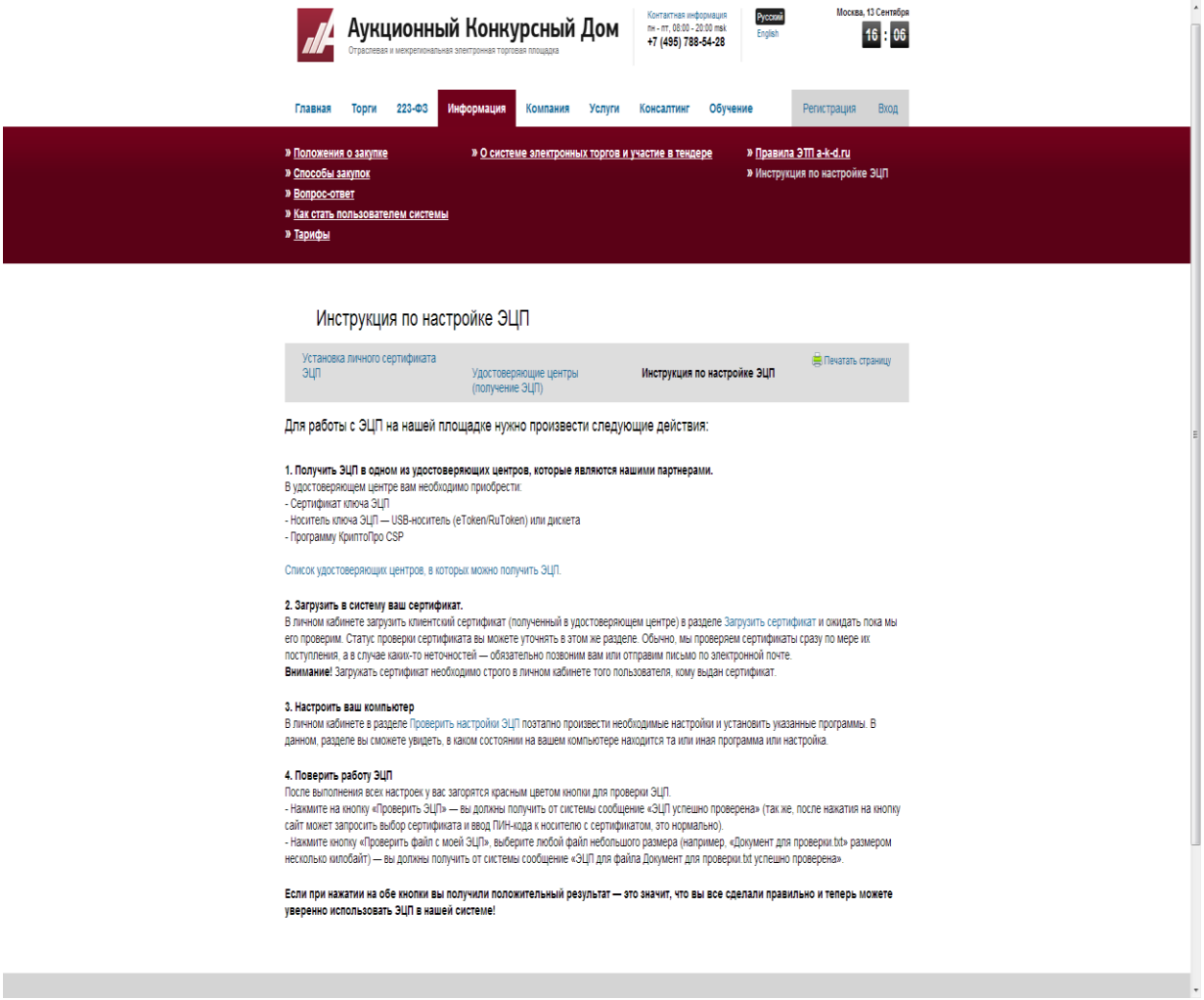

Рис. 4.7 – Настройка ЭП

На рис. 4.8 приводится образец подписи файла.

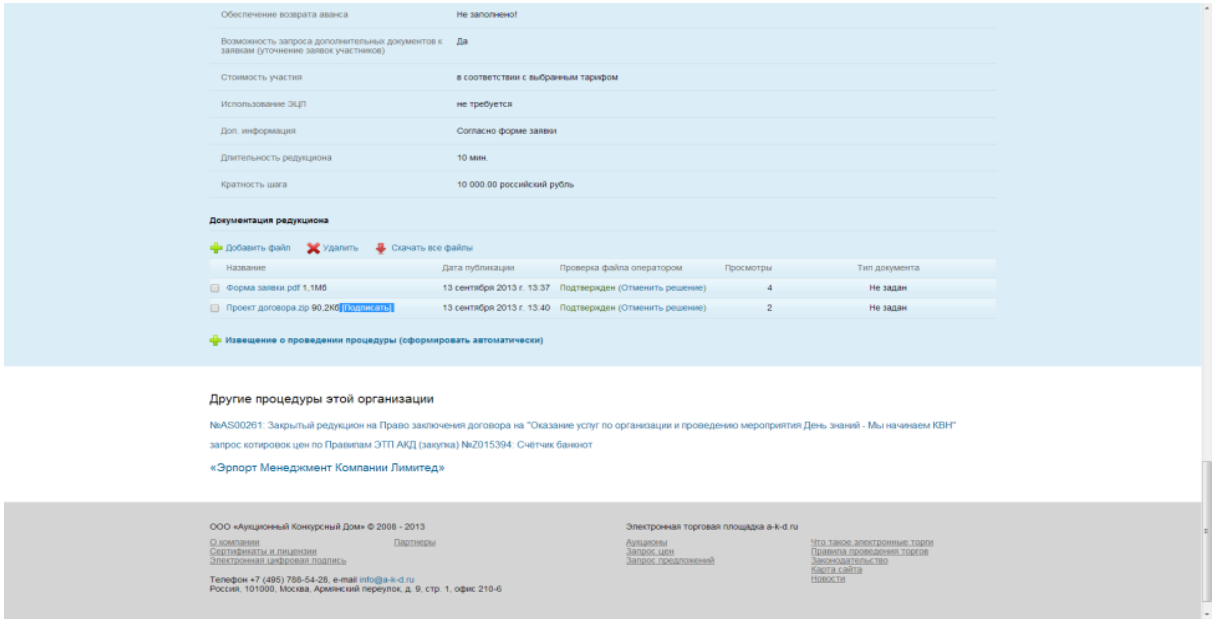

Рис. 4.8 – Образец подписи файла

При загрузке в систему сертификата клиента в личном кабинете нужно загрузить клиентский сертификат (полученный в УЦ). Далее проводится проверка сертификата и будет получен статус проверки сертификата.

В процессе настройки компьютера клиента следует произвести необходимые настройки и установить программы; при этом проводится проверка настройки ЭП и диагностика состояния на компьютере клиента программ или настроек.

Клиентский сертификат – это файл с расширением .cer, .der или .pem. В таком файле в разделе «Кому выдан» указаны ФИО клиента; в разделе «Кем выдан» указано название УЦ, в котором получена ЭП. Если неизвестно, где хранится файл с клиентским сертификатом, то его можно скопировать из USB-ключа (токен). Предполагается, что КриптоПро CSP уже установлен на клиентском компьютере.

Далее необходимо вставить в компьютер USB-устройство (токен), на котором содержится закрытый ключ клиентского сертификата и «Просмотреть сертификаты в контейнере...». Нужно выбрать контейнер с пользовательским сертификатом и посмотреть «Свойства».

На рис. 4.9 показан процесс установки личного сертификата.

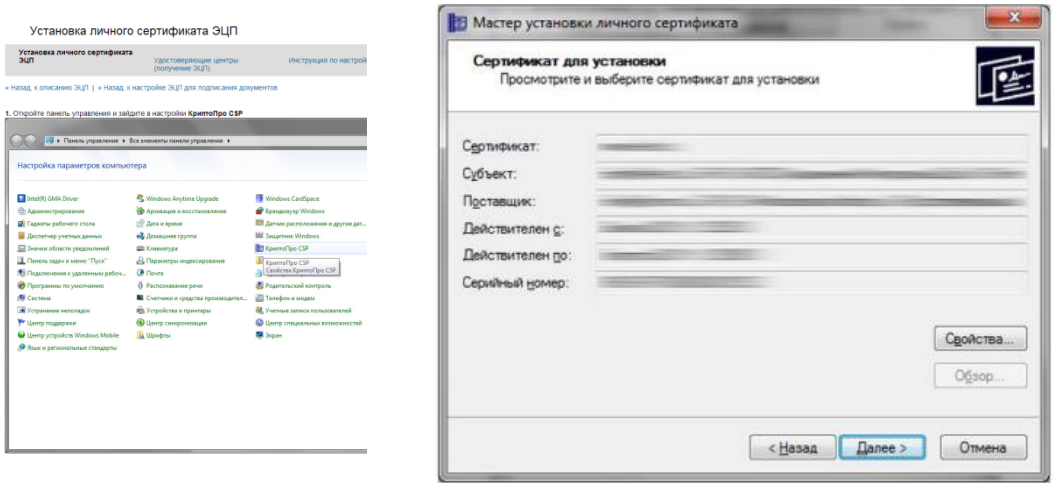

Рис. 4.9 – Установки личного сертификата

После открытия клиентского сертификата необходимо скопировать этот сертификат в отдельный файл с помощью мастера экспорта сертификатов,

предварительно выбрав место, в котором следует сохранить файл с пользовательским сертификатом.

На рис. 4.10 - 4.11 проиллюстрирована отправка дежурному оператору документов с электронной подписью и подтверждение сертификата пользователя, соответственно.

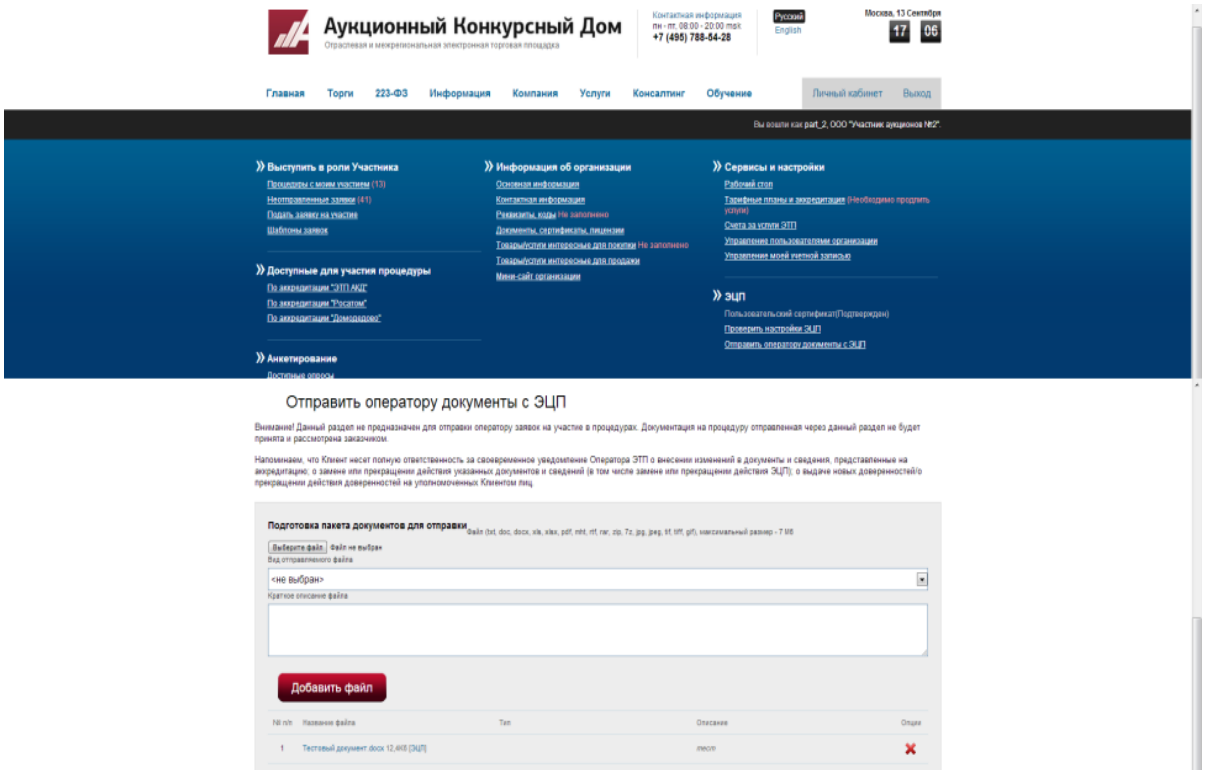

Рис. 4.10 - Отправка дежурному оператору документов с ЭП

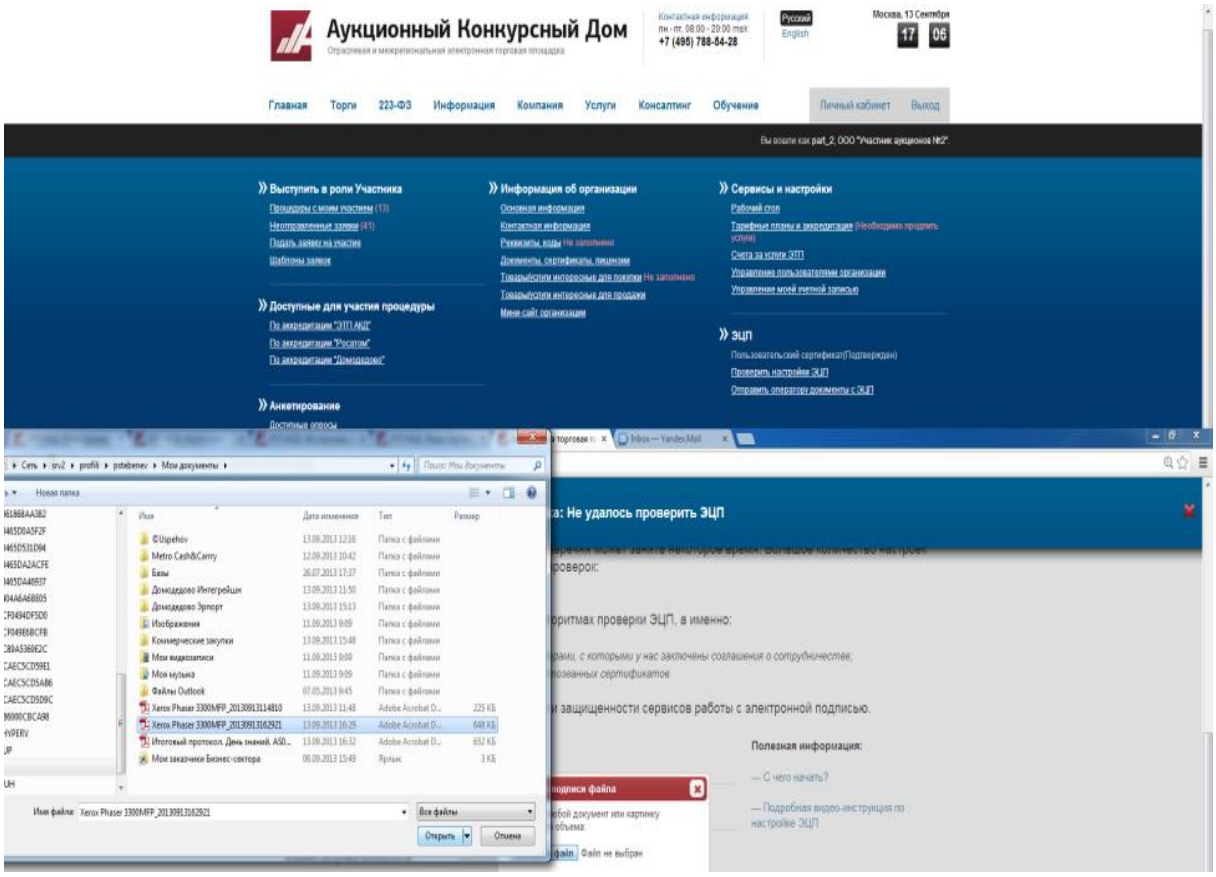

Рис. 4.11 - Пользовательский сертификат подтвержден

Поверка электронной подписи. После выполнения всех настроек необходимо провести проверку ЭП. При успешной проверке система выдает сообщение «ЭП успешно проверена». После этого может быть выдан запрос выбора сертификата и ввод ПИН-кода к носителю с сертификатом. Далее следует «Проверить файл с моей ЭП», т.е. нужно выбрать любой файл небольшого размера (например, «Документ для проверки.txt» размером несколько килобайт) и получить от системы сообщение «ЭП для файла. Документ для проверки.txt. Успешно проверена». Если клиент получил положительный результат – это значит, что все сделало правильно и можно уверенно использовать ЭП в системе АКД.

На рис. 4.12 – 4.13 представлены проверка подписи файла и проверка электронной подписи.

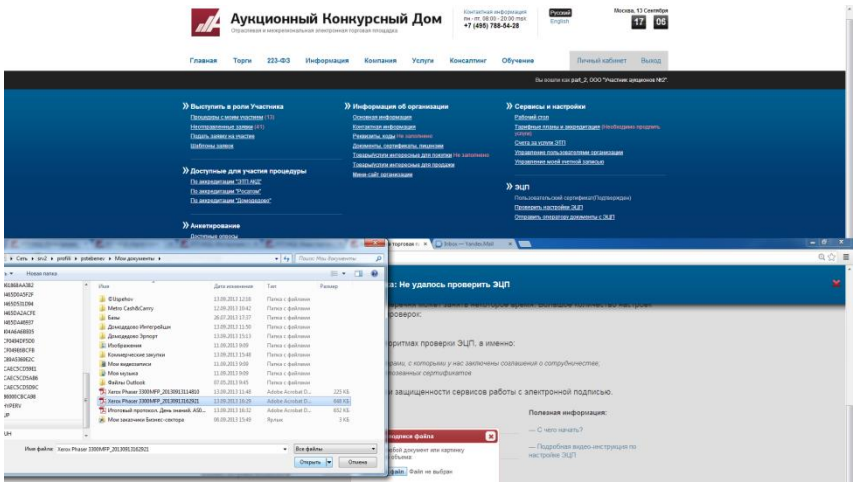

Рис. 4.12 - Проверка подписи файла

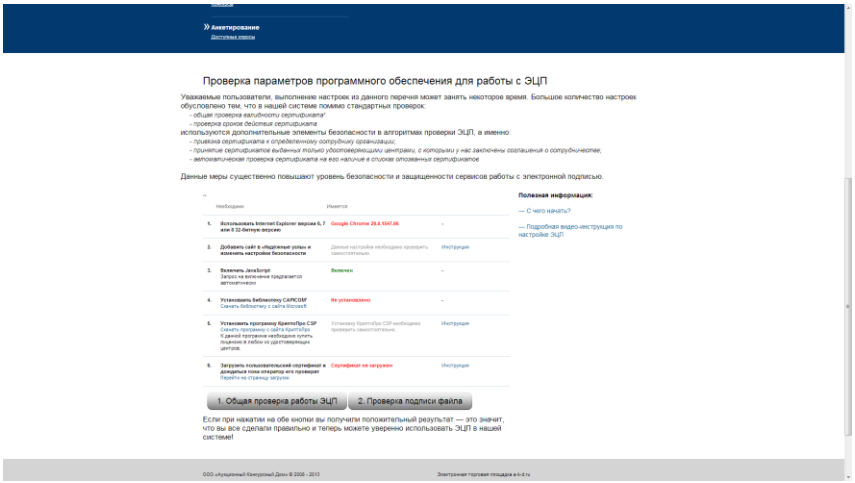

Рис. 4.13 - Проверка ЭП

Разработанное программное обеспечение системы оценки надежной передачи и защиты информации электронной торговой площадки в телекоммуникационных сетях электронной коммерции, в отличие от существующих, позволяет:

– проводить расчеты и оценку аппаратурной надежности, как отдельных элементов, так и всей сети корпоративной телекоммуникационной

сети;

– проводить обработку данных больших размерностей;

– реализовывать функции по защите коммерческой информации ЭТП;

– позволяет получать достоверные результаты.

Результаты экспериментального исследования разработанного программного обеспечения системы показали, что ее временные характеристики определяются сложностью корпоративной сети и количеством параметров.

4.4 Использование разработанного математического аппарата в автоматизированных системах электронных торгов

Одной из главных тенденции современной индустрии информатики является следование концепции открытых систем. Здесь открытость означает:

- переносимость программного обеспечения на различные аппаратные платформы;
- приспособленность к модификациям;
- интегрируемость - комплексирование с другими системами для расширения функциональных возможностей и/или придания системе новых качеств.

Важное значение для создания открытых систем имеет унификация и стандартизация среды межпрограммного интерфейса, т.е. необходимо наличие профилей для информационного взаимодействия программ, входящих в систему. Следует отметить, что профилем открытой системы называется совокупность стандартов и нормативных документов, обеспечивающих выполнения системой заданных функций [22, 82]. Можно выделить основные 4 принципа создания программного обеспечения системы оценки надежной передачи и защиты информации электронной торговой площадки в телекоммуникационных сетях электронной коммерции: системное единство, развитие, совместимость, стандартизация.

Принцип системного единства при создании, функционировании и развитии программного обеспечения должен обеспечивать целостность связей между ее компонентами.

Принцип развития состоит в том, что ПО должно создаваться и функционировать с учетом пополнения, совершенствования и обновления компонент.

Принцип совместимости должен обеспечивать совместное функционирование языков, символов, кодов, информации и связей между компонентами и сохранять открытую структуру системы в целом.

Принцип стандартизации заключается в проведении унификации, типизации и стандартизации ПО, инвариантного к исследуемым объектам [22].

В соответствии с этими общими принципами, основными требованиями, предъявляемыми к программному обеспечению системы оценки надежной передачи и защиты информации электронной торговой площадки в телекоммуникационных сетях электронной коммерции, являлись: эволюционируемость, адаптируемость, универсальность, гибкость, переносимость, экономичность, достоверность получаемых результатов, простота информационного интерфейса с пользователем.

Удовлетворение выше перечисленных требований определяет «живучесть» системы, которую можно определить, как способность сохранять эффективность ее функционирования во времени и при изменяющихся условиях. Благодаря тому, что при разработке системы оценки надежной передачи и защиты информации электронной торговой площадки в телекоммуникационных сетях электронной коммерции учитывались эти необходимые требования, система легко может быть интегрирована в автоматизированные системы электронных торгов.

Разработанные математические модели и алгоритмы расчета аппаратурной надежности корпоративных телекоммуникационных сетей предъявляют не слишком высокие к программной реализации требования и могут также использоваться в современных системах проектирования и моделирования сетей при решении задач расчета аппаратурной надежности (глава 2 диссертационной работы).

Внедрение/использование научных и практических результатов диссертационной работы представлено соответствующими актами в Приложении.

ВЫВОДЫ К ГЛАВЕ 4

1. Проведенная экспериментальная проверка разработанных методов, моделей и алгоритмов расчета аппаратурной надежности корпоративных телекоммуникационных сетей электронной коммерции показала, что точность результатов является достаточной для оценки надежности сетей и их элементов, а показатели надежности соответствуют международным стандартам, определенным в рекомендациях МСЭ-Т G.602, рек. G.821 ITU-T. Полученные значения для вероятности отказа элемента и вероятности потери данных при передаче мультимедийного трафика сети АКД/ЭТП, соответствуют допустимым значениям, согласно существующим стандартам. Разница между экспериментальными и расчетными данными при оценке вероятности безотказной работы элементов сети составляет не более $\Delta P(t_j)$=0,00001.

2. Эксперименты показали, что вероятность безотказной работы корпоративной телекоммуникационной сети электронной коммерции АКД в результате использования резервирования устройств, основанного на разработанном алгоритме повысилась до 0,9998. Канал связи на физическом уровне обеспечивает средний показатель безотказной передачи данных от 99,965% до 99,991% в течение непрерывного 24-х часового периода при скорости передачи 1 Гбит/с, при требовании не хуже 99,95%.

3. Показано, что эффективность функционирования сети и ЭТП за счет применения предложенного теоретического аппарата можно повысить более чем на 30%.

4. Представлено программное обеспечение системы оценки надежной передачи и защиты информации электронной торговой площадки в телекоммуникационных сетях электронной коммерции, разработанное на основе предложенного математического аппарата и являющиеся практическим подтверждением решения поставленной научной задачи. Определены основные принципы создания ПО системы и сформулированы требования,

предъявляемые к программному обеспечению. Удовлетворение этим требованиям определяет «живучесть» разработанной системы в целом, которая заключается в способности сохранять эффективность ее функционирования во времени и при изменяющихся условиях.

5. Разработанная система, в отличие от существующих, позволяет:

- проводить расчеты и оценку аппаратурной надежности, как отдельных элементов, так и всей сети корпоративной телекоммуникационной сети;

- реализовывать функции по защите коммерческой информации ЭТП;

- проводить обработку данных больших размерностей и получать достоверные результаты.

Результаты экспериментального исследования разработанного программного обеспечения системы показали, что ее временны*е* характеристики определяются сложностью корпоративной сети и количеством параметров. Как показала практика, при использовании системы время расчета сетевых параметров и параметров ЭТП на основе разработанного математического аппарата сокращается на 30% ÷ 50%.

6. Обосновано практическое применение, предложенного математического аппарата и разработанного на его основе ПО системы оценки надежной передачи и защиты информации электронной торговой площадки в телекоммуникационных сетях электронной коммерции для современных автоматизированных систем электронных торгов.

ЗАКЛЮЧЕНИЕ

Основные результаты теоретических и экспериментальных исследований, проведенных в диссертационной работе в соответствии с поставленной научной задачей, могут быть сформулированы следующим образом:

1. Исследованы средства интеллектуализации бизнес-процессов. Показано, что электронная коммерция объединяет множество коммуникационных технологий, а самой распространенной, простой и удобной формой применения систем электронной торговли являются электронные торговые площадки (ЭТП). Проанализированы существующие способы обеспечение надежности функционирования автоматизированных систем электронных торгов. Показано, что системы электронных торгов переходят с уровня электронных торговых площадок на уровень полномасштабных систем управления торгово-закупочной детальностью с использованием телекоммуникационных сетей, следовательно, основой электронной коммерции являются телекоммуникационные сети. Проанализированы особенности использования телекоммуникационных сетей в электронной коммерции, выявлены основные критерии эффективности их работы. Проведенный анализ показал, что к таким сетям предъявляются повышенные требования к надежности передачи и защите информации.

2. Разработан метод оценки надежности устройств телекоммуникационных сетей электронной коммерции, критичных к задержке результатов вычислений, позволяющий определить и прогнозировать вероятность выхода из строя узла/элемента сети и ЭТП, как при обслуживании заявок электронной торговой площадки, так и в свободном состоянии.

3. Разработаны графовая модель оценки аппаратурной надежности телекоммуникационной электронной коммерции сети и алгоритм ее анализа, позволяющие:

- проверять правильность проектных решений, находить «слабые места» и применять существенные меры по повышению надежности сетей, а также эффективности их функционирования, обеспечивая необходимую надежность передачи коммерческой информации ЭТП по

телекоммуникационным сетям;

- проводить оптимизацию аппаратурной надежности для широко спектра сетей;
- проводить многоуровневое моделирование с учетом специфики работы сетевых устройств разных уровней,
- прогнозировать стратегию модернизации и развития корпоративных сетей электронной коммерции.

4. Разработан алгоритм резервирования устройств корпоративной телекоммуникационной сети электронной коммерции и ЭТП, который в отличие от уже существующих требует значительно меньше вычислительных ресурсов (примерно в 1,5 раза), и позволяет за небольшое число шагов получать удовлетворительные результаты. Как показывает практика, задачи оптимизации аппаратурной надежности сетевых элементов не отличаются точностью и достоверностью, и использование строгих методов дискретной оптимизации является с практической точки зрения некорректным, но в приближенных методах каждый элемент характеризуется обязательным возрастанием показателя надежности при росте суммарных затрат. С учетом этого, разработанный алгоритм основан на методе наискорейшего покоординатного спуска, а процесс создания оптимальной резервированной системы, т.е. какого-либо участка или элемента сети, а также ЭТП представляется в виде многошагового процесса. На первом шаге определяется такая подсистема, добавление к которой одного резервного элемента дает наибольший «удельный» выигрыш в приросте показателя аппаратурной надежности в целом. На втором шаге определяется следующая подсистема (включая и ту, к которой был добавлен резервный элемент), характеризующаяся тем, что добавление к ней одного резервного элемента дает опять наибольшее относительное приращение результирующего показателя надежности. Аналогичным образом процесс построения оптимальной системы продолжается далее. Разработанный алгоритм позволяет эффективно реализовать резервирование элементов сети и ЭТП, обеспечив не только заданные показатели надежности, но и добиться этого как можно более экономично, с наименьшими суммарными затратами на резервные элементы,

либо при заданных ресурсных ограничениях достичь максимально возможной аппаратурной надежности всей сети. Алгоритм проверен на большом числе практических примеров и показал свою эффективность.

5. Проведен анализ методов и средств обеспечения информационной безопасности в телекоммуникационных сетях электронной коммерции. Исследованы преимущества использования хэш-функций в схемах электронной подписи для зашиты коммерческой информации ЭТП в телекоммуникационных сетях. Разработан эффективный метод поэтапного подписания документов ЭП для электронной торговой площадки, который содержит 8 основных этапов: подготовка данных; получение комплекта ЭП; подготовка к работе с ЭП; проверка данных; проверка сертификатов оператором ЭТП; использование ЭП; проверка ЭП, принятие решения об участии пользователя в электронных торгах. Метод основан на современных ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012. Обосновано применение ГОСТ Р 34.11-2012 в схеме ЭП – подписываемые документы ЭТП имеют переменный и/или большой объем, поэтому электронная подпись ставится не на сам документ, а на его хэш, следовательно, целесообразно применять хэш-функцию для защиты информации ЭТП в телекоммуникационных сетях электронной коммерции. Как показали исследования, производительность нового алгоритма ГОСТ Р 34.11-2012, используемого в разработанном методе для схемы ЭП примерно в 1,5 раза выше, чем у предыдущего стандарта.

6. Разработана методика проверки сертификатов, которая является уникальной и позволяет проводить проверку сертификатов сразу по 5 позициям. Это - проверка сроков действия пользовательского сертификата, сроков действия корневого сертификата, наличие соответствующего корневого сертификата в базе, проверка в списках отозванных, соответствия пользователя и сертификата. Имеющиеся аналоги проводят проверку только по 1 или 2 позициям. Следовательно, разработанная методика позволяет более, чем в 2 раза повысить эффективность защиты коммерческой информации ЭТП в телекоммуникационных сетях.

7. Разработана процедура принятия решения ЛПР (это сотрудники ЭТП) об участии пользователя в электронных торгах. Анализ существующих

подходов к реализации этой задачи показал целесообразность принятия решения на базе экспертных процедур, где наиболее эффективным является метод анализа иерархий, так как:

- метод дает возможность провести декомпозицию и анализ проблемы оценивания альтернативных решений в конкретной ситуации;
- позволяет учитывать предпочтения ЛПР на множестве критериев и требуется только определить важность критерия путем их попарного сравнения;
- иерархическое представление дает ЛПР простую для понимания картину влияния изменений приоритетов на верхних уровнях на приоритеты элементов нижних уровней;
- метод достаточно хорошо автоматизируется.

8. Проведенная экспериментальная проверка разработанных методов, моделей и алгоритмов расчета аппаратурной надежности корпоративных телекоммуникационных сетей электронной коммерции показала, что точность результатов является достаточной для оценки надежности сетей и их элементов, а показатели надежности соответствуют международным стандартам, определенным в рекомендациях МСЭ-Т G.602, рек. G.821 ITU-T. Полученные значения для вероятности отказа элемента и вероятности потери данных при передаче мультимедийного трафика АКД, соответствуют допустимым значениям, согласно существующим стандартам. Разница между экспериментальными и расчетными данными при оценке вероятности безотказной работы элементов сети и ЭТП составляет не более $\Delta P(t_j)$=0,00001. Эксперименты показали, что вероятность безотказной работы корпоративной телекоммуникационной сети электронной коммерции АКД в результате использования резервирования устройств, основанного на разработанном алгоритме повысилась до 0,9998. Канал связи на физическом уровне обеспечивает средний показатель безотказной передачи данных от 99,965% до 99,991% в течение непрерывного 24-х часового периода при скорости передачи 1 Гбит/сек, при требовании не хуже 99,95%. Эффективность функционирования сети и ЭТП за счет применения предложенного теоретического аппарата может повыситься более чем на 30%.

9. Разработано программное обеспечение системы оценки надежной передачи и защиты информации электронной торговой площадки в телекоммуникационных сетях электронной коммерции, созданное на основе предложенного математического аппарата и являющиеся практическим подтверждением решения поставленной научной задачи. Определены основные принципы создания ПО системы и сформулированы, предъявляемые к нему требования. Удовлетворение этим требованиям определяет «живучесть» разработанной системы в целом, которая заключается в способности сохранять эффективность ее функционирования во времени и при изменяющихся условиях. Разработанная система, в отличие от существующих, позволяет:

- проводить расчеты и оценку аппаратурной надежности, как отдельных элементов, так и всей сети, включая ЭТП;
- проводить обработку данных больших размерностей и получать достоверные результаты.
- реализовывать функции по защите коммерческой информации ЭТП и Экспериментальное исследование разработанного программного обеспечения системы показали, что ее временные характеристики определяются сложностью корпоративной сети и количеством параметров. При использовании системы время расчета сетевых параметров и параметров ЭТП на основе разработанного математического аппарата сокращается на 30% ÷ 50%.

Обосновано практическое применение, предложенного математического аппарата и разработанного на его основе ПО системы оценки надежной передачи и защиты информации электронной торговой площадки в телекоммуникационных сетях электронной коммерции для современных автоматизированных систем электронных торгов.

Таким образом, в диссертационной работе была решена актуальная научная задача, имеющая важное теоретическое и практическое значение.

ЛИТЕРАТУРА

1. Artalejo J.R. G – networks: versatile approach for work removal in queuing networks // European Journal of Operational Research. 2000.V.125.P.233-249.
2. CableProotExan Software URL: http://www.win-uk.net/~exan/exan.htm (дата обращения: 03.10.2012).
3. Chakravarthy S. The batch markovian arrival process: a review and future work // Advances in probability theory and stochastic processes. 2001. № 3. P. 21-39.
4. Computer Emergency Response Team URL: ftp://cert.cei.cms.edu /pub/cert_advisories (дата обращения: 20.08.2012).
5. Graham Paul Hackers & Painters: Big Ideas from the Computer Age. O'Reilly Media. – 2013. - 276с.
6. http://www.pcweek.ru/ (дата обращения: 08.03.2012).
7. Kouns Jake, Minoli Daniel. Information Technology Risk Management in Enterprise Environments: A Review of Industry Practices and a Practical Guide to Risk Management Teams. Jake Kouns, Daniel Minoli. – 2013. - 421с.
8. Mao W., Hall P. Modern Cryptography: Theory & Practice // Professional Technical Reference. New Jersey. 2004. - 308 p.
9. Tomlinson A. Introduction to the TPM // Smart Cards, Tokens, Security and Applications/ Springer, 2012. С. 155 -172.
10. Андронов А.В., Королев П.Е. Проектирование беспроводных сетей Wi-Fi по критерию качества обслуживания // Качество и ИПИ (CALS) - технологии. 2006. № 3 (11). С. 6-10.
11. Афанасьев В.В., Волков Н.В., Максименко В.Н. Защита информации в сетях сотовой подвижной связи [под ред. О.Б.Макаревич]. М.:РиС, 2007. - 360 с.
12. Афонина С.В. Электронные Деньги. СПБ: Питер, 2001. – 180с.
13. Ачилов Р. Построение защищенных корпоративных сетей. ДМК Пресс. – 2013. – 250с.
14. Бакланов И. Г. NGN: принципы построения и организации. М.: Эко-Трендз, 2008. - 400с.

15. Балабанов И.Т. Электронная коммерция, Учебное пособие для вузов, СПб, 2001. – 300 с.
16. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности. Учебное пособие для вузов. М.: Горячая линия – Телеком, 2006. 544с.
17. Бельтов А.Г., Жуков И.Ю., Михайлов Д.М., Стариковский А.В. Технологии мобильной связи. Услуги и сервисы. Инфра-М. 2012. - 208с.
18. Берлин А. Н. Коммутация в системах и сетях связи. М.: Эко-Трендз, 2006. 344с.
19. Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А. Элементарное введение в эллиптическую криптографию. Алгебраический и алгоритмические основы. М: КомКнига, 2006. 328с.
20. Бройдо В.Л., Ильина О.П. Вычислительные системы, сети и телекоммуникации. Книга по Требованию. – 2013. – 560с.
21. Вадим Эйдлин. Все, что нужно знать для создания успешного коммерческого Интернет проекта. URL: http://www.vadimeidlin.com/e-dictionary.htm (дата обращения: 02.06.2012).
22. Василенко Н.В., Макаров В.А. Модели оценки надежности программного обеспечения //Вестник новгородского государственного университета. - 2004. - №28. – С.126 - 132.
23. Васильев М., Хомков И., Кравченко С., Шаповаленко С. Моделирование и анализ корпоративных информационных систем.URL: www.pcweek.ru (дата обращения: 03.08.2013).
24. Вентцель Е.С. Теория вероятностей. М.: Высшая школа, 1999.749с.
25. Виноградов Н.Н. Защита компьютерной информации. Эффективные методы и средства. ДМК–Пресс. 2010. 387с.
26. Вишневский В.М. Теоретические основы проектирования компьютерных сетей. М.: Техносфера, 2003. 396 с.
27. Гольдштейн Б.С., А. Е. Кучерявый А.Е. Сети связи пост-NGN. БХВ-Петербург. – 2013. – 160с.
28. Гончаров В.А. Методы оптимизации. М.: Высшее образование, 2008. 91с.
29. ГОСТ Р 34.10-2012: Национальный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации.

Процессы формирования и проверки электронной цифровой подписи. Издание официальное. М.: Стандартинформ. 2012.

30. ГОСТ Р 34.10-94 Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма. М. Госстандарт России. 1995.
31. ГОСТ Р 34.11-2012: Национальный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция хэширования. Издание официальное. М.: Стандартинформ. 2012.
32. ГОСТ Р 34.11-94: Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция хэширования. Издание официальное. М. Госстандарт России. 1995.
33. Гулевич Д.С. Сети связи следующего поколения. Интернет-университет информационных технологий, 2008. 183 с.
34. Демченко Ю.В. Архитектура безопасности INTERNET и компьютерных сетей на основе протоколов TCP/IP. URL: http://cad.ntu-kpi.kiev/ua/~demch/ (дата обращения: 21.12.2012).
35. Дианова Т. Некоторые особенности электронной торговли: от «мифов» к «эффекту скольжения» // Вопросы экономики. 2012. № 05. С. 139-146.
36. Дудин А.Н., Клименок В.И. Системы массового обслуживания с коррелированными потоками. Мн.: Изд-во Белорус. Ун-та, 2000. 120 с.
37. Ершов Ю. Л., Палютин Е. А. Математическая логика: Учебное пособие. СПб: Лань, 2004. 336с.
38. Жуков Ю. Основы веб-хакинга. Нападение и защита. Книга по Требованию. – 2013. - 208с.
39. Запечников С.В. Основы построения виртуальных частных сетей. М.: Горячая линия–Телеком, 2006. 249 с.
40. Защита информации и Информационная безопасность. [сайт]URL: http://zashita-informacii.ru (дата обращения: 01.06.2013).
41. Клейнрок Л. Вычислительные системы с очередями. М.: Мир, 1979. 432с.

42. Кнэпп Э. Эллиптические кривые. // Пер. с англ. Попеленского Ф.Ю. М.: Факториал Пресс, 2004. 488с.
43. Коваленко И.Н., Филиппова А.А. Теория вероятностей и математическая статистика. М.: Высшая школа, 1982. 256 с.
44. Корнеев И.Н., Фень С.Г. Сетевые структуры телекоммуникационной индустрии. М.: Горячая линия-Телеком, 2005. 136 с.
45. Корпоративные сети банков // Pcweek. 2005. № 26.
46. Корячко В.П., Д. А. Перепелкин Д.А. Анализ и проектирование маршрутов передачи данных в корпоративных сетях. Горячая Линия - Телеком. - 2013. - 236 с.
47. Костин М.В., Костина А.В. Имитационное моделирование системы передачи конфиденциальной информации в широковещательных каналах связи: [портал GPSS.RU]. URL: http://www.gpss.ru/immod05/s2/kostin/ (дата обращения: 20.05.2013).
48. Ларичев О.И. Теория и методы принятия решений. М.: Логос, 2000. 296с.
49. Линец Г.И., Турлянский Я.В., Калаханов Р.Х. Моделирование законов распределения случайных величин, используемых при проектировании телекоммуникационных сетей // Материалы XI регион.науч.-техн. конф.: Вузовская наука – Северо-Кавказскому региону. Ставрополь: СевКавГТУ. Т.1. 2007. 278 с.
50. Маклафлин Б., Поллайс Г., Уэст Д. Объектно-ориентированный анализ и проектирование. Питер. – 2013. 608с.
51. Малюк А.А. Теория защиты информации. М.: Горячая линия-Телеком. 2012. 150с.
52. Матвеев И.А. Электронная экономика: сущность и этапы развития. //Управление экономическими системами: электронный научный журнал. № гос.рег.статьи: 0421200034/. [Электронный ресурс]. Публикация от 29.06.12. URL: http:// uecs.ru (дата обращения 01.09.2012).
53. Международные стандарты по оценке безопасности информационных технологий. [сайт]URL: http://deHack.ru (дата обращения: 10.05.2013).
54. Мелтон Кит Офисный шпионаж. Альпина нон-фикшн. – 2013. -192с.
55. Мещеряков Р.В. Технические средства и методы защиты информации. М.: Горячая линия – Телеком. 2012. 320с.

56. Моисеев Н.Н. Математические задачи системного анализа. Либроком. - 2013. – 492с.
57. Мушик Э., Мюллер П. Методы принятия технических решений. М.: Мир, 1990. 197 с.
58. Нахавандипур Вандад iOS. Разработка приложений для iPhone, iPad и iPod. Питер. – 2013. – 864с.
59. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы. СПб.: Питер, издание - 4, 2009. 958 с.
60. Поляк-Брагинский А.В. Локальные сети. Модернизация и поиск неисправностей. СПб.: BHV, 2008. 832 с.
61. Поляков К.А., Мобильная торговая платформа в российских банках – вопрос ближайшего времени // i-business.ru – 28.09.2012
62. Поляков К.А., Компании получили возможность работать в условиях открытой конкуренции // Журнал Коммерческий Директор – 2013 №1 – С. 100-107
63. Поляков К.А., Колонка Полякова Кирилла – Новости законодательства электронной коммерции // Электронная торговая площадка Госкорпорации «Росатом» a-k-d.ru – 2012
64. Поляков К.А. В электронной форме закупкам придаётся больше огласки // Atominfo.ru – декабрь 2012
65. Поляков К.А. Учимся проводить аукцион в электронной форме // Атомекс. 2009. № 2. С. 34 - 36.
66. Поляков К.А. К вопросу о повышении надежности функционирования телекоммуникационных сетей при использовании их в электронной коммерции // Качество. Инновации. Образование. – 2013. - № 93. С.5
67. Поляков К.А. Компания получила возможность работать в условиях открытой конкуренции. //Коммерческий директор. 2013. № 1.–С.100-107.
68. Поляков К.А., Сафонова И.Е., Голдовский Я.М. Оптимизация аппаратурной надежности корпоративных телекоммуникационных сетей // Телекоммуникации. - 2013. - № 3. - С. 6 – 9,
69. Поляков К.А., Сафонова И.Е., Иванов В.В. Графовая модель расчета аппаратурной надежности корпоративной телекоммуникационной сети // Телекоммуникации. 2012. № 12. С. 7 – 9.

70. Пролетарский А.В., Баскаков И.В. Беспроводные сети Wi-Fi. М.: Бином, 2007. 215с.
71. ПроферансовД.Ю. Особенности современной корпоративной телекоммуникационной инфраструктуры Proceedings of Fifth International Conference «Information and Telecommunication Technologies in Intelligent systems», France, 2011,p.44-48.
72. Проферансов Д.Ю., Сафонова И.Е. Многоуровневая графовая модель корпоративной телекоммуникационной сети // Телекоммуникации. - 2011. - № 11. - С. 2 – 5.
73. Пятибратов А.П., Гудыно Л.П., Кириченко А.А. Вычислительные системы, сети и телекоммуникации. СПб.: Питер, 2009. 734 с.
74. Росляков А.В. Виртуальные частные сети - основы построения и применения. М.: Эко-Трендз, 2006. 304 с.
75. Рэндалл Н., Сосински Б. Беспроводные решения. М.: Техносфера, 2007. 376 с.
76. Саати Т.Л. Принятие решений при зависимостях и обратных связях // Пер.с англ. Андрейчикова О.Н. М.: Либроком. 2009. – 360с.
77. Сафонова И.Е. Методика качественной оценки надежной работы сервера корпоративной сети и отображение состояний его работоспособности // Качество и ИПИ (CALS)-технологии. - 2006. - № 1. - С. 2-10.
78. Сафонова И.Е., Королев П.Е. Методика оценки надежной работы серверов корпоративной сети // Научный вестник МГТУ ГА. Серия – Прикладная математика. Информатика. - 2006. - № 105. - С. 42 - 50.
79. Семёнов Ю.А. «Телекоммуникационные технологии» [2008]. URL: http://www. book.itep.ru (дата обращения: 23.05.2012).
80. Семенов Ю.А. Алгоритмы телекоммуникационных сетей. В 3-х частях. Часть 3: Процедуры, диагностика, безопасность. М.: Бином. 2007. 511с.
81. Семенов Ю.А. Телекоммуникационные технологии [2008]. URL: http://www. book.itep.ru (дата обращения: 23.05.2012).
82. Семенов Ю.А. Электронная торговля в Интернет [Электронный ресурс]. URL: http://www. book.itep.ru (дата обращения: 23.05.2012).
83. Сердюк В.А. Новое в защите от взлома корпоративных систем. М.: Техносфера, 2007. 360 с.

84. Серр Ж.-П. Абелевы l-адические представления и эллиптические кривые. А-Медиа. 2012. 192с.
85. Скорняков Л.А. Абелевы группы и модули. А-Медиа. 2012. 356с.
86. Скотт Хогдал Дж. Анализ и диагностика компьютерных сетей. М.: Лори, 2007. 354 с.
87. Смирнова Е.В., Козик П.В. Технологии современных сетей Ethernet. Методы коммутации и управления потоками данных. БХВ-Петербург. – 2013. - 272 с.
88. Соловьев Ю.П. Гипотеза Таниямы и последняя теорема Ферма. [Соросовский образовательный журнал]. URL: http://www.pereplet.ru/obrazovanie/stsoros/500.html (дата обращения: 20.04.2013).
89. Сычев К.И. Многокритериальное проектирование мультисервисных сетей связи // Телекоммуникации. 2007. № 9.С.2– 7.
90. Таненбаум Э. Компьютерные сети. СПб.: Питер, 2008. 992 с.
91. Таненбаум Э., Уэзеролл Д. Компьютерные сети. Питер. – 2013. – 960с.
92. Томсетт Роб Экстремальное управление проектами. Лори. -2013. – 292с.
93. Трулав Джеймс Сети. Технологии, прокладка, обслуживание. М.: НТ Пресс, 2007. 560с.
94. Уилсон Эд. Мониторинг и анализ сетей. Методы выявления неисправностей. Лори. – 2013. - 386с.
95. Ушаков И.А. Вероятностные модели надежности информационно-вычислительных систем. М.: Радио и связь, 1991. 132 с.
96. Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи».
97. Филимонов А.Ю. Построение мультисервисных сетей Ethernet. СПб.: BHV, 2007. 592с.
98. Фишман Е.Б. Анализ алгоритмов обслуживания очередей в сетях с поддержкой «качества обслуживания» (QoS) // Качество. Инновации. Образование. 2006. № 6. С. 63-71.
99. Хамадулин Э.Ф. Методы и средства измерений в телекоммуникационных системах . М.: Высшее образование, 2009. 365 с.
100. Черноруцкий И.Г. Методы принятия решений. СПб.: BHV, 2005. 416с.

101. Шапкин Ю.А., Сафонова И.Е., Целевая функция для оптимизации вероятности безотказного функционирования и критерий гарантированного запаса работоспособности устройств корпоративной сети // Научный вестник МГТУ ГА. Серия - Прикладная математика. Информатика. - 2006. -№ 105. - С.140-143.
102. Шепитько Г. Теория информационной безопасности и методология защиты информации. М.: РГСУ. 2012. 135с.
103. Шляхтина С. Электронная коммерция - все быстрее, надежнее, привычнее. // КомпьютерПресс. 2005. № 2. С. 5 – 20.
104. Шнайер Б. Прикладная криптография. 2-е издание. Протоколы, алгоритмы и исходные тексты на языке Си. М.: Триумф, 2002. 816с.
105. Юдин Д.Б. Вычислительные методы теории принятия решений. Либроком. – 2013. – 320с.
106. Ямпольский В. З., Комагоров В. П., Солдатов В. Н. Моделирование сетей: [портал GPSS.RU]. [2005]. URL: http://www.gpss.ru//immod05/s3/ (дата обращения: 13.09.2012).

ПРИЛОЖЕНИЕ

Акты использования результатов диссертационной работы