

Федеральное государственное автономное образовательное
учреждение высшего образования
«Омский государственный технический университет»

На правах рукописи



Сагайдак Дмитрий Анатольевич

МОДЕЛИ И АЛГОРИТМЫ РЕАЛИЗАЦИИ
СИСТЕМНОГО ПОДХОДА К ОРГАНИЗАЦИИ
РАСПРЕДЕЛЕННОЙ ПЕРЕДАЧИ ВИДЕОДАНЫХ

Специальность 2.3.1. Системный анализ,
управление и обработка информации, статистика

ДИССЕРТАЦИЯ
на соискание ученой степени
кандидата технических наук

Научный руководитель:
доктор технических наук, профессор
Денисова Людмила Альбертовна

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ.....	4
1 ПРОБЛЕМЫ РАСПРЕДЕЛЕННОЙ ПЕРЕДАЧИ ВИДЕОДАНЫХ	16
1.1 Современное состояние вопроса распределенной передачи видеоданных в многоканальных системах связи.....	16
1.2 Анализ работ по использованию методов и алгоритмов кодирования видеоданных.....	21
1.3 Обзор систем параллельной обработки и передачи данных.....	29
1.4 Аналитический метод исследования систем распределенной передачи данных	33
1.5 Имитационное моделирование и оптимизация систем передачи данных	35
1.6 Выводы по главе	38
2 РАЗРАБОТКА АЛГОРИТМОВ КОДИРОВАНИЯ ИЗОБРАЖЕНИЙ НА ОСНОВЕ СХЕМ РАЗДЕЛЕНИЯ ДАННЫХ	41
2.1 Разработка алгоритма деления изображений по дробным частям десятичных чисел	41
2.2 Разработка алгоритма деления изображений с помощью префиксного кодирования	50
2.3 Исследование возможности восстановления закодированных изображений	59
2.4 Выводы по главе	66
3 РАЗРАБОТКА МЕТОДИКИ АНАЛИТИЧЕСКОГО РАСЧЕТА ПРОПУСКНЫХ СПОСОБНОСТЕЙ КАНАЛОВ СВЯЗИ	68
3.1 Постановка задачи оптимизации пропускных способностей каналов связи .	68
3.2 Исследование системы с независимыми каналами связи	72
3.3 Оптимизация двухканальной системы связи с разделением видеокадров в постоянном соотношении и их синхронной передачей	75
3.4 Исследование пропускных способностей каналов при отсутствии синхронной передачи данных в двухканальной системе связи	85
3.5 Выводы по главе	91
4 ИМИТАЦИОННАЯ МОДЕЛЬ ДВУХКАНАЛЬНОЙ СИСТЕМЫ С РАЗДЕЛЕНИЕМ ДАННЫХ ПО КАНАЛАМ СВЯЗИ	93
4.1 Обоснование подхода к решению задачи оптимизации параметров двухканальной системы связи как многокритериальной.....	93
4.2 Разработка имитационной модели двухканальной системы связи и решение задачи оптимизации с учетом стоимостных и временных характеристик	97

4.3 Оценка достоверности результатов имитационного моделирования.....	110
4.4 Выводы по главе.....	117
5 КОМПЛЕКС ПРОГРАММ И РЕЗУЛЬТАТЫ ЭКСПЕРИМЕНТАЛЬНЫХ ИССЛЕДОВАНИЙ РАСПРЕДЕЛЕННОЙ ПЕРЕДАЧИ ДАННЫХ В ДВУХКАНАЛЬНОЙ СИСТЕМЕ СВЯЗИ.....	120
5.1 Описание структуры и функционирования проблемно-ориентированного программного комплекса.....	120
5.2 Формирование набора кодированных видеокадров для распределенной передачи.....	128
5.3 Проведение экспериментальных исследований распределённой передачи видеоданных.....	134
5.4 Выводы по главе.....	140
ЗАКЛЮЧЕНИЕ	141
СПИСОК СОКРАЩЕНИЙ.....	144
БИБЛИОГРАФИЧЕСКИЙ СПИСОК	145
ПРИЛОЖЕНИЕ А1. ПРИМЕР РАБОТЫ АЛГОРИТМА РАЗДЕЛЕНИЯ ИЗОБРАЖЕНИЙ ПО ДРОБНЫМ ЧАСТЯМ ДЕСЯТИЧНЫХ ЧИСЕЛ.....	164
ПРИЛОЖЕНИЕ А2. ПРИМЕР РАБОТЫ АЛГОРИТМА РАЗДЕЛЕНИЯ ИЗОБРАЖЕНИЙ С ПОМОЩЬЮ ПРЕФИКСНОГО КОДИРОВАНИЯ.....	172
ПРИЛОЖЕНИЕ Б. СВИДЕТЕЛЬСТВА О РЕГИСТРАЦИИ ПРОГРАММ ЭВМ	174
ПРИЛОЖЕНИЕ В. АКТЫ ВНЕДРЕНИЯ.....	179

ВВЕДЕНИЕ

Актуальность темы исследования. Системы видеонаблюдения и передачи видеoinформации сегодня используются повсеместно – от охранного видеонаблюдения на территориально удаленных площадках производственных предприятий и опасных объектов до систем передачи видеоданных с беспилотных транспортных средств.

Так, в соответствии с постановлением Правительства Российской Федерации от 2 ноября 2009 г. № 1629-р определен перечень критически важных объектов, подлежащих постоянному видеонаблюдению. В связи с этим развитие и внедрение комплексных систем удаленного видеомониторинга, таких как «Безопасный город», приводят к формированию больших объемов видеоданных, для которых необходимо обеспечивать надежность передачи (ГОСТ Р 51558–2014 «Средства и системы охранные телевизионные. Классификация. Общие технические требования. Методы испытаний»), а также их конфиденциальность и подлинность (ГОСТ Р 56035–2014 «Системы охранные телевизионные. Защита оцифрованных видеоданных от случайного и преднамеренного искажения. Общие требования»).

Кроме того, перспективным направлением является развитие беспилотного транспорта, неотъемлемой частью которого выступают системы передачи видеоданных и телеметрии. Согласно Транспортной стратегии Российской Федерации до 2030 года с прогнозом до 2035 года, утвержденной распоряжением Правительства РФ от 27 ноября 2021 г. № 3363-р, для бесперебойного функционирования беспилотных транспортных средств на всех видах транспорта (автомобильного, железнодорожного, водного и воздушного) необходимо обеспечить стабильность, защищенность и достаточную скорость передачи видеоданных.

Поэтому, развитие вычислительных сетей и систем связи, а также использование производственными предприятиями двух каналов связи с различными пропускными способностями (передача большого объема открытых данных по одному каналу и защищенная корпоративная сеть по другому), наряду с оснащением беспилотных транспортных средств двухканальными системами связи

(распределенная передача данных от технических средств полезной нагрузки и телеметрии), способствует внедрению алгоритмов кодирования изображений (кадров видеоданных), основанных на схемах разделения данных [1, 2], для их распределенной передачи по каналам связи. Поскольку используются два канала связи с разной пропускной способностью, алгоритмы кодирования должны предусматривать разделение изображений на две части разного размера. Кроме того, такие алгоритмы могут обеспечивать конфиденциальность передаваемых данных — при этом по любой из частей, полученных в результате разделения, невозможно восстановить исходное изображение или даже получить его приблизительное представление. В случае разделения изображения на части неравного размера имеет смысл рассматривать только попытки восстановления по большей части. При этом алгоритмы должны опираться на простые математические операции, обеспечивающие быстрое разделение и восстановление изображений.

При передаче разделенных кадров видеоданных через двухканальную систему связи необходимо учитывать минимизацию задержек. Поэтому такую систему следует рассматривать как систему с параллельной и распределенной обработкой данных, для которой требуется решение оптимизационных задач.

В качестве модели такой системы может выступать система массового обслуживания с делением и слиянием заявок (в западной классификации — «fork-join queueing systems») [3–5]. В такой системе поступающая заявка в точке распределения не передается на обслуживание по одному из каналов связи, а разделяется (демультиплексируется) на сопряженные фрагменты. Эти фрагменты обрабатываются параллельно, а после завершения их обслуживания выполняется объединение (мультиплексирование). Только после этого заявка считается обслуженной и покидает систему.

Минимизация задержек при передаче кадров видеоданных через такую систему обеспечивается за счет определения оптимальных пропускных способностей каналов связи, при этом учитываются минимизация простоя и максимальная загруженность каналов, а также выполняется синхронизация передачи частей кадров, полученных в результате кодирования. Выбор

оптимальных пропускных способностей способствует снижению средних издержек (материально-технических затрат) в течение всего периода эксплуатации системы.

Актуальность темы диссертации обусловлена необходимостью разработки моделей и алгоритмов, обеспечивающих бесперебойную передачу данных в системах видеонаблюдения при соблюдении конфиденциальности видеоданных и снижении затрат на их эксплуатацию.

Основная идея диссертационной работы заключается в том, что бесперебойность и конфиденциальность передачи данных в системах видеосвязи могут быть обеспечены за счет комплексной разработки научно-технических решений. К таким решениям относятся: (1) алгоритмы кодирования видеоданных, основанные на разделении кадров для передачи по разным каналам, (2) методика аналитического расчета пропускных способностей каналов, (3) имитационная модель двухканальной системы связи.

Состояние вопроса. Анализ исследований, посвященных распределенной передаче изображений с использованием схем разделения данных, а также проектированию систем демультиплексирования видеоданных для их передачи по многоканальным системам связи, выявляет необходимость в развитии системного подхода. Такой подход должен включать не только разработку алгоритмов кодирования видеоданных, основанных на схемах разделения данных, но и создание методик аналитических расчетов и имитационных моделей, которые позволят определять оптимальные параметры каналов связи в системах с распределенной передачей данных, обеспечивая их надежность.

По вопросам разработки методов и алгоритмов по разделению цифровых изображений на части в целях их кодирования и распределённой передачи опубликовано множество работ зарубежных авторов, среди которых можно отметить работы авторов: M. Naor, A. Shamir, C. Asmuth, J. Bloom, D. Jin, W.Q. Yan, M.S Kankanhalli, Y.C. Hou, A. Adhikari, S. Sikdar, Liu Feng. В более современных работах, таких как исследования M.H. Tsai, C.C. Chen, G. Ulutas, V.V. Nabyev, I. Padiya, V. Manure, A. Vidhate, S. Rathnamala предлагаются новые алгоритмы разделения цифровых изображений, которые не только повышают уровень конфиденциальности, но и уменьшают размер

частей изображений, полученных в результате работы алгоритмов.

Среди работ отечественных ученых выделяются работы: Р.Т. Файзуллина, Е.В. Щербы, А.А. Свенча, В.И. Ефимова, В.И. Дулькейта. В настоящее время в ряде работ авторов: Д.Н. Лаврова, Н.И. Червякова, М.Г. Бабенко, Ю.В. Косолапова, Н.И. Глумова рассматриваются подходы к выбору алгоритмов, которые не только предусматривают разделение изображений на части, но также включают предварительное сжатие и последующую передачу через системы связи с параллельными каналами.

Анализ результатов, полученных как зарубежными, так и отечественными авторами, показал, что исследования в данной области охватывают вопросы кодирования изображений, а также включают теоретические разработки (например, математические выкладки, формализованные алгоритмы) и практические реализации (например, программное обеспечение для ЭВМ). Однако вопросы передачи частей изображений через системы и сети связи остаются недостаточно проработанными, в частности, не учитываются или учитываются лишь частично параметры и технические характеристики систем передачи данных.

Указанный недостаток объясняется необходимостью проведения исследований в другой области знаний, которые могут быть затруднительными для исследователя или даже восприниматься как несущественные. Однако следует отметить, что использование дополнительных каналов связи приводит к увеличению аппаратных и финансовых затрат. Поэтому выбор оптимальных параметров системы связи становится важным. Решение данной задачи возможно найти с помощью методов теории массового обслуживания, анализа, оптимизации и синтеза систем массового обслуживания. Среди зарубежных авторов можно выделить основополагающие работы J. Jackson, L. Kleinrock, K. Candy, F. Baccelli, D. Towsley, S. Foss, J.P. Buzen, F. Baskett, J.M. Harrison, E. Gelenbe, среди отечественных авторов выделяются работы В.М. Вишневого, П.П. Бочарова, Г.П. Башарина, В.В. Рыкова, В.А. Ивницкого, Ю.И. Митрофанова, А.Ф. Терпугова, А.А. Назарова, В.Н. Задорожного.

В связи с развитием систем параллельной передачи и обработки данных в сочетании с алгоритмами кодирования видеоданных, основанных на схемах

разделения, следует выделить работы авторов, изучающих системы с делением и слиянием заявок («fork-join queueing systems»). Среди зарубежных авторов можно отметить работы: L. Flatto, R. Nelson, A.N. Tantawi, A. Thomasian, I. Tsimashenka, W.J. Knottenbelt, M. Mandelbaum, A. Duda, T. Czachorski, L. Green, Y. Narahari, R. Nelson. В свою очередь, среди отечественных исследователей стоит выделить работы Ю.И. Рыжикова, А.В. Горбуновой, С.П. Моисеевой, В.М. Вишневого, П.П. Бочарова, И.С. Зарядова, К.Е. Самуйлова, Э.С. Сопина. В этих работах приводятся преимущественно аналитические результаты, касающиеся среднего времени пребывания заявок в системе (времени отклика системы).

В последних работах А.В. Горбуновой, А.В. Лебедева, В.М. Вишневого рассматриваются результаты имитационного моделирования систем с делением и слиянием заявок, в которых используется распределение Парето для времени обслуживания. Перспективным представляется подход, объединяющий методику аналитического расчета с имитационным моделированием, поскольку он позволит более точно оценить работу систем с распределенной передачей данных. Особенно это важно для владельцев таких систем, для которых ключевым является вопрос оптимального распределения ресурсов, в частности пропускной способности каналов связи, стоимость которых может быть весьма высока. Необходимо найти баланс между затратами на содержание системы и выделяемыми техническими ресурсами. Поэтому задача оптимизации двухканальной системы связи при передаче частей видеокладов по её каналам (полученных в результате работы алгоритмов кодирования, основанных на схемах разделения) рассматривается как многокритериальная. Эта задача может быть решена с использованием Парето-аппроксимации на основе генетических алгоритмов в процессе имитационного моделирования.

Исследования авторов L. Fogel, J. Holland стали основой для разработки генетических алгоритмов и методов эволюционного программирования, которые используют принципы естественного отбора для решения сложных оптимизационных задач. В этих работах основное внимание уделяется моделированию эволюционных процессов и адаптивных систем. Генетический алгоритм – это вероятностная оптимизационная процедура, основанная на

принципах естественного отбора, способная находить глобальный оптимум даже при большом числе параметров. Генетические алгоритмы могут применяться как для задач с одним критерием оптимизации, так и для многокритериальных задач, благодаря своей высокой эффективности в формировании множества Парето-оптимальных решений за разумное время.

На сегодняшний день большинство исследователей, включая К. Deb, Н.В. Gurocak, Ф. Herrera и J. Wu, а также отечественных авторов, таких как А.И. Змитровича, В.М. Курейчика, В.П. Северина, А.Н. Скурихина, считают генетические алгоритмы одним из самых перспективных методов оптимизации. В связи с этим рассматривается целесообразность применения генетических алгоритмов при имитационном моделировании систем передачи данных. Стоит отметить, что имитационное моделирование позволяет находить такие параметры системы, которые удовлетворяют всем условиям выполнения модели, в то время как аналитический расчет определяет только нижние границы (минимальные значения) параметров исследуемой двухканальной системы связи, без учета их взаимосвязи.

Таким образом, анализ существующих методов и алгоритмов позволяет сделать вывод о том, что они не учитывают (либо в недостаточной степени учитывают) технические требования, предъявляемые к системам распределенной передачи данных. В то же время при проектировании таких систем, как правило, не принимаются во внимание вычислительные сложности применяемых алгоритмов. В связи с этим перспективным направлением является разработка алгоритмов, методики аналитических расчетов и имитационной модели, реализующих системный подход к организации распределенной передачи данных. Это позволит повысить стабильность систем связи, сократить расходы по их содержанию и обеспечить конфиденциальность передаваемых в них данных.

Целью диссертационной работы является обеспечение бесперебойности и конфиденциальности передачи видеоданных путем применения системного подхода к организации видеосвязи, включая кодирование данных с разделением кадров, определение параметров каналов связи с помощью моделирования и аналитического обоснования пропускных способностей. Для достижения

указанной цели в работе поставлены и решены следующие **задачи**:

1. Провести анализ проблем обработки и бесперебойной распределенной передачи данных в системах видеосвязи.

2. Разработать алгоритмы разделения кадров видеоданных на неравные части для обеспечения конфиденциальности их передачи за счет невозможности декодирования кадров по большей их части без знания меньшей.

3. Разработать методику аналитического расчета пропускных способностей каналов двухканальной системы связи с учетом характеристик передаваемого потока кодируемых видеокадров, разделенных на неравные части.

4. Создать имитационную модель двухканальной системы видеосвязи для оптимизации ее параметров с помощью генетического алгоритма, позволяющую осуществить обоснованный выбор пропускных способностей каналов связи, обеспечивая синхронную и бесперебойную передачу данных при минимизации временных и стоимостных затрат.

5. Создать программный комплекс двухканальной системы передачи видеоданных и провести экспериментальные исследования разработанных модели и алгоритмов реализации системного подхода к организации распределенной передачи, позволяющие оценить синхронность получения частей кадров и подтвердить обеспечение бесперебойной и конфиденциальной передачи видеоданных.

Научная новизна. В процессе исследований получены следующие новые научные результаты:

1. Предложено выполнить организацию распределенной передачи видеоданных на основе системного подхода, реализуя комплексную разработку алгоритмов кодирования, аналитической методики и имитационной модели для расчетов параметров каналов связи.

2. Разработаны алгоритмы кодирования видеоданных, отличительной особенностью которых является разделение кадров на части неравного размера, позволяющие исключить возможность восстановления исходного изображения кадров по одной из частей без информации о второй части. Это позволяет выполнять передачу видеоданных в двухканальных системах с ограниченными

вычислительными ресурсами, но имеющими каналы с различными пропускными способностями.

3. Разработана методика аналитического расчета пропускных способностей каналов связи с оптимизацией временных затрат, отличительной особенностью которой является возможность оценивания издержек на содержание двухканальной системы связи (на основе доказанной теоремы: пропускная способность двухканальной и одноканальной систем связи одинаковы).

Кроме того, особенностью является возможность оценивания условий синхронизации (на основе доказанной теоремы: двухканальная система связи при передаче по ее каналам данных, разделенных в постоянном соотношении, является системой с их синхронной передачей). Это позволяет свести решение двумерных задач оптимизации таких систем связи к одномерным.

4. Разработана имитационная модель двухканальной системы видеосвязи, которая в совокупности с использованием генетического алгоритма позволяет выполнить многокритериальную оптимизацию параметров. Отличительной особенностью такого подхода к оптимизации параметров является выполнение синхронной передачи частей разделяемых кадров видеоданных, что позволяет обеспечить бесперебойную передачу видеоданных при минимальных временных и стоимостных и издержках.

Теоретическая значимость работы заключается в:

- разработке алгоритмов кодирования видеоданных разделения кадров на части неравного размера, позволяющих исключить возможность восстановления изображения кадров по одной из частей без информации о второй части;
- получении расчетных формул для определения минимально необходимых значений (нижних границ) пропускных способностей каналов связи двухканальной системы в зависимости от характера входящего потока кодируемых кадров видеоданных.

Практическая значимость работы заключается в разработке:

- программ, реализующих алгоритмы разделения кадров видеоданных на части неравного размера для повышения конфиденциальности данных при передаче;

– проблемно-ориентированного программного комплекса, позволяющего выполнить экспериментальные исследования для оценки синхронности получения частей разделенных кадров и оценки возможности восстановления исходного изображения кадра по его большей части.

Внедрение результатов исследований. Результаты работы использовались при выполнении НИОКТР № 01201258286 «Алгебро-логический подход к исследованию задач ВЫПОЛНИМОСТЬ, ассоциированных с криптоанализом асимметричных шифров» (грант – РФФИ № 12-07-00294-а, 2012-2014 г.).

Имитационная модель двухканальной системы связи, алгоритмы разделения изображений используются в производственном процессе филиала АО «ОДК» «ОМО им. П.И. Баранова (2023–2025 г.) – оперативное решение задач по оптимизации и выбору параметров каналов связи; конфиденциальный обмена изображениями.

Полученные аналитические и практические результаты исследований, посвящённых анализу систем распределённой передачи данных, успешно интегрированы в образовательный процесс ОмГТУ и активно используются в рамках дисциплин кафедры «Автоматизированные системы управления и обработки информации» (АСОИУ) (2024 г.).

Основные результаты, полученные автором и выносимые на защиту:

1. Алгоритмы кодирования видеоданных, предусматривающие разделение кадров на части различного размера, обеспечивающие конфиденциальность (исключена возможность восстановления полного изображения кадра по большей части без доступа к меньшей) и распределённую передачу видеоданных.

2. Методика аналитического расчета пропускных способностей каналов связи с оптимизацией временных затрат, позволяющая выполнить оценку издержек на содержание двухканальной системы связи и условий синхронизации передачи данных. Доказательство теорем, сводящих решение двумерных задач оптимизации таких систем к одномерным. Теорема 1: пропускная способность двухканальной системы равна пропускной способности одноканальной системы связи (следствие – Теорема 2). Теорема 3: двухканальная система связи при передаче по ее каналам данных, разделенных в постоянном соотношении, является системой с их синхронной передачей (следствие – Теорема 4).

3. Имитационная модель двухканальной системы видеосвязи, позволяющая в совокупности с генетическим алгоритмом выполнить многокритериальную оптимизацию параметров. Особенностью такого подхода к оптимизации параметров системы является обеспечение синхронной передачи частей разделяемых кадров видеоданных, что позволяет при минимальных временных и стоимостных и издержках осуществлять бесперебойную передачу видеоданных.

4. Проблемно-ориентированный программный комплекс, реализующий системный подход к организации распределенной передачи видеоданных. Результаты экспериментальных исследований для оценки распределенной передачи частей кадров (по критерию синхронности их получения), а также алгоритмов кодирования изображений при помощи разделения их на части неравного размера (по критерию возможности восстановления).

Объектом исследования являются технологии и системы кодирования видеоданных, предназначенные для их распределенной передачи, двухканальные системы связи с каналами, обладающими различной пропускной способностью.

Предметом исследования являются методы и алгоритмы кодирования видеоданных, математические модели, методы и алгоритмы, предназначенные для анализа и оптимизации пропускных способностей систем связи.

Методология исследования базируется на основах системного анализа; теории кодирования; методах математического моделирования и теории массового обслуживания; интеллектуальных технологиях, включающих в себя применение генетических алгоритмов при многокритериальной оптимизации.

Соответствие паспорту специальности. Полученные в диссертационной работе научные результаты соответствуют следующим пунктам области исследований паспорта специальности 2.3.1 – «Системный анализ, управление и обработка информации, статистика»: п. 1 «Теоретические основы и методы системного анализа, оптимизации, управления, принятия решений, обработки информации и искусственного интеллекта»; п. 4 «Разработка методов и алгоритмов решения задач системного анализа, оптимизации, управления, принятия решений, обработки информации и искусственного интеллекта»; п. 5 «Разработка специального

математического и алгоритмического обеспечения систем анализа, оптимизации, управления, принятия решений, обработки информации и искусственного интеллекта»; п. 11 «Визуализация, трансформация и анализ информации на основе компьютерных методов обработки информации».

Достоверность полученных результатов. Обоснованность и достоверность теоретических результатов, положений и выводов диссертационной работы основаны на использовании апробированных научных методов и положений, таких как численные методы решения систем уравнений, методы теории кодирования, аналитические и математические методы теории массового обслуживания, а также методы дискретно-событийного моделирования. Кроме того, результатам придается дополнительная достоверность за счет корректного применения математического аппарата и согласованности новых выводов с известными теоретическими положениями.

Апробация результатов исследования. Основные положения и результаты диссертационной работы были представлены на следующих научных конференциях и семинарах: II, IV Всероссийская молодежная научно-техническая конференция «Россия молодая: передовые технологии - в промышленность» (г. Омск, 2009, 2011); Научно-практический семинар «Актуальные проблемы обеспечения информационной безопасности: подходы и решения» в рамках ежегодного промышленно-инновационного форума «ПромТехЭкспо-2011» (г. Омск, 2011); XII Всероссийский конкурс-конференция студентов и аспирантов по информационной безопасности «SIBINFO-2012» (г. Томск, 2012); VIII Международная научно-практическая конференция «Электронные средства и системы управления» (г. Томск, 2012); 11-ая Международная конференция «Распознавание образов и анализ изображений – 2013» (г. Самара, 2013); XIV Всероссийский конкурс-конференция студентов и аспирантов по информационной безопасности «SIBINFO-2014» (диплом III степени) (г. Томск, 2014); III Всероссийская научно-практическая конференция с международным участием «Системы управления, информационные технологии и математическое моделирование» (г. Омск, 2021); XV, VIII Международная научно-техническая конференция

«Динамика систем, механизмов и машин» (г. Омск, 2021, 2012); 24th International Conference named after A. F. Terpugov «Informational technologies and mathematical modeling» (ITMM – 2021) (г. Томск, 2021); VI Международная научно-техническая конференция «Проблемы машиноведения» (г. Омск, 2022); XIV Всероссийская научно-практическая конференция студентов, аспирантов, работников образования и промышленности «Информационные технологии и автоматизация управления» (г. Омск, 2023); VII Всероссийская научно-практическая конференция «Научный потенциал молодежи и технический прогресс» (Санкт-Петербург, 2024).

Публикации по теме исследования. По теме диссертации опубликовано 15 научных работ, в том числе в том числе 7 научных статей в рецензируемых научных изданиях, рекомендованных ВАК при Минобрнауки России, 2 научных статьи в изданиях, индексируемых в международной реферативной базе данных Scopus, 5 свидетельств о государственной регистрации программ для ЭВМ.

Структура и объем диссертации. Диссертационная работа состоит из введения, пяти глав, заключения, списка использованных источников (174 наименования) и трех приложений. Общий объем работы 181 страница, в том числе 163 страницы основного текста, включая 64 рисунка и 6 таблиц.

Личный вклад автора. Решение задач диссертации; разработка алгоритмов разделения изображений на части неравного размера, их программная реализация; постановка задачи для методики аналитического расчета пропускных способностей каналов двухканальной системы связи; разработка имитационной модели двухканальной системы связи; теоретические и экспериментальные результаты, выносимые на защиту, принадлежат лично автору.

Автор благодарен и признателен своим научным руководителям, ушедшим из жизни: д.т.н., профессору Файзуллину Р.Т. и д.т.н., профессору Задорожному В.Н. за помощь в формировании основ диссертационной работы. Автор выражает искреннюю признательность и благодарность научному руководителю, д.т.н., профессору Денисовой Л.А. за помощь в систематизации полученных ранее результатов, завершении работы и подготовке ее к защите.

1 ПРОБЛЕМЫ РАСПРЕДЕЛЕННОЙ ПЕРЕДАЧИ ВИДЕОДАНЫХ

В первой главе рассматривается комплекс проблем, связанных с реализацией системного подхода к организации распределенной передачи видеоданных по распределенным системам связи. Приводятся существующие методы и алгоритмы, основанные на схемах разделения данных, которые могут быть использованы при кодировании кадров видеоданных. Анализируются способы передачи частей кадров видеоданных, полученных в результате кодирования, по многоканальным системам связи. Рассматриваются системы обслуживания с делением и слиянием требований, а также методы аналитического подхода и имитационного моделирования для оптимизации параметров таких систем.

1.1 Современное состояние вопроса распределенной передачи видеоданных в многоканальных системах связи

Современное состояние вопроса распределенной передачи данных показывает, что все чаще производственные и коммерческие предприятия для обмена данными с удаленными производственными площадками или дополнительными офисами используют несколько каналов связи. Как правило, один из них предназначен для закрытой (защищенной) корпоративной сети передачи данных, а второй – для обмена данными, не имеющими грифа конфиденциальности, либо он используется как резервный канал [8–10]. Канал закрытой корпоративной связи может не иметь достаточных ресурсов для передачи больших объемов данных из-за мощностных ограничений средств криптографической защиты информации [11]. В таких случаях данные большого объема, включая видеоданные, обычно передаются по второму каналу связи, который имеет гарантированную пропускную способность, предоставленную провайдером связи. Возникает вопрос об оптимальности использования каналов связи и минимизации затрат на их аренду, особенно в случаях возможной избыточности пропускной способности этих каналов.

Кроме того, за последние пять лет в Российской Федерации наблюдается рост применения беспилотных транспортных средств во всех сферах транспорта. В

соответствии с Транспортной стратегией Российской Федерации до 2030 года с прогнозом на период до 2035 года, утвержденной распоряжением Правительства Российской Федерации от 27 ноября 2021 г. № 3363-р, в ближайшие десять лет в стране должна быть сформирована информационная и сетевая инфраструктура для бесперебойного функционирования беспилотных автомобилей в качестве такси, а также беспилотного железнодорожного и водного транспорта для доставки крупногабаритных грузов и пассажиров, воздушных судов для транспортировки малогабаритных грузов, а также колесных городских средств доставки товаров.

В беспилотных транспортных средствах одним из основных аспектов, повышающих их надежность, является применение технологии MIMO (Multiple Input Multiple Output) [12], которая позволяет одновременно передавать несколько потоков данных через различные каналы связи [13, 14]. Это увеличивает пропускную способность системы связи и способствует более стабильному соединению, что, в свою очередь, повышает надежность передачи данных. В случае возникновения помех или отказа одного из каналов, второй канал может обеспечить непрерывность связи, что особенно важно в транспортных системах, где стабильность и безопасность коммуникаций имеют решающее значение [15].

В работах [16–18] рассматриваются варианты использования беспилотных транспортных средств с двумя радиоканалами связи для распределенной передачи командно-телеметрических данных и данных от технических средств полезной нагрузки. Командно-телеметрический канал предназначен для передачи команд управления от наземного пункта управления к беспилотному транспортному средству и обратной передачи телеметрической информации о его состоянии. Этот канал обычно работает в дуплексном или полудуплексном режиме и требует высокой надежности передачи данных. Канал передачи данных полезной нагрузки используется для передачи информации, собранной с помощью бортовых сенсоров и других технических средств, таких как видеокамеры или радары. Этот канал, как правило, работает в симплексном режиме и обеспечивает высокоскоростную передачу больших объемов данных [19]. При этом совместно используются сети мобильных операторов связи поколений 2G...4G, радиоканалы на основе

стандартных технологий радиосвязи (RC433, RC868, CDMA, GSM900, GSM1800, 3G и 4G), каналы цифрового телевидения DVB, а также специально выделенные радиоканалы с различными частотными характеристиками. Необходимость применения двух радиоканалов связи обусловлена требованием обеспечить распределенную передачу командно-телеметрических данных и данных от технических средств полезной нагрузки. Видеоданные, принимаемые оператором на пункте управления, имеют большой объем и требуют передачи в режиме реального времени. Это предполагает использование широкой полосы пропускания частот (большой пропускной способности). В то время как для передачи командно-телеметрических данных не требуется такая высокая пропускная способность, поскольку эти данные имеют небольшой объем. Таким образом, разделение каналов позволяет использовать различные частотные диапазоны и модуляционные схемы, оптимально подходящие для каждого типа данных, что повышает общую эффективность системы связи.

В беспилотных транспортных средствах с малыми габаритами, таких как беспилотные колесные или летающие средства для доставки товаров, отсутствует возможность размещения крупногабаритных остронаправленных антенн. В связи с этим видеоданные от таких средств передаются через всенаправленные антенны или антенны с широким главным лепестком диаграммы направленности (порядка 60–90°). Это, в свою очередь, приводит к тому, что сигнально-частотные параметры радиоканалов можно относительно легко вскрывать, а также получать доступ к передаваемым видеоданным, осуществлять их подмену или блокировку [20]. Таким образом, для стабильной работы беспилотных транспортных средств необходимо не только обеспечение надежной связи, но и обеспечение достаточного уровня конфиденциальности передаваемых данных.

Из-за недостатка собственной компонентной базы в Российской Федерации, как правило, используются импортные вычислительные платформы, которые на компонентном уровне не поддерживают отечественные алгоритмы обеспечения конфиденциальности данных. Это затрудняет их применение в составе большинства беспилотных транспортных средств. Согласно данным, приведенным

в работах [21–25], в большинстве беспилотных транспортных средств могут применяться алгоритмы обеспечения конфиденциальности, соответствующие стандартам: NSA Type I, Triple DES, AES-128, или, в случае отсутствия возможности использовать высокопроизводительное оборудование для обработки данных, возможна передача данных в открытом виде. При попытках внедрения дополнительных программно-аппаратных комплексов для обеспечения конфиденциальности [26] в беспилотных транспортных средствах возникают проблемы, связанные с дополнительным потреблением энергии [27, 28] и ограниченной грузоподъемностью малых беспилотных транспортных средств [29–32].

С учетом обозначенных технических особенностей корпоративных сетей передачи данных и систем связи беспилотных транспортных средств, а именно наличия двух каналов связи, представляют интерес исследования, направленные на разработку алгоритмов кодирования видеоинформации, основанных на схемах разделения данных. В этих системах, где имеется как минимум два канала связи с различными пропускными способностями, разделение кадров видеоданных должно осуществляться на две части неравного размера. При этом меньшая часть кадра передается по каналу с меньшей пропускной способностью, а большая – по каналу с большей пропускной способностью [33]. Разрабатываемые схемы разделения данных должны предъявлять минимальные требования к вычислительным ресурсам центрального процессора [34–38], обладать высокими показателями быстродействия и решать несколько ключевых задач: минимизация временных задержек при преобразовании видеоданных, обеспечение конфиденциальности при попытках незаконного восстановления данных. С физической точки зрения перехват обеих частей кадра видеоданных является затруднительным, как и восстановление исходного изображения без хотя бы одной из частей [39–41]. При передаче частей кадров по каналам связи применяются методы многопутевой маршрутизации, позволяющие использовать несколько маршрутов, пролегающих через разные параллельные каналы связи. Однако возрастающая нагрузка на канал связи, связанная с передачей большей части, или простой канала связи при передаче меньшей части, могут снизить

привлекательность выбранных маршрутов с точки зрения скорости передачи, надежности и отказоустойчивости [42]. Поэтому, учитывая большой объем видеоданных, ограниченность пропускных способностей и необходимость выбора оптимальных параметров каналов связи для передачи больших и меньших частей данных, возникает потребность использования различных методов оптимизации, синхронизации и балансировки пропускных способностей каналов связи.

Как правило, синхронизация и балансировка используются для равномерного распределения трафика данных или вычислительных задач в высоконагруженных системах [43–45]. При передаче разделенных видеоданных в реальном времени в двухканальной системе связи, синхронизация передачи частей кадров, передаваемых по параллельным каналам связи, может быть достигнута за счет выявления резервов времени передачи данных в этих каналах и выравнивания их временных характеристик [46, 47]. Однако, в случае значительных различий в объемах передаваемых данных по двум параллельным каналам связи, алгоритмы синхронизации, основанные на выравнивании средних значений времен передачи данных, могут оказаться неэффективными. Это объясняется тем, что, помимо синхронизации передачи данных по каналам, необходимо обеспечить их максимальную загрузку (или минимальный простой) в целях экономии издержек. Синхронизация передачи данных по двум каналам связи важна для исключения формирования очередей данных и их потери, что критично для своевременного восстановления переданных кадров видеоданных. Максимальная загрузка каналов связи требуется для использования всей их пропускной способности, а минимальный простой необходим для передачи наибольших объемов данных, поскольку через эти каналы передаются потоки видеоданных. Проблема заключается в том, что оптимизация сразу по нескольким критериям требует значительных временных и вычислительных ресурсов, так как целевые функции с несколькими переменными создают многомерное пространство поиска решений, что повышает вычислительную сложность задачи и может стать препятствием для ее решения в допустимое время. Аналитическое описание и строгое решение такой задачи зачастую невозможно или возможно только при ряде допущений.

Таким образом, учитывая тот факт, что центральные процессоры управления в системах кодирования и передачи видеоданных, как правило, не предназначены для решения сложных математических и оптимизационных задач, целесообразно рассмотреть возможность применения результатов предварительных расчетов нижних границ интервалов (минимально необходимых) пропускных способностей, а также результатов имитационного моделирования, позволяющего выполнять многокритериальную оптимизацию двухканальной системы связи с использованием генетических алгоритмов, которые обладают значительно меньшей вычислительной емкостью. Генетические алгоритмы позволяют, не исследуя полностью область допустимых решений, с определенной вероятностью находить глобальный экстремум в однокритериальных задачах и фронт Парето в многокритериальных.

Таким образом, повышение эффективности достигается за счет синергии методов кодирования видеоданных, динамической адаптации параметров каналов связи и распределенной архитектуры системы, что способствует снижению затрат.

1.2 Анализ работ по использованию методов и алгоритмов кодирования видеоданных

Достоинствами схем разделения для распределенной передачи видеоданных по нескольким каналам являются: высокая скорость работы, надежность (обеспечение конфиденциальности), сопоставимая с надежностью одноразового блокнота, при условии случайного подхода к разбиению пикселей на блоки [48–51]. Классический вариант схем разделения изображений (кадров видеоданных) предполагает передачу каждому участнику части изображения, размер которой равен размеру самого изображения. В частности, в схеме разделения, предложенной Moni Naor и Adi Shamir [2], черно-белое изображение делится на «теневые» изображения, которые представляют собой «белый шум» и не дают никакой информации об исходном изображении, кроме его размера. Восстановление осуществляется наложением «теневых» изображений и применением логических операций *AND*, *OR*, *XOR*. Эта схема разделения

ориентирована только на черно-белые изображения, но существуют улучшения и расширения этой схемы. Например, в работах D. Jin, W.Q. Yan, M.S. Kankanhalli, Y.C. Hou, A. Adhikari, S. Sikdar, Liu Feng, Chuan Kun Wu [52–55] предложены схемы разделения для цветных изображений, где цвет используется как дополнительный канал передачи информации об исходном изображении.

Простейшим примером применения схем разделения данных может являться тот случай, когда разделение исходных данных осуществляется между двумя людьми. Например, если обладатель некоторого сообщения хочет осуществить его разделение на две части, тогда первым делом он генерирует строку случайных битов R такой же длины, что и исходные разделяемые данные M , а затем выполняет операцию XOR : $R \oplus M = S$. Полученные данные S передаются получателю, а строка случайных битов R остается у отправителя. Тем самым, чтобы восстановить исходное сообщение, получателю и отправителю необходимо выполнить над имеющимися у них частями единственное действие: $R \oplus S = M$. Понятно, что можно осуществить разделение данных и для большего числа участников, например, отправитель (доверенное лицо) генерирует случайным образом три битовые последовательности: R , S и T , такой же длины, что и исходные разделяемые данные M . Затем выполняется операция XOR над M и созданными битовыми последовательностями: $M \oplus R \oplus S \oplus T = U$. Битовые последовательности R , S и T передаются трем абонентам соответственно, а вычисленное значение U передается получателю. Аналогично, как и для разделения данных между двумя участниками, три абонента и получатель собираются вместе и выполняют восстановление исходных данных: $R \oplus S \oplus T \oplus U = M$. В данном случае при разделении данных используется арбитражный протокол, где отправитель (доверенное лицо) обладает абсолютной властью и может делать все, что он хочет, например, он может раздать «подменные данные» и утверждать, что это настоящие части исходных данных, и никто не сможет это проверить, пока собравшиеся вместе участники протокола не попробуют выполнить восстановление. Возможна ситуация, когда только три абонента смогут восстановить исходные данные, а получателю при этом достались

«подменные данные». Недостатками алгоритмов, работающих по такому принципу, является то, что в данной ситуации каждому из участников сразу становится известен замер исходных данных M , и следует понимать, что исходные данные M делятся не в прямом смысле этого слова, а подвергаются операции XOR со случайными величинами. Например, существует файл изображения, который необходимо разделить при помощи арбитражного протокола, тогда, полученные в результате преобразований части будут равны объёму самого файла изображения. Кроме того, выполнение побитовой операции XOR над файлом большого объёма может потребовать значительного времени. Возможна ситуация, когда файл исходных данных большого объёма, и необходимо чтобы объёмы его частей, полученных в результате применения схемы разделения, не превышали или же вовсе были меньше по объёму, чем объём исходных данных. В такой ситуации прибегают к использованию идеальных схем разделения [56, 57], технологий разделения данных, например, таких как шардинг [58] или к разработке новых схем разделения данных под конкретные задачи.

Существуют пороговые схемы разделения данных, идея которых была впервые предложена А. Shamir [1] и G.R. Blakley [59]. Эти схемы основаны на том, что исходные данные разделяются на k частей, которые распределяются между участниками таким образом, что любые n из них могут объединить свои части и восстановить исходные данные. В случае применения такой схемы разделения для изображений – n участников после объединения своих «теневых» изображений друг с другом в произвольной последовательности смогут увидеть исходное изображение. Для восстановления исходных чёрно-белых изображений, наложение частей осуществляется путем применения логических операции AND , OR , XOR . На рисунке 1.1 приведён пример разделения исходного пикселя разделяемого изображения на «подпиксели» при схеме разделения данных (2, 2).

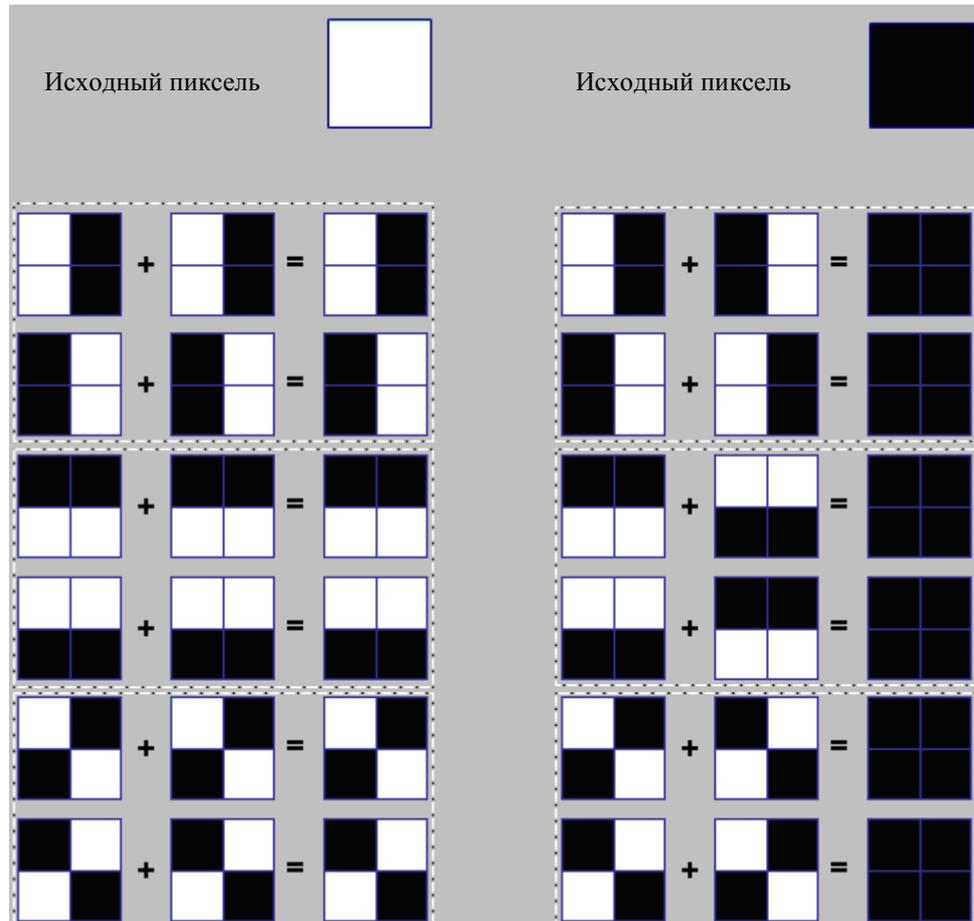


Рисунок 1.1 – Разделения пикселя на «подпиксели»

Процесс получения теневого изображения для исходного изображения по схеме (2, 2) выглядит следующим образом: для каждого пикселя исходного изображения, для первого «теневого» изображения случайным образом выбирается одно из шести возможных состояний пикселя, приведенных на рисунке 1.1. Состояние пикселя второго «теневого» изображения выбирается идентичным или симметричным состоянию пикселя первого «теневого» изображения в зависимости от того, белый или черный был пиксель в исходном изображении соответственно [2]. Такая схема разделения черно-белых изображений обладает высокой скоростью работы и может использоваться для обеспечения их конфиденциальности, недостатком является то, что теньевые изображения могут быть равны или же вовсе превосходить по размеру исходное изображение.

Задачу разделения цифровых изображений можно сравнить с задачей сегментации, где результатом разделения является множество отличных друг от друга сегментов, которые при объединении покрывают всё изображение. Выборка

пикселей изображения в сегмент выполняется по какой-либо характеристике или свойству, например, по цвету, яркости или текстуре, и сформированные соседние сегменты значительно отличаются по этой характеристике [60]. Можно выполнить распределенную передачу таких сегментов изображения, а в случае перехвата какого-либо из сегментов, состоящего из набора пикселей, обладающих одинаковыми характеристиками, нарушитель не сможет получить информацию о передаваемых данных. В такой схеме разделения данных важен порядок выполнения сегментации и объединения сегментов в исходное изображение, который в свою очередь может выступать в качестве ключевой информации. Но, применение подобных способов сегментации не всегда возможно, так как это зависит от характера самого исходного изображения – одноцветное оно или многоцветное. Например, в случае одноцветного изображения сегментация не всегда возможна, а в случае многоцветного изображения может наблюдаться высокая детальность сегментации, что приведёт к использованию алгоритмов уменьшения детальности, путем слияния сегментов, а это приводит к повышению и без того высокой вычислительной сложности [61, 62].

Организация распределенной передачи видеоданных с помощью алгоритмов кодирования, основанных на классических схемах разделения, не всегда целесообразна, так как имеет существенный недостаток, который заключается в том, что объем передаваемой информации увеличивается пропорционально числу частей (количеству участников), на которые разбивается исходное изображение. В таком случае, для двухканальных систем связи наиболее перспективным представляется использовать неклассические подходы к разделению цифровых изображений, где имелась бы возможность разделять цифровые изображения на части разного размера, учитывалась минимизация задержек при преобразовании потока цифровых изображений и обеспечивалась конфиденциальность. В работах [33–40, 63–69] предложены неклассические варианты применения схемы разделения данных для их распределенной передачи по открытым каналам связи, но в приведенных работах не всегда делается акцент на размер получаемых частей при разделении исходных данных. В работах [33–38, 63, 64, 68, 69] поставлена

задача по разделению цифровых изображений на части неравного размера. В данных работах предложены теоретические выкладки о возможном разделении цифровых изображений на части неравного размера, не везде приведены практические данные о том, насколько хорошо будет выполнено разделение, возможно ли восстановление изображения по большей части при помощи различного рода выполняемых им преобразований, не определен процент объема меньшей части от общего объема. Также некоторые предложенные схемы разделения данных не пригодны для однотоновых и чёрно-белых изображений, в работе [65] указан этот недостаток. Во многих работах отсутствует практическая составляющая применения подобных схем разделения цифровых изображений.

В работах [66, 67] предложены методы разделения цифровых изображений при их передаче в распределённых компьютерных сетях, основанные на системах демультиплексирования трафика. Эти системы позволяют распределять видеоданные по нескольким физическим каналам. В частности, в работе [66] предлагается схема разделения, использующая геометрический объект, формируемый на основе RGB-представления изображения.

В работах [66, 67] предложены методы разделения цифровых изображений для их передачи в распределенных компьютерных сетях, основанные на системах демультиплексирования трафика. Эти системы позволяют распределять видеоданные по нескольким физическим каналам [66]. Однако, при разделении изображений с однотоновыми областями, данный метод может приводить к получению частей с одинаковыми или схожими координатами, что может раскрыть передаваемое сообщение. Также в работе приводится описание фильтров кодирования видеоданных, реализованных с использованием технологии Microsoft DirectShow и среды разработки Microsoft Visual Studio.

В работе [67] предложена система демультиплексирования (мультиплексирования), основанная на схеме разделения цифровых изображений, участниками которой являются промежуточные узлы сети, а проекциям в системе мультиплексирования трафика соответствуют проекции схемы разделения, образованные на основе исходного изображения. Предложенная система свободно

реализуется на стеке протоколов TCP/IP на сеансовом уровне OSI, благодаря использованию промежуточных передатчиков. Схема системы, предложенная в работе [67], приведена на рисунке 1.2.

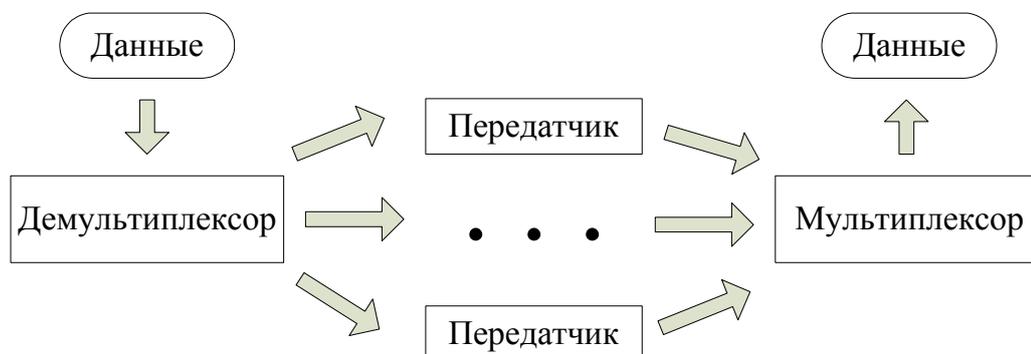


Рисунок 1.2 – Система мультиплексирования

В основу такой схемы разделения положен принцип разбиения множества всех точек изображения на некоторое количество непересекающихся классов, который позволяет распределить передачу по нескольким физическим каналам без увеличения избыточности передаваемых данных, и как следствие, объема передаваемой по сети информации.

Разделение данных осуществляется на основе значений функции яркости пикселя $f(x, y)$. Каждая проекция в результате разбиения будет включать в себя пиксели из определенного диапазона яркости. Недостатком данного метода является то, что при перехвате одной или нескольких проекций изображения, возможно получить информацию о передаваемом изображении с помощью методов интерполяции и экстраполяции [72, 73].

В работе [74] при помощи свободно распространяемого ПО VirtualDubMod смоделирована мультиплексированная система передачи файла видеоданных. Предложено разделение файла видеоданных на определённое количество фрагментов – частей файла видеоданных или кадров (шардирование), определено, что в случае утраты одного или нескольких кадров системе удастся восстановить исходный файл видеоданных с незначительными потерями. В случае покадрового разделения видеоданных по каналам связи, потребуются каналы с одинаковыми пропускными способностями, что является затратным при реализации подобной системы.

В работе [75] рассмотрены три широко используемых метода Shamir-Based Method [1], Blakley-Based Method [59], Asmuth-Based Method [76, 77], основанных на пороговых схемах разделения данных (k, n) , где восстановить исходное изображение возможно, обладая не менее k теньвыми изображениям из общего набора n тневых изображений. Указано, что в Shamir-Based Method используется схема полиномиальной интерполяции Лагранжа, что может позволить раскрыть некоторые детали исходного разделяемого изображения в тневых изображениях, если не выполнить его предварительную обработку, например, перестановку строк или столбцов пикселей исходного изображения [75]. Достоинством является то, что тневые изображения могут иметь размер $1/k$ от общего размера конфиденциального изображения. Blakley-Based Method обладает длительным временем работы, и не может быть использован для изображений большего объема. Asmuth-Based Method является быстрее, чем Shamir-Based Method и Blakley-Based Method. Но в случае разделения 8 битного изображения в градациях серого, количество получаемых тневых изображений ограничено десятью. В методах Blakley-Based Method и Asmuth-Based Method размер получаемых тневых изображений равен размеру исходного разделяемого изображения.

В работе [78] предложена схема разделения изображений, основанная на принципах использования головоломки Sudoku, которая удовлетворяет следующим критериям: обеспечение конфиденциальности, малый размер тневых изображений, но данная схема первоначально ориентирована только на чёрно-белые изображения.

Дополнительно в работах [79–87] рассматриваются методы компьютерной стеганографии для встраивания информации и цифровых водяных знаков в видеоданные и изображения, где задача внедрения цифровых водяных знаков, по сути, является обратной задачей по разделению данных.

В связи увеличением вычислительных мощностей, развитием сетей передачи данных, возможностями применения нейронных сетей, генетических алгоритмов и искусственного интеллекта, современными авторами в настоящее время предлагается множество вариантов модернизации классических схем разделения

данных, а также разрабатываются специальные схемы разделения данных для реализации определенных задач [88–92].

1.3 Обзор систем параллельной обработки и передачи данных

В терминах теории массового обслуживания под системами параллельной обработки разделенных данных будем понимать сети массового обслуживания (Семо) с делением и слиянием заявок, в англоязычной литературе используется термин «fork-join queueing system» (fork-join) [3, 4, 5]. Исследования сетей fork-join, начатые еще в XX веке, продолжают в настоящее время, так как, ввиду развития информационных технологий, систем и сетей обработки и передачи данных, Семо fork-join нашли применение в различных областях [93]:

- параллельные вычисления: моделирование процессов, где задачи разделяются на подзадачи для параллельного выполнения с последующим объединением результатов;

- распределённые системы: оптимизация процессов в системах, использующих распределённые (параллельные) вычисления или обработку данных, либо системах, где исходная сложная задача делится на части (простые подзадачи) для повышения эффективности;

- системы хранения данных: моделирование процессов в системах хранения данных, где запросы могут требовать одновременного доступа к нескольким серверам или устройствам.

Основная идея функционирования Семо fork-join заключается в том, что в момент поступления в систему заявка Z в точке f-p (fork point) разделяется на K сопряженных (родственных) фрагментов, каждый из которых попадает в K обслуживающих подсистем, представляющих из себя одноканальный прибор обслуживания (одноканальная система массового обслуживания – СМО). Обработанные фрагменты попадают в очереди синхронизации (буфер синхронизации), где дожидаются обработки остальных сопряженных фрагментов. И только после окончания обслуживания всех фрагментов, они объединяются в

точке j-p (join point) в исходную заявку, и она покидает сеть. Схема сети приведена на рисунке 1.3.

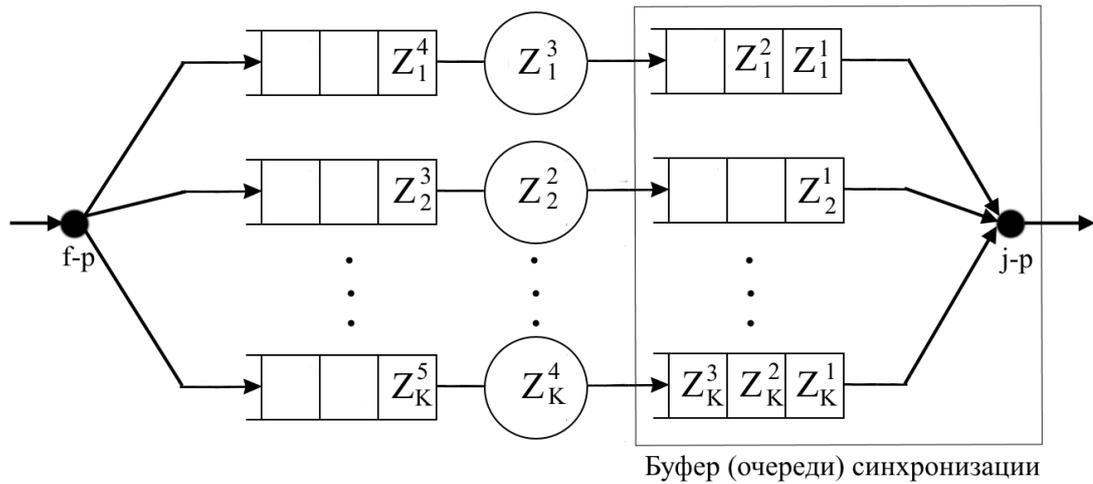


Рисунок 1.3 – Схема сети fork-join

В работе [94] в зависимости от возможных вариантов деления заявок при поступлении в систему и слияния фрагментов после завершения обслуживания выделяют три основных класса:

- с центральным делением без синхронизирующей очереди (centralized splitting model without synchronization queue, split-merge model);
- с центральным делением и синхронизирующей очередью (centralized splitting model with synchronization queue);
- с распределённым делением и синхронизирующей очередью (distributed splitting model with synchronization queue).

В работах [93, 95, 96] описываются разновидности сетей fork-join, в частности описывается работа [97] в которой рассматривается сеть обслуживания с двумя $K = 2$ одноканальными СМО, с пуассоновским входящим потоком заявок интенсивности $\lambda = 1$ и экспоненциальным распределением времени обслуживания. Каждая из заявок при поступлении делится соответственно на два фрагмента, каждый из которых поступает в одну из двух одноканальных СМО типа M/M1 с интенсивностями обслуживания фрагментов μ_1 и μ_2 для первой и второй системы соответственно, которые удовлетворяют условию $1 < \mu_1 \leq \mu_2$, гарантируя, что со временем сеть не переполнится. Поведение системы описывается непрерывным

марковским процессом $X(t) = \{x_1(t), x_2(t), t \geq 0\}$, где $x_k(t)$ – число подзапросов k -го тип ($k = \overline{1, 2}$). Т.е. в некоторый момент времени t состояние сети определяется парой (i, j) , где i – число фрагментов в первой СМО, j – во второй. Стационарная вероятность состояния (i, j) обозначается как $p(i, j)$, стационарный режим сети существует когда $\min(\mu_1, \mu_2) > 1$. Основным результатом работы [99] стало нахождение двойной производящей функции: $P(z, w) = \sum_{i, j \geq 0} p(i, j) z^i w^j$ стационарного распределения, поиск которой осуществляется с помощью функционального уравнения [98–100]:

$$Q(z, w)P(z, w) = N(z, w), \quad |z|, |w| \leq 1,$$

где:

$$Q(z, w) = (1 + \mu_1 + \mu_2)zw - \mu_1 w - \mu_2 z - z^2 w^2 P(z, 0) = P(0, z) = \frac{(\mu - 1)^{3/2}}{\mu(\mu - 1)^{1/2}},$$

$$N(z, w) = \mu_2 z(w - 1)P(z, 0) + \mu_1 w(z - 1)P(0, w)$$

Анализ производящей функции $P(z, w)$ позволяет получить выражение для $P(z, 0)$ и $P(0, w)$, которые в случае $\mu_1 = \mu_2 = \mu$ равны между собой:

$$P(z, 0) = P(0, z) = \frac{(\mu - 1)^{3/2}}{\mu(\mu - 1)^{1/2}}$$

Для сетей с $K > 2$ параллельных систем в работах авторов [101-105] приведены только приближенные результаты. Используя результаты работы [97], в работе [3] был предложен приближенный метод, который применяется для анализа экспоненциальной сети с произвольным числом параллельных систем обслуживания. Данный метод позволяет определить математическое ожидание T_K длительности пребывания заявки в сети, характеризующее среднее время пребывания заявки. В данной работе [3] для сети с двумя параллельными системами найдено точное значение T_2 . Предполагается, что в сеть поступает пуассоновский поток с интенсивностью λ , параллельные системы в сети одноприборные (одноканальные СМО), интенсивности обслуживания фрагментов

заявки в этих системах одинаковые и равны μ , т.е. $\mu_1 = \mu_2 = \mu$, причем $\lambda < \mu$, поэтому нагрузка на каждую из систем $\rho = \lambda/\mu < 1$.

$$T_2 = \frac{12 - \rho}{8} T_1,$$

где $T_1 = 1/\mu - \lambda$, $\rho_1 = \lambda/\mu$.

Вывод величины T_2 основан на наблюдении, что эта величина есть сумма времени пребывания фрагмента в первой одноканальной СМО М/М/1 и времени, проведенного этим фрагментом в очереди синхронизации в ожидании сопряженного второго фрагмента. В работе [106] приводится один из вариантов сети fork-join с использованием примитивов синхронизации (мьютексы, семафоры и пр.), называемый сетью типа split-merge queueing system (split-merge). Отличие заключается в том, что в свободные СМО не поступит ни один фрагмент следующего запроса до того момента, пока не обслужатся все фрагменты текущего запроса, обрабатываемого в сети. Т.е. с помощью примитивов синхронизации выполняется блокировка освободившейся СМО до окончания обработки всех задач запроса. Схема сети типа split-merge приведена на рисунке 1.4.

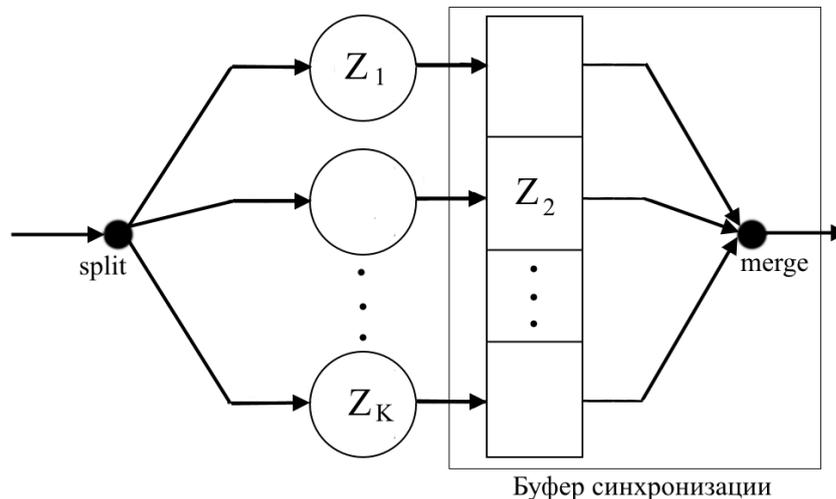


Рисунок 1.4 – Схема сети split-merge

Также в работе [106] рассмотрена еще одна разновидность сети fork-join, называемая fission-fusion queueing system, в которой предполагается, что поступающие заявки являются идентичными и, соответственно, они разбиваются

на K идентичных фрагментов. Следовательно, заявка может кинуть сеть после обработки любых K фрагментов, которые могут принадлежать любым заявкам.

Для сети типа split-merge в работе [107] представлено точное решение по определению максимума времени обслуживания независимых каналов с экспоненциальным временем обслуживания и различными интенсивностями, а также аппроксимации для случая общего распределения.

Там образом, для передачи разделяемых кадров видеоданных возможно рассмотреть применение разновидностей сетей массового обслуживания с делением и слиянием заявок. Для этого требуется выполнить необходимые аналитические расчеты и построить имитационную модель системы связи в целях определения её оптимальных показателей, таких как пропускная способность двух используемых каналов связи.

1.4 Аналитический метод исследования систем распределенной передачи данных

В последние время одним из наиболее востребованных аналитических методов моделирования систем массового обслуживания (СМО) является подход, основанный на теории цепей Маркова с непрерывным временем (уравнения А.Н. Колмогорова). Этот подход позволяет анализировать вероятности различных состояний системы как в динамическом, так и в стационарном режимах, что способствует вычислению ключевых эксплуатационных характеристик СМО, таких как пропускная способность системы, средняя занятость каналов и очередей, вероятность потери заявки, продолжительность нахождения заявки в системе и пр. Указанные показатели определяются на основе предварительно найденных вероятностей возможных состояний системы заданной структуры.

Аналитический подход к моделированию достаточно легко реализуется и часто удобен в использовании. Однако он не свободен от ряда недостатков, которые, в основном, связаны с упрощающими допущениями при формализации. Одним из ключевых ограничений является требование, чтобы как входной поток заявок, так и поток обслуживания были простейшими Пуассоновскими

процессами. Это предполагает, что потоки заявок должны удовлетворять требованиям стационарности (статистические характеристики процессов не зависят от времени), ординарности (вероятность появления двух или более событий в малом интервале времени пренебрежимо мала), отсутствия последствия (каждое событие не зависит от предыдущих, что соответствует марковскому свойству). Также предполагается, что случайные величины, описывающие интервалы между событиями, распределены экспоненциально. В реальных системах это не всегда так, что может привести к несоответствию модели реальному поведению системы. Такие упрощающие допущения могут не учитывать сложные зависимости, корреляции между заявками, сезонность, влияние внешних факторов и другие реальные особенности работы СМО. Тем не менее, использование уравнений А.Н. Колмогорова для анализа поведения СМО имеет весьма широкое распространение [108, 109].

В качестве математической модели для оптимизации двухканальной системы связи, служащей для передачи разделяемых на неравные части кадров потока видеоданных является СеМО с делением и слиянием заявок с двумя одноканальными СМО типа fork-join или её разновидность split-merge. Таким образом, исследуемая СеМО имеет две одноканальные СМО (СМО-1, СМО-2) и неограниченную очередь из поступающих заявок. Поступающий на вход системы поток обладает экспоненциальным законом распределения величины промежутка времени между заявками и средней интенсивностью λ . Поступающие заявки разбиваются на сопряженные фрагменты с тем допущением, что между весами (размерами) заявок сохраняется одна и та же пропорция: $h_2/h_1 = \gamma = const$. Фрагмент, имеющий наибольший вес, имеет большее время обслуживания в одноканальной СМО. Интенсивности обслуживания фрагментов заявки в этих системах одинаковые и равны μ , т.е. $\mu_1 = \mu_2 = \mu$, причем $\lambda < \mu$, поэтому нагрузка на каждую из систем $\rho = \lambda/\mu < 1$, все три потока – входящий поток заявок, поток фрагментов в СМО-1 и поток фрагментов в СМО-2 описываются одними и теми же вероятностными законами. После обслуживания каждый фрагмент попадает в

соответствующую ему очередь синхронизации, где дожидается обслуживания сопряженного с ним фрагмента, только после этого оба фрагмента объединяются в заявку и покидают СеМО. В очереди синхронизации фрагменты поступают в той же последовательности, в которой заявка входит в СеМО. Дисциплина обслуживания заявок в СеМО – FIFO (First In – First Out, первым поступил – первым ушел).

С учетом допущения, что между фрагментами сохраняется одна и та же пропорция: $h_2/h_1 = \gamma = const$, можно добиться максимальной положительной корреляции между процессами перемещения сопряженных фрагментов по одноканальным СМО-1 и СМО-2, тем самым сократить время задержки сопряженных фрагментов в очередях синхронизации. Тогда пропускные способности одноканальных СМО-1 и СМО-1 также можно связать условием $C_2 = \gamma C_1$. Таким образом, приведенные допущения позволят с помощью аналитического подхода исследовать двухканальную систему связи и в дальнейшем выполнить сравнение с результатами, полученными при помощи имитационного моделирования.

1.5 Имитационное моделирование и оптимизация систем передачи данных

Для исследования и проектирования сложных систем требуется применение методов, способных учесть множественность взаимодействующих компонентов, динамику, стохастические эффекты и высокую неопределённость. Основной подход здесь возможен за счет применения имитационного моделирования, которое позволяет исследовать системы и решать поставленные задачи в тех случаях, когда проведение экспериментов на реальном объекте дорого, небезопасно или практически невозможно, а также когда аналитическая модель системы слишком сложна для получения точного решения.

Имитационное моделирование систем распределенной передачи данных по двум параллельным каналам связи позволяет создать виртуальную копию системы, в которой учитываются особенности параллельной передачи, взаимодействие каналов и влияние случайных факторов. Основные свойства такой модели можно охарактеризовать следующим образом [110–113]:

– параллельность и отказоустойчивость: использование двух независимых (но взаимодействующих) каналов связи позволяет обеспечить дублирование данных и резервирование. В случае отказа одного канала система может продолжать работу за счет второго, что повышает надежность передачи информации;

– синхронизация потоков данных: для корректной работы модели важно учесть необходимость синхронизации потоков, поступающих по разным каналам. Это включает обработку временных задержек, выравнивание временных меток и координацию обмена данными между каналами;

– стохастическая природа передачи: моделирование должно учитывать случайные задержки, ошибки передачи, потери пакетов и помехи, которые естественны для реальных систем связи. Это позволяет оценить устойчивость и производительность системы при различных условиях нагрузки и внешних воздействиях;

– адаптивное управление нагрузкой: имитационная модель предоставляет возможность протестировать алгоритмы балансировки нагрузки между каналами, динамической маршрутизации пакетов и распределения ресурсов, что помогает оптимизировать работу системы при изменении условий эксплуатации;

– многоуровневая детализация: модель может быть построена на разных уровнях абстракции. На макроуровне анализируются общие параметры (пропускная способность, среднее время задержки), а на микроуровне — моделируются индивидуальные события (передача отдельного пакета, обработка ошибок). Такой подход позволяет проводить как стратегический, так и тактический анализ системы.

В качестве имитационной модели двухканальной связи рассматривается СеМО с двумя одноканальными СМО (СМО-1, СМО-2), в которую при поступлении данных (в терминах теории массового обслуживания – заявок) они тут же разделяются на две сопряжённые части (фрагмента), каждая из которых передаётся на обслуживание в соответствующую им СМО. Для данной СеМО необходимо задать данные о характере входящего в неё на обслуживание потока заявок, о дисциплине обслуживания очереди из заявок, правилу распределения заявок по СМО. Входящий поток заявок описывается моментами времени их поступления в СеМО. Закон поступления может быть двух типов:

детерминированный – заявки поступают через точно установленные, фиксированные интервалы времени, такой подход характерен для систем, где нагрузка предсказуема и изменения во времени незначительны; вероятностный – интервалы между заявками являются случайными величинами и описываются с использованием вероятностных распределений, наиболее часто применяется пуассоновский процесс, в рамках которого время между заявками имеет экспоненциальное распределение. При проектировании СеМО с двумя одноканальными СМО входящий поток заявок описывается распределением вероятностей интервалов времени между соседними заявками. Правила обслуживания заявок в СеМО характеризуются длительностью обслуживания (распределением времени обслуживания) и дисциплиной обслуживания. Для характеристики свойств каждой СМО задается длительность обслуживания фрагментов заявок или временем занятия фрагментов соответствующей СМО как случайной величиной с заданным законом распределения. Все поступающие в СеМО заявки обслуживаются в порядке очереди – выполняется разделение их на сопряженные фрагменты, и передача этих фрагментов по соответствующим СМО, после передачи по одной из СМО обслуженный фрагмент дожидается свой сопряженный фрагмент из другой СМО в очереди синхронизации (буфере). После получения обоих фрагментов они объединяются в исходную заявку, которая покидает СеМО. Дисциплина обслуживания заявок в СеМО определяется как FIFO.

Так как, для моделируемой двухканальной системы связи требуется обеспечить синхронную доставку разделенных кадров видеоданных разного объема при помощи выбора оптимальных пропускных способностей каналов связи, в имитационной модели СеМО необходимо предусмотреть обратную связь, которая может быть реализована с помощью примитивов синхронизации и позволяющая блокировать поступление следующей заявки на обслуживание до тех пор, пока не обслужена предыдущая. Таким образом СеМО становится сетью split-merge, являющейся разновидностью сетей fork-join, это необходимо для того, чтобы имитационная модель смогла самостоятельно автоматически подстраивать параметры времени занятия фрагментами соответствующих СМО. С учетом того,

что в двухканальной системе связи передаются части кадра разного объема, то в имитационной модели СеМО требуется предусмотреть такое свойство фрагмента заявки, как его вес, смысл которого проявляется в увеличении времени обслуживания фрагмента с большим весом [114].

Выходными параметрами для двухканальной системы связи являются величины, характеризующие издержки по её содержанию и качество её функционирования как СеМО с двумя одноканальными СМО. Такими параметрами являются: минимальные показатели финансовых затрат, приходящихся на аренду такой системы; оптимальные пропускные способности, необходимые для синхронной передачи данных по двум каналам связи; количество переданных кадров видеоданных. Такие параметры системы достигаются за счет максимальной загрузки и минимального простоя каналов связи, а также за счет привлечения механизмов синхронизации передачи данных.

Имитационная модель двухканальной системы связи позволит определить её характеристики и изменения состояния во времени при определённых свойствах потока данных, поступающего на вход системы, а также осуществить исследования алгоритмов распределения данных и выполнить оптимизацию характеристик системы.

Имитационное моделирование целесообразно проводить с помощью современных программных средств, обеспечивающих визуальное представление модели и позволяющих программировать недостающий функционал, а также проводить комплексный анализ имитационных экспериментов. В качестве таких программных средств могут выступать AnyLogic, Arena, GPSS, Matlab/Simulink/Simevents, которые позволяют описывать входящие потоки заявок, анализировать распределение заявок между параллельными каналами и проводить оптимизацию характеристик системы, учитывая случайные и детерминированные законы поступления информации. Выбор конкретного средства зависит от поставленных задач, требуемого уровня детализации модели и специфики исследуемой системы.

1.6 Выводы по главе

1. Проведённый анализ проблем распределённой передачи видеоданных в

информационных системах и системах связи с ограниченными вычислительными ресурсами выявил необходимость применения системного подхода для повышения стабильности работы системы. Это включает оптимизацию пропускных способностей каналов связи, сокращение расходов на их аренду и обеспечение конфиденциальности передаваемой информации.

Установлено, что системный подход должен реализовываться посредством разработки комплекса научно-технических решений, включающих: алгоритмы кодирования видеоданных с использованием схем разделения; методику аналитического расчёта оптимальных пропускных способностей каналов для определения нижних границ доверительных интервалов; модель двухканальной системы связи, предназначенную для имитационных и модельных исследований с целью оптимизации параметров системы связи по следующим критериям: максимизация объёма передаваемых данных, минимизация требуемых пропускных способностей и сокращение времени простоя каналов при обеспечении синхронной передачи информации.

2. При обзоре существующих алгоритмов и схем разделения, используемых для изображений, выявлена необходимость разработки таких алгоритмов, которые выполняли бы их разделение на части неравного размера. Это позволит использовать подобные алгоритмы при кодировании кадров видеоданных и организации их распределенной передачи по двум каналам связи, которые обладают различными пропускными способностями. Обозначено, что алгоритмы, разрабатываемые в рамках данного исследования, должны быть ориентированы на решение конкретной задачи, а именно – использование простых математических операций, что может положительно сказаться на увеличении скорости преобразований. Также сопутствующим решением является – решение по обеспечению конфиденциальности передаваемых видеоданных.

3. Показано, что в исследованиях, посвященных системам и сетям распределенной обработки данных существует определенный класс СеМО с делением и слиянием заявок (fork-join), которые могут быть использованы для проведения оптимизационных процессов в системах, использующих

распределённые (параллельные) вычисления или обработку данных, либо в системах, где исходная сложная задача делится на части (простые подзадачи) для повышения эффективности. В частности, определена разновидность сетей fork-join, подходящих для проведения аналитических расчетов и построения имитационной модели системы двухканальной системы связи в целях определения её оптимальных показателей.

4. Обозначена возможность применения аналитического подхода к моделированию двухканальной системы связи для передачи данных. На основе проведённого обзора приведена математическая модель для оптимизации параметров данной системы связи, а также приведены её основные характеристики. В дополнение, сформулированы допущения, позволяющие обеспечить положительную корреляцию между процессами обслуживания сопряжённых фрагментов в системе, что, в свою очередь, способствует упрощению задачи оптимизации пропускных способностей каналов связи.

5. Определено, что имитационное моделирование не только позволяет оптимизировать параметры двухканальной системы связи для повышения её стабильности, но и способствует сокращению финансовых затрат на её обслуживание и эксплуатацию за счёт разработки эффективных стратегий распределения ресурсов.

2 РАЗРАБОТКА АЛГОРИТМОВ КОДИРОВАНИЯ ИЗОБРАЖЕНИЙ НА ОСНОВЕ СХЕМ РАЗДЕЛЕНИЯ ДАННЫХ

Как было отмечено выше, что, ввиду увеличивающегося числа многоканальных систем передачи данных, перспективным направлением является разработка алгоритмов распределенной передачи данных. Определено, что наиболее пригодными являются алгоритмы, основанные на разделении данных, обоснование их пригодности и эффективности приведено в первой главе данной диссертационной работы. Данная глава посвящена разработке алгоритмов разделения изображений, основанных на схемах разделения данных. Основная особенность – отсутствие необходимости выполнения сложных вычислительных операций, разделение изображений на части неравного размера. Восстановление исходного состояния изображения по большей части, полученной в результате разделения, невозможно выполнить без значения меньшей, таким образом, дополнительно обеспечивается конфиденциальность.

Предложено два алгоритма, основанных на разделении данных на неравные части, проведена их оценка по критерию возможности восстановления исходного изображения только по большей части, определена пригодность применимости к черно-белым и цветным изображениям. Первый алгоритм в дальнейшем называется – «Алгоритм разделения изображений по дробным частям десятичных чисел» (АРДЧ), второй – «Алгоритм разделения изображений с помощью префиксного кодирования» (АРПК) [33–38].

2.1 Разработка алгоритма разделения изображений по дробным частям десятичных чисел

В описываемом в данном разделе алгоритме, разделение несжатого изображения на неравные части осуществляется путем построения из значений пикселей в двоичной системе счисления системы уравнений, из коэффициентов при слагаемых левой части которой можно составить квадратную матрицу с частичным диагональным преобладанием, и определителем равным нулю [33, 34, 36]. Выбор матрицы такого вида обусловлен тем, что в дальнейшем требуется выполнить быстрое восстановление исходного изображения при помощи

поиска решений системы алгебраических уравнений. Быстрый поиск решений выполняется с применением метода простой итерации, в частности метода Якоби.

Алгоритм разделения изображения.

Предварительная обработка. На вход алгоритма от источника подается несжатый поток цифровых изображений W размером $M \times N$. Осуществляется деление данного потока на кадры w_i , $i = \overline{1, K}$, где K – число кадров потока. Или же от источника на вход алгоритма сразу осуществляется покадровая передача цифровых изображений. На рисунке 2.1 приведен алгоритм получения частей изображения, который состоит из следующих шагов.

Шаг 1. Для каждого поступившего на обработку кадра w_i выполняется построчное чтение пикселей (от 1 до M). Для прочитанного пикселя находится его представление в соответствии с цветовой моделью RGB (Red, Green, Blue) [115], кодируемое тремя десятичными числами в диапазоне от 0 до 255 включительно. Соответственно, определяющими интенсивность красного, зеленого и синего цветов пикселя. Полученные десятичные значения интенсивностей цветовых составляющих переводятся в двоичную систему исчисления, и записываются последовательно друг за другом. В результате получается 24-х битовая последовательность:

$$T = [r_1 r_2 r_3 r_4 r_5 r_6 r_7 r_8 g_1 g_2 g_3 g_4 g_5 g_6 g_7 g_8 b_1 b_2 b_3 b_4 b_5 b_6 b_7 b_8] \quad (2.1)$$

где $r_1 - r_8$, $g_1 - g_8$, $b_1 - b_8$ – порядковые номера 24-х битовой последовательности, соответствующие красному, зелёному и синему цветам соответственно.

Шаг 2. Для каждой последовательности (2.1) выполняется перестановка:

$$T' = [r_1 g_1 b_1 r_2 g_2 b_2 r_3 g_3 b_3 r_4 g_4 b_4 r_5 g_5 b_5 r_6 g_6 b_6 r_7 g_7 b_7 r_8 g_8 b_8] \quad (2.2)$$

Шаг 3. Последовательность T' разбивается на блоки по четыре бита, которые будут являться дробной частью десятичных чисел a_p , $p = 1, \dots, 6$: $a_1 = 0, r_1 g_1 b_1 r_2$; $a_2 = 0, g_2 b_2 r_3 g_3$; $a_3 = 0, b_3 r_4 g_4 b_4$; $a_4 = 0, r_5 g_5 b_5 r_6$; $a_5 = 0, g_6 b_6 r_7 g_7$; $a_6 = 0, b_7 r_8 g_8 b_8$.

Таким образом, для каждой строки пикселей n_j , $j = \overline{1, N}$ изображения формируется массив A_j размерностью $6M$, состоящий из a_p каждого пикселя.

Шаг 4. Находится среднее значение элементов массива A_j :

$$sr_{A_j} = \sum_{i=1}^{6M} a_i / 6M \quad (2.3)$$

Шаг 5. Формируется массив A'_j размером $6M$, состоящий из элементов:

$$a'_i = sr_{A_j} - a_i, \quad (2.4)$$

где $i = \overline{1, 6M}$, sr_{A_j} - значение, полученное в (2.3).

Шаг 6. Находится массив F_j , $j = \overline{1, N}$ размером $6M$, состоящий из f_i :

$$\begin{aligned} -a'_{6M} + 2a'_i - a'_{i+1} &= f_i, \text{ при } i=1 \\ -a'_{i-1} + 2a'_i - a'_{i+1} &= f_i, \text{ при } 1 < i < 6M \\ -a'_{i-1} + 2a'_i - a'_1 &= f_i, \text{ при } i=6M \end{aligned} \quad (2.5)$$

Шаги 1-6 повторяются для каждой строки писклей поступившего для кодирования изображения, в результате преобразований формируются все F_j , $j = \overline{1, N}$ массивы данных.

Уравнения (2.5) вводятся для того, чтобы из коэффициентов при слагаемых левой части составить квадратную матрицу с частичным диагональным преобладанием и определителем равным нулю. Так как, при восстановлении исходного изображения необходимо будет использовать поиск решений при помощи метода простой итерации для системы линейных алгебраических уравнений:

$$H = \begin{pmatrix} 2 & -1 & \dots & 0 & -1 \\ -1 & 2 & -1 & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & -1 & 2 & -1 \\ -1 & 0 & \dots & -1 & 2 \end{pmatrix} \quad (2.6)$$

Все полученные элементы f_i меньше 1 (т.е. $f_i < 1$), аналитически получено, что при восстановлении изображения необходимо производить вычисление f_i с точностью до шести, максимум девяти знаков после запятой.

Выход: В зависимости от технических требований двухканальной системы связи, в качестве передаваемой меньшей части, могут выступать:

а) последовательность из знаков *всех* элементов f_i массивов F_j , тогда

большей частью являются массивы F'_j , состоящие из элементов $|f_i|$. Дополнительно, последовательность, образующая меньшую часть, может быть сжата без потерь;

б) последовательность из знаков *некоторых* элементов f_i массивов F_j , тогда большей частью являются массивы F'_j . Меньшая часть состоит из изъятых знаков и мест их изъятия;

в) последовательность из средних значений sr_{A_j} , полученных для каждой строки пикселей изображения по (2.4);

г) комбинации выше описанных вариантов.

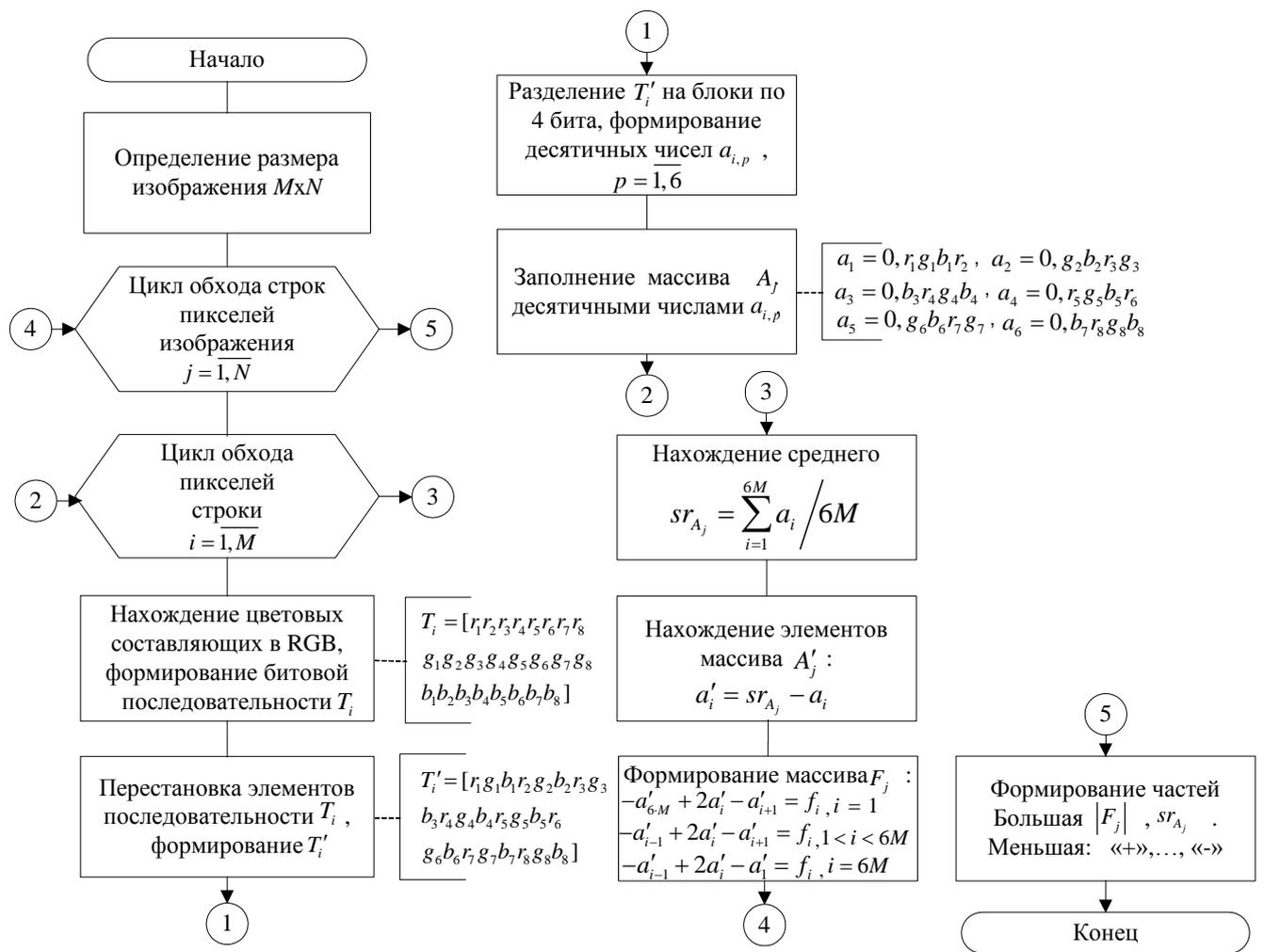


Рисунок 2.1 – Алгоритм получения частей изображения

На рисунках 2.2, а, 2.3, а приведены исходные изображения кадра, а на рисунках 2.2, б, 2.3, б изображения кадров, полученное при попытках преобразования больших частей, состоящих из элементов $|f_i|$ массивов F'_j , в

значения пикселей в соответствии с цветовой моделью RGB.

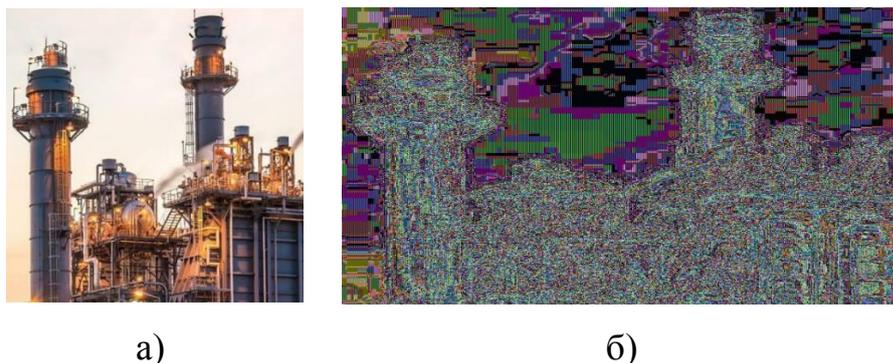


Рисунок 2.2 – Попытка восстановления цветного изображения по большей части:

а) исходное изображение; б) результат восстановления

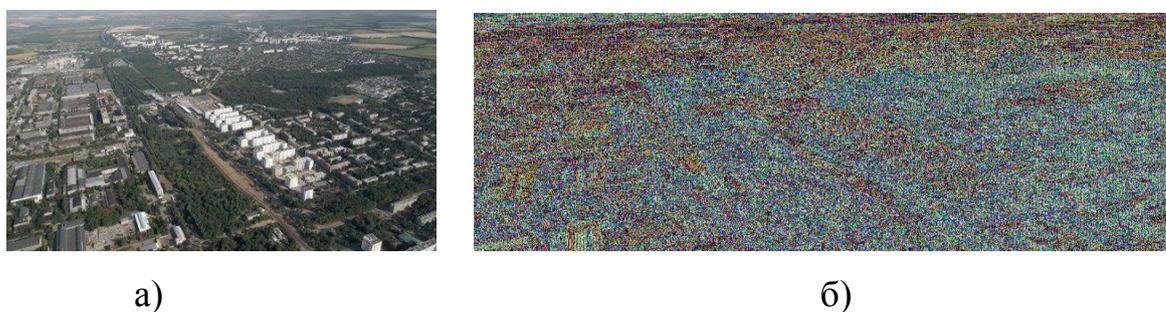


Рисунок 2.3 – Попытка восстановления цветного изображения по большей части:

а) исходное изображение; б) результат восстановления

Из рисунка 2.2, б, видно, что при попытке восстановления исходного изображения кадра по элементам $|f_i|$ массивов F'_i проявляются резкие границы (переходы) изображения, а на рисунка 2.3, б подобных границ не наблюдается. Например, чтобы избежать проявления этих границ, преобразование исходного кадра может осуществляться в несколько раундов следующим образом: полученное изображение после первого раунда поворачивается на 90 градусов и осуществляется второй раунд преобразований. Кроме того, вместо выполнения второго раунда преобразований можно выполнить перестановку строк и столбцов, описанную в [64].

Определено, что предложенный алгоритм пригоден для многоцветных изображений, но если на вход алгоритма подать чёрно-белое изображение с чётко выраженными границами, например, как на рисунке 2.4, а, то в результате

выполнения попытки восстановления по большей части, полученной в результате разделения, будут прослеживаться границы перехода цвета (рис. 2.4, б) [33, 34].

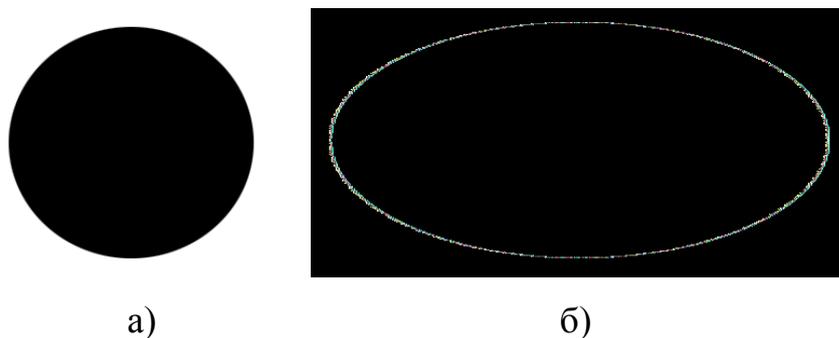


Рисунок 2.4 – Попытка восстановления черно-белого изображения по большей части: а) исходное изображение; б) результат восстановления

Чтобы избежать осуществления преобразований в несколько раундов или перестановки столбцов (срок), в уравнениях, приведенных в (2.5), вместо «2» можно использовать другие положительные значения, например, «10», «100» и т.д. На рисунке 2.5 приведены изображения при попытках его восстановления по большей части, когда по главной диагонали матрицы (2.6) вместо «2» стоят «10» и «100» соответственно.



Рисунок 2.5 – Попытка восстановления цветного изображения по большей части при замене чисел по главной диагонали в матрице (2.6): а) результат восстановления при «10»; б) результат восстановления при «100»

Из рисунка 2.5 видно, что с увеличением числа стоящего по главной диагонали матрицы (2.6), увеличивается степень размытости, и резкие границы цветового перехода становятся менее заметны.

Для черно-белых изображений при увеличении числа, стоящего по диагонали матрицы (2.6), при попытках восстановления получены изображения на рисунке 2.6.

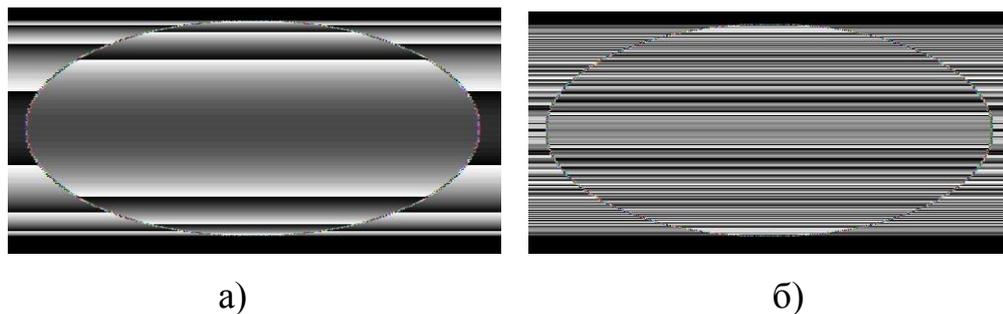


Рисунок 2.6 – Попытка восстановления черно-белого изображения по большей части при замене чисел по главной диагонали в матрице (2.6): а) результат восстановления при «10»; б) результат восстановления при «100»

Из рисунка 2.6 видно, что для чёрно-белых изображений всё равно прослеживаются границы резкого перехода цвета, но изменяется фон.

Таким образом, можно утверждать, что в случаях необходимости дополнительного обеспечения конфиденциальности при кодировании потока видеоданных при распределенной передаче через двухканальную систему связи, предложенный алгоритм вполне пригоден для многоцветных изображений и для изображений в градациях серого без ярко выраженных границ. Также он может применяться в случаях, когда не требуется полного сокрытия передаваемых чёрно-белых изображений с ярко выраженными границами.

Алгоритм восстановления изображения.

На рисунке 2.7 приведен алгоритм восстановления изображения, который состоит из следующих шагов [33, 34, 36].

Шаг 1. Определение размера передаваемых изображений – $M \times N$ (передается системой связи).

Шаг 2. Меньшая часть S' , например, состоит из N последовательностей знаков всех элементов f_i ($i = \overline{1, 6M}$) массивов F_j ($j = \overline{1, N}$) (как один из примеров меньшей части). Тогда N массивов F'_j из элементов $|f_i|$ являются большей частью – F' . Выполняется объединение S' с F' , т.е. каждому элементу $|f_i|$ подставляется соответствующий из S' знак (+) или (-): $S = S' \cup F'$. Полученные в результате объединения данные обозначаются как S . В случае, если осуществлялось какое-либо сжатие

меньшей части S' , то вначале осуществляется её преобразование к первостепенному виду.

Шаг 3. Так как требуется обеспечить быстрое восстановление исходного изображения, то предполагается использование, например, метода Якоби для вычисления собственных значений для матрицы H , приведенной в (2.6). Метод Якоби для собственных значений представляет собой итерационный алгоритм для вычисления собственных значений и собственных векторов вещественной симметричной матрицы. Назван в честь Карла Густава Якоби, предложившего данный метод в 1846 году [116]. Широкое распространение данный метод получил в 1950-х годах в связи с появлением компьютеров.

Для матрицы H находятся собственные значения (числа) λ_i и собственные векторы v_i . Следует заметить, что размеры изображения заранее известны, тогда для увеличения скорости преобразования собственные векторы v_i и собственные числа λ_i , могут быть вычислены заранее и храниться в любом доступном месте.

Восстановление выполняется по следующему принципу: $HA' = S$, где H – матрица симметричная относительно главной диагонали (2.6), A' – одномерный массив данных a'_i , необходимый для восстановления данных (в данном случае является вектором), S – одномерный массив данных, полученных после объединения S' с F' на шаге 2 (в данном случае также является вектором).

Шаг 4. Вычисляются скалярные произведения β_i вектора S на собственные векторы v_i матрицы H :

$$\beta_i = (S, v_i) \quad (2.7)$$

Находятся значения a'_i одномерного массива данных (вектора):

$$A' = \sum_{i=1}^{6M} \frac{\beta_i}{\lambda_i} v_i \quad (2.8)$$

Шаг 5. Находятся элементы исходного массива A :

$$a_i = sr_A - a'_i \quad (2.9)$$

Шаг 6. Выполняется обратная перестановка для (2.2), т.е. $T' \Rightarrow T$.

Шаг 7. Осуществляется преобразование полученных на шаге 6 значений пикселей из двоичной системы счисления в десятичную, и выполняется переход к модели RGB.

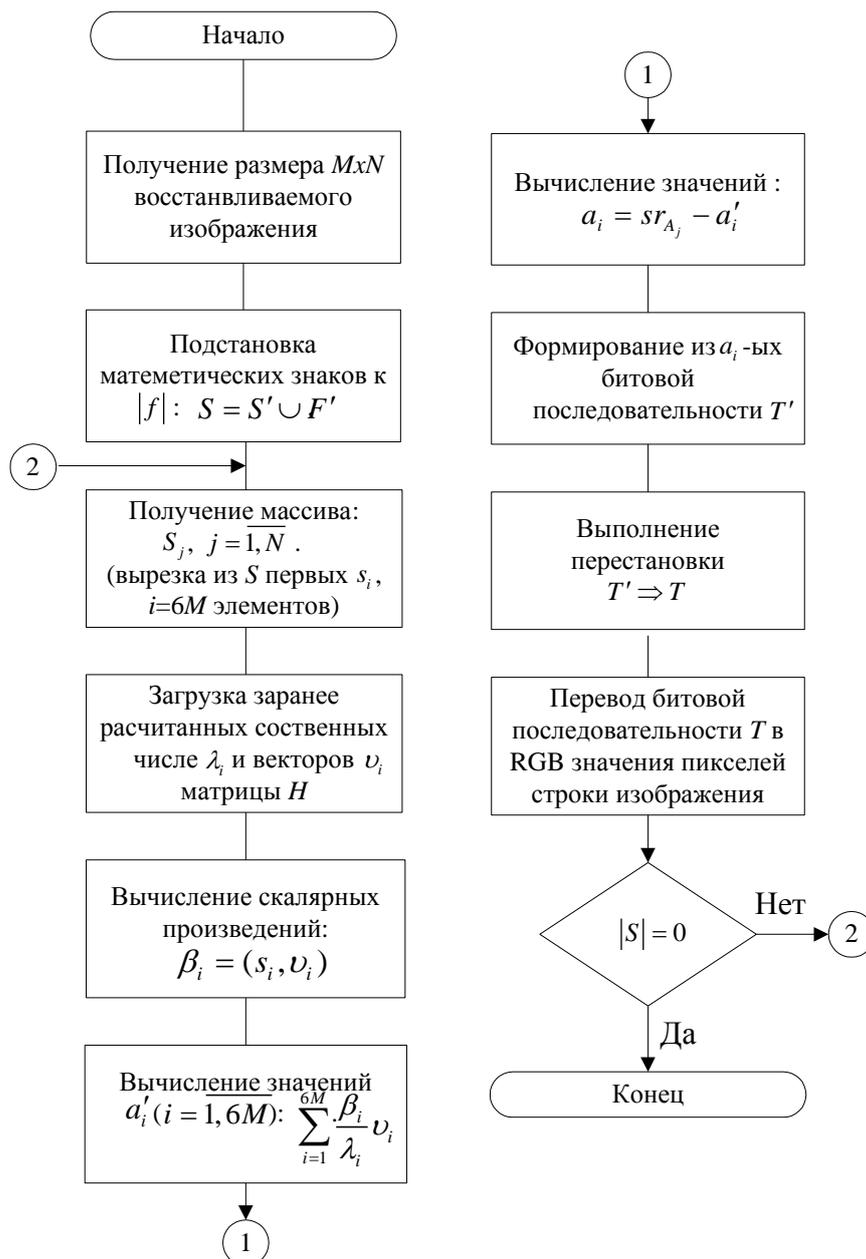


Рисунок 2.7 – Алгоритм восстановления изображения

В приложении А1 приведен пример работы АДЧ. Также в среде программирования C++ Builder (RAD Studio) выполнена программная реализация в виде модуля, который позволяет проводить эксперименты по разделению и объединению кадров видеоданных на части. Интерфейс модуля приведен на рисунке 2.8, получено свидетельство о государственной регистрации программ для ЭВМ № 2013661618 (Приложение Б).

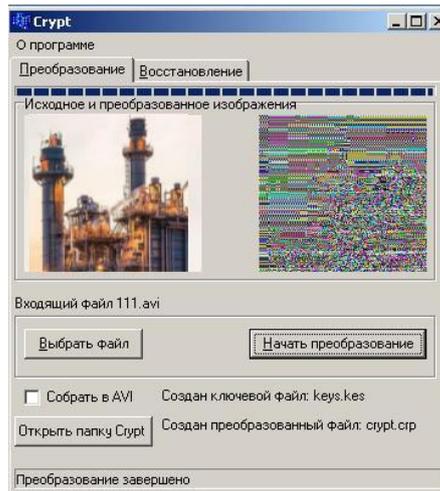


Рисунок 2.8 – Интерфейс программного модуля, реализующего АДЧ

В данном программном модуле реализована многопоточная обработка видеок кадров с использованием классов TThread. В зависимости от разрешения входящих изображений и доступных вычислительных ресурсов удалось обеспечить производительность от 12 до 20 кадров в секунду [33, 34].

2.2 Разработка алгоритма разделения изображений с помощью префиксного кодирования

Разработанный и описанный в 2.1. алгоритм пригоден для обеспечения конфиденциальности многоцветных изображений и изображений в градациях серого без ярко выраженных границ. Но для однотонных цветных или чёрно-белых изображений и изображений с ярко выраженными границами, например, печатного текста данный алгоритм не пригоден. К тому же, формируемая большая часть по объему не всегда может отвечать техническим требованиям двухканальной системы связи. Поэтому, целесообразно разработать ещё один алгоритм разделения изображения на части неравного размера.

Вначале рассмотрим задачу хранения большого числа массивов данных, длины записи которых существенно различаются. Пусть даны n битовых векторов A_1, \dots, A_n , размерности которых равны M_1, \dots, M_n соответственно, и дисперсии D_i распределены равномерно в достаточно большом интервале. В данном случае возникает проблема экономичной записи данных, которая в настоящее время решается различными способами, например, грубым физическим разделением

данных по различным носителям данных [68], введение различных типов данных, наподобие CHAR и VARCHAR, разделение данных маркерами, создание дисковых массивов типа RAID 0. Но, если M_1 варьируются от 10^3 до 10^{10} , а число битовых векторов n изменяется, то отведение равных областей памяти для каждого A_i нецелесообразно, а разделение данных специальной строкой бит (маркером) неэффективно по времени поиска этого маркера, и нет никакой гарантии, что выбранная в качестве маркера строка не встретится ни в одном из A_i [118].

Рассмотрим кодирование положительных целых чисел при помощи дельта-кода Элиаса осуществляется по следующему алгоритму [119]:

- 1) считается количество значащих битов L в двоичном представлении числа N ;
- 2) считается количество значащих битов M в двоичном представлении числа L ;
- 3) осуществляется запись $M - 1$ нулей и одной единицы;
- 4) дописывается $L_2 - M - 1$ младших битов двоичного представления числа L без старшей единицы (2^{M-1});
- 5) дописывается $N_2 - L - 1$ младших битов двоичного представления числа N без старшей единицы (2^{L-1}).

Например, необходимо закодировать $L = 4_{10} = 100_2$ с помощью дельта-кода Элиаса число 10:

- 1) число 10 переводится в двоичную систему счисления, число значащих битов $L = 4$; $N = 10_{10} = 1010_2$
 - 2) в двоичном представлении число имеет $M = 3$ значащих бита;
 - 3) осуществляется запись $M - 1$ нулей и одной единицы, т.е. $3-1=2$ нулей и 1 единицы $\rightarrow 001$;
 - 4) дописываются младшие биты двоичного представления числа L без старшей единицы $\rightarrow 00$;
- дописываются младшие биты двоичного представления числа N без старшей единицы $\rightarrow 010$;
- 5) результат 00100010.

В предлагаемом АРПК используется «примитивизация» дельта-кода Элиаса [33, 37, 38]:

1) первые l бит заполняются нулями, где l – это длина записи числа n (количество битовых последовательностей) в двоичной системе счисления, далее осуществляется сама запись числа n в двоичной системе счисления, например, даны $n = 3$ битовые последовательности, тогда запись числа n в двоичной системе счисления равна $n_2 = 11$, тогда $l = 00$. Следовательно, на первом этапе получается битовая последовательность $\rightarrow 0011$.

2) m_i бит заполняются нулями, где m_i – это число бит необходимых для записи длины M_i битовой последовательности A_i в двоичной системе счисления, затем осуществляется непосредственная запись длины M_i в двоичной системе счисления. Например, так как $n = 3$, следовательно, имеется три битовые последовательности A_1, A_2, A_3 , пусть $A_1 = 111011$, $A_2 = 10111$, $A_3 = 101$, размерности этих битовых последовательностей равны $M_1 = 6_{10} = 110_2$, $M_2 = 5_{10} = 101_2$, $M_3 = 3_{10} = 11_2$, а $m_1 = 000$, $m_2 = 000$, $m_3 = 00$. Следовательно, после второго этапа формируется битовая последовательность $\rightarrow 00110001100001010011$.

3) выполняется непосредственная запись справа битовой последовательности A_i к сформированной в п.п. 1 и п.п. 2 части префикса $\rightarrow 00110001100001010011111011$.

Полученная в результате битовая последовательность (префикс) в дальнейшем используется как меньшая часть.

Алгоритм разделения изображения.

Разделение изображения осуществляется с учетом описанного выше порядка формирования префикса. На рисунке 2.9 приведен алгоритм получения частей изображения с помощью префиксного кодирования, который состоит из следующих шагов.

Шаг 1. Имеется поток видеоданных размером $W \times H$, размер является стандартным и известен всем. Выполняется разбиение потока на кадры – изображения. Производится построчное чтение пикселей изображения и для каждого пикселя находятся их цветовые составляющие в двоичной системе счисления в

соответствии с цветовой моделью RGB, которые записываются последовательно друг за другом в одну строку, создавая последовательность, состоящую из нулей и единиц.

Шаг 2. Последовательность, полученная на шаге 1, разбивается на n битовых векторов A_1, A_2, \dots, A_n разных размерностей M_1, M_2, \dots, M_n . Генерация размерностей M_1, M_2, \dots, M_n осуществляется произвольным образом при помощи датчика псевдослучайных чисел, причём, $M_1 + M_2 + \dots + M_n = 24WH$. Например, для данных целей подойдёт функция `RandomRange()`, встроенная в среду программирования Borland. Данная функция выполняет генерацию псевдослучайных чисел в пределах заданного диапазона и удовлетворяет общим требованиям к датчикам псевдослучайных чисел, описанных в стандарте FIPS 140-1 (Federal Information Processing Standards) [120]. Понятно, что можно использовать и другие генераторы псевдослучайных чисел, удовлетворяющие более важным требованиям. Полученные при помощи датчика случайных чисел размерности последовательностей M_1, M_2, \dots, M_n для первого кадра в дальнейшем применяются для всех остальных кадров потока видеоданных.

Шаг 3. Над полученными битовыми последовательностями A_1, A_2, \dots, A_n осуществляются операции: $X_1 = A_2 \oplus A_3$, $X_2 = A_3 \oplus A_4, \dots$, $X_{n-2} = A_{n-1} \oplus A_n$, $X_{n-1} = A_n \oplus A_1$ (где « \oplus » – операция XOR (побитовое сложение по модулю 2)).

Полученные битовые последовательности X_1, X_2, \dots, X_{n-1} записываются последовательно друг за другом. Следует заметить, что битовые векторы A_1, A_2, \dots, A_n имеют разную размерность и при выполнении операции \oplus , в случае, если $A_{n-1} > A_n$ или $A_{n-1} < A_n$, меньшая битовая последовательность дополняется до большей битовой последовательности собственным повторением символов справа, начиная с первого. Выполнение операции \oplus осуществляется с сохранением длины записи полученных битовых векторов X_i , т.е., если в ходе операции \oplus получены впередистоящие нули, то они не отбрасываются.

Шаг 4. Префикс для битовых последовательностей A_1, A_2, \dots, A_n находится по описанному выше алгоритму, представляющему из себя примитивизацию

дельта-кода Элиаса, и является меньшей частью. Записанные последовательно друг за другом битовые последовательности X_1, X_2, \dots, X_{n-1} являются большей частью.

Кроме того, для формирования битовых векторов X_1, X_2, \dots, X_{n-1} , вместо операции \oplus можно использовать один из режимов блочных шифров таких, как CBC (Cipher Block Chaining), CFB (Cipher Feedback). Это позволит убрать возможную корреляцию между битовыми последовательностями X_1, X_2, \dots, X_{n-1} .

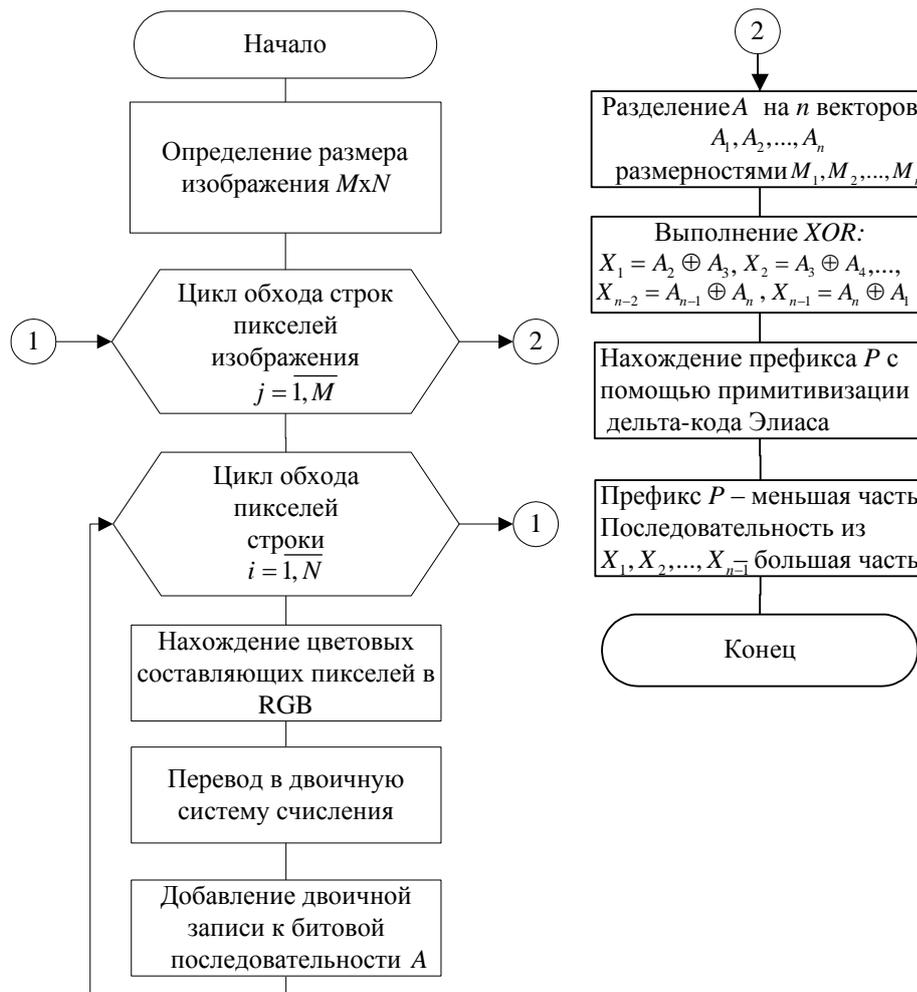


Рисунок 2.9 – Алгоритм получения частей изображения с помощью префиксного кодирования

При попытках восстановить исходное изображение, зная его размеры, информацию о том, что оно представлено в цветовой модели RGB, и только битовую последовательность из последовательно записанных X_i , будут получены изображения, приведенные на рисунках 2.10, б, 2.11, б, 2.12, б, не дающие представление об исходных изображениях.

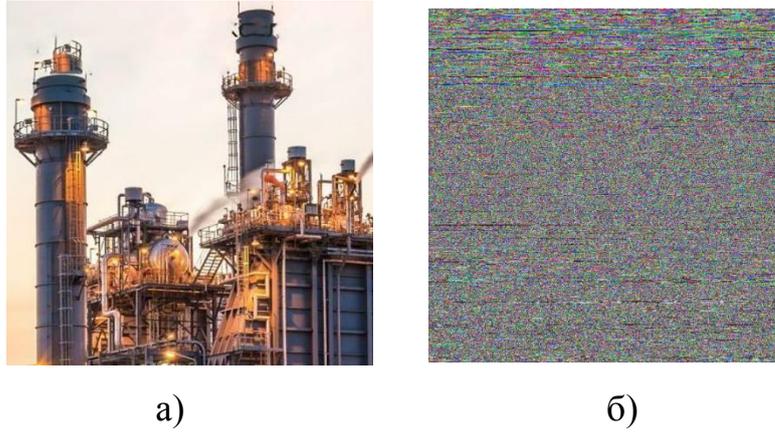


Рисунок 2.10 – Попытка восстановления цветного изображения с резкими границами по большей части: а) исходное изображение; б) результат восстановления

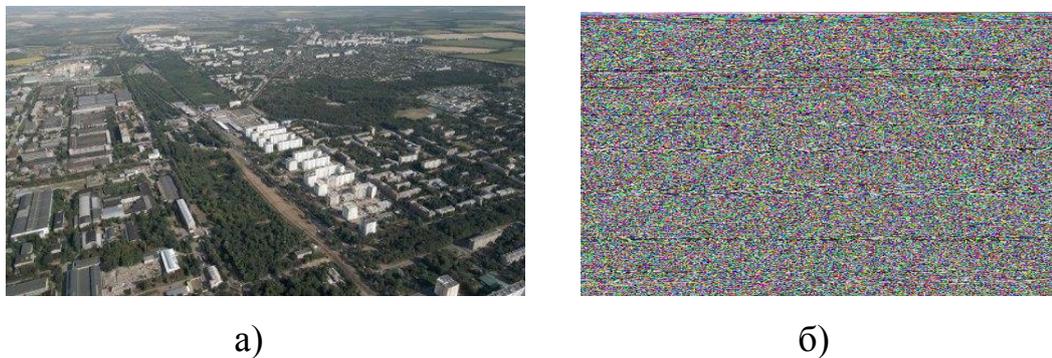


Рисунок 2.11 – Попытка восстановления цветного изображения без резких границ по большей части: а) исходное изображение; б) результат восстановления

Подобная картина наблюдается и для чёрно-белого изображения с ярко выраженными границами (рис. 2.12).

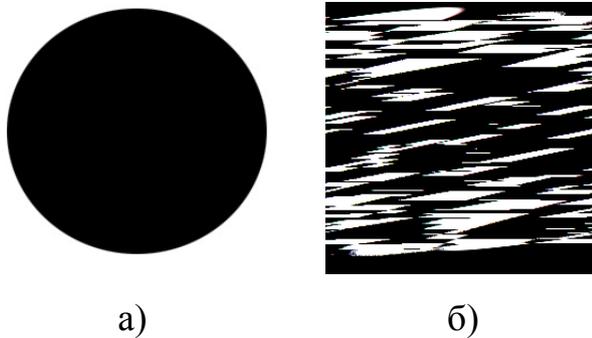


Рисунок 2.12 – Попытка восстановления черно-белого изображения по большей части: а) исходное изображение; б) результат восстановления

Анализируя рисунки 2.10, б, 2.11, б, 2.12, б можно предположить, что даже зная информацию из подряд записанных битовых последовательностей X_i , и применяя разного рода выборки, перестановки и изменения цветовых моделей, не удастся восстановить исходное изображение.

Необходимо отметить, что для одного и того же потока видеоданных при каждом новом преобразовании формируется различный префикс (данного результата можно добиться и для каждого нового кадра в потоке), в виду того, что каждый раз разбиение исходной битовой последовательности на части осуществляется произвольным образом, следовательно, выполняется преобразование с так называемой изменяющейся ключевой последовательностью [38].

Формируемый префикс, являющийся меньшей частью, гораздо меньше чем вся исходная битовая последовательность, соответствующая исходному изображению. Например, для изображения размером 352x288, приведённого на рисунке 2.10, а, исходная последовательность равна 2433024 бита, а полученный префикс, равен 41867 бит, что составляет 1,72 % от исходной битовой последовательности.

Даже, если будет раскрыта часть префикса (но не битовая последовательность A_1) и данные будут разделены на равные части, все равно не удастся восстановить исходное изображение, т.к. задача сводится к решению неопределенной системы из n уравнений с $n + 1$ неизвестными [36]:

$$\begin{cases} A_2 \oplus A_3 = X_1 \\ \dots\dots\dots \\ A_n \oplus A_1 = X_{n-1} \end{cases}$$

Восстановить изображение можно только подбором бит, но из Леммы 1, приведенной в [118], следует, что гарантированная на сегодняшний день стойкость, равная 2^{80} , будет обеспечиваться при длине записи A_1 большей или равной 64 битам. Тем самым, осуществить перебор в настоящее время практически невозможно.

Алгоритм восстановления изображения.

На рисунке 2.13 приведен алгоритм восстановления изображения, который состоит из следующих шагов [33, 37, 38].

Шаг 1. Анализируется количество первых l бит префикса равных нулю. После записи нулей в префиксе выбирается последовательность, состоящая из нулей и единиц равная по длине последовательности этих нулей, и выбранная последовательность переводится из двоичной системы счисления в десятичную и, тем самым, определяется количество битовых последовательностей A_i .

Шаг 2. Подсчитывается количество нулей, записанных после двоичной записи количества битовых последовательностей, и после записи этих нулей отсчитывается битовая последовательность, равная по количеству подсчитанных нулей. Полученная битовая последовательность равна двоичной записи размера M_1 битовой последовательности A_1 .

Шаг 3. Осуществляется аналогичная операция шагу 2 для всего количества битовых последовательностей A_i , определенных в шаге 1. Т.е. определяются размеры всех битовых последовательностей A_i .

Шаг 4. Из префикса изымается битовая последовательность A_1 .

Шаг 5. С учётом длин битовых последовательностей A_i решается система уравнений и находятся все A_i :

$$\begin{cases} A_2 \oplus A_3 = X_1 \\ \dots\dots\dots \\ A_n \oplus A_1 = X_{n-1} \end{cases}$$

Шаг 6. Битовые последовательности A_i записываются друг за другом и в соответствии с размером $W \times H$ преобразовываются десятичные значения цветовых составляющих пикселей в формате RGB.

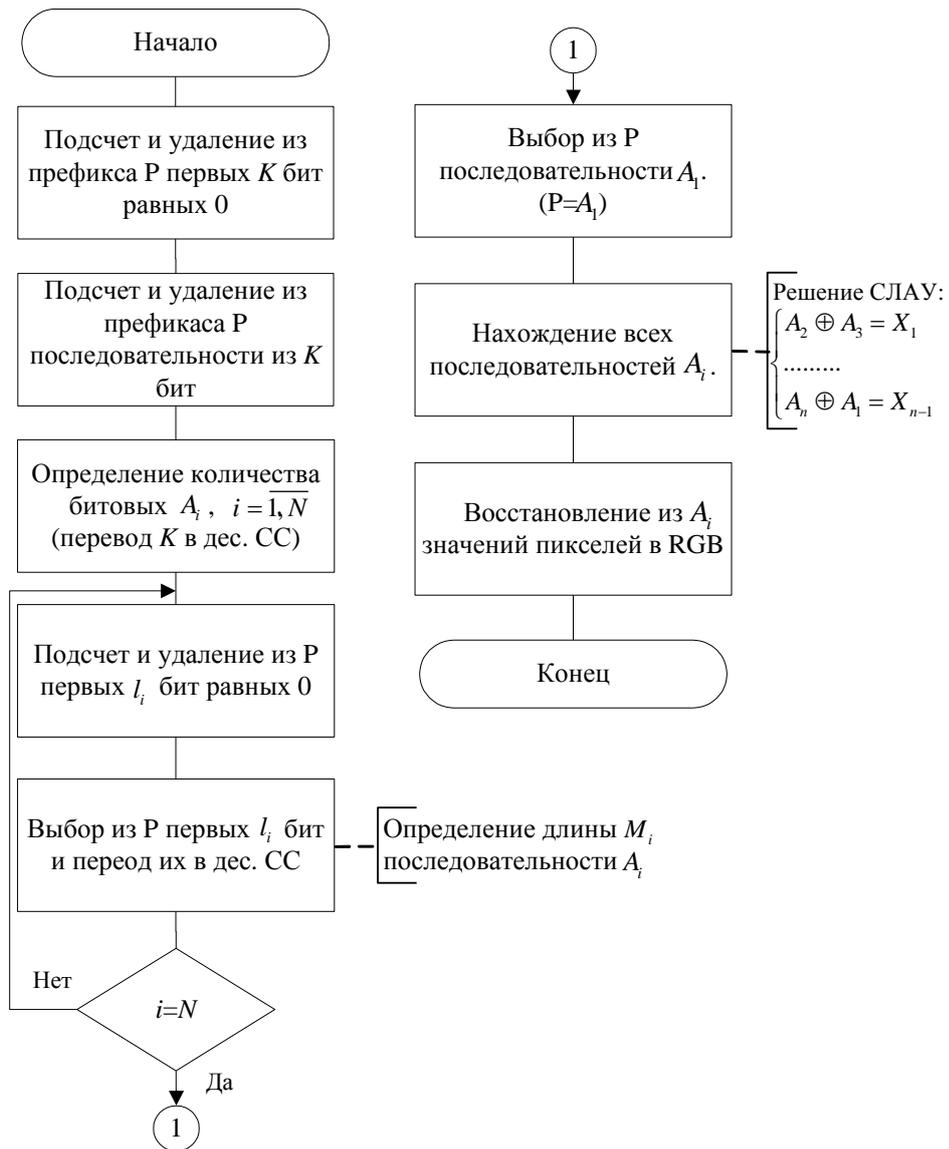


Рисунок 2.13 – Алгоритм восстановления изображения из частей, полученных с помощью префиксного кодирования

В приложении А2 приведен пример работы АРПК. Также в среде программирования C++ Builder (RAD Studio) для разработанного алгоритма выполнена программная реализация в виде модуля, который позволяет проводить эксперименты по разделению и объединению кадров видеоданных на части. Интерфейс модуля приведен на рисунке 2.14, получено свидетельство о государственной регистрации программ для ЭВМ № 2013661611 (Приложение Б). Для разработанного алгоритма в программной реализации осуществляется многопоточная обработка видеок кадров с использованием классов TThread.

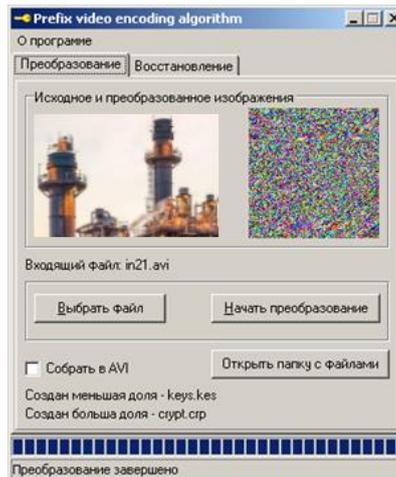


Рисунок 2.14 – Интерфейс программного модуля, реализующего АРПК

Стоит отметить, что поступающие на обработку потоки видеок кадров обрабатываются за разные промежутки времени, для синхронизации процесса обработки в программной реализации используются примитивы TMutex, TEvent и TSemaphore. С учётом разрешения входящих изображений и доступных вычислительных ресурсов, удалось обеспечить скорость обработки на уровне от 15 до 25 кадров в секунду.

2.3 Исследование возможности восстановления закодированных изображений

Для дальнейшей оценки эффективности разработанных алгоритмов разделения данных, предполагается, что попытки восстановления исходного изображения осуществляются по большей части. Определение возможности восстановления исходного состояний изображения относятся к теории цифровой обработки изображений, где под восстановлением подразумеваются действия, связанные с повышением визуального качества изображения. Однако, в отличие от улучшения, критерии которого субъективны, восстановление изображения является объективным в том смысле, что методы восстановления изображений опираются на математические или вероятностные модели искажений изображения. При восстановлении исходного состояния делается попытка реконструировать (воссоздать) изображение, которое было до этого искажено, используя априорную информацию о явлении, которое вызвало ухудшение изображения. Поэтому,

методы восстановления основаны на моделировании процессов искажения и применения обратных процедур для воссоздания исходного изображения [121].

Желательно при помощи обработки придать восстанавливаемому изображению такие качества, благодаря которым его восприятие человеком было бы по возможности комфортным. Важно восстановить особенности, нюансы изображения с целью улучшения его субъективного восприятия. Задача восстановления состоит в построении некоторого приближения $f'(x, y)$ к исходному изображению $f(x, y)$ по искажённому изображению $g(x, y)$, некоторой информации об искажающем операторе (искажающей функции $h(x, y)$, представляющей искажающий оператор) и некоторой информации относительно шума $\eta(x, y)$. Само искаженное изображение $g(x, y)$ может быть представлено в пространственной области в виде: $g(x, y) = h(x, y) * f(x, y) + \eta(x, y)$, где «*» – свертка. Если предположить, что искажающий оператор $h(x, y)$ является тождественным, то искажение изображений будет вызвано только наличием шумов $\eta(x, y)$: $g(x, y) = f(x, y) + \eta(x, y)$. Изображения подвержены воздействию различных шумов, которые могут появляться, например, при передаче по каналам связи [122, 123]. Для разработанных алгоритмов в результате попыток восстановления исходных изображений по большей части были получены искаженные изображения, где искажения по большей степени обусловлены наличием искажающей функции. Поэтому, необходимо выполнить оценку искажающей функции, которая полностью неизвестна, то процесс восстановления изображения осуществляется с использованием приближения искажающей функции. Такой процесс называется реконструкцией «вслепую». Только после удачной реконструкции исходного изображения в дальнейшем можно проводить фильтрацию шумов [121].

Существует три основных способа оценки искажающей функции (искажающего оператора): визуальный анализ, эксперимент и математическое моделирование.

Визуальный анализ. Пусть имеется искаженное изображение $g(x, y)$, но информация о функции $h(x, y)$, представляющей искажающий оператор,

отсутствует, тогда при визуальном анализе одним из способов оценить данную функцию является выделение информации непосредственно из самого искаженного изображения. Для того, чтобы уменьшить влияние искажений и шума для наблюдения, выбирается та область искаженного изображения, которая содержит полезный сигнал большой амплитуды. Используя яркости, контуры объекта и фона можно выполнить приблизительное построение изображения $f'_s(x, y)$ тех же размеров, что и рассматриваемая область $g_s(x, y)$. Тогда искажающая функция для выбранной области будет $h_s(x, y) = g_s(x, y) / f'_s(x, y)$. Исходя из свойств функции $h_s(x, y)$, можно сделать вывод о свойствах полной искажающей функции $h(x, y)$ для всего искаженного изображения [121].

Так как размер исходного изображения известен, а изображения, полученные при попытках восстановления по большей части в АРДЧ, растянуты в ширину (см. Рис. 2.2, б, 2.3, б). Следовательно, можно выполнить (геометрическое, пространственное) сжатие изображения по ширине, например, при помощи графического редактора или в среде Matlab [124]. На рисунке 2.15 приведены изображения, полученные в результате выполнения преобразований в среде Matlab.

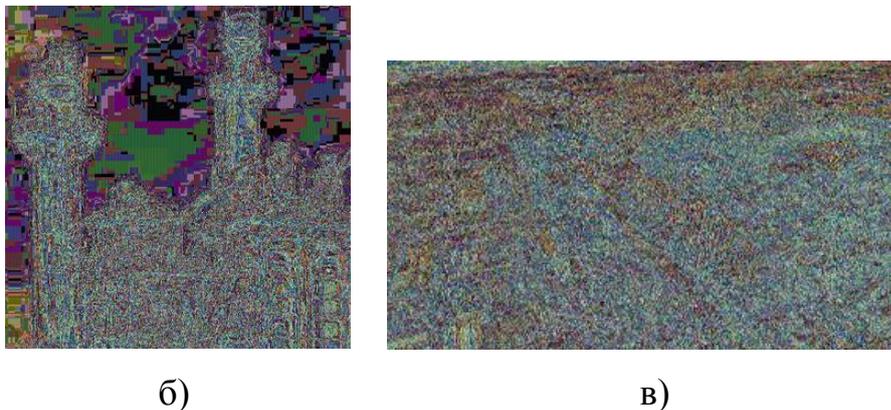


Рисунок 2.15 – Сжатие изображений по ширине а) сжатое изображение рисунка 2.2, б; б) сжатое изображение рисунка 2.3, б

Как видно из рисунка 2.15, что, выполнив сжатие изображения по ширине можно получить представление о некоторых контурах и границах цвета изображения. Но, не имея представления об исходном изображении, определение границ при помощи визуального анализа у каждого человека будет носить

индивидуальный характер, следовательно, для каждой оценки границ будет присутствовать человеческий фактор. Чтобы исключить человеческий фактор при определении границ, используются алгоритмы повышения резкости изображения, алгоритмы определения границ или алгоритмы слепой деконволюции для «угадывания» искажений [125–127]. Применение таких алгоритмов возможно при проведении оценки искажений с помощью экспериментов и моделирования.

Визуальный анализ изображений, приведённых на рисунке 2.15, позволяет сделать вывод, что АРДЧ более пригоден для цветных изображений, чем для чёрно-белых.

При визуальном анализе изображений, приведённых на рисунках 2.10, б; 2.11, б; 2.12, б, не удастся получить какую-либо информацию об исходном состоянии изображения. Возможно определить только цветность исходного изображения.

Оценка на основе эксперимента и моделирования. Идея оценки на основе эксперимента заключается в том, что, если существуют и доступны аналогичные методы или алгоритмы тем методам или алгоритмам, при помощи которых были получены искажённые изображения, то, не исключена возможность получения оценки искажающей функции. В таком случае выполняется подбор параметров в аналогичных методах или алгоритмах таким образом, чтобы искажения на получаемых искажённых экспериментальных изображениях были похожи на искажения на изображениях, которые подлежат восстановлению [121]. При оценке на основе эксперимента и моделирования возможны две ситуации. Первая ситуация – для оценки имеется возможность передавать для преобразования любые экспериментальные изображения и после преобразований для анализа известна только большая часть изображения. В таком случае, выполняя эксперименты по передаче для преобразований определенных экспериментальных изображений и впоследствии анализируя полученный результат (большую часть), можно оценить характер вносимых искажений в экспериментальные изображения. В случае совпадения искажений можно сделать предположение об исходном изображении. Вторая ситуация – имеется возможность передавать для преобразования любые экспериментальные изображения, и после преобразований для анализа известны обе части (большая и

меньшая). В таком случае основной задачей является анализ полученных частей, в частности меньших, для осуществления их подбора для исходных изображений.

Например, имеется экспериментальное изображение, рисунок 2.16, а, которое разделяется по АДЧ, в результате по большим частям (с учетом пространственного сжатия) получено изображение, приведенное на рисунке 2.16, б.

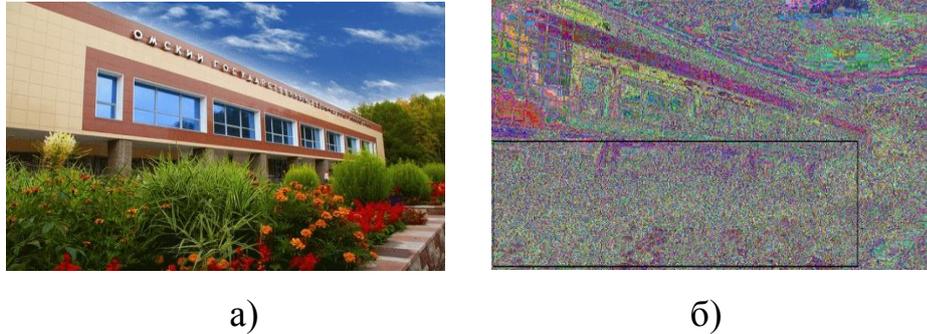


Рисунок 2.16 – Экспериментальное изображение: а) исходное; б) полученное при попытке восстановления.

Зная исходные изображения, можно оценить характер проявления границ на изображении, полученном при попытках восстановления по большей части. Для этого используются фильтры Кэнни и Собела, чтобы выделить границы на исходном изображении, которые затем наложить на изображения, полученные при попытках восстановления. Определение границ можно осуществить в среде Matlab.

Для экспериментального изображения, приведённого на рисунке 2.16, а, определены следующие границы: рисунок 2.17, а – границы, полученные с помощью фильтра Собела, рисунок 2.17, б – границы, полученные с помощью фильтра Кэнни.



Рисунок 2.17 – Анализ границ: а) границы, полученные с помощью фильтра Собела; б) границы, полученные с помощью фильтра Кэнни

Проводя эксперименты и анализируя набор изображений, полученный при проведении экспериментов, удастся смоделировать подходящую искажающую функцию, но только такую, при которой можно получить только общее представление об исходных изображениях, и лишь тех, в которых преобладают однотонные цвета. На рисунке 2.18 приведены восстановленные изображения с обведёнными границами, полученные при помощи фильтра Кэнни для исходных изображений.

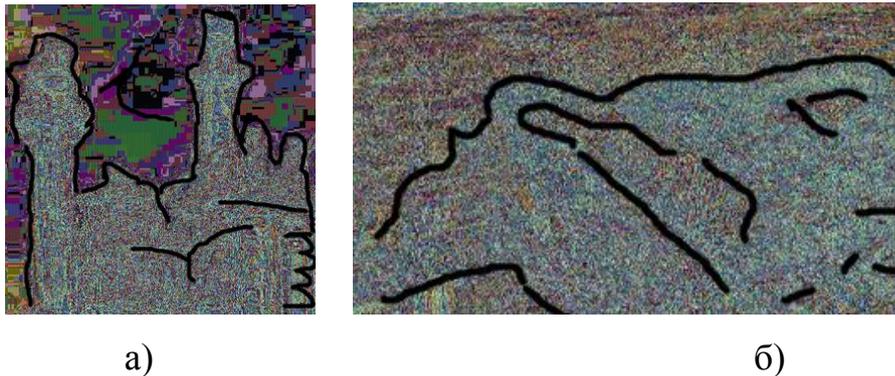


Рисунок 2.18 – Наложение границ, полученных с помощью фильтра Кэнни:
 а) границы для изображения на рисунке 2.2, б) границы для изображения на рисунке 2.3, б

При попытках восстановления экспериментальных изображений после преобразований по АРПК, имеется экспериментальное изображение (рис. 2.19, а) и изображения, полученные при попытках восстановления по большей части (рис. 2.19, б; рис. 2.19, в).

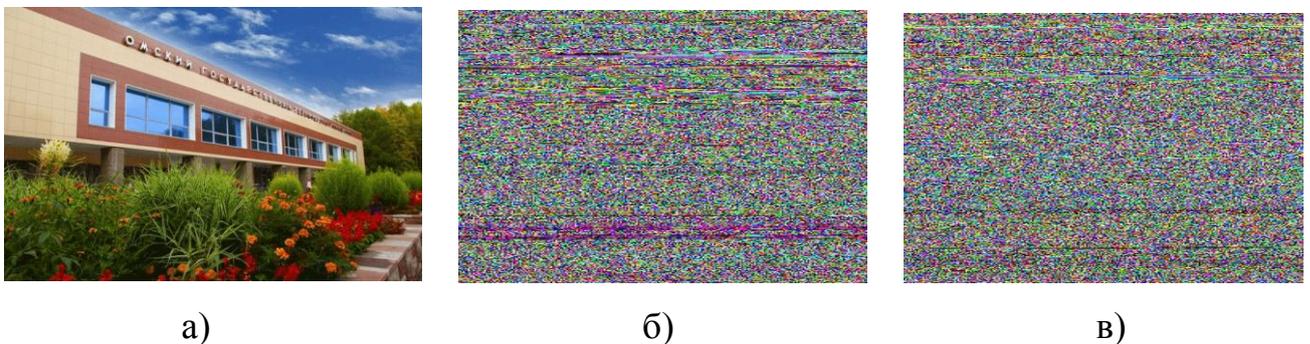


Рисунок 2.16 – Экспериментальное изображение: а) исходное;
 б) полученное при первой попытке восстановления; в) полученное при второй попытке восстановления

Выполняя анализ набора изображений, полученных при попытках восстановления по большим частям (рис. 2.19, б; рис. 2.19, в) в лучшем случае удастся сделать предположение только о цветности исходных изображений. Выполнить экспериментальную оценку искажений и моделирование искажающей функции представляется маловероятным, так как в предложенном алгоритме разбиение преобразуемой битовой последовательности осуществляется произвольным образом при помощи датчика псевдослучайных чисел и каждый раз для одного и того же потока видеоданных будут формироваться разные большие и меньшие части кадров.

Сравнение разработанных алгоритмов с подобными. Наиболее близкими к предложенным в данной диссертационной работе алгоритмам разделения изображений, являются алгоритмы разделения изображений на основе их цветовых и яркостных характеристик. В частности, в разделе 1.2 приведено описание алгоритма разделения изображения, с помощью построения геометрического объекта, формируемого при помощи цветовых характеристик исходного изображения на основе его RGB-представления [66, 70]. Данный алгоритм непригоден для однотонных изображений и для изображений с преобладаем какого-либо цвета. Также, полученные в результате разделения части (теневые изображения), обладают таким же размером что и исходное изображение.

В разработанных АДЧ и АРПК, разделение изображения также осуществляется на основе цветовых составляющих исходного изображения, улучшение заключается в том, что:

1) при разделении изображения основной акцент делается на размер меньшей части для организации распределенной передачи полученных частей через двухканальные системы связи с каналами, обладающими различными пропускными способностями. А также, что без меньшей части невозможно выполнить полное восстановление исходного изображения, в соответствии с анализом, приведенным в разделе 2.3.

2) АДЧ наиболее пригоден для многоцветных изображений, но в сравнении

с методами и алгоритмами, предложенными в [66, 70], после преобразований однотонных изображений или изображений с ярко выделенными границами даст лишь некоторое, а не полное представление об исходном конфиденциальном изображении. Тогда, в соответствии с методом, описанном в [66], при восстановлении можно воспользоваться интерполяцией недостающих пикселей и получить более полное представление об исходном изображении.

3) в АРПК, при попытках восстановления по большей части не удастся получить представление об исходном состоянии однотонных изображений и изображений с ярко выделенными границами.

Описанные в разделах 2.1 и 2.2 алгоритмы разделения изображений предлагается использовать для кодирования потока видеоданных и его последующей передачи в системах с двумя каналами связи. Предлагаемое улучшение заключается в возможности применения каналов с различной пропускной способностью: где по каналу с наименьшей пропускной способностью передается меньшая часть, а с большей пропускной способностью соответственно – большая. Здесь, с точки зрения системного подхода к решению задачи распределенной передачи данных, дополнительно требуется проработка вопроса оптимизации параметров используемой двухканальной системы связи. Это включает в себя выбор критериев распределения данных между каналами, учет характеристик каналов связи, а также разработку методов адаптации к возможным изменениям их пропускной способности в процессе передачи.

2.4 Выводы по главе

В результате проведенных исследований в данной главе сформулирована задача распределенной передачи видеокадров (изображений) через двухканальные системы связи с применением кодирующих алгоритмов, основанных на схемах разделения данных. Для решения данной задачи разработаны соответствующие алгоритмы, выполняющие разделение несжатых изображений на части разного размера.

1. Выполнено подробное описание разработанных алгоритмов разделения изображений на части неравного размера. Даны оценки возможности получения

представления об исходном изображении по полученным в результате разделения большим частям. Приведены примеры работы, приведено сравнение с аналогами.

2. Отмечено, что разработанные алгоритмы используют простые математические операции, и при их программной реализации преобразования изображений выполняются в отдельных потоках, что обеспечивает параллельную обработку без значительной нагрузки на центральный процессор. Такой параллелизм способствует быстрому разделению и восстановлению изображений даже в системах с ограниченными вычислительными ресурсами. Простота используемых математических операций позволяет обеспечить высокую стабильность и предсказуемость работы алгоритмов, что особенно важно для приложений, требующих обработки в реальном времени, таких как системы передачи видеоданных и видеонаблюдения.

3. Выявлено, что разработанные алгоритмы разделения изображений гарантируют, что по большей части (без доступа к меньшей) исходное изображение практически невозможно восстановить полностью. Кроме того, подбор нужной меньшей части для соответствующей большей сводится к трудоемкому перебору, требующему значительных временных затрат.

4. Разработанные программные модули позволили провести оценку размеров частей, полученных в результате применения предложенных алгоритмов разделения изображений. Экспериментальные исследования показали, что при использовании АРДЧ, меньшая часть, полученная в результате разделения, составляет в среднем 24% от общего объема исходного изображения, тогда как при применении АРПК – около 13%.

5. Определено, что при реализации многопоточной обработки видеок кадров с использованием в среде программирования C++ Builder (RAD Studio) классов TThread, с учётом разрешения видеок кадров и доступных вычислительных ресурсов, для АРДЧ удалось обеспечить обработку от 12 до 20 кадров в секунду, а для АРПК – от 15 до 25 кадров в секунду.

3 РАЗРАБОТКА МЕТОДИКИ АНАЛИТИЧЕСКОГО РАСЧЕТА ПРОПУСКНЫХ СПОСОБНОСТЕЙ КАНАЛОВ СВЯЗИ

В третьей главе описана методика аналитического расчета пропускных способностей каналов двухканальной системы связи. Приведены математическая модель системы; задача оптимизации пропускных способностей каналов связи, которая сводится к задаче минимизации средних издержек (материально-технических затрат), приходящихся на период эксплуатации системы. Получены расчетные формулы, позволяющие аналитическим путем определить минимально необходимые значения пропускных способностей каналов связи двухканальной системы в зависимости от характера входящего потока данных.

3.1 Постановка задачи оптимизации пропускных способностей каналов связи

Во второй главе данной диссертационной работы, а также в работах [33–38], предложены алгоритмы деления видеоданных на неравные части, которые позволят отправителю и получателю, используя два канала связи с разными пропускными способностями, осуществлять разнесение передаваемого TCP/IP трафика по этим каналам, как, например, это описано в работах [39–42]. При делении видеок кадров на неравные части, меньшая часть каждого кадра передается по каналу с меньшей пропускной способностью, а большая – по каналу с большей пропускной способностью. Такая передача данных от отправителя к получателю осуществляется на транспортном уровне семиуровневой сетевой модели OSI [128], где протоколом TCP обеспечивается гарантированная доставка данных.

При одновременном использовании двух каналов связи возникают вопросы, связанные с эффективностью использования вычислительных ресурсов, оптимизацией пропускных способностей каналов, синхронизацией передаваемых потоков, буферизацией. Эти вопросы можно решить с помощью соответствующих клиент-серверных приложений и оптимизации пропускных способностей каналов связи. Оптимизацию пропускных способностей целесообразно осуществлять по критериям минимизации издержек, одна часть которых связана с задержками в сети

(рост которых приводит к запаздыванию доставки данных к пользователю), другая часть – с оплатой, растущей с ростом пропускных способностей.

В качестве математической модели для оптимизации двухканальной системы связи предлагается СеМО с делением и слиянием заявок с двумя одноканальными СМО, в дальнейшем называемая «S-сетью» (рис. 3.1). В терминах теории массового обслуживания (ТМО) видеокадры обозначим как заявки, и их части – фрагменты заявок, демультиплексирование – разделением заявок, мультиплексирование – слиянием (ассемблированием) фрагментов заявок. Два фрагмента заявки, соответствующие двум частям одного и того же разделенного видеокадра, обозначим как сопряженные фрагменты. Дисциплина обслуживания очередей перед каналами определяется как дисциплина FIFO [129].

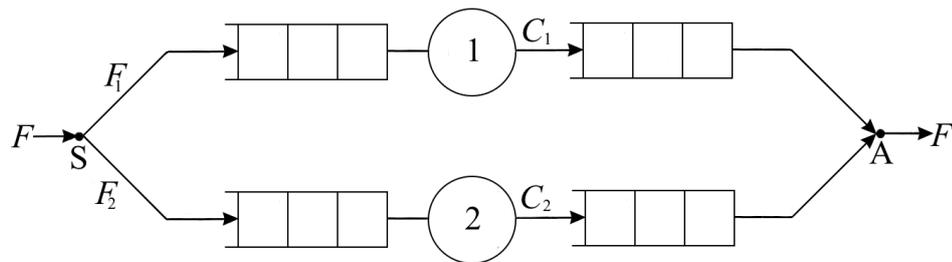


Рисунок 3.1 – СеМО с делением и слиянием заявок:

S – точка деления, A – точка слияния

Заявки передаются через два канала с разными пропускными способностями C_1 и C_2 , измеряемыми, например, в Кбит/с. В отличие от традиционных сетей в точке S заявка не переходит в одну из ветвей (СМО), а разделяется на два фрагмента, один из которых поступает в СМО-1, а другой – в СМО-2. В точке A происходит слияние двух сопряженных фрагментов в целую заявку. Соответственно, входящий в сеть трафик F (Кбит/с) делится на две части F_1 и F_2 , где $F_1 + F_2 = F$. Момент входа заявки в сеть является одновременно моментом ее разделения и моментом входа получаемых сопряженных фрагментов в каждую из двух ветвей сети (в каждую из двух одноканальных СМО). Следовательно, интенсивности λ , λ_1 и λ_2 потоков заявок, поступающих в сеть, и их фрагментов, поступающих в СМО-1 и в СМО-2 соответственно, одинаковы, и все три потока

заявок описываются одним и тем же вероятностным законом. Рассматриваемая сеть, являются сетью типа fork-join [129].

Перед точкой А формируются еще две очереди – очереди синхронизации. Фрагменты в момент выхода из СМО-1 (СМО-2) попадают перед точкой А в первую (во вторую) очередь синхронизации, в которой находится до момента обнаружения в соседней очереди синхронизации своего сопряженного фрагмента. Иначе говоря, тот из двух сопряженных фрагментов, который первый приходит к точке А, дожидается прихода второго сопряженного фрагмента и в момент его прихода они сливаются в покидающую сеть заявку, и передача заявки завершается.

В каждую очередь синхронизации все фрагменты заявок поступают в той же последовательности, в которой входят исходные неразделенные заявки в сеть. Поэтому, если в одной очереди синхронизации в состоянии ожидания находится хотя бы один фрагмент заявки, то другая очередь синхронизации пустая. На любом конечном интервале времени либо первая очередь синхронизации пустая, либо вторая, либо обе очереди пустые. Непустыми обе эти очереди одновременно могут быть только в течение одного момента времени – момента, когда становится истинным условие «в точке слияния имеется пара сопряженных друг с другом фрагментов заявок». Отсюда вытекает также, что из двух сопряженных фрагментов тот, который приходит позже, не задерживается в очереди синхронизации. И, следовательно, время u передачи видеокadra (в терминах ТМО – время пребывания заявки в сети, т.е. время, проходящее от момента прихода заявки в точку S до момента ее ухода из точки А) определяется формулой [130]:

$$u = \max(u_1, u_2), \quad (3.1)$$

где u_1 – время пребывания фрагмента заявки в СМО-1:

$$u_1 = w_1 + x_1, \quad (3.2)$$

u_2 – время пребывания сопряженного с ним фрагмента заявки в СМО-2:

$$u_2 = w_2 + x_2, \quad (3.3)$$

w_1 – время ожидания фрагмента в очереди 1,

x_1 – время обслуживания фрагмента в канале 1,

w_2 – время ожидания сопряженной фрагмента в очереди 2,

x_2 – время обслуживания сопряженной фрагмента в канале 2.

Среднее время U пребывания заявки в S-сети, согласно (3.1), выражается формулой:

$$U = M[\max(u_1, u_2)] = M[\max(w_1 + x_1, w_2 + x_2)]. \quad (3.4)$$

Время U зависит от пропускных способностей C_1, C_2 :

$$U = U(C_1, C_2).$$

Пусть цена пропускной способности любого канала в расчете на время эксплуатации сети составляет m у.е./(Кбит/с). Тогда задача оптимизации пропускных способностей C_1, C_2 каналов S-сети (или, другими словами, задача оптимизации S-сети) может быть сформулирована так:

$$f = lU(C_1, C_2) + mC_1 + mC_2 \rightarrow \min_{C_1, C_2}, \quad (3.5)$$

$$\begin{cases} C_1 \geq F_1 \\ C_2 \geq F_2, \end{cases} \quad (3.6)$$

где $U(C_1, C_2) = M[\max(u_1, u_2)]$,

l (у.е./с) – цена средней задержки заявки в сети на одну секунду.

Стоимостный коэффициент l равен потерям (происходящим из-за ожидания заявок), рассчитанным на период эксплуатации сети.

Таким образом, задача (3.5), (3.6) ставится как задача минимизации средних издержек, приходящихся на период эксплуатации сети. Сеть с оптимальными пропускными способностями каналов будет называться «оптимальной». Для решения этой задачи, с учетом имеющихся предположений о входящем потоке заявок, способах их деления и исследований сетей fork-jon, необходимо разработать соответствующие точные или приближенные способы расчета параметров [129, 130].

3.2 Исследование системы с независимыми каналами связи

В качестве математической модели для исследования системы связи с двумя независимыми ветвями, рассматривается СеМО с двумя независимыми одноканальными СМО (рис. 3.2), которую имеет смысл исследовать как упрощенное первое приближение S-сети, изображенной на рисунке 3.1.

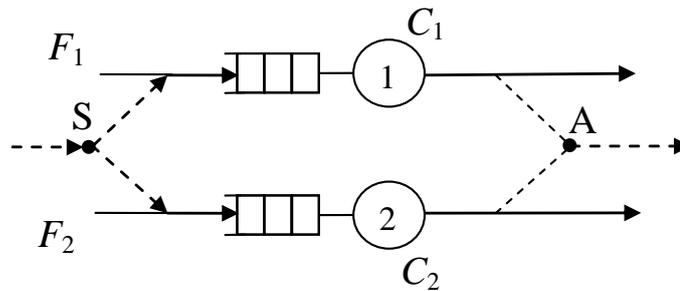


Рисунок 3.2 – СеМО с независимыми ветвями

В данной сети с независимыми ветвями СМО-1 и СМО-2 функционируют независимо, обслуживая каждая свой поток заявок. Каждая из этих СМО в отдельности эквивалентна соответствующей СМО в S-сети, но пара СМО в сети с независимыми ветвями (рис. 3.2) не эквивалентна паре СМО в S-сети (рис. 3.1). В сети на рисунке 3.2 СМО функционируют независимо, в S-сети процессы в одной и другой СМО статистически зависимы. Статистическая независимость ветвей сети на рисунке 3.2 упрощает ее анализ. Если потоки заявок в такой сети экспоненциальные, и время обслуживания заявок также имеет экспоненциальное распределение, то задачу оптимизации сети решается аналитически [129, 131].

Пунктиром на рисунке 3.2 изображено однократное прохождение через сеть единственной разделяемой заявки, поступающей в стационарном режиме функционирования сети в случайный момент времени (либо можно считать, что поступает поток фрагментов (разделяемых заявок), но отношение его интенсивности к интенсивности каждого из неразделенных потоков заявок сходится к нулю). Сопряженные фрагменты заявки в момент их прихода поступают в соответствующие СМО, затем проходят очереди и обслуживание и ассемблируются в одну заявку, так, как это описано выше. Время прохождения

разделяемой заявки через сеть выражается формулой (3.1), задача оптимизации такой сети ставится в форме (3.5), (3.6). Для того, чтобы решить эту задачу аналитически, необходимо выразить $M[\max(u_1, u_2)]$ через пропускные способности C_1, C_2 каналов.

Вначале находятся функция распределения времени пребывания неразделенных заявок в СМО-1 СМО-2. Поскольку эти СМО экспоненциальные, то нужные функции распределения известны. Поскольку величины u_1 и u_2 независимы, то можно найти распределение максимума этих величин. А через него – искомое $M[\max(u_1, u_2)]$.

Функция распределения времени пребывания в СМО-1 имеет вид [129, 132]:

$$P(u_1 \leq t) = 1 - e^{-\mu_1(1-\rho_1)t}, \quad (3.7)$$

аналогично в СМО-2 она описывается в виде

$$P(u_2 \leq t) = 1 - e^{-\mu_2(1-\rho_2)t}, \quad (3.8)$$

где μ_1, μ_2 – интенсивности обслуживания в первом и, соответственно, втором канале, ρ_1, ρ_2 – коэффициенты загрузки первого и второго каналов.

Функция распределения $\max(u_1, u_2)$ находится как вероятность одновременного наступления двух независимых событий: как вероятность того, что первая величина не превосходит t , и что вторая величина не превосходит t :

$$P[\max(u_1, u_2) \leq t] = [1 - e^{-\mu_1(1-\rho_1)t}] [1 - e^{-\mu_2(1-\rho_2)t}]. \quad (3.9)$$

Используя известную расчетную формулу для математического ожидания положительной случайной величины. (без расчета плотности вероятностей) находится:

$$M[\max(u_1, u_2)] = \int_0^{\infty} 1 - [1 - e^{-\mu_1(1-\rho_1)t}] [1 - e^{-\mu_2(1-\rho_2)t}] dt = \quad (3.10)$$

$$\frac{1}{\mu_1(1-\rho_1)} + \frac{1}{\mu_2(1-\rho_2)} - \frac{1}{\mu_1(1-\rho_1) + \mu_2(1-\rho_2)}.$$

Полученное выражение можно подставить в задачу (3.5), (3.6), чтобы решить ее для сети с независимыми ветвями. Для этого выражение (3.10) необходимо

привести к параметрам, используемым в задаче (5), (6): $\rho_1 = F_1/C_1$, $\rho_2 = F_2/C_2$, $\mu_1 = C_1/H_1$, $\mu_2 = C_2/H_2$. Переходя к этим обозначениям в выражении (3.10) и подставляя его в задачу (3.5), (3.6), получаем [129, 133]:

$$f = \frac{lH_1}{(C_1 - F_1)} + \frac{lH_2}{(C_2 - F_2)} - \frac{l}{H_1^{-1}(C_1 - F_1) + H_2^{-1}(C_2 - F_2)} + mC_1 + mC_2 \rightarrow \min_{C_1, C_2}, \quad (3.11)$$

$$\begin{cases} C_1 \geq F_1 \\ C_2 \geq F_2 \end{cases} \quad (3.12)$$

Точка (C_1, C_2) локального минимума этой положительной функции может быть найдена из системы уравнений:

$$\begin{aligned} \frac{\partial f}{\partial C_1} &= 0, \\ \frac{\partial f}{\partial C_2} &= 0. \end{aligned}$$

т.е из уравнений

$$-\frac{lH_1}{(C_1 - F_1)^2} + \frac{lH_1^{-1}}{(H_1^{-1}(C_1 - F_1) + H_2^{-1}(C_2 - F_2))^2} + m = 0, \quad (3.13)$$

$$-\frac{lH_2}{(C_2 - F_2)^2} + \frac{lH_2^{-1}}{(H_1^{-1}(C_1 - F_1) + H_2^{-1}(C_2 - F_2))^2} + m = 0. \quad (3.14)$$

Обозначив $C_1 - F_1$ через x , $C_2 - F_2$ – через y . В результате система (3.13), (3.14) примет вид, хорошо решаемый численными методами:

$$-\frac{lH_1}{x^2} + \frac{lH_1^{-1}}{(H_1^{-1}x + H_2^{-1}y)^2} + m = 0, \quad (3.15)$$

$$-\frac{lH_2}{y^2} + \frac{lH_2^{-1}}{(H_1^{-1}x + H_2^{-1}y)^2} + m = 0. \quad (3.16)$$

Пример 1. Пусть стоимостные коэффициенты $l = 1$, $m = 0,001$ и параметры $H_1 = 100$, $H_2 = 800$, $F_1 = 700$, $F_2 = 5600$. В этом случае система (3.15), (3.16) имеет 4

вещественных корней, из них два положительных: $x \approx 230,461$, $y \approx 848,818$. Соответственно, минимум целевой функции (3.11) достигается в точке $C_1 = F_1 + x \approx 930,461$, $C_2 = F_2 + y \approx 6448,818$. Расчет целевой функции по формуле (3.11) в этой точке дает при указанных параметрах сети значение $f = 8,458558$ у.е. При небольшом увеличении или уменьшении рассчитанных оптимальных C_1 , C_2 значения целевой функции (3.11) возрастают.

Вывод 1. Рассмотрен способ оптимизации каналов, который на практике можно использовать в случае, когда разделяемые данные составляют малую часть общего трафика, проходящего через два канала системы связи.

Имитационное моделирование сети с независимыми СМО (рис. 3.2) показывает, что, когда относительная интенсивность потока разделяемых заявок возрастает, процессы в СМО начинают сильно коррелировать, а в очередях синхронизации фрагменты заявок начинают проводить время, сравнимое с временем передачи фрагментов заявок по каналам вместе с очередями к каналам. Это затрудняет аналитическое исследование таких S-сетей.

Один из основных подходов, позволяющих сократить время задержки сопряженных фрагментов в очередях синхронизации состоит во введении максимальной положительной корреляции между процессами перемещения сопряженных фрагментов по соответствующим им СМО. Этот подход исследуется в следующих разделах данной главы диссертационной работы [129, 131].

3.3 Оптимизация двухканальной системы связи с разделением видеокадров в постоянном соотношении и их синхронной передачей

В качестве математической модели для исследования двухканальной системы связи с синхронной передачей разделенных видеокадров рассматривается СеМО с делением заявок в постоянном соотношении и со связанными в постоянном соотношении пропускными способностями каналов (т.е. $h_2/h_1 = \gamma = \text{const}$, $C_2 = \gamma C_1$).

Основные положения.

Рассмотрим S-сеть, каждая входящая в которую заявка имеет случайный размер h (Кбит) и разделяется на два сопряженных фрагмента так, что между их

размерами h_1 и h_2 (где $h_1 + h_2 = h$) всегда сохраняется одна и та же пропорция:

$$h_2/h_1 = \gamma = \text{const.} \quad (3.17)$$

Если при этом пропускные способности каналов связать условием:

$$C_2 = \gamma C_1, \quad (3.18)$$

то время x_1 обслуживания фрагмента заявки в канале 1 и время x_2 обслуживания сопряженного с ним фрагмента заявки в канале 2 совпадут:

$$\begin{aligned} x_1 &= h_1/C_1, \\ x_2 &= h_2/C_2 = (\gamma h_1)/(\gamma C_1) = h_1/C_1 = x_1. \end{aligned} \quad (3.19)$$

Поскольку равенство (3.19) выполняется для каждой пары сопряженных фрагментов, то в каждой паре оба сопряженных фрагмента попадают в очереди к каналам, в каналы и в точку сборки одновременно [129, 134].

Определение. Сеть с разделением заявок в постоянном соотношении и со связанными в постоянном соотношении пропускными способностями каналов связи назовем S-сетью с синхронными каналами, или «Ss-сетью» [129].

Видно, что в Ss-сети из $C_2 = \gamma C_1$ вытекает $C = (1 + \gamma)C_1$, где $C = C_1 + C_2$ – суммарная пропускная способность каналов. Аналогично, из $h_2/h_1 = \gamma$ следует, что входящий во второй канал трафик F_2 и весь входящий в сеть трафик F выражаются через F_1 соотношениями $F_2 = \gamma F_1$, $F = (1 + \gamma)F_1$.

Задача оптимизации Ss-сети. Задачу (3.5), (3.6) оптимизации S-сети, данные в которой передаются синхронно, можно решить точно при любых потоках заявок.

Действительно, поскольку в Ss-сети время u_1 пребывания любого фрагмента заявки в СМО-1 и время u_2 пребывания соответствующего сопряженного фрагмента заявки в СМО-2 совпадают, то в (3.1) имеем $u = \max(u_1, u_2) = u_1$, и, следовательно, в (3.4) $U = M[\max(u_1, u_2)] = M[u_1] = U_1$, где U_1 – среднее время пребывания фрагмента заявки в СМО-1. Выполняя в задаче (3.5), (3.6) подстановки $U(C_1, C_2) = U_1(C_1)$, $C_2 = \gamma C_1$ и $F_2 = \gamma F_1$, получена эквивалентная формулировка с использованием только одного варьируемого параметра C_1 :

$$f = lU_1(C_1) + m(1 + \gamma)C_1 \rightarrow \min_{C_1}, \quad (3.20)$$

$$C_1 \geq F_1. \quad (3.21)$$

Заметим, что после выполнения этих подстановок второе ограничение в (3.6) становится эквивалентным первому и поэтому в ограничениях (3.21) отсутствует.

Решение задачи (3.20), (3.21) оптимизации Ss-сети определяет оптимальную пропускную способность C_1 первого канала и, одновременно, соответствующие пропускные способности $C_2 = \gamma C_1$ и $C = (1 + \gamma)C_1$. Для разработки общего подхода к оптимизации Ss-сетей целесообразно рассмотреть особенности оптимизации задачи (3.20), (3.21) на нескольких конкретных примерах.

Ss-сеть с регулярным входящим потоком и фиксированным размером заявок.

Оптимизация. При регулярном входящем потоке время τ между приходами заявок в сеть (и, следовательно, в каждый из двух ветвей) постоянно: $\tau = \text{const}$. Размер фрагментов заявок, поступающих в СМО-1, также фиксирован ($h_1 = \text{const}$), поэтому в СМО-1 фиксировано и время $x_1 = h_1/C_1$ обслуживания. Из ограничения $C_1 \geq F_1$ следует, что $x_1 \leq \tau$, т.е. каждый фрагмент, поступающий в СМО-1, обслуживается раньше, чем поступает следующий. Поэтому очередь перед каналом 1 не формируется, и среднее время пребывания фрагмента в СМО-1 $U_1 = x_1 = h_1/C_1$. Подставляя это выражение для U_1 в (3.20), (3.21) вместо $U_1(C_1)$, получаем задачу [129–131]:

$$f = l \frac{h_1}{C_1} + m(1 + \gamma)C_1 \rightarrow \min_{C_1}, \quad (3.22)$$

$$C_1 \geq F_1, \quad (3.23)$$

решение которой сводится к решению алгебраического уравнения:

$$\frac{df(C_1)}{dC_1} = 0 \quad \text{или} \quad -l \frac{h_1}{C_1^2} + m(1 + \gamma) = 0,$$

определяющего точку локального минимума целевой функции f :

$$C_1 = \sqrt{\frac{lh_1}{m(1 + \gamma)}}. \quad (3.24)$$

Если полученное значение C_1 удовлетворяет ограничению $C_1 \geq F_1$, то (3.24) является решением задачи (3.22), (3.23). Иначе решением является наименьшее ближайшее к точке (3.24) значение C_1 , удовлетворяющее ограничению $C_1 \geq F_1$, т.е. значение $C_1 = F_1$ [129, 133].

Пример 2. При $l = 1, h_1 = 100, h_2 = 800, \gamma = h_2/h_1 = 8, F_1 = 700, F_2 = \gamma F_1 = 5600, m = 0,001$ локальный минимум функции (3.22) достигается в точке $C_1 = 105,409 < F_1$. Поэтому оптимальным является значение $C_1 = F_1 = 700$. При этом коэффициент загрузки первого канала $\rho_1 = F_1/C_1 = 1$ (канал не простаивает). Оптимальное значение $C_2 = \gamma C_1 = \gamma F_1 = 5600$. Из синхронности процессов в двух каналах сети вытекает, что и $\rho_2 = 1$, т.е. и второй канал загружается по максимуму. Очереди к каналам отсутствуют. И средние издержки (3.22) при оптимальном значении C_1 , составляют 6,443 у.е [129].

Оптимальное решение задачи (3.22), (3.23) найдено на границе области (3.23) в связи с тем, что точка локального (и глобального) минимума (3.24) оказалась левее наименьшего допустимого решения $C_1 = F_1$. Из (3.24) видно, что это произошло вследствие достаточно малой цены l задержки сообщений и/или достаточно высокой цены m единицы пропускной способности.

Пример 3. Если при числовых параметрах, заданных в примере 1, снизить цену m , например, на два порядка, то координата C_1 локального минимума (3.24) увеличится на порядок и достигнет величины 1054,09, удовлетворяющей ограничению $C_1 \geq F_1 = 700$. Следовательно, это значение C_1 станет решением задачи (3.22), (3.23). При этом коэффициенты загрузки каналов $\rho_1 = \rho_2 = F_1/C_1 = F_2/C_2 \approx 0,66$, а издержки (3.22) на передачу одного сообщения снизятся с 6,443 у.е., полученных в примере 1, до 0,1897 у.е [129].

Пример 4. Пусть отношение размеров заявок (частей кадров потока видеоданных, полученных в результате применения алгоритмов, основанных на схемах разделения данных) составляет $h_2/h_1 = \gamma = const = 11,2$, где $h_1 = 0,0040$ Мбит, $h_2 = 0,0448$ Мбит. Объём информации передаваемый за единицу времени по каналу 1 и каналу 2, соответственно составляет $F_1 = 0,179$ Мбит/с, $F_2 = 2,021$ Мбит/с.

Подставляя в формулу (3.24) значения γ , h_1 и учитывая, что издержки составляют, например, $m = 0,01$ у.е./(Мбит/с) и в канале связи отсутствует ожидание поступления заявок ($l = 1$ у.е./с), то получим $C_1 = 0,181$ Мбит/с и $C_2 = 2,027$ Мбит/с ($C_1 > F_1$ и $C_2 > F_2$). Средние издержки на содержание системы связи по формуле (3.22) составляют $f = 0,0442$ у.е.

Сравнение с одноканальной версией. Двухканальная передача видеок кадров повышает эффективность передачи, а также, как определено в главе 2, повышает конфиденциальность их передачи. Чтобы оценить потери, за счет которых это достигается, необходимо сравнить издержки, получаемые в оптимальной Ss-сети, с издержками, характеризующими соответствующую базовую (одноканальную, рис. 3.3) оптимальную систему [129–131].

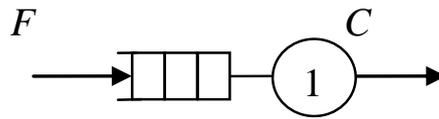


Рисунок 3.3 – Базовая одноканальная СМО

В рассматриваемом случае регулярного входящего потока и фиксированного размера заявок среднее время U передачи видеок кадра по одному каналу при $C \geq F$ равно среднему времени обслуживания заявки (поскольку очередь перед каналом не возникает). Т.е. $U = h/C$, где $h = h_1 + h_2 = \text{const}$ – размер заявок. Поэтому задача оптимизации базовой одноканальной системы принимает вид

$$f = lh / C + mC \rightarrow \min_c, \quad (3.25)$$

$$C \geq F. \quad (3.26)$$

Локальный минимум целевой функции (3.25) достигается в точке:

$$C = \sqrt{\frac{lh}{m}}. \quad (3.27)$$

При числовых параметрах, заданных в примере 2, точка локального минимума

(3.27) равная $C = \sqrt{l \cdot (h_1 + h_2) / m} \approx 948,7$ не удовлетворяет ограничению $C \geq F$, (где $F = F_1 + F_2 = 6300$) поэтому оптимальным является решение $C = F = 6300$, при котором потери (3.25) $f(C) \approx 6,443$ у.е. Сравнивая их с потерями в оптимизированной Ss-сети (см. пример 2), видно, что они точно такие же. Таким образом, в приведенном численном примере повышение конфиденциальности видеоданных за счет их разделения и передачи по разным каналам связи достигается без повышения издержек.

К такому же заключению приводит сравнение использования двухканальной системы и одноканальной в условиях примера 3, т.е. при снижении цены m на два порядка. Тогда точкой локального минимума издержек (3.27) одноканальной системы становится значение $C = 9486,8$, которое удовлетворяет ограничению (3.26) и, следовательно, становится решением задачи (3.25), (3.26). При таком C издержки (3.25) одноканальной системы равны 0,1897 у.е. – вновь точно такие же, как при использовании соответствующей двухканальной Ss-сети (см. пример 3). И в этом примере повышение конфиденциальности не приводит к дополнительным издержкам.

Обнаруженное совпадение издержек вряд ли случайно. Выявляя его причины, сформулирована следующая обобщающая обнаруженные факты теорема [129].

Теорема 1. Передача регулярного потока заявок фиксированного размера через оптимальную Ss-сеть (оптимальную двухканальную систему с синхронной передачей данных) приводит к таким же издержкам, как его передача через оптимальную одноканальную систему. При этом суммарная пропускная способность оптимальной Ss-сети (оптимальной двухканальной системы с синхронной передачей данных) равна пропускной способности оптимальной одноканальной системы [129, 131].

Доказательство. Для доказательства теоремы достаточно заметить, что постановка задачи (3.22), (3.23) оптимизации Ss-сети отличается от постановки задачи (3.25), (3.26) оптимизации одноканальной системы только вследствие формулировки задачи (3.22), (3.23) в терминах оптимального выбора пропускной способности C_1 . Но поскольку в Ss-сети любым из C_1 , C_2 и C однозначно

определяются два других, то задачу ее оптимизации можно сформулировать в терминах оптимального выбора любого из этих трех параметров. При выборе в качестве варьируемого параметра переменной C – суммарной пропускной способности каналов – постановка задачи оптимизации Ss-сети становится эквивалентной постановке задачи оптимизации одноканальной системы.

Действительно, в задаче (3.22), (3.23) $C_1 = C/(1 + \gamma)$, $F_1 = F/(1 + \gamma)$ и $h_1 = h/(1 + \gamma)$. Выполнив в задаче (3.22), (3.23) соответствующие замены, получена формулировка

$$f = l \frac{h/(1 + \gamma)}{C/(1 + \gamma)} + m(1 + \gamma)C/(1 + \gamma) \rightarrow \min_c \Leftrightarrow f = l \frac{h}{C} + mC \rightarrow \min_c ,$$

$$C/(1 + \gamma) \geq F/(1 + \gamma) \qquad C \geq F$$

эквивалентная формулировке задачи (3.25), (3.26). Таким образом, из эквивалентности формулировок двух рассматриваемых содержательно разных задач вытекает численное совпадение их решений. Теорема доказана.

Следовательно, можно сделать вывод, т.к. рассматриваемые две задачи являются задачами оптимизации двух разных систем – Ss-сети и одноканальной системы. Формальное совпадение их решений означает, что передача регулярного входящего потока с фиксированным размером заявок через оптимальную Ss-сеть приводит к точно таким же издержкам, как его передача через оптимальную одноканальную систему [129, 131].

Ss-сеть с произвольным входящим потоком заявок.

Теорему 1 обобщает следующая теорема (как следствие).

Теорема 2. Передача любого потока заявок через оптимальную Ss-сеть (оптимальную двухканальную систему с синхронной передачей данных) приводит к таким же издержкам, как его передача через оптимальную одноканальную систему. При этом суммарная пропускная способность оптимальной Ss-сети (оптимальной двухканальной системы с синхронной передачей данных) равна пропускной способности оптимальной одноканальной системы [129, 131].

Доказательство теоремы основано на сопоставлении процессов прохождения через Ss-сеть и через одноканальную систему одной и той же

реализации входящего потока заявок. Тогда при условии, что пропускная способность одноканальной системы равна пропускной способности Ss-сети продвижение фрагментов заявок в каждой ветви Ss-сети происходит синхронно с продвижением заявок в одноканальной системе. Из этого вытекает:

- эквивалентность задачи оптимизации сети и задачи оптимизации одноканальной системы (в том числе и при независимом их рассмотрении, т.е. при подаче на вход сети и на вход одноканальной системы независимых реализаций одного и того же потока заявок),
- совпадение суммарной пропускной способности каналов оптимальной сети с пропускной способностью оптимальной одноканальной системы,
- совпадение издержек, рассчитанных на период эксплуатации оптимальной Ss-сети и издержек оптимальной одноканальной системы за такой же период.

Проиллюстрировать теорему 2 можно на примере экспоненциальной Ss-сети, рассматриваемой в следующем примере [129, 131].

Пример оптимизации экспоненциальной Ss-сети.

Определение. Ss-сеть называется экспоненциальной, если в нее входит пуассоновский поток заявок, и размеры фрагментов заявок распределены по экспоненциальному закону. Соответственно, обе СМО в такой сети являются системами M/M/1. Их расчет выполняется по известным формулам [132].

Оптимизация Ss-сети. Среднее время U_1 пребывания в СМО-1 экспоненциальной Ss-сети составляет [132]:

$$U_1 = \frac{1/\mu_1}{1-\rho_1} = \frac{1}{\mu_1 - \lambda_1} = \frac{H_1}{H_1\mu_1 - H_1\lambda_1} = \frac{H_1}{C_1 - F_1}, \quad (28)$$

где μ_1 – интенсивность обслуживания заявок в СМО-1,

$\rho_1 = \lambda_1/\mu_1 = F_1/C_1$ – коэффициент загрузки СМО-1,

$H_1 = M(h_1)$ – средний размер заявок, поступающих в СМО-1.

Поэтому задача (3.20), (3.21) применительно к экспоненциальной Ss-сети конкретизируется следующим образом [130, 133]:

$$f = l \frac{H_1}{C_1 - F_1} + m(1 + \gamma)C_1 \rightarrow \min_{C_1}, \quad (3.29)$$

$$C_1 \geq F_1. \quad (3.30)$$

Единственный минимум целевой функции (3.29), определяемый из уравнения:

$$\frac{df}{dC_1} = -\frac{lH_1}{(C_1 - F_1)^2} + m(1 + \gamma) = 0 \quad (3.31)$$

достигается в точке:

$$C_1 = F_1 + \sqrt{\frac{lH_1}{m(1 + \gamma)}} \quad (3.32)$$

и является решением задачи (3.29, 3.30), так как удовлетворяет ограничению (30).

Подставляя пропускную способность (3.32) в выражение целевой функции (3.29), находятся издержки применения оптимальной экспоненциальной Ss-сети:

$$f = l \frac{H_1}{\sqrt{\frac{lH_1}{m(1 + \gamma)}}} + m(1 + \gamma) \sqrt{\frac{lH_1}{m(1 + \gamma)}} = 2\sqrt{(1 + \gamma)mlH_1}. \quad (3.33)$$

Оптимизация одноканальной экспоненциальной системы.

Поток заявок, входящий в рассмотренную экспоненциальную Ss-сеть, имеет интенсивность $\lambda = F/H = F_1/H_1$ и средний размер заявок $H = (1 + \gamma)H_1$. При передаче этого потока через одноканальную систему среднее время передачи заявки составляет

$U = \frac{1/\mu}{1-\rho} = \frac{H}{C-F}$. Задача оптимизации такой одноканальной СМО имеет вид [129]:

$$f(C) = l \frac{H}{C - F} + mC \rightarrow \min_C, \quad (3.34)$$

$$C \geq F \quad (3.35)$$

и определяет пропускную способность:

$$C = F + \sqrt{\frac{lH}{m}}, \quad (3.36)$$

при которой средние суммарные издержки (3.33) минимальны и составляют:

$$f(C) = l \frac{H}{\sqrt{\frac{lH}{m}}} + m \left(F + \sqrt{\frac{lH}{m}} \right) = 2\sqrt{mlH} + mF. \quad (3.37)$$

Сравнение оптимальной экспоненциальной Ss-сети и соответствующей одноканальной СМО. Чтобы сравнить с решением (3.36) решение (3.32) задачи (3.29), (3.30) необходимо переписать решение (3.32) в терминах суммарной пропускной способности Ss-сети. Выполняя в (3.32) эквивалентные для всякой Ss-сети замены $C_1 = C/(1 + \gamma)$, $F_1 = F/(1 + \gamma)$, $H_1 = H/(1 + \gamma)$, получено выражение:

$$\frac{C}{1 + \gamma} = \frac{F}{1 + \gamma} + \sqrt{\frac{lH}{m(1 + \gamma)^2}}, \quad (3.38)$$

и, упрощая которое, находится суммарная пропускная способность оптимальной экспоненциальной Ss-сети:

$$C = F + \sqrt{\frac{lH}{m}},$$

совпадающую, с пропускной способностью (3.35) оптимальной одноканальной экспоненциальной СМО. Аналогично, выполнив в (3.33) эквивалентную для Ss-сетей замену $H_1 = H/(1 + \gamma)$, получено, что издержки, обусловленные применением оптимальной экспоненциальной Ss-сети совпадают с издержками, обусловленными применением оптимальной одноканальной экспоненциальной системы.

Таким образом, полученные в общем виде решения задачи оптимизации экспоненциальной Ss-сети и задачи оптимизации, соответствующей одноканальной экспоненциальной СМО подтверждают и иллюстрируют сформулированную выше теорему 2, доказанную для любого потока заявок, который может быть не рекуррентным, не стационарным, размеры заявок в нем могут быть зависимыми, не одинаково распределенными, и т.д. [129–131, 134].

3.4 Исследование пропускных способностей каналов при отсутствии синхронной передачи данных в двухканальной системе связи

Определение. В качестве математической модели для исследования двухканальной системы связи с разделением видеокадров в постоянном соотношении рассматривается СеМО с делением и слиянием заявок, в которой при разделении заявок для фрагментов выполняется условие $h_2/h_1 = \gamma = \text{const}$, но не накладывається условие $C_2 = \gamma C_1$. Такие сети назовем сетями с разделением заявок в равном отношении, или «Se-сетями» [129, 131].

Таким образом, рассмотренные выше Ss-сети – это подмножество Se-сетей, в котором выполняются оба условия (3.17), (3.18).

Задача оптимизация Se-сетей. Задача оптимизации Se-сетей имеет определенные особенности. Она записывается, как и общая задача (3.5), (3.6) оптимизации S-сетей, в виде:

$$f = lU(C_1, C_2) + mC_1 + mC_2 \rightarrow \min_{C_1, C_2}, \quad (3.39)$$

$$\begin{cases} C_1 \geq F_1 \\ C_2 \geq F_2, \end{cases} \quad (3.40)$$

(где $U(C_1, C_2) = M[\max(u_1, u_2)]$), и наследует то ее свойство (в отличие от сети с независимыми ветвями, см. рис. 3.2), что в общем случае в элементарных функциях не выражаемая зависимость математического ожидания $M[\max(u_1, u_2)]$ от варьируемых параметров C_1, C_2 здесь определена на стохастически взаимозависимых случайных величинах u_1, u_2 (временах пребывания в СМО-1 и СМО-2).

От задачи оптимизации Ss-сетей, варьируемые параметры C_1, C_2 в (3.39), (3.40) независимы, не связаны условием $C_2 = \gamma C_1$, поэтому в ограничениях (3.40) сохраняются оба неравенства. И поэтому же продвижение фрагментов заявок в ветвях сети в общем случае здесь асинхронно, что затрудняет нахождение явной формулы, точно выражающей время $U(C_1, C_2) = M[\max(u_1, u_2)]$ через параметры сети [129, 130].

Вместе с тем, найти точное решение задачи (3.39), (3.40) необходимо, это обусловлено следующими соображениями. Рассмотренная ранее задача (3.20),

(3.21) оптимизации Ss-сетей является задачей нахождения условного минимума целевой функции (3.39), так как связывает аргументы функции (3.39) дополнительным условием $C_2 = \gamma C_1$, т.е. ограничивает в системе координат $(C_1, 0, C_2)$ область поиска минимума f одномерным множеством точек прямой $C_2 = \gamma C_1$. И при решении задачи (20), (21) было найдено на этой прямой решение, не увеличивающее издержек по использованию распределенной по двум каналам передачи видеокадров по сравнению с одноканальной реализацией. И если в двухмерной области допустимых решений (ОДР) задачи (3.39), (3.40) единственная точка минимума целевой функции (3.39) находится вне прямой $C_2 = \gamma C_1$, то решение задачи (3.39), (3.40) будет лучшим, чем решение задачи (3.20), (3.21).

Содержательным смыслом такого решения будет являться обнаружение возможности перехода к распределённой передаче видеокадров через двухканальную систему связи не только без увеличения издержек (см. теорему 1), но и с попутным их снижением. Далее необходимо провести оценку возможности применения данного утверждения. Однако, далее устанавливается, что в классе Se-сетей такая возможность исключена – оптимальные решения задачи (3.39), (3.40) всегда лежат на прямой $C_2 = \gamma C_1$ [129–131, 133].

Se-сеть с регулярным входящим потоком и фиксированным размером заявок.

Теорема 3. Оптимальная для передачи регулярного потока заявок фиксированного размера Se-сеть является Ss-сетью, т.е. при передаче регулярного потока заявок фиксированного размера оптимальное решение задачи (3.39), (3.40) всегда лежит на прямой $C_2 = \gamma C_1$ [129, 131].

Доказательство. Учитывая определяющее Se-сети условие $h_2/h_1 = \gamma = \text{const}$, ОРД задачи (3.39), (3.40) может быть представлена в виде объединения двух областей R_1 и R_2 (рис. 3.4).

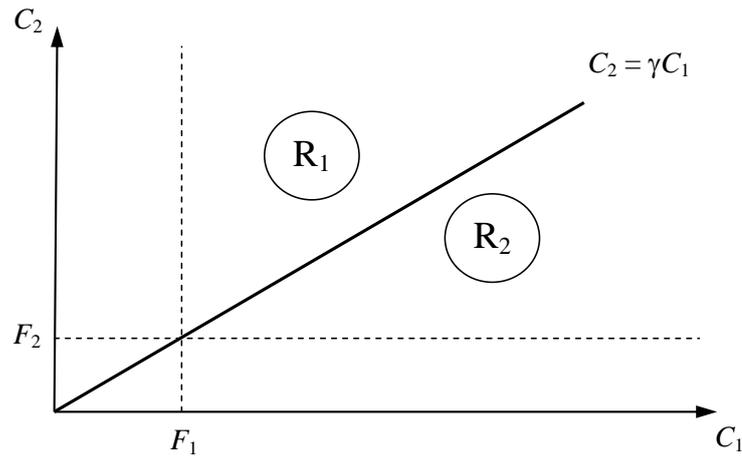


Рисунок 3.4 – Область допустимых решений задачи (3.39), (3.40)

Область R_1 определяется условиями $C_1 \geq F_1$, $C_2 \geq \gamma C_1$, область R_2 – условиями $C_2 \geq F_2$, $C_2 \leq \gamma C_1$. Прямая $C_2 = \gamma C_1$ при $C_1 \geq F_1$ принадлежит обеим областям. Точка (F_1, F_2) лежит на этой прямой, так как $F_2/F_1 = \lambda h_2/\lambda h_1 = \gamma$ (координаты точки удовлетворяют уравнению прямой). Всякая принадлежащая ОДР точка (C_1, C_2) определяет для СМО-1 время обслуживания в ней фрагментов заявок $x_1 \equiv b_1 = h_1/C_1 \leq h_1/F_1 = \tau_1$, т.е. постоянное время обслуживания фрагментов заявок в первой ветви сети не превосходит постоянного периода τ_1 поступления фрагментов в эту ветвь. Очереди к каналу в первой ветви не возникает, время u_1 пребывания фрагментов заявок в СМО-1 постоянно и равно h_1/C_1 . Аналогично находим, что очереди к каналу второй ветви не возникает и время u_2 пребывания фрагментов заявок в СМО-2 равно константе h_2/C_2 .

Используя методом доказательства от противного и можно предположить, что наименьшее значение целевой функции (3.39) достигается в точке $\bar{C} = (C_1, C_2)$, не лежащей на прямой $C_2 = \gamma C_1$. Тогда искомая точка лежит либо в области R_1 и выше этой прямой, либо в области R_2 и правее этой прямой.

В первом случае координаты точки \bar{C} , лежащей в ОДР и доставляющей наименьшее значение целевой функции, имеют вид $(C_1, C_2) = (C_1, \gamma C_1 + \varepsilon)$, где $\varepsilon > 0$. При этом периодический процесс обслуживания фрагментов заявок в СМО-1 характеризуется временем обслуживания $x_1 \equiv h_1/C_1$, в СМО-2 – временем обслуживания $x_2 \equiv h_2/C_2 = \gamma h_1/(\gamma C_1 + \varepsilon) = h_1/(C_1 + \varepsilon/\gamma) < x_1$. Каждая заявка в первой

ветви и сопряженная с нею заявка во второй ветви начинают обслуживаться в один и тот же момент времени. Заявка во второй ветви заканчивает обслуживаться раньше и ожидает завершения обслуживания сопряженной заявки, которая должна поступить из СМО-1. В результате время u пребывания заявки в сети (до момента сборки) становится равно $x_1 = h_1/C_1$. Но такое же время пребывания получено в точке $\bar{C}^* = (C_1, \gamma C_1)$, в которой $x_2 = x_1$. И, так как в точке \bar{C}^* при том же времени пребывания и той же пропускной способности C_1 пропускная способность C_2 ниже, чем в точке \bar{C} , получено что: $f(\bar{C}^*) < f(\bar{C})$ – см. (3.39). Полученное противоречие исключает возможность нахождения решения задачи (3.39), (3.40) в области R_1 вне прямой $C_2 = \gamma C_1$.

К аналогичному противоречию приводит предположение о возможности нахождения искомой точки минимума в области R_2 вне прямой $C_2 = \gamma C_1$.

Таким образом, решение задачи (3.39), (3.40) всегда лежит на прямой $C_2 = \gamma C_1$. При оптимальном выборе пропускных способностей рассматриваемая Se-сеть (с регулярным потоком заявок фиксированного размера) становится Ss-сетью. Оптимальные пропускные способности для которой найдены в разделе 3.3 данной диссертационной работы. Там же показано, что передача такого потока через оптимальную Ss-сеть приводит к точно таким же издержкам, как его передача через оптимальную одноканальную систему. Теперь соответствующий вывод распространяется и на оптимальные Se-сети [129–131, 133].

Se-сеть с произвольным входящим потоком заявок.

Теорема 4. Оптимальная для передачи любого потока заявок Se-сеть является Ss-сетью, т.е. оптимальные пропускные способности C_1, C_2 Se-сети лежат на прямой $C_2 = \gamma C_1$ [192, 131].

Доказательство теоремы основано на сопоставлении процессов прохождения заявок Se-сети через ее ветви и установлению факта, что если C_1, C_2 не связаны условием $C_2 = \gamma C_1$, т.е. если время обслуживания двух сопряженных заявок не совпадает, то случайное время $u^i = \max(u_1^i, u_2^i)$ пребывания i -й заявки в Se-сети определяется формулой:

$$u^i = \max(u_1^i, u_2^i) = \begin{cases} u_1^i, & \text{если } C_2 \geq \gamma C_1, \\ u_2^i, & \text{если } C_2 \leq \gamma C_1. \end{cases} \quad (3.41)$$

При $C_2 = \gamma C_1$ для всех i получаем $u_1^i = u_2^i$.

Опустив подробное доказательство, основанное на анализе периода регенерации Se-сети (т.е. периода между двумя последовательными моментами поступления заявок в сеть, оказавшуюся в эти моменты пустой), можно проиллюстрировать формулу (3.41) примером прохождения заявок через экспоненциальную Se-сеть. Экспоненциальная Se-сеть получается из экспоненциальной Ss-сети снятием условия $C_2 = \gamma C_1$, эквивалентного условию $b_2 = b_1$ (где $b_i = 1/\mu_i$). На рисунке 3.5 приводится GPSS-модель экспоненциальной Se-сети, в которой это условие снято, в результате чего время x_1 обслуживания фрагмента заявки в СМО-1 всегда получается меньшим времени x_2 обслуживания сопряженного фрагмента заявки в СМО-2 [129].

```

U1_      MATRIX      ,1,100
U2_      MATRIX      ,1,100

b1_      EQU         1
b2_      EQU         1.2#b1_

          GENERATE    (Exponential(1,0,1.5)),,100
          ASSIGN      PART1,(Exponential(1,0,b1_))
          ASSIGN      PART2,(P$PART1#b2_/b1_)
          QUEUE       TRANSFERT
          SMO_1      SPLIT      1,SMO_2
          QUEUE       1
          SEIZE       1
          DEPART      1
          ADVANCE     P$PART1
          RELEASE     1
          SAVEVALUE   1+,1
          MSAVEVALUE  U1_,1,X1,C1
          QUEUE       11
          TRANSFER    ,SB_

          SMO_2      QUEUE      2
          SEIZE       2
          DEPART      2
          ADVANCE     P$PART2
          RELEASE     2
          SAVEVALUE   2+,1
          MSAVEVALUE  U2_,1,X2,C1
          QUEUE       12
          SB_        ASSEMBLE   2
          DEPART      11
          DEPART      12
          DEPART      TRANSFERT
          TERMINATE   1

          START      100

```

Рисунок 3.5 – Модель экспоненциальной Se-системы с несинхронными процессами в ветвях

На рисунке 3.6 показан фрагмент файла REPORT с результатами моделирования. Статистика по очередям 11 и 12 – очередям синхронизации – показывает, что очередь 12 (очередь фрагментов заявок, приходящих в точку сборки из СМО-2) всегда была пустой (точнее, всегда было не более одного фрагмента заявки, который проходил очередь за нулевое время).

FACILITY	ENTRIES	UTIL.	AVE. TIME	AVAIL.	OWNER	PEND	INTER	RETRY	DELAY
1	100	0.655	1.037	1	0	0	0	0	0
2	100	0.785	1.244	1	0	0	0	0	0
QUEUE	MAX	CONT.	ENTRY	ENTRY (0)	AVE. CONT.	AVE. TIME	AVE. (-0)	RETRY	
1	10	0	100	31	1.334	2.113	3.062	0	
2	12	0	100	19	2.388	3.784	4.671	0	
11	7	0	100	0	1.186	1.878	1.878	0	
12	1	0	100	100	0.000	0.000	0.000	0	
TRANSFERT	13	0	100	0	3.174	5.028	5.028	0	

Рисунок 3.6 – Фрагмент распечатки результатов моделирования

На рисунке 3.7 показаны графики моментов выхода i -ого фрагмента заявки из СМО-1 и моменты выхода, сопряженного с нею фрагмента заявки из СМО-2. По графикам видно, что, несмотря на случайность сравниваемых моментов, фрагменты заявки в СМО-1 всегда обслуживаются раньше соответствующих сопряженных с ними фрагментов заявок из СМО-2. Поэтому в очереди 11 всегда есть ожидающие фрагменты заявки, и ни один фрагмент заявка не проходит эту очередь за нулевое время. При $b_2 = b_1$ два графика сливаются в один [129, 131].

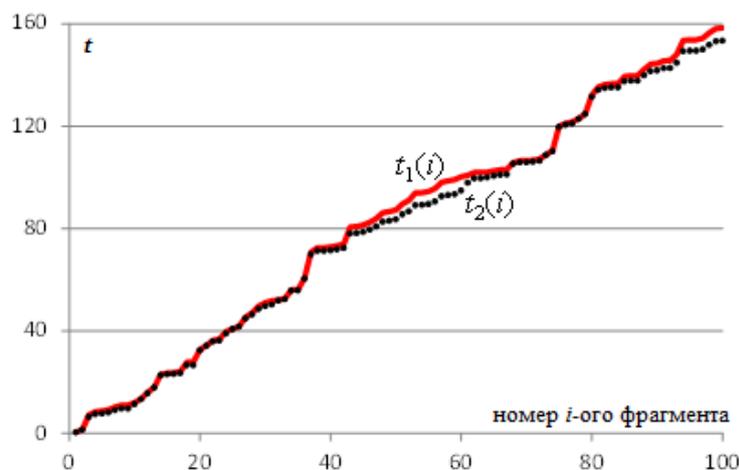


Рисунок 3.7 – Моменты $t_1(i)$ завершения обслуживания i -ого фрагмента заявки и моменты $t_2(i)$ завершения обслуживания сопряженного с ним фрагмента в рассматриваемой Se-сети

Итак, усредняя время пребывания (3.41) по всем заявкам, получается справедливое для любых Se-сетей выражение:

$$U = \begin{cases} U_1, & \text{если } C_2 \geq \gamma C_1, \\ U_2, & \text{если } C_2 \leq \gamma C_1. \end{cases} \quad (3.42)$$

И далее установление справедливости теоремы 4 можно завершить ее доказательством от противного (по аналогии с доказательством теоремы 3).

Стоит отметить два важных следствия теоремы 4:

- при любом входящем потоке оптимальной Se-сетью является Ss-сеть;
- применение оптимальной двухканальной системы связи (в виде Se-сети) не повышает эксплуатационных издержек по сравнению с оптимальной (и, следовательно, по сравнению с любой) одноканальной системой связи [129].

Теорема 4 упрощает решение сложной нелинейной задачи оптимизации Se-сетей, поскольку сводит поиск значений двух варьируемых параметров C_1 , C_2 , доставляющих минимум функции двух переменных, к поиску значения одного варьируемого параметра, доставляющего минимум функции одной переменной. Это особенно важно, когда для расчета целевой функции приходится применять имитационное моделирование, например, когда СМО относятся к системам класса G/G/1, для которых в ТМО нет точных формул, выражающих среднее время пребывания в СМО через ее параметры [129–131].

3.5 Выводы по главе

1. Представлена методика аналитического расчета пропускных способностей каналов двухканальной системы связи, заключающаяся в исследовании систем с различными свойствами, получении расчетных формул, для вычисления минимальных пропускных способностей каналов связи (нижних границ).

2. Представлена математическая модель двухканальной системы передачи видеокадров, разделяемых на меньшую и большую части и отправляемых по разным каналам, имеющим разную пропускную способность. В качестве такой модели в терминах теории массового обслуживания определена сеть с делением и слиянием (S-сеть). В этой сети учитывается передача разделенной заявки по двум

разным каналам, формирование очередей перед каналами и сборка разделенных заявок на принимаемой стороне канала. Необходимость сборки приводит к формированию на принимаемой стороне каналов двух очередей синхронизации, в которых фрагменты разделенных заявок (сопряженные фрагменты) ожидают прихода недостающих фрагментов для сборки.

2. Поставлена математическая задача оптимизации пропускных способностей двух каналов S-сети. Сформулированы и исследованы способы решения этой задачи. Аналитически решена задача оптимизации экспоненциальной S-сети с независимыми каналами. На практике решение этой задачи может использоваться для оптимизации S-сетей, в которых передача разделяемых заявок составляет малую часть общего трафика, передаваемого через два канала.

3. Исследованы задачи оптимизации S-сетей, в которых передача разделяемых заявок составляет основной график, передаваемый по двум каналам. Доказано четыре теоремы, позволяющие свести двумерные задачи оптимизации таких S-сетей (т.е. задачи с двумя варьируемыми параметрами) к одномерным.

4. Рассмотрены несколько S-сетей с последовательно усложняющимися свойствами, в результате установлена возможность сведения двумерной задачи оптимизации к одномерной с самыми общими предположениями относительно вида потока поступающих заявок и законов распределения размеров заявок. Это позволяет эффективно использовать для оптимизации таких сетей имитационное моделирование, поскольку решение задачи оптимизации сводится при этом фактически к табуляции функции вдоль некоторой траектории.

4 ИМИТАЦИОННАЯ МОДЕЛЬ ДВУХКАНАЛЬНОЙ СИСТЕМЫ С РАЗДЕЛЕНИЕМ ДАННЫХ ПО КАНАЛАМ СВЯЗИ

В четвертой главе приводится постановка и решение многокритериальной задачи оптимизации двухканальной системы связи. Описана разработанная имитационная модель двухканальной системы с разделением видеок кадров по каналам связи. Проведены имитационные исследования распределения данных, приведены результаты.

4.1 Обоснование подхода к решению задачи оптимизации параметров двухканальной системы связи как многокритериальной

Требуется обеспечить распределенную передачу видеоданных от источника к получателю, через двухканальную систему с каналами связи, обладающими различной пропускной способностью. Для этих целей предлагается использовать какой-либо из алгоритмов разделения кадров, описанных во второй главе данной диссертационной работы, или иных подобных, осуществляющих разделение данных на две части неравного размера. При этом двухканальная система должна обеспечивать необходимые пропускные способности каналов связи для передачи заданного объема данных при их максимальной загрузке, а также синхронизацию получения передаваемых частей кадров.

В качестве такой системы связи (рис. 4.1) рассматривается система с двумя каналами связи (DL – datalink: DL-1, DL-2) и обратной связью (SL – synchronizationlink) [135].

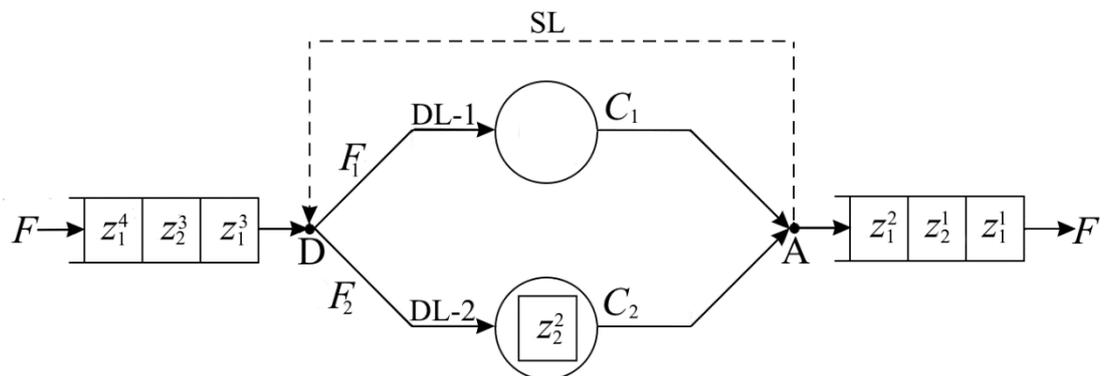


Рисунок 4.1 – Схема системы связи с передачей видеоданных по двум
каналам

Разделение изображения (кадра) z^i производится на две части z_1^i и z_2^i

($i=1,2,\dots$), которые в качестве заявок (в терминах ТМО) передаются на обслуживание по каналам связи, обладающими различными пропускными способностями C_1 и C_2 . Порядок распределения заявок между каналами связи осуществляется на основе алгоритма кругового распределения RR (Round-robin) [136], реализуемого с помощью дисциплины обслуживания «первым пришел – первым обслужен» FIFO (first in – first out) [137].

В точке D (distribute) осуществляется круговое распределение заявок по каналам связи DL-1 и DL-2, соответственно, входящий в систему трафик F (Мбит/с) делится на две части F_1 и F_2 , где $F=F_1+F_2$. В качестве модели трафика в системе связи рассматривается простейший пуассоновский поток [135].

Обратная связь SL служит для синхронизации работы каналов связи, то есть для передачи в точку D информации (сигнала) о том, что в точке сборки A (assemble) получена пара из заявок z_1^i и z_2^i , отправленных по каналам связи DL-1 и DL-2, и только после этого в системе осуществляется передача следующей пары заявок.

В двухканальной системе связи не рассматривается вопрос применения более сложных протоколов обмена (например, на транспортном уровне модели OSI [138] с применением принципа «скользящего окна» как в протоколе TCP), а используется «простой» протокол с подтверждением получения заявок [139]. Такой подход при имитационном моделировании принят в целях определения необходимых пропускных способностей C_1 и C_2 каналов связи DL-1 и DL-2, ввиду того, что к функционированию двухканальной системы связи одновременно предъявляется несколько критериев обеспечивающих максимальную загрузку и минимальный простой каналов связи при синхронной передаче по ним заявок [135].

Так как рассматривается применение нескольких критериев качества функционирования двухканальной системы связи, то задача по оптимизации этих критериев рассматривается и решается как многокритериальная, что приводит к необходимости поиска компромиссных решений, поскольку улучшение поведения системы связи по одному критерию может приводить к ухудшению её поведения с точки зрения других критериев [135].

Для системы связи одновременно требуется обеспечить выполнение трех

критериев – максимизация загрузки, минимизация простоя каналов связи и обеспечение синхронной передачи данных. Поэтому задача многокритериальной оптимизации может быть сформулирована следующим образом: пусть X – вектор варьируемых параметров вектор-функции критериев $J(X) = (J_1(X), J_2(X), J_3(X))$, тогда множеством допустимых значений, включенных в X , является ограниченное и замкнутое множество $R_X \subset \{X\}$. Если вектор-функция $J(X)$ является непрерывной и ограниченной на множестве R_X , то целью оптимизации этой вектор-функции $J(X)$, является минимизация во множестве R_X каждого из показателей $J_1(X)$, $J_2(X)$, $J_3(X)$. Тогда во введенных обозначениях задачу многокритериальной оптимизации можно записать в виде:

$$\min_{X \in R_X} J(X) = J(X^o) = J^o, \quad (4.1)$$

где X^o , J^o – решения задачи.

Векторный критерий оптимальности $J(X)$ отображает в область R_X во множество R_J , называемой множеством достижимости (критериальным множеством) задачи многокритериальной оптимизации (4.1).

На множества R_X вводится отношение предпочтения, обозначаемой символом « \succ_X ». Говорят, что вектор $X' \in R_X$ предпочтительнее вектора $X'' \in R_X$, то есть $X' \succ_X X''$, если среди равенств и неравенств $J_i(X') \leq J_i(X'')$, $i = \overline{1, m}$ существует хотя бы одно строгое неравенство (при выполнении соотношения $X' \succ_X X''$ также говорят, что решение X' доминирует над решением X'').

Отношение предпочтения « \succ_X », заданное на множестве возможных параметров, порождает отношение предпочтения « \succ_J » на множестве возможных векторов $J(X)$: $J(X') \succ_J J(X'') \Leftrightarrow X' \succ_X X''$, при $X', X'' \in \{X\}$. Это означает, что вектор $J' = J(X')$ предпочтительнее вектора $J'' = J(X'')$ (то есть $J' \succ_J J''$), тогда им только тогда когда предпочтительнее X'' (то есть $X' \succ_X X''$).

Ввиду того, что требуется обеспечить синхронную передачу заявок, то параметрами настройки двухканальной системы связи являются: время занятия

(обслуживания) канала связи DL-1 τ_1 , время занятия (обслуживания) канала связи DL-2 τ_2 , тогда вектор варьируемых параметров имеет следующий вид: $X = (\tau_1, \tau_2)$.

Максимальная нагрузка каналов связи двухканальной системы связи, обеспечивается следующим критерием:

$$J_1(X) = N_1 + N_2 \rightarrow \max, \quad (4.2)$$

где N_1, N_2 – количество переданных заявок в каналах связи DL-1 и DL-2, соответственно.

Для того, чтобы решать задачу по минимизации критерия $J_1(X)$, (4.2) представим в виде:

$$-J_1(X) = -(N_1 + N_2) \rightarrow \min \quad (4.3)$$

Минимальный простой каналов двухканальной системы связи достигается при помощи минимизации критерия:

$$J_2(X) = \sum_{i=1}^{N_1} t_{z_1}^i + \sum_{k=1}^{N_2} t_{z_2}^k \rightarrow \min, \quad (4.4)$$

где t_{z_1}, t_{z_2} – времена занятия заявками каналов связи DL-1 и DL-2, соответственно.

Синхронная передача заявок в двухканальной системе связи достигается при помощи минимизации критерия:

$$J_3(X) = |t_{z_1}^i - t_{z_2}^i| \rightarrow \min, \quad (4.5)$$

где $i = \overline{1, N_1}$. N_1 – так как выполняется синхронизация по первому каналу связи.

Таким образом, целью задачи оптимизации двухканальной системы связи является нахождение таких значений варьируемых параметров τ_1, τ_2 при которых минимизируются критерии $J_i(X)$, $i = \overline{1, 3}$ [135], указанные в (4.3), (4.4), (4.5).

Согласно принципу Эджворта-Парето [140] наилучшее решение многокритериальной задачи следует выбирать в пределах множества Парето решений $P_j(X)$, определяемого соотношением: $P_j(X) = \{X^o \in \{X\} \text{ не существует } X \in \{X\} \text{ такого, что } J_i(X) \leq J_i(X^o), i = \overline{1, m}, J_i(X) \neq J_i(X^o)\}$.

Одновременная минимизация критериев соответствует построению

множества Парето-оптимальных решений $P_j(X)$, то есть таких допустимых решений, которые не могут быть улучшены (уменьшены) ни по одному из имеющихся критериев без ухудшения (увеличения) по какому-то хотя бы одному другому критерию. Иначе говоря, предпочитая одному Парето-оптимальному решению другое Парето-оптимальное решение, мы вынуждены идти на определенный компромисс, соглашаясь на некоторую потерю хотя бы по одному критерию (получая определенный выигрыш, по крайней мере, по какому-то другому критерию).

Получение множества Парето-оптимальных решений $P_j(X)$ еще не является окончательным решением при выборе вариантов параметров, так как необходимо получить не несколько, а одно предпочтительное решение. То есть после получения множества Парето-оптимальных решений возникает задача его сужения, которая может быть решена с помощью привлечения дополнительных критериев выбора единственного решения [135, 141].

4.2 Разработка имитационной модели двухканальной системы связи и решение задачи оптимизации с учетом стоимостных и временных характеристик

При многокритериальной оптимизации двухканальной системы связи необходимо выполнить построение множества Парето-оптимальных решений, не улучшаемых одновременно по всем рассматриваемым критериям. Существует значительное число методов и алгоритмов приближенного построения множества Парето, осуществляющих аппроксимацию множества Парето решений (параметров), а тем самым и множества Парето векторных критериев [142, 143].

Относительно новыми и высокоэффективными являются методы Парето-аппроксимации на основе генетических алгоритмов (ГА). Главным достоинством ГА является то, что они могут применяться для решения сложных неформализованных задач, для которых не разработано специальных методов, но даже в тех случаях, для которых хорошо работают существующие методики, можно достигнуть интересных результатов сочетая их с ГА. [144, 145].

Для решения задачи многокритериальной оптимизации использовалась интерактивная среда для научных и инженерных расчетов Matlab/Simulink/

SimEvents [146–149]. В результате проведения имитационного моделирования в данной среде выполнена оптимизация параметров двухканальной системы связи с помощью Парето-аппроксимации на основе многоцелевого ГА NSGA-II (Non-Dominated Sorting Genetic Algorithm) [150], который может использоваться в связке с метамоделями, что позволяет применять его в инженерных задачах при многокритериальной оптимизации [151-153].

Алгоритм NSGA-II основан на процедуре быстрой сортировки множества решений на слои не доминирующих друг над другом решений (fast non-dominated sort – FNDS) и процедуре оценки скрученности решений в пространстве функционалов (crowding distance-assignment). Для отбора индивидуумов вводят две характеристики: ранг r и расстояние $dist$. Значение r для каждого решения вычисляется с помощью процедуры FNDS, после чего решения с одинаковым рангом r объединяются в подмножества F_r , называемые фронтами ранга r . Для

каждого значения $x \in F_r$, вычисляется величина расстояния: $dist(x) = \sum_{m=1}^M dist_m(x)$,

где $dist_m(x)$ – расстояние x для m -ого функционала. Пусть $l = |F_r|$. Решения сортируются в F_r так, чтобы $F_r(1) = f_m^{\min}$ и $F_r(l) = f_m^{\max}$. Граничные решения с (решения с f_m^{\min} и f_m^{\max}) объявляются решениями с $dist_m = 10^6$. Для остальных промежуточных решений $F_r(i)$ значения $dist_m$ определяются по формуле: $dist_m(F_r(i)) = (F_r(i+1).m - F_r(i-1).m) / (f_m^{\max} - f_m^{\min})$, где $i \in [2, l-1]$, а $F_r(i).m$ – значение m -ого функционала для i -ого индивидуума в F_r . Данный алгоритм имеет название crowding distance assignment [150, 154].

При отборе решений лучшими считаются те, которые имеют меньший ранг r . При равенстве рангов лучшими считаются решения с большим значением расстояния $dist$. Таким образом, на всем множестве решений вводится отношение \prec_n . Выражение $p \prec_n q$ означает, что p лучше q , и равносильно выполнению: $p \prec_n q \Leftrightarrow (r(p) < r(q))$ или $(r(p) = r(q) \text{ и } dist(p) > dist(q))$.

Процесс оптимизации в алгоритме NSGA-II состоит из следующих шагов.

1. Случайным образом формируется начальная популяция родителей P_0 , состоящая из N индивидуумов. Для каждого индивидуума в P_0 вычисляются соответствующие значения функционалов и ограничений.

2. Случайным образом формируется начальная популяция детей Q_0 , также состоящая из N индивидуумов.

3. Для каждого индивидуума в популяции детей Q_t , $t \geq 0$, вычисляются соответствующие значения функционалов и ограничений.

4. Популяции детей и родителей объединяются: $R_t = P_t \cup Q_t$. С помощью использования FNDS множество R_t разбивается на фронты разного ранга F_r , $r = 1, \dots, r_{\max}$. Для каждого индивидуума $x \in F_r$ определяется значение расстояния $dist_m(x)$ с помощью описанной выше процедуры crowding-distance assignment.

5. Отбор. На этом этапе из R_t отбираются N лучших индивидуумов (согласно отношению \prec_n), остальные отбрасываются. Отобранные индивидуумы объединяются в новую популяцию родителей P_{t+1} .

6. Построение новой популяции детей Q_{t+1} , состоящей из N индивидуумов, с использованием процедуры рекомбинации и мутации. В алгоритме NSGA-II применяются SBX-рекомбинация и полиномиальная мутация [155].

7. Переход на шаг 3, пока не будет рассчитано N_{Gen} поколений.

Допускается использование других ГА, например, модифицированного алгоритма NSGA-II_m [156] или MOGA (Multi-Objective Genetic Algorithm) [157-160]. В работе [154] приведено достаточно подробное сравнение трех алгоритмов, получено, что фронт Парето, полученный с помощью ГА MOGA на первых 50 поколениях, сходится к точному фронту быстрее, однако после 50 поколений NSGA-II показал более лучшие результаты, а также NSGA-II и NSGA-II_m дают большую точность, то есть лучше определяют экстремальные значения целевых функций. При этом, оба алгоритма сопоставимы и могут применяться для решения сложных инженерных задач [154, 159, 160].

Для построения множества Парето решений использовались специально созданные m-файлы (сценарии на языке Matlab), выполняющие многократные

вызовы модели, реализующей схему исследуемой двухканальной системы связи, приведенную на рисунке 4.1. При генерации множества Парето-оптимальных решений в среде Matlab/Simulink применялись функции из инструментария Global Optimization, в частности, для применения ГА Парето-аппроксимации NSGA-II, использовалась функция *gamultiobj* [135, 140–143].

Задание параметров функции ГА выполнялось через оператор *gaoptimset* функции *gamultiobj*. Число «особей» в популяции ГА устанавливалось в диапазоне от 100...200. Для получения результатов требовалось 10...15 последовательных поколений, не дающих улучшения целевой функции, после чего работа ГА останавливалась. При оптимизации критериев функционирования двухканальной системы связи осуществлялся поиск параметров времен занятия τ_1 , τ_2 каналов связи в DL-1 и DL-2, соответственно, доставляющих минимум принятым критериям (4.3), (4.4), (4.5). В качестве «особи» для ГА использовался вектор настраиваемых параметров $X = (\tau_1, \tau_2)$.

На первом этапе из принятых критериев $J_i(X)$ ($i = \overline{1,3}$), выбираются основные частные критерии $J_1(X)$ и $J_2(X)$, характеризующие показатели загруженности и простоя каналов связи. Далее задача рассматривалась как двухкритериальная.

На втором этапе для основных критериев $J_1(X)$ и $J_2(X)$ находится множество Парето-оптимальных решений. Так как найденное множество Парето-оптимальных решений не является окончательным решением, то для его сужения используется так называемый лексикографический подход [134.], сущность которого заключается в том, что частные критерии упорядочиваются по важности и привлекаются поочередно для выбора параметров в качестве дополнительной информации, пока не будет получено единственное решение.

На заключительном, третьем этапе для окончательного выбора оптимальных параметров двухканальной системы связи (оптимальных пропускных способностей каналов связи) вводится критерий $J_3(X)$, минимальное значение которого отыскивается среди множества Парето-оптимальных решений,

полученных по критериям $J_1(X)$ и $J_2(X)$.

Вычисление и передача в рабочую область значений $J(X)$ выполнялись с помощью m-файла – сценария. Значения критериев $J_i(X)$ ($i = \overline{1,3}$) для каждого вектора X , полученные в результате имитационного моделирования передавались в основной ГА. На каждом этапе работы алгоритма рассматривался полученный вектор параметров X и соответствующее ему значение критерия $J(X)$. Так как начальная популяция ГА формируется с использованием генератора случайных чисел, то для выбора лучших решений выполнялось несколько реализаций расчетов [135].

Для определения оптимального состояния функционирования двухканальной системы связи требовалось выполнить модельные исследования этой системы со значениями вектора настраиваемых параметров, изменяющимися в диапазонах, определяемых качеством и, соответственно, параметрами трафика F , создаваемого техническими средствами (источниками видеоданных). Для проведения имитационного моделирования использовались следующие начальные параметры. Пусть технические средства формируют поток видеоданных с расширением 1280x720 пикселей и частотой 60 кадров/с. Трафик при передаче такого потока видеоданных составляет $F = F_1 + F_2 = 900$ МБ/час (2 Мбит/с) [161, 162].

При реализации разделения кадров видеоданных определено, что F разбивается в соотношении $F_1/F_2 = \gamma = const = 11,2$ ($F_1 = 1,837$ Мбит/с, $F_2 = 0,164$ Мбит/с) [33-38]. По двухканальной системе связи совместно с трафиком от технических средств передаются дополнительные данные (например, командно-телеметрические), объем которых не превышает 10% от общего объема передаваемых данных [163, 164]. Тогда $F = F_1 + F_2 = 2,2$ Мбит/с, $F_1 = 2,021$ Мбит/с, $F_2 = 0,179$ Мбит/с и учитывая то, что поступающие в каналы связи заявки сразу передаются на обслуживание, то для данных каналов диапазон варьируемых параметров составит $\tau_1 \in [5,092; 5,587]$ и $\tau_2 \in [0,495; 6,082]$. Вычисление значений диапазона варьируемых параметров для других форматов качества потоков видеоданных осуществлялся аналогично [135].

Параметры для ГА задаются при помощи следующих опций в среде

Matlab/Communications Toolbox:

```

lb = [5.092 0.495];           % верхняя граница варьируемых значений критериев.
ub = [5.587 6.082];         % нижняя граница варьируемых значений критериев.
options = gaoptimset('PopInitRange', [lb;ub], 'PopulationSize', 200);
                                % задание параметров генетического алгоритма:
                                % диапазон варьируемых параметров;
                                % размер популяции.
options = gaoptimset(options, 'PlotFcns', {@gaplotpareto, @gaplotparetodistance});
                                % задание параметров генетического алгоритма:
                                % отображения прогресса работы алгоритма;
                                % зависимости функций на множестве Парето;
                                % расстояния каждой особи от его соседей.
options = gaoptimset(options, 'TolFun', 1e-4, 'StallGenLimit', 10);
                                % задание параметров генетического алгоритма:
                                % нижняя граница целевой функции;
                                % число последовательных поколений, не дающих
                                % улучшения целевой функции, после которого
                                % останавливается алгоритм.
options.Generations = 20;      % количество генераций.
[x, fval, exitflag, output] = gamultiobj(@GoalFunland3_s22, 2, [], [], [], [], lb,
ub, options);                 % вызов функции оптимизации на основе
                                % генетического алгоритма NSGA-II.

```

Для того чтобы исследовать двухканальную систему связи, создана имитационная модель распределения заявок между её каналами связи, реализованная с помощью инструментов моделирования пакета Matlab/Simulink/SimEvents. (рис. 4.2). Модель собрана из библиотечных блоков SimEvents и Simulink, для настройки свойств и параметров которых используются диалоговые окна. Схема состоит из 6 составных модулей – Generator, Gateway, DL-1, DL-2, Receiver, F1-F3 [135].

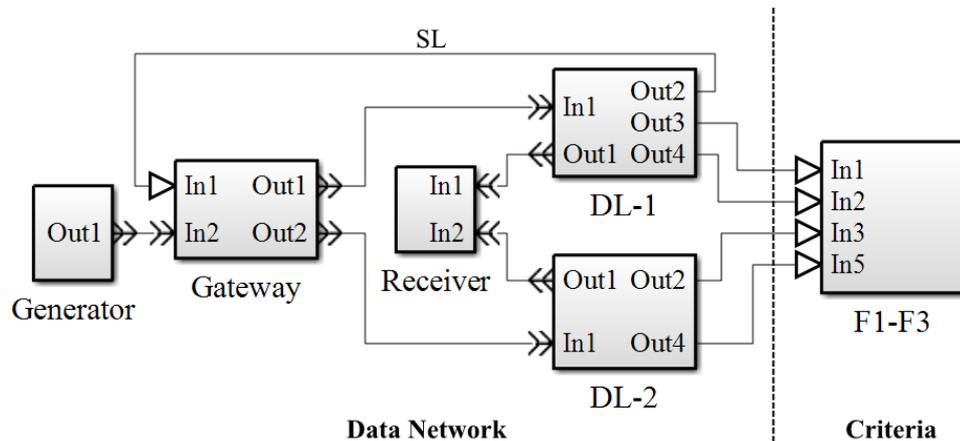


Рисунок 4.2 – Модель системы связи с распределенной передачей заявок по двум каналам в среде Matlab/SimEvents

Источником заявок в модели является блок Time-Based Entity Generator из составного модуля формирования заявок – Generator (рис. 4.3). Закон распределения и время между возникновением поступающих заявок заданы в

параметрах блока генерации случайных чисел Event-Based Random Number. Сгенерированные заявки поступают в блок очереди FIFO Queue и ожидают обслуживания. Очередь обслуживания не имеет ограничения по емкости [135].

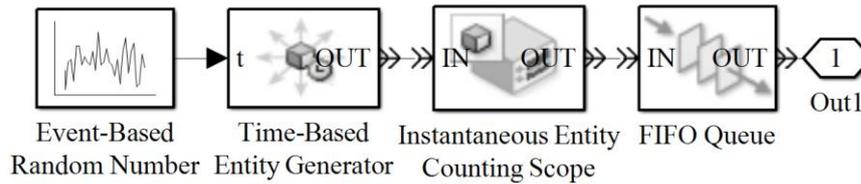


Рисунок 4.3 – Структура составного модуля формирования заявок – Generator

В составном модуле распределения заявок – Gateway (рис. 4.4) осуществляется циклическое распределение заявок по составным модулям DL-1 и DL-2 с помощью алгоритма Round-robin.

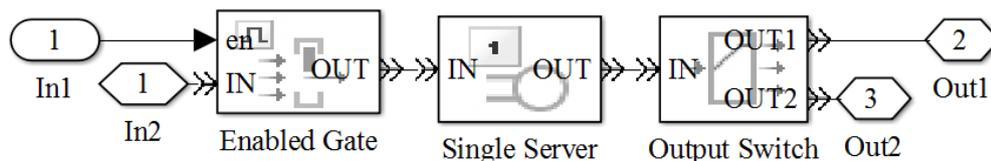


Рисунок 4.4 – Структура составного модуля распределения заявок – Gateway

Блок Enabled Gate, на основании управляющего сигнала на порту In1, выполняет блокировку поступления в составные модули DL-1 и DL-2 заявок, до тех пор, пока отправленная ранее пара заявок не будет обслужена. Блок Single Server – вспомогательный блок, который отправляет заявку на обработку блоку Output Switch, который служит для выбора необходимого канала связи. Параметр Switching criterion блока Output Switch, задан как Round-robin [135].

В составных модулях обработки заявок DL-1 и DL-2, являющихся моделями двух параллельных каналов связи, осуществляется обработка поступивших в них заявок. Составной модуль DL-1 (рис. 4.5) имеет идентичную структуру с составным модулем DL-2 (рис. 4.6), за исключением того, что в нем имеется вывод Out2, выполняющий передачу управляющего сигнала о том, что в блоке Single Server на обслуживании находится заявка. Вывод Out2 составного модуля DL-1 соединен с входом In1 составного модуля распределения заявок Gateway (см. рис. 4.2).

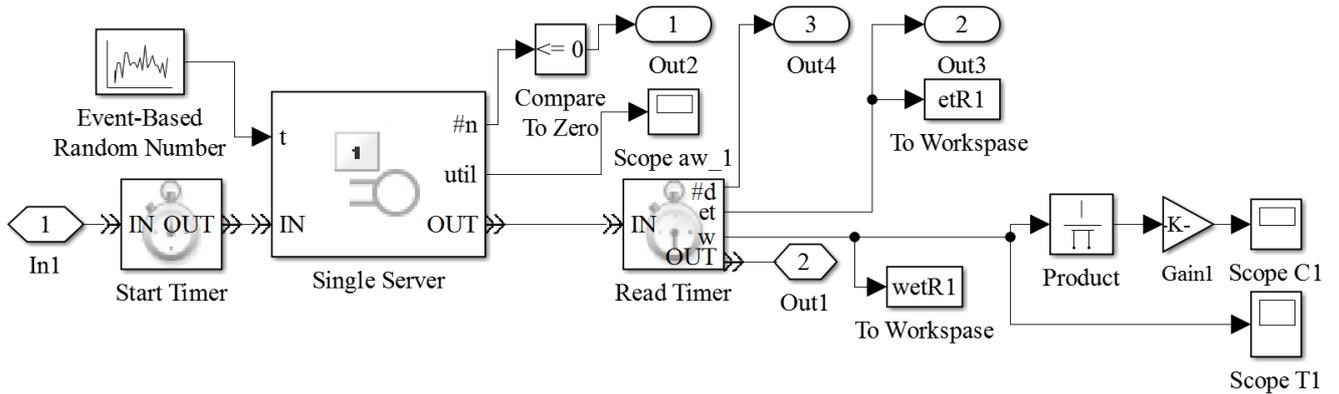


Рисунок 4.5 – Структура составного модуля обработки заявок – DL-1

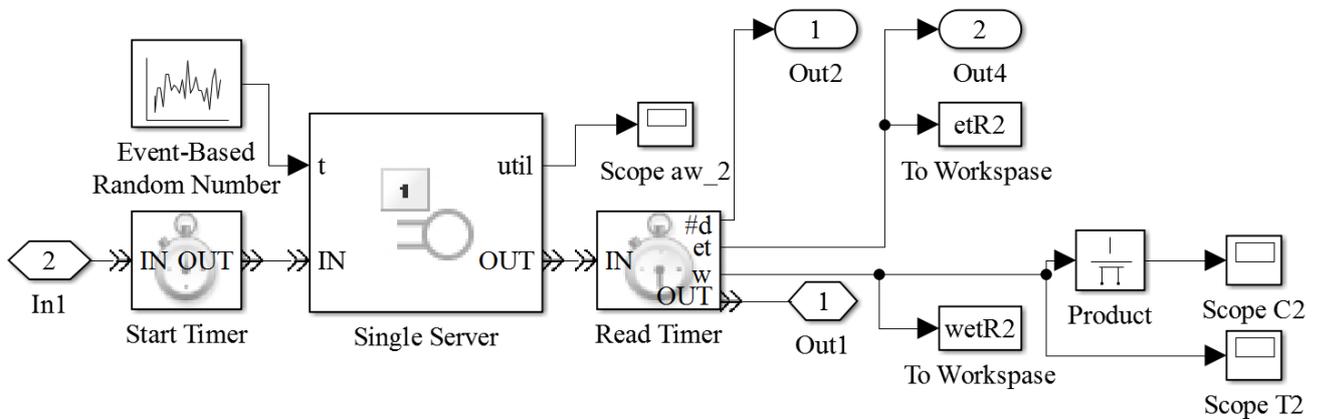


Рисунок 4.6. – Структура составного модуля обработки заявок – DL-2

Так как трафик рассматривается в виде классического представления в качестве пуассоновского потока, то время между последовательными поступлениями заявок и время их обслуживания, будучи случайными величинами, при моделировании систем массового обслуживания количественно описываются экспоненциальным распределением. Плотность вероятности длительности пауз между генерациями заявок $p(t) = \lambda e^{-\lambda t}$, где λ – интенсивность потока, $\tau = 1/\lambda$ – среднее время занятия канала (обслуживания заявки). Следовательно, в свойствах блоков Event-Based Random Number составных модулей DL-1 и DL-2 параметры Distribution заданы как Exponential, а параметры Mean заданы, как τ_1 и τ_2 , соответственно, и изменяются в рамках заданных диапазонов. Для учета времени пребывания заявок в каналах связи используются блоки Start Timer и Read Timer, показания которых передаются в рабочую область Matlab для организации синхронной передачи заявок [135].

Составной модуль объединения заявок – Receiver (рис. 4.7) ожидает поступления заявок из составных модулей обслуживания заявок DL-1 и DL-2.

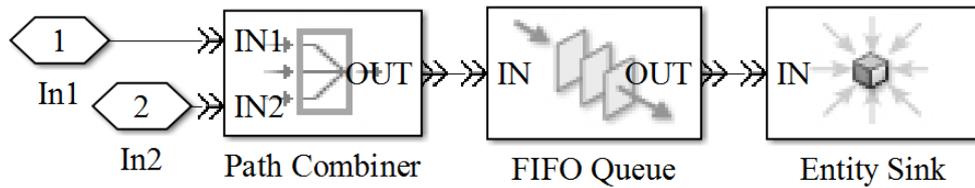


Рисунок 4.7 – Структура составного модуля объединения заявок для завершения их обслуживания – Receiver

Блок Path Combiner служит для объединения заявок в одну очередь с дисциплиной обслуживания FIFO. Блок Entity Sink служит для завершения обслуживания заявок.

Составной модуль передачи параметров F1-F3 выполняет передачу оптимизируемых значений критериев $J_1(X)$, $J_2(X)$, $J_3(X)$ в программную область Matlab, для последующей их обработки и принятия решения ГА о необходимости дальнейших генераций или оптимальности полученного решения.

При помощи ГА найдено множество Парето решений, на котором минимизируются критерии $J_1(X)$, $J_2(X)$. Графики характеристик двухканальной системы связи для $J_1(X)$, $J_2(X)$ приведены на рисунках 4.8 и 4.9.

Для решения задачи многокритериальной оптимизации выбраны основные частные критерии $J_1(X)$, $J_2(X)$, характеризующие максимальную загрузку и минимальный простой каналов связи двухканальной системы, и задача оптимизации рассматривалась как двухкритериальная. Для основных критериев $J_1(X)$, $J_2(X)$ было получено множество Парето-оптимальных решений. Затем, для окончательного выбора решения в качестве дополнительного вводился критерий $J_1(X)$ обеспечивающий синхронную передачу заявок, минимальное значение, которого отыскивалось среди множества Парето-решений, полученных по критериям $J_1(X)$, $J_2(X)$ [135].

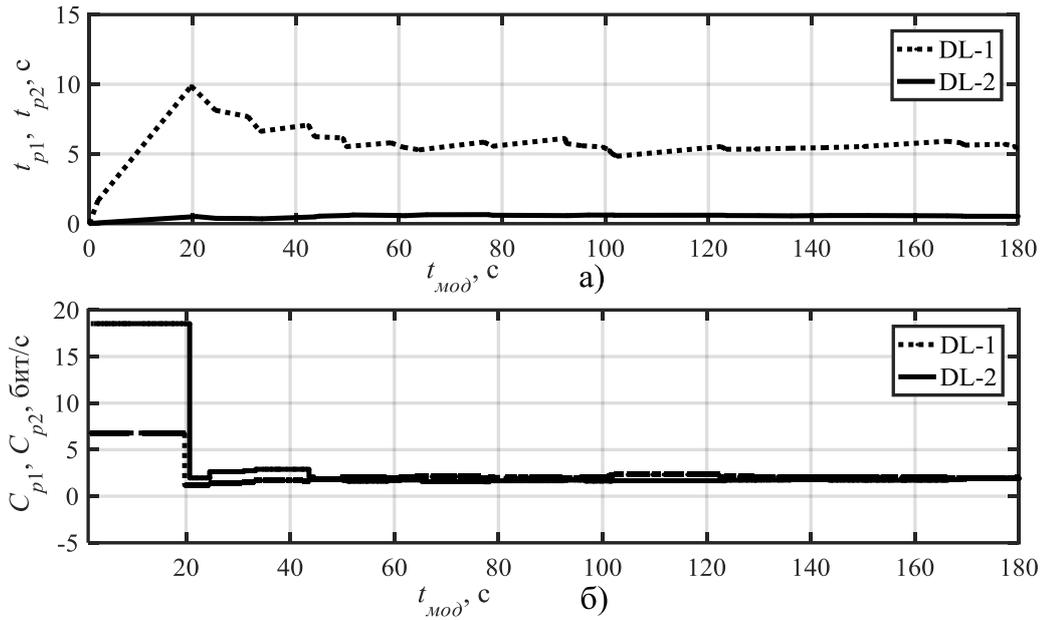


Рисунок 4.8 – Характеристики двухканальной системы при $J_1(X) \rightarrow \min$:

- а) изменение времени пребывания заявок в каналах связи;
- б) изменение пропускных способностей каналов связи

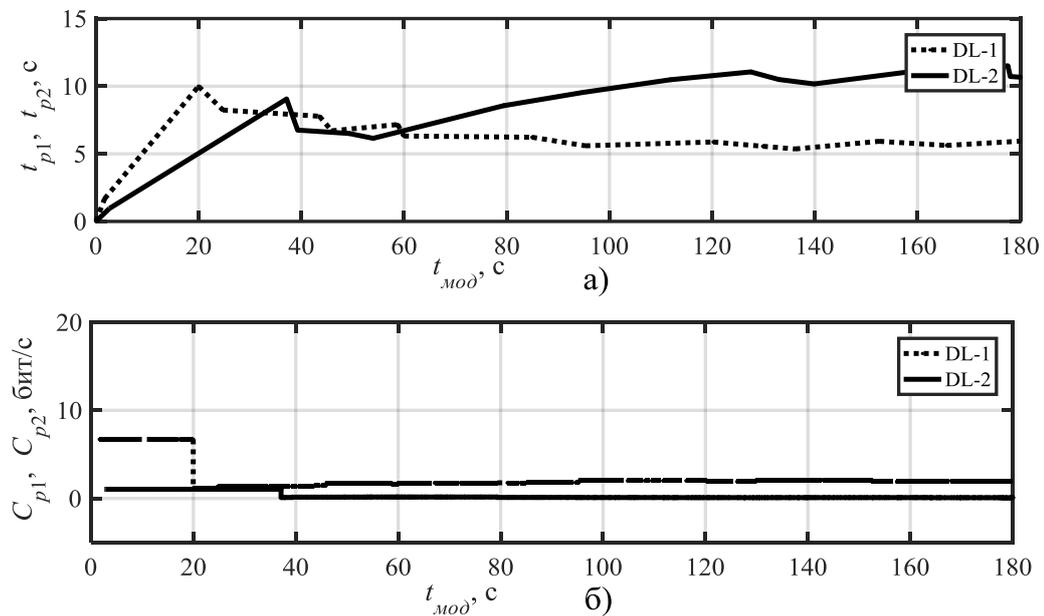


Рисунок 4.9 – Характеристики двухканальной системы при $J_2(X) \rightarrow \min$:

- а) изменение времени пребывания заявок в каналах связи;
- б) изменение пропускных способностей каналов связи

Результат оптимизации для одной из реализаций решения двухкритериальной задачи с использованием критериев $J_1(X)$, $J_2(X)$ приведен на рисунке 4.10, на

котором выполнено отображение плоскости параметров (множества Парето решений) на критериальную плоскость (множества Парето векторных решений). Точки, соответствующие минимумам критериев $J_1(X)$, $J_2(X)$, соединены прямой, являющейся отображением фронта Парето на плоскость параметров системы связи. Видно, что «особи» ГА, расположены вокруг фронта Парето [135].

Целью оптимизации являлось получение минимальных пропускных способностей C_1 , C_2 при выполнении условия синхронизации передачи заявок, т.е. при $t_{p1} = t_{p2}$. В результате привлечения критерия $J_3(X)$ из множества точек Парето-оптимальных решений выбрано единственное, соответствующее минимуму критерия $J_3(X)$, которое обозначено на рисунке 4.10, а, кружком и стрелкой показан соответствующий ему выделенный элемент множества Парето-оптимальных решений (рис. 4.10, б).

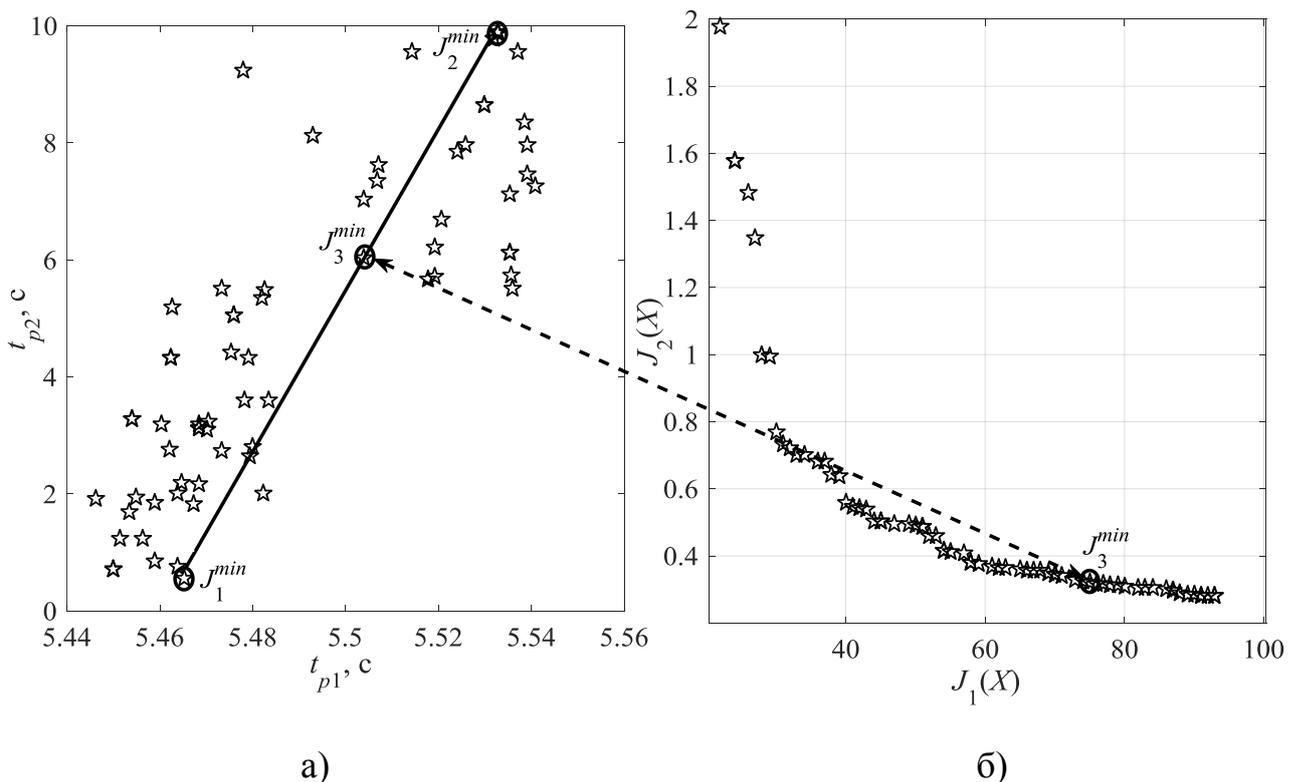


Рисунок 4.10 – Отображение параметрического пространства в критериальное при оптимизации параметров двухканальной системы связи с помощью ГА:

а) множество Парето-решений на параметрической плоскости; б) множество Парето для критериев $J_1(X)$, $J_2(X)$

В проведенном имитационном моделировании при заданных параметрах ГА и $J_3(X) \rightarrow \min$ синхронизация передачи данных по каналам связи DL-1 и DL-2 достигается при значении времен занятия каналов связи $t_p = t_{p1} = t_{p2} = 5,5$ с. График $J_3(X)$ и графики времен занятия каналов связи DL-1 и DL-2 приведены на рисунке 4.11. Точка пересечения графиков времен занятия каналов связи DL-1 и DL-2 (рис. 4.11, б) соответствует моменту синхронизации [135].

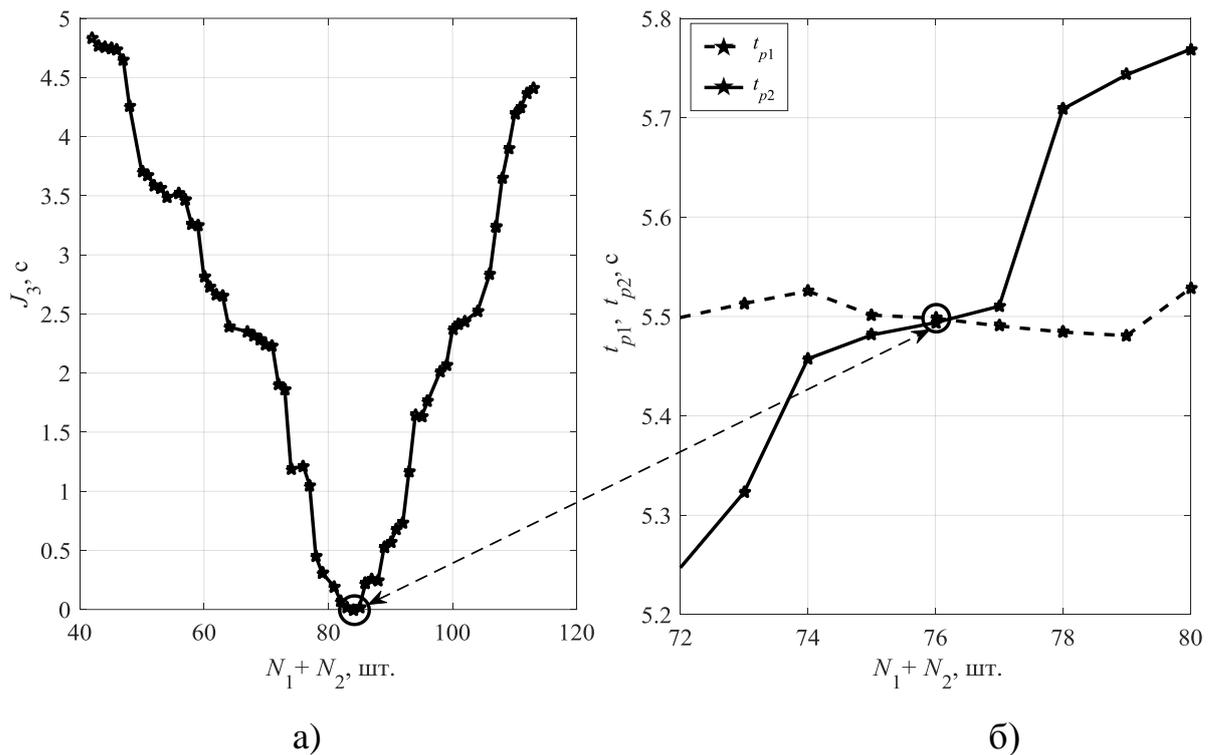


Рисунок 4.11 – Характеристики при синхронизации каналов связи: а) график функции $J_3(X)$; б) графики длительности занятия каналов связи DL-1 и DL-2

Процесс настройки синхронизации с помощью ГА при привлечении критерия $J_3(X)$ отображен на рисунке 4.12. Из рисунка 4.12, а видно, что с привлечением критерия $J_3(X)$ ГА в течение 80 с. осуществляет настройку параметров двухканальной системы связи. Таким образом, обеспечивая синхронную передачу данных с необходимыми пропускными способностями $C_1 = 2,0384$ Мбит/с, $C_2 = 0,186$ Мбит/с. Значение финансовых (или материально-технических) издержек, описываемых формулой (3.29), при подстановке пропускной способности C_1 , $m = 0,01$ у.е./(Мбит/с) и $l = 1$ у.е./с, будет составлять $f = 0,0464$ у.е.

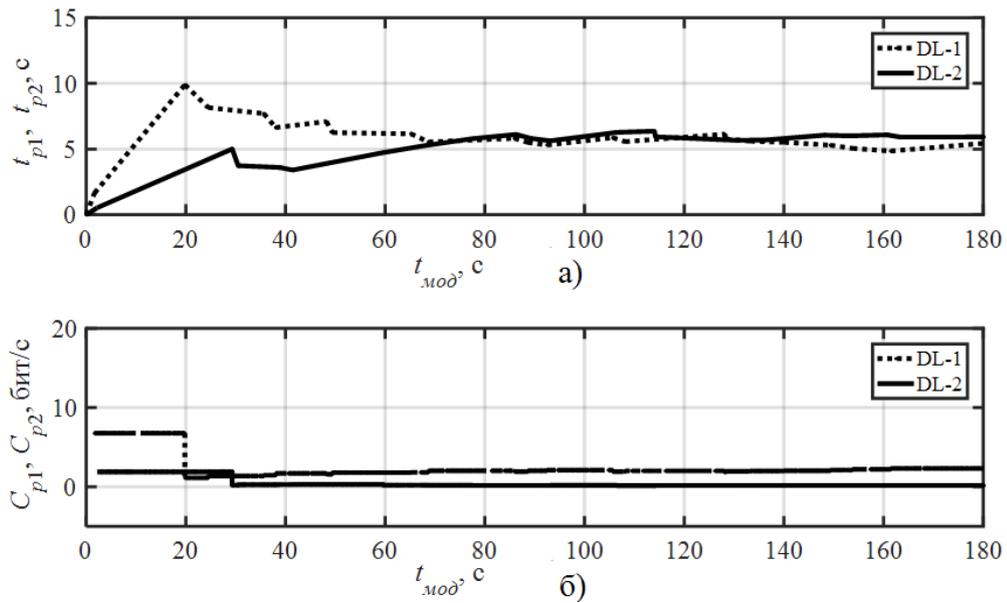


Рисунок 4.12 – Характеристики двухканальной системы при $J_3(X) \rightarrow \min$: а) изменение времени занятия каналов связи; б) изменение пропускных способностей каналов связи

Значения, полученные при помощи имитационного моделирования, в допустимых пределах совпадают со значениями, полученными при аналитическом расчете (см. пример 4), что подтверждает пригодность применяемых методов имитационного моделирования. Таким образом, применение современных методов оптимизации с использованием ГА позволяет за короткое время найти такие параметры системы двухканальной передачи данных, которые одновременно сокращают время передачи (уменьшают задержки) и снижают затраты (уменьшают стоимость эксплуатации). То есть, за счёт минимизации целевой функции (3.5) достигается более эффективная и экономически выгодная работа системы [135].

Численные эксперименты показали, что использование ГА для многокритериальной оптимизации распределения данных между двумя каналами позволяет эффективно балансировать требования к качеству передачи и экономии вычислительных ресурсов. То есть, подход обеспечивает обоснованное (приемлемое) решение, которое достигается при минимальных затратах по времени и вычислительной мощности. Этот результат особенно важен для систем реального времени, где скорость обработки данных критична, а ограниченные вычислительные ресурсы требуют использования быстрых и адаптивных оптимизационных методов [135].

4.3 Оценка достоверности результатов имитационного моделирования

Оценить достоверность результатов имитационного моделирования можно, применяя комплексный подход, включающий, как минимум следующие методы:

- верификация модели – проверка корректности реализации самой модели, её алгоритмов и программного кода (например, через отладку, тестирование на простых случаях и сравнение с аналитическими решениями);
- статистический анализ результатов – применение методов статистической обработки данных, таких как вычисление доверительных интервалов, анализ дисперсии (ANOVA), позволяет оценить устойчивость и надежность полученных показателей;
- валидация модели – сравнение результатов моделирования с экспериментальными или эмпирическими данными реальной системы для подтверждения адекватности модели;

Совокупное применение этих методов позволяет комплексно оценить точность, надежность и адекватность имитационной модели.

Верификация модели. Ввиду того, что в третьей главе данной диссертационной работы приведена методика аналитического расчета пропускных способностей каналов связи, позволяющая свести решение многокритериальной (двумерной) задачи оптимизации к однокритериальной (одномерной) и найти необходимые пропускные способности каналов двухканальной системы связи, то целесообразно оценить достоверность результатов имитационного моделирования с помощью статистического анализа результатов. Для этих целей достаточно выполнить сравнение результатов имитационного моделирования с результатами, полученными с помощью методики аналитического расчета. Так как разделение данных (заявок) между каналами двухканальной системы связи осуществляется в постоянном соотношении, и система имеет экспоненциальное распределение и в неё входит пуассоновский поток заявок, то аналитическое решение будет иметь единственное решение при заданных условиях.

Кроме того, в целях дальнейшего статистического анализа результатов (генеральной совокупности), полученных с помощью имитационной модели, и

ввиду отсутствия данных о стандартном отклонении σ генеральной совокупности, для оценки рассеяния возможных значений случайной величины (пропускных способностей каналов связи) квантилями t_n (нормированная квантиль стандартного нормального распределения) необходима выборка при $n \geq 30$ наблюдений [165]. Поэтому, целесообразно, сформировать для имитационной модели выборку не менее чем из 30 наблюдений, так как считается, что закон распределения среднего значения (\bar{X}) при $n \geq 30$ близок к нормальному при любом законе распределения исходных данных с контрэксцессом $\kappa \neq 0$. В таблице 4.1 приведены результаты из 30 (тридцати) значений пропускных способностей каналов связи, полученных в результате имитационного моделирования при передаче несжатого потока видеоданных формата HD (1280*720) (для других форматов оценка достоверности результатов осуществляется аналогично) и соответственно с размером кадра 22118400 бит. Для потока 60 кадров/с $F = 1327104000$ бит/с (1,327104000 Гбит/с) применяется АРПК, описанный в разделе 2.2 главы 2 данной диссертационной работы, в результате разделения формируются потоки $F_1 = 0,10789959$ Гбит/с, $F_2 = 1,21920441$ Гбит/с. Кадры разбиваются на части $H_1 = 1798327$ бит, $H_2 = 20320073$ бит, $\gamma = H_2/H_1 = 11,24$.

Таблица 4.1 – Результаты имитационного моделирования

№	C_1 , (Гбит/с)	C_2 , (Гбит/с)	№	C_1 , (Гбит/с)	C_2 , (Гбит/с)	№	C_1 , (Гбит/с)	C_2 , (Гбит/с)
1	0,111427541	1,252445546	11	0,109671417	1,232706726	21	0,110984471	1,247465439
2	0,115120087	1,293949773	12	0,114712491	1,289368393	22	0,112513351	1,264650052
3	0,110632258	1,243506582	13	0,112796588	1,267833653	23	0,113908084	1,280326863
4	0,111618472	1,254591620	14	0,110982356	1,247441684	24	0,112170147	1,260792454
5	0,109203849	1,227451261	15	0,113233205	1,272741221	25	0,110474735	1,241736027
6	0,110171999	1,238333264	16	0,111421022	1,252372284	26	0,109350209	1,229096348
7	0,112096725	1,259967184	17	0,111057143	1,248282284	27	0,113412939	1,27476143
8	0,113733138	1,278360473	18	0,110158585	1,238182497	28	0,110294713	1,239712573
9	0,109770836	1,233824194	19	0,109790539	1,234045653	29	0,112878661	1,268756137
10	0,114317073	1,284923905	20	0,113539385	1,276182688	30	0,111993561	1,258807620

Приведенные в таблице 4.1 результаты имитационного моделирования в среде Matlab для пар пропускных способностей C_1 и C_2 имеют различные значения. Это

обусловлено тем, что при оптимизации параметров системы с использованием генетического алгоритма ГА, результат может изменяться из-за следующих факторов:

- случайность начальной популяции – ГА NSGA-II в Matlab (из Global Optimization Toolbox) использует случайно сгенерированную начальную популяцию. Поэтому при каждом запуске результаты могут отличаться;
- операторы мутации и кроссовера – эти операторы тоже содержат элементы случайности, что приводит к вариативности решений;
- ограниченное количество итераций – если алгоритм завершает работу до достижения глобального оптимума, итоговое решение отличится при разных запусках;
- ограничения и параметры алгоритма – настройки, такие как размер популяции, вероятность мутации, вероятность кроссовера и критерии останова, могут влиять на результат;
- генератор псевдослучайных чисел в Matlab.

Так как было обозначено выше, что входящий в систему поток заявок имеет вероятностный закон поступления, то есть в нее входит пуассоновский поток заявок, и размеры фрагментов заявок распределены по экспоненциальному, то в соответствии с методикой аналитического расчета (см. главу 3) пропускная способность первого канала связи может быть найдена по формуле (3.32), подставляя значения γ , H_1 и учитывая, что издержки составляют, например, $m = 0,00001$ у.е./Гбит/с) и цена средней задержки заявки в сети ($l = 100$ у.е./с), то получим $C_1 = 0,109111704$ Гбит/с и $C_2 = 1,226415553$ Гбит/с ($C_1 > F_1$ и $C_2 > F_2$).

Результаты аналитического расчета для параметров C_1 и C_2 не превышают значений, полученных в ходе имитационного моделирования, а как раз являются минимально необходимыми. Результаты имитационного моделирования находятся вблизи аналитических значений (расхождение в среднем не более 9%), это свидетельствует о корректности реализации модели, её соответствии формальным требованиям, математическим уравнениям и алгоритмам, что подтверждает её верификацию.

Статистический анализ результатов. Так как закон распределения среднего значения (\bar{X}) при $n \geq 30$ результатов имитационного

моделирования близок к нормальному, то возможно применить оценивание с помощью доверительного интервала (ДИ) для параметров нормального распределения [166]. ДИ для параметра θ называется интервал (θ_1, θ_2) накрывающий истинное значение θ с заданной вероятностью $\beta = 1 - \alpha$, т.е. $P[\theta_1 < \theta < \theta_2] = 1 - \alpha$. Число α – уровень значимости, то есть вероятность с которой значение параметра не попадет в ДИ. Число $\beta = 1 - \alpha$ называется доверительной вероятностью (уровнем доверия), это вероятность того, что ДИ накрывает значение параметра. Обычно уровень значимости равен 0,01; 0,05; 0,1, что соответствует уровню доверия 0,99 (99%); 0,95 (95%), 0,9 (90%).

Для каждой полученной совокупности результатов для C_1 и C_2 , приведенных в таблице 4.1, находятся среднее значения $\bar{C}_1 = 0,111781186$, $\bar{C}_2 = 1,256420528$. ДИ для каждого среднего имеет вид $(\bar{C}_1 - \Delta_{C_1}; \bar{C}_1 + \Delta_{C_1})$; $(\bar{C}_2 - \Delta_{C_2}; \bar{C}_2 + \Delta_{C_2})$, где Δ_{C_1} , Δ_{C_2} – точности интервальной оценки. Правило для вычисления точности зависит от замера выборки (n) о от информации о стандартном отклонении σ (известно оно или нет). Так как изначально предполагается, что стандартное отклонение σ неизвестно, $n \geq 30$, то оценки ДИ можно воспользоваться выборочным стандартным (среднеквадратическим) отклонением [167]:

$$S = \sqrt{\sum_1^n (x_i - \bar{X})^2 / (n-1)}, \quad (4.6)$$

где n – количество наблюдений, x_i – результат i -ого наблюдения, $\bar{X} = \sum_1^n x_i / n$ – среднее арифметическое значение результатов наблюдения.

Таким образом, применительно к C_1 и C_2 , ДИ для среднего при неизвестном стандартном отклонении (дисперсии):

$$\left(\bar{C}_i - z_{\alpha_i} \frac{S_{C_i}}{n}; \bar{C}_i + z_{\alpha_i} \frac{S_{C_i}}{n} \right), \quad i = \bar{1}, \bar{2}, \quad (4.7)$$

Выполняя эквивалентные замены в (4.6) и подставляя соответствующие

числовые значения, получено: $S_{C_1} = 0,001691561$; $S_{C_2} = 0,019013133$.

В исследовании [165] рассмотрены методы статистической обработки данных, а также даны рекомендации по выбору уровня доверия – 95%, с учётом допустимой погрешности и требований к точности измерений. Выбор уровня доверия 95% обусловлен стремлением минимизировать как систематические, так и случайные ошибки, обеспечивая при этом оптимальный баланс между шириной ДИ и точностью результатов. Поэтому, найдем 95% ДИ. z_{α_i} – квантиль нормального распределения уровня $1 - \alpha / 2$ (пусть, $z_{\alpha_1} = z_{\alpha_2}$), по таблице нормального распределения для 95% ДИ $1 - \alpha / 2 = 0,975$, квантиль $z_{\alpha} = 1,96$, тогда точность для C_1 : $\Delta_{C_1} = 0,000605317$, для C_2 : $\Delta_{C_2} = 0,006803762$. Искомый 95% ДИ для пропускных способностей C_1 : $(0,111175869; 0,112386503)$, для C_2 : $(1,249616765; 1,263224290)$.

С помощью среды Matlab для значений параметров C_1 и C_2 . построены 95% ДИ. Исходный код для построения ДИ для C_1 приведен ниже, для C_2 исходный код аналогичен, за исключением массива data[], в котором содержится значения параметров C_1 и C_2 полученные при моделировании.

```
data = [0.11142754 0.115120087 0.110632258 0.111618472 0.109203849 0.110171999
0.112096725 0.113733138 0.109770836 0.114317073 0.109671417 0.11471249
0.112796588 0.110982356 0.113233205 0.111421022 0.111057143 0.110158585
0.109790539 0.113539385 0.11098447 0.11251335 0.113908084 0.112170147
0.110474735 0.109350209 0.113412939 0.110294713 0.11287866 0.11199356];
% Вычисление среднего и стандартного отклонения
mean_value = vpa(mean(data),9);
std_value = vpa(std(data),9);
n = length(data); % Размер выборки
% Уровень доверия (95%)
alpha = 0.05; % 1 - уровень доверия
t_critical = vpa(tinv(1 - alpha/2, n - 1),9); % Крит. значение t-распределения
margin_of_error = vpa(t_critical * (std_value / sqrt(n)),9);
ci_lower = mean_value - margin_of_error; % Доверительный интервал
ci_upper = mean_value + margin_of_error;
m = length(data);
for i = 1:m, T(i) =i; end;
figure; hold on; plot(T,data,'*');
plot([0, 30], [ci_lower, ci_lower], '--', 'LineWidth', 1.5); % Нижняя граница
plot([0, 30], [ci_upper, ci_upper], '--', 'LineWidth', 1.5); % Верхняя граница
plot([0, 30], [0.109111704, 0.109111704], '--', 'LineWidth', 1.5); % Аналит.
xlabel('Номер исследования'); ylabel('C_1, Гбит/с');
text(0, 0.111, 'Верхняя граница ДИ для C_1');
text(0, 0.112, 'Нижняя граница ДИ для C_1');
text(0, 0.109, 'C_1=0,109111704 Гбит/с при аналитическом расчете');
title('ДИ (95%) при неизвестной дисперсии');
```

На рисунках 4.13 и 4.14 представлены результаты имитационного

моделирования для пропускных способностей C_1 , C_2 и 95% ДИ соответственно.

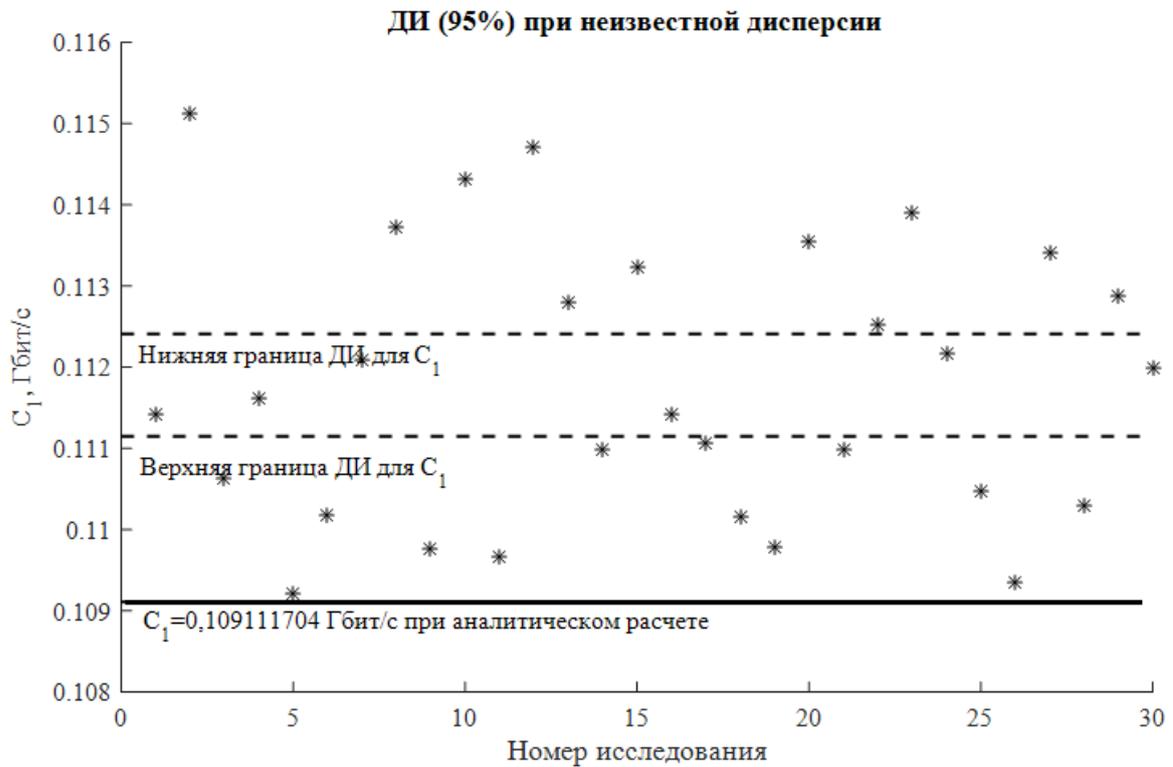


Рисунок 4.13 – Результаты имитационного моделирования двухканальной системы для оценки ДИ пропускной способности C_1 первого канала связи.

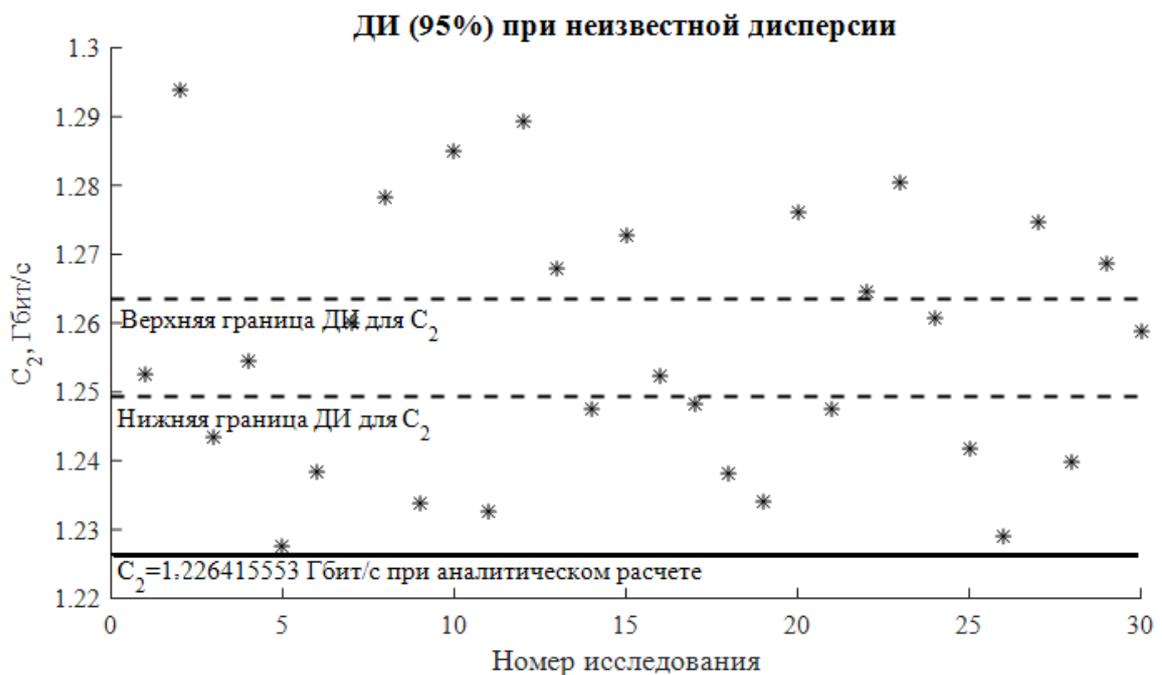


Рисунок 4.14 – Результаты имитационного моделирования двухканальной системы для оценки ДИ пропускной способности C_2 второго канала связи.

Из рисунков 4.13, 4.14 видно, что полученные ДИ для C_1 и C_2 узкие, это указывает на более точную оценку исследуемых параметров, их однородность, а также позволяет утверждать, о том, что истинное значение параметров находится в пределах полученных границ. Таким образом, можно утверждать, что оценка среднего значения параметров осуществляется с высокой точностью, а случайные ошибки сведены к минимуму. Узкие интервалы свидетельствует о том, что все измерения сосредоточены в узком диапазоне, что позволяет предположить однородное поведение исследуемой системы связи. Это важно для обеспечения стабильности ее работы.

Также для статического анализа результатов эксперимента возможно использовать бутстрэп-метод позволяющий оценить точность и стабильность результатов эксперимента без необходимости проведения дополнительных испытаний и предположений о форме распределения данных [168]. Для этих целей в среде Matlab можно провести бутстрапирование полученных в результате работы имитационной модели значений пропускных способностей C_1 и C_2 . Исходный код для построения ДИ с помощью бутстрэп-метода для пропускной способности C_1 приведен ниже (для C_2 исходный код аналогичен, за исключением массива data[]):

```
data = [0.11142754 0.115120087 0.110632258 0.111618472 0.109203849 0.110171999
0.112096725 0.113733138 0.109770836 0.114317073 0.109671417 0.11471249
0.112796588 0.110982356 0.113233205 0.111421022 0.111057143 0.110158585
0.109790539 0.113539385 0.11098447 0.11251335 0.113908084 0.112170147
0.110474735 0.109350209 0.113412939 0.110294713 0.11287866 0.11199356];
% Параметры бутстрэпа
nBoot = 1000; % Количество бутстрэп-выборок
alpha = 0.05; % Уровень значимости для 95% доверительного интервала
bootfun = @(x) mean(x); % Функция для вычисления статистики (среднего значения)
bootstat = bootstrp(nBoot, bootfun, data); % Выполнение бутстрэп-анализа
% Вычисление доверительных интервалов
ci = vpa(prctile(bootstat, [100*alpha/2, 100*(1-alpha/2)]), 9);
% Вычисление среднего значения исходных данных
mean_data = mean(data);
fprintf('Оценка среднего значения: %.4f\n', vpa(mean(bootstat), 9));
fprintf('95% ДИ: [%.4f, %.4f]\n', vpa(ci(1), 9), vpa(ci(2), 9));
figure; hold on; % Визуализация результатов
plot(data, '*', 'DisplayName', 'Исходные данные'); % Исходные данные
plot([0,30], [mean_data,mean_data], '--', 'LineWidth', 1.5); % Нижняя граница
plot([0,30], [ci(1),ci(1)], '--', 'LineWidth', 1.5); % Нижняя граница ДИ
plot([0,30], [ci(2),ci(2)], '--', 'LineWidth', 1.5); % НВерхняя граница ДИ
hold off;
xlabel('Номер наблюдения'); ylabel('Значение');
title('Бутстрэп-анализ с доверительными интервалами');
legend('show');
```

Выходные данные, полученные в результате применения бутстрэп-метода:

>> Оценка среднего значения: 0.1118 95% доверительный интервал: [0.1112, 0.1124]

По результатам применения бутстрэп-метода в отношении значений пропускных способностей C_1 и C_2 построены 95% ДИ, которые идентичны тем, что представленные на рисунках 4.13 и 4.14.

Полученные экспериментальные данные для C_1 и C_2 , с помощью имитационной модели вместе с доверительным интервалом, соответствуют ожидаемым теоретическим значениям т.е. находятся выше границы, полученной при аналитическом расчете и отвечающей за минимальные допустимые значения исследуемых параметров. Кроме того, полученные в ходе имитационного моделирования для пропускных способностей C_1 и C_2 результаты подтверждают доказательство теорем 3 и 4, приведенных в разделе 3.4 главы 3 данной диссертационной работы, то есть: $C_2 = \gamma C_1$. Это говорит о правильности реализации модели, а также о корректном подборе методики измерений. Таким образом, результаты статистического анализа вместе с границами 95% ДИ подтверждают, что система работает стабильно и измерения выполнены точно, что является важным аргументом в поддержку надежности и корректности исследуемой модели.

Стоит отметить, что использование статистических методов анализа позволяет не только оценить точность и надежность полученных результатов, но и выявить возможные систематические погрешности, что является важным этапом при верификации и валидации имитационных моделей. Таким образом, построение доверительных интервалов и применение методов статистического анализа являются ключевыми инструментами для повышения достоверности выводов и обеспечения корректности модели. Валидация имитационной модели с помощью сравнения результатов моделирования и работы реальной системы проведена в главе 5 данной диссертационной работы при проведении экспериментальных исследований.

4.4 Выводы по главе

1. Представленное решение по оптимизации параметров двухканальной системы связи с использованием имитационной модели позволяет оценить

возможность применения алгоритмов кодирования видеоданных, основанных на схемах разделения данных, а также способствует выбору оптимальных пропускных способностей используемых каналов связи, что позволяет обеспечить стабильность передачи данных и уменьшить издержки на содержание такой системы

2. Проведена оценка достоверности результатов имитационного моделирования с помощью верификации модели и статистического анализа результатов. Полученные с помощью имитационной модели значения пропускных способностей каналов связи C_1 и C_2 соответствуют ожидаемым теоретическим, находятся выше (являются больше) значений параметров C_1 и C_2 вычисленных аналитически. Установлено, что расхождение между теоретическими значениями и результатами, полученными с помощью имитационной модели, в среднем не превышает 9%, что считается приемлемым и это объясняется тем, что аналитические расчеты часто выполняются в идеализированных условиях, где предполагается отсутствие внешнего влияния, например, трафика от других устройств. Поэтому, модель демонстрирует достаточную точность.

Для значения параметров C_1 и C_2 выполнено построение 95% ДИ для среднего при неизвестной дисперсии, а также с помощью бутстрэп-метода, получены одинаковые результаты. Определено, что для C_1 и C_2 ДИ – узкие, это означает, что истинное значение параметров с большой вероятностью находится в пределах вычисленных границ, что подтверждает надежность модели. В контексте имитационной модели двухканальной системы связи такой результат указывает на то, что модель корректно воспроизводит характеристики системы, и её результаты можно считать достоверными.

3. Проведённое исследование подтверждает, что программные средства Matlab/Simulink/SimEvents являются эффективными инструментами для моделирования двухканальной системы связи как системы с дискретными состояниями на основе теории массового обслуживания. SimEvents предоставляет специализированные блоки для моделирования очередей, серверов, каналов и маршрутизации, что позволяет анализировать производительность систем связи и

оптимизировать их параметры. Разработанная имитационная модель может использоваться при проектировании и исследовании двухканальных систем связи или включаться в состав программного обеспечения технических средств, имеющих два канала связи, где требуется применение методов динамической адаптации параметров каналов связи с использованием ГА, позволяющих оптимизировать передачу данных в условиях изменяющейся среды.

5 КОМПЛЕКС ПРОГРАММ И РЕЗУЛЬТАТЫ ЭКСПЕРИМЕНТАЛЬНЫХ ИССЛЕДОВАНИЙ РАСПРЕДЕЛЕННОЙ ПЕРЕДАЧИ ДАННЫХ В ДВУХКАНАЛЬНОЙ СИСТЕМЕ СВЯЗИ

В пятой главе представлено описание проблемно-ориентированного комплекса программ, предназначенного для распределённой передачи частей кадров видеоданных, освещены следующие аспекты: структура программного комплекса – описывается модульная архитектура, где каждая программа выполняет свою функцию в общей схеме передачи; схема распределения задач между модулями по подготовке кадров к отправке, принцип работы системы – кодирование, выбор пропускных способностей, распределенная передача; обсуждение полученных результатов – приводятся результаты тестирования системы, анализируются параметры системы.

5.1 Описание структуры и функционирования проблемно-ориентированного программного комплекса

Проблемно-ориентированный программный комплекс состоит из:

1) программ, реализующих описанные во второй главе данной диссертационной работы алгоритмы кодирования видеок кадров, основанные на разделении данных (АРДЧ; АРПК);

2) программы, выполняющей аналитические расчеты определения теоретических нижних границ интервалов пропускных способностей каналов связи на основании информации о размерах частей кадров, полученных при выполнении программ из п.1, и в соответствии с расчетными формулами, полученными в третьей главе данной диссертационной работы;

3) имитационной модели, описанной в четвертой главе данной диссертационной работы, осуществляющей расчет и оптимизацию пропускных способностей каналов связи на основании информации о размерах частей кадров, полученных при выполнении программ из п.1, а также на основании нижних границ интервалов (из программы п.2);

4) клиент-серверного приложения, выполняющего отправку и прием по двум

каналам связи частей кадров, полученных при выполнении программ из п.1;

5) стороннего программного обеспечения (ПО «NetLimiter»), выполняющего функции управления трафиком (контроль скорости приема и передачи данных).

Для проведения экспериментальных исследований используется стенд, представляющий из себя объединение из автоматизированных рабочих мест (АРМ) с двумя сетевыми картами на каждом и объединенных между собой в локальную вычислительную сеть по принципу точка-точка. В качестве АРМ используется две виртуальные машины в среде виртуализации Red Hat Virtualization [169]. Схема приведена на рисунке 5.1.

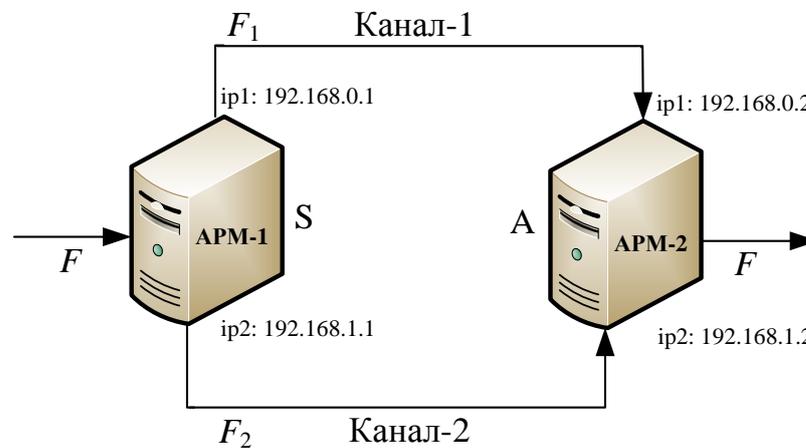


Рисунок 5.1 – Схема объединения двух АРМ

АРМ управляются операционными системами семейства Windows, имеют одинаковую архитектуру и не самую мощную конфигурацию: процессор Intel Xeon 2.39 GHz, ОЗУ 4 Гб, две сетевые карты на 10 Гбит, адресация указана на рисунке 5.1. В среде виртуализации можно задавать качество обслуживания хоста (QoS – quality of service), тем самым выставить желаемые ограничения скорости передачи данных, что, например, может заменить использование стороннего ПО «NetLimited». На АРМ-1 размещены: программа «Демультимплексор/Мультимплексор», реализующая разделение (объединение) кадров (п. 1); программа «Расчет», выполняющая аналитические расчеты (п. 2); программа «Оптимизация» имитационного моделирования (имитационная модель) (п. 3); программа «Сервер» клиент-серверного приложения (п. 4), стороннее ПО «NetLimited» (п. 5).

На АРМ-2 размещены: программа «Демультимплексор/Мультимплексор», реализующая объединение (разделение) кадров (п. 1); две программы «Клиент» клиент-серверного приложения (п. 4); стороннее ПО «NetLimited» (п. 5).

Порядок проведения работ по оценке синхронности поступления частей разделенных видеоданных состоит из следующих этапов:

1. На АРМ-1 при помощи программы «Демультимплексор/Мультимплексор» выполняется разделение на части поступающего на обработку несжатого потока видеоданных на кадры. Для проведения экспериментальных исследований с помощью ПО VirtualDub [170] предварительно подготовлены видеофайлы из несжатых изображений различного формата (LQ, SD, HD, FullHD, 2K).

2. После выполнения процедуры разделения кадров и на основании информации о размерах частей кадров, с помощью программы «Расчет» выполняется аналитическое определение пропускных способностей каналов связи: C_1^a , C_2^a .

3. С помощью программы «Оптимизация» выполняется определение пропускных способностей каналов связи, в соответствии с имитационной моделью системы связи. Выполняется $n = 30$ запусков имитационной модели, формируются последовательности для пропускных способностей каналов связи и строятся 95% ДИ, выбираются соответствующие значения для C_1^u и C_2^u попадающие в построенные ДИ.

4. С помощью экспертной оценки, основанной на ретроспективных данных, профессиональной интуиции, на основании объемов передаваемых данных, выбираются экспертные оценки пропускных способностей $C_1^э$ и $C_2^э$.

5. С учетом пунктов 2-4 для проведения экспериментов имеется три набора значений: (C_1^a, C_2^a) , (C_1^u, C_2^u) , $(C_1^э, C_2^э)$. В целях дальнейшего сравнения этих наборов, выполняется поочередное их выставление в ПО «NetLimiter» (на АРМ-2).

6. С помощью программы «Сервер» на АРМ-1, с учетом выставленных ограничений пропускных способностей для каналов связи (п.5), выполняется отправка частей видеокадров по разным каналам на АРМ-2.

7. С помощью программы «Клиент» выполняется прием частей кадров и оценивается их синхронная доставка при помощи сопоставления времени окончания приема данных.

8. При помощи программы «Демультимплексор/Мультимплексор» выполняется объединение частей видеокадров.

Передача параметров в стороннее ПО «NetLimiter» автоматически невозможна, в ходе проведения экспериментов значения пропускных способностей задаются в ручном режиме. Имеется возможность задавать ограничения как для исходящего соединения, так и для входящего. В случае разработки собственного отдельного программного модуля или включение подобной процедуры по ограничению скорости передачи данных (пропускных способностей) в разработанное клиент-серверное приложение данный процесс в дальнейшем можно автоматизировать.

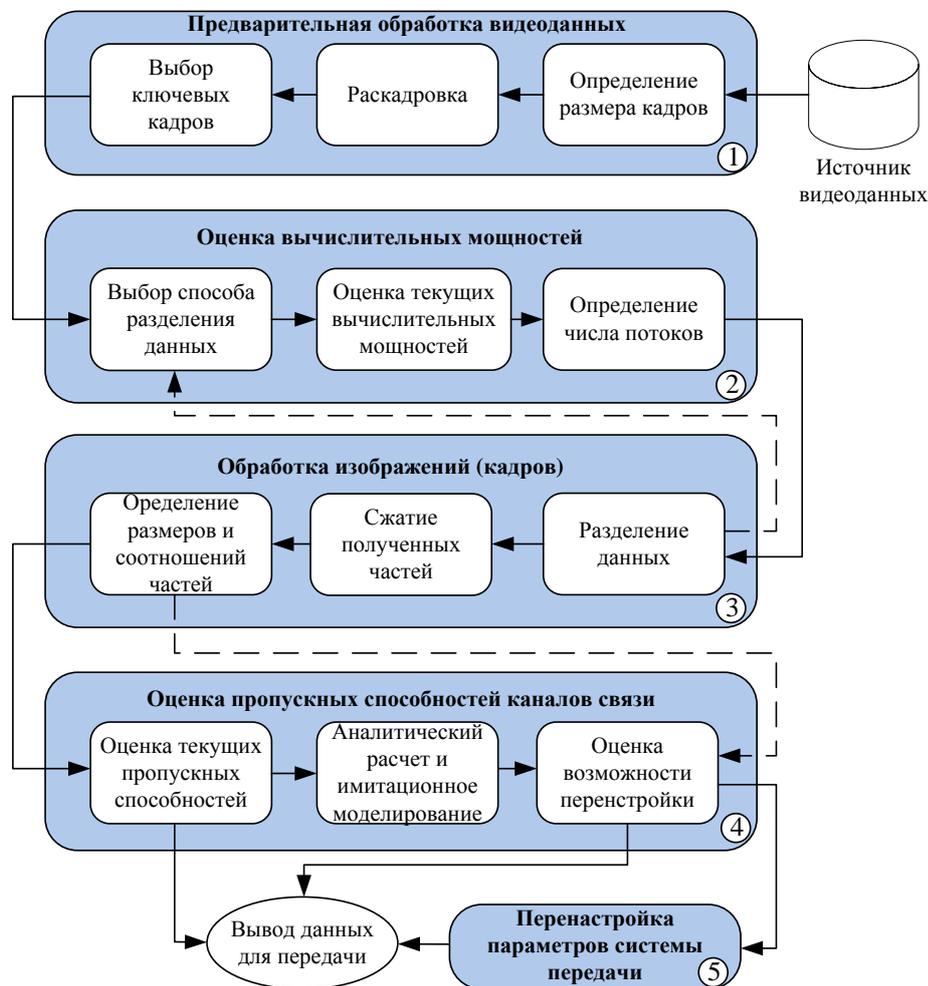


Рисунок 5.2 – Схема подготовки кадров видеоданных на АРМ-1

На рисунке 5.2 приведена схема подготовки кадров видеоданных на АРМ-1 для передачи по двум каналам связи, учитывающая разделение кадров на части при условии выполнения многопоточного их преобразования, определение размеров

частей, оценку текущих пропускных способностей, проведение аналитического расчета и имитационного моделирования параметров системы, определение необходимости перенастройки параметров системы передачи данных.

В описанных во второй главе данной диссертационной работы методах кодирования используются одинаковые процедуры разбиения видеопотока на кадры:

```

void AviToBmp()
{AVISTREAMINFO    psi;
PAVISTREAM        pavi;
PGETFRAME        pgf;
int               width, height;
char              *pdata;
AnsiString InFile=MainForm->OpenDialog1->FileName;
if(AVISTreamOpenFromFile(&pavi,InFile.c_str(), streamtypeVIDEO, 0, OF_READ, NULL)
!= 0)
    {ShowMessage("Ошибка открытия файла"); return;}
else { if (!DirectoryExists(ExtractFilePath(Application->ExeName)+"\\frames"))
    CreateDir(ExtractFilePath(Application->ExeName)+"\\frames");
    AVIStreamInfo(pavi, &psi, sizeof(psi));
    width = psi.rcFrame.right-psi.rcFrame.left;
    height = psi.rcFrame.bottom-psi.rcFrame.top;
    lastframe = AVIStreamLength(pavi);
    pgf = AVIStreamGetFrameOpen(pavi, NULL);
    LPBITMAPINFOHEADER pBitmapInfoHeader; LPBYTE pData;
    fprintf(keys,IntToStr(width).c_str()+"|"+IntToStr(height).c_str()+"\n");
    for ( long i = 0; i < AVIStreamLength(pavi); i++ )
        {Graphics::TBitmap *bitmap = new Graphics::TBitmap();
        bitmap->PixelFormat = pf24bit;
        bitmap->Width = width; bitmap->Height = height;
        HDC hdc = bitmap->Canvas->Handle;
        pBitmapInfoHeader = (LPBITMAPINFOHEADER)AVIStreamGetFrame(pgf,i);
        pData = (LPBYTE)pBitmapInfoHeader + (int)pBitmapInfoHeader->biSize +
        (int)pBitmapInfoHeader->biClrUsed*sizeof(RGBQUAD);
        StretchDIBits(hdc, 0, 0, bitmap->Width, bitmap->Height, 0, 0, width,
        height, pData, LPBITMAPINFO(pBitmapInfoHeader), DIB_RGB_COLORS,
        SRCCOPY);
        bitmap->SaveToFile("\\frames\\"+IntToStr(i)+".bmp"); }
    AVIStreamGetFrameClose(pgf); AVIStreamRelease(pavi); AVIFileExit();
}
}

```

Разделение кадров на части выполняется в соответствии с приведенными во

второй главе алгоритмами. При обработке поступающих кадров используется класс TThread среды разработки C++ Borland, позволяющий использовать несколько потоков обработки данных. Основные фрагменты кода приведены ниже. АДЧ:

```

for (int x = 0; x <=bmp->Width-1; x++)
    {
        s1=IntToBin(scanLine[x].rgbtRed).SubString(25,8);
        s2=IntToBin(scanLine[x].rgbtGreen).SubString(25,8);
        s3=IntToBin(scanLine[x].rgbtBlue).SubString(25,8);
        Sobinv=s1.SubString(8,1)+s2.SubString(8,1)+s3.SubString(8,1)+
        s1.SubString(7,1)+s2.SubString(7,1)+s3.SubString(7,1)+
        . . .
        s1.SubString(1,1)+s2.SubString(1,1)+s3.SubString(1,1);
        a[n]=StrToFloat("0,"+Sobinv.SubString(1,4));
        a[n+1]=StrToFloat("0,"+Sobinv.SubString(5,4));
        a[n+2]=StrToFloat("0,"+Sobinv.SubString(9,4));
        a[n+3]=StrToFloat("0,"+Sobinv.SubString(13,4));
        a[n+4]=StrToFloat("0,"+Sobinv.SubString(17,4));
        a[n+5]=StrToFloat("0,"+Sobinv.SubString(21,4));
        n=n+6;
    }
    . . .
for (int k=0; k<bmp->Width*3;k++)
    {summa=summa+a[k];}
double sr=summa/(bmp->Width*3);
fprintf(sred,FloatToStr(sr).c_str());
for (int k=0; k<bmp->Width*3;k++)
    {fprintf(ai,FloatToStr(a[k]).c_str()); a[k]=sr-a[k];
    }
    . . .
for (int y=0; y<w=bmp->Width*3; y++)
    {zn=-a[w-1]+2*a[y]-a[y+1];
    . . .
    zn=-a[y-1]+2*a[y]-a[y+1];
    . . .
    zn=-a[y-1]+2*a[y]-a[0];
    }

```

APIK:

```

void bmptopix(int inFN)
{
bmp->LoadFromFile("\\frames\\"+IntToStr(inFN)+".bmp");
bmp->PixelFormat = pf24bit;
String sbit;
for (int y =0; y <=bmp->Height-1; y++)
    {TRGBTriple* scanLine = (TRGBTriple*)bmp->ScanLine[y];
    for (int x = 0; x <=bmp->Width-1; x++)
        {String str1=IntToBin(scanLine[x].rgbtRed).c_str
        String str2=IntToBin(scanLine[x].rgbtGreen).c_str();
        String str3=IntToBin(scanLine[x].rgbtBlue).c_str();
        sbit=str1.SubString(25,8)+str2.SubString(25,8)+str3.SubString(25,8);
        fprintf(pixels,sbit.c_str());
        }
    }
    . . .
void razdelenie(int nt)
{FILE* razdel = fopen ("razdel","w");
long int sum=0;
for (int i=0; i<nt+1; i++)
    {if (i==0)
    {A1=pixelbuf.SubString(1,StrToInt(kolns->Strings[i])).c_str();
    fprintf(razdel,A1.c_str());
    . . .
    printf(razdel,pixelbuf.SubString(sum+1,StrToInt(kolns->Strings[i])).c_str());
    . . .
    fprintf(razdel,pixelbuf.SubString(sum+1,pixelbuf.Length()-sum).c_str());
    . . .
    }
}
}

```

Отправка частей разделенных видеок кадров осуществляется с помощью клиент-серверного приложения. С помощью программы «Сервер» выполняется передача частей кадров по двум каналам связи в соответствующие программы «Клиент». Передача данных осуществляется с помощью компонентов среды разработки C++ Borland (RAD Studio) TClientSocket, TClientServer поддерживавших протокол обмена TCP/IP. В случае реализации более быстрого, но менее надежного протокола обмена данными, как UDP, при реализации клиент-серверного приложения можно воспользоваться компонентами из пакета Indy

(Internet Direct). В свойствах компонента TClientSocket задаются соответствующие параметры подключения (ip-адрес сервера, порт подключения, ip-адрес хоста). В свойствах компонента TClientServer задаются используемые сетевые порты для получения данных от программы «Сервер». Ниже приведены фрагменты исходного кода для клиент-серверного приложения.

Фрагмент процедуры отправки данных в программе «Сервер»:

```
Server1->Socket->Connections[0]->SendText("file#" + File1 + "#" + IntToStr(MS1->Size) + '#');
MS1->Position = 0 ;
P1 = MS1->Memory;
Size1 = Server1->Socket->Connections[0]->SendBuf(P1, MS1->Size);
Mem1->Lines->Add(IntToStr(Size1) + " из " + IntToStr(MS1->Size) + " IP 1");

Server2->Socket->Connections[0]->SendText("file#" + File2 + "#" + IntToStr(MS2->Size) + '#');
MS2->Position = 0;
P2 = MS2->Memory;
Size2 = Server2->Socket->Connections[0]->SendBuf(P2, MS2->Size);
Mem1->Lines->Add(IntToStr(Size2) + " из " + IntToStr(MS2->Size) + " IP 2");
```

Фрагмент процедур чтения и приема данных в программе «Клиент»:

```
void __fastcall TForm1::Client1Read(TObject *Sender, TCustomWinSocket *Socket)
{
  AnsiString Rtext1;
  Rtext1 = Client1->Socket->ReceiveText();
  if(Receive1 == true) {Write1(Rtext1);}
  else {if(Rtext1.SubString(0, Rtext1.Pos("#")-1) == "file")
    Rtext1.Delete(1, Rtext1.Pos("#"));
    Name = Rtext1.SubString(0, Rtext1.Pos("#")-1);
    FileName1 = Name.SubString(Name.LastDelimiter("\\")+1, Name.Length());
    Rtext1.Delete(1, Rtext1.Pos("#"));
    Size1 = StrToInt(Rtext1.SubString(0, Rtext1.Pos("#")-1));
    Rtext1.Delete(1, Rtext1.Pos("#"));
    Receive1 = true;
  }
}
```

```

void Writel(AnsiString Text1)
{
if(MS1->Size < Size1{
MS1->Write(Text1.c_str(),Text1.Length()); }
if(MS1->Size == Size1)
{
Receive1 = false;
MS1->Position = 0;
Form1->Client1->Socket->SendText("end1");
MS1->SaveToFile("Downloads_ip1\\"+FileName1);
MS1->Clear() ; Size1 = 0 ;
}
}
}

```

5.2 Формирование набора кодированных видеок кадров для распределенной передачи

На вход алгоритмов (см. глава 2) по разделению кадров подаются предварительно подготовленные в ПО VirtualDub видеофайлы из несжатых изображений формата (LQ, SD, HD, FullHD, 2K). Видеофайлы содержат запись длиной в 1 секунду, состоящую из 60 кадров, то есть FPS (frame per second) 60 кадров в секунду. Стоит отметить, что для созданий непрерывного движения достаточно 24-30 кадров в секунду [171]. Видеофайлы содержат одну и ту же запись, но в разных форматах качества. Пример одного из кадров представлен на рисунке 5.3.



Рисунок 5.3 – Пример кадра

В результате разделения несжатых изображений в соответствии с алгоритмами приведенными в главе 2, получены соответствующие части кадров, пропорции которых приведены в таблице 5.1.

Таблица 5.1 – Результаты разделения кадров.

Формат видеоданных	Исходный размер (бит)	АРДЧ		АРПК	
		Меньшая часть (бит)	Большая часть (бит)	Меньшая часть (бит)	Большая часть (бит)
LQ	5529600	1105920	4423680	449581	5080019
SD	8294400	1658880	6635520	674372	7620023
HD	22118400	4423680	17694720	1798326	20320074
FullHD	49766400	9953280	39813120	4046234	45720166
2K	53084160	10616832	42467328	4315983	48768177

В таблице 5.2 приведены пропорции и проценты соотношения для полученных частей кадров с помощью двух алгоритмов разделения. Так как разделение осуществляется в постоянном соотношении, то для всех форматов видеоданных будет одна и та же пропорция частей кадров.

Таблица 5.2 – Соотношение частей кадров.

АРДЧ		АРПК	
Большая/Меньшая	% отношения	Большая/Меньшая	% отношения
4	25%	11,24	8,85%

Так как в видеофайле содержится 60 кадров, то после разделения их на части для передачи формируются потоки F_1 и F_2 , информация размере которых приведена в таблице 5.3.

Таблица 5.3 – Информация размере потоков F_1 и F_2

Формат видеоданных	АРДЧ		АРПК	
	F_1 , Гбит/с	F_2 , Гбит/с	F_1 , Гбит/с	F_2 , Гбит/с
LQ	0,0663552	0,2654208	0,02697489	0,30480111
SD	0,0995328	0,3981312	0,04046236	0,45720165
HD	0,2654208	1,0616832	0,10789959	1,21920441
FullHD	0,5971968	2,3887872	0,24277408	2,74320992
2K	0,6370099	2,5480397	0,25895902	2,92609058

Для пропускных способностей каналов связи должны выполняться условия: $C_1 \geq F_1$, $C_2 \geq F_2$. Входящий в систему поток заявок имеет вероятностный закон поступления (пуассоновский поток заявок), следовательно, C_1^a , C_2^a могут быть рассчитаны по формуле (3.32), результаты расчета приведены в таблице 5.4.

Как описано выше, пропускные способности C_1^u , C_2^u выбираются из результатов имитационного моделирования входящих в вычисленный ДИ. На рисунках 5.4–5.13. приведены графики работы имитационной модели для каждого из алгоритмов разделения кадров и форматов видеоданных.

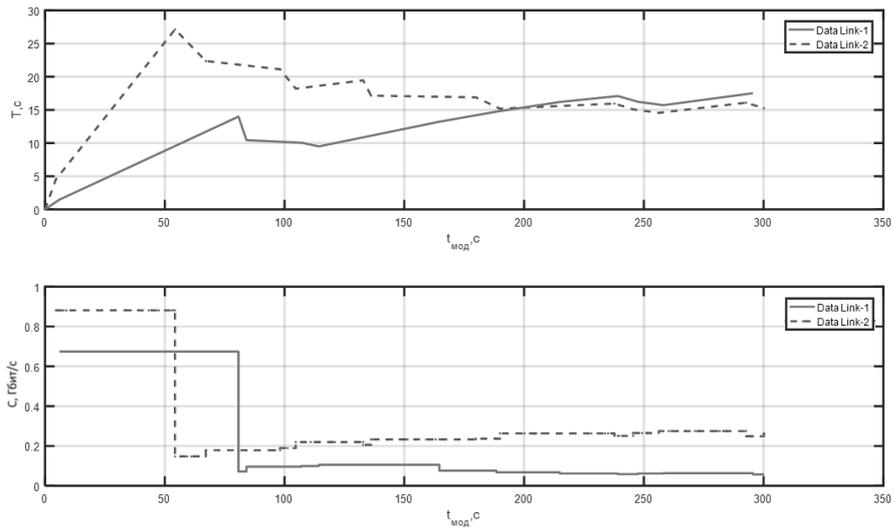


Рисунок 5.4 – Результат нахождения C_1'' , C_2'' (АРДЧ, формат – LQ)

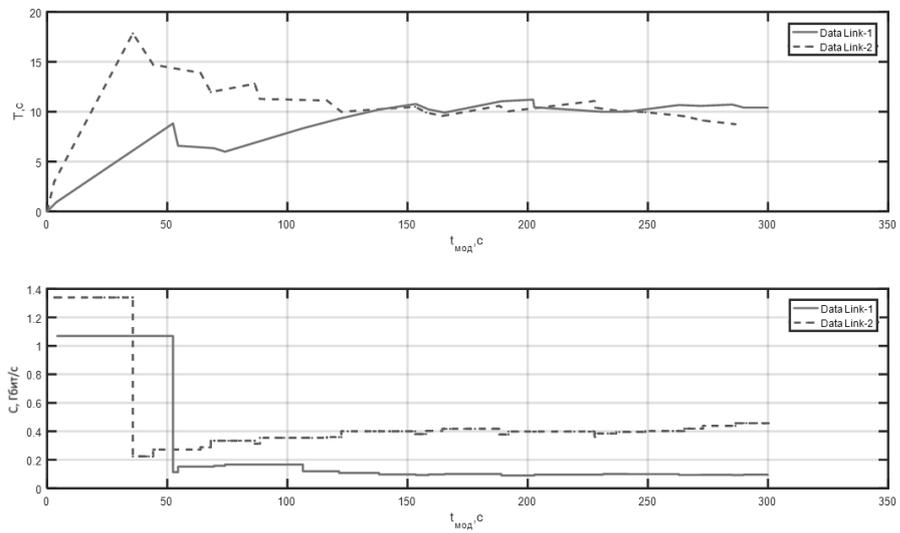


Рисунок 5.5 – Результат нахождения C_1'' , C_2'' (АРДЧ, формат – SD)

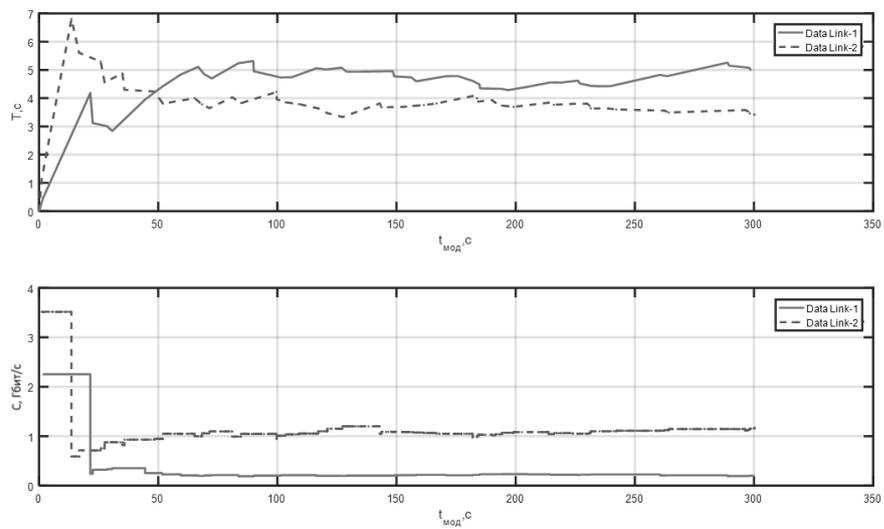


Рисунок 5.6 – Результат нахождения C_1'' , C_2'' (АРДЧ, формат – HD)

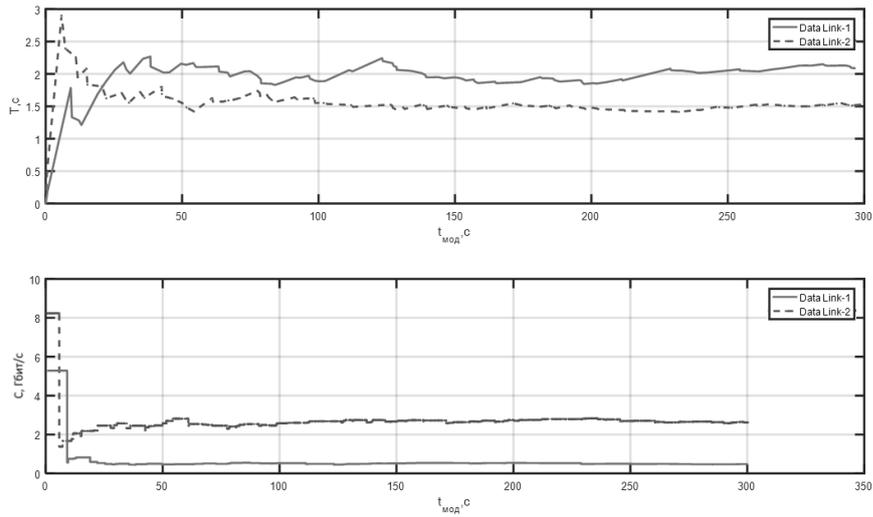


Рисунок 5.7 – Результат нахождения C_1^u, C_2^u (АРДЧ, формат – FHD)

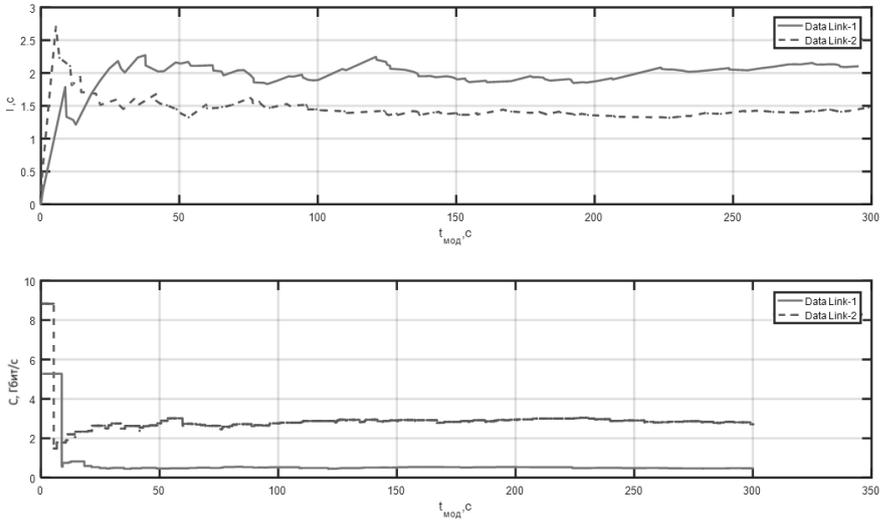


Рисунок 5.8 – Результат нахождения C_1^u, C_2^u (АРДЧ, формат – 2К)

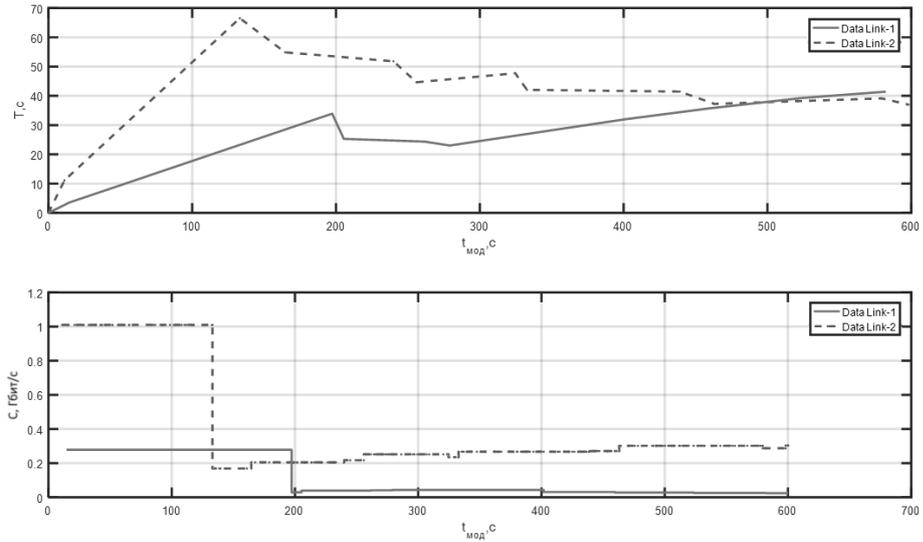


Рисунок 5.9 – Результат нахождения C_1^u, C_2^u (АРПК, формат – LQ)

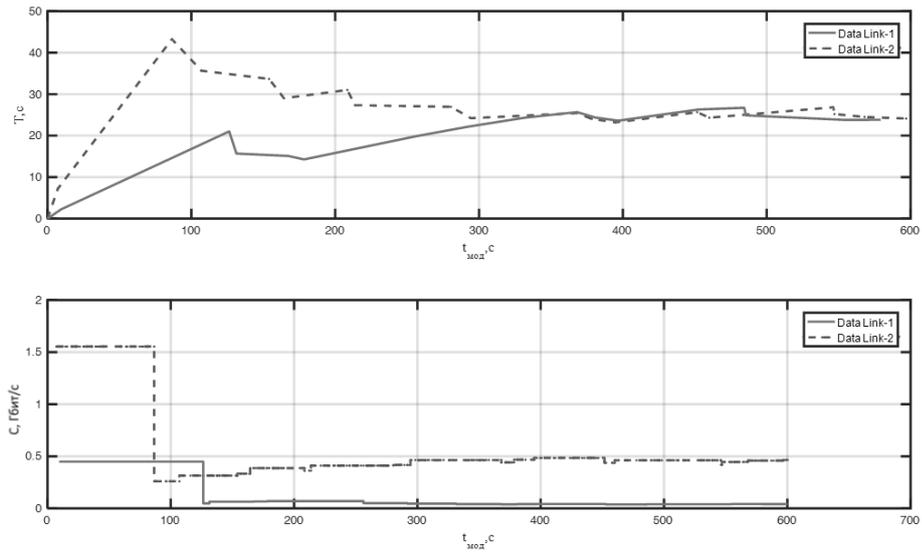


Рисунок 5.10 – Результат нахождения C_1^u , C_2^u (АРПК, формат – SD)

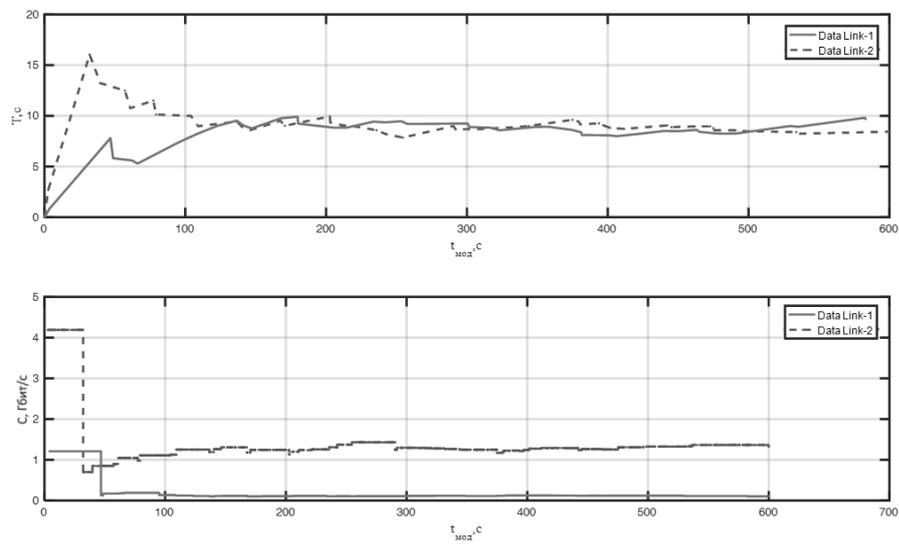


Рисунок 5.11 – Результат нахождения C_1^u , C_2^u (АРПК, формат – HD)

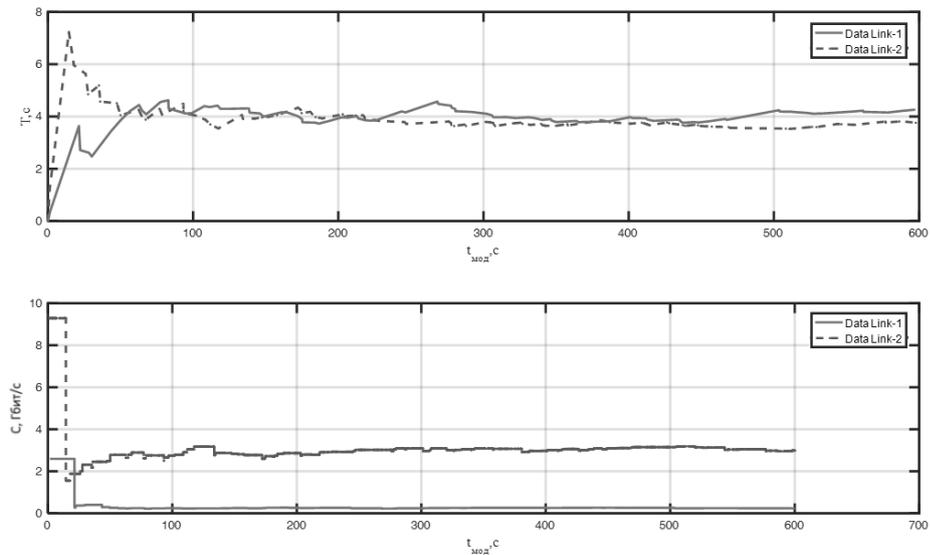


Рисунок 5.12 – Результат нахождения C_1^u , C_2^u (АРПК, формат – FHD)

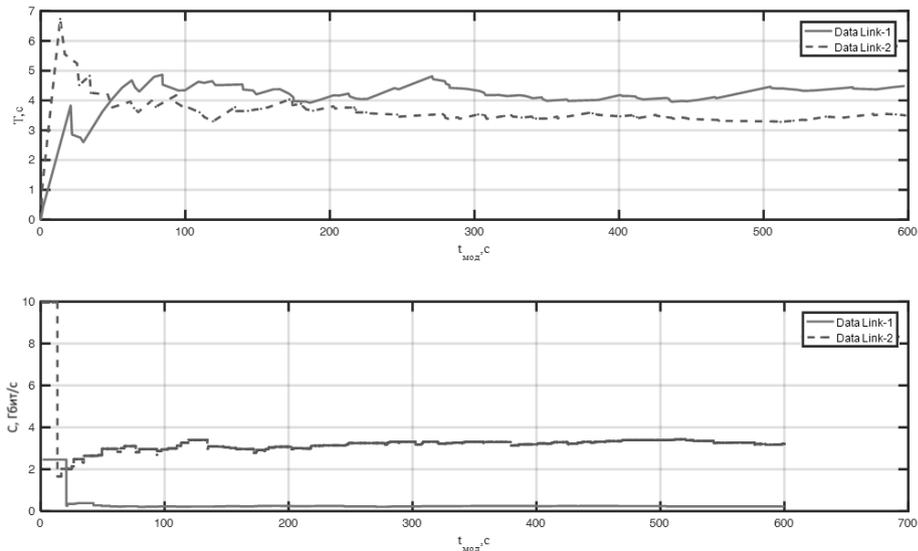


Рисунок 5.13 – Результат нахождения C_1^u , C_2^u (АРПК, формат – 2К)

Оценки пропускных способностей $C_1^э$, $C_2^э$ определяются экспертом методом подбора на основе комплексного анализа ретроспективных данных, накопленного профессионального опыта и статистического анализа объемов передаваемых данных. Значения C_1^a , C_2^a , полученные в результате аналитического расчета, значения C_1^u , C_2^u , полученные при имитационном моделировании, и значения, полученные в результате экспертной оценки $C_1^э$, $C_2^э$ приведены в таблице 5.4.

Таблица 5.4 – Набор экспериментальных данных.

Формат видеоданных	АРДЧ			АРПК		
	$C_1^a; C_2^a$ Гбит/с	$C_1^u; C_2^u$ Гбит/с	$C_1^э; C_2^э$ Гбит/с	$C_1^a; C_2^a$ Гбит/с	$C_1^u; C_2^u$ Гбит/с	$C_1^э; C_2^э$ Гбит/с
LQ	0,067355; 0,269421	0,068123 0,272492	0,09 0,31	0,027975; 0,314438	0,029015; 0,326124	0,04; 0,4
SD	0,101352; 0,405411	0,102124; 0,408496	0,15 0,5	0,041202; 0,463114	0,042127; 0,473507	0,05; 0,5
HD	0,268395; 1,073581	0,272329; 1,089314	0,3 1,5	0,109112; 1,226416	0,109808; 1,234246	0,2; 1,5
FullHD	0,601656; 2,406627	0,625021; 2,500084	0,8 2,8	0,244594; 2,749237	0,246121; 2,766401	0,3 2,8
2K	0,641621; 2,566481	0,648512; 2,594048	0,9 3,0	0,260839; 2,931831	0,264211; 2,969732	0,3; 3,0

Таким образом, в таблице 5.4 сформированы наборы данных для каждого из форматов видеоданных.

5.3 Проведение экспериментальных исследований распределённой передачи видеоданных

Порядок проведения экспериментальных исследований состоит из следующих этапов:

1. Значения пропускных способностей каналов связи из таблицы 5.4 поочередно выставляются ПО «NetLimiter», и с помощью приложения «Сервер» на приложения «Клиент» (192.168.0.2, 192.168.1.2) выполняется одновременная отправка сформированных в результате разделения частей видеоданных (формируя потоки F_1 и F_2).

2. После завершения получения данных в приложении «Клиент» отображается время (T^1 и T^2) затраченное на прием этих данных с миллисекундной точностью. Следует отметить, что на АРМ-1 и АРМ-2 системное время синхронизировано.

Для каждой пары пропускных способностей (C_1^a, C_2^a) , (C_1^u, C_2^u) , (C_1^g, C_2^g) (каждого из алгоритмов и, соответственно, для каждого формата качества видеоданных) эксперимент проводится $n = 30$ раз, и формируются последовательности из результатов эксперимента: $T_i^{1a}, T_i^{2a}, T_i^{1u}, T_i^{2u}, T_i^{1g}, T_i^{2g}, i = \overline{1, 30}$.

3. С помощью бутстрап-метода, код для Matlab которого приведен в разделе 4.3 главы 4 данной диссертационной работы, выполняется бутстрапирование каждой полученной последовательности $T_i^{1a}, T_i^{2a}, T_i^{1u}, T_i^{2u}, T_i^{1g}, T_i^{2g}, i = \overline{1, 30}$ для построения 95% ДИ. Среди значений из каждой пар последовательностей, попавших в ДИ, выбираются такие, которые дают минимальные значения $\Delta T^a = |T_i^{1a} - T_i^{2a}| \rightarrow \min$, $\Delta T^u = |T_i^{1u} - T_i^{2u}| \rightarrow \min$, $\Delta T^g = |T_i^{1g} - T_i^{2g}| \rightarrow \min$, данные значения приведены в таблице 5.5.

Ограничение пропускных способностей осуществляется с помощью следующих настроек в ПО «NetLimiter», приведённых на рисунке 5.14. Возможно задать ограничения как для входящих данных, так и для исходящих. Так как оценка времени получения выполняется на приложении «Клиент», то ПО «NetLimiter», задаются ограничения на входящий трафик.

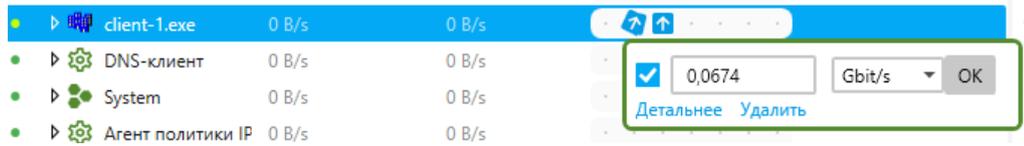
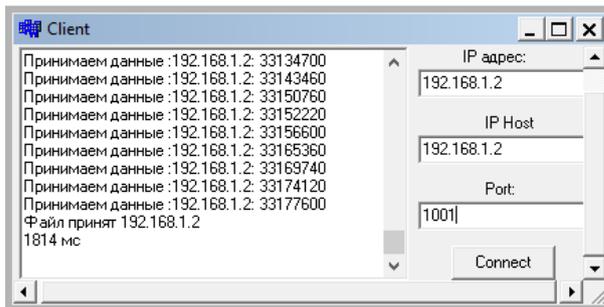
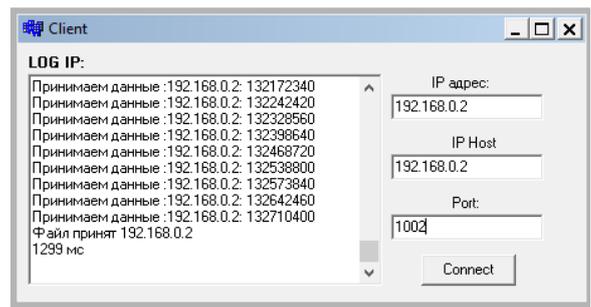


Рисунок 5.14 – Ограничение пропускных способностей с помощью ПО «NetLimiter»

На рисунке 5.15 приведены результаты получения частей видеоданных приложением «Клиент».



а)



б)

Рисунок 5.15 – Информация о результатах получения частей:

а) первый канал; б) второй канал

На рисунке 5.16 приведены результаты отправки частей видеоданных приложением «Сервер».

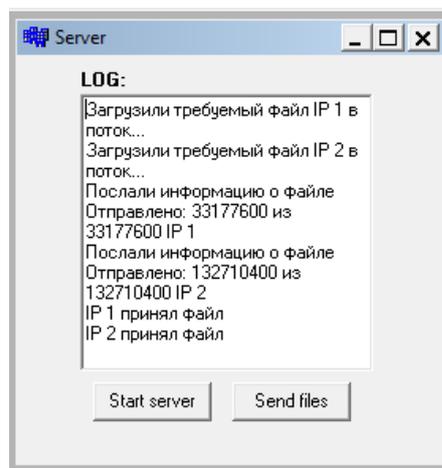


Рисунок 5.16 – Информация об отправке сервером файлов:

а) первый канал; б) второй канал

Таблица 5.5 – Расхождение времени получения данных.

Формат видеоданных	АРДЧ			АРПК		
	ΔT^a , мс	ΔT^u , мс	ΔT^o , мс	ΔT^a , мс	ΔT^u , мс	ΔT^o , мс
LQ	515	321	2114	374	301	1982
SD	471	301	1874	401	340	2143
HD	441	287	3212	398	299	1793
FullHD	511	311	2341	412	317	2004
2K	482	295	3143	441	332	1937

Из данных, приведённых в таблице 5.5 видно, что наименьшее расхождение времени получения частей видеоданных удается достичь при пропускных способностях каналов связи, полученных с помощью имитационного моделирования. На рисунках 5.17 и 5.18 приведены графики сравнения результатов времени расхождения получения частей видеоданных по каналам связи, для первого и второго алгоритмов соответственно. Видно, что идеальной синхронизации достичь не представляется возможным. Расхождение между временными интервалами между моментами получения частей видеоданных по каналам связи, полученными с помощью аналитического расчета и с помощью имитационной модели для АРДЧ в среднем для всех форматов качества видеоданных составляет – 37%, для АРПК – 22%. А оценка эксперта не позволяет достичь приемлемых результатов.

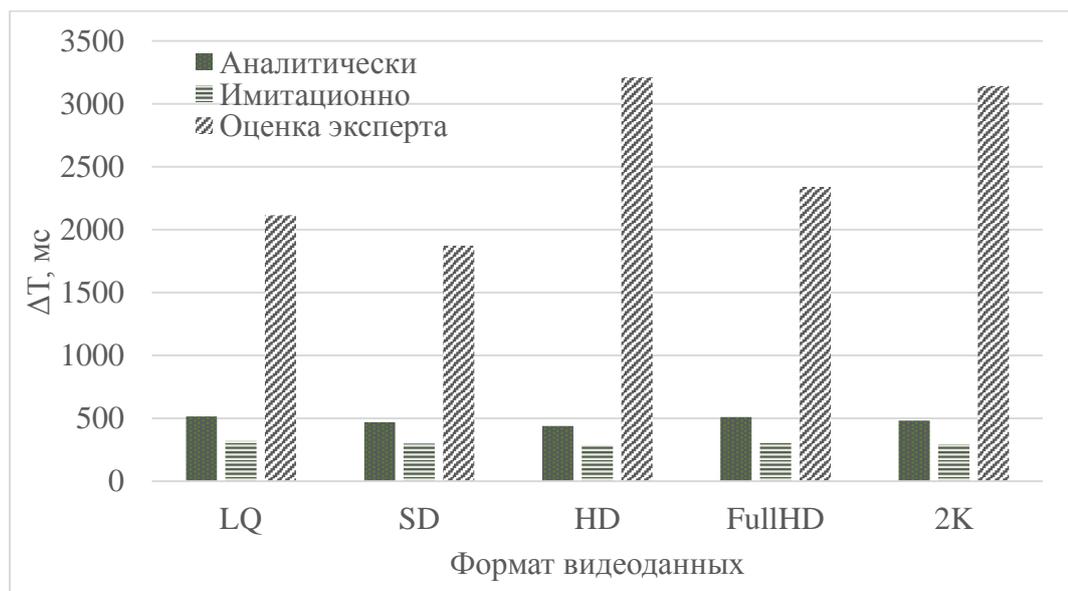


Рисунок 5.17 – Временные интервалы между моментами получения частей видеоданных по каналам связи (АРДЧ)

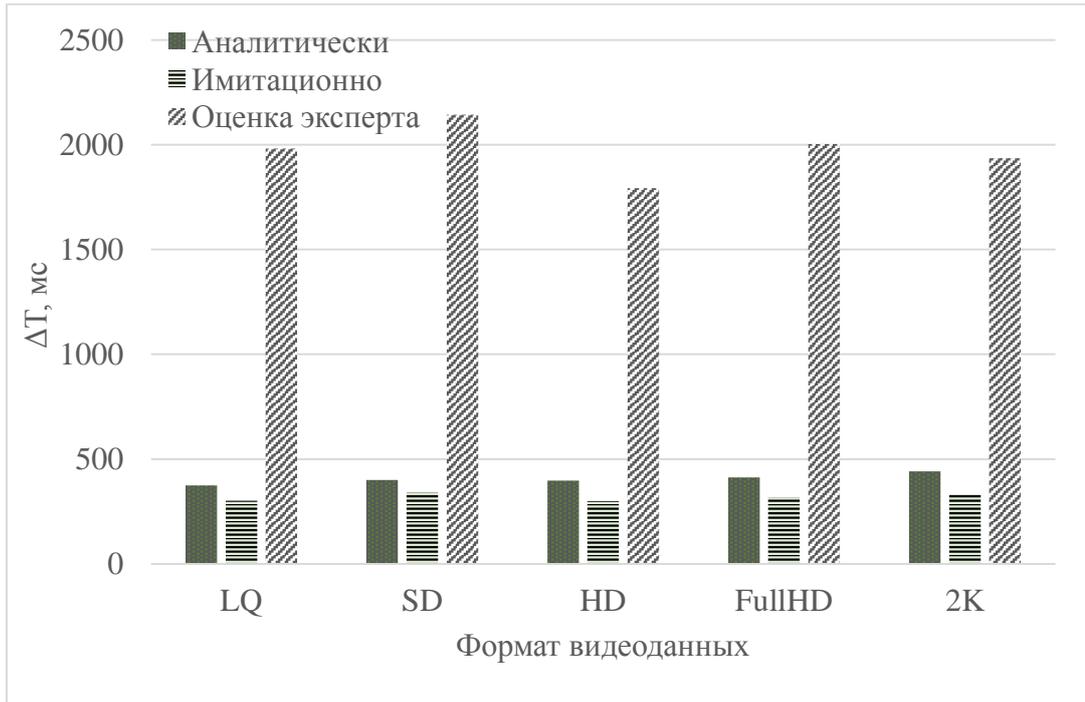


Рисунок 5.18 – Временные интервалы между моментами получения частей видеоданных по каналам связи (АРПК)

На рисунках 5.19, 5.20 для обоих алгоритмов разделения данных приведено сравнение (целевых функций) финансовых затрат, приходящихся на содержание двухканальной системы связи в соответствии с пропускными способностями, приведёнными в таблице 5.4.

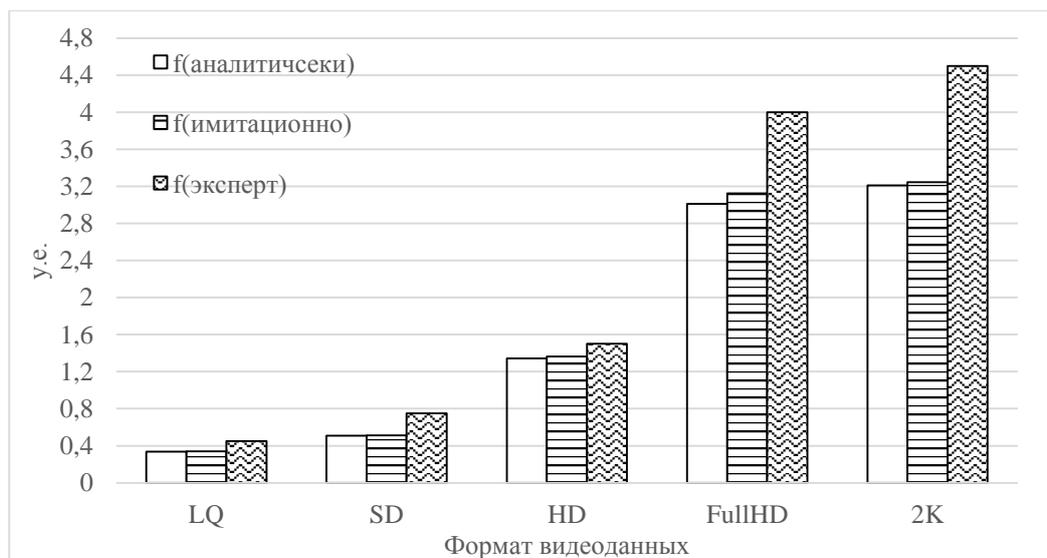


Рисунок 5.19 – Сравнение целевых функций при аналитическом решении, имитационном моделировании и экспертной оценке (АРДЧ)

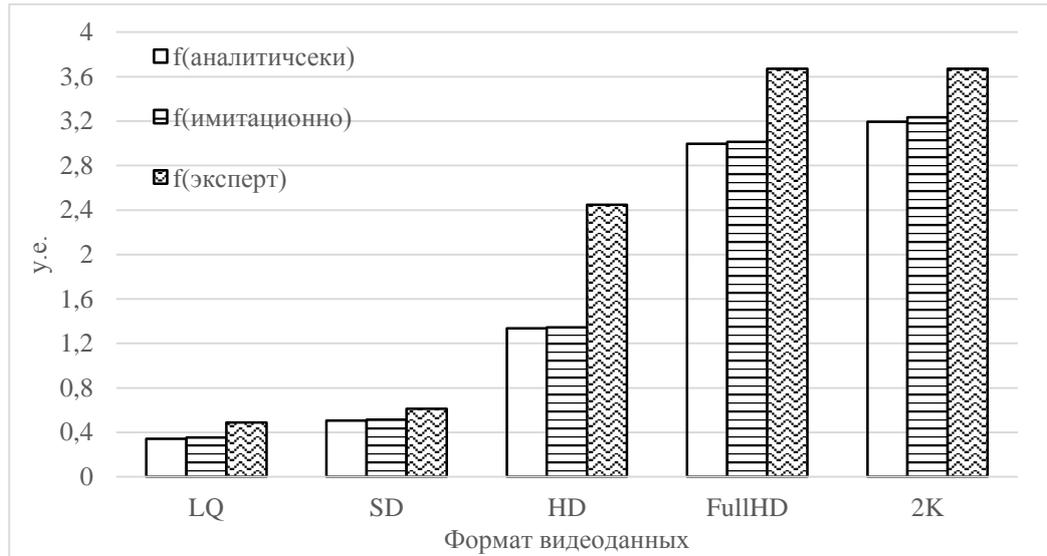


Рисунок 5.20 – Сравнение целевых функций при аналитическом решении, имитационном моделировании и экспертной оценке (АРПК)

Из рисунков 5.19 и 5.20 видно, что привлечение аналитических расчетов и имитационного моделирования позволяет добиться снижения финансовых затрат и подобрать такие значения пропускных способностей каналов связи, которые были бы достаточны для передачи заданных объемов трафика. Экспериментальные исследования показали, что для значений пропускных способностей, полученных с помощью аналитического расчета, разница времени передачи частей видеоданных по двум каналам связи больше чем для значений, полученных при имитационном моделировании. Это объясняется тем, что имитационная модель позволяет оценить наличие возможных задержек в системе передачи данных. Тем самым подтверждается валидность имитационной модели, то есть модель адекватно отражает поведение реальной системы, для которой она разработана, и её результаты могут быть использованы для принятия решений.

Полученные аналитическим расчётами данные можно использовать для определения минимально необходимых пропускных способностей. Для обоих алгоритмов разделения установлено, что разница между значениями целевых функций, полученными аналитическим расчётом и имитационным моделированием, составляет в среднем 1,7%, это означает, что удорожание системы связи при выборе пропускных способностей по результатам

имитационного моделирования не превышает 2%. Кроме того, выявленное расхождение во времени получения частей видеоданных при пропускных способностях, определённых имитационной моделью, считается приемлемым и в ряде случаев не превышает 300 мс. Стоит отметить, что в соответствии с рекомендациями ITU-T Recommendation G.114 [172] время задержки при передаче видео в режиме реального времени не должно превышать 200 мс, поэтому, чтобы сгладить и уменьшить воспринимаемую задержку для конечного пользователя возможно применение буферизации данных (синхронизирующих очередей). Абсолютная синхронизация передачи данных по двум каналам связи практически недостижима из-за множества факторов, обусловленных как физическими ограничениями, так и особенностями сетевого оборудования и протоколов. Основные причины включают: задержки распространения сигнала (физические расстояния между узлами сети приводят к неизбежным задержкам, так как сигнал распространяется со скоростью, меньшей скорости света); джиттер (небольшие случайные колебания во времени передачи возникают из-за вариаций в обработке сигналов, переключении коммутаторов и маршрутизаторов, что затрудняет достижение точной синхронизации); несовершенство тактовых генераторов (часы в сетевых устройствах имеют свою погрешность (дрейф), что приводит к накоплению временных расхождений между различными узлами); обработка и задержки в оборудовании (время, необходимое для обработки пакетов, маршрутизации данных, вносит дополнительные вариации во временные метки и задержки передачи); протоколы синхронизации: (даже современные протоколы (например, IEEE 1588 – Precision Time Protocol [173] или NTP [174]) не могут обеспечить абсолютную синхронизацию, а лишь достигают очень высокой точности, близкой к идеалу, но с небольшими погрешностями). Таким образом, совокупность этих факторов делает невозможным достижение полной, идеальной синхронизации, однако минимизация временной разницы до уровня обеспечивающего бесперебойную работу двухканальных систем связи все же возможна, что подтверждено экспериментально.

5.4 Выводы по главе

1. Представлено описание проблемно-ориентированного комплекса программ, предназначенных для распределённой передачи частей кадров видеоданных. В данной главе освещены следующие аспекты: структура программного комплекса – описывается модульная архитектура системы, каждая программа выполняет свою функцию в общей схеме передачи; схема распределения задач между модулями по подготовке кадров к отправке, принцип работы системы – кодирование, выбор пропускных способностей, распределённая передача; обсуждение полученных результатов – приводятся результаты тестирования системы, анализируются параметры системы, такие как задержка передачи, объем переданных данных.

2. В результате экспериментальных исследований установлено, для пропускных способностей каналов связи, найденных с помощью имитационной модели, расхождение времени получения частей видеоданных является наименьшим (меньше чем при аналитическом расчете и экспертном подборе), приемлемым, и в ряде случаев не превышает 300 мс.

3. Применение пропускных способностей, определённых с помощью имитационного моделирования, приводит к увеличению затрат на систему связи не более чем на 2% по сравнению с использованием значений, полученных аналитическими расчётами. Однако этот подход обеспечивает более высокую стабильность передачи данных и снижение задержек.

4. Представленный проблемно-ориентированный комплекс может использоваться целиком как для предварительной оценки параметров двухканальной связи, так и составные программные модули комплекса могут использоваться для решения отдельных не системных (не комплексных) задач, например, для: разделения цифровых изображений; передачи данных (файлов) по двум каналам связи; оптимизационных задач систем связи.

ЗАКЛЮЧЕНИЕ

В результате проведённых исследований были получены новые теоретические и практические результаты, направленные на повышение стабильности, обеспечение конфиденциальности и сокращение затрат при распределённой передаче видеоданных благодаря системному подходу к созданию и оптимизации двухканальной системы связи.

1. В результате анализа работ, посвященных вопросам распределенной передачи видеоданных выявлено, что известные методы и алгоритмы разделения данных (в том числе изображений), не учитывают или учитывают не в полной мере характеристики используемых систем связи. Установлено, что для обеспечения стабильности при распределенной передаче видеоданных и уменьшения временных затрат на синхронизацию получения частей кадров необходимо применять системный подход, который предусматривает комплексную разработку научно-технических решений в таких областях исследований как, системы связи, кодирование информации, математическое моделирование и системный анализ.

2. Разработаны алгоритмы кодирования изображений, основанные на схемах разделения: алгоритм разделения изображений по дробным частям десятичных чисел (АРДЧ), алгоритм разделения изображений с помощью префиксного кодирования (АРПК). Установлено, что алгоритмы позволяют выполнять разделение изображений на части неравного размера с невозможность их последующего полного декодирования по большим частям без знания меньших. Отличительной особенностью алгоритмов является использование простых математических операций при разделении и восстановлении изображений, это позволило добиться быстрого действия обработки видеокадров при программной реализации.

Получено, что АРДЧ пригоден для кодирования неконтрастных изображений, это исключает возможность его применения для черно-белых изображений. Показано, что АРПК пригоден для кодирования любых изображений и не дает никаких сведений об исходных изображениях, за исключением их цветовых представлений. Определено, что в АРДЧ меньшая часть в среднем составляет 24% от исходного объема, скорость обработки – 12-20 кадров/с (учитывая расширения изображений, мощности

вычислительных ресурсов). Для АРПК меньшая часть составляет 13%, скорость обработки – 15-25 кадров/с. Полученные результаты подтверждают возможность применения АРДЧ, АРПК при распределённой передаче видеоданных.

3. Представлена методика аналитического расчета пропускных способностей каналов двухканальной системы связи, заключающаяся в исследовании систем связи с учетом характеристик передаваемого потока данных и получении расчетных формул для вычисления минимальных пропускных способностей каналов связи.

Предложено доказательство четырех теорем, позволяющих свести двумерные задачи оптимизации двухканальных систем с разделением данных по каналам связи (задачи с двумя варьируемыми параметрами) к одномерным. Доказано, что для передачи любого потока данных, разделяемых в постоянном соотношении, оптимальные пропускные способности каналов двухканальной системы связи имеют линейную зависимость.

4. Разработана имитационная модель двухканальной системы видеосвязи, позволяющая в совокупности с генетическим алгоритмом Парето-аппроксимации выполнить многокритериальную оптимизацию параметров. Определено, что полученные с помощью имитационной модели значения пропускных способностей каналов связи, позволяют добиться синхронизации передачи данных с наименьшим рассогласованием времени доставки частей видеокадров, а также соответствуют ожидаемым теоретическим. Среднее расхождение между теоретическими значениями и результатами имитационной модели не превышает 9%, это объясняется тем, что аналитические расчеты проводятся в идеальных условиях, без учета внешних факторов.

5. Создан проблемно-ориентированный комплекс программ для двухканальной системы передачи видеоданных, который позволяет провести экспериментальные исследования. Установлено, что при значениях пропускных способностей каналов связи, определенных с помощью имитационной модели, достигается наименьшее рассогласование времени доставки частей видеокадров по параллельным каналам связи (меньше чем при аналитическом расчете и экспертном подборе), которое не превышает 300 мс. Определено, что такие значения, с учетом применения алгоритмов буферизации, позволяют

воспроизводить видеоданные без заметных задержек, при увеличении затрат не превышающих 2% по сравнению с затратами, полученными при применении аналитически рассчитанных значений пропускных способностей. Незначительное увеличение стоимости сопровождается рядом преимуществ – повышение стабильности в условиях переменной нагрузки, снижение задержек доставки данных.

СПИСОК СОКРАЩЕНИЙ

АРМ – автоматизированное рабочее место;

ГА – генетический алгоритм;

ДИ – доверительный интервал;

МО – математическое ожидание;

ОРД – область допустимых решений;

СеМО – сеть массового обслуживания;

СМО – система массового обслуживания;

ТМО – теория массового обслуживания;

ЦФ – целевая функция;

ЭВМ – электронно-вычислительная машина;

FIFO – дисциплина обслуживания заявок (First In – First Out);

IP – уникальный числовой идентификатор устройства в компьютерной сети (Internet Protocol);

OSI – сетевая модель стека сетевых протоколов (Open Systems Interconnection model);

TCP – транспортный протокол для передачи данных (Transmission Control Protocol).

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Shamir, A. How to share a secret / A. Shamir. – DOI: 10.1145/359168.359176 // Communications of the ACM. – 1979. – Vol. 22, no. 11. – P. 612–613.
2. Naor, M. Visual cryptography / M. Naor, A. Shamir. – DOI: doi.org/10.1007/BFb0053418 // Advances in Cryptology - Eurocrypt '94: workshop on the theory and application of cryptographic techniques : proceedings (Perugia, 9–12 May 1994) / Heidelberg : Springer, 1995. – Vol. 950. – P. 1–12.
3. Nelson, R. Approximate Analysis of For/Join Synchronization in Parallel Queues / R. Nelson, A. N. Tantawi. – DOI: 10.1109/12.2213 // IEEE Transactions on Computers. – 1988. – Vol. 37, no. 6. – P. 739–743.
4. Thomasian, A. Analysis of Fork/Join and Related Queueing Systems / A. Thomasian. – DOI: 10.1145/2628913 // ACM Computing Surveys (CSUR). – 2014. – Vol. 47, no. 2. – P. 17-1–17-71.
5. Tsimashenka, I. Reduction of Subtask Dispersion in Fork-Join Systems / I. Tsimashenka, W. J. Knottenbelt. – DOI: 10.1007/978-3-642-40725-3_25 // Computer Performance Engineering : 10th European Workshop, EPEW 2013 : proceedings (Venice, 16–17 September 2013). – Heidelberg : Springer, 2013. – P. 325–336.
6. Близно, Л. В. Система информационной безопасности на современном предприятии : моногр. / Л. В. Близно, И. А. Евенко, А. Н. Мирная. – Ставрополь : ООО «Губерния», 2021. – 119 с. – ISBN 978-5-6044710-8-1.
7. Обеспечение избыточности для повышения надежности функционирования корпоративной компьютерной сети передачи информации / А. В. Самохвалов, Д. С. Соловьев, И. А. Соловьева, А. А. Скворцов // Прикаспийский журнал: управление и высокие технологии. – 2022. – № 4 (60). – С. 68–76.
8. Защита информации в телекоммуникационных системах / Г. Ф. Коначович, В. П. Климчук, С. М. Паук, В. Г. Потапов. – Киев : МК-Пресс, 2005. – 288 с. – ISBN 966-8806-03-4.
9. Цветков, К. Ю. Формирование резервных путей на основе алгоритма Дейкстры в целях повышения устойчивости информационно-

телекоммуникационных сетей / К. Ю. Цветков, С. И. Макаренко, Р. Л. Михайлов // Информационно-управляющие системы. – 2014. – № 2 (69). – С. 71–78.

10. Макаренко, С. И. Модифицированный алгоритм Беллмана-Форда с формированием кратчайших и резервных путей и его применение для повышения устойчивости телекоммуникационных систем / С. И. Макаренко, М. Н. Квасов. – DOI: 10.18469/ikt.2016.14.3.06 // Инфокоммуникационные технологии. – 2016. – Т. 14, № 3. – С. 264–274.

11. Макаренко, С. И. Защита компьютерных сетей и телекоммуникаций : учеб. пособие / С. И. Макаренко. – Санкт-Петербург : Научное издание, 2024. – 311 с. – ISBN 978-5-907618-79-4.

12. Васильев, Е. В. Радиопередатчики для исследования ММО канала связи с беспилотным летательным аппаратом / Е. В. Васильев // Вестник Рязанского государственного радиотехнического университета. – 2015. – № 54-1. – С. 9–14.

13. Системы связи на транспорте: тенденции развития и задачи регулирования / В. Н. Васильев, В. А. Григорьев, И. А. Хворов, Ю. А. Распаев // Электросвязь. – 2016. – № 2. – С. 18–23.

14. Яронова, Н. В. Применение беспроводных технологий для организации видеонаблюдения на железнодорожном транспорте / Н. В. Яронова, А. Х. ъ. Шосалманов. – DOI: 10.32743/UniTech.2021.93.12.12835 // Universum: технические науки. – 2021. – № 12-2 (93). – С. 59–61.

15. Закалюжный, А. А. Развитие беспроводных сетей как средство контроля и управления удаленными системами / А. А. Закалюжный // Молодой исследователь Дона. – 2018. – № 4 (13). – С. 46–51.

16. Боев, Н. М. Анализ командно-телеметрической радиолинии связи с беспилотными летательными аппаратами / Н. М. Боев // Вестник Сибирского государственного аэрокосмического университета имени академика М. Ф. Решетнева. – 2012. – Т. 13, № 2 (42). – С. 86–91.

17. Винокуров, А. В. Анализ уязвимостей комплексов с беспилотными летательными аппаратами и классификация угроз безопасности циркулирующей в них информации / А. В. Винокуров // I-methods. – 2016. – Т. 8, № 1. – С. 5–9.

18. Гель, В. Э. Обоснование принципов построения канала управления, телеметрии и информационных каналов малогабаритных БПЛА / В. Э. Гель, Е. В. Евдокимов, О. Г. Сенин. – DOI: 10.37882/2223-2966.2021.01.10 // Современная наука: актуальные проблемы теории и практики. Сер. Естественные и технические науки. – 2021. – № 1. – С. 69–73.

19. Боев, Н. М. Построение систем связи беспилотных летательных аппаратов для передачи информации на большие расстояния / Н. М. Боев, П. В. Шаршавин, И. В. Нигруца // Известия Южного федерального университета. Технические науки. – 2014. – № 3 (152). – С. 147–158.

20. Макаренко, С. И. Противодействие беспилотным летательным аппаратам: моногр. / С. И. Макаренко – Санкт-Петербург : Научное издательство «Лань», 2020. – 204 с. – ISBN 978-5-6044793-6-0.

21. Развитие интеллектуальных транспортных систем в Российской Федерации: определение требований и организация создания полигонов тестирования информационной безопасности / О. М. Писарева, В. А. Алексеев, Д. Н. Медников, А. В. Стариковский // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Сер. Экономические науки. – 2020. – Т. 13, № 5. – С. 7–23.

22. Характеристика зон уязвимости и источников угроз информационной безопасности эксплуатации беспилотных автомобилей в интеллектуальной транспортной системе / О. М. Писарева, В. А. Алексеев, Д. Н. Медников, А. В. Стариковский // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Сер. Экономические науки. – 2021. – Т. 14, № 4. – С. 20–36.

23. Информационные системы беспилотных комплексов стратегической и оперативной воздушной разведки США / С. Г. Белов, А. Д. Крайлюк, В. И. Меркулов, В. С. Чернов. – DOI: 10.18127/j20700784-202001-02 // Успехи современной радиоэлектроники. – 2020. – № 1. – С. 28–42.

24. Слюсар, В. Передача данных с борта БПЛА: стандарты НАТО / В. Слюсар // Электроника: наука, технология, бизнес. – 2010. – № 3 (101). – С. 80–87.

25. Самойленко, Д. В. Распределённая обработка и защита информации в группировке комплексов с беспилотными летательными аппаратами / Д. В. Самойленко, О. А. Финько, М. А. Еремеев // Теория и техника радиосвязи. – 2017. – № 4. – С. 93–100.
26. Митращук, В. В. Программно-аппаратный комплекс защиты телеметрии и телеуправления специализированного беспилотного летательного аппарата / В. В. Митращук, М. П. Баранова // Журнал Сибирского федерального университета. Техника и технологии. 2019. – Т. 12, № 5. – С. 585–598.
27. Халютин, С. П. Алгоритм определения состава и параметров первичных источников электроэнергии БПЛА / С. П. Халютин, Б. В. Жмуров // Труды международного симпозиума «Надежность и качество». – 2010. – Т. 1. – С. 425–429.
28. Капелько, К. В. Алгоритм оптимизации параметров комбинированной системы электроснабжения электрических беспилотных летательных аппаратов / К. В. Капелько, Э. Ю. Хохулин. – DOI: 10.17277/vestnik.2022.01.pp.046-054 // Вестник Тамбовского государственного технического университета. – 2022. – Т. 28, № 1. – С. 46–54.
29. Карякин, В. В. Беспилотные летательные аппараты - новая реальность войны / В. В. Карякин // Проблемы национальной стратегии. – 2015. – № 3 (30). – С. 130–145.
30. Шаталов Н. В. Особенности классификации БПЛА самолетного типа / Н. В. Шаталов // Перспективы развития информационных технологий. – 2016. – № 29. – С 34–39.
31. Каршов, Р. С. Классификация беспилотных летательных аппаратов / Р. С. Каршов // Проблемы современной науки и образования. – 2016. – № 11 (53). – С. 38–40.
32. Классификация беспилотных летательных аппаратов (в контексте современных войн в арабском мире) / С. И. Безруков, В. Ю. Гумелев, А. В. Пархоменко, Д. А. Филиппов // Оригинальные исследования. – 2020. – Т. 10, № 4. – С. 66–81.
33. Сагайдак, Д. А. Организация распределенной передачи видеоданных по двум каналам связи в целях их защиты / Д. А. Сагайдак. – DOI: 10.25728/avtprom.2024.12.11 // Автоматизация в промышленности. – 2024. – № 12. – С. 53–56.

34. Сагайдак, Д. А. Модели схем разделения секрета в системах передачи видеoinформации / Д. А. Сагайдак, Р. Т. Файзуллин // Компьютерная оптика. – 2013. – Т. 37, № 1. – С. 10–112.

35. Файзуллин, Р. Т. Приложение алгоритма префиксного кодирования массива данных в схеме разделения секрета потока видеоданных / Р. Т. Файзуллин, Д. А. Сагайдак // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2012. – № 1-2(25). – С. 136–140.

36. Алгоритмы обработки информации при передаче и хранении данных, основанные на процедуре разделения секрета / В. В. Михеев, Д. А. Сагайдак, А. А. Свенч, Р. Р. Файзуллин // Вестник Сибирской государственной автомобильно-дорожной академии. – 2012. – № 5 (27). – С. 82–87.

37. Сагайдак, Д. А. Применение примитивизированного дельта-кода Элиаса в схеме разделения секрета / Д. А. Сагайдак, Р. Т. Файзуллин // Динамика систем, механизмов и машин. – 2012. – № 1. – С. 371–374.

38. Сагайдак, Д. А. Приложение алгоритмов разделения секрета в целях сокрытия передаваемой видеoinформации / Д. А. Сагайдак // Электронные средства и системы управления. Материалы докладов Международной научно-практической конференции. – 2012. – № 2. – С. 51–56.

39. Лавров, Д. Н. Схема разделения секрета для потоков данных маршрутизируемой сети / Д. Н. Лавров // Математические структуры и моделирование. – 2002. – № 10. – С. 192–197.

40. Ефимов, В. И. Система мультиплексирования разнесенного TCP/IP трафика / В. И. Ефимов, Р. Т. Файзуллин // Математические структуры и моделирование. – 2002. – № 10. – С. 170–171.

41. Анализ надежности алгоритма разделения секрета в сетевых потоках / Д. Н. Лавров, В. И. Дулькейт, П. И. Михайлов, А. А. Свенч // Математические структуры и моделирование. – 2003. – № 12. – С. 146–154.

42. Гусс, С. В. Подходы к реализации сетевого протокола обеспечения гарантированной доставки при мультимаршрутной передаче данных / С. В. Гусс,

Д. Н. Лавров. – DOI: 10.24147/2222-8772.2018.2.95-101 // Математические структуры и моделирование. – 2018. – № 2 (46). – С. 95–101.

43. Балансировка трафика в высоконагруженных системах с помощью протокола TRILL / А. Багинян, А. Долбилов, И. Кашунин, В. Кореньков // Т-Comm: телекоммуникации и транспорт. – 2017. – Т. 11, № 4. – С. 14–19.

44. Денисова, Л. А. Событийное моделирование цифровой системы регулирования / Л. А. Денисова // Омский научный вестник. – 2011. – № 3 (103). – С. 261–265.

45. Перепелкин, Д. А. Концептуальный подход динамического формирования трафика программно-конфигурируемых телекоммуникационных сетей с балансировкой нагрузки / Д. А. Перепелкин // Информационные технологии. – 2015. – Т. 21, № 8. – С. 602–610.

46. Эйдуc, Г. С. Асинхронные адресные системы связи / Г. С. Эйдуc, В. В. Марков, М. Д. Венедиктов. – Москва : Связь, 1968. – 272 с.

47. Синхронизация каналов компьютерной сети при передаче трафика реального времени / О. А. Шибанова, Н. В. Кравчук, А. В. Башев, А. П. Шибанов // Вестник Рязанского государственного радиотехнического университета. – 2007. – № 22. – С. 53–57.

48. Молотков, С. Н. Одноразовый блокнот, сложность перебора ключей и практическая секретность квантовой криптографии / С. Н. Молотков // Журнал экспериментальной и теоретической физики. – 2016. – Т. 150, № 5. – С. 903–916.

49. Организация защищенного канала передачи данных между беспилотным летательным аппаратом и наземной станцией управления на основе одноразовых блокнотов / И. А. Авдонин, С. С. Беляев, М. Б. Будько [и др.] // Информатизация и связь. – 2018. – № 5. – С. 78–84.

50. Авдонин, И. А. Организация защиты данных, передаваемых между беспилотным летательным аппаратом и наземной станцией управления, на основе шифра Вернама / И. А. Авдонин, М. Б. Будько, В. А. Грозов // Научно-технический вестник информационных технологий, механики и оптики. – 2016. – Т. 16, № 5. – С. 850–855.

51. Трушечкин, А. С. Об операционном смысле и практических аспектах использования параметра стойкости в квантовом распределении ключей / А. С. Трушечкин // Квантовая электроника. – 2020. – Т. 50, № 5. – С. 426–439.
52. Jin, D. Progressive color visual cryptography / D. Jin, W. Q. Yan, M. S. Kankanhalli. – DOI:10.1117/1.1993625 // Journal of Electronic Imaging. – 2005. – Vol. 13, no. 3. – P. 033019.
53. Feng, L. Embedded extended visual cryptography schemes / L. Feng, W. ChuanKun. – DOI: 10.1007/978-3-030-03146-6_144 // IEEE Transactions on Information Forensics & Security. – 2011. – Vol. 6, no. 2. – P. 307–322.
54. Hou, Y. C. Visual cryptography for color images / Y. C. Hou // Pattern Recognition. – 2003. – Vol. 36, no. 7. – P. 1619–1629.
55. Liu, F. The alignment problem of visual cryptography schemes / F. Liu, C. K. Wu, X. J. Lin / 10.1007/s10623-008-9225-3 // Designs, Codes and Cryptography. – 2009. – Vol. 50. – P. 215–227.
56. Brickell, E. F. On the classification of Ideal Secret Sharing Schemes / E. F. Brickell, D. M. Davenport // Journal of Cryptology. – 1991. – Vol. 4. – P. 123–134.
57. Блейкли, Р. Г. Обобщенные идеальные схемы, разделяющие секрет, и матроиды / Р. Г. Блейкли, Г. А. Кабатянский // Проблемы передачи информации. – 1997. – Т. 33, вып. 3. – С. 102–110.
58. Соколов, С. С. Методы обеспечения доступности информации в высоконагруженных информационных системах / С. С. Соколов, Р. Ю. Новоселов, А. В. Митрофанова // Вестник УрФО. Безопасность в информационной сфере. – 2018. – № 2 (28). – С. 31–35.
59. Blakley, G. R. Safeguarding cryptographic keys / G. R. Blakley DOI: 10.1109/AFIPS.1979.98 // Managing Requirements Knowledge, International Workshop : proceedings (New York, 4–7 June 1979). – Los Alamitos : IEEE Computer Society, 1979. – Vol. 48. – P. 313–317.
60. Shapiro, L. G. Computer Vision / L. G. Shapiro, G. C. Stockman. – New Jersey: Prentice-Hall, 2001. – 608 p. – ISBN 0-13-030796-3.

61. Шитова, О. В. Анализ методов сегментации текстурных областей изображений в системах обработки изображений / О. В. Шитова, А. Н. Пухляк, Е. М. Дроб // Научные ведомости Белгородского государственного университета. Сер. История. Политология. Экономика. Информатика. – 2014. – № 8, вып. 30/1. – С. 182–188.
62. Стругайло, В. В. Обзор методов фильтрации и сегментации цифровых изображений / В. В. Стругайло // Наука и образование. – 2012. – № 5. – С. 270–281.
63. Файзуллин, Р. Т. Алгоритм разделения секрета с использованием принципиально малой части секрета в качестве ключа / Р. Т. Файзуллин, И. Р. Файзуллин, О. Т. Данилова // Вестник Тюменского государственного университета. Сер. Физико-математические науки. Информатика. – 2011. – № 7. – С. 175–179.
64. Файзуллин, Р. Т. Построение системы защиты видеоданных с использованием решения задач проверки изоморфизма графов / Р. Т. Файзуллин, Г. С. Ржаницын // Компьютерная оптика. – 2006. – № 29. – С. 127–134.
65. Файзуллин, И. Р. Алгоритм кодирования и передачи информации базирующийся на стеганографическом подходе / И. Р. Файзуллин, Р. Т. Файзуллин // Вестник Тюменского государственного университета. – 2010. – № 6. – С. 147–152.
66. Свенч, А. А. Схема разделения секрета на основе метрических характеристик данных для защищенной передачи видеопотоков / А. А. Свенч, Р. Т. Файзуллин // Компьютерная оптика. – 2007. – Т. 31, № 1. – С. 47–51.
67. Щерба, Е. В. Метод защиты канала передачи видеоинформации на основе мультиплексирования трафика / Е. В. Щерба // Вопросы защиты информации. – 2008. – № 1 (80). – С. 55–60.
68. Сагайдак, Д. А. Метод обеспечения безопасного хранения данных на серверах ЦОД (центров обработки данных) / Д. А. Сагайдак // Россия молодая: передовые технологии - в промышленность : материалы IV Всерос. молодеж. науч.-техн. конф. с междунар. участием (Омск, 15–17 нояб. 2011 г.) : в 2 кн. / Ом. гос. техн. ун-т. – Омск : Изд-во ОмГТУ, 2011. – Кн. 1. – С. 304–307.
69. Сагайдак, Д. А. Применение алгоритма разделения секрета в системах передачи и хранения данных / Д. А. Сагайдак // Прикладная математика и фундаментальная информатика. – 2021. – Т. 8, № 1. – С. 50–58.

70. Свенч, А. А. Представление геометрического объекта списком метрических характеристик / А. А. Свенч, Р. Т. Файзуллин // Математические методы распознавания образов. – 2005. – Т. 12, № 1. – С. 434–437.

71. Linetsky, M. Programming Microsoft Directshow / M. Linetsky. – Wordware Publishing, 2001. – 415 p.

72. Теоретические основы цифровой обработки изображений / В. А. Соيفер, В. В. Сергеев, С. Б. Попов, В. В. Мясников ; Самар. гос. аэрокосм. ун-т им. акад. С. П. Королева. – Самара : [б. и.], 2000. – 255 с. – ISBN 5-7883-0109-2.

73. Щерба, Е. В. Анализ применимости методов интерполяции и экстраполяции для решения задачи восстановления изображения / Е. В. Щерба // Компьютерная оптика. – 2009. – Т. 33, № 3. – С. 336–339.

74. Молчанов, А. Л. Изучение свойств эффективности и робастности работы мультиплексированной системы / А. Л. Молчанов, Р. Т. Файзуллин // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2013. – № 1 (27). – С. 83–86.

75. Tsai, Ming-Hong. A study on secret image sharing / Ming-Hong Tsai, Chaur-Chin Chen // The Sixth International Workshop on Image Media Quality and its Applications, IMQA 2013 : Proceedings (Tokyo, Japan, 12–13 September 2013). – Tokyo, Japan, 2013. – P. 135–139.

76. Asmuth, C. A Modular Approach to Key Safeguarding / C. Asmuth, J. Bloom // IEEE Transactions on Information Theory. – 1983. – Vol. 29, no. 2. – P. 208–210.

77. Ulutas, M. A New Secret Image Sharing Technique Based on Asmuth Bloom's Scheme / M. Ulutas, V. V. Nabiyeu, G. Ulutas // International conference on Application of Information and Communication Technologies : Proceedings (Baku, Azerbaijan, 14–16 October 2009). – IEEE, 2009. – P. 1–5.

78. Chang, Chin-Chen. Efficient Searching Strategy for Secret Image Sharing with Meaningful Shadows / Chin-Chen Chang, Ngoc-Tu Huynh, Ting-Feng Chung // International Journal of Machine Learning and Computing. – 2014. – Vol. 4, no. 5. – P. 423–427.

79. Ренжин, П. А. Методика защиты цифровых видеодоказательств от фальсификации встраиванием цифрового водяного знака / П. А. Ренжин,

Р. Т. Файзуллин // Научная сессия ТУСУР-2010 : материалы докл. Всерос. науч.-техн. конф. студ., аспирантов и молодых ученых (Томск, 4–7 мая 2010 г.) : в 5 ч. / Том. гос. ун-т систем упр. и радиоэлектроники. – Томск : В-Спектр, 2010. – Ч. 3. – С. 191–192.

80. Файзуллин, Р. Т. Пределы применения способа встраивания изображения в видеопоследовательность случайными частями с помощью замены / Р. Т. Файзуллин, П. А. Ренжин // Роль регионов в реализации Стратегии развития информационного общества в Российской Федерации : материалы III Межрегион. информац. конгресса (Омск, 1–3 окт. 2008 г.). – Омск : КАН, 2008. – С. 262–269.

81. Митекин, В. А. Метод встраивания информации в видео, стойкий к ошибкам потери синхронизации / В. А. Митекин, В. А. Федосеев // Компьютерная оптика. – 2014. – Т. 38, № 3. – С. 564–573.

82. Митекин, В. А. Алгоритм формирования информационных последовательностей меток для использования в алгоритмах встраивания цифровых водяных знаков / В. А. Митекин // Компьютерная оптика. – 2011. – Т. 35, № 4. – С. 523–530.

83. Глумов, Н. И. Алгоритм поблочного встраивания стойких ЦВЗ в крупноформатные изображения / Н. И. Глумов, В. А. Митекин // Компьютерная оптика. – 2011. – Т. 35, № 3. – С. 368–372.

84. Глумов, Н. И. Алгоритм встраивания полухрупких цифровых водяных знаков для задач аутентификации изображений и скрытой передачи информации / Н. И. Глумов, В. А. Митекин // Компьютерная оптика. – 2011. – Т. 35, № 2. – С. 262–367.

85. Шляхтина, С. Водяной знак для фотографии / С. Шляхтина // Компьютер Пресс. – 2005. – № 1. – С. 177–181.

86. Кобозева, А. А. Стеганографический метод, обеспечивающий проверку целостности и аутентичности передаваемых данных / А. А. Кобозева, М. А. Козина // Проблемы региональной энергетики. – 2014. – № 3 (26). – С. 93–106.

87. Сагайдак, Д. А. Способ формирования цифрового водяного знака для физических и электронных документов / Д. А. Сагайдак, Р. Т. Файзуллин // Компьютерная оптика. – 2014. – Т. 38, № 1. – С. 94–104.

88. Нейроподобная структура вычисления секрета для динамических пороговых схем / Н. И. Червяков, А. А. Евдокимов, В. В. Сляднев, О. П. Малофей // Нейрокомпьютеры: разработка, применение. – 2008. – № 3-4. – С. 64–68.

89. Алгебраические и практические аспекты реализации нейросетевой пороговой схемы разделения секрета / Н. И. Червяков, М. Г. Бабенко, И. Н. Лавриненко [и др.] // Наука. Инновации. Технологии. – 2014. – № 2. – С. 14–26.

90. Гусарова, М. А. Построение и реализация некоторых совершенных проверяемых схем разделения секрета / М. А. Гусарова // Автоматизация процессов управления. – 2021. – № 2 (64). – С. 13–17.

91. Рацеев, С. М. Конструкции некоторых схем разделения секрета на основе линейных кодов / С. М. Рацеев // Известия Саратовского университета. Новая серия. Сер. Математика. Механика. Информатика. – 2024. – Т. 24, № 3. – С. 330–341.

92. Рацеев, С. М. Схема разделения секрета с заданным на множестве участников отношением порядка / С. М. Рацеев, А. М. Иванцов // Ученые записки УлГУ. Сер. Математика и информационные технологии. – 2023. – № 2. – С. 99–103.

93. Исследование fork-join системы с марковским входным потоком и распределением времени обслуживания фазового типа / В. М. Вишневский, В. И. Клименок, А. М. Соколов, А. А. Ларионов // Проблемы информатики. – 2023. – № 4 (61). – С. 29–56.

94. Narahari, Y. Performability Analysis of Fork-join Queueing Systems / Y. Narahari, P. Sundarrajan // Journal of the Operational Research Society. – 1995. – Vol. 46, no. 10. – P. 1237–1249.

95. Обзор систем параллельной обработки заявок / А. В. Горбунова, И. С. Зарядов, К. Е. Самуйлов, Э. С. Сопин // Вестник Российского университета дружбы народов. Сер. Математика, информатика, физика. – 2017. – Т. 25, № 4. – С. 350–362.

96. Хабаров, Р. С. Аппроксимация времени пребывания для системы массового обслуживания Fork-Join на основе инвариантов отношения / Р. С. Хабаров, В. А. Лохвицкий, А. С. Дудкин // Интеллектуальные технологии на транспорте. – 2020. – № 2 (22). – С. 46–50.

97. Flatto, L. Two Parallel Queues Created By Arrivals With Two Demands I / L. Flatto, S. Hahn // *SIAM Journal on Applied Mathematics*. – 1984. – Vol. 44, no. 5. – P. 1041–1053.
98. Baccelli, F. Two Parallel Queues Created by Arrivals with Two Demands: the $M|G|2$ Symmetrical Case / F. Baccelli ; INRIA Rapport de Recherche. – France, 1985. – Vol. 426. – 34 p.
99. Башарин, Г. П. Введение в теорию вероятностей : учеб. пособие / Г. П. Башарин. – Москва : Изд-во Ун-та дружбы народов, 1990. – 228 с. – ISBN 5-209-00382-5.
100. Бочаров, П. П. Теория массового обслуживания : учеб. для вузов / П. П. Бочаров, А. В. Печинкин. – Москва : Изд-во Рос. ун-та дружбы народов, 1995. – 529 с. – ISBN 5-209-00796-0.
101. Baccelli, F. Queueing models for systems with synchronization constraints / F. Baccelli, A. M. Makowski // *Proceedings of the IEEE*. – 1989. – Vol. 77, no 1. – P. 138–161.
102. Baccelli, F. The fork-join queue and related systems with synchronization constraints: stochastic ordering and computable bounds / F. Baccelli, A. M. Makowski, A. Shwartz // *Advances in Applied Probability*. – 1989. – Vol. 21, no. 3. – P. 629–660.
103. Thomasian, A. Approximate Solutions for $M/G/1$ Fork/Join Synchronization / A. Thomasian, A. N. Tantawi // *26th Conference on Winter Simulation : Proceedings (Lake Buena Vista, FL, USA, 11–14 December 1994)*. – IEEE, 1994. – P. 361–368.
104. Varma, S. Interpolation approximations for symmetric Fork-Join queues / S. Varma, A. M. Makowski // *Performance Evaluation*. – 1994. – Vol. 20, no. 1–3. – P. 245–265.
105. Kim, C. Analysis of the fork-join queue / C. Kim, A. K. Agrawala // *IEEE Transactions on Computers*. – 1989. – Vol. 38, no. 2. – P. 250–255.
106. Duda, A. Performance Evaluation of Fork and Join Synchronization Primitives / A. Duda, T. Czachórski // *Acta Informatica*. – 1987. – Vol. 24, no. 5. – P. 525–553.
107. Fiorini, P. M. Exact Analysis of Some Split-Merge Queues / P. M. Fiorini, L. Lipsky // *ACM SIGMETRICS Performance Evaluation Review*. – 2015. – Vol. 43, no. 2. – P. 51–53.
108. Советов, Б. Я. Моделирование систем : учеб. для вузов / Б. Я. Советов, С. А. Яковлев. – Москва : Высшая школа, 2007. – 343 с. – ISBN 978-5-06-003860-6.

109. Романцев, В. В. Аналитические модели систем массового обслуживания : учеб. пособие / В. В. Романцов ; С.-Петербург. гос. электротехн. ун-т (ЛЭТИ). – Санкт-Петербург : Изд-во ЛЭТИ, 1998. – 66 с.

110. Задорожный, В. Н. Введение в имитационное моделирование : учеб. пособие для вузов / В. Н. Задорожный ; Ом. гос. техн. ун-т. – Омск : Изд-во ОмГТУ, 2014. – 194 с. – ISBN 978-5-8149-1899-4.

111. Задорожный, В. Н. Имитационное и статистическое моделирование: учеб. пособие для вузов / В. Н. Задорожный ; Ом. гос. техн. ун-т. – Омск : Изд-во ОмГТУ, 2013. – 136 с. – ISBN 978-5-8149-1461-3.

112. Максимей, И. В. Разработка имитационных моделей сложных технических систем / И. В. Максимей, В. С. Смородин, О. М. Демиденко ; Гом. гос. ун-т им. Ф. Скорины. – Гомель : Изд-во ГГУ им. Ф. Скорины, 2014. – 298 с. – ISBN 978-985-439-951-5.

113. Сажина, Ю. В. Имитационное моделирование при проектировании распределенных интеллектуальных систем / Ю. В. Сажина, А. С. Свиридова // Теория и практика современной науки. – 2018. – № 2 (32). – С. 481–492.

114. Моделирование систем массового обслуживания инструментальным средством Matlab/Simulink : метод. указания / сост. В. В. Извозчикова. – Оренбургский гос. ун-т. – Оренбург : Изд-во ОГУ, 2021. – 53 с.

115. Фотокинетика : энциклопедия / гл. ред. Е. А. Иофис. – Москва : Советская энциклопедия, 1981. – 447 с.

116. Хейгеман, Л. Прикладные итерационные методы / Л. Хейгеман, Д. Янг ; пер. с англ. А. Ю. Еремина, И. Е. Капорина ; под ред. Ю. А. Кузнецова. – Москва : Мир, 1986. – 446 с.

117. Файзуллин, И. Р. Аппаратно-эффективный алгоритм формирования маркера начала сообщения / И. Р. Файзуллин, Р. Т. Файзуллин // Компьютерная оптика. – 2010. – Т. 34, № 4. – С. 552–554.

118. Elias, P. Universal codeword sets and representations of the integers / P. Elias // IEEE Transactions on Information Theory. – 1975. – Vol. 21, no. 2. – P. 194–203.

119. FIPS PUB 140-1. Security Requirements for Cryptographic Modules : Federal Information Processing Standards Publication / National institute of standards and technology. – Washington, 1994. – 41 p.

120. Чугунков, И. В. Методы и средства оценки качества генераторов псевдослучайных последовательностей, ориентированных на решение задач защиты информации : учеб. пособие для студентов вузов / И. В. Чугунков ; Нац. исслед. ядерный ун-т «МИФИ». – Москва : Изд-во НИЯУ «МИФИ», 2012. – 235 с. – ISBN 978-5-7262-1690-4.

121. Гонсалес, Р. С. Цифровая обработка изображений / Р. С. Гонсалес, Р. Э. Вудс. – Москва : Техносфера, 2006. – 1070 с. – ISBN 5-94836-028-8.

122. Engelken, E. J. A new approach to the analysis of nystagmus: an application for order-statistic filters / E. J. Engelken, K. W. Stevens // Aviation, space, and environmental medicine. – 1990. – Vol. 61, no. 9. – P. 859–864.

123. Обработка и анализ цифровых изображений с примерами на LabVIEW IMAQ Vision / Ю. В. Визильтер, С. Ю. Желтов, В. А. Князь [и др.]. – Москва : ДМК Пресс, 2007. – 463 с. – ISBN 5-94074-348-X.

124. Cho, S. Removing non-uniform motion blur from images / S. Cho, Y. Matsushita, S. Lee // 11th International Conference on Computer Vision : Proceedings (Rio de Janeiro, Brazil, 14–21 October 2007). – IEEE, 2007. – P. 1–8.

125. Yuan, L. Image deblurring with blurred/noisy image pairs / L. Yuan, J. Sun, L. Quan, H. Y. Shum // ACM Transactions on Graphics. – 2007. – Vol. 26, no. 3. – P. 1–10.

126. Shan, Q. High-quality motion deblurring from a single image / Q. Shan, J. Jia, A. Agarwala // ACM Transactions on Graphics. – 2008. – Vol. 27, no. 3. – P. 1–10.

127. Efficient Filter Flow for Space-Variant Multiframe Blind Deconvolution / M. Hirsch, S. Sra, B. Scholkopf, S. Harmeling // Computer Society Conference on Computer Vision and Pattern Recognition : Proceedings (San Francisco, CA, USA, 13–18 June 2010). – IEEE, 2010. – P. 607–614.

128. ISO/IEC 7498-1:1994 Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model. – URL:

[http://standards.iso.org/ittf/PubliclyAvailableStandards/s020269_ISO_IEC_7498-1_1994\(E\).zip](http://standards.iso.org/ittf/PubliclyAvailableStandards/s020269_ISO_IEC_7498-1_1994(E).zip) (date accessed: 03.03.2024).

129. Задорожный, В. Н. Оптимизация передачи сообщений, разделяемых на разные доли, передаваемые по двум разным каналам / В. Н. Задорожный, Д. А. Сагайдак // Системы управления, информационные технологии и математическое моделирование : Материалы III Всероссийской научно-практической конференции с международным участием. В 2-х томах, Омск, 20 мая 2021 года. Том I. – Омск: Омский государственный технический университет, 2021. – С. 59-80.

130. Сагайдак, Д. А. Математическое обеспечение системы обработки видеоданных, разделяемых для передачи по двум каналам связи с целью их защиты / Д. А. Сагайдак // Автоматизация в промышленности. – 2024. – № 7. – С. 14-18.

131. Zadorozhnyi, V. Optimization of message transmission when implementing the secret sharing scheme / V. Zadorozhnyi, D. Sagaydak // Informational technologies and mathematical modelling (ITMM-2021), 01–05 декабря 2021 года. – Национальный исследовательский Томский государственный университет, 2022. – P. 137-144.

132. Клейнрок, Л. Вычислительные системы с очередями / Л. Клейнрок ; пер. с англ. под ред. Б. С. Цыбакова. – Москва : Мир, 1979. – 600 с.

133. Сагайдак, Д. А. Оптимизации передачи видеоданных с демультимплексированием по двум каналам связи с различными характеристикам / Д. А. Сагайдак // Информационные технологии и автоматизация управления : Материалы XIV Всероссийской научно-практической конференции студентов, аспирантов, работников образования и промышленности, Омск, 26–27 мая 2023 года / Отв. редактор А.В. Никонов. – Омск: Омский государственный технический университет, 2023. – С. 196-201.

134. Сагайдак, Д. А. Оптимизация передачи данных при реализации схем разделения секрета / Д. А. Сагайдак // Научный потенциал молодежи и технический прогресс : Материалы VII Всероссийской научно-практической конференции, Санкт-Петербург, 15 мая 2024 года. – Санкт-Петербург: ИП Жукова Е.В., 2024. – С. 16-17.

135. Сагайдак, Д. А. Защищенная двухканальная система видеосвязи с использованием схемы разделения секрета и оптимизацией параметров на основе

генетического алгоритма / Д. А. Сагайдак, Л. А. Денисова // Системы управления, связи и безопасности. – 2024. – № 3. – С. 126-156.

136. DNS Round Robin // The Technology chronicle. – URL: <https://thetechnologychronicle.blogspot.com/2013/11/dns-round-robin.html> (date accessed: 20.04.2024).

137. Цыбаков, Б. С. Наилучшая и наихудшая дисциплины передачи пакетов / Б. С. Цыбаков, П. Папантони-Казакос // Проблемы передачи информации. – 1996. – Т. 32, № 4. – С. 72–92.

138. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы : учеб. пособие для вузов / В. Г. Олифер, Н. А. Олифер. – 5-е изд. – Санкт-Петербург : Питер, 2016. – 991 с. – ISBN 978-5-496-01967-5.

139. Протоколы информационно-вычислительных сетей / С. А. Аничкин, С. А. Белов, А. В. Бернштейн [и др.] ; под ред. И. А. Мизина, А. П. Кулешова. – Москва : Радио и связь, 1990. – 504 с. – ISBN 5-256-00359-3.

140. Подиновский, В. В. Парето-оптимальные решения многокритериальных задач : моногр. / В. В. Подиновский, В. Д. Ногин. – Москва : Физматлит, 2007. – 255 с. – ISBN 978-5-9221-0812-6.

141. Денисова, Л. А. Автоматизация параметрического синтеза системы регулирования на основе многокритериальной оптимизации с использованием генетического алгоритма / Л. А. Денисова // Автоматизация в промышленности. – 2013. – № 12. – С. 24–31.

142. Карпенко, А. П. Популяционные методы аппроксимации множества Парето в задаче многокритериальной оптимизации. Обзор / А. П. Карпенко, А. С. Семенихин, Е. В. Митина // Наука и образование. – 2012. – № 4. – С. 1–36.

143. Денисова, Л. А. Многокритериальная оптимизация на основе генетических алгоритмов при синтезе систем управления : моногр. / Л. А. Денисова ; Ом. гос. техн. ун-т. – Омск : Изд-во ОмГТУ, 2014. – 170 с. – ISBN 978-5-8149-1822-2.

144. Макаренко, С. И. Интеллектуальные информационные системы : учеб. пособие / С. И. Макаренко ; Ставропольский филиал ГОУ ВПО «Моск. гос.

гуманитар. ун-т им. М. А. Шолохова». – Ставрополь : Изд-во СФ МГГУ им. М. А. Шолохова. 2009. – 206 с.

145. Кузюрин, Н. Н. Генетические алгоритмы в задаче поиска часто встречающихся комбинаций / Н. Н. Кузюрин, С. А. Мартишин, М. В. Храпченко // Труды Института системного программирования РАН. – 2004. – Т. 6. – С. 109–126.

146. Ануфриев, И. Е. MATLAB 7 / И. Е. Ануфриев, А. Б. Смирнов, Е. Н. Смирнова. – Санкт-Петербург : БХВ-Петербург, 2005. – 1104 с. – ISBN 5-94157-494-0.

147. Штовба, С. Д. Проектирование нечетких систем средствами MATLAB / С. Д. Штовба. – Москва : Горячая линия-Телеком, 2007. – 288 с. – ISBN 5-93517-359-X.

148. SimEvents Documentation. – URL: <https://ch.mathworks.com/help/simevents/> (date accessed: 10.02.2024).

149. Simulink: software for numerical simulation of continuous processes // MathWorks. – URL: <http://www.mathworks.com/products/simulink/> (date accessed: 10.02.2024).

150. A fast and elitist multiobjective genetic algorithm: NSGA-II / K. Deb, A. Pratap, S. Agarwal, T. Meyarivan // IEEE Transactions on Evolutionary Computation. – 2002. – Vol. 6, no. 2. – P. 182–197.

151. A review of surrogate assisted multiobjective evolutionary algorithms / A. Diaz-Manriquez, G. Toscano, J. H. Barron-Zambrano, E. Tello-Leal // Computational Intelligence and Neurosci. – 2016. – Vol. 2016. – P. 1–14.

152. Denisova, L. A. Automatic parametric synthesis of a control system using the genetic algorithm / L. A. Denisova, V. A. Meshcheryakov // Automation and Remote Control. – 2015. – Vol. 76, no. 1. – P. 149–156.

153. Викулов, Е. О. Автоматизированное распределение больших объемов данных высоконагруженных система / Е. О. Викулов, Е. А. Леонов, Л. А. Денисова // Динамика систем, механизмов и машин. – 2014. – № 3. – С. 146–149.

154. Гарагулова, А. К. Сравнение генетических алгоритмов MOGA и NSGA-II на задаче оптимизации формы рабочего колеса гидротурбины / А. К. Гарагулова, Д. О. Горбачева, Д. В. Чирков // Вычислительные технологии. – 2018. – Т. 23, № 5. – С. 21–36.

155. Deb, K. Multi-objective optimization using evolutionary algorithms / K. Deb. – New York : John Wiley & Sons Ltd, 2001. – 497 p.

156. Zitzler, E. Comparison of multiobjective evolutionary algorithms: Empirical results / E. Zitzler, K. Deb, L. Thiele // *Evolutionary Computation*. – 2000. – Vol. 8, no. 2. – P. 173–195.

157. Fonseca, C. M. Genetic algorithms for multiobjective optimization: Formulation, discussion and generalization / C. M. Fonseca, P. J. Fleming // *Genetic Algorithms : Proceedings of the 5th International Conference (Urbana-Champaign, IL, USA, 1993)*. – San Francisco, CA, USA : Morgan Kaufmann Publ., 1993. – P. 416–423.

158. Horn, J. Multiobjective optimization using the niched Pareto genetic algorithm / J. Horn, N. Nafpliotis // *Proceedings of the First IEEE Conference on Evolutionary Computation, IEEE World Congress on Computational Intelligence*. – Piscataway, New Jersey : IEEE Service Center, 1994. – Vol. 1. – P. 1–33.

159. Оптимизация проточной части осевого насоса с использованием поверхности отклика / Д. Г. Свобода, Е. А. Иванов, А. А. Жарковский, С. Ю. Щуцкий // *Известия высших учебных заведений. Машиностроение*. – 2022. – № 8 (749). – С. 74–83.

160. Тарутин, А. В. Применение методов генетических алгоритмов для построения множества Парето в задачах многокритериальной оптимизации / А. В. Тарутин, А. В. Набатов // *Инженерный вестник Дона*. – 2015. – № 4 (38). – С. 39.

161. Зеленин, С. А. Развитие технологий телевидения высокой четкости / С. А. Зеленин, В. Г. Орлов // *Фундаментальные проблемы радиоэлектронного приборостроения*. – 2013. – Т. 13, № 5. – С. 155–158.

162. Сколько трафика расходует 1 минута видео в YouTube? – URL: <https://dzen.ru/a/X1srH9XhXTDekaOw?experiment=948515> (дата обращения: 20.04.2024).

163. Как рассчитать объем потребляемого сервером трафика // ColoCat : сайт. – URL: <https://www.colocat.ru/texts/traffic.html> (дата обращения: 22.04.2024).

164. Что такое служебный трафик // Я ИТ специалист или Жизнь ИТшника: блог. – URL: <http://www.denaie.ru/?p=2874> (дата обращения: 22.04.2024).

165. Новицкий, П. В. Оценка погрешностей результатов измерений / П. В. Новицкий, И. А. Зограф. – Ленинград : Энергоатомиздат. Ленингр. отд-ние, 1991. – 303 с. – ISBN 5-283-04513-7.

166. Сидорова, О. И. Математическая статистика: практикум по получению первичных профессиональных умений и навыков, в том числе первичных умений и

навыков научно-исследовательской деятельности : учеб. пособие для студ. естественнонаучных направлений / О. И. Сидорова, И. В. Захарова, Ю. С. Хохлов. – Тверь : Изд-во Твер. гос. ун-та, 2018. – 125 с.

167. Ивин, Е. А. Методическое пособие по эконометрике: для социально-экономических специальностей / Е. А. Ивин, Н. В. Артамонов, А. Н. Курбацкий. – Вологда : ИСЭРТ РАН, 2018. – 183 с. – ISBN 978-5-93299-331-6.

168. Efron, B. Bootstrap Methods: Another Look at the Jackknife / B. Efron // The Annals of Statistics. – 1979. – Vol. 7, no. 1. – P. 1–26.

169. Red Hat Virtualization // Red Hat Customer Portal. – URL: <https://access.redhat.com/products/red-hat-virtualization> (date accessed: 30.04.2024).

170. Virtualdub.org. – URL: <https://www.virtualdub.org/index.html> (date accessed: 30.04.2024).

171. Hecht, S. Energy, quanta, and vision / S. Hecht, S. Shlaer, M. H. Pirene // Journal of General Physiology. – 1942. – Vol. 25, no. 6. – P. 819–840.

172. Recommendation ITU-T G.114. One-way transmission time. – URL: <http://www.itu.int/rec/T-REC-G.114-200305-I/en> (date accessed: 05.09.2024).

173. IEEE 1588-2008. IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems. – URL: <https://standards.ieee.org/ieee/1588/4355> (date accessed: 05.09.2024).

174. Network Time Protocol (NTP). – URL: <https://www.meinbergglobal.com/english/info/ntp.htm> (date accessed: 05.09.2024).

ПРИЛОЖЕНИЕ А1. ПРИМЕР РАБОТЫ АЛГОРИТМА РАЗДЕЛЕНИЯ ИЗОБРАЖЕНИЙ ПО ДРОБНЫМ ЧАСТЯМ ДЕСЯТИЧНЫХ ЧИСЕЛ

Пусть имеется изображение размером 3x2 пикселя, приведенное рисунку А1.1.

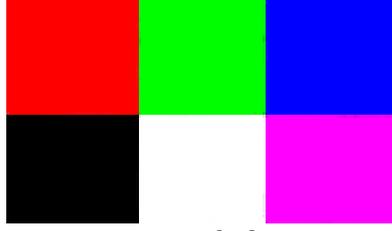


Рисунок А1.1 – Изображение размером 3x2 пикселя (изображение увеличено).

Разделение. Чтение изображения осуществляется построчно слева направо. Значения пикселей первой строки в формате RGB следующие: $(255,0,0)$; $(0,255,0)$; $(0,0,255)$. Выполняется перевод из десятичной системы счисления в двоичную значений всех пикселей в формате RGB первой строки изображения. Полученные значения записываются последовательно друг за другом:

$$T_1 = 111111110000000000000000; T_2 = 000000001111111110000000;$$

$$T_3 = 000000000000000011111111.$$

Для каждого полученного значения выполняется перестановка по формуле (2.2):

$$T'_1 = 100100100100100100100100; T'_2 = 010010010010010010010010;$$

$$T'_3 = 001001001001001001001001.$$

Последовательности T'_1 , T'_2 , T'_3 разбиваются на блоки по четыре бита, которые будут являться дробной частью десятичных чисел a_p , $p=1,\dots,18$:

$$a_1 = 0,1001; a_2 = 0,0010; a_3 = 0,0100; a_4 = 0,1001; a_5 = 0,0010; a_6 = 0,0100; a_7 = 0,0100;$$

$$a_8 = 0,1001; a_9 = 0,0010; a_{10} = 0,0100; a_{11} = 0,1001; a_{12} = 0,0010; a_{13} = 0,0010; a_{14} = 0,0100;$$

$$a_{15} = 0,1001; a_{16} = 0,0010; a_{17} = 0,0100; a_{18} = 0,1001.$$

$$\text{По (2.3) находится среднее значение } a_p: a_{s_1} = \frac{\sum_{p=1}^{18} a_p}{18} = \frac{0,6666}{18} = 0,037033333, \text{ и по (2.7),}$$

вычисляются значения a'_p , $p=1,\dots,18$:

$$a'_1 = -0,063066667; a'_2 = 0,036033333; a'_3 = 0,027033333; a'_4 = -0,063066667; a'_5 = 0,036033333;$$

$$a'_6 = 0,027033333; a'_7 = 0,027033333; a'_8 = -0,063066667; a'_9 = 0,036033333; a'_{10} = 0,027033333;$$

$$a'_{11} = -0,063066667; a'_{12} = 0,036033333; a'_{13} = 0,036033333; a'_{14} = 0,027033333; a'_{15} = -0,063066667;$$

$$a'_{16} = 0,036033333; a'_{17} = 0,027033333; a'_{18} = -0,063066667;$$

По (2.5) находятся значения f_i , $i=1,\dots,18$:

$$f_1 = -(-0,063066667) + 2 \cdot (-0,063066667) - 0,036033333 = -0,0991;$$

$$f_2 = -(-0,063066667) + 2 \cdot 0,036033333 - 0,027033333 = 0,1081;$$

$$f_3 = -0,036033333 + 2 \cdot 0,027033333 - (-0,063066667) = 0,0811;$$

$$f_4 = -0,027033333 + 2 \cdot (-0,063066667) - 0,036033333 = -0,1892;$$

$$f_5 = -(-0,063066667) + 2 \cdot 0,036033333 - 0,027033333 = 0,1081;$$

$$f_6 = -0,036033333 + 2 \cdot 0,027033333 - 0,027033333 = -0,009;$$

$$\begin{aligned}
f_7 &= -0,027033333 + 2 \cdot 0,027033333 - (-0,063066667) = 0,0901; \\
f_8 &= -0,027033333 + 2 \cdot (-0,063066667) - 0,036033333 = -0,1892; \\
f_9 &= (-0,063066667) + 2 \cdot 0,036033333 - 0,027033333 = 0,1081; \\
f_{10} &= -0,036033333 + 2 \cdot 0,027033333 - (-0,063066667) = 0,0811; \\
f_{11} &= -0,027033333 + 2 \cdot (-0,063066667) - 0,036033333 = -0,1892; \\
f_{12} &= (-0,063066667) + 2 \cdot 0,036033333 - 0,036033333 = 0,0991; \\
f_{13} &= -0,036033333 + 2 \cdot 0,036033333 - 0,027033333 = 0,009; \\
f_{14} &= -0,036033333 + 2 \cdot 0,027033333 - (-0,063066667) = 0,0811; \\
f_{15} &= -0,027033333 + 2 \cdot (-0,063066667) - 0,036033333 = -0,1892; \\
f_{16} &= (-0,063066667) + 2 \cdot 0,036033333 - 0,027033333 = 0,1081; \\
f_{17} &= -0,036033333 + 2 \cdot 0,027033333 - (-0,063066667) = 0,0811; \\
f_{18} &= -0,027033333 + 2 \cdot (-0,063066667) - (-0,063066667) = -0,0901.
\end{aligned}$$

В итоге получается числовая последовательность:

$$F_1 = [-0,0991; 0,1081; 0,0811; -0,1892; 0,1081; -0,009; 0,0901; -0,1892; 0,1081; 0,0811; -0,1892; 0,0991; 0,009; 0,0811; -0,1892; 0,1081; 0,0811; -0,0901].$$

Аналогичные действия выполняются и для второй строки пикселей изображения, приведённого на рисунке А1.1., в итоге получается числовая последовательность $F_2 = [0,1101; 0; 0; 0; 0; 0,1111; -0,1111; 0; 0; 0; 0; -0,01; -0,0801; 0,1892; -0,1081; -0,0811; 0,1892; -0,2092]$.

Пусть меньшей частью является последовательность знаков чисел из последовательностей F_1 и F_2 и a_{sr_1} , a_{sr_2} , а большей частью являются значения $|f_i|$ из тех же последовательностей F_1 и F_2 .

Таким образом меньшей частью является:

$$\begin{aligned}
& - + + - + - + - + + - + + - + + - \\
& \cdot + + + + + - + + + - - + - - + - \cdot \\
& 0,037033333; 0,061722222
\end{aligned}$$

Большой частью является:

$$\begin{aligned}
& 0,0991; 0,1081; 0,0811; 0,1892; 0,1081; 0,009; 0,0901; 0,1892; 0,1081; 0,0811; 0,1892; 0,0991; \\
& 0,009; 0,0811; 0,1892; 0,1081; 0,0811; 0,0901; \\
& 0,1101; 0; 0; 0; 0; 0,1111; 0,1111; 0; 0; 0; 0; 0,01; 0,0801; 0,1892; 0,1081; 0,0811; 0,1892; 0,2092
\end{aligned}$$

Восстановление. Для восстановления исходного состояния изображения в конкретном примере необходима матрица H размером 18×18 :

$$H = \begin{pmatrix} 2 & -1 & \dots & 0 & -1 \\ -1 & 2 & -1 & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & -1 & 2 & -1 \\ -1 & 0 & \dots & -1 & 2 \end{pmatrix}$$

Для данной матрицы H находятся собственные значения (числа) λ_i и собственные векторы v_i :

$\lambda_i =$	3	$v_i :$
	3	$v_1 = 0,1667 \ 0,1667 \ -0,3333 \ 0,1667 \ 0,1667 \ -0,3333 \ 0,1667 \ 0,1667 \ -0,3333$
	0,4679	$0,1667 \ 0,1667 \ -0,3333 \ 0,1667 \ 0,1667 \ -0,3333 \ 0,1667 \ 0,1667 \ -0,3333;$
	0,4679	$v_2 = 0,2887 \ -0,2887 \ -0,0000 \ 0,2887 \ -0,2887 \ 0,0000 \ 0,2887 \ -0,2887 \ 0,0000$
	0,1206	$0,2887 \ -0,2887 \ -0,0000 \ 0,2887 \ -0,2887 \ 0,0000 \ 0,2887 \ -0,2887 \ 0,0000;$
	0,1206	$v_3 = -0,2143 \ -0,3283 \ -0,2887 \ -0,1140 \ 0,1140 \ 0,2887 \ 0,3283 \ 0,2143 \ -0,0000$
	1	$-0,2143 \ -0,3283 \ -0,2887 \ -0,1140 \ 0,1140 \ 0,2887 \ 0,3283 \ 0,2143 \ 0,0000;$
	1	$v_4 = -0,2553 \ -0,0579 \ 0,1667 \ 0,3132 \ 0,3132 \ 0,1667 \ -0,0579 \ -0,2553 \ -0,3333$
	1,6527	$-0,2553 \ -0,0579 \ 0,1667 \ 0,3132 \ 0,3132 \ 0,1667 \ -0,0579 \ -0,2553 \ -0,3333;$
	1,6527	$v_5 = 0,1140 \ 0,2143 \ 0,2887 \ 0,3283 \ 0,3283 \ 0,2887 \ 0,2143 \ 0,1140 \ -0,0000$
	2,3473	$0,1140 \ -0,2143 \ -0,2887 \ -0,3283 \ -0,3283 \ -0,2887 \ -0,2143 \ -0,1140 \ 0,0000;$
	2,3473	$v_6 = 0,3132 \ 0,2553 \ 0,1667 \ 0,0579 \ -0,0579 \ -0,1667 \ -0,2553 \ -0,3132 \ -0,3333$
	3,5321	$-0,3132 \ -0,2553 \ -0,1667 \ -0,0579 \ 0,0579 \ 0,1667 \ 0,2553 \ 0,3132 \ 0,3333;$
	3,5321	$v_7 = -0,2887 \ -0,2887 \ 0,0000 \ 0,2887 \ 0,2887 \ -0,0000 \ -0,2887 \ -0,2887 \ 0,0000$
	3,8794	$0,2887 \ 0,2887 \ 0,0000 \ -0,2887 \ -0,2887 \ -0,0000 \ 0,2887 \ 0,2887 \ 0,0000;$
	3,8794	$v_8 = -0,1667 \ 0,1667 \ 0,3333 \ 0,1667 \ -0,1667 \ -0,3333 \ -0,1667 \ 0,1667 \ 0,3333$
	0	$0,1667 \ -0,1667 \ -0,3333 \ -0,1667 \ 0,1667 \ 0,3333 \ 0,1667 \ -0,1667 \ -0,3333;$
	4	$v_9 = -0,0579 \ 0,3132 \ 0,1667 \ -0,2553 \ -0,2553 \ 0,1667 \ 0,3132 \ -0,0579 \ -0,3333$
	$-0,0579 \ 0,3132 \ 0,1667 \ -0,2553 \ -0,2553 \ 0,1667 \ 0,3132 \ -0,0579 \ -0,3333;$	
	$v_{10} = 0,3283 \ 0,1140 \ -0,2887 \ -0,2143 \ 0,2143 \ 0,2887 \ -0,1140 \ -0,3283 \ 0,0000$	
	$0,3283 \ 0,1140 \ -0,2887 \ -0,2143 \ 0,2143 \ 0,2887 \ -0,1140 \ -0,3283 \ 0,0000;$	
	$v_{11} = 0,0579 \ 0,3132 \ -0,1667 \ -0,2553 \ 0,2553 \ 0,1667 \ -0,3132 \ -0,0579 \ 0,3333$	
	$-0,0579 \ -0,3132 \ 0,1667 \ 0,2553 \ -0,2553 \ -0,1667 \ 0,3132 \ 0,0579 \ -0,3333;$	
	$v_{12} = 0,3283 \ -0,1140 \ -0,2887 \ 0,2143 \ 0,2143 \ -0,2887 \ -0,1140 \ 0,3283 \ -0,0000$	
	$-0,3283 \ 0,1140 \ 0,2887 \ -0,2143 \ -0,2143 \ 0,2887 \ 0,1140 \ -0,3283 \ 0,0000;$	
	$v_{13} = 0,2553 \ -0,0579 \ -0,1667 \ 0,3132 \ -0,3132 \ 0,1667 \ 0,0579 \ -0,2553 \ 0,3333$	
	$-0,2553 \ 0,0579 \ 0,1667 \ -0,3132 \ 0,3132 \ -0,1667 \ -0,0579 \ 0,2553 \ -0,3333;$	
	$v_{14} = -0,2143 \ 0,3283 \ -0,2887 \ 0,1140 \ 0,1140 \ -0,2887 \ 0,3283 \ -0,2143 \ 0,0000$	
	$0,2143 \ -0,3283 \ 0,2887 \ -0,1140 \ -0,1140 \ 0,2887 \ -0,3283 \ 0,2143 \ 0,0000;$	
	$v_{15} = 0,1140 \ -0,2143 \ 0,2887 \ -0,3283 \ 0,3283 \ -0,2887 \ 0,2143 \ -0,1140 \ 0,0000$	
	$0,1140 \ -0,2143 \ 0,2887 \ -0,3283 \ 0,3283 \ -0,2887 \ 0,2143 \ -0,1140 \ 0,0000;$	
	$v_{16} = -0,3132 \ 0,2553 \ -0,1667 \ 0,0579 \ 0,0579 \ -0,1667 \ 0,2553 \ -0,3132 \ 0,3333$	
	$-0,3132 \ 0,2553 \ -0,1667 \ 0,0579 \ 0,0579 \ -0,1667 \ 0,2553 \ -0,3132 \ 0,3333;$	
	$v_{17} = 0,2357 \ 0,2357 \ 0,2357 \ 0,2357 \ 0,2357 \ 0,2357 \ 0,2357 \ 0,2357 \ 0,2357$	
	$0,2357 \ 0,2357 \ 0,2357 \ 0,2357 \ 0,2357 \ 0,2357 \ 0,2357 \ 0,2357 \ 0,2357;$	
	$v_{18} = 0,2357 \ -0,2357 \ 0,2357 \ -0,2357 \ 0,2357 \ -0,2357 \ 0,2357 \ -0,2357 \ 0,2357$	
	$-0,2357 \ 0,2357 \ -0,2357 \ 0,2357 \ -0,2357 \ 0,2357 \ -0,2357 \ 0,2357 \ -0,2357.$	

Выполняется объединение частей (подстановка соответствующих знаков) и находится скалярное произведение, полученных после объединения частей, с собственными векторами v_i матрицы H по (2.7):

$$\beta_1 = (S, \nu_1) = \begin{pmatrix} -0,0991 \\ 0,1081 \\ 0,0811 \\ -0,1892 \\ 0,1081 \\ -0,009 \\ 0,0901 \\ -0,1892 \\ 0,1081 \\ 0,0811 \\ -0,1892 \\ 0,0991 \\ 0,009 \\ 0,0811 \\ -0,1892 \\ 0,1081 \\ 0,0811 \\ -0,0901 \end{pmatrix} \cdot \begin{pmatrix} 0,2886 \\ -0,2887 \\ 0,0001492 \\ 0,2886 \\ -0,2887 \\ 0,0001492 \\ 0,2886 \\ -0,2887 \\ 0,0001492 \\ 0,2886 \\ -0,2887 \\ 0,0001492 \\ 0,2886 \\ -0,2887 \\ 0,0001492 \\ 0,2886 \\ -0,2887 \\ 0,0001492 \end{pmatrix} = -0,0991 \cdot 0,2886 + 0,1081 \cdot (-0,2887) +$$

$$+0,0811 \cdot 0,0001492 + (-0,1892) \cdot 0,2886 + 0,1081 \cdot (-0,2887) + (-0,009) \cdot 0,0001492 + \\ +0,0901 \cdot 0,2886 + (-0,1892) \cdot (-0,2887) + 0,1081 \cdot 0,0001492 + 0,0811 \cdot 0,2886 + \\ + (-0,1892) \cdot (-0,2887) + 0,0991 \cdot 0,0001492 + 0,009 \cdot 0,2886 + 0,0811 \cdot (-0,2887) + \\ + (-0,1892) \cdot 0,0001492 + 0,1081 \cdot 0,2886 + 0,0811 \cdot (-0,2887) + (-0,0901) \cdot 0,0001492 = 0$$

Аналогично находятся другие значения скалярных произведений:

$$\beta_2 = (S, \nu_2) = 0; \quad \beta_3 = (S, \nu_3) = 0,0053; \quad \beta_4 = (S, \nu_4) = -0,0192; \quad \beta_5 = (S, \nu_5) = -0,0009; \\ \beta_6 = (S, \nu_6) = -0,0034; \quad \beta_7 = (S, \nu_7) = 0; \quad \beta_8 = (S, \nu_8) = 0; \quad \beta_9 = (S, \nu_9) = -0,0366; \\ \beta_{10} = (S, \nu_{10}) = 0,0278; \quad \beta_{11} = (S, \nu_{11}) = -0,2907; \quad \beta_{12} = (S, \nu_{12}) = 0,2296; \quad \beta_{13} = (S, \nu_{13}) = 0,1037; \\ \beta_{14} = (S, \nu_{14}) = 0,0726; \quad \beta_{15} = (S, \nu_{15}) = -0,1215; \quad \beta_{16} = (S, \nu_{16}) = -0,2861; \quad \beta_{17} = (S, \nu_{17}) = 0; \\ \beta_{18} = (S, \nu_{18}) = 0.$$

Находятся значения одномерного массива данных (вектора) A' по (2.8):

$$A' = \sum_{i=1}^{6-M} \frac{\beta_i}{\lambda_i} \cdot v_i = \frac{0}{3} \cdot \begin{pmatrix} 0,2886 \\ -0,2887 \\ 0,0001492 \\ 0,2886 \\ -0,2887 \\ 0,0001492 \\ 0,2886 \\ -0,2887 \\ 0,0001492 \\ 0,2886 \\ -0,2887 \\ 0,0001492 \\ 0,2886 \\ -0,2887 \\ 0,0001492 \\ 0,2886 \\ -0,2887 \\ 0,0001492 \end{pmatrix} + \frac{0}{3} \cdot \begin{pmatrix} -0,1668 \\ -0,1665 \\ 0,3333 \\ -0,1668 \\ -0,1665 \\ 0,3333 \\ -0,1668 \\ -0,1665 \\ 0,3333 \\ -0,1668 \\ -0,1665 \\ 0,3333 \\ -0,1668 \\ -0,1665 \\ 0,3333 \\ -0,1668 \\ -0,1665 \\ 0,3333 \end{pmatrix} + \frac{0,0053}{0,4679} \cdot \begin{pmatrix} -0,2141 \\ -0,3282 \\ -0,2887 \\ -0,1141 \\ 0,1139 \\ 0,2886 \\ 0,3283 \\ 0,2144 \\ 0,0001478 \\ -0,2141 \\ -0,3282 \\ -0,2887 \\ -0,1141 \\ 0,1139 \\ 0,2886 \\ 0,3283 \\ 0,2144 \\ 0,0001478 \end{pmatrix} + \\
 -\frac{0,0192}{0,4679} \cdot \begin{pmatrix} 0,2554 \\ 0,05803 \\ -0,1665 \\ -0,3132 \\ -0,3133 \\ -0,1668 \\ 0,05774 \\ 0,2553 \\ 0,3333 \\ 0,2554 \\ 0,05803 \\ -0,1665 \\ -0,3132 \\ -0,3133 \\ -0,1668 \\ 0,05774 \\ 0,2553 \\ 0,3333 \end{pmatrix} + \frac{0,0009}{0,1206} \cdot \begin{pmatrix} 0,1105 \\ 0,2114 \\ 0,2868 \\ 0,3276 \\ 0,3289 \\ 0,2905 \\ 0,2171 \\ 0,1175 \\ 0,003768 \\ -0,1105 \\ -0,2114 \\ -0,2868 \\ -0,3276 \\ -0,3289 \\ -0,2905 \\ -0,2171 \\ -0,1175 \\ -0,003768 \end{pmatrix} + \frac{-0,0034}{0,1206} \cdot \begin{pmatrix} -0,3145 \\ -0,2578 \\ -0,1699 \\ -0,06159 \\ 0,05417 \\ 0,1634 \\ 0,2529 \\ 0,3119 \\ 0,3333 \\ 0,3145 \\ 0,2578 \\ 0,1699 \\ 0,06159 \\ -0,05417 \\ -0,1634 \\ -0,2529 \\ -0,3119 \\ -0,3333 \end{pmatrix} + \frac{0}{1} \cdot \begin{pmatrix} 0,2359 \\ 0,3219 \\ 0,08599 \\ -0,2359 \\ -0,3219 \\ -0,08599 \\ 0,2359 \\ 0,3219 \\ 0,08599 \\ -0,2359 \\ -0,3219 \\ -0,08599 \\ 0,2359 \\ 0,3219 \\ 0,08599 \\ -0,2359 \\ -0,3219 \\ -0,08599 \end{pmatrix} +$$

$$\begin{aligned}
 & + \frac{0}{1} \cdot \begin{pmatrix} -0,2355 \\ 0,08656 \\ 0,3221 \\ 0,2355 \\ -0,08656 \\ -0,3221 \\ -0,2355 \\ 0,08656 \\ 0,3221 \\ 0,2355 \\ -0,08656 \\ -0,3221 \\ -0,2355 \\ 0,08656 \\ 0,3221 \\ 0,2355 \\ -0,08656 \\ -0,3221 \end{pmatrix} + \frac{-0,0366}{1,6527} \cdot \begin{pmatrix} 0,3331 \\ 0,06888 \\ -0,3092 \\ -0,1763 \\ 0,248 \\ 0,2624 \\ -0,1569 \\ -0,3169 \\ 0,04682 \\ 0,3331 \\ 0,06888 \\ -0,3092 \\ -0,1763 \\ 0,248 \\ 0,2624 \\ -0,1569 \\ -0,3169 \\ 0,04682 \end{pmatrix} + \frac{0,0278}{1,6527} \cdot \begin{pmatrix} -0,0112 \\ 0,3261 \\ 0,1245 \\ -0,2829 \\ -0,2227 \\ 0,2056 \\ 0,2941 \\ -0,1034 \\ -0,33 \\ -0,0112 \\ 0,3261 \\ 0,1245 \\ -0,2829 \\ -0,2227 \\ 0,2056 \\ 0,2941 \\ -0,1034 \\ -0,33 \end{pmatrix} + \frac{-0,2907}{2,3473} \cdot \begin{pmatrix} 0,3198 \\ -0,1483 \\ -0,2683 \\ 0,2414 \\ 0,1844 \\ -0,3055 \\ -0,07833 \\ 0,3327 \\ -0,03721 \\ -0,3198 \\ 0,1483 \\ 0,2683 \\ -0,2414 \\ -0,1844 \\ 0,3055 \\ 0,07833 \\ -0,3327 \\ 0,03721 \end{pmatrix} + \\
 & + \frac{0,2296}{2,3473} \cdot \begin{pmatrix} 0,09417 \\ 0,2985 \\ -0,1979 \\ -0,2298 \\ 0,2777 \\ 0,1334 \\ -0,324 \\ -0,02087 \\ 0,3312 \\ -0,09417 \\ -0,2985 \\ 0,1979 \\ 0,2298 \\ -0,2777 \\ -0,1334 \\ 0,324 \\ 0,02087 \\ -0,3312 \end{pmatrix} + \frac{0,1037}{3,5321} \cdot \begin{pmatrix} -0,2881 \\ 0,3285 \\ -0,2151 \\ 0,001125 \\ 0,2134 \\ -0,3281 \\ 0,2892 \\ -0,1151 \\ -0,1129 \\ 0,2881 \\ -0,3285 \\ 0,2151 \\ -0,001125 \\ -0,2134 \\ 0,3281 \\ -0,2892 \\ 0,1151 \\ 0,1129 \end{pmatrix} + \frac{0,0726}{3,5321} \cdot \begin{pmatrix} 0,1676 \\ 0,05677 \\ -0,2546 \\ 0,3333 \\ -0,2561 \\ 0,05899 \\ 0,1657 \\ -0,3128 \\ 0,3136 \\ -0,1676 \\ -0,05677 \\ 0,2546 \\ -0,3333 \\ 0,2561 \\ -0,05899 \\ -0,1657 \\ 0,3128 \\ -0,3136 \end{pmatrix} +
 \end{aligned}$$

$$\begin{pmatrix} 0,2935 \\ -0,2217 \\ 0,1232 \\ -0,009873 \\ -0,1047 \\ 0,2066 \\ -0,2836 \\ 0,3264 \\ -0,3298 \\ 0,2935 \\ -0,2217 \\ 0,1232 \\ -0,009873 \\ -0,1047 \\ 0,2066 \\ -0,2836 \\ 0,3264 \\ -0,3298 \end{pmatrix} + \frac{-0,1215}{3,8794} \cdot \begin{pmatrix} -0,158 \\ 0,2489 \\ -0,3097 \\ 0,3332 \\ -0,3165 \\ 0,2616 \\ -0,1751 \\ 0,06758 \\ 0,04813 \\ -0,158 \\ 0,2489 \\ -0,3097 \\ 0,3332 \\ -0,3165 \\ 0,2616 \\ -0,1751 \\ 0,06758 \\ 0,04813 \end{pmatrix} + \frac{-0,2861}{3,8794} \cdot \begin{pmatrix} -0,2357 \\ -0,2357 \\ -0,2357 \\ -0,2357 \\ -0,2357 \\ -0,2357 \\ -0,2357 \\ -0,2357 \\ -0,2357 \\ -0,2357 \\ -0,2357 \\ -0,2357 \\ -0,2357 \\ -0,2357 \\ -0,2357 \\ -0,2357 \\ -0,2357 \\ -0,2357 \end{pmatrix} + \frac{0}{0} \cdot \begin{pmatrix} 0,2357 \\ -0,2357 \\ 0,2357 \\ -0,2357 \\ 0,2357 \\ -0,2357 \\ 0,2357 \\ -0,2357 \\ 0,2357 \\ -0,2357 \\ 0,2357 \\ -0,2357 \\ 0,2357 \\ -0,2357 \\ 0,2357 \\ -0,2357 \\ 0,2357 \\ -0,2357 \end{pmatrix} + \frac{0}{4} \cdot \begin{pmatrix} 0,2357 \\ -0,2357 \\ 0,2357 \\ -0,2357 \\ 0,2357 \\ -0,2357 \\ 0,2357 \\ -0,2357 \\ 0,2357 \\ -0,2357 \\ 0,2357 \\ -0,2357 \\ 0,2357 \\ -0,2357 \\ 0,2357 \\ -0,2357 \\ 0,2357 \\ -0,2357 \end{pmatrix} = \begin{pmatrix} -0,0631 \\ 0,036 \\ 0,027 \\ -0,0631 \\ 0,036 \\ 0,027 \\ 0,027 \\ -0,0631 \\ 0,036 \\ 0,027 \\ -0,0631 \\ 0,036 \\ 0,036 \\ 0,027 \\ -0,0631 \\ 0,036 \\ 0,027 \\ -0,0631 \end{pmatrix}$$

Далее по (2.9) находятся a_i :

$$\begin{aligned}
a_1 &= 0,0370 - (-0,0631) = 0,1001; & a_2 &= 0,0370 - 0,0360 = 0,0010; & a_3 &= 0,0370 - 0,0270 = 0,0100; \\
a_4 &= 0,0370 - (-0,0631) = 0,1001; & a_5 &= 0,0370 - 0,0360 = 0,0010; & a_6 &= 0,0370 - 0,0270 = 0,0100; \\
a_7 &= 0,0370 - 0,0270 = 0,0100; & a_8 &= 0,0370 - (-0,0631) = 0,1001; & a_9 &= 0,0370 - 0,0360 = 0,0010; \\
a_{10} &= 0,0370 - 0,0270 = 0,0100; & a_{11} &= 0,0370 - (-0,0631) = 0,1001; & a_{12} &= 0,0370 - 0,0360 = 0,0010; \\
a_{13} &= 0,0370 - 0,0360 = 0,0010; & a_{14} &= 0,0370 - 0,0270 = 0,0100; & a_{15} &= 0,0370 - (-0,0631) = 0,1001; \\
a_{16} &= 0,0370 - 0,0360 = 0,0010; & a_{17} &= 0,0370 - 0,0270 = 0,0100; & a_{18} &= 0,0370 - (-0,0631) = 0,1001.
\end{aligned}$$

Дробные части полученных a_i записываются последовательно друг за другом и разбиваются на три части по 24 бита:

$$T'_1 = 100100100100100100100100;$$

$$T'_2 = 010010010010010010010010;$$

$$T'_3 = 001001001001001001001001.$$

Затем выполняется обратная перестановка перестановке (2.2)

$$T_1 = 111111110000000000000000;$$

$$T_2 = 000000001111111100000000;$$

$$T_3 = 000000000000000011111111.$$

Полученные последовательности делятся по 8 бит, которые затем переводятся в десятичную систему счисления, в результате чего будут получены значения пикселей первой строки изображения, приведенного рисунке А1.1: $(255, 0, 0)$; $(0, 255, 0)$; $(0, 0, 255)$.

Аналогичные действия осуществляются и для второй строки пикселей изображения, приведенного на рисунке А1.1.

Находится скалярное произведение по формуле (2.7):

$$\beta_1 = -0,1561; \beta_2 = -0,108; \beta_3 = -0,0117; \beta_4 = -0,0374; \beta_5 = 0,0148; \beta_6 = -0,0126; \beta_7 = 0; \beta_8 = 0;$$

$\beta_9 = 0,062$; $\beta_{10} = -0,0284$; $\beta_{11} = -0,1184$; $\beta_{12} = 0,0497$; $\beta_{13} = -0,1566$; $\beta_{14} = 0,2283$; $\beta_{15} = 0,198$;
 $\beta_{16} = -0,0637$; $\beta_{17} = 0$; $\beta_{18} = 0$.

Находятся значения одномерного массива данных (вектора) A' по (2.8):

$$A' = \sum_{i=1}^{6-M} \frac{\beta_i}{\lambda_i} \cdot v_i = \begin{pmatrix} 0,0617 \\ 0,0617 \\ 0,0617 \\ 0,0617 \\ 0,0617 \\ 0,0617 \\ -0,0494 \\ -0,0494 \\ -0,0494 \\ -0,0494 \\ -0,0494 \\ -0,0494 \\ -0,0494 \\ -0,0394 \\ 0,0507 \\ -0,0484 \\ -0,0394 \\ 0,0507 \\ -0,0484 \end{pmatrix}$$

Далее по формуле (2.9) находятся значения a_i :

$a_1 = 0,0617 - 0,0617 = 0,0000$; $a_2 = 0,0617 - 0,0617 = 0,0000$; $a_3 = 0,0617 - 0,0617 = 0,0000$;
 $a_4 = 0,0617 - 0,0617 = 0,0000$; $a_5 = 0,0617 - 0,0617 = 0,0000$; $a_6 = 0,0617 - 0,0617 = 0,0000$;
 $a_7 = 0,0617 - (-0,0494) = 0,1111$; $a_8 = 0,0617 - (-0,0494) = 0,1111$; $a_9 = 0,0617 - (-0,0494) = 0,1111$;
 $a_{10} = 0,0617 - (-0,0494) = 0,1111$; $a_{11} = 0,0617 - (-0,0494) = 0,1111$; $a_{12} = 0,0617 - (-0,0494) = 0,1111$;
 $a_{13} = 0,0617 - (-0,0394) = 0,1011$; $a_{14} = 0,0617 - 0,0507 = 0,0110$; $a_{15} = 0,0617 - (-0,0484) = 0,1101$;
 $a_{16} = 0,0617 - (-0,0394) = 0,1011$; $a_{17} = 0,0617 - 0,0507 = 0,0110$; $a_{18} = 0,0617 - (-0,0484) = 0,1101$

Полученные дробные части a_i записываются последовательно друг за другом и разбиваются на три части по 24 бита:

$$T_1' = 00000000000000000000000000000000;$$

$$T_2' = 11111111111111111111111111111111;$$

$$T_3' = 101101101101101101101101101101.$$

Затем выполняется обратная перестановка перестановке (2.2)

$$T_1 = 00000000000000000000000000000000;$$

$$T_2 = 11111111111111111111111111111111;$$

$$T_3 = 11111111000000000111111111.$$

Полученные последовательности делятся по 8 бит, которые переводятся в десятичную систему счисления, в результате чего будут получены значения пикселей второй строки изображения, приведенного рисунке A1.1: $(0,0,0)$; $(255,255,255)$; $(255,0,255)$.

ПРИЛОЖЕНИЕ Б. СВИДЕТЕЛЬСТВА О РЕГИСТРАЦИИ ПРОГРАММ ЭВМ

РОССИЙСКАЯ ФЕДЕРАЦИЯ



СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2013661618

Программа, реализующая алгоритм схемы разделения секрета с принципиально малой частью секрета, основанный на нахождении собственных чисел и собственных векторов по методу Якоби для квадратной и симметричной относительно главной диагонали матрицы

Правообладатель: *Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Омский государственный технический университет» (RU)*

Автор: *Сагайдак Дмитрий Анатольевич (RU)*

Заявка № 2013619791

Дата поступления 28 октября 2013 г.

Дата государственной регистрации

в Реестре программ для ЭВМ 11 декабря 2013 г.



Руководитель Федеральной службы
по интеллектуальной собственности

Б.П. Симонов

РОССИЙСКАЯ ФЕДЕРАЦИЯ



СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2013661611

Программа, реализующая алгоритм префиксного кодирования видеoinформации, основанного на примитивизации дельта-кода Элиаса в схеме разделения секрета с принципиально малой частью секрета

Правообладатель: *Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Омский государственный технический университет» (RU)*

Автор: *Сагайдак Дмитрий Анатольевич (RU)*

Заявка № 2013619795

Дата поступления 25 октября 2013 г.

Дата государственной регистрации

в Реестре программ для ЭВМ 11 декабря 2013 г.



Руководитель Федеральной службы
по интеллектуальной собственности

Б.П. Симонов

РОССИЙСКАЯ ФЕДЕРАЦИЯ



СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2014615225

Программа, реализующая способ формирования и внедрения цифрового водяного знака, способного нести в себе какую-либо определенную информацию, в изображениях, представленные в цифровом виде

Правообладатель: *Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Омский государственный технический университет» (RU)*

Автор: *Сагайдак Дмитрий Анатольевич (RU)*

Заявка № **2014612760**

Дата поступления **31 марта 2014 г.**

Дата государственной регистрации
в Реестре программ для ЭВМ **21 мая 2014 г.**



*Руководитель Федеральной службы
по интеллектуальной собственности*

Б.П. Симонов

РОССИЙСКАЯ ФЕДЕРАЦИЯ



СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2024688412

**Программа моделирования экспоненциальной сети с
двумя каналами связи и произвольным входящим
потокком заявок**

Правообладатель: *Федеральное государственное автономное
образовательное учреждение высшего образования
«Омский государственный технический университет»
(RU)*

Автор(ы): *Сагайдак Дмитрий Анатольевич (RU)*



Заявка № **2024685986**

Дата поступления **01 ноября 2024 г.**

Дата государственной регистрации

в Реестре программ для ЭВМ **27 ноября 2024 г.**

*Руководитель Федеральной службы
по интеллектуальной собственности*

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат 0492e7b3ae3005b54240670bca2026
Экземляр: **Зубов Юрий Сергеевич**
Действителен с 10.11.2024 по 03.10.2025

Ю.С. Зубов

РОССИЙСКАЯ ФЕДЕРАЦИЯ



СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2024686592

Программа моделирования системы связи с двумя синхронными каналами, обладающими разными пропускными способностями

Правообладатель: *Федеральное государственное автономное образовательное учреждение высшего образования «Омский государственный технический университет» (RU)*

Авторы: *Сагайдак Дмитрий Анатольевич (RU), Денисова Людмила Альбертовна (RU)*

Заявка № **2024686077**

Дата поступления **01 ноября 2024 г.**

Дата государственной регистрации

в Реестре программ для ЭВМ **11 ноября 2024 г.**



Руководитель Федеральной службы по интеллектуальной собственности

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат 0492e7b3ae3005b54240670bca2026
Владелец: **Зубов Юрий Сергеевич**
Действителен с 10.11.2024 по 03.10.2025

Ю.С. Зубов

ПРИЛОЖЕНИЕ В. АКТЫ ВНЕДРЕНИЯ

УТВЕРЖДАЮ



АКТ

о практическом использовании научных исследований и разработок, полученных в диссертационной работе Сагайдака Дмитрия Анатольевича.

Результаты диссертационной работы начальника отдела управления безопасности филиала АО «ОДК» «ОМО им. П.И. Баранова» (далее – филиал) Д.А. Сагайдака были применены:

– при реализации проекта по внедрению в филиале информационной системы цифровизации промышленных предприятий «Диспетчер» (определена необходимая пропускная способность внедряемого межсетевого экрана в зависимости от объема трафика в промышленной сети);

– для оптимизации параметров пропускных способностей каналов связи корпоративной системы передачи данных (осуществлен переход на новые тарифы провайдера с гарантированной скоростью передачи данных для необходимого объема передаваемого трафика);

– при реализации проекта по организации защищенного канала связи передачи данных, связывающего филиал и удаленные производственные площадки (выполнен расчет необходимых пропускных способностей каналов связи и осуществлен выбор необходимых для внедрения криптографических шлюзов/коммутаторов определенной производительности);

– при организации в филиале режима защиты и конфиденциальности данных (защищённая передача цифровых изображений большого объема).

Непосредственно использованы следующие научные результаты:

– аналитические методы оптимизации двуканальной системы с разделением данных по каналам связи;

– методика, основанная на имитационной модели двуканальной системы связи, позволяющая с использованием генетического алгоритма определять оптимальные пропускные способности каналов;

– методика повышения уровня защищённости цифровых изображений основанная на схемах разделения их на неравные части;

– модули из комплекса программ, реализующего системный подход к организации защищенной передачи данных.

Настоящим актом подтверждается, что результаты диссертационного исследования Д.А. Сагайдака актуальны, представляют практический интерес в области системного подхода для решения задач, связанных со стабильностью работы и защищенностью систем передачи данных.

Начальник управления безопасности

Е.А. Шевченко

Федеральное государственное автономное образовательное учреждение
 высшего образования
 «Омский государственный технический университет»
 Кафедра «Автоматизированные системы обработки информации и управления (АСОИУ)»

от «13» марта 2025 г.
 г. Омск
 Об использовании научных исследований и разработок в учебном процессе



УТВЕРЖДАЮ

Проректор по образовательной деятельности

Н.А. Прокудина

«14» марта 2025 г.

АКТ ВНЕДРЕНИЯ

Основание: научные исследования, выполненные аспирантом кафедры АСОИУ Сагайдаком Д.А.

Составлен комиссией в составе:

Белик А.Г. – зав. кафедрой АСОИУ, председатель комиссии;
 Цыганенко В.Н., доцент кафедры АСОИУ;
 Викулов Е.О. – доцент кафедры АСОИУ.

1. Теоретические разработки Сагайдака Д.А., опубликованные в статьях:

– Сагайдак, Д.А. Организация распределенной передачи видеоданных по двум каналам связи в целях их защиты / Д.А. Сагайдак // Автоматизация в промышленности. – 2024. – № 12. – С. 53-56.

– Сагайдак, Д.А. Математическое обеспечение системы обработки видеоданных, разделяемых для передачи по двум каналам связи с целью их защиты / Д.А. Сагайдак // Автоматизация в промышленности. – 2024. – № 7. – С. 14-18.

– Сагайдак, Д.А. Защищенная двухканальная система видеосвязи с использованием схемы разделения секрета и оптимизацией параметров на основе генетического алгоритма / Д.А. Сагайдак, Л.А. Денисова // Системы управления, связи и безопасности. – 2024. – № 3. – С. 126-156.

– Свидетельство о государственной регистрации программ для ЭВМ № 2024686592. Российская Федерация. Программа моделирования системы связи с двумя синхронными каналами, обладающими разными пропускными способностями; заяв. 01.11.2024; опубл. 11.11.2024 / Д.А. Сагайдак, Л.А. Денисова; заявитель и патентообладатель ФГБОУ ВПО ОмГТУ.

– Сагайдак, Д.А. Оптимизации передачи видеоданных с демультимплексированием по двум каналам связи с различными характеристикам / Д.А. Сагайдак // Информационные технологии и автоматизация управления: Материалы XIV Всероссийской научно-практической конференции студентов, аспирантов, работников образования и промышленности. – Омск: ОмГТУ, 2023. – С. 196-201.

– Задорожный, В.Н. Оптимизация передачи сообщений, разделяемых на разные доли, передаваемые по двум разным каналам / В.Н. Задорожный, Д.А. Сагайдак // Системы управления, информационные технологии и математическое моделирование: Материалы III Всероссийской научно-практической конференции с международным участием. Том I. – Омск: ОмГТУ, 2021. – С. 59-80.

– Zadorozhnyi, V. Optimization of message transmission when implementing the secret sharing scheme / V. Zadorozhnyi, D. Sagaydak // Informational technologies and mathematical modelling (ITMM-2021), 01–05 декабря 2021 года. – Национальный исследовательский Томский государственный университет, 2022. – P. 137-144.

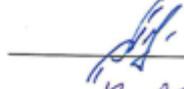
используются в следующих учебных дисциплинах кафедры АСОИУ:

- «Теоретические основы автоматизированного управления»
- «Обеспечивающие подсистемы информационных и автоматизированных систем»
- «Автоматизированные системы управления»;
- «Моделирование систем».

2. В основе учебно-методических разработок, используемых в перечисленных учебных дисциплинах кафедры АСОИУ, лежат следующие научные результаты исследований Сагайдака Д.А.:

- аналитический метод расчета оптимальных пропускных способностей двухканальной системы с учетом характеристик передаваемого потока данных, разделяемых на неравные части;
- методика, основанная на имитационной модели двухканальной системы связи, которая с использованием генетического алгоритма позволяет определять оптимальные пропускные способности каналов при максимальном объеме передаваемых данных с обеспечением их синхронной работы;
- алгоритмы разделения данных между двумя каналами связи, структура программного комплекса для проведения экспериментальных исследований.

Председатель комиссии

 _____ /А.Г. Белик/

Члены комиссии

 _____ /В.Н. Цыганенко/
 _____ /Е.О. Викулов/