



Сагайдак Дмитрий Анатольевич

**МОДЕЛИ И АЛГОРИТМЫ РЕАЛИЗАЦИИ
СИСТЕМНОГО ПОДХОДА К ОРГАНИЗАЦИИ
РАСПРЕДЕЛЕННОЙ ПЕРЕДАЧИ ВИДЕОДАННЫХ**

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

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Работа выполнена в федеральном государственном автономном образовательном учреждении высшего образования «Омский государственный технический университет» (ОмГТУ).

Научный руководитель: **Денисова Людмила Альбертовна**,
доктор технических наук, профессор.

Официальные оппоненты: **Сервах Владимир Вицентьевич**,
доктор физико-математических наук, старший научный сотрудник, старший научный сотрудник лаборатории дискретной оптимизации Омского филиала федерального государственного бюджетного учреждения науки «Институт математики им. С.Л. Соболева Сибирского отделения Российской академии наук», г. Омск.

Матренин Павел Викторович,
кандидат технических наук, ведущий научный сотрудник научной лаборатории цифровых двойников в электроэнергетике федерального государственного автономного образовательного учреждения высшего образования «Уральский федеральный университет имени первого президента России Б.Н. Ельцина», г. Екатеринбург.

Ведущая организация: Федеральное государственное бюджетное образовательное учреждение высшего образования «Алтайский государственный технический университет им. И.И. Ползунова», г. Барнаул.

Защита состоится «27» июня 2025 г. в 15-00 на заседании диссертационного совета 24.2.350.07, созданного на базе ФГАОУ ВО «Омский государственный технический университет», по адресу: 644050, Омск, просп. Мира, д. 11, Главный корпус, ауд. П-202.

С диссертацией можно ознакомиться в библиотеке ФГАОУ ВО «Омский государственный технический университет» и на сайте www.omgtu.ru.

Автореферат разослан «__» _____ 2025 года.

Ученый секретарь диссертационного совета
24.2.350.07, канд. техн. наук, доцент



Грицай А.С.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Системы видеонаблюдения и передачи видеoinформации в настоящий время используются повсеместно, будь то системы охранного видеонаблюдения или системы передачи видеоданных от 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. Поэтому развитие и внедрение комплексных систем удаленного видеомониторинга приводит к формированию больших объемов данных, для которых требуется обеспечивать надежность передачи, конфиденциальность и подлинность. Также в связи с развитием беспилотного транспорта, неотъемлемой частью которого являются системы передачи видеоданных и телеметрии, в соответствии с Транспортной Стратегией Российской Федерации до 2030 года с прогнозом на период до 2035 года, при функционировании беспилотных транспортных средств на всех видах транспорта (беспилотные автомобили, воздушные суда, железнодорожный и водный транспорт) требуется обеспечивать бесперебойность, защищенность и приемлемую скорость передачи видеоданных. Поэтому в условиях развития вычислительных сетей и систем с многоканальной архитектурой актуальность темы диссертационной работы определяется необходимостью организации распределённой передачи видеоданных с применением системного подхода. Это позволит обеспечить бесперебойность, скорость и конфиденциальность передачи информации при одновременной минимизации затрат на содержание систем связи.

Состояние вопроса. Анализ исследований, направленных на решение задач распределенной передачи изображений с использованием схем разделения данных, а также разработки систем демультиплексирования видеоданных для их распределенной передачи по многоканальным системам связи, выявил необходимость применения системного подхода. Такой подход предполагает не только создание эффективных алгоритмов кодирования изображений и видеоданных, но и применение аналитических расчетов и имитационных моделей для оптимизации параметров системы связи.

Разработке методов и алгоритмов разделения изображений на части в целях их кодирования и распределенной передачи посвящены работы зарубежных и отечественных авторов: M. Naor, A. Shamir, C. Asmuth, J. Bloom, D. Jin, W.Q. Yan, M.S. Kankanhalli, P.T. Файзуллина, В.И. Ефимова, В.И. Дулькейта и др., а в настоящее время в работах авторов: М.Н. Tsai, I. Padiya, A. Vidhate, S. Rathnamala, Д.Н. Лаврова, Н.И. Червякова, Ю.В. Косолапова и др. – предлагаются новые алгоритмы разделения

изображений, повышающие уровень их конфиденциальности и позволяющие уменьшить части, полученные в результате разделения.

Исследования систем с делением и слиянием заявок, систем с параллельной передачей данных представлены в работах таких авторов, как L. Flatto, R. Nelson, A. Thomasian, I. Tsimashenka, W.J. Knottenbelt, A. Duda, Ю.И. Рыжиков, С.П. Моисеева, П.П. Бочаров, И.С. Зарядов, Э.С. Сопин, А.Ф. Терпугов и др. В указанных исследованиях преимущественно представлены аналитические результаты. В более поздних работах А.В. Горбуновой, А.В. Лебедева, В.М. Вишневского, В.Н. Задорожного рассматривается имитационное моделирование систем с делением и слиянием заявок. Оптимизация двухканальных систем связи формулируется как многокритериальная задача и решается с использованием Парето-аппроксимации на основе генетических алгоритмов. Большинство зарубежных исследователей: L. Fogel, J. Holland, K. Deb, H.B. Gurocak, F. Herrera и J. Wu, а также отечественные ученые, такие как А.И. Змитрович, В.М. Курейчик, В.П. Северин, А.Н. Скурихин и др. рассматривают генетические алгоритмы как один из наиболее перспективных методов оптимизации.

Анализ существующих методов и алгоритмов разделения изображений показал, что они не учитывают или учитывают не в полной мере технические требования, предъявляемые к системам распределенной передачи данных. В то же время при проектировании таких систем не принимаются во внимание вычислительные сложности используемых алгоритмов кодирования видеоданных. В связи с этим перспективным направлением является разработка алгоритмов кодирования видеоданных, методики аналитических расчетов и имитационной модели, реализующих системный подход к организации распределенной передачи данных. Такой подход позволит повысить стабильность работы систем передачи видеоданных, сократить расходы на их содержание 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.

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: алгоритмы кодирования видеоданных, основанные на разделении кадров для передачи по разным каналам (1), методика аналитического расчета пропускных способностей каналов (2), имитационная модель двухканальной системы связи (3).

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, позволяющее исключить возможность восстановления исходного изображения кадра по одной из его частей без информации о второй. Это дает возможность передавать видеоданные 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: пропускные способности двухканальной и одноканальной систем связи одинаковы).

Кроме того, особенностью методики 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 определение условий синхронной передачи частей разделяемых кадров видеоданных, что позволяет обеспечить бесперебойную передачу видеоданных при минимальных временных и стоимостных издержках.

Теоретическая значимость работы заключается в:

- разработке алгоритмов кодирования видеоданных с помощью разделения кадров на части неравного размера, позволяющего исключить возможность восстановления изображения кадра по одной из его частей без информации о второй;
- 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 их конфиденциальности при передаче;
- 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 гг.) для решения поставленных задач по оптимизации и выбору параметров каналов связи, для обеспечения конфиденциального обмена изображениями.

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

Объектом исследования являются технологии и системы кодирования видеоданных, предназначенные для распределенной передачи, двухканальные системы связи с каналами, обладающими различными пропускными способностями.

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.

Основные результаты, полученные автором и выносимые на защиту.

1. Алгоритмы кодирования видеоданных, предусматривающие разделение кадров на части неравного размера, обеспечивающие конфиденциальность (исключение возможности восстановления полного изображения кадра по его большей части без доступа к меньшей) и распределенную 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: свойство сохраняется для любого потока данных). Теорема 3: двухканальная система связи при передаче по ее каналам данных, разделенных в постоянном соотношении, является системой с их синхронной передачей (следствие – Теорема 4: свойство сохраняется для любого потока данных).

3. Имитационная модель двухканальной системы видеосвязи, позволяющая в совокупности с генетическим алгоритмом выполнить многокритериальную

оптимизацию ее параметров. Особенностью такого подхода к оптимизации параметров системы является обеспечение синхронной передачи частей разделяемых кадров видеоданных, что позволяет при минимальных временных и стоимостных 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).

Соответствие паспорту специальности. Диссертация соответствует областям исследований: 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. Результаты работы отражались в научных докладах, которые представлялись на II, IV Всероссийских молодежных научно-технических конференциях «Россия молодая: передовые технологии – в промышленность» (г. Омск, 2009, 2011); Научно-практическом семинаре «Актуальные проблемы обеспечения информационной безопасности: подходы и решения» в рамках форума «ПромТехЭкспо-2011» (г. Омск, 2011);

XII Всероссийском конкурсе–конференции студентов и аспирантов по информационной безопасности «SIBINFO-2012» (г. Томск, 2012); VIII Международной научно-практической конференции «Электронные средства и системы управления» (г. Томск, 2012); 11-ой Международной конференции «Распознавание образов и анализ изображений – 2013» (г. Самара, 2013); XIV Всероссийском конкурсе–конференции студентов и аспирантов по информационной безопасности «SIBINFO-2014» (диплом III степени, г. Томск, 2014); III Всероссийской научно-практической конференции с международным участием «Системы управления, информационные технологии и математическое моделирование» (г. Омск, 2021); VIII, XV Международных научно–технических конференциях «Динамика систем, механизмов и машин» (г. Омск, 2012, 2021); 24th International Conference named after A. F. Terpugov «Informational technologies and mathematical modeling» (ITMM–2021) (г. Томск, 2021); VI Международной научно-технической конференции «Проблемы машиноведения» (г. Омск, 2022); XIV Всероссийской научно-практической конференции студентов, аспирантов, работников образования и промышленности «Информационные технологии и автоматизация управления» (г. Омск, 2023); VII Всероссийской научно-практической конференции «Научный потенциал молодежи и технический прогресс» (Санкт-Петербург, 2024).

Публикации по теме исследования. По теме диссертации опубликовано 15 научных работ, в том числе 7 научных статей в рецензируемых 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.

Личный вклад автора. Решение задач диссертации, разработка алгоритмов разделения изображений на части неравного размера и 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.

Структура и объем диссертации. Диссертация 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, включающих 64 рисунка и 6 таблиц.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы диссертации, проведен анализ степени разработанности исследуемой научной проблемы и обоснованы подходы к ее решению, поставлена цель работы, сформулированы задачи исследования и основные результаты, выносимые на защиту, указаны научная новизна, теоретическая и практическая значимости работы, а также степень достоверности результатов.

В первой главе проведен анализ современного состояния вопроса распределенной передачи видеоданных в многоканальных системах связи. Исследованы методы и алгоритмы кодирования, основанные на разделении изображений на части. Представлены разновидности систем параллельной передачи (обработки) данных, рассмотрены аналитический способ исследования, имитационное моделирование и оптимизация таких систем.

Установлено, что известные методы и алгоритмы кодирования изображений не учитывают или учитывают не в полной мере характеристики используемых систем связи. Определено, 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, включающих алгоритмы кодирования видеоданных с использованием схем разделения (1), методику аналитического расчёта оптимальных пропускных способностей каналов связи (2), имитационную модель выбора оптимальных пропускных способностей каналов двухканальной системы связи (3).

Во второй главе представлены результаты исследования распределенной передачи видеокадров через двухканальные системы связи с применением кодирующих алгоритмов. Предложены два алгоритма кодирования видеокадров, основанных на схемах разделения данных, что позволяет выполнить их распределенную передачу и обеспечить конфиденциальность. Основная особенность алгоритмов – отсутствие необходимости выполнения сложных вычислительных операций и разделение изображений выполняется на части неравного размера.

В предложенном *алгоритме разделения изображений по дробным частям десятичных чисел (АРДЧ)* разделение несжатого изображения на неравные части выполняется с помощью нахождения решения для системы уравнений по поиску значений элементов f_i , $i = \overline{1, 6M}$ массивов F_j , $j = \overline{1, N}$ (см. рис. 1), из левой части которой можно составить квадратную матрицу с частичным диагональным преобладанием и определителем, равным нулю (матрица кодирования).

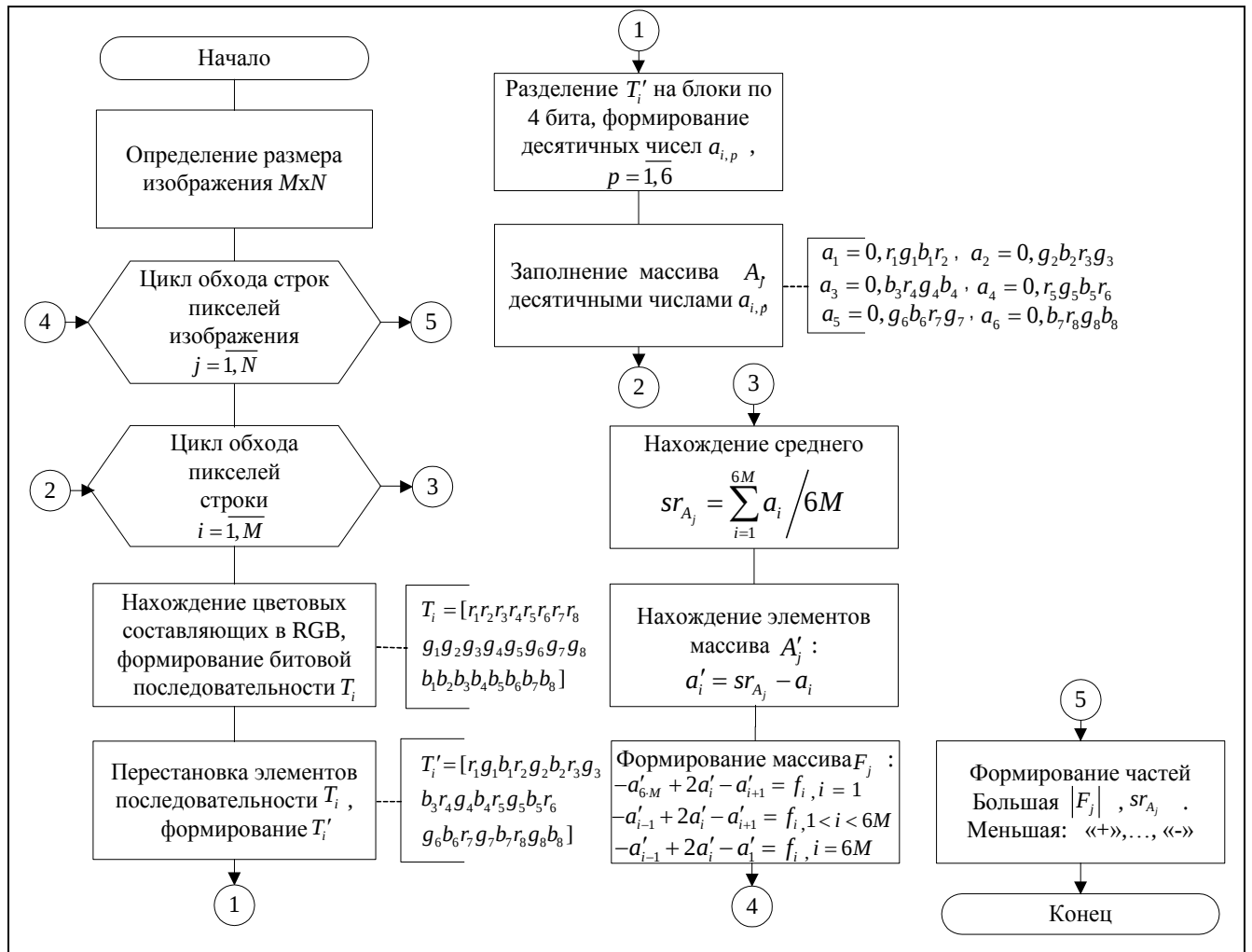


Рисунок 1 – Алгоритм разделения изображения по дробным частям десятичных чисел (АРДЧ)

Выбор матрицы такого вида обусловлен тем, что в дальнейшем требуется выполнить быстрое восстановление исходного изображения при помощи поиска решений системы алгебраических уравнений (метод Якоби). Обозначено, что в зависимости от технических требований двухканальной системы связи в качестве меньшей части могут выступать: последовательность из знаков всех элементов f_i массивов F_j (большая часть – массивы F'_j , состоящие из элементов $|f_i|$), последовательность из знаков некоторых элементов f_i массивов F_j , средние значения sr_{A_j} или комбинации описанных вариантов.

На рисунках 2, а и 3, а приведены исходные изображения, а на рисунках 2, б и 3, б представлены изображения, полученные при попытках преобразования больших частей (состоящих из элементов $|f_i|$ массивов F'_j) в десятичные значения пикселей в соответствии с цветовой моделью RGB (red, green and blue).

Если в матрице кодирования подобрать соответствующие значения, стоящие по главной диагонали, то наблюдается скрытие цветовых границ для цветных изображений (рис.4, а), но для черно-белых они видны (рис.4, б).

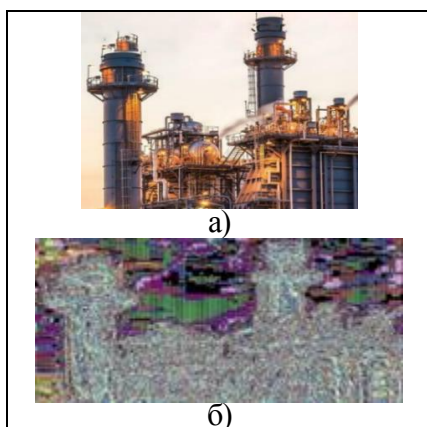


Рисунок 2 – Результат восстановления цветного изображения (АРЧД): а) исходное; б) результат

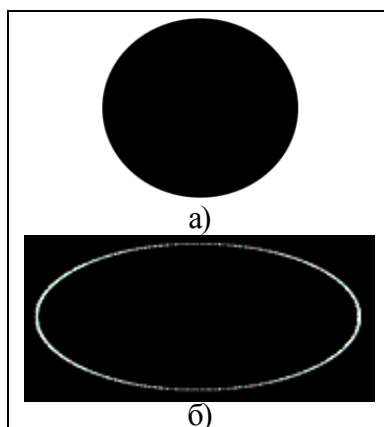


Рисунок 3 – Результат восстановления черно-белого изображения (АРЧД): а) исходное; б) результат

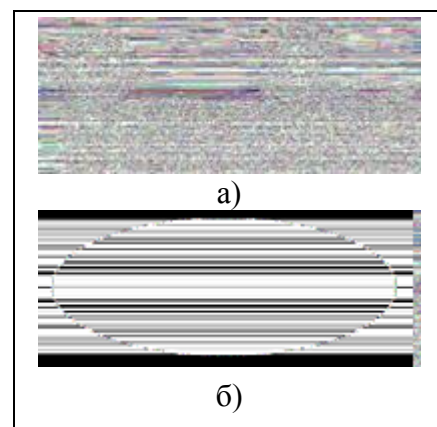


Рисунок 4 – Результат восстановления после замены значений в матрице кодирования: а) для цветного; б) для черно-белого

Восстановление изображения выполняется по строкам пикселей по принципу: $HA' = S$, где H – матрица кодирования, A' – искомый массив данных из элементов a'_i , S – массив данных, полученный при объединении частей (элементам $|f_i|$ подставлены соответствующие знаки). Для матрицы кодирования заранее найдены собственные значения λ_i и векторы v_i , вычисляются скалярные произведения $\beta_i = (S, v_i)$. Находятся значения a'_i массива $A' = \sum_{i=1}^{6M} \frac{\beta_i v_i}{\lambda_i}$. Вычисляются элементы исходного массива A : $a_i = sr_A - a'_i$, из дробных частей которых формируется битовая последовательность T' , и после её обратной перестановки выполняется восстановление цветовых значений пикселей из двоичной системы счисления (СС).

В следующем предложенном алгоритме разделения изображений с помощью префиксного кодирования (АРПК) используется «примитивизация» дельта-кода Элиаса: 1) l бит заполняются нулями (l – длина записи количества битовых последовательностей n в двоичной СС), дописывается число n в двоичной СС; 2) m_i , $i = \overline{1, n}$ бит заполняются нулями (m_i – число бит, необходимых для записи длины M_i , $i = \overline{1, n}$ битовой последовательности A_i , $i = \overline{1, n}$ в двоичной СС), выполняется запись длины M_i в двоичной СС; 3) осуществляется запись последовательности A_i к полученной в п.п. 1 и п.п. 2 части префикса.

Для разделяемого изображения формируется битовая последовательность A , состоящая из записанных значений пикселей в двоичной СС. Обход пикселей изображения выполняется построчно. Сформированная последовательность A разделяется на n частей A_i , $i = \overline{1, n}$, с соответствующими длинами M_i , $i = \overline{1, n}$. Для полученных последовательностей A_i формируется префикс с помощью «примитивизации»

дельта-кода Элиаса, являющийся меньшей частью. Над полученными битовыми последовательностями A_i выполняются операции: $X_1 = A_2 \oplus A_3$, $X_2 = A_3 \oplus A_4, \dots$, $X_{n-1} = A_n \oplus A_1$. Если последовательности A_i имеют разную длину, то для выполнения операции $XOR (\oplus)$ последовательность меньшей длины дополняется до большей собственным повторением справа. Выполнение дизъюнкции осуществляется с сохранением длины записи полученных битовых последовательностей X_i , $i = \overline{1, n-1}$. Полученные последовательности X_i записываются друг за другом, образуя большую часть.

Восстановление изображения осуществляется в соответствии с сформированным префиксом: анализируется количество первых l бит, равных нулю, после выбирается битовая последовательность равная по длине последовательности этих нулей, которая переводится из двоичной СС в десятичную, и определяется число n последовательностей A_i . Далее подсчитывается следующее количество нулей и после их записи выбирается битовая последовательность, равная по количеству подсчитанных нулей, представляющая из себя двоичную запись размера M_1 битовой последовательности A_1 . Для оставшейся части префикса выполняется аналогичная операция по определению размеров всех A_i . На последнем этапе из префикса изымается битовая последовательность A_1 и с учётом длин последовательностей A_i решаются уравнения $A_2 = X_1 \oplus A_3$, $A_3 = X_2 \oplus A_4, \dots$, $A_n = X_{n-1} \oplus A_1$, позволяющие найти последовательности $A_2, \dots, A_n$, которые, с учетом A_1 , записываются друг за другом и, в соответствии с размером изображения, преобразовываются в десятичные значения пикселей в формате RGB. Если будет раскрыта часть префикса (но не A_1) и данные будут разделены на равные части, все равно не удастся восстановить исходное изображение, так как задача сводится к решению системы из n уравнений с $n+1$ неизвестными.

Определено, что АРДЧ пригоден для многоцветных изображений, а для черно-белых изображений он дает лишь представление о цветовых границах. Для АРПК при попытках восстановления по большей части не удастся получить представление о любых исходных изображениях. Предложено применение разработанных алгоритмов разделения изображений для кодирования потока видеоданных и его последующей передачи в системах с двумя каналами связи. Улучшением является возможность использования каналов связи с различными пропускными способностями: по каналу с наименьшей пропускной способностью передается меньшая часть, а с большей – большая часть.

В третьей главе предложена методика аналитического расчета пропускных способностей каналов двухканальной системы связи с последовательно усложняющимися свойствами. В качестве математической модели для оптимизации параметров такой системы предлагается сеть массового обслуживания (СеМО) с двумя одноканальными системами массового обслуживания (СМО), с делением и слиянием заявок (рис. 5).

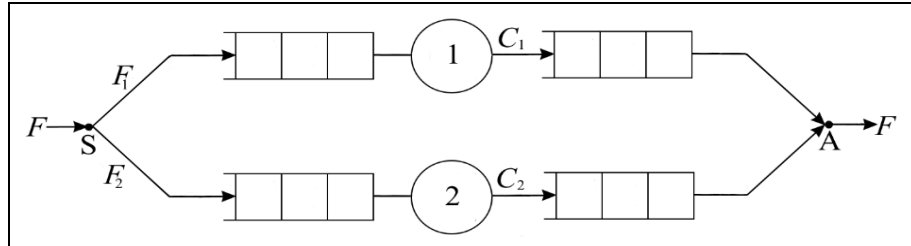


Рисунок 5 – Сеть массового обслуживания; S и A – точки деления и слияния соответственно

В точке S заявка (кадр) не переходит в одну из СМО, а разделяется на два сопряженных фрагмента, один из которых поступает в СМО-1, а другой – в СМО-2, в точке A происходит их слияние. Входящий трафик F делится на две части F_1 и F_2 ($F_1 + F_2 = F$). Интенсивности λ , λ_1 и λ_2 потоков заявок, поступающих в сеть, и их фрагментов, поступающих в СМО-1 и в СМО-2, одинаковы, и все три потока описываются одним и тем же вероятностным законом. Фрагменты в момент выхода из СМО-1 (СМО-2) перед точкой A попадают в первую (во вторую) очередь синхронизации, в которой находятся до момента обнаружения в соседней очереди синхронизации своих сопряженных фрагментов. Из двух сопряженных фрагментов тот, который приходит позже, не задерживается в очереди синхронизации. И, следовательно, время передачи заявки $u = \max(u_1, u_2)$, где u_1 (u_2) – время пребывания фрагмента заявки в СМО-1 (СМО-2): $u_1 = w_1 + x_1$, $u_2 = w_2 + x_2$, w_1 , w_2 – время ожидания фрагмента в очереди 1 (очереди 2), x_1 (x_2) – время обслуживания фрагмента в СМО-1 (СМО-2). Среднее время пребывания заявки в сети $U = U(C_1, C_2) = M[\max(u_1, u_2)] = M[\max(w_1 + x_1, w_2 + x_2)]$.

Пусть цена пропускной способности каналов связи в расчете на время эксплуатации системы составляет m у.е./(Кбит/с). Тогда целевая функция (ЦФ) для задачи оптимизации пропускных способностей C_1 , C_2 каналов связи имеет вид:

$$f = lU(C_1, C_2) + m(C_1 + C_2) \rightarrow \min_{C_1, C_2}; C_1 \geq F_1; C_2 \geq F_2, \quad (1)$$

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

Задача (1) ставится как задача минимизации средних издержек, приходящихся на период эксплуатации системы. Для исследования двухканальной системы связи с синхронной передачей разделенных видеокадров рассмотрена СеМО с делением заявок в постоянном соотношении и со связанными в постоянном соотношении пропускными

способностями каналов связи (т.е. $h_2/h_1 = \gamma = \text{const}$, $C_2 = \gamma C_1$). Время обслуживания x_1 и x_2 фрагментов заявки в СМО-1 и СМО-2 совпадает: $x_1 = h_1/C_1$, $x_2 = h_2/C_2 = (\gamma h_1)/(\gamma C_1) = h_1/C_1 = x_1$, время пребывания u_1 и u_2 фрагментов в СМО-1 и СМО-2 также совпадает, тогда $u = \max(u_1, u_2) = u_1$ и $U = M[\max(u_1, u_2)] = M[u_1] = U_1$, U_1 – среднее время пребывания фрагмента в СМО-1. Выполняя в задаче (1) подстановки $U(C_1, C_2) = U_1(C_1)$, $C_2 = \gamma C_1$ и $F_2 = \gamma F_1$, получена формулировка с использованием только одного параметра C_1 :

$$f = lU_1(C_1) + m(1 + \gamma)C_1 \rightarrow \min_{C_1}; C_1 \geq F_1. \quad (2)$$

При регулярном входящем потоке время между приходами заявок постоянно ($\tau = \text{const}$). Размер фрагментов заявок, поступающих в СМО-1, также фиксирован ($h_1 = \text{const}$), поэтому в СМО-1 фиксировано и время обслуживания $x_1 = h_1/C_1$. Из ограничения $C_1 \geq F_1$ следует, что $x_1 \leq \tau_1$ (каждый фрагмент обслуживается раньше, чем поступает следующий). Поэтому очередь перед СМО-1 не формируется и среднее время пребывания фрагмента $U_1 = x_1 = h_1/C_1$. Подставляя U_1 в (2) вместо $U_1(C_1)$, получим:

$$f = lh_1/C_1 + m(1 + \gamma)C_1 \rightarrow \min_{C_1}; C_1 \geq F_1. \quad (3)$$

Решение задачи (3) находится с помощью решения уравнения $df(C_1)/dC_1 = 0$, определяющего точку локального минимума f : $C_1 = \sqrt{lh_1/(m(1 + \gamma))}$. Чтобы оценить потери, за счет которых достигается повышение конфиденциальности передачи видеоданных при использовании двухканальной системы связи, выполнено сравнение издержек для оптимальной двухканальной системы с издержками, характеризующими одноканальную оптимальную систему. Среднее время U передачи видеокadra по одному каналу равно среднему времени обслуживания заявки (так как очередь перед каналом не возникает), $U = h/C$, где $h = h_1 + h_2 = \text{const}$. Задача оптимизации одноканальной СМО имеет вид:

$$f = lh / C + mC \rightarrow \min_C; C \geq F. \quad (4)$$

Локальный минимум ЦФ достигается при $C = \sqrt{lh/m}$. При расчетах получено, что значения ФЦ (3) и (4) одинаковы, т.е. повышение конфиденциальности видеоданных за счет их разделения и передачи по разным каналам связи достигается без повышения издержек.

Сформулирована и доказана *теорема 1*: передача *регулярного* потока видеокadров фиксированного размера через 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 двухканальной системы равна пропускной способности оптимальной одноканальной системы. Доказательство *теоремы 1* осуществляется путем замены в задаче (3) $C_1 = C/(1 + \gamma)$, $F_1 = F/(1 + \gamma)$ и $h_1 = h/(1 + \gamma)$. *Теорему 1* обобщает *теорема 2*: передача *любого*

потока видеок кадров через оптимальную двухканальную систему с синхронной передачей данных приводит к таким же издержкам, как его передача через оптимальную одноканальную систему. Доказательство *теоремы 2* приведено на примере экспоненциальной оптимальной двухканальной системы с синхронной передачей данных.

Кроме того, рассмотрена система связи, где разделение видеок кадров выполняется в постоянном соотношении ($h_2/h_1 = \gamma = \text{const}$), но не накладывается условие $C_2 = \gamma C_1$, задача оптимизации такой системы записывается как общая задача (1). Сформулирована и доказана *теорема 3* о том, что оптимальная для передачи *регулярного* потока видеок кадров фиксированного размера система связи, где разделение видеок кадров выполняется в постоянном соотношении ($h_2/h_1 = \gamma = \text{const}$), но не накладывается условие $C_2 = \gamma C_1$, является оптимальной двухканальной системой с синхронной передачей данных, т.е. оптимальное решение задачи (1) всегда лежит на прямой $C_2 = \gamma C_1$.

Приведено доказательство *теоремы 3* с помощью метода от противного, получено противоречие, исключающее возможность нахождения решения задачи (1) вне прямой $C_2 = \gamma C_1$. *Теорему 3* дополняет проверенная с помощью имитационного моделирования *теорема 4*: оптимальная для передачи *любого* потока видеок кадров фиксированного размера система связи, где разделение видеок кадров выполняется в постоянном соотношении ($h_2/h_1 = \gamma = \text{const}$), но не накладывается условие $C_2 = \gamma C_1$, является оптимальной двухканальной системой с синхронной передачей данных, т.е. оптимальное решение задачи (1) всегда лежит на прямой $C_2 = \gamma C_1$.

Теорема 4 упрощает решение сложной нелинейной задачи оптимизации двухканальных систем связи, поскольку сводит поиск значений двух варьируемых параметров C_1 , C_2 , доставляющих минимум ЦФ двух переменных, к поиску значения одного варьируемого параметра.

В **четвертой главе** приводится описание разработанной имитационной модели двухканальной системы с разделением видеок кадров по каналам связи. В качестве такой системы связи (рис. 6) рассматривается система с двумя каналами связи (DL – datalink: DL-1, DL-2) и обратной связью (SL – synchronizationlink).

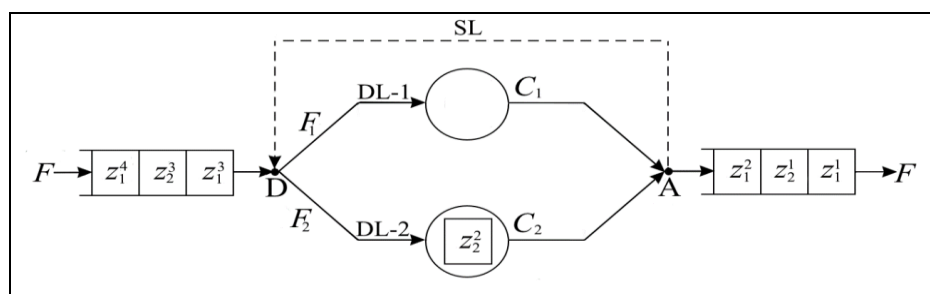


Рисунок 6 – Схема системы связи с передачей видеоданных по двум каналам

параметров $X = (\tau_1, \tau_2)$. В составных модулях DL-1 и DL-2 осуществляется обработка заявок, модуль DL-1 (рис. 8) имеет идентичную структуру с DL-2, за исключением того, что в нем имеется выход Out2, выполняющий передачу сигнала о том, что в блоке Single Server на обслуживании находится заявка.

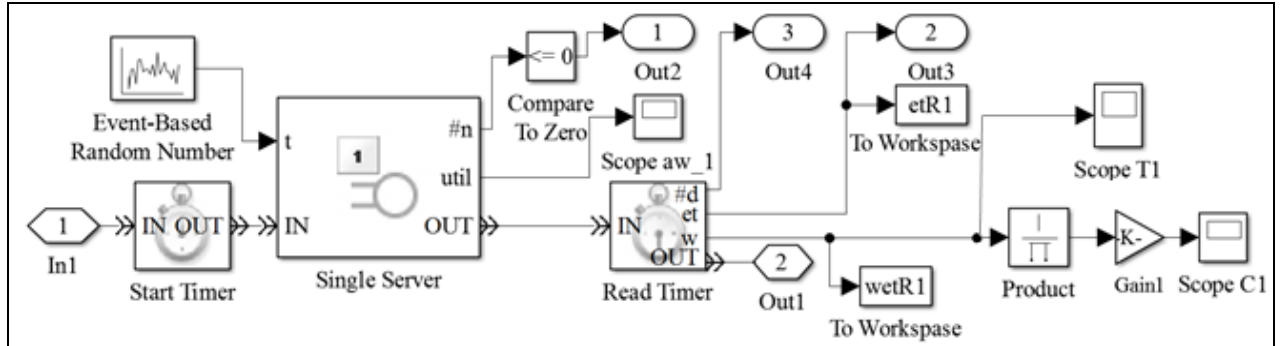


Рисунок 8 – Структура составного модуля обработки заявок – DL-1

Результат оптимизации для одной из реализаций решения двухкритериальной задачи с использованием критериев $J_1(X)$, $J_2(X)$ приведен на рисунке 9, на котором выполнено отображение плоскости параметров на критериальную плоскость. 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.

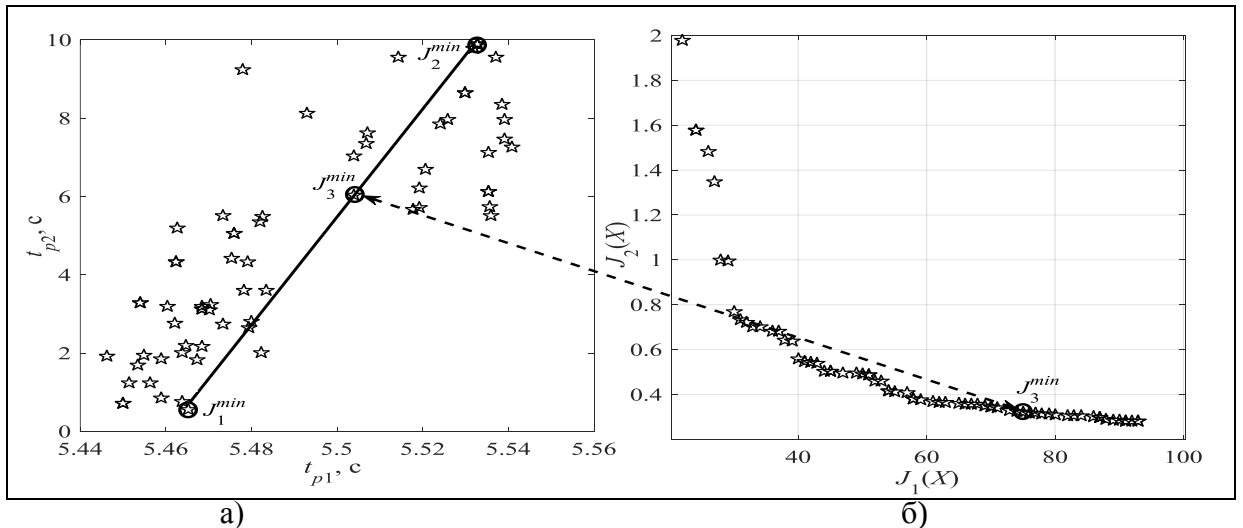


Рисунок 9 – Результаты оптимизации системы с помощью ГА: а) множество Парето-решений; б) множество Парето для критериев $J_1(X)$, $J_2(X)$

Целью оптимизации являлось получение минимальных пропускных способностей C_1 , C_2 при выполнении условия синхронизации передачи данных, 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 $J_3(X)$, (обозначено на рисунке 9, а кружком, стрелкой показан соответствующий ему выделенный элемент множества Парето-оптимальных решений). В проведенном

имитационном моделировании при заданных параметрах ГА и $J_3(X) \rightarrow \min$ синхронизация передачи данных достигается при $t_p = t_{p_1} = t_{p_2} = 5,5$ с. Процесс настройки синхронизации с помощью ГА при привлечении критерия $J_3(X)$ отображен на рисунке 10, где видно, что за 80 с. осуществляется настройка параметров системы связи, обеспечивающая синхронную передачу данных с необходимыми пропускными способностями.

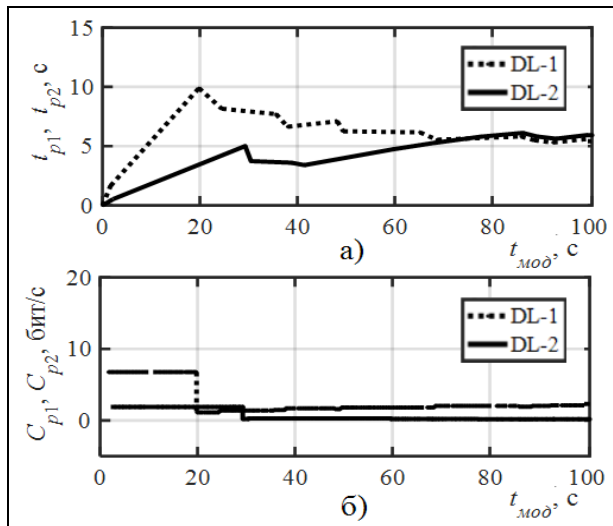


Рисунок 10 – Характеристики системы:

- а) время занятия каналов связи;
- б) изменение пропускных способностей каналов связи при $J_3(X) \rightarrow \min$

Значения, полученные при помощи имитационного моделирования, в допустимых пределах совпадают со значениями, полученными при аналитических расчетах, что подтверждает пригодность применяемых методов имитационного моделирования. Применение методов оптимизации с использованием ГА позволяет за короткое время найти такие значения параметров системы двухканальной передачи данных, которые одновременно сокращают время передачи и снижают затраты.

В пятой главе описаны результаты исследований с помощью комплекса программ для распределенной передачи видеокладов по двухканальной системе связи. Комплекс состоит из программы «Демультимплексор/Мультимплексор» (разделение и объединение кадров), программы «Расчет» (аналитические расчеты), программы «Оптимизация» (имитационная модель), программы «Клиент/Сервер» (передача данных), программы NetLimited (ограничение скорости передачи данных).

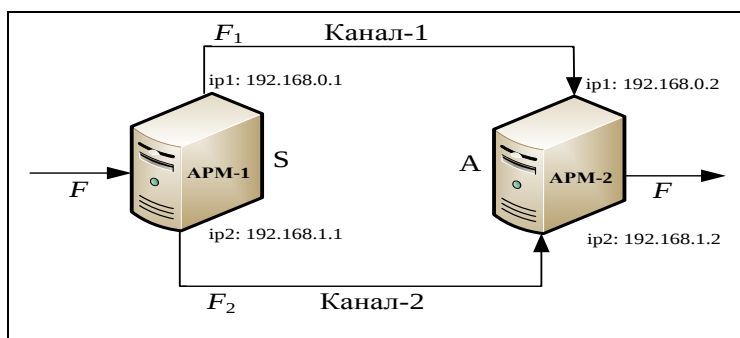


Рисунок 11 – Схема объединения двух ПК

Для проведения экспериментов собран стенд из двух ПК с двумя сетевыми картами на каждом и объединенных в локальную сеть по принципу точка-точка (рис. 11). Для того чтобы оценить время расхождения получения

частей видеокладов по двум каналам связи, проведено тридцать натурных экспериментов для каждого из форматов качества видеоданных. Вначале с помощью программы «Демультимплексор/Мультимплексор» выполнено разделение кадров и проведена оценка соотношения полученных с помощью алгоритмов разделения (АРДЧ и АРПК) размеров

частей кадров и потоков F_1 и F_2 , передаваемых по первому и второму каналам соответственно. Определено, что для АРДЧ размер меньшей части составляет 25 % от большей, для АРПК 8,85 %. С помощью методики аналитических расчетов (программы «Расчет») и имитационной модели определены пропускные способности каналов связи (C_1^a, C_2^a) , (C_1^u, C_2^u) . По результатам экспертной оценки получены пропускные способности (C_1^3, C_2^3) . С помощью программы NetLimited выполнено поочередное ограничение пропускных способностей каналов связи в соответствии с полученными значениями, а с помощью программы «Клиент/Сервер» осуществлена параллельная передача соответствующих частей видеок кадров. Для каждой пары пропускных способностей (C_1^a, C_2^a) , (C_1^u, C_2^u) , (C_1^3, C_2^3) эксперимент проводился $n=30$ раз и были сформированы последовательности из результатов эксперимента $T_i^{1a}, T_i^{2a}, T_i^{1u}, T_i^{2u}, T_i^{13}, T_i^{23}, i = \overline{1,30}$, для которых с помощью бутстрап-метода выполнено построение 95% доверительного интервала (ДИ). Среди значений из каждой пар последовательностей, попавших в ДИ, выбраны такие, которые дают минимальные значения расхождения времени получения частей видеоданных $\Delta T^a = |T_i^{1a} - T_i^{2a}| \rightarrow \min, \Delta T^u = |T_i^{1u} - T_i^{2u}| \rightarrow \min, \Delta T^3 = |T_i^{13} - T_i^{23}| \rightarrow \min$ (табл. 1).

Таблица 1 – Расхождение времени получения частей видеоданных разных форматов, переданных по двум каналам связи

Формат видеоданных	Алгоритм разделения АРДЧ			Алгоритм разделения АРПК		
	ΔT^a , мс	ΔT^u , мс	ΔT^3 , мс	ΔT^a , мс	ΔT^u , мс	ΔT^3 , 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

Определено, что точной синхронизации достичь невозможно, а наименьшее расхождение времени получения частей кадров получено при значениях пропускных способностей каналов связи, найденных с помощью имитационного моделирования, оно считается приемлемым и в ряде случаев не превышает 300 мс. Расхождение между временными интервалами получения частей видеоданных при значениях пропускных способностей, полученных с помощью аналитического расчета и имитационной модели, для АРДЧ в среднем (для всех форматов качества видеоданных) составляет 37 %, для АРПК 22 %. Оценка эксперта не всегда позволяет получить приемлемые результаты. На рисунке 12 для обоих алгоритмов разделения данных приведено сравнение издержек (ЦФ), приходящихся на содержание двухканальной системы связи в соответствии с найденными пропускными способностями для передачи заданных форматов качества видеоданных.

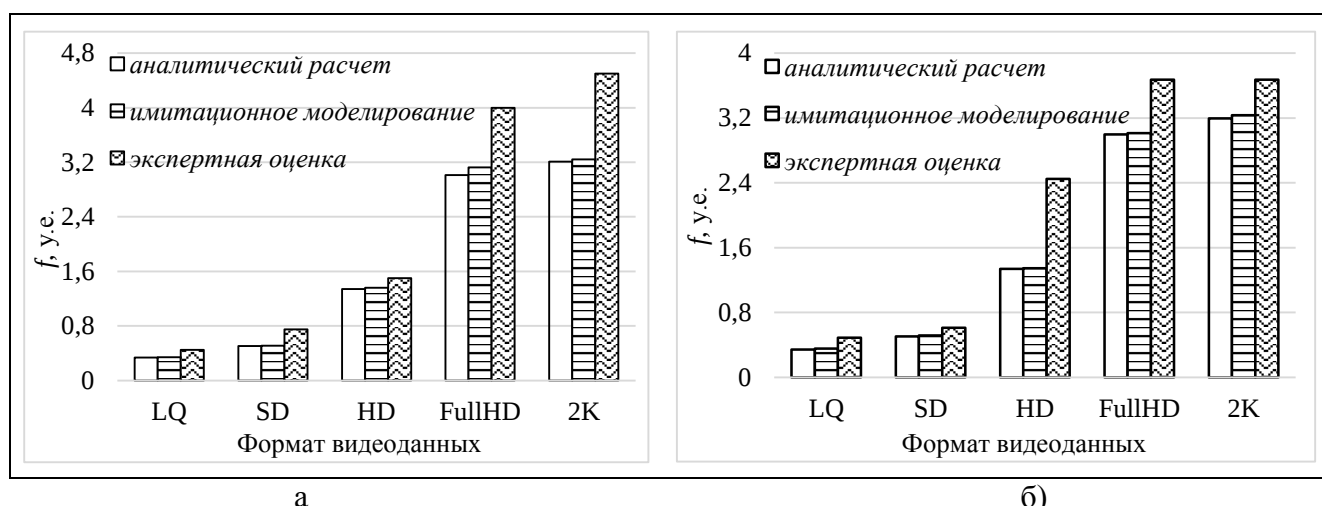


Рисунок 12 – Издержки на содержание двухканальной системы связи при аналитическом решении, имитационном моделировании и экспертной оценке: а) АРДЧ; б) АРПК

Из рисунка 12 видно, что аналитические расчеты и имитационное моделирование позволяют добиться снижения финансовых затрат. Для обоих алгоритмов разделения установлено, что разница между значениями ЦФ, полученными аналитическими расчётами и имитационным моделированием, в среднем составляет 1,7 %, то есть удорожание системы связи при выборе пропускных способностей по результатам имитационного моделирования не превышает 2 %.

ЗАКЛЮЧЕНИЕ

В результате проведённых исследований получены новые научные, 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: АРДЧ (по дробным частям десятичных чисел) и АРПК (с помощью префиксного кодирования). Установлено, что предлагаемые алгоритмы кодирования

позволяют выполнять разделение изображений на части неравного размера с невозможностью их последующего полного декодирования по большим частям.

Получено, что АРДЧ пригоден для кодирования неконтрастных изображений, это исключает возможность его применения для черно-белых изображений, а АРПК пригоден для кодирования любых изображений. 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 для распределённой передачи видеоданных.

3. Предложена методика аналитического расчета пропускных способностей каналов связи при известных отношении частей разделяемых видеок кадров и цене средней задержки данных в сети на одну секунду, обеспечивающая минимизацию издержек на содержание системы связи. Установлено, что для передачи любого потока данных, разделяемых в постоянном соотношении, оптимальные пропускные способности каналов двухканальной системы связи имеют линейную зависимость. Предложено доказательство теорем, позволяющих свести двумерные задачи оптимизации двухканальных систем с разделением данных по каналам связи к одномерным.

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 синхронной передачи данных с наименьшим рассогласованием времени доставки частей видеок кадров, а также соответствуют ожидаемым теоретическим. Среднее расхождение между теоретическими значениями и результатами имитационной модели не превышает 9 %.

5. Создан комплекс программ для двухканальной системы передачи видеоданных, который позволил провести экспериментальные исследования. Установлено, что при значениях пропускных способностей каналов связи, определенных с помощью имитационной модели, достигается наименьшее рассогласование времени доставки частей видеок кадров (меньше чем при аналитическом расчете и экспертном подборе), которое в среднем не превышает 300 мс. Полученные значения, с учетом 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: повышением стабильности в условиях переменной нагрузки, снижением задержек доставки данных.

ОСНОВНЫЕ РАБОТЫ, ОПУБЛИКОВАННЫЕ ПО ТЕМЕ ДИССЕРТАЦИИ

Статьи в научных журналах, рекомендованных ВАК при Минобрнауки России

1. **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. (К2).
2. **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. (К1).
3. **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. (К2).
4. **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. (Белый список, уровень 1).
Англ. версия: Sagaydak, D.A. Method of forming a digital watermark for physical and electronic documents / D.A. Sagaydak, R.T. Faizullin // Computer Optics. – 2014. – Vol. 38, No. 1. – P. 94-104. (Scopus, Q3; Web of Science, Q4).
5. **Сагайдак, Д.А.** Модели схем разделения секрета в системах передачи видеоинформации / Д.А. Сагайдак, Р.Т. Файзуллин // Компьютерная оптика. – 2013. – Т. 37, № 1. – С. 105-112. (Белый список, уровень 1).
Англ. версия: Sagaydak, D.A. Model secret sharing schemes in systems transmit video / D.A. Sagaydak, R.T. Faizullin // Computer Optics. – 2013. – Vol. 37, No. 1. – P. 105-112. (Scopus, Q3; Web of Science, Q4).
6. 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. (К2).
7. Михеев, В.В. 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 СибАДИ. – 2012. – № 5(27). – С. 82-87. (К2).

Статьи в других рецензируемых научных журналах

8. **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.
9. **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.
10. **Сагайдак, Д.А.** Метод обеспечения безопасного хранения данных на серверах ЦОД (центров обработки данных) / Д.А. Сагайдак // Россия молодая: передовые технологии – в промышленность. – 2011. – № 1. – С. 304-307.

Статьи в материалах конференций

11. **Сагайдак, Д.А.** Оптимизация передачи данных при реализации схем разделения секрета / Д.А. Сагайдак // Научный потенциал молодежи и технический прогресс. – ИП Жукова Е.В. – СПб, 2024. – С. 16-17.

12. **Сагайдак, Д.А.** Оптимизации передачи видеоданных с демультиплексированием по двум каналам связи с различными характеристикам / Д.А. Сагайдак // Информационные технологии и автоматизация управления. – ОмГТУ. – Омск, 2023. – С. 196-201.

13. Zadorozhnyi, V. Optimization of message transmission when implementing the secret sharing scheme / V. Zadorozhnyi, **D. Sagaydak** // Informational technologies and mathematical modelling (ITMM-2021). – TSU. – Tomsk, 2022. – P. 137-144.

14. 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. – ОмГТУ. Том I. – Омск, 2023. – С. 196-201.

15. **Сагайдак, Д. А.** Приложение алгоритмов разделения секрета в целях сокрытия передаваемой видеоинформации / Д.А. Сагайдак // Электронные средства и системы управления. – ТУСУР. – Томск, 2012. – № 2. – С. 51-56.

Государственная регистрация программ для ЭВМ

16. Свид. о гос. рег. прогр. для ЭВМ № 2024688412. Российская Федерация. Программа моделирования экспоненциальной сети с двумя каналами связи и произвольным входящим потоком заявок № 2024685986; заяв. 01.11.2024; опубл. 27.11.2024 / **Д.А. Сагайдак**.

17. Свид. о гос. рег. прогр. для ЭВМ № 2024686592. Российская Федерация. Программа моделирования системы связи с двумя синхронными каналами, обладающими разными пропускными способностями № 2024686077; заяв. 01.11.2024; опубл. 11.11.2024 / **Д.А. Сагайдак**, Л.А. Денисова.

18. Свид. о гос. рег. прогр. для ЭВМ № 2013661611. Российская Федерация. Программа, реализующая алгоритм префиксного кодирования видеоинформации, основанного на примитивизации дельта-кода Элиаса в схеме разделения секрета с принципиально малой частью секрета № 2013619795; заяв. 25.10.2013; опубл. 11.12.2013 / **Д.А. Сагайдак**.

19. Свид. о гос. рег. прогр. для ЭВМ № 2013661618. Российская Федерация. 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 №2013619791; заяв. 28.10.2013; опубл. 11.12.2013 / **Д.А. Сагайдак**.

20. Свид. о гос. рег. прогр. для ЭВМ № 2014615225. Российская Федерация. Программа, реализующая способ формирования и внедрения цифрового водяного знака, способного нести в себе какую-либо определенную информацию, в изображения, представленные в цифровом виде № 2014612760; заяв. 31.03.2014; опубл. 21.05.2014 / **Д.А. Сагайдак**.