Федеральное государственное бюджетное образовательное учреждение
высшего образования
«УЛЬЯНОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

На правах рукописи

Кузнецов Николай Алексеевич

РАЗРАБОТКА АЛГОРИТМОВ И МОДЕЛИРОВАНИЕ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ОБМЕНА ДИСКРЕТНОЙ ИНФОРМАЦИЕЙ

Специальность 05.13.18 – Математическое моделирование, численные методы и комплексы программ

ДИССЕРТАЦИЯ
на соискание ученой степени
кандидата технических наук

Научный руководитель:
доктор технических наук,
профессор Смагин А.А.

Ульяновск – 2022

СОДЕРЖАНИЕ

ВВЕДЕНИЕ……4
ГЛАВА 1. ОБЗОР ПРЕДМЕТНОЙ ОБЛАСТИ ИССЛЕДОВАНИЯ…….13
1.1 Классификация, структура и характеристики систем передачи-приема данных……..……..13
1.2 Концептуальная модель системы передачи-приема данных…….....15
1.3 Основные виды уязвимостей и угрозы целостности дискретной информации, возникающие в системах передачи-приема данных…….....18
1.4 Выводы по первой главе…….....25
ГЛАВА 2. РАЗРАБОТКА ПОДСИСТЕМЫ ОБНАРУЖЕНИЯ ПРИЗНАКОВ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В СИСТЕМАХ ПЕРЕДАЧИ-ПРИЕМА ДАННЫХ……..27
2.1 Способы получения информации о состоянии системы передачи-приема данных и основные методы выявления угроз нарушения целостности данных……..…...……27
2.2 Методы обеспечения целостности дискретной информации в системах передачи-приема данных…….....31
2.3 Разработка подсистемы обнаружения признаков несанкционированного доступа в системах передачи-приема данных на основе аппарата теории массового обслуживания…….……35
2.4 Применение метода градиентного спуска для вычисления интенсивностей поступивших пакетов данных, интенсивностей принятых к обработке пакетов данных, интенсивностей находящихся в очереди и ожидающих обработки пакетов данных…….58
2.5 Выводы по второй главе……..……..61
ГЛАВА 3. РАЗРАБОТКА ПОДСИСТЕМЫ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ ДАННЫХ НА ОСНОВЕ КОДОВ С ПЕРЕМЕННЫМ ВЕСОМ……63
3.1 Анализ моделей каналов передачи данных в системах обмена дискретной информацией…….63
3.2 Состав информации в системах передачи-приема данных……..…..64
3.3 Контроль ошибок при передаче двоичных кодовых последовательностей……..…….....67
3.4 Определение параметров двоичных кодов с фиксированным весом……...70

3.5 Генерация двоичных кодов целых чисел с переменным весом (алгоритмический подход)……....75
3.5.1 Формирования двоичного кода передаваемых данных с помощью матрично-алгоритмического кодирования…….……77
3.5.2 Алгоритм декодирования кода с заданным весом…….…..78
3.6 Обнаружение искажений в передаваемых данных на основе использования кодов с переменным весом…….…80
3.7.1 Определение координат кодируемых чисел в матрицах весов……....87
3.7.2 Определение порядкового номера числа, образующего строку, внутри подматрицы……88
3.8 Выводы по третьей главе……...….91
ГЛАВА 4. РАЗРАБОТКА ПОДСИСТЕМЫ ОЦЕНКИ РИСКА ВОЗНИКНОВЕНИЯ ПОВТОРНЫХ ОШИБОК, ВЫЗВАННЫХ СБОЯМИ ПРИЕМНОЙ АППАРАТУРЫ И ПРОГРАММНЫХ СРЕДСТВ……..93
4.1 Разработка подсистемы оценки риска возникновения повторных ошибок, вызванных сбоями приемной аппаратуры и программных средств……94
4.2 Выводы по четвертой главе……..117
ЗАКЛЮЧЕНИЕ……...……..119
БИБЛИОГРАФИЧЕСКИЙ СПИСОК……...……...123

ВВЕДЕНИЕ

Актуальность. На практике большое распространение получили системы удаленного доступа, которые имеют важное народно-хозяйственное значение для обеспечения обмена данными между центрами управления и удаленными объектами. Такие системы передачи-приема данных (СППД) могут быть разнесены на значительные расстояния (несколько тысяч километров) и соединены разнородными средами передачи данных, такими как оптоволокно, медные кабели, радиорелейные линии передачи данных.

Если рассматривать СППД как системы, связывающие центры управления с удаленными объектами, и сами передаваемые данные как телеметрические, несущие информацию о работе удаленного объекта, то есть о его состоянии, и как данные о выпускаемых изделиях или добыче природных ископаемых, например, таких как нефть и газ, то не исключены случаи несанкционированного доступа для получения этих данных или их преднамеренного искажения.

Таким образом, в условиях разнообразных сред передачи данных, передаваемая информация подвержена воздействиям множества отрицательных как внешних, так и внутренних факторов. Причем искажения данных могут быть также вызваны сбоями и отказами средств приема и обработки СППД. Разнородность сред передачи данных характеризуется использованием разного по своим свойствам телекоммуникационного оборудования, технологиями приема и передачи данных, необходимостью совместимости форматов передаваемых данных, а также архитектурой и территориальными особенностями построения и эксплуатации СППД.

Применяемая приемная аппаратура СППД является достаточно уязвимой в условиях динамической и быстро изменяющейся обстановки [1, 2]. Разработка средств обеспечения целостности передаваемых данных обусловлена увеличением их объемов, необходимостью совершенствования способов и средств обнаружения признаков несанкционированного доступа, искажениями передаваемых данных и появлением новых видов угроз со стороны злоумышленников. Под целостностью данных понимается неискаженное их представление в СППД, причем строго соблюдается отношение биективности между отправленными и получаемыми кодами.

На практике с этой целью широко применяется помехоустойчивое кодирование, дублирование данных, резервирование каналов [3]. Методы и

средства помехоустойчивого кодирования ориентированы на сохранение целостности данных из-за воздействия случайных отрицательных факторов и не могут решать задачу обнаружения признаков несанкционированного доступа. Такие известные методы как, дублирование данных требует хранения копий на физически разделяемых отказоустойчивых дорогостоящих носителях, резервирование аппаратуры требует дополнительного места для их размещения и увеличивает ее стоимость. Также следует отметить недостаточную эффективность используемых методов обеспечения целостности данных, а именно, большую вычислительную сложность, высокую избыточность и как следствие, ограниченные области применения [3].

Теоретически в системах передачи-приема данных (СППД) целостность обеспечивается при помощи двух подходов. Первый подход позволяет согласовать преобразованный шум с корректирующими свойствами помехоустойчивого кода. Подобные преобразования описаны в работе В. Коржика, Л. Финка [4]. Данный подход подразумевает применение известных методов помехоустойчивого кодирования (сверточные коды, коды Рида-Соломона). Согласование метода модуляции сигнала и помехоустойчивого кода является наглядным примером согласующих преобразований [4]. Однако применение известных методов помехоустойчивого кодирования позволяет эффективно бороться с пачками ошибок, но не подходит для обнаружения и исправления единичных аддитивных ошибок различной кратности (в том числе и их различных комбинаций), которые наиболее часто распространены на практике.

Второй подход основан на использовании специальных методов преобразования данных и предусматривает применение нелинейных кодов, которые обладают высокими корректирующими свойствами и способны обнаруживать и исправлять различные виды ошибок [5].
В реальных СППД наиболее перспективным считается самоконтроль. Существенным недостатком этого подхода является то, что время обмена данными – строго ограниченная величина и временные промежутки обмена фиксированы [6].

Автономный контроль целостности включает две группы: внешние и внутренние [7]. Внешние базируются на использовании информации, получаемой от других источников, и осуществляют комплексную обработку данных, внутренние методы используют собственную информацию,

основанную на статистике нарушений целостности. Таким образом, обмен информацией о нарушениях целостности передаваемых данных между наземными станциями требует выполнения временных ограничений, которые должны не нарушаться.

В диссертации рассмотрены наземные СППД, источниками информации в которых могут быть: радиолокационные станции, GPS – навигаторы, ГЛОНАСС – навигаторы, наземные станции управления полетами [2]. Основным недостатком организации функционирования современных систем передачи-приема данных являются: «неустойчивая работа оборудования из-за влияния помех на канал распространения радиосигнала, возможности преднамеренного искажения передаваемой навигационной информации и ненадёжность приемо-передающей аппаратуры» [7].

В работе предлагается комплексный подход к созданию средств, включающих в свой состав модели проведения анализа нештатных ситуаций, в которых возникает необходимость защиты целостности передаваемых по каналам потоков данных, в виде трех взаимодействующих подсистем.

Первая подсистема позволяет обнаруживать признаки несанкционированного доступа в СППД. В ее основу заложен аппарат теории массового обслуживания, позволяющий выявлять задержки, возникающие при передаче пакетов данных, которые можно интерпретировать как вмешательство в порядок очереди и в сами пакеты данных. Таким образом, можно регистрировать сам факт нарушения целостности.

Вторая подсистема позволяет обеспечивать целостность телеметрических данных на основе кодов переменного веса. В ее основу заложено применение трех методов: метода обнаружения ошибок на основе контроля веса двоичного кода, метода генерации кодов переменной веса и метода подсчета веса двоичного кода. Эта подсистема позволяет идентифицировать места локализации, как пачек ошибок, так и единичных аддитивных ошибок различной кратности.

Третья подсистема служит для оценки риска повторных ошибок, вызванных сбоями приемной аппаратуры и программных средств СППД, и выполняет вычисление значений показателя этого риска, тем самым позволяя определять приемлемый уровень достоверности принимаемых данных.

Введение трех подсистем в состав СППД предполагает исследование их свойств и поведения в нештатных режимах работы, создания их

адекватных моделей, проведения моделирования и эффективного использования результатов на практике.

В настоящей диссертации выполнены работы по комплексному решению задач обеспечения целостности информации, базирующихся на теоретических посылках в области использования математического моделирования и численных методов.

В первой главе диссертации рассмотрена классификация, структура и характеристики систем передачи-приема данных, построена концептуальная модель системы передачи-приема данных с нарушениями целостности. Приведены основные угрозы, которым подвергаются системы передачи-приема данных, произведен анализ известных моделей обеспечения целостности данных.

Во второй главе диссертации разработана математическая модель обнаружения признаков несанкционированного доступа в СППД на основе применения математического аппарата теории массового обслуживания (ТМО) с использованием семимартингального описания точечных процессов, индикаторных функций и их компенсаторов, позволяющих повысить точность обнаружения факта несанкционированного доступа. Определены формулы для проведения компьютерного моделирования, позволяющие вычислять значения интенсивностей поступивших пакетов данных, интенсивностей принятых к обработке пакетов данных и интенсивностей, находящихся в очереди и ожидающих обработки пакетов данных. С их помощью предложено формировать таблицы интенсивностей с заранее вычисленными их значениями за заданное модельное время. На основе построенной модели проведены экспериментальные исследования с использованием имитационного моделирования, которые позволили выявлять факт несанкционированного доступа и возможные причины нарушения целостности.

В третьей главе диссертации разработана структурно-функциональная модель подсистемы обработки пакетов данных на основе использования неразделимых кодов с постоянным весом. С их помощью решается задача быстрого обнаружения факта наличия ошибок путем сравнения значений отправленных и полученных весов на приемной аппаратуре системы передачи-приема данных. При передаче данные представляют собой параметры управляемых процессов и объектов, к которым подключены системы передачи-приема данных, выражаемых целыми десятичными

числами, обоснован выбор контроля их целостности по переменным параметрам кодовых последовательностей, в качестве которых выбран их вес. Предложен быстрый численный метод вычисления их веса. В основу положено рекурсивное разложение кодируемого целого числа в убывающий ряд, а вес вычисляется рекуррентно, через значения весов, полученных на предыдущих шагах разложения.

Предложен матрично-алгоритмический метод к кодированию и декодированию целых чисел на основе матрицы Паскаля, на базе которого строится программный генератор для образования двоичных кодов с переменными весами. Разработаны новые формы алгоритмов кодирования и декодирования, которые позволяют формировать двоичное представление кодируемого числа, проводить его декодирование и имеют достаточно простую программную реализацию и высокую скорость.

Для решения задачи восстановления целостности переданных кодовых данных, искаженных шумами среды передачи данных, предложен подход для определения прообраза данных, опирающийся на сравнение прообразов, полученных путем декодирования данных матрично-алгоритмическим методом. Показана эффективность подхода, и возможность достаточно простой его реализации на практике.

В четвертой главе с помощью разработанных математических моделей, алгоритмов обеспечения целостности данных, проведенного имитационного моделирования решена задача оценки риска возникновения повторных ошибок с использованием функции Гомперца, позволяющей описывать с более высокой точностью угрозы нарушения целостности данных на начальной и завершающей стадиях функционирования системы передачи-приема данных.

Разработан комплекс программ, на основе построенных моделей, включающий обнаружение признаков несанкционированного доступа с использованием аппарата теории массового обслуживания, выявление и исправление ошибок в пакетах данных, вызванных средой передачи данных и сбоями приемной аппаратуры СППД с оценкой риска повторного возникновения ошибок.

Объект исследования: информационные системы обмена дискретной информацией.

Предмет исследования: математические модели, численные методы и программные средства, применяемые для обеспечения целостности дискретной информации в системах передачи-приема данных.

Цель исследования: повышение эффективности функционирования систем обеспечение целостности данных на основе использования математического аппарата теории массового обслуживания, методов кодирования передаваемых данных на базе двоичных последовательностей с переменными весами, с оценкой риска возникновения повторных ошибок, возникающих в приемной аппаратуре систем передачи-приема данных.

Для достижения поставленной цели решаются следующие задачи.

Основная задача исследования: разработка алгоритмов и средств моделирования обеспечения целостности информации, передаваемой в системах передачи-приема данных в условиях воздействия внутренних и внешних отрицательных факторов.

Задачи исследований:

1. Анализ и классификация современных угроз целостности данных в системах обмена дискретной информацией, на предмет выявления недостатков существующих методов, алгоритмов и средств обеспечения целостности с целью повышения их эффективности.

2. Разработка комплексного подхода к созданию средств обеспечения целостности данных, включающего способы обнаружения признаков несанкционированного доступа, выявления и исправления ошибок, вычисления риска возникновения повторных ошибок, вызванных средой передачи данных и сбоев приемной аппаратуры.

3. Разработка математической модели процесса приема и обработки информации на основе аппарата теории массового обслуживания для выявления признаков несанкционированного доступа в передаваемых пакетах данных.

4. Организация эффективного применения кодов с переменным весом, позволяющих обнаруживать ошибки, вызванные шумами среды передачи данных, а также разработка генератора кодов переменного веса и численного метода быстрого вычисления веса двоичных последовательностей для проведения их структурного анализа.

5. Разработка математической модели оценки риска возникновения повторных ошибок, вызванных сбоями приемной аппаратуры и программных средств.

6. Разработка комплекса программных средств для проведения имитационного моделирования обнаружения признаков несанкционированного доступа, выявления и исправления ошибок в передаваемых пакетах данных, в условиях отрицательно действующих факторов и риска возникновения повторных ошибок.

Научная новизна исследования состоит в применении комплексного подхода к решению основной задачи работы путем декомпозиции ее на составные части:

1. Обнаружении фактов несанкционированного доступа на основе построения модели системы передачи-приема данных в виде системы массового обслуживания, путем введения семимартингального описания точечных процессов, индикаторных функций и их компенсаторов, что позволяет повысить точность обнаружения признаков несанкционированного доступа и расширить область эффективного применения предложенной модели.

2. Эффективном применении кодов с переменным весом, позволяющих обнаруживать ошибки, вызванные шумами среды передачи данных, и с помощью разработанного численного метода быстро вычислять веса двоичных последовательностей для проведения их структурного анализа.

3. Оценки риска возникновения повторных ошибок, вызванных средой передачи данных и сбоями приемной аппаратуры систем передачи-приема данных с использованием сигмовидной функции Гомперца, позволяющей описывать с более высокой точностью угрозы нарушения целостности данных на начальной и завершающей стадиях функционирования системы передачи-приема данных.

Положения, выносимые на защиту:

1. Комплексный подход к созданию средств обеспечения целостности пакетов данных, передаваемых в системах передачи-приема данных, включающий алгоритмы обнаружения признаков несанкционированного доступа и нарушения корректности передачи данных, определения риска возникновения повторных ошибок.

2. Математическая модель обнаружения признаков несанкционированного доступа к системе передачи-приема данных, которая в **отличие от известных** построена на основе аппарата теории массового обслуживания с применением индикаторных функций и их компенсаторов,

повышающих точность проведения научных исследований и их результатов в разных режимах функционирования системы, что позволяет на практике создавать эффективные средства обнаружения несанкционированного доступа во время обмена данными.

3. Организация эффективного применения кодов с переменным весом, позволяющая обнаруживать ошибки и нарушения целостности данных путем контроля веса двоичного кода, генерировать код переменного веса, а также производить быстрый подсчет на основе предложенного численного метода расчета весов закодированных данных и анализ структуры их двоичного кода, **отличающаяся от известных тем**, что имеется возможность автоматической генерации кодов с любым весом для представления телеметрических данных на стороне отправителя и получателя, декодирования и восстановления прообразов данных с высокой точностью за счет использования таблиц кодов заданных весов.

4. Математическая модель определения риска повторных ошибок, вызванных сбоями приемной аппаратуры, которая в **отличие от известных** использует для оценки риска нарушения целостности сигмовидную функцию Гомперца, **позволяющую** описывать с более высокой точностью угрозы нарушения целостности данных на начальной и завершающей стадиях функционирования системы передачи-приема данных.

5. Разработанный программный комплекс, позволяющий проводить моделирование для исследования систем передачи-приема данных на стадиях их проектирования и эксплуатации, и создавать на его основе программно-аппаратные средства обеспечения целостности передаваемых данных.

Методика исследования. В ходе теоретического исследования применялись системный анализ, теория вероятностей и математическая статистика, функциональный анализ и теория функций. В процессе разработки алгоритмов использовались численные методы, методы аппроксимации и проектирования инфокоммуникационных систем.

Достоверность результатов диссертации подтверждается обоснованным и корректным применением аппарата теории вероятностей, теории кодирования, имитационного моделирования, численных методов и системного анализа, а также корректностью постановки научной задачи, решаемой в работе. Полученные научные результаты не противоречат известным, а также согласуются с экспериментальными данными.

Публикации и апробация работы. По результатам диссертационного исследования опубликовано 7 печатных работ. Среди них 4 работы опубликованы в изданиях, включенных в перечень ВАК, 3 работы опубликованы в иных печатных изданиях. Автором диссертации принято заочное участие в международной научно-технической конференции «Перспективные информационные технологии» г. Самара в 2022 году.

Личный вклад. Алгоритмы, математические модели, анализ результатов, содержащихся в диссертации, разработаны автором самостоятельно. Вклад соискателя в опубликованные работы является решающим.

Объем и структура работы. Диссертации состоит из введения, четырех глав, заключения, списка литературы. Объем диссертации составляет «131» страницы. Список литературы содержит «92» источника.

ГЛАВА 1. ОБЗОР ПРЕДМЕТНОЙ ОБЛАСТИ ИССЛЕДОВАНИЯ

В первой главе диссертации рассмотрена классификация, структура и характеристики систем передачи-приема данных (СППД), построена концептуальная модель СППД с нарушениями целостности. Приведены основные угрозы, которым подвергаются СППД, произведен анализ известных моделей обеспечения целостности данных.

1.1 Классификация, структура и характеристики систем передачи-приема данных

Применение различных дополнительных средств, которые обеспечивают надежный обмен дискретной информацией, является необходимым условием для комплексного развития современных наземных систем передачи-приема данных (СППД). Благодаря использованию современных методов и средств обеспечения целостности данных в СППД повышается защищенность передаваемой дискретной информации [8-10]. В связи с увеличением объемов передаваемых данных, появлением новых приемов со стороны злоумышленников, сложностью устройства приемной и передающей аппаратуры СППД разработка новых методов и программно-аппаратных средств обеспечения целостности является важной и актуальной задачей.

На рисунке 1.1 представлена классификация СППД, которая отражает известные способы «повышения достоверности, передаваемой по СППД дискретной информации» [10].

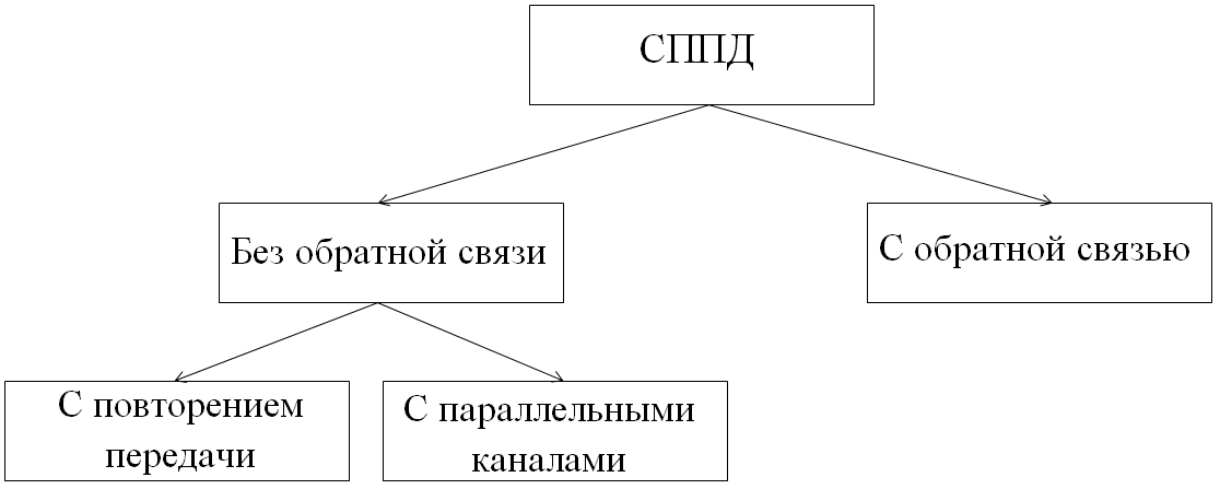

Рисунок 1.1 Классификация СППД

В СППД «без обратной связи информация от передатчика к приемнику передается по симплексным каналам передачи данных» [10]. «Состояние этих каналов определяется исключительно, по априорным сведениям, которые, как правило, являются неточными» [10]. В связи с этим приходится использовать достаточно сложные методы повышения достоверности передаваемой дискретной информации, что на практике приводит к усложнению используемой аппаратуры. Одним из возможных решений проблемы высокой сложности методов повышения достоверности передаваемой информации является «многократное повторение процесса передачи данных и передача информации по параллельным каналам, что неминуемо приводит к увеличению энергетических ресурсов, а также к усложнению реальной аппаратуры СППД» [10].

«Для СППД с обратной связью необходимы дуплексные и полудуплексные каналы передачи данных. В таких СППД за счет обратной связи появляется возможность повышения достоверности передаваемой дискретной информации. В известных вариантах в прямом канале применяется код, обнаруживающий ошибки. Данные об обнаруженной ошибке отправляются передающей стороне, а затем осуществляется повторная передача информации. Не трудно заметить, что при такой организации минимизируется вероятность потери передаваемых данных, а также пропадает необходимость в использовании сложных методов кодирования информации» [10, 11].

«Основными характеристиками, по которым можно осуществлять сравнение СППД и производить их оценку, являются: достоверность передачи информации, скорость передачи, а также время задержки данных» [10]. Для оценивания «количественной достоверности» [9] используют коэффициент не обнаружения ошибки, которые определяется как отношение между числом знаков, принятых с ошибкой, и общим количеством переданных знаков за заданный временной промежуток (выражение 1.1).

$$K_{НЕОШ} = \frac{C_{НЕОШ}}{C_{ОБЩ}}, \qquad (1.1)$$

где $K_{НЕОШ}$ - коэффициент не обнаружения ошибки, $C_{НЕОШ}$ - число знаков, принятых с ошибкой, $C_{ОБЩ}$ - общее количество знаков, переданных за заданный промежуток времени.

Скорость передачи битов данных определяется количеством символов данных, которая выражена числом битов данных, переданных за единицу времени [10]. Следует отметить возникающее противоречие между требованиями по достоверности и скорости передачи – чем выше достоверность передаваемой информацией, тем ниже скорость передачи данных.

В результате произведенного анализа классификации, характеристик и структуры СППД можно сделать вывод о насущной необходимости в разработке новых алгоритмов и подходов к повышению достоверности и защищенности передаваемой дискретной информации. При этом необходимо учитывать возникающие новые угрозы целостности данных, сложность устройства реальной аппаратуры СППД и возможности несанкционированного доступа к каналу передачи данных СППД.

1.2 Концептуальная модель системы передачи-приема данных

Разработка концептуальной модели СППД (рисунок 1.2) обусловлена достаточно сложным устройством реальных СППД и предназначена для описания основных составляющих, процессов и их взаимосвязей. При ее построении учитывались влияния дестабилизирующих факторов [12, 13], различные виды атак злоумышленников, сбои в работе оборудования из-за программно-аппаратных ошибок.

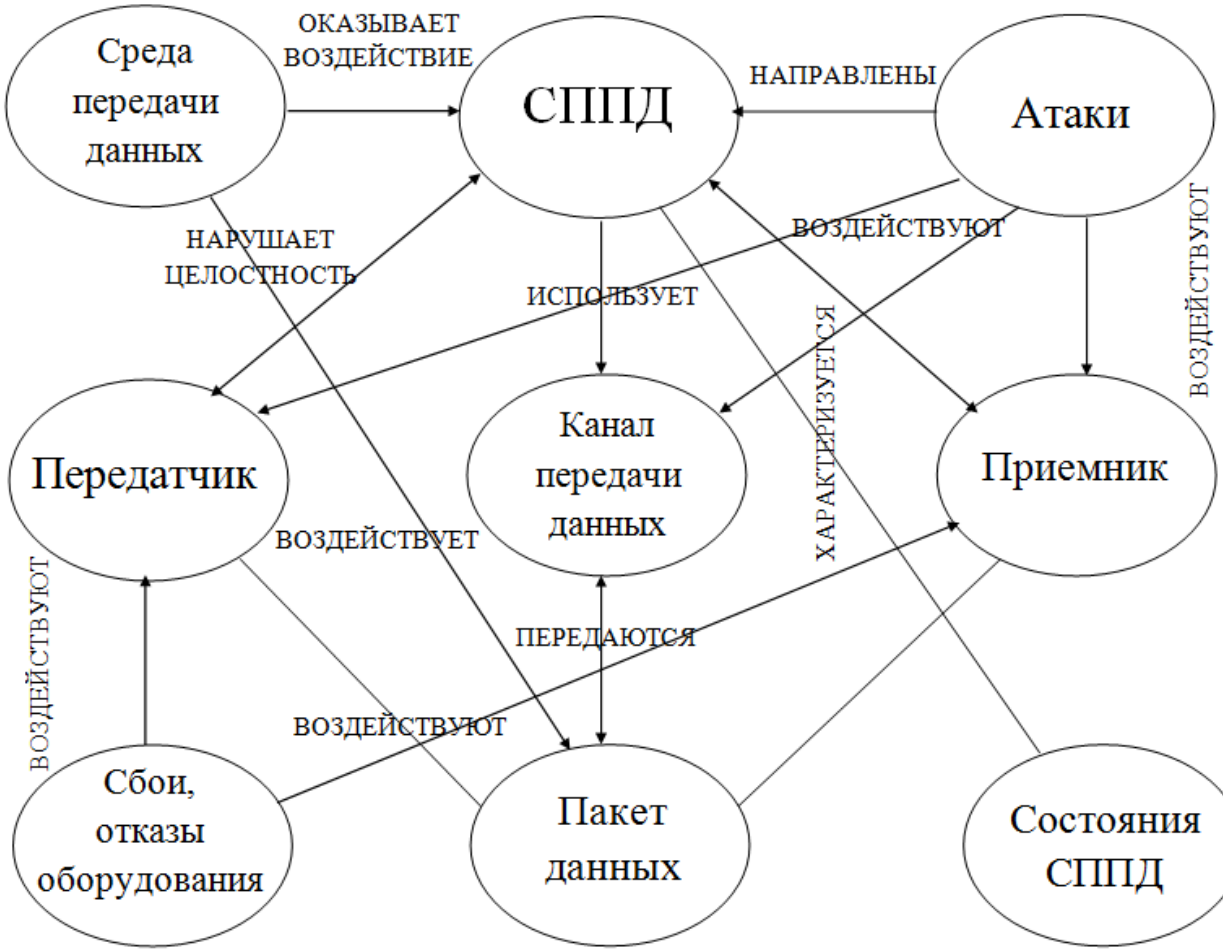

Рисунок 1.2 Концептуальная модель системы передачи-приема данных

Характерной особенностью разработанной концептуальной модели СППД являются отношения между ее составляющими (компонентами). Среда передачи данных оказывает воздействие на СППД, а производимые атаки злоумышленников направлены на нарушение ее работоспособности. Также среда передачи данных влияет на целостность данных, передаваемых по СППД. В результате возникновения сбоев и отказов оборудования (например, из-за его естественного старения), различных вредоносных атак злоумышленников происходит изменение состояния всей СППД.

Детализированное представление концептуальной модели СППД представлено на рисунке 1.3.

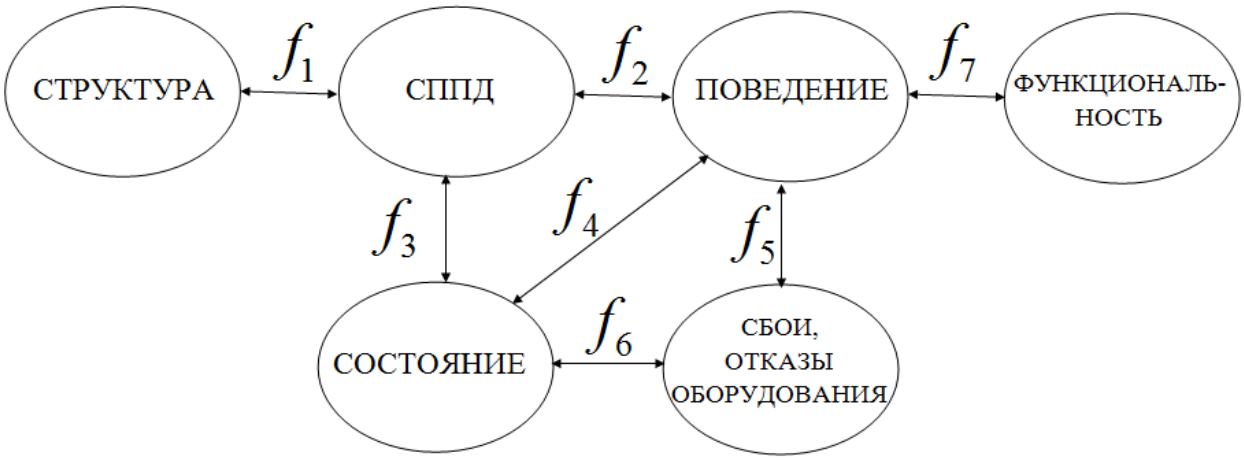

Рисунок 1.3 Детализированное представление концептуальной модели системы передачи-приема данных

В паре «СППД.←→ f1 ←→ Структура» СППД определяет множество последовательных операций по обмену информацией, представленными пакетами данных. В свою очередь СППД задает перечень и состав операций кодирования, декодирования, реагирования на внешние события и видов переходов между ними.

Пара «СППД←→ f2 ←→ Поведение» имеет двухстороннюю зависимость: СППД определяет результаты выполнения всех операций, а «поведение» позволяет оценивать СППД со стороны ее надежности, корректности и соответствие заложенной в ней протоколов телеметрии.

Пара «СППД←→ f3 ←→ Состояние» задается множеством состояний по всем выполняемым операциям, а состояние на всех шагах определяет режим функционирования СППД (штатный, неработоспособный). Пара «Поведение ←→ f4 ←→ Состояние» - это глубоко связанные понятия. Поведение определяется через множество состояний СППД на протяжении заданного отрезка времени. Состояние определяет поведение СППД, т.е. функционирование в штатном или нештатном режимах. Характерной особенностью пары «Поведение ←→ f5 ←→ Сбои, отказы оборудования, вмешательство» является наличие факта несанкционированного доступа, нарушения целостности состояния в получаемых данных. Сбой приводит к потере данных, а отказ – к полной остановке. Пара «Состояние ←→ f6 ←→ Сбои, отказы оборудования» – это взаимная связь.

Разработанная структурно-функциональная модель СППД учитывает состав операций, их связь, переходы, возможные риски возникновения сбоев, отказов оборудования или аппаратуры, постороннего вмешательства,

необходимые доработки в случае некорректного функционирования СППД, а также время, затрачиваемое на оценку параметров показателей, с помощью которых анализируется состояние СППД.

СППД с учетом ее перечисленных свойств и характеристик рассматривается как событийно-процессная последовательность, в которой под событием понимается результат завершения операции на каждом шаге, под переходом – переход к выполнению следующей по порядку операции. Отслеживая состояния и корректность упорядоченного перехода состояний, можно контролировать их соответствие заданным требованиям. Количество параметров для каждого состояния – фиксированное, конечное и имеет дискретное значение. Находясь в каждом из состояний, процесс обмена данными подвергается контролю параметров, принадлежащих к этому состоянию. Если хотя бы одно значение из контролируемого параметра текущего состояния системы выходит за пределы, установленные протоколом или требованиями, то процесс окончательной передачи данных приостанавливается для установления причины и места нарушения в потоке пакетов данных.

Такое представление СППД необходимо для определения основных функций подсистемы обнаружения признаков несанкционированного доступа, подсистемы обеспечения целостности телеметрических данных на основе кодов переменного веса, подсистемы определения риска возникновения повторных ошибок, вызванных сбоями приемной аппаратуры и программных средств. Построенная концептуальная модель системы передачи-приема данных позволяет найти зависимости между средой функционирования, отрицательно влияющими факторами и работоспособностью соответствующего оборудования. В реальных СППД имеется насущная необходимость в разработке дополнительных средств, направленных на обеспечение целостности данных, модернизации и усовершенствовании применяемого программного обеспечения.

1.3 Основные виды уязвимостей и угрозы целостности дискретной информации, возникающие в системах передачи-приема данных

Для предупреждения несанкционированного доступа, преднамеренного вмешательства и вредоносных атак злоумышленников необходим качественный анализ потенциальных уязвимостей, которым подвержена СППД. Угрозы возникают в случае наличия в системе уязвимостей, которые

могут привести к нарушению целостности передаваемой и обрабатываемой информации. Под угрозой будем понимать определенный фактор, стремящийся нарушить функционирование системы.

Обеспечение безопасности принимаемых и обрабатываемых данных является важной задачей при проектировании и разработке оборудования для СППД. Для прогнозирования, оценивания и минимизации вредоносных воздействий естественного и искусственного характера, в том числе вредоносных атак злоумышленников, необходимо рассмотреть актуальные угрозы целостности информации, которая принимается, обрабатывается и передается по СППД.

Носители данных могут содержать следующее:

- информацию в виде электрических, электромагнитных, оптических сигналов;
- информацию в виде бит, байт или иных логических структур.

В целях формирования перечня угроз информации, передаваемой по СППД, а также при ее обработке в них, угрозы классифицируются по следующим признакам (рисунок 1.4):

Рисунок 1.4 Классификация угроз целостности информации, передаваемой по СППД

По видам источников угроз выделяют: угрозы, связанные с преднамеренными действиями злоумышленников, не имеющих непосредственный доступ к данным, а также угрозы, возникающие в результате внедрения в СППД различных закладок или вредоносного программного обеспечения.

По способу реализации выделяют угрозы утечки данных по техническим каналам и угрозы специальных воздействий на СППД.

По виду нарушаемого свойства информации выделяют следующие: «угрозы конфиденциальности, при реализации которых не осуществляются воздействия на содержание информации, угрозы несанкционированного воздействия на целостность информации, приводящие к ее непосредственному изменению» [14], угрозы несанкционированного воздействия на программно-аппаратные элементы системы, угрозы, в результате реализации которых происходит полное уничтожение информации.

По используемой уязвимости выделяют следующие: угрозы, которые реализуются при помощи уязвимостей системного программного обеспечения; угрозы, которые реализуются при помощи уязвимостей прикладного программного обеспечения; угрозы, которые реализуются с использованием уязвимости, вызванной наличием аппаратной закладки; угрозы, которые реализуются с использованием уязвимостей каналов передачи данных; угрозы, которые реализуются с использованием уязвимостей штатных средств защиты системы.

По объекту воздействия выделяют следующие: угрозы безопасности данных, передаваемых по СППД, угрозы прикладным программам, при помощи которых осуществляется обработка данных, угрозы системному программному обеспечению, при помощи которого осуществляется функционирования всей СППД.

В результате реализации вышеописанных угроз безопасности информации могут быть нарушены ее следующие свойства:

- целостность данных (в результате воздействия окружающей среды, вредоносных атак злоумышленников, направленных на искажение (в том числе фрагментацию, встраивание дополнительных пакетов, изменения формы сигналов и т.д.) передаваемых данных);

- конфиденциальность данных (вследствие возникновения уязвимостей в системе, обусловленных программно-аппаратными сбоями в работе оборудования);

- доступность данных (вследствие нарушения структуры системы).

Угрозы, которым подвергается СППД, – это неправомерные изменения параметров или структуры элементов системы. Остановимся на угрозах целостности информации:

- неправомерное добавление (удаление) объекта;

- изменение атрибутов системы или компрометация отдельных связей между объектами системы;

- создание дополнительных каналов между элементами системы (что создает дополнительные риски нарушения целостности принимаемых и обрабатываемых данных);

- различные аппаратные и программные сбои в СППД.

Угрозы целостности на аппаратном уровне зачастую возникают в результате ошибок выбора области памяти при отправке данных. На программном уровне из-за возникновения ошибок в протоколах передачи данных. Такие угрозы могут быть реализованы в результате воздействия случайных аддитивных помех (комбинаций аддитивных помех) на канал передачи данных СППД. Необходимо учитывать, что с развитием технологий передачи данных возникают новые способы неправомерных воздействий, требующих разработки принципиально новых средств защиты информации.

На рисунке 1.5 приведена классификация уязвимостей, которым подвержена СППД.

Рисунок 1.5 Классификация уязвимостей, которым подвержена СППД

Более подробно рассмотрим уязвимости программного обеспечения и реализацию атаки «Отказ в обслуживании». «Уязвимости системного программного обеспечения обычно рассматривают с привязкой к архитектуре построения вычислительных систем» [13]. При этом следует отдельно отметить уязвимости в средствах системы, которые представляют собой фрагменты кода программ и позволяют обходить процедуры проверки целостности, а также отсутствие необходимых средств защиты, (проверки форматов данных). К уязвимостям прикладного программного обеспечения относятся отсутствие механизмов предотвращения перезагрузок буфера, а также отсутствие механизма проверки корректности содержимого пакета. Атака «Отказ в обслуживании» основана на недостатках штатных средств защиты и системного программного обеспечения, позволяющего злоумышленнику создавать условия, при которых система не способна обрабатывать поступающие пакеты. На рисунке 1.6 представлены несколько ее разновидностей.

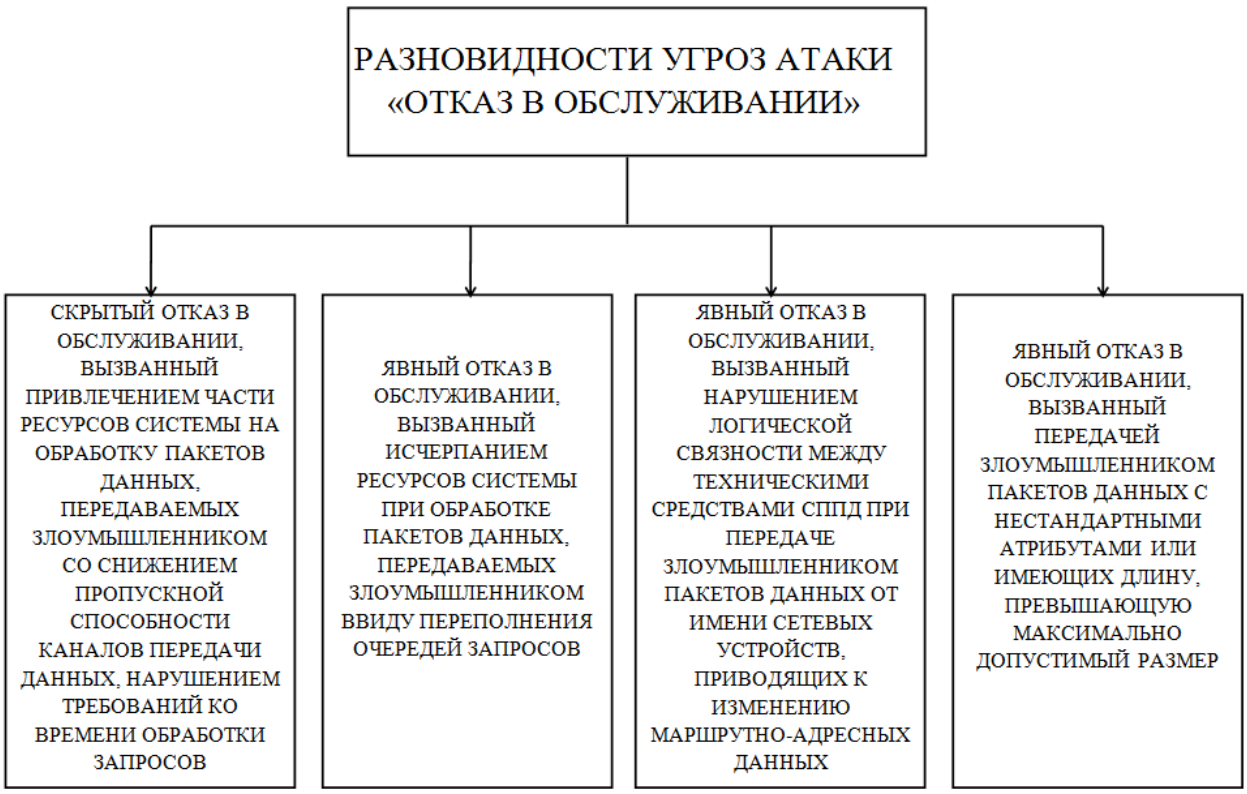

Рисунок 1.6 Разновидности угроз атаки «Отказ в обслуживании»

«Процесс реализации этих угроз в общем случае состоит из четырех этапов:

- сбора необходимой информации о системе;
- проникновения в среду;
- осуществление несанкционированного доступа;
- ликвидация следов несанкционированного доступа» [15].

Исходя из статистики нарушений целостности данных, штатные средства защиты данных не способны в полной мере справляться с переполнением очередей запросов, передаваемых злоумышленниками для вывода из рабочего состояния приемного устройства СППД. Также необходимо учитывать, что при совершенствовании аппаратуры СППД возрастает сложность ее устройства, что неминуемо влечет к возникновению новых угроз безопасности информации. Как показывают исследования [16], актуальным является разработка дополнительных средств идентификации нарушений конфиденциальности, целостности и доступности информации при ее непосредственном поступлении в СППД, разработка новых более быстрых методов исправления выявленных нарушений, а также разработка соответствующих механизмов, способных оценивать и прогнозировать риски нарушения безопасности данных.

Для определения параметров и критериев к модели обеспечения целостности данных для СППД произведем анализ известных моделей целостности и выявим их сильные и слабые стороны. Наглядным примером является мандатная модель целостности данных Биба. По своим свойствам эта модель является инверсией классической модели Белла-Лападула (МБЛ) [17]. Их достоинствами считается использование следующих правил:

- «первое правило заключается в запрещении субъектом считывания данных из объекта с низким уровнем целостности;

- второе правило заключается в запрещении субъектом записи данных в объект с более высоким уровнем целостности» [17].

Недостатком модели Биба является противоречивость правил построения. Обычно в случае возникновения такого противоречия переходят к построению модели понижения уровня субъекта. Эта модель позволяет совершать запись в объект с более высоким уровнем целостности, тем самым, не предусматривая механизмов для повышения целостности объектов, что приводит к снижению уровня целостности всей системы.

Еще одной известной моделью целостности данных является модель целостности Кларка-Вилсона. [17]. В этой модели процедуры преобразования информации описываются в виде функций, которые определяют любые неправомерные действия субъектов над данными. Основными правилами построения модели целостности Кларка-Вилсона являются:

1. В системе должны существовать процедуры проверки целостности, например, проверка контрольной суммы, которая позволяет определять уровень целостности передаваемых данных;
2. Использование процедуры преобразования должно сохранять их целостность;
3. Вносить изменения в данные разрешается только процедурам преобразования;
4. Субъекты могут инициализировать определенные процедуры преобразования над ограниченными элементами данных;
5. Система определяет правила, не позволяющие субъектам изменять целостность;
6. Любые преобразования целостности должны регистрироваться в специальном журнале;

7. Система должна определять механизмы предотвращения атак, в результате которых, происходит подмена одного субъекта другим;

8. Изменения в списках авторизации доступно только специальным субъектам.

Вышеуказанные правила позволяют определять подходы к построению механизмов проверки целостности данных. Очевидно, что представленные в этом разделе модели обеспечения целостности не могут быть применимы в современных СППД, так как, не учитывают риски, связанные с условиями (средами) функционирования оборудования этих систем. Произведенный анализ моделей целостности данных Биба и Кларка-Вилсона позволил определить их основные достоинства и недостатки и предназначался для формирования модели обеспечения целостности данных, лишенной выявленных недостатков.

В процессе разработки средств обеспечения целостности данных для СППД следует учитывать условия и среду передачи данных, множество отрицательно влияющих факторов и особенно тех, противодействие которым затруднено.

Исходя из современных тенденций к построению моделей обеспечения целостности данных, наиболее распространённым является стохастический подход к описанию воздействия угроз нарушения целостности данных. С использованием аппарата теории массового обслуживания (ТМО) для обнаружения фактов несанкционированного доступа к СППД построен специальный механизм идентификации признаков нарушения целостности данных с использованием точечных процессов, индикаторных функций и компенсаторов процессов в семимартингальном описании [18, 19], что на практике позволяет обеспечивать агрегируемость данных (переход от единичных параметров модели к комплексным (интегральным)).

1.4 Выводы по первой главе

1. Представлена классификация СППД, анализ которой показал, что СППД имеет сложную информационную структуру, для которой требуется использовать наиболее эффективные методы обеспечения целостности данных. Также в процессе анализа выявлено, что используемые на практике существующие методы обеспечения целостности имеют ряд существенных недостатков, что не позволяет обеспечивать необходимый уровень безопасности передаваемой дискретной информации.

2. Предложена концептуальная модель системы передачи-приема данных, которая представлена множеством компонентов и связей между ними, определяющих ее смысловую структуру и позволяющую на ее основе создавать модели систем обеспечения целостности передаваемых данных с учетом различных видов атак злоумышленников и сбоев оборудования.

3. Произведен анализ наиболее известных угроз нарушения безопасности данных, циркулирующих в СППД. Представлены известные модели целостности, их достоинства и недостатки. Основным недостатком является сложность и большие временные затраты на обнаружение нарушений целостности и контроль надежности аппаратуры передачи – приёма данных.

ГЛАВА 2. РАЗРАБОТКА ПОДСИСТЕМЫ ОБНАРУЖЕНИЯ ПРИЗНАКОВ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В СИСТЕМАХ ПЕРЕДАЧИ-ПРИЕМА ДАННЫХ

Во второй главе диссертации рассмотрены основные процедуры по выявлению угроз нарушения целостности данных, способы получения информации о состоянии СППД, известные методы обеспечения целостности данных, применяемых в СППД.

Целью главы является разработка математической модели подсистемы обнаружения признаков несанкционированного доступа в СППД на основе аппарата теории массового обслуживания. Для построения модели использовались эффективные с точки зрения количества необходимых вычислений методы аппроксимации, индикаторные функции и компенсаторы процессов. Параметры модели построены в семимартингальном описании [20], что позволяет обеспечивать агрегируемость данных (возможность перехода от единичных параметров модели к комплексным).

2.1 Способы получения информации о состоянии системы передачи-приема данных и основные методы выявления угроз нарушения целостности данных

В настоящее время существует достаточно обширный перечень угроз целостности информации, передаваемой по СППД. В результате развития СППД, увеличения объемов передаваемой информации появляются новые угрозы целостности данных, противодействие которым при помощи известных методов и средств недостаточно эффективно. Несанкционированное изменение данных злоумышленником является примером нарушения статической целостности. Изменение структуры пакетов данных является примерами нарушения динамической целостности.

Для разработки эффективных подходов, направленных на совершенствование процессов по выявлению угроз нарушения целостности данных в СППД, необходимо рассмотреть классификацию угроз по ряду признаков. Для наглядности на рисунке 2.1 представлена следующая классификация угроз нарушения целостности данных в СППД. В результате детального анализа приведенной классификации можно заметить, что угрозы характеризуются множеством параметров, имеющих различную природу источников, степень влияния и проявления, что

существенно усложняет противодействие им и приводит к усложнению средств, осуществляющих эти процедуры.

Реализация угроз, представленных на рисунке 2.1, возможна при несанкционированном изменении пакетов данных, при возникновении различных видов ошибок (пачек ошибок) в приемном устройстве, а также при вредоносном воздействии (атаках) злоумышленников. В связи с этим разработка новых моделей и средств, направленных на противодействие угрозам нарушения целостности данных, является важной и актуальной задачей для СППД. Основными процедурами по выявлению угроз нарушения целостности данных в СППД являются [15]:

- анализ показателей функционирования СППД;
- прогнозирование показателей функционирования СППД;
- идентификация вредоносных воздействий злоумышленников на приемное устройство СППД.

Анализ состояния СППД может осуществляться различными способами и зависит от его конкретных характеристик. Основными способами получения информации о состоянии СППД являются:

- «использование Марковских моделей» [21];
- «имитационное моделирование» [22];
- «анализ временных рядов» [21].

Рисунок 2.1 Классификация угроз нарушения целостности данных

Для верификации способов, направленных на своевременное выявление угроз нарушения целостности данных в СППД, используют технологии имитационного моделирования, представляющие собой средства, использующие набор стандартных функций, отражающих работу типовых элементов модели, а также ориентированных на ее отладку и организацию вычислительных экспериментов [22, 23]. Построение прогнозов на основе анализа временных рядов применяется для моделирования процессов, протекающих в СППД [24].

Для своевременного выявления признаков несанкционированного доступа и других угроз нарушения целостности данных используют методы контроля (самоконтроля) состояний СППД, которые отличаются друг от друга используемыми критериями [22]. Определение коэффициента ошибок $K_{ОШ}$ осуществляется с помощью прямого и косвенного методов. Прямой метод предполагает определение коэффициента ошибок путем подсчета числа искаженных символов в заранее известной на приеме последовательности символов на интервале анализа [24]:

$$K_{ОШ} = n_{ОШ} / N ,$$

где $n_{ОШ}$ – количество ошибочных символов, а N – общее количество символов, переданных на интервале анализа.

Косвенные методы основаны на подсчете количества искаженных сигналов с последующим определением вероятности ошибки. Основной задачей при применении прямого и косвенного методов контроля состояний СППД является получение оценки вероятности ошибки за минимальное время. Наиболее эффективным из данных методов будет тот, которой при определенном объеме выборки дает наименьшее значении дисперсии вероятности ошибки.

Структура атаки, осуществляемой злоумышленниками, как правило, имеет комплексную и сложную организацию, которую практически невозможно выявить без дополнительных специальных программно-аппаратных средств. При разработке средств обеспечения целостности данных для СППД необходимо учитывать влияние дестабилизирующих факторов (вызванной средой, в которой функционирует аппаратура СППД), сложность устройства реальной аппаратуры (оборудования) СППД (что является дополнительным источником возникновения угроз и уязвимостей), а также модификации основных видов атак злоумышленников.

2.2 Методы обеспечения целостности дискретной информации в системах передачи-приема данных

С развитием технологий приема, обработки и передачи данных возникают новые угрозы целостности информации, следовательно, появляется необходимость в совершенствовании уже известных методов защиты. В этом разделе представлен краткий анализ, приведены достоинства и недостатки известных методов обеспечения целостности данных в СППД.

Существует несколько факторов, приводящих к несанкционированной модификации принимаемых и обрабатываемых данных, в результате воздействия которых может быть нарушена их целостность. Нарушение целостности данных в СППД возможно в результате возникновения аппаратной или программной ошибки [27]. Целостность информации также может быть нарушена в результате несанкционированных изменений данных, что является следствием неправомерного повышения привилегий пользователей системы, а также различных модификаций программного обеспечения. Нарушение целостности данных также происходит из-за вредоносных воздействий злоумышленников, которые вносят изменения в содержимое пакетов данных и их атрибутов. В системах, в которых отсутствуют механизмы проверки целостности данных, несанкционированные изменения не обнаруживаются и приводят к нарушению функционирования ее программно-аппаратного обеспечения [28, 29].

На рисунке 2.2 приведены основные причины нарушения целостности данных.

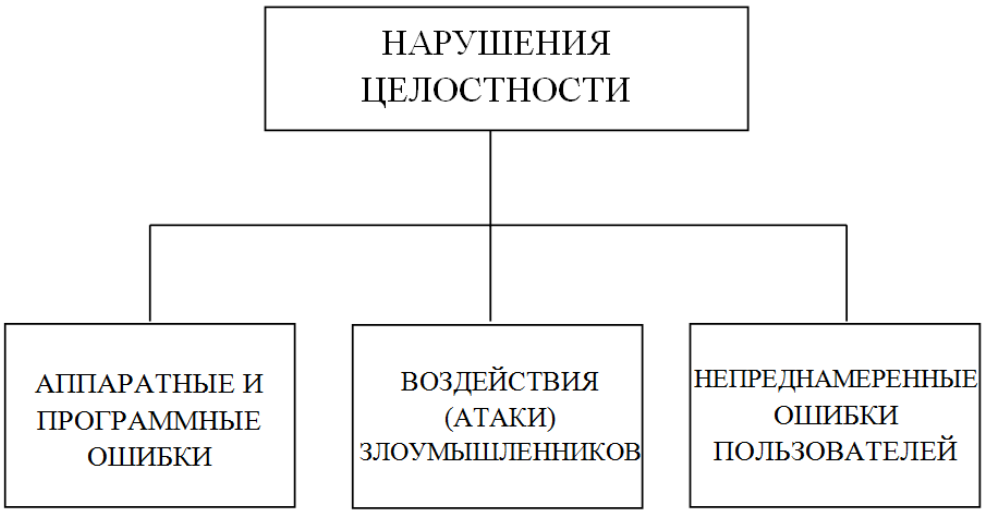

Рисунок 2.2 Основные причины нарушения целостности данных в СППД

1. Программные и аппаратные ошибки. В результате развития СППД возросли требования к механизмам обеспечения целостности передаваемой

информации. По причине возрастающей сложности в структуре средств приема и передачи данных увеличивается количество новых ошибок, которые проблематично обнаружить и исправить с применением известных средств [28, 29]. Зачастую такие ошибки характеризуются видом и интенсивностью помех, которые постоянно воздействуют на СППД. Различают флуктуационные, гармонические и импульсные помехи [23]. Флуктуационная помеха представляет явление, проявляющееся во времени случайным образом. Одной из причин ее появления является тепловой шум элементов аппаратуры. Гармоническая помеха приближенно описывается синусоидальным колебанием. Эти помехи возникают в аппаратуре из-за проникновения в СППД различных несущих колебаний. Импульсной помехой называется помеха, максимальное значение которой соизмеримо с амплитудой сигнала [23]. Импульсные помехи, как правило, появляются пачками. Характер процесса появления пачек помех во времени и отдельных помех внутри одной пачки существенно изменяется в различные периоды времени.

Следует отметить, что в реальных условиях ошибки, появляющиеся в принимаемых и обрабатываемых данных, в большинстве случаев являются коррелированными и сгруппированы в пачки. Законы распределения ошибок в СППД исследуют преимущественно экспериментальным путем и на основании этого создают различные математические модели.

2. Вредоносные воздействия злоумышленников. Информация, которая принимается, обрабатывается и передается по СППД, может быть искажена в результате воздействий злоумышленников. Изменения вносятся при воздействии на штатные средства защиты системы, а также с использованием различного вредоносного программного обеспечения.

3. Ошибки пользователей. Как правило, такие ошибки происходят на уровне приложений [23]. Примером являются действия, в результате которых возможно удаление конфигурационных файлов, баз данных и приложений. Изменение настроек приложений часто становиться причиной нарушения целостности данных.

Рассмотрим известные методы обеспечения целостности данных в СППД (рисунок 2.3).

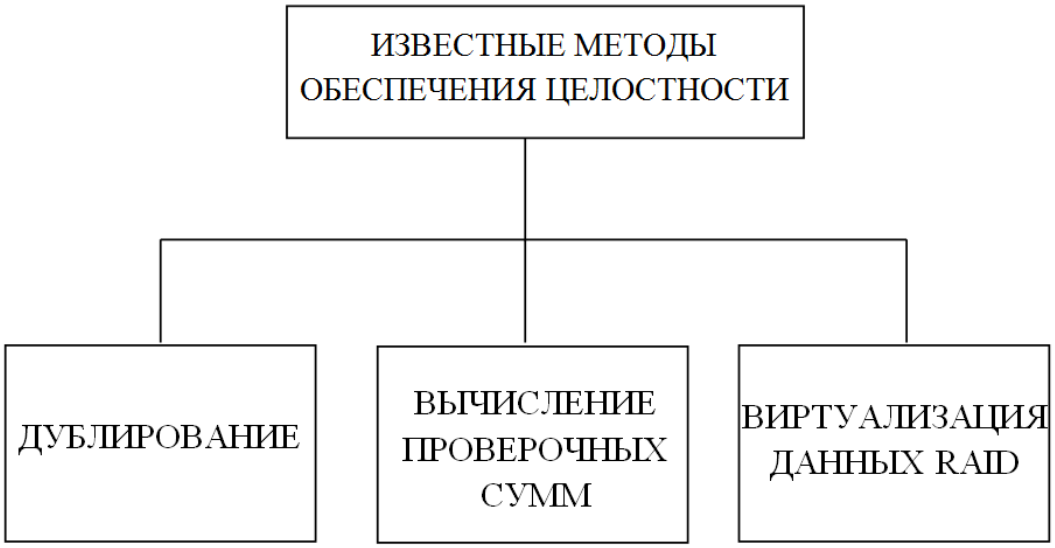

Рисунок 2.3. Известные методы обеспечения целостности данных в СППД

1. Дублирование данных. Достаточно продуктивным методом обеспечения целостности данных является формирование их копии. Такой метод обеспечения целостности данных крайне неэффективен для защиты от действий злоумышленников [24]. Злоумышленник может иметь доступ к дубликату, вследствие модификации которого, обнаружить изменения и восстановить данные будет невозможно. Дублирование является крайне затратным методом обеспечения целостности, поскольку использует большие объемы памяти для хранения копии объекта защиты. Этот метод обладает малой вычислительной сложностью, но при этом имеет ряд недостатков, среди которых следует отметить большую избыточность и, как следствие, высокую стоимость реализации.

2. Вычисление проверочных сумм (помехоустойчивое кодирование). Данный метод обеспечения целостности осуществляется при помощи хеш-функций. Необходимым требованием к этим функциям является их устойчивость к различным коллизиям. Основными требованиями, предъявляемыми к помехоустойчивым кодам, являются: уменьшение избыточности, увеличение скорости кодирования, увеличение корректирующей способности. Главным отличием помехоустойчивых кодовых конструкций от хеш-функций является их способность непосредственного исправления обнаруженной ошибки. Помехоустойчивые коды применяются для обеспечения целостности данных в СППД. С увеличением скорости передачи данных в дискретных каналах СППД и возрастанием количества аддитивных ошибок становится актуальной разработка новых алгоритмов помехоустойчивых кодовых конструкций. Помехоустойчивое кодирование, по сравнению с дублированием,

обладает большой вычислительной сложностью, но при этом меньшей избыточностью. Среди преимуществ данного метода следует отметить относительно небольшую стоимость реализации.

3. Технология виртуализации данных RAID позволяет объединять несколько физических жестких дисков в логический модуль для повышения производительности и отказоустойчивости. При этом виртуализация данных весьма затратна с точки зрения ее практической реализации. «Виртуализация данных не подходит для обеспечения целостности данных в СППД, поскольку она не может гарантировать своевременное обнаружение ошибок непосредственно при получении, преобразовании и отправке» [24]. Данный метод обладает небольшой вычислительной сложностью, но в сравнении с вышеописанными методами обеспечения целостности является довольно затратным с точки зрения его практической реализации.

В результате произведенного анализа выявлены достоинства и недостатки известных методов обеспечения целостности данных, применяемых в современных системах. Очевидно, что использование данных методов (как по отдельности, так в совокупности) в условиях динамической и быстро изменяющейся обстановки не позволяет обеспечить необходимый уровень защищенности данных, циркулирующих в СППД. Следовательно, возникает насущная необходимость в разработке дополнительных программно-аппаратных средств, способных обеспечивать своевременное обнаружение и исправление нарушений целостности передаваемых данных.

2.3 Разработка подсистемы обнаружения признаков несанкционированного доступа в системах передачи-приема данных на основе аппарата теории массового обслуживания

Рассмотрим основные признаки нарушений целостности дискретной информации, передаваемой по СППД в виде следующей схемы (рисунок 2.4).

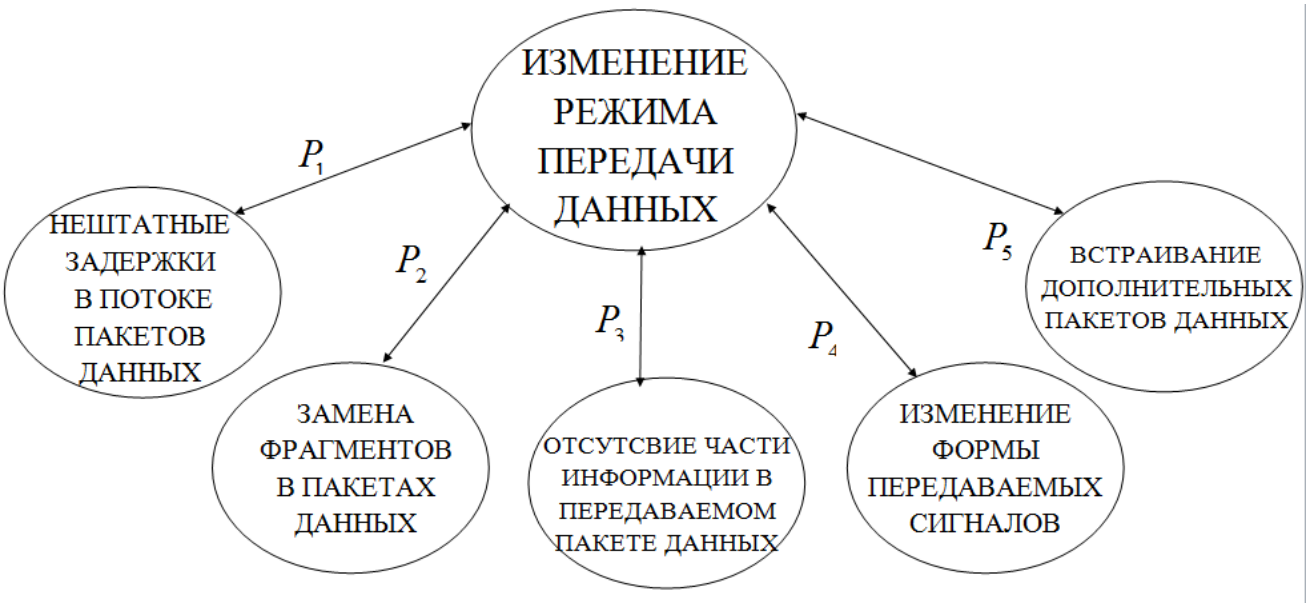

Рисунок 2.4 Признаки нарушений целостности данных в СППД

На рисунке 2.4 представлены основные признаки нарушений целостности данных, передаваемых по СППД. Наличие в СППД любого из указанных на рисунке 2.4 признаков приводит к изменению режима передачи данных, что идентифицируется системой как факт нарушения целостности. Все признаки нарушения целостности данных могут быть включены в один общий интегральный признак, по которому можно зафиксировать их присутствие. К изменению режима передачи данных может привести: отсутствие части данных, замена фрагментов в передаваемом пакете данных, изменение веса пакета данных, встраивание дополнительных пакетов данных, изменение формы передаваемых сигналов. Другими словами, такие изменения особенно характерны в случаях несанкционированного доступа к режиму передачи данных со стороны злоумышленников.

Для разработки модели обнаружения признаков несанкционированного доступа в СППД воспользуемся хорошо зарекомендовавшим себя аппаратом теории массового обслуживания (ТМО) [25, 27, 30]. Отличительной особенностью разрабатываемой модели от известных, является применение вероятностного подхода с использованием точечных процессов, индикаторных функций и их

компенсаторов в семимартингальном описании [18, 20]. Использование семимартингального описания позволяет осуществлять переходы от единичных параметров модели к комплексным (интегральным) и своевременно выявлять пакеты данных с признаками нарушения целостности.

Систему обеспечения целостности данных (СОЦД) представим в виде трех взаимосвязанных и взаимодействующих между собой подсистем: подсистемы обнаружения признаков несанкционированного доступа к СППД, подсистемы обеспечения целостности данных на основе кодов с переменным весом и подсистемы определения риска повторного возникновения ошибок (рисунок 2.5).

Рисунок 2.5 Система обеспечения целостности данных

В результате несанкционированного доступа и отрицательно действующих факторов возникает вероятность сбоев в работе программно-аппаратных средств СППД. Находящиеся в приемном устройстве пакеты данных, поступают в буферную память системы (всех поступающих пакетов данных за заданный период времени), формируют очередь и отправляются в первую подсистему обнаружения признаков несанкционированного доступа, построенной на основе аппарата теории массового обслуживания, в которой происходит анализ информации о состоянии очереди и оценка интенсивностей поступления пакетов данных.

После обнаружения признака несанкционированного доступа, пакет данных поступает в подсистему обеспечения целостности данных на основе кодов с переменным весом, после чего начинается новая проверка на возможность появления вторичных ошибок, вызванных сбоями приемной аппаратуры. На выходе формируется следующая информация: исправленный пакет данных, данные об обнаруженной ошибке.

Структуру передаваемых телеметрических данных рассмотрим, как сочетание самих данных в виде пакета, согласно Госстандарту по телеметрии (рисунок 2.6) [26].

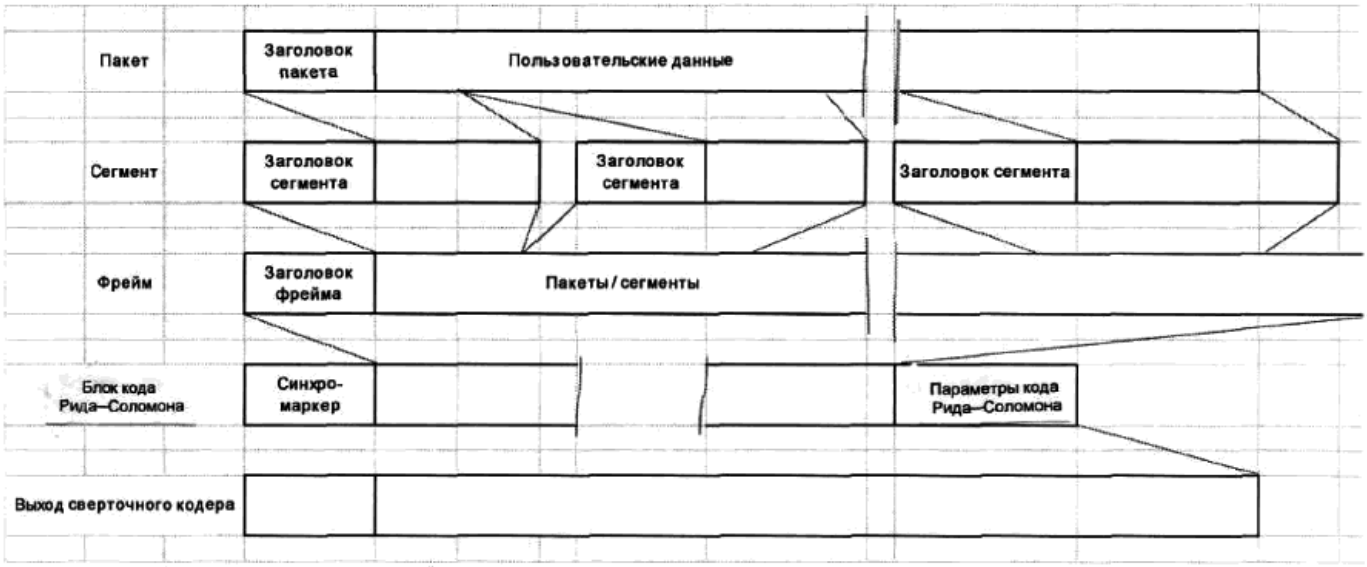

Рисунок 2.6 Структура данных, циркулирующих в СППД

Структура пакета данных позволяет вносить в нее некоторую дополнительную информацию, а именно указания на процедуры выполнения поиска несанкционированного доступа, поиска ошибок, исправления этих ошибок и хранения восстановленных данных. На рисунке 2.7 представлен пример потока телеметрических данных [26].

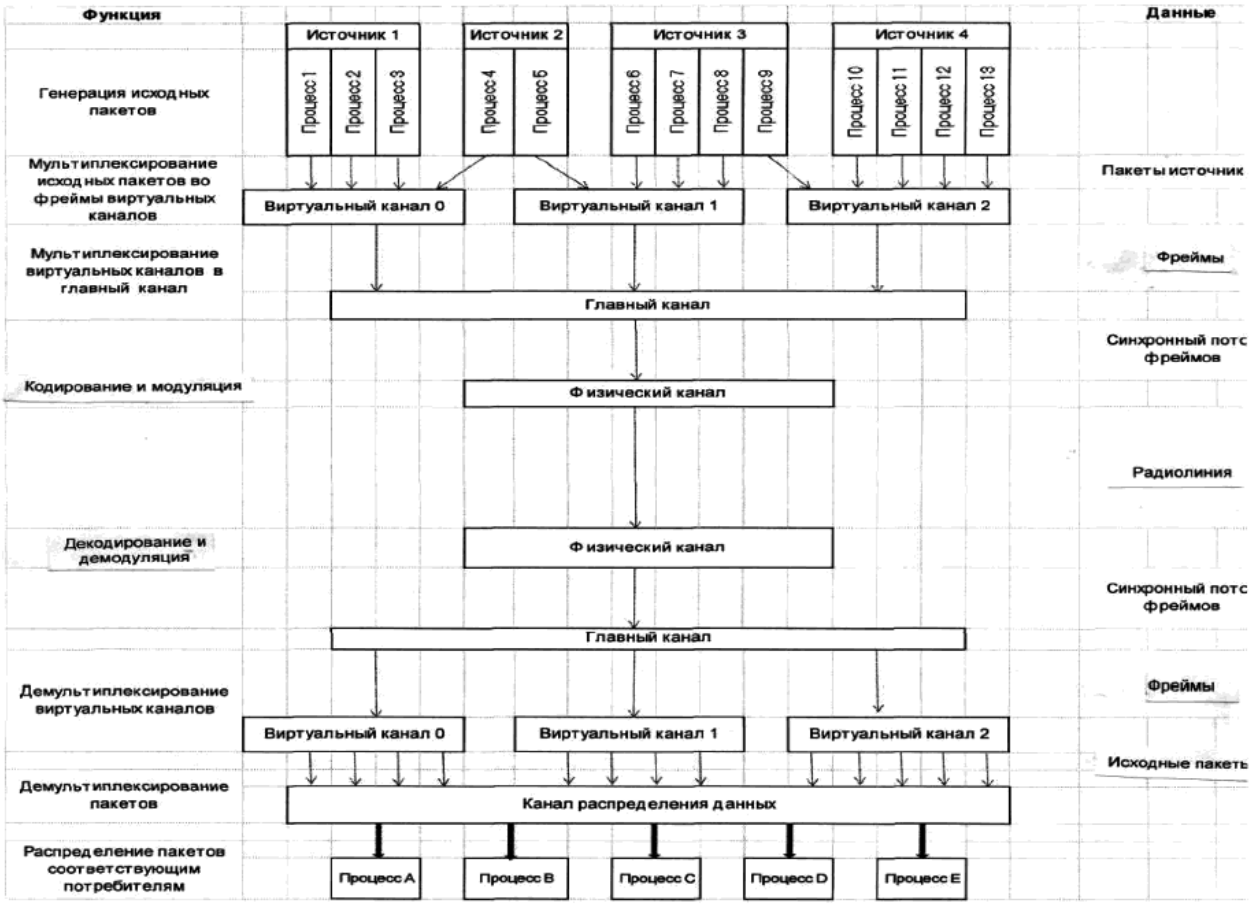

Рисунок 2.7 Пример потока телеметрических данных

Содержание пакета данных представлено на рисунке 2.8 [26].

Рисунок 2.8 Содержание пакета данных

Под воздействием отрицательно влияющего фактора (например, встраивания дополнительной информации) происходит изменение структуры пакета данных, следовательно, осуществляется переход в другой формат пакета с признаком нарушения целостности. Структура измененного пакета данных представлена на рисунке 2.9.

Рисунок 2.9 Структура измененного пакета данных

Граф переходных состояний передаваемых данных представлен на рисунке 2.10.

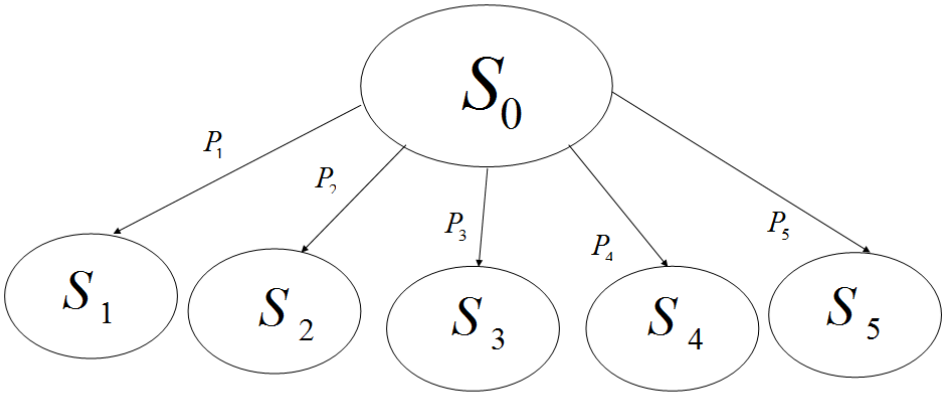

Рисунок 2.10 Граф переходных состояний передаваемых данных

Из-за воздействия дестабилизирующих факторов среды передачи данных, несанкционированного доступа к СППД происходит изменение структуры

передаваемых пакетов данных и переход из нормального состояние в одно из состояний с признаком нарушения целостности. Такими признаками могут быть: отсутствие части данных, замена фрагментов в передаваемом пакете данных, изменение веса пакета данных, встраивание дополнительных пакетов данных, изменение формы передаваемых сигналов. На рисунке 2.10 представлен граф переходных состояний данных, где S_0 – состояние данных в момент его передачи (нормальное состояние), S_1, S_2, S_3, S_4, S_5 – состояния данных с признаком нарушения целостности, P_1, P_2, P_3, P_4, P_5 – вероятности перехода к одному из состояний с признаком нарушения целостности. Переход данных из штатного состояния в состояния с нарушением целостности носит случайный (вероятностный) характер и зависит от отрицательно влияющих факторов (как внутренних, так и внешних). Под внутренними факторами подразумевается среда передачи данных, под внешними – вредоносные воздействия (атаки) злоумышленников. Индикатором внештатного состояния системы передачи-приема данных являются наличие одного из признаков нарушения целостности, представленных на рисунке 2.4.

Задача построения модели подсистемы обнаружения признаков несанкционированного доступа к СППД – проведение моделирования процесса передачи-приема дискретной информации по каналу передачи данных, в котором действуют внешние и внутренние отрицательные факторы: шумы, сбои аппаратуры, что приводит к нарушению целостности передаваемых данных.

Цель – установление возможностей оперативного обнаружения этих отрицательно действующих факторов и принятие решений по их сокращению.

Математические модели обладают универсальностью ко многим областям применения, и особенно, при описании и проведении моделирования вероятностных процессов. Для построения модели используется прием подбора одного из хорошо изученных вариантов математических моделей в области систем массового обслуживания (СМО), которые широко используются на практике, имеют результативность и хорошую реализуемость в виде программного приложения. Кроме этих свойств системы передачи-приема данных имеют структурные аналогии с СМО: заявки интерпретируются как пакеты данных, очереди как задержки, так и сами процессы обработки заявок (пакетов данных), что при определенных допущениях обеспечивает адекватность построения модели.

«Модель СМО строится из совокупности элементов, таких как канал, источник заявок, очередь, заявка, дисциплина обслуживания, стек, что позволяет имитировать множество задач типовым образом.

Заявки образуют потоки: поток заявок на входе СМО, поток обслуженных заявок, поток отказанных заявок. Поток характеризуется количеством заявок определенного сорта, наблюдаемым в некотором месте СМО за единицу времени (час, сутки, месяц), то есть поток есть величина статистическая.

Очереди характеризуются дисциплиной обслуживания, количеством мест в очереди (сколько клиентов максимум может находиться в очереди), структурой очереди (связь между местами в очереди). Очереди делятся на ограниченные и неограниченные» [27].

«Судить о результатах работы СМО можно по показателям. Для решения поставленной задачи представляют интерес:

- вероятность обслуживания системой пакета данных;
- пропускная способность системы;
- среднее время занятости канала;
- среднее количество пакетов данных, находящихся в очереди;
- среднее время ожидания пакета данных в очереди;
- среднее время обслуживания пакета данных;
- среднее время нахождения пакета данных в системе» [27].

В «качестве параметров СМО могут быть использованы: интенсивность потока пакетов данных, интенсивность потока обслуживания, среднее время, в течение которого пакет готов ожидать обслуживания в очереди, дисциплина обслуживания. Параметры влияют на показатели системы массового обслуживания» [27].

Меняя управление, можно влиять на значение другого контролируемого показателя и добиться улучшения этого показателя. В качестве цели может служить вероятность отказов, пропускная способность, среднее время обслуживания.

Нарушение целостности данных предлагается обнаруживать, анализируя состояния модели через множество выделенных контролируемых параметров, которые зависят от параметров состояния внешних воздействующих факторов. Эта зависимость обнаруживается в процессе изменения значений последних.

С помощью моделирования выявляются задержки поступления пакетов по величине, времени и их месте в потоке пакетов, а по получаемой информации

можно судить о признаках возникновении несанкционированного доступа и видах нарушений целостности.

Перейдем к выбору типа системы массового обслуживания для проведения моделирования и сопоставлению ее параметров с элементами системы. «Системы массового обслуживания активно применяются во многих областях экономики (производстве, технике, военной области и др.) и предназначены для выполнения различных однотипных задач» [27]. С помощью аппарата теории массового обслуживания можно описать работу большого числа процессов в реальном мире, например, работу автопилота, современных систем хранения данных, а также функционирования современных телекоммуникационных систем [28].

СМО подразделяются на следующие виды: «СМО с потерями (отказами), СМО с ожиданием, СМО с ограниченной длиной очереди, СМО с ограниченным временем ожидания. СМО подразделяются по числу каналов или приборов системы и делятся на одноканальные и многоканальные» [30]. В качестве модели СППД будем использовать одноканальную систему массового обслуживания. Одноканальная система массового обслуживания с интенсивностью обслуживания λ и простейшим пуассоновским потоком заявок имеет неограниченное число мест в очереди (поток обслуживания имеет интенсивность μ). Время облуживания очередной заявки является случайной величиной с заданным законом распределения. Поступившие заявки обслуживаются в порядке очередности. Если очередная поступившая заявка застает канал занятым, то она покидает систему обслуживания. Следовательно, логичным является представления процесса передачи данных между СППД в виде одноканальной системы массового обслуживания. Состояния СМО имеют следующую интерпретацию:

S_0 – *канал свободен*;

S_1 – *канал занят* (*очереди нет*);

S_2 – *канал занят* (*одна заявка стоит в очереди*);

S_k – *канал занят* ($k-1$ *заявка стоит в очереди*);

S_{m+1} – *канал занят* (*m заявок стоит в очереди*).

Определим основные характеристики выбранного типа СМО с ограниченной длиной очереди, равной m [25]:

- «вероятность отказа в обслуживании пакета» $P_{ОТК} = P_{m+1} = \frac{p^{m+1}(1-p)}{1-p^{m+2}}$;
- «относительная пропускная способность системы» $q = 1 - P_{ОТК.}$;

- «абсолютная пропускная способность» $A = q\lambda$;
- «среднее число пакетов, находящихся в очереди» $M[r] = \frac{p^2\left[1-p^m(m+1-mp\right]}{(1-p^{m+2})(1-p)}$;
- «среднее число пакетов, находящееся под обслуживанием» $M[r] = 0 \cdot P_0 + \lambda(1-P_0) = \frac{p-p^{\lambda+2}}{1-p^{m-2}}$;
- «среднее число пакетов, находящихся в системе» $M[r] = M[r] + M[n]$;
- «среднее время пребывания пакета в очереди»: $T_{сист.} = \frac{1}{p\mu}M[r] = \frac{M[r]}{\lambda}$.

Важными показателями для их моделирования являются показатели, характеризующие качество и условия работы исследуемого объекта этой системы. Использование аппарата системы массового обслуживания для решения поставленных задач обусловлено следующим:

1. Использование СМО позволяет с применением формулы Литтла [25] оценить среднее время пребывания пакета данных в системе контроля и сделать предварительные оценки среднего числа пакетов данных, принятых к дополнительной обработке. Эти формулы применимы для любой СМО с любым характером потока данных и любой дисциплиной очереди.
2. Использование СМО как хорошо изученной имитационной модели позволяет задавать характеристики систем генерации запросов.
3. Использование СМО позволяет осуществить вычисление оценок для пропускной способности современных каналов передачи данных.

Установим адекватность компонентов между параметрами модели СМО и СППД: требование будет интерпретироваться, как пакет данных, который несет данные о телеметрии и который требуется отправить по незащищенному каналу передачи данных. В качестве источника выступает передающее устройство. Каналом является дискретный канал передачи данных. Очередь сообщений – последовательность пакетов данных. Очередь заявок рассматривается как последовательность пакетов данных. Под операцией кодирования интерпретируется точечный процесс (процесс, соответствующий последовательности случайных величин, в котором значения времени описывает случайная величина, порожденная моментами поступления пакетов данных для обслуживания).

Продолжительность обслуживания заявок рассматривается как моменты времени, связанные с поступлениями пакетов, определяемым своим

компенсатором (процесс, обладающий свойством предсказуемости и возможностью устанавливать причины нарушения целостности). «Такое семимартингальное (траекторное) описание СМО (в терминах считающих процессов и их компенсаторов) позволяет легко переходить от математической модели к итерационным формулам, по которым проводится имитационное моделирование, а сложность математической и компьютерной модели практически не растет с ростом числа каналов в СМО» [18].

Применение точечных процессов позволяет фиксировать факт временной задержки пакета в реальном канале передачи данных, что идентифицируется системой, как возможный признак нарушения целостности пакета данных. Для своевременного обнаружения таких пакетов используются соответствующие интенсивности поступления пакетов данных, которые позволяют эффективно обнаруживать в реальном канале пакеты данных с признаками нарушения целостности.

В процессе анализа известных средств обнаружения признаков нарушения целостности данных, разработанных на основе аппарата ТМО, были выявлены следующие недостатки:

1. Не регламентировано время поступления пакетов данных в систему обработки данных;
2. Отсутствует система контроля за поступлением пакетов данных с признаками нарушения целостности, следовательно, идентификация таких пакетов весьма затруднительна;
3. Не учитывается влияние внешних факторов среды передачи данных, из-за воздействия которых, происходит искажение содержимого передаваемого пакета данных.

Для обеспечения бесперебойной работы СППД идеально подходят навигационные комплексы наземных подвижных объектов, которые способны определять текущие координаты подвижного объекта с точностью до единиц метров [31]. Одним из недостатков разработанной в [2] модели автономной системы контроля целостности данных является то, что она не учитывает интенсивный рост единичных аддитивных ошибок различной кратности, а средства контроля описаны в виде некоторого «черного ящика», в результате чего достаточно сложно сделать вывод об эффективности их применения в реальной аппаратуре СППД.

Перейдем к построению подсистемы обнаружения нарушений целостности данных на основе аппарата ТМО с использованием индикаторных функций и их

компенсаторов на основе вероятностного подхода в семимартингальном описании, лишенной выявленных выше недостатков. Общую схему функционирования подсистемы обнаружения признаков несанкционированного доступа можно представить в следующем виде (рисунок 2.11).

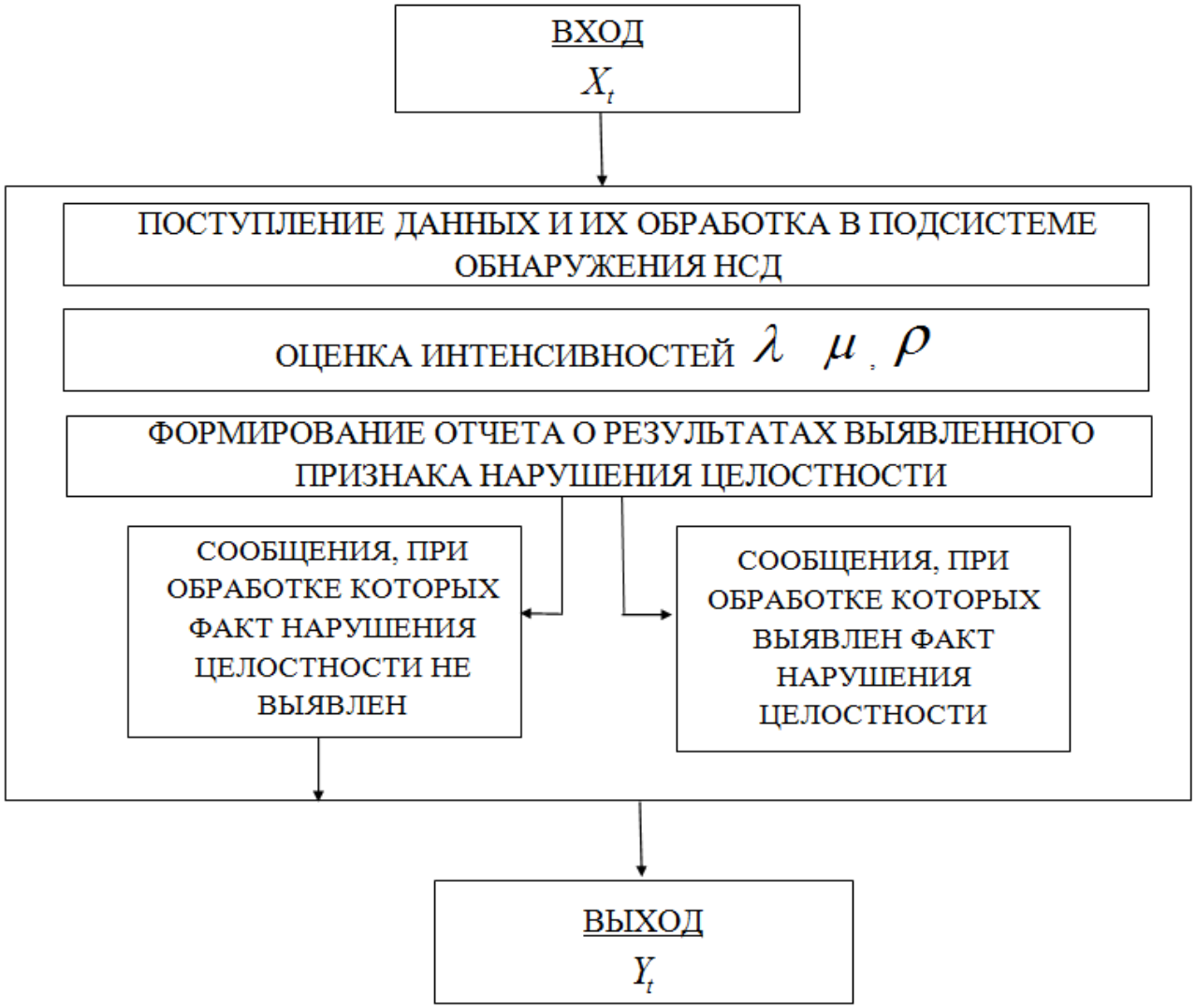

Рисунок 2.11 Схема подсистемы обнаружения признаков несанкционированного доступа к СППД

При поступлении данных в подсистему обнаружения признаков несанкционированного доступа осуществляется анализ (оценка) интенсивностей поступления и его последующая обработка, а также вычисление значений этих интенсивностей для установления фактов отклонения от установленных значений. При наличии временной задержки при поступлении данных или одного из признаков нарушения их целостности, представленных на рисунке 2.4, данные не ретранслируется и отправляется в следующую подсистему, в которой

осуществляется их дополнительная обработка, обнаружение места искажения и непосредственное исправление обнаруженной ошибки. В разрабатываемой математической модели на основе описания, применяемого в системах массового обслуживания (СМО), абстрактному понятию «заявка» из теории массового обслуживания (ТМО) на практике в СППД соответствует пакет данных (представленный в виде структурированного массива бит), который, на физическом уровне представляет собой электромагнитный сигнал.

Уравнение системы массового обслуживания представим в следующем виде [20]:

$$Q_t = Q_0 + A_t + R_t - D_t, \tag{2.1}$$

где « Q_t – число пакетов данных в момент времени $t \in [0,T]$, $Q_0 = Q_{t=0}$ – число пакетов данных в момент времени $t = 0$ ($Q_0 \in N = \{0,1,2,...\}$), A_t – число пакетов данных поступивших за время t, R_t – число пакетов данных поступивших в очередь за время t, D_t – число пакетов данных обслуженных за время t» [20]

Точечные процессы A_t, D_t, R_t $(t \geq 0)$ определяются своими компенсаторами (предсказуемый возрастающий случайный процесс). В результате имеют место следующие соотношения [20]:

$$A_t = \lambda \cdot t, \tag{2.2}$$

$$D_t = \int_0^t \mu \cdot Q_s \, ds, \tag{2.3}$$

$$R_t = \int_0^t \rho \cdot Q_s \, ds, \tag{2.4}$$

где λ – интенсивность поступающих в систему пакетов данных, μ – интенсивность обслуживаемых пакетов данных, ρ – интенсивность находящихся в очереди и ожидающих обслуживания пакетов данных, Q_s – число пакетов данных в момент времени $t = s$,. $\lambda, \mu, \rho > 0$

Перейдем к оцениванию параметров модели в семимартингальном описании, воспользовавшись следующими соотношениями [20]:

$$\begin{cases} (A_t)_{0 \leq s \leq t}, \\ \left(X_t^0\right)_{0 \leq s \leq t}, \\ \left(X_t^m\right)_{0 \leq s \leq t}, \end{cases} \tag{2.5}$$

$$X_t^0 = \int_0^t I\left(Q_s = 0\right) ds, \tag{2.6}$$

$$X_t^m = \int_0^t I\left(Q_s = m\right) ds,\ m \geq 1, \tag{2.7}$$

где $I\left(Q_s = m\right)$ – индикаторная функция (функция, определенная на множестве, которая указывает на принадлежность элемента множеству), которая представима в виде $I\left(Q_t = 0\right) = I\left(Q_s = 0\right) - \int_0^t I\left(Q_s = 0\right) dA_s + \int_0^t I\left(Q_s = 1\right) dD_s$.

Далее осуществим расчет оценки интенсивности поступающих в систему пакетов данных. Несмещенной состоятельной оценкой [32] для интенсивности поступающих в систему пакетов данных λ является:

$$\lambda_t = \frac{A_t}{t}. \tag{2.8}$$

Действительно,

$$E \cdot \lambda_t = E \cdot \frac{A_t}{t} = \frac{\lambda \cdot t}{t} = \lambda. \tag{2.9}$$

Выражение (2.8) позволяет оценить интенсивность поступающих в систему пакетов данных, а выражение (2.9) позволяет сделать вывод, что данная оценка является несмещенной и состоятельной. Воспользовавшись неравенством Чебышева, которое утверждает, что случайная величина в основном принимает значения, близкие к своему среднему, получим следующее:

$$\forall \varepsilon > 0 \quad P\left\{\left|\frac{A_t}{t} - \lambda\right| > \varepsilon\right\} < \frac{D\left(A_t/t\right)}{\varepsilon^2}, \tag{2.10}$$

где $D(A_t/t)$ – дисперсия, для которой справедлива оценка $\lambda \cdot \frac{t}{t^2 \cdot \varepsilon^2} \underset{t \to \infty}{\to} 0 \ \ \forall \varepsilon > 0$.

Для получения оценки интенсивности обслуженных в системе пакетов данных μ_t и оценки, находящихся в очереди и ожидающих обслуживания пакетов данных ρ_t, рассмотрим разложение индикаторной функции $I\left(Q_t = k\right)$, $k \geq 0$. Индикаторная функция $I\left(Q_t = k\right)$, $k \geq 0$ представима в виде [20]:

$$I\left(Q_t = k\right) = I\left(Q_0 = 0\right)k + \lambda \int_0^t I\left(Q_s = k-1\right) ds + \rho\left(k-1\right) \int_0^t I\left(Q_s = k-1\right) ds -$$

$$-\left(\lambda - \mu \cdot k + \rho \cdot k\right) \int_0^t I\left(Q_s = k\right) ds + \mu\left(k+1\right) \int_0^t I\left(Q_s = k+1\right) ds.$$

Для выражения параметров λ, μ, ρ, произведем расчет компенсаторов найденных индикаторов. Для индикаторной функции $I(Q_s=0)$ компенсатор определяется выражением [20]:

$$I\left(Q_t=0\right)=I\left(Q_0=0\right)-\lambda\int_0^t I\left(Q_s=0\right)ds+\mu\int_0^t I\left(Q_s=1\right)ds. \qquad (2.11)$$

Для индикаторной функции $I(Q_s=k)$ компенсатор определяется выражением [20]:

$$\begin{aligned} I\left(Q_t=k\right)=I\left(Q_0=0\right)k+\lambda\int_0^t I\left(Q_s=k-1\right)ds+\rho\left(k-1\right)\int_0^t I\left(Q_s=k-1\right)ds- \\ -\left(\lambda-\mu\cdot k+\rho\cdot k\right)\int_0^t I\left(Q_s=k\right)ds+\mu\left(k+1\right)\int_0^t I\left(Q_s=k+1\right)ds. \end{aligned} \qquad (2.12)$$

Обозначим локальные времена [20]

$$\lambda\int_0^t I\left(Q_s=0\right)ds=X_t^k,\quad k=0,1,2,\ldots\ . \qquad (2.13)$$

Получим систему:

$$\begin{cases} -\lambda\cdot a^{(0)}+\mu\cdot a^{(1)}=0, \\ \lambda\cdot a^{(0)}-\left(\lambda+\mu+\rho\right)\cdot a^{(1)}+2\cdot\mu\cdot a^{(2)}=0, \\ \left(\lambda+\rho\right)\cdot a^{(1)}-\left(\lambda+2\cdot\mu+2\cdot\rho\right)\cdot a^{(2)}+3\cdot\mu\cdot a^{(3)}=0, \\ \left(\lambda+2\cdot\rho\right)\cdot a^{(2)}-\left(\lambda+3\cdot\mu+3\cdot\rho\right)\cdot a^{(3)}+4\cdot\mu\cdot a^{(4)}=0. \end{cases} \qquad (2.14)$$

Преобразуем систему (3.20) к следующему виду:

$$\begin{cases} a^{(1)}=\dfrac{\lambda}{\mu}\cdot a^{(0)}, \\ a^{(2)}=\dfrac{\lambda+\rho}{2\cdot\mu}\cdot a^{(1)}, \\ a^{(3)}=\dfrac{\lambda+2\cdot\rho}{3\cdot\mu}\cdot a^{(2)}, \\ a^{(4)}=\dfrac{\lambda+3\cdot\rho}{4\cdot\mu}\cdot a^{(3)}. \end{cases} \qquad (2.15)$$

В результате анализа полученной системы (2.15) следует вывод, что каждый последующий аппроксимирующий коэффициент $a^{(k)}$ находится рекуррентно. Получим выражение:

$$a^{(k)}=\frac{(k-1)!\cdot\lambda\cdot a^{(0)}\rho^{(k-1)}\prod_{i=1}^{k-1}\left(1+\dfrac{\lambda}{i\cdot\rho}\right)}{k!\cdot\mu^{(k)}}=\frac{\lambda\cdot a^{(0)}\rho^{(k-1)}\prod_{i=1}^{k-1}\left(1+\dfrac{\lambda}{i\cdot\rho}\right)}{k\cdot\mu^{(k)}}. \qquad (2.16)$$

Заметим, что разность

$$1-a^{(0)}=\sum_{k=1}^{\infty}a^{(k)}=\sum_{k=1}^{\infty}\frac{\lambda\cdot a^{(0)}\rho^{(k-1)}\prod_{i=1}^{k-1}\left(1+\frac{\lambda}{i\cdot\rho}\right)}{k\cdot\mu^{(k)}}. \quad (2.17)$$

Применив метод аппроксимации к выражению (2.17) получим выражение:

$$\sum_{k=1}^{\infty}\frac{\lambda\cdot a^{(0)}\rho^{(k-1)}\prod_{i=1}^{k-1}\left(1+\frac{\lambda}{i\cdot\rho}\right)}{k\cdot\mu^{(k)}}=c(\lambda,\mu,\rho), \quad (2.18)$$

где $c(\lambda,\mu,\rho)=1+\frac{1}{2}\cdot\left(\frac{\rho}{\mu}\right)\cdot\left(1+\frac{\lambda}{\mu}\right)+\frac{1}{3}\cdot\left(\frac{\rho}{\mu}\right)^{2}\cdot\left(1+\frac{\lambda}{\rho}\right)\cdot\left(1+\frac{\lambda}{2\cdot\rho}\right)+\ldots$.

Из выражения (2.18) выразим $a^{(0)}$, получим:

$$a^{(0)}=\left(1+\frac{\lambda}{\mu}\cdot c(\lambda,\mu,\rho)\right)^{-1}. \quad (2.19)$$

В нулевом приближении $a^{(0)}=\left(1+\frac{\lambda}{\mu}\right)^{-1}$. Выразим из уравнения (2.19) оценку параметра интенсивности обслуживания поступивших в систему пакетов данных μ_t :

$$\mu_t=\frac{\lambda\cdot a^{(0)}}{1-a^{(0)}}.$$

В результате последовательно произведенных математических операций построена оценка интенсивности принятых к обработке пакетов данных, которая на практике позволяет определить их исходное количество.

«Воспользовавшись процедурами аппроксимации, примем $\frac{1}{2}\cdot\left(\frac{\rho}{\mu}\right)\cdot\left(1+\frac{\lambda}{\rho}\right)\sim\frac{\rho}{2\cdot\mu}$ и из приближения $a^{(0)}=\left(1+\frac{\lambda}{\mu}\cdot\left(1+\frac{\rho}{2\cdot\mu}\right)\right)^{-1}$ выразим оценку, поступивших в очередь и ожидающих обслуживания пакетов данных ρ_t » [20]:

$$\rho_t=\frac{2\cdot\mu^{(2)}}{\lambda\cdot a^{(0)}}\cdot\left(1-a^{(0)}-\frac{\lambda}{\mu}\cdot a^{(0)}\right). \quad (2.20)$$

Построенные оценки линейно зависимы, следовательно, оценку ρ_t выразим через $a^{(m)}$, $m>1$. Отметим, что при $m=1$ оценку интенсивности обслуживания поступивших в систему пакетов данных с использованием метода аппроксимации можно выразить по формуле:

$$\mu_t = \frac{\lambda \cdot a^{(0)}}{a^{(1)}}. \quad (2.21)$$

При $m = 2$ оценку интенсивности, находящихся в очереди и ожидающих обслуживания данных ρ_t, выразим следующим образом:

$$\rho_t = \frac{2 \cdot \mu^{(2)} \cdot a^{(2)}}{\lambda \cdot a^{(0)}} - \lambda. \quad (2.22)$$

Равносильно:

$$\rho_t = \frac{2 \cdot \lambda \cdot a^{(0)} \cdot a^{(2)}}{\left(1 - a^{(0)}\right)^2} - \lambda. \quad (2.23)$$

Далее найдем оценку ρ_t при $m > 2$.

Получим:

$$a^{(m)} = \frac{\lambda + (m-1) \cdot \rho}{m \cdot \mu} \cdot a^{(m-1)}. \quad (2.24)$$

Воспользовавшись методом аппроксимации, будем считать, что

$$a^{(m)} \sim \frac{(m-1) \cdot \rho}{m \cdot \mu} \cdot a^{(m-1)}. \quad (2.25)$$

В результате получено следующее приближение:

$$a^{(m)} = \frac{(m-1)! \cdot \rho^{(m-1)} \cdot \lambda \cdot a^{(0)}}{m! \cdot \mu^{(m)}} = \frac{\rho^{(m-1)} \cdot \lambda \cdot a^{(0)}}{m! \cdot \mu^{(m)}}, \quad (2.26)$$

из которого выразим оценку параметра ρ_t при $m > 2$. Получим выражение:

$$\rho_t = \left(\frac{m \cdot \mu^{(m)} \cdot a^{(m)}}{\lambda \cdot a^{(0)}} \right)^{\frac{1}{m-1}}. \quad (2.27)$$

Итогом выше приведенных операций является получение оценок следующих параметров: интенсивности поступивших в систему пакетов данных, интенсивности принятых к обработке пакетов данных и интенсивности, находящихся в очереди и ожидающих обработки пакетов данных (выражение 2.28).

$$\begin{cases} \lambda_t = \dfrac{A_t}{t}, \\ \mu_t = \dfrac{\lambda \cdot a^{(0)}}{1 - a^{(0)}}, \\ \rho_t = \left(\dfrac{m \cdot \lambda^{(m)} \cdot a^{(m)}}{\lambda \cdot a^{(0)}} \right)^{\frac{1}{m-1}}, \end{cases} \tag{2.28}$$

где

$$a^m = \frac{1}{t} \cdot \lim_{t \to \infty} X_t^m = \frac{1}{t} \cdot \lim_{t \to \infty} \int_0^t I\left(Q_s = m\right) ds, \quad m \geq 1. \tag{2.29}$$

Система выражений (2.28) позволяет определять значения интенсивностей поступивших пакетов данных, интенсивностей принятых к обработке пакетов данных, и интенсивностей, находящихся в очереди и ожидающих обработки пакетов данных, для установления факта несанкционированного доступа. Учитывая, что для каждого отдельно взятого типа СППД устанавливаются свои допустимые значения интенсивностей поступления и обработки пакетов данных, а также то, что в большинстве случаев такая информация имеет закрытый характер, в диссертационной работе за основу взяты допустимые значения интенсивностей СППД «Ямал 202» (Газпром космические системы), представленные в открытом источнике [33]. Алгоритм функционирования построенной подсистемы обнаружения признаков несанкционированного доступа и нарушений целостности на основе аппарата ТМО представлен на рисунке 2.12.

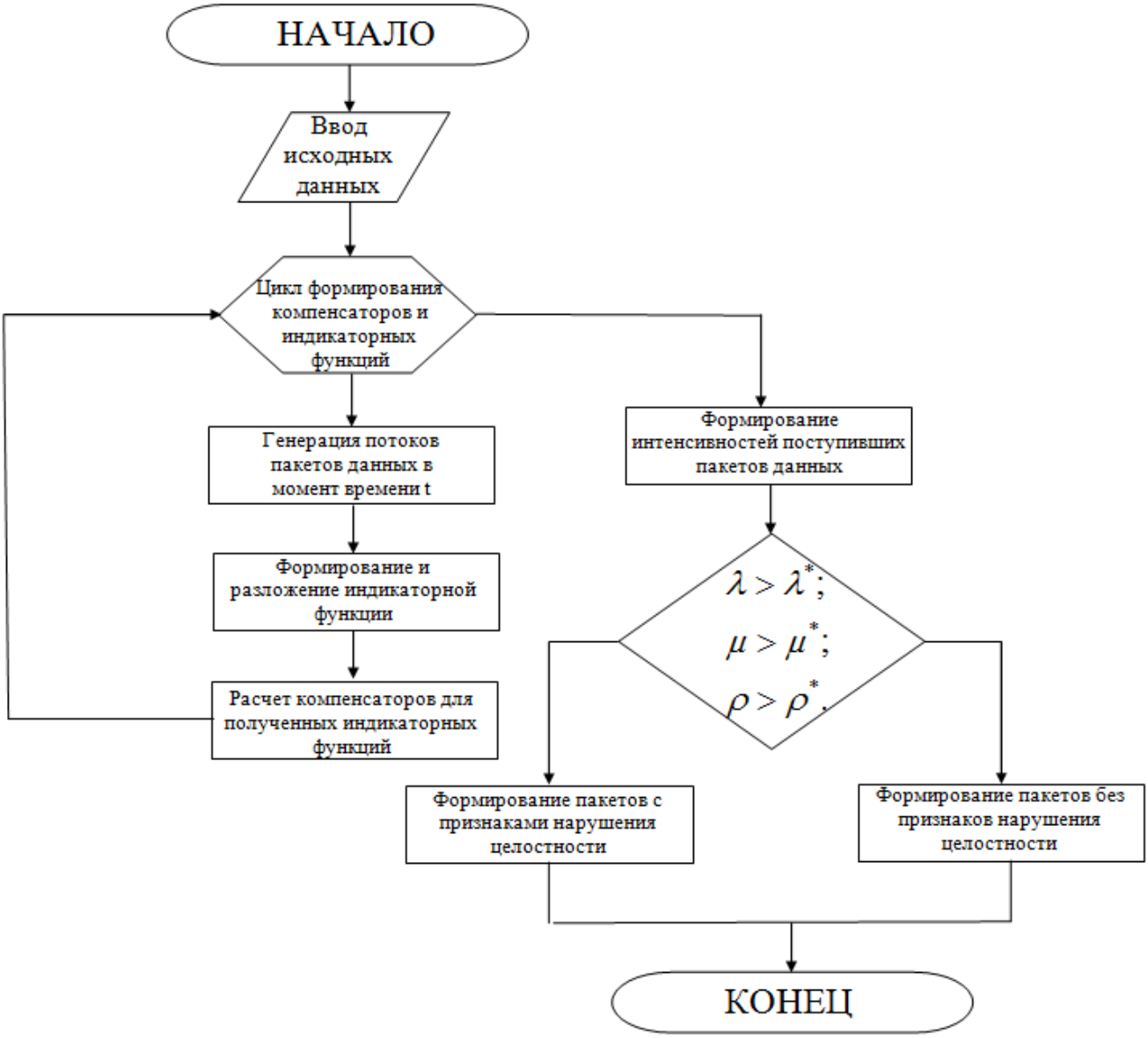

Рисунок 2.12 Алгоритм функционирования разработанной подсистемы обнаружения признаков несанкционированного доступа

Разработанный алгоритм описывает основные этапы функционирования построенной подсистемы обнаружения признаков несанкционированного доступа на основе аппарата ТМО. На начальном этапе осуществляется ввод исходных данных (задается количество пакетов данных, поступающих в приемное устройство СППД, максимальная длина очереди на обслуживание и т.д.). На следующем этапе происходит формирование индикаторных функций и их компенсаторов, необходимых для расчета оценок интенсивностей, поступивших и принятых к обработке данных, путем их непосредственного вычисления при помощи соответствующего программного приложения. На завершающих этапах работы алгоритма формируются оценки интенсивностей поступивших данных,

интенсивностей принятых к обработке данных и интенсивностей, находящихся в очереди и ожидающих обработки данных, осуществляется сравнение полученных значений с заранее установленными допустимыми значениями интенсивностей (λ^*, μ^*, ρ^*) и статистическая обработка полученных результатов (формирование потоков пакетов данных с признаками нарушений целостности и пакетов данных, при обработке которых нарушений целостности не выявлено).

При $m=1$ оценку параметра μ_t также можно выразить по формуле [20]:

$$\mu_t = \frac{\lambda \cdot a^{(0)}}{a^{(1)}}. \tag{2.30}$$

Оценку параметра ρ_t в данном случае можно выразить по формуле

$$\rho_t = \frac{2 \cdot \mu^{(2)}}{\lambda \cdot a^{(0)}} \cdot \left(1 - a^{(0)} - \frac{\lambda}{\mu} \cdot a^{(0)}\right), \tag{2.31}$$

а оценку этого параметра при $m=1$ выразить по другой формуле [20]:

$$\rho_t = \frac{2 \cdot \lambda \cdot a^{(0)} \cdot a^{(2)}}{\left(1 - a^{(0)}\right)^2} - \lambda. \tag{2.32}$$

Предложенная система оценивания, на основе разработанного алгоритма позволяет проводить моделирование и вычислять значения интенсивностей поступивших пакетов данных, интенсивностей принятых к обработке пакетов данных, а также интенсивностей, находящихся в очереди и ожидающих обслуживания пакетов данных. Реализация в реальном времени установления факта несанкционированного доступа предполагает, что в состав СППД будет входить подсистема анализа задержек поступления пакетов данных, причем строго соблюдаются требования к формату пакета данных в соответствии с Госстандартом телеметрии пакетной передачи информации ГОСТ Р 56096 -2014 [26].

Для анализа задержек предусмотрены следующие параметры:

– номер пакета для образования очереди;

– параметр идентификации пакета (проверки его присутствия в очереди);

– длина пакета, которая допускается фиксированной и переменной для оценки загруженности канала передачи данных;

– код времени для привязки к шкале времени функционирования СППД, а также счетчик пакета.

При создании программного приложения допускается введение в заголовок пакета идентификатора прикладного процесса с указанием веса пакета и веса последовательности пакетов. Таким образом, можно заранее вводить в пакеты всю необходимую информацию об их состоянии во время присутствия в очереди, которую можно использовать при получении и предварительной обработке для выявления задержки, то есть идентификации признака нарушения целостности.

Граф состояний подсистемы обнаружения признаков несанкционированного доступа на основе аппарата ТМО представлен на рисунке 2.13.

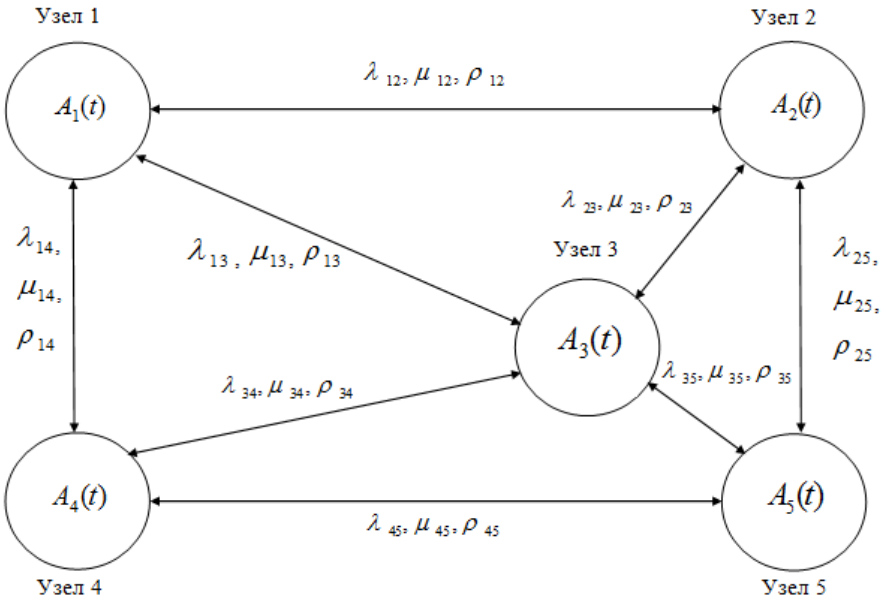

Рисунок 2.13 Граф состояний подсистемы обнаружения признаков несанкционированного доступа к СППД

Роль параметров для узлов подсистемы обнаружения признаков несанкционированного доступа к СППД выполняют $A_i(t)$ – точечные процессы. В качестве переменных выбраны $\lambda_{ij}, \mu_{ij}, \rho_{ij}$, которые являются, соответственно, интенсивностями поступивших в подсистему пакетов данных, интенсивностями принятых к «обработке» пакетов данных, интенсивностями находящихся в очереди и ожидающих обработки пакетов данных. Обнаружение нарушений целостности в пакетах данных происходит за счет контроля интенсивностей поступления данных.

Таким образом, средство реализации подсистемы обнаружения признаков несанкционированного доступа представляет собой программное приложение, которое вводится в состав приемной аппаратуры СППД. Построенный на рисунке 2.13 граф является основой для разработанного алгоритма функционирования модели подсистемы обнаружения признаков несанкционированного доступа и его программной реализации путем вычисления задержек по формулам, изложенным выше. На рисунках 2.14, 2.15, 2.16 показаны зависимости оценок λ_t , μ_t и ρ_t от модельного времени t (время моделирования измеряется в минутах) при фиксированном значении компенсатора процесса $I\left(Q_t = k\right)$.

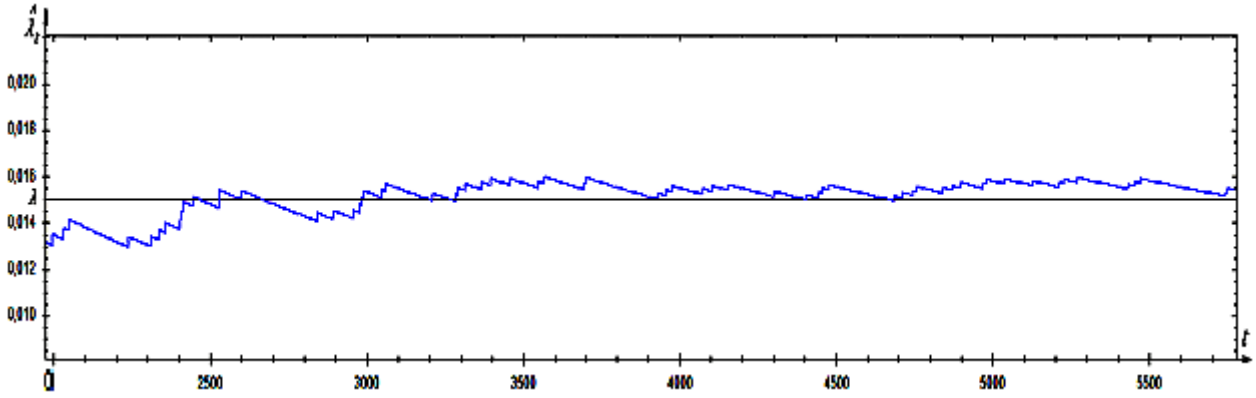

Рисунок 2.14 График оценки интенсивности поступивших пакетов данных в СППД λ_t

На данном рисунке представлен график оценки интенсивности поступивших в систему пакетов данных. Из анализа графика следует вывод, что при помощи выражений (2.2) – (2.8) произведена оценка интенсивности поступивших в систему пакетов при фиксированном значении компенсатора $I\left(Q_t = k\right)$ и модельном времени t.

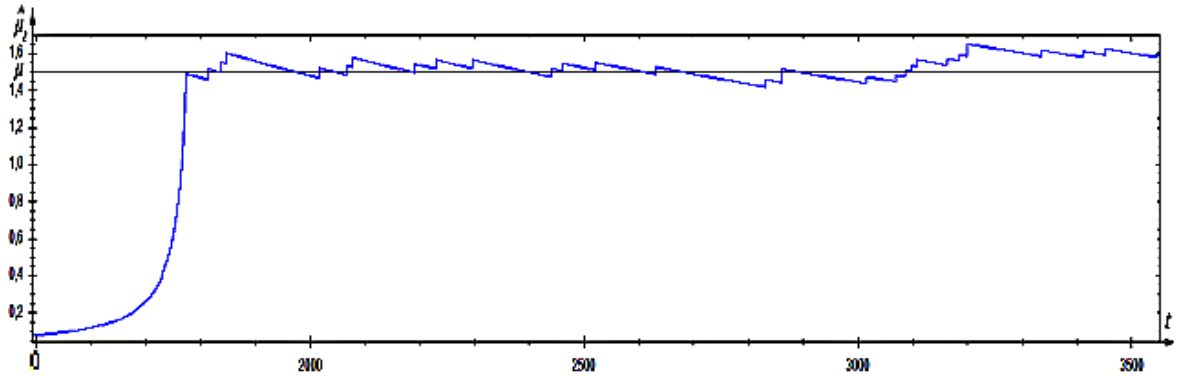

Рисунок 2.15 График оценки интенсивности принятых к обработке пакетов данных μ_t

На рисунке 2.15 представлен график оценки интенсивности принятых к обработке пакетов данных. Из анализа графика следует вывод, что с использованием выражений (2.10) – (2.16) и выражение (2.18), получена оценка интенсивности принятых к обработке пакетов при фиксированном значении компенсатора $I\left(Q_t = k\right)$ и модельном времени t. Использование формул (2.10) – (2.18), позволяет установить тот факт, что обслуживание пакетов происходит без существенных отклонений в течение заданного времени моделирования.

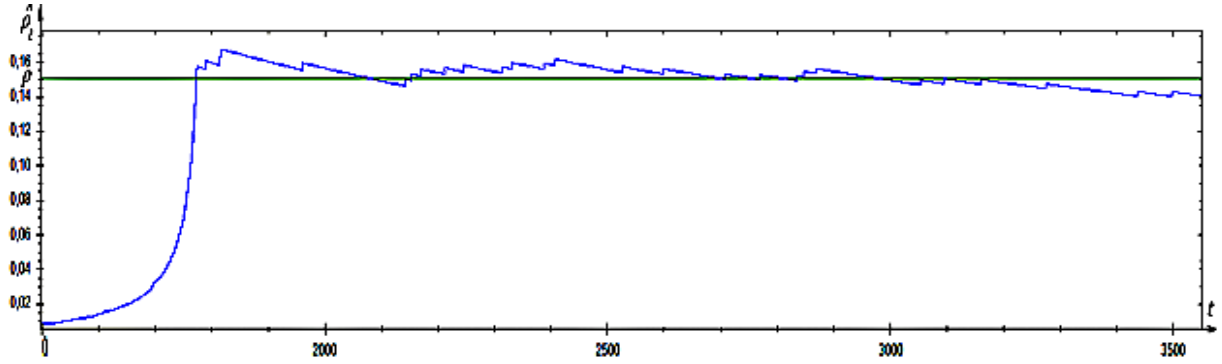

Рисунок 2.16 График оценки интенсивности, находящихся в очереди и ожидающих обслуживания пакетов данных ρ_t

На рисунке 2.16 представлен график оценки интенсивности, находящихся в очереди и ожидающих обслуживания пакетов данных. Из графика следует вывод, что использование формул (2.25) – (2.32) позволяет проводить моделирование для оценки интенсивности, находящихся в очереди и ожидающих обслуживания пакетов данных, при фиксированном значении компенсатора и модельном времени t.

Разработанная подсистема обнаружения признаков несанкционированного доступа на основе аппарата ТМО с использованием индикаторных функций и их компенсаторов в семимартингальном описании позволяет эффективно идентифицировать пакеты данных с признаками нарушений целостности. В связи с развитием СППД, сложностью устройства реальной аппаратуры СППД, постоянным воздействием на нее дестабилизирующих факторов среды передачи информации становиться актуальным внедрение дополнительных средств обеспечения целостности данных. Из-за дороговизны оборудования СППД проведение практических экспериментов зачастую не предоставляется возможным, следовательно, апробация полученных результатов осуществима исключительно с помощью средств имитационного моделирования.

2.4 Применение метода градиентного спуска для вычисления интенсивностей поступивших пакетов данных, интенсивностей принятых к обработке пакетов данных, интенсивностей, находящихся в очереди и ожидающих обработки пакетов данных

С учетом влияния дестабилизирующих факторов среды передачи информации для вычисления точных значений интенсивностей поступивших пакетов данных, интенсивностей принятых к обработке пакетов данных, интенсивностей, находящихся в очереди и ожидающих обработки пакетов данных, возникает острая необходимость в применении численных методов быстрой обработки данных при поступлении большой очереди потока пакетов. В реальном масштабе времени при приеме и обработке информации в СППД, как показывают исследования [34, 35], имеет место значительная нехватка временных ресурсов для проведения различных вычислительных операций.

Суть разработанного метода состоит в применение табличных методов быстрой обработки пакетов данных в реальном масштабе времени при поступлении большой очереди потока пакетов. Этот метод позволяет производить вычисление значений интенсивностей поступивших пакетов данных, интенсивностей принятых к обработке пакетов данных, интенсивностей, находящихся в очереди и ожидающих обработки пакетов данных с использованием готовых таблиц, построенных при помощи пакета прикладных программ MATLAB.

Рассчитать значения индикаторных функций, определяемых выражениями (2.11) - (2.12), в явном виде достаточно проблематично, в виду высокой сложности необходимых расчетов и значительных временных затрат. Другими словами, возникает необходимость в разработке процедуры, с помощью которой можно произвести быстрый расчет значений индикаторных функций и их компенсаторов, а также значений соответствующих интенсивностей для выявления факта несанкционированного доступа в СППД.

За основу используемого метода возьмем наиболее эффективный с точки зрения производимых вспомогательных вычислительных операций метод градиентного спуска. Для оценки возможности его использования в работе проведем расчёты, по которым можно оценить эффективность применения этого метода в реальных условиях. Рассмотрим целевую функцию, которая имеет следующий вид: $F(\vec{x}) : \mathrm{X} \to \mathbb{R}$. Задача оптимизации определена следующим образом: $F(\vec{x}) \to \min\limits_{x \in \mathrm{X}}$ [36]. «Основная идея метода заключается в том, чтобы

идти в направлении наискорейшего спуска, это направление задается антиградиентом – ∇F » [36].

$$\vec{x}^{|j+1|} = \vec{x}^{|j|} - \lambda^{|j|}\nabla F(\vec{x}^{|j|}),$$

где $\lambda^{|j|}$ задает скорость градиентного спуска.

Для поиска минимума определим параметр $\lambda^{|j|}$, который задается выражением:

$$\lambda^{|j|} = \arg\min_{\lambda} F(\vec{x}^{|j+1|}) = \arg\min_{\lambda} F(\vec{x}^{|j|} - \lambda\nabla F(\vec{x}^{|j|})).$$

Алгоритм работы метода локальной оптимизации представлен ниже:

1. Задают начальное приближение и точность расчета $\vec{x}^{|0|}, \varepsilon$;
2. Рассчитывают $\vec{x}^{|j+1|} = \vec{x}^{|j|} - \lambda^{|j|}\nabla F(\vec{x}^{|j|}),$ *где* $\lambda^{|j|} = \arg\min_{\lambda} F(\vec{x}^{|j|} - \lambda\nabla F(\vec{x}^{|j|}))$;
3. Проверяют условия остановки:

если $\left|\vec{x}^{|j+1|} - \vec{x}^{|j|}\right| \geq \varepsilon \left|F(\vec{x}^{|j+1|}) - F(\vec{x}^{|j|})\right| > \varepsilon$ *или* $\left\|\nabla F(\vec{x}^{|j+1|}))\right\| > \varepsilon$ (выбирают одно из условий), иначе $\vec{x}^{|j|} = \vec{x}^{|j+1|}$.

В качестве примера рассмотрим выражение (2.11), которое определяет индикаторную функцию для вычисления оценки интенсивности поступления потоков пакетов данных в подсистему обнаружения признаков несанкционированного доступа.

Будем искать решение в точках: $s_i = 0.00; 0.02; 0.04; 0.06; 0.08; 0.10.$

При построении численного метода необходимо уточнить среднее время задержки пакета (в очереди на обслуживание). Используем обобщенную формулу трапеций для замены интегрального выражения квадратурной суммой [37].

Пользуясь результатами, изложенными в [38], для решения стохастических интегральных выражений, получим значения шага $h = 0.02.$

Определим среднее время задержки на участке формулой [39]:

$$T = \frac{\rho\bar{t}}{2(1-\rho)}\left(1 - \frac{\sigma^2}{\bar{t}^2}\right) + \bar{t},$$

где $\rho = \alpha\bar{t};$

α - интенсивность поступления пакета за время $\bar{t}$;

$\bar{t}$ - среднее время обслуживания пакета;

σ^2 - дисперсия времени обслуживания.

Далее определим уровень доверительной вероятности и ширину доверительного интервала. Путем проведения вычислений установим, что

оптимальный уровень доверительной вероятности составляет $0,9(\alpha-1)$, а ширина доверительного интервала 3,86 (пакетов/секунду). Обозначим $K_{i,j} = I(Q_s = 0)$ и $f_i = I(Q_s = 0)$.

Получим следующие выражения:

$$I_1^{(6)} = f_1 = 1.0000;$$

$$I_2^{(6)} = (1-\frac{h}{2}K_{22})^{-1}(f_2 + \frac{h}{2}K_{21}I_1^{(6)}) = 1.00001;$$

$$I_3^{(6)} = (1-\frac{h}{2}K_{33})^{-1}(f_3 + \frac{h}{2}K_{31}I_1^{(6)} + hK_{32}I_2^{(6)}) = 0.999405;$$

$$I_4^{(6)} = (1-\frac{h}{2}K_{44})^{-1}(f_4 + \frac{h}{2}K_{41}I_1^{(6)} + h(K_{42}I_2^{(6)} + K_{43}I_3^{(6)}) = 1.00000002;$$

$$I_5^{(6)} = (1-\frac{h}{2}K_{55})^{-1}(f_5 + \frac{h}{2}K_{51}I_1^{(6)} + h(K_{52}I_2^{(6)} + K_{53}I_3^{(6)} + K_{53}I_3^{(6)} + K_{54}I_3^{(6)}) = 0.99999991;$$

$$I_6^{(6)} = (1-\frac{h}{2}K_{66})^{-1}(f_6 + \frac{h}{2}K_{61}I_1^{(6)} + h(K_{62}I_2^{(6)} + K_{63}I_3^{(6)} + K_{64}I_3^{(6)} + K_{65}I_3^{(6)}) = 0.99999991.$$

Проведенные расчеты показали что использование метода градиентного спуска при его программной реализации дает существенный выигрыш по быстродействию вычислений значений интенсивностей поступивших пакетов данных, интенсивностей принятых к обработке пакетов данных и интенсивностей, находящихся в очереди и ожидающих обработки пакетов данных. Также при его применении можно построить готовые таблицы значений интенсивностей, с которыми сравниваются оценки уровня отклонения заданных значений интенсивностей и интенсивностей, полученных в реальных условиях.

В результате численного моделирования получена следующая таблица (рисунок 2.17).

Номер интервала	Начало интервала	Конец интервала	Количество попаданий в интервал	Вероятность попадания в интервал	Значение интенсивности λ
1	0,0001	0,003	28	0,0048	1,6
2	0,0003	0,006	8	0,0014	0,5
3	0,0006	0,009	6	0,0010	0,3
4	0,0009	0,0012	5	0,0009	0,3
5	0,0012	0,0015	23	0,0039	1,3
6	0,0015	0,0018	254	0,0433	14,4
7	0,0018	0,0021	191	0,3260	108,7
8	0,0021	0,0024	111	0,0189	6,3
9	0,0024	0,0027	0	0,0000	0,0
10	0,0027	0,0030	0	0,0000	0,0
11	0,0030	0,0033	1	0,0002	0,1
12	0,0033	0,0036	14	0,0024	0,8
13	0,0036	0,0039	34	0,0058	1,9
14	0,0039	0,0042	154	0,00247	8,2
15	0,0042	0,0045	4	0,00007	0,2
16	0,0045	0,0048	1	0,0002	0,1
17	0,0048	0,0051	0	0,0000	0,0
18	0,0051	0,0054	0	0,0000	0,0
19	0,0054	0,0057	0	0,0000	0,0
20	0,0057	0,0061	0	0,0000	0,1
21	0,0061	0,304	18	0,00391,6	1,3

Рисунок 2.17 Применение численного метода градиентного спуска для расчета значения интенсивностей поступления пакетов данных

При расчете значений интенсивностей с использованием разработанного численного метода установлено, что относительная ошибка результата составляет 7 процентов, что является существенным преимуществом перед известными численными методами (значения такой ошибки при применении известных численных методов составляет порядка 10-11%), применяемыми для решения интегральных стохастических уравнений. Использование построенных таблиц в реальных условиях позволяет сократить количество производимых вычислений в реальном масштабе времени для фиксации фактов несанкционированного доступа к СППД.

2.5 Выводы по второй главе

1. Выполнен анализ нарушений целостности данных при их передаче по дискретным каналам СППД. Полученная в результате анализа информация, позволила определить подход к построению подсистемы обнаружения признаков несанкционированного доступа за счет использования временного признакового

параметра – задержки поступления пакетов, нарушения порядка следования пакетов в очереди, влияния изменения веса пакета и самой очереди.

2. Разработан подход к обнаружению признаков несанкционированного доступа к СППД на основе аппарата теории массового обслуживания с использованием индикаторных функций и их компенсаторов. С помощью него можно определять факт нарушения целостности в передаваемых пакетах данных, оценивая значения интенсивностей поступивших пакетов данных, интенсивностей принятых к обработке пакетов данных и интенсивностей, находящихся в очереди и ожидающих обработки пакетов данных, и учета отклонений этих значений от интенсивностей, заданных протоколами телеметрии.

3. Построены математические модели оценки интенсивностей входных пакетов данных, поступивших для обработки в СППД, интенсивностей пакетов данных, находящихся в очереди и ожидающих обслуживания при фиксированном значении компенсатора $I\left(Q_t = k\right)$ и заданного модельного времени t, которые позволяют установить тот факт, что обслуживание (обработка) пакетов данных происходит без существенных отклонений в течение заданного времени моделирования.

4. Предложен вариант эффективного использования численного метода градиентного спуска для решения стохастических интегральных уравнений, применительно к индикаторным функциям и их компенсаторам для использования в подсистеме обнаружения признаков несанкционированного доступа в СППД. Отличительной особенностью этого метода является его использование для подготовки таблиц заранее вычисленных значений интенсивностей поступивших пакетов данных, интенсивностей принятых к обработке пакетов данных, интенсивностей, находящихся в очереди и ожидающих обработки пакетов данных, что позволяет существенно ускорить процесс обработки пакетов на этом отрезке времени.

ГЛАВА 3. РАЗРАБОТКА ПОДСИСТЕМЫ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ ДАННЫХ НА ОСНОВЕ КОДОВ С ПЕРЕМЕННЫМ ВЕСОМ

В третьей главе диссертации произведен сравнительный анализ используемых приемов и средств обнаружения и исправления ошибок в пакетах данных при передаче по СППД.

Рассмотрен подход к обнаружению ошибок на основе применения кодов с фиксированными весами. На практике использование таких кодов позволяет обнаружить и исправить любые одиночные ошибки и большинство многократных ошибок, сгруппированных в пачки.

3.1 Анализ моделей каналов передачи данных в системах обмена дискретной информацией

Часто рассматривают модели каналов передачи данных с переменными параметрами, что обусловлено их повсеместным применением на практике [40-43]. Достаточно редко на практике встречаются каналы с постоянными параметрами, поэтому в большинстве исследований рассматривают их абстрактные модели, которые отражают явления группирования пачек ошибок на выходе. Первой моделью канала передачи с переменными параметрами была модель Гильберта, предполагающая два состояния, в которых он может находиться. В первом состоянии – штатном, ошибки отсутствуют, а в неработоспособном состоянии – имеют место с вероятностью $P_{0Ш}$. Последовательности таких состояний представляют простую цепь Маркова с матрицей переходных вероятностей, определяемую выражением [40]:

$$P_{i.j} = \begin{Vmatrix} P_{00} & P_{01} \\ P_{10} & P_{11} \end{Vmatrix},$$

где P_{00} – вероятность пребывания в штатном состоянии; P_{01} – вероятность изменения состояния, P_{11} – вероятность пребывания в неработоспособном состоянии и P_{10} – вероятность перехода из штатного в неработоспособное состояние. При наличии и выполнении условий $P_{01} \ll P_{00}$, $P_{01} \ll P_{11}$ ошибки на выходе могут группироваться в пачки.

Модель канала передачи данных Гильберта-Элиота по своим свойствам близка к релеевскому каналу с переменными параметрами (с замиранием без поворота фазы). Элиот допустил, что $P_{0Ш0} \ll P_{0Ш1}$, где $P_{0Ш0}$ – вероятность

ошибки для штатного состояния, а $P_{0Ш1}$ – вероятность ошибки для неработоспособного состояния. Модель Гильберта-Элиота применяется в исследованиях каналов передачи данных с переменными параметрами.

Обобщением модели Гильберта-Элиота является другая модель канала передачи данных Смита – Боуэна – Джойса [41]. Ниже представлено выражение, при помощи которого формируется матрица переходных вероятностей (при выполнении условия формирования пакетов $P_{02} \ll P_{12}$):

$$P_{i.j} = \begin{Vmatrix} P_{00} & 0 & P_{02} \\ 0 & P_{11} & P_{12} \\ P_{20} & P_{21} & P_{12} \end{Vmatrix}.$$

В модели канала передачи данных Бергера-Мандельброта интегральная функция распределения длин интервалов между ошибками определяется по закону Парето с показателем $a < 1$ [42]:

$$W(t) = \frac{a}{t^{a+1}} \text{ для } t > 1;$$

$$W(t) = 0 \text{ для } t \le 1.$$

В основе этих результатов лежат вероятностные характеристики сигналов на выходе, чем объясняется недостаточная адекватность подобных моделей в сравнении с реальными каналами передачи данных, и, следовательно, это требует большого количества статистических данных, получаемых на практике при эксплуатации, и необходимости проведения стрессового тестирования перед началом работы [43].

Для достоверного описания статистики ошибок при передаче данных необходимо прибегнуть к усложнению модели, что приводит к повышению сложности производимых вычислительных расчетов. В результате, с учетом вышесказанного, возникает необходимость в разработке более эффективных подходов к обнаружению и исправлению выявленных фактов нарушения целостности пакетов данных для их непосредственной интеграции в средства защиты информации СППД.

3.2 Состав информации в системах передачи-приема данных

Рассмотрим состав передаваемой телеметрической информации. Телеметрия рассматривается в настоящей работе как технический аспект, ориентированный на особенности эксплуатации наземных телеметрических систем – «комплекса автоматизированных средств, обеспечивающих получение,

преобразование, и передачу по каналу, прием, обработку и регистрацию измерительной информации и информации о событиях с целью контроля на расстоянии различных объектов и процессов» [43]. Отметим, что телеметрию с использованием передачи информации по радиоканалу, принято называть радиотелеметрией, которая получила широкое распространение благодаря возможностям работы с подвижными или труднодоступными объектами. В качестве среды передачи данных могут использоваться специальные телеметрические каналы передачи данных, в которые входят такие среды передачи данных как оптоволоконные линии, кабельные системы, радиолинии. Сущность телеметрии заключается в преобразовании измеряемой величины в информационный сигнал, пригодный для передачи по каналу, ее декодирования, преобразования и регистрации на приемной стороне [26].

Для ее осуществления используется мониторинг – постоянное наблюдение, оценка и прогноз какого-либо процесса. Для «получения данных о контролируемом объекте используются датчики телеметрии, способные работать в телеметрических системах со специально разработанными модулями» [26], позволяющие собирать, преобразовывать, передавать на расстояние и визуализировать в любом удобном для приемника виде все принимаемые данные (ток, напряжение, давление, температуру).

«Различают телеметрию по вызову и по выбору текущих значений» [26]:

1. «Телеметрия по вызову – телеизмерение по команде, посылаемой с пункта управления на контролируемый пункт и вызывающий подключение на контролируемом пункте передающих устройств, а на пункте управления – соответствующих приемных устройств. Телеизмерения по вызову позволяют использовать один канал передачи данных для поочередного наблюдения за многими объектами телеизмерения» [26].
2. «На пункте управления, показания можно наблюдать на общем выходном приборе. Если показания имеют различные шкалы, то измеряемые величины подключаются к разным приборам. При телеизмерении по вызову можно применять автоматический опрос объектов циклически по заданной программе» [26].
3. «Телеизмерение по выбору – телеизмерение путем подключения к устройствам пункта управления соответствующих приемных приборов при постоянно подключенных передающих устройствах на контролируемом пункте» [26].

4. «Телеизмерение текущих параметров – получение информации о значении измеряемого параметра в момент опроса устройством телемеханики» [26].

5. «Телеизмерение интегральных значений – получение информации об интегральных значениях измеряемых величин, проинтегрированных по заданному параметру, например, времени в месте передачи» [26].

Основной единицей телеметрической информации являются числовые данные о контролируемых или наблюдаемых объектах, удаленных и расположенных на больших расстояниях от получателя, из которых формируются передаваемые данные по каналу передачи данных.

Управление осуществляется автоматизированной системой, состоящей из двух основных частей: бортовой и наземной. «Идея запроса с остановками заключается в том, что передатчик ожидает от приемника подтверждения успешного приема предыдущего блока данных перед тем, как начать передачу следующего. В случае если блок данных был принят с ошибкой, приемник передает отрицательное подтверждение, и передатчик повторяет передачу блока. Данный метод подходит для полудуплексного канала передачи данных. Его недостатком является низкая скорость из-за высоких накладных расходов на ожидание» [44].

«При использовании метода непрерывного запроса с выборочным повторением осуществляется передача только ошибочно принятых блоков данных» [44]. Примером такой системы является ECC (Error Correcting Coding) [45], которая отличается от других систем обнаружения ошибок тем, «что возникающие ошибки могут быть исправлены, а не просто обнаружены» [45]. «Преимущество заключается в том, что в системе, использующей ECC, не требуется обратный канал для запроса повторной передачи данных при возникновении ошибки» [45]. «Недостатком является то, что к данным добавляется фиксированные накладные расходы, что требует более высокой пропускной способности прямого канала и требуется наличие канала обратной связи» [45]. Поэтому ECC применяется в ситуациях, когда повторная передача данных является дорогостоящей или невозможной, например, по односторонним каналам передачи данных и при передаче нескольким получателям в многоадресной передаче [46].

Цель теории канального кодирования состоит в том, чтобы найти коды, которые быстро передают данные, содержат много допустимых вариантов генерирования кодовых слов и могут исправить или, по крайней мере,

обнаружить много ошибок. Такой подход является компромиссным, обладает эффективностью и в настоящее время широко применяется из-за широты охвата задач в этих областях. Подход обладает универсальностью и может быть оптимальным для разных конкретных приложений. Необходимые свойства использования такого подхода зависят от вероятностей возникновения в каналах ошибок во время передачи.

Наиболее распространенным является код повторения и исправления ошибки для передачи данных по зашумленному каналу, который может нарушить передачу в нескольких местах. Повторение состоит в том, чтобы передать данные несколько раз, при этом канал возвращает лишь меньшинство этих повторов, получатель может восстановить исходные данные, просмотрев полученные данные в потоке, которые встречаются чаще всего [47].

Большинство телекоммуникационных систем используют код фиксированного веса, предназначенного для обеспечения ожидаемой частоты битовых ошибок в наихудшем случае, а затем совсем перестает функционировать, если частота битовых ошибок становится еще больше. Некоторые экземпляры гибридного автоматического запроса используют фиксированный метод ECC [46].

В случае, когда генерируется сильный код с низкой скоростью передачи, он может вызвать значительное увеличение значения отношения сигнал/шум, в результате чего снижается частота битовых ошибок, «за счет снижения эффективной скорости передачи данных» [45]. С другой стороны, отсутствие использования какого-либо метода, дает кодовую скорость равную 1, и при этом используются возможности полноты занятости канала.

3.3 Контроль ошибок при передаче двоичных кодовых последовательностей

«В случае полностью ассиметричного канала код с постоянным весом считается совершенным применительно к обнаружению ошибок, так как он обнаруживает все ошибки. Ассиметричным является канал, в котором имеет место только один вид ошибок, то есть, возможно, только преобразование нулей в единицы (или наоборот)» [45].

При использовании кодов с постоянным весом в первую очередь необходимо определить основной алфавит системы. После чего осуществляется выбор кода, который обладает необходимым количеством кодовых слов. Затем каждому символу алфавита сопоставляется кодовое слово с постоянным весом. Одним из существенных недостатков представленного закрепления кодовых слов

является случай, когда буквы в своем подавляющем количестве передаются группами. При применении неразделимых кодов, избыточность заложена в каждой закодированной букве, следовательно, экономичность повышается исключительно с помощью кодирования лишь целой группы букв.

Известно, что соотношение (3.1) определено для любого числа n элементов:

$$C_n^m = C_n^{n-m}. \qquad (3.1)$$

«Максимальное число разрешенных кодовых комбинаций для элементов кода с постоянным весом с учетом соотношения» [46, 47] (3.1) определяется выражениями:

$$C_{n\,макс.}^m = C_n^{\frac{n+1}{2}} = C_n^{\frac{n-1}{2}} \text{ при } n \text{ нечетном};$$

$$C_{n\,макс.}^m = C_n^{\frac{n}{2}} \text{ при } n \text{ четном.}$$

$$P_{необ.} = \sum_{t=1}^{m} C_m^t C_{n-m}^t p_n^{2t} (1-p)^{n-2t};$$

$$P_{об.} = 1-(1-p_n)^n - \sum_{t=1}^{m} C_m^t C_{n-m}^t p_n^{2t} (1-p)^{n-2t}.$$

«Очевидно, что во всех остальных случаях, когда $\frac{n+1}{2} < m < n-1$ или $1 < m < \frac{n-1}{2}$ при n нечетном, $\frac{n}{2} < m < n-1$ или $1 \le m < \frac{n}{2}$ при n четном, количество разрешенных комбинаций $C_n^m < C_{n\,макс.}^m$» [48].

«Декодирование принятых комбинаций кода с постоянным весом сводится к определению их веса» [45]. В случае, если полученный вес отличается от заданного, следует вывод, что комбинация принята с ошибкой. Отдельно отметим, что при проведении проверки на постоянство веса, как правило, идентифицируются ошибки любой кратности. Исключение составляют лишь ошибки сдвига описанные выше [48].

Определим «вероятность не обнаружения ошибки сдвига, обусловленной только одиночными преобразованиями единиц и нулей данной комбинации» [48]. «Рассматривая случай передачи данных по симметричному каналу, когда вероятность преобразования единицы в нуль равна вероятности преобразования нуля в единицу, замечаем, что вероятность преобразования одной из трех единиц в нуль равна $C_3^1 p_3 (1-p_3)^2$, а вероятность преобразования одного из четырех нулей в единицу составляет $C_4^1 p_3 (1-p_3)^3$» [46].

Воспользуемся «теоремой умножения вероятностей совместных и независимых событий» [46]. Получим следующее:

$$P_{необ.} = C_3^1 p_3 (1-p_3)^2 C_4^1 p_3 (1-p_3)^3 = 12 p_3^2 (1-p_3)^5 .$$

«Очевидно, что вероятность обнаруженных ошибок равна разности между вероятностью P_k всех ошибок кодовой комбинации и вероятностью, не обнаруживаемых ошибок $P_{необ.}$» [48]:

$$P_{об.} \approx P_k - P_{необ.} = 1-(1-p_3)^7 - 12 p_3^2 (1-p_3)^5 .$$

В общем случае для n-элементной видовой последовательности можно записать [48]:

$$P_{необ.} = \sum_{i=1}^{m} C_m^l C_{n-m}^l p_3^{2l} (1-p_3)^{n-2l};$$

$$P_{об.} = 1-(1-p_3)^n - \sum_{i=1}^{m} C_m^l C_{n-m}^l p_3^{2l} (1-p_3)^{n-2l} .$$

Однако, несмотря на преимущества и простоту кодов с постоянным весом, они обладают следующим недостатком. Так, в случае неопределенности получаемых данных, вся контролирующая канал информация заключена в использовании кода с конкретным фиксированным весом. Для последующего уменьшения возникающей неопределенности требуется быстро сформировать код с новым весом. Если это производится вручную, то такая процедура занимает дополнительное время, в которое входит поиск подходящего веса и сама генерация кода.

Следует отметить, особую эффективность этих кодов, проявляющуюся в быстроте обнаружения ошибки в передаваемых данных. Недостатком являются случаи, «когда источник информации выдает случайную последовательность двоичных сигналов» [48], в результате чего применение кодов с постоянным весом весьма затруднительно. Например, «код «3 из 7» широко используется при частотной манипуляции в каналах с селективными замираниями, где вероятность ошибок невелика» [45]. Расчёты по приведенным формулам показали, что одна ошибка приходится на 58000 тысяч необнаруженных ошибок [49].

Вероятность появления не обнаруживаемых ошибок смещения:

$$P_{bo} = P_{a1} + P_{a2} + P_{a3}, \text{, где}$$

$$P_{a1} = C_3^1 * C_4^1 * p^2 * (1-p)^5$$

$$P_{a2} = C_3^2 * C_4^2 * p^1 * (1-p)^3$$

$$P_{a3} = C_3^3 * C_4^3 * p^5 * (1-p)^1 ,$$

При $p \ll 1 \quad P_{a3} \ll P_{a2} \ll P_{a1}$, тогда $P_{bo} = 12p^2(1-p)^5$.

Вероятность появления всевозможных ошибок как обнаруживаемых, так и не обнаруживаемых будет составлять $P_E = 1-1-(1-p)^7$.

Вероятность обнаруживаемых ошибок $P_{00} = P_E - P_{bo}$. Тогда коэффициент обнаружения будет равен $K_{обн.} = \frac{P_{00}}{P_E} = \frac{1-(1-p)^n - 12 * p^2 * (1-p)^5}{1-(1-p)^n}$.

Например, код C_7^3 при $p = 10^{-2}$ - коэффициент обнаружения составит $K_{обн} = 0,985$, избыточность $L = 27\%$ [50].

3.4 Определение параметров двоичных кодов с фиксированным весом

Рассмотрим передачу телеметрических данных, которые кодируются с использованием двоичных кодов с постоянным весом для обнаружения ошибок при передаче и, которые исходно представляют собой целые десятичные числа, служащие для указания значений контролируемых данных. Кодовое слово включает код самого числа и указания количества содержащихся в нем единиц (веса). На стороне приемника требуется: вычислять веса десятичных чисел, а также при необходимости декодирования и восстановления целостности двоичного кода определять позиции в нем единиц, веса последовательности единиц (нулей), расстояния между ними.

Кратко рассмотрим существующие способы подсчета единиц в двоичном коде:

1. Одним из таких способов является способ, построенный на принципе «разделяй и властвуй». Исходная последовательность разбивается на пары символов, затем значения числа бит в соседних парах складываются, и сумма помещается в четырех разрядное поле. Далее процесс аналогичен – соседние четверки объединяются в восьмерки и т.д. Последняя композиция определяет количество единиц. Весь алгоритм может быть выполнен за $\log n$ шагов, где n - длина исходной последовательности символов.

2. Алгоритм бинарного поиска.

3. Алгоритм быстрой сортировки.

Второй и третий способы достаточно затратны по времени, так как алгоритмы носят циклический характер, а число циклов зависит от веса двоичной последовательности.

4. Разложение числа в ряд вида: $N_1 = x - [(\frac{x}{2})] - [(\frac{x}{4})] - [(\frac{x}{8})] - ... - [(\frac{x}{2^n})]$,

где N_1 – число единиц. Для реализации в разрядной сетке длиной 31 бит требуется последовательность из 31 команды сдвига вправо на единицу и 31 команды вычитания (при длине исходного кода 32 бита).

5. Одним из ранних методов являлся метод, реализованный на компьютере DEC PDP-10, в который встроена команда (на языке Ассемблер), ускоряющая вычисление остатка от деления целого числа в системе с основанием b на $(b-1)$ для проведения операции сравнения по модулю $(b-1)$ с суммой значений бит, содержащихся в 6-битовых полях разбитой исходной последовательности. Несмотря на этот прием, требуется 10 команд (для случая исходных слов большого веса (62 бита)), при этом вычисление числа единиц считается достаточно медленным.

6. Использование циклического сдвига. Здесь идет сброс крайнего справа единичного сдвига до тех пор, пока слово не станет равным нулю. Метод может дать эффект для случая небольшого количества единиц.

Основными недостатками рассмотренных подходов являются сравнительно невысокая скорость вычислений, особенно серий единиц или нулей, отсутствие возможностей указания позиций единиц в последовательностях в процессе вычислений.

В настоящей работе предлагается метод вычисления веса целого десятичного числа и определение позиций единиц, не прибегая к его двоичному разложению, а также позволяющий получать эти же результаты и в случае работы с двоичными эквивалентами десятичного числа.

Пусть α_1 – такой наибольший индекс, что $x_{\alpha_1} = 1$, тогда $M = M_0 = 2^{\alpha_1} + M_1$, причём $\alpha_1 = \log M_0$, где $[x]$ – целая часть числа. Если $M_1 \neq 0$, то продолжая процесс разложения, получим $M_1 = 2^{[\log_2 M_1]} + M_2$. Этот процесс носит рекурсивный характер и завершается на шаге k, когда $M_k = 0$. Пусть $\alpha_1 = [\log_2 M_{i-1}], i = 1.2,...,k$. Тогда k равно весу числа M, а последовательность $\alpha_1,...,\alpha_k$ задаёт позиции единиц в двоичной записи числа M, то есть $M = \sum_{i=1}^{k} 2^{\alpha_i}$.

Общая формула рекурсивного разложения имеет вид [48]:

$$M = M_{i-1} - 2^{[\log_2 M_{i-1}]}. \qquad (3.2)$$

«Число рекурсий m в точности совпадает с весом числа M: $m = W(M)$, где W - вес числа, при этом весовые значения W_1 на каждом шаге рекурсии определяются как» [47]:

$$W'_i = \begin{cases} 1 \ \textit{при} \ M_i \geq 0 \\ 0 \ \textit{при} \ M_i < 0, \end{cases}$$

а вес числа заданного веса вычисляется с помощью выражения [48]:

$$W_i = \sum_{m=1}^{i} W'_m,$$

где $m = 1, 2, 3...$

Рассмотрим конкретный пример: $M = 41$.

$$M_1 = 41 - 2^{[log_2 41]} = 41 - 32 = 9 \to W1 = 1;$$
$$M_2 = 9 - 2^{[log_2 9]} = 9 - 8 = 1 \to W_2 = W1_i + 1 = 2;$$
$$M_3 = 1 - 2^{[log_2 1]} = ...0 \to W_3 = W_2 + 1 = 3.$$

В результате двоичное число M имеет вид 101001, а его вес $W(41) = 3$. «Для чисел N_i, не кратных 2 и лежащих в интервале $[2^{i-1}; 2^i]$, вычитаемые числа вида $[2^{\log_2 M}]$ имеют одинаковые значения, поэтому разности, получаемые на каждом шаге рекурсии уникальны» [48].

Примеры:

$$M_i = 17, log_2 17 = 4.087..., 2^{[log_2 17]} = 2^4,$$
$$M_i = 25, log_2 25 = 4.643..., 2^{[log_2 25]} = 2^4,$$
$$M_i = 31, log_2 31 = 4.954..., 2^{[log_2 31]} = 2^4.$$

«Отсюда разложение целого десятичного числа по формуле (3.2) дает единственную последовательность чисел, получаемых на каждом шаге рекурсии. Так для рассмотренного выше примера, для $M = 41$, такая последовательность

$$41 \to 9 \to 1,$$

а для $M = 83$,

имеет вид 41-9-1:

$$103 \to 39 \to 7 \to 3 \to 1.$$

Вес каждого следующего числа в последовательностях уменьшается на единицу: $103\,(W = 5) \to 39\,(W = 4) \to 7(W = 3) \to 3(W = 2) \to 1(W = 1)$» [47].

Рассмотрим следующий пример.

Пример: $M = 15$.

$$1-й\ шаг: выделяем\ из\ 2^{[\log_2 15]} \to [\log 15] = 3,$$
$$2-й\ шаг: выделяем\ из\ 2^{[\log 7]} \to [\log 7] = 2,$$
$$3-й\ шаг: выделяем\ из\ 2^{[\log 3]} \to [\log 3] = 1,$$
$$4-й\ шаг: выделяем\ из\ 2^{[\log 1]} \to [\log 1] = 0.$$

«Полученные значения (3; 2; 1; 0) задают позиции единиц в числе $M = 15$. По результатам разложения достаточно легко получить двоичный эквивалент десятичного числа. Для этого необходимо последовательность $x_n x_{n-1} ... x_1 x_0, где\ x = \{0,1\}$ заполнить единицами в тех позициях, которые были вычислены на каждом шаге разложения по (3.2), остальные позиции обнуляются, при этом n определяется как $\log_2 M_i$» [48]. Отсюда любое десятичное число можно записывать множеством индексов, полученных в результате разложения.

Рассмотрим способы реализации метода, который может быть реализован программным путем и аппаратным способом.

Остановимся на программной реализации разработанного метода, как наиболее быстрого. В формуле (3.2) необходимо определять значение вычитаемого. Эта операция связана с вычислением двоичного логарифма, что вызывает временные потери и снижает общую скорость определения веса числа. С целью уменьшения влияния этого недостатка предложено заменить эту операцию следующими действиями. Так как вычисление $2^{[\log_2 M]}$ дает всегда целые значения, то всевозможные значения этого вычитаемого сводятся к ряду значений $2^1, 2^2, 2^3, ..., 2^n$, где n – длина числа M_i. Отсюда можно сформировать n интервалов вида $[2^1 ... 2^2], [2^2 ... 2^3], ..., [2^{n-1} ... 2^n]$, причем правые (меньшие) границы этих интервалов представляют собой значения вычитаемых $2^{[\log_2 M]}$. Производя сравнения исходного числа M_i с границами всех интервалов и определяя интервал, в который число попадет, можно правую меньшую границу этого интервала использовать как готовое вычисленное значение вычитаемого. Составляя список значений всех правых границ и, поставив ее каждое значение в соответствие своему интервалу, можно операцию определения значения вычитаемого из выражения (3.2) заменить поиском соответствующего интервала и выбора из списка правых границ его значения.

Таким образом, требуется провести n сравнений исходного числа M_i с границами интервалов. Следует отметить, что применение логарифмического поиска сокращает число сравнений до значения $\log_2 M_i$.

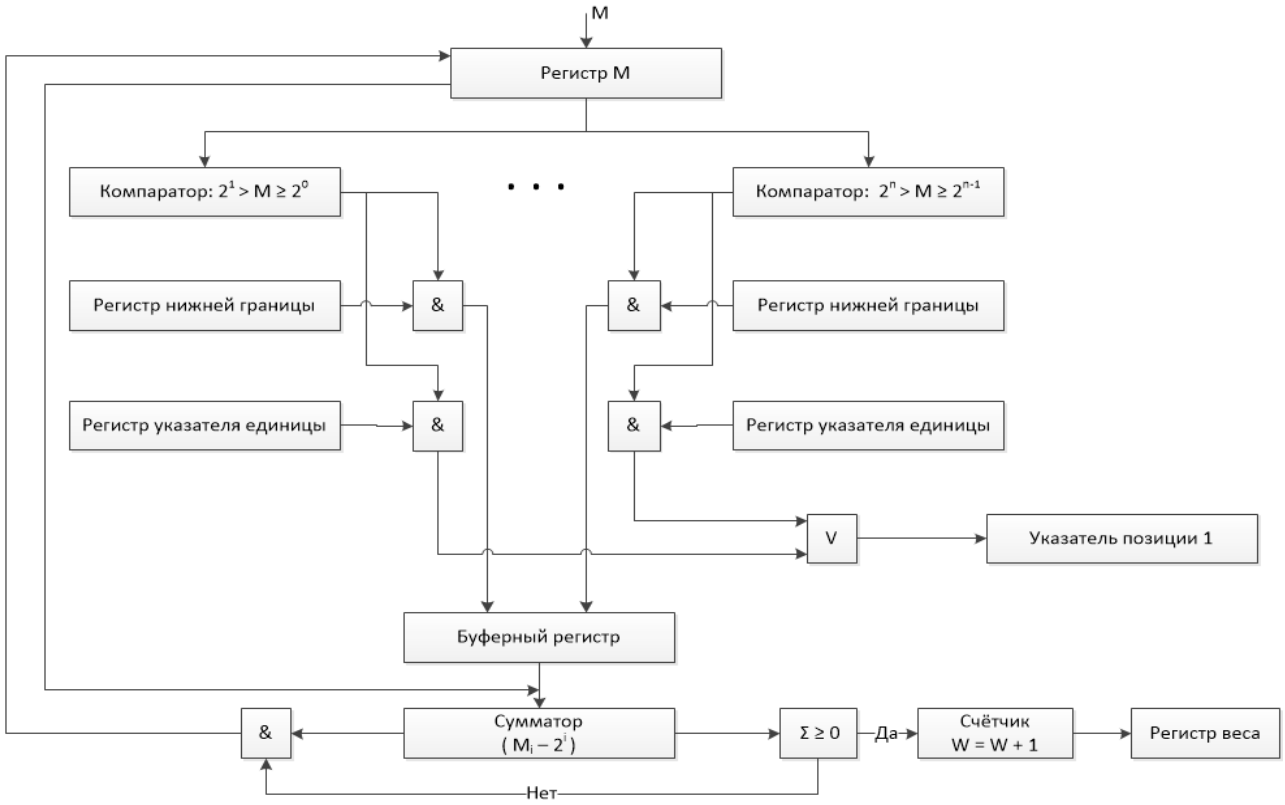

Рисунок 3.1 Схема получения единицы двоичного числа на текущем шаге рекурсии

С целью ускорения процесса вычисления веса целого числа, рассмотрим аппаратную реализацию метода [48]. При аппаратной реализации число M_i подается одновременно на входы n стандартных компараторов, активизированный выход одного из которых разрешает присоединенному к нему регистру, хранящему значение нижней границы, посылать это значение на сумматор, на котором происходило вычитание по формуле (3.2). Если на сумматоре результат больше или равен нулю, то в счетчик веса добавляется единица и результат вычитания передается на вход схемы - он становится входным числом для следующего шага рекурсии. В противном случае вычисление веса заканчивается.

Номер позиции текущей единицы определяется следующим образом. К выходу компаратора присоединен второй регистр, на котором записан код номера единицы $\log_2 M_i$, указывающий ее местоположение в числе на текущем шаге рекурсии. Это значение указателя общее для всех чисел, попавших в интервал компаратора. Количество таких чисел в каждом интервале составляет $(2^i - 2^{i-1})$. Значения веса числа и указателей текущей единицы после

срабатывания компаратора передаются на выходные регистры схемы. Схема получения единицы двоичного числа на текущем шаге рекурсии представлена на рисунке 3.1 и достаточно просто реализуется на стандартных компонентах, причем задержка в основном определяется временем последовательного срабатывания двух компараторов (первый отвечает за выбранный интервал, второй – за оценку результата вычитания на сумматоре) и временем работы сумматора.

Отметим основные достоинства предлагаемого метода:

1. «Любое целое десятичное число $M \neq 2^k$, *где* $k = 1, 2, 3...$ может быть разложено по формуле (3.2) на конечную убывающую последовательность целых чисел, причем вес числа на каждом шаге рекурсии уменьшается на единицу» [47].

2. «Результат вычисления $\log M_i$ в формуле (3.2) на каждом i-шаге рекурсии представляет собой индекс позиции единицы веса десятичного числа» [47].

3. «Количество рекурсий по формуле (3.2) в точности совпадает с весом разлагаемого десятичного числа» [47].

4. «Разложение целого числа по формуле (3.2) дает единственную последовательность целых чисел, получаемых на каждом шаге рекурсии» [47].

5. Длина последовательности нулей в двоичном коде исходного числа равна разности значений индексов единиц, получаемых на соседних шагах рекурсии минус единица $L = \alpha_{\upsilon} - \alpha_{\upsilon-1} - 1$, *где* υ - индекс шага рекурсии ($\upsilon = 1, 2, 3...$), а для случая четного числа, в котором последовательность нулей может начинаться с единицы и заканчиваться нулем в разряде двоичного кода с весом равном единице, длина последовательности нулей равна номеру позиции этой единицы.

3.5 Генерация двоичных кодов целых чисел с переменным весом (алгоритмический подход)

Важной характеристикой двоичного кода десятичного числа является его вес, по которому можно эти числа группировать в множества и организовывать их по определенному правилу в соответствии с выбранной структурой представления этого множества. Вес двоичного числа может использоваться как параметр, который можно использовать как признак при решении классификационных задач в помехоустойчивом кодировании, при распознавании образов можно судить о качестве производимых изделий.

Особенностью веса является его длина, выражаемая количеством единиц присущих конкретному числу. Очевидно, что максимальный вес равен длине двоичного кода закодированного десятичного числа. Она меняется и зависит от величины десятичного числа. Кроме этого, вес имеет спектр, который выражается расположением единиц на позициях двоичного кода. Можно считать вес как переменную величину и при необходимости ей управлять. Отсюда вес можно рассматривать как управляемую переменную, и она может быть признаком различия и принадлежности объекта к конкретной предметной области.

Структуризация двоичного кода, то есть установление количества единиц двоичной последовательности (веса) и расположение единиц на нумерационной подложке при большой длине, вручную длительный и не всегда безошибочный процесс. Изменение веса конкретного числа или местоположений единиц в нем приводит к изменению его значения, а это означает, что можно любое десятичное число представить другим десятичным числом с прежним или с другим весом. Для этого требуется создание ряда чисел, на который раскладывается исходное число, причем ряд должен сходиться, а при переходе от одного числа к другому меняется вес числа ряда. В таком ряду числа уменьшаются, а веса возрастают на каждом шаге. В итоге такого разложения исходное число обращается в нуль, а вес должен достичь заданной величины. Отсюда появляется возможность кодирования целых десятичных чисел множеством целых десятичных числе с наперед заданным весом. При этом длина двоичного кода числа также становится переменной - изменяется при изменении величины веса. В этом случае появляются свойства многозначности кодирования целых чисел.

Основные положения предлагаемого подхода изложены в [49].

Отметим, что такой подход представляет «собой двухуровневый процесс кодирования данных, включающий попеременное обращение к матричным числам и дугам наложенного графа, наложенного по времени (маршруту) и плоскости (позициям матрицы)» [50]. Исследования показали, что перечисленным выше требованиям отвечает матрица Паскаля и биномиальные числа, содержащиеся в ней [48, 49].

В качестве поля матричных чисел рассматривается матрица биномиальных коэффициентов Паскаля, в которой «левая верхняя граница треугольника занимает левый столбец матрицы и формируется нижнетреугольная матрица с правой нулевой диагональю» [48]. Такое представление матрицы обеспечивает построение маршрутов по выбираемым числам, по которым шаг за шагом формируется двоичный код и путь заканчивается всегда в левом верхнем углу на

значениях чисел равных нулю. Фактически кодируемое число раскладывается в виде уменьшающегося ряда чисел матрицы Паскаля.

«Матрица Паскаля P после модификации имеет следующую структуру:

1. По главной диагонали матрицы расположены нулевые элементы; Элементы первого столбца равны номеру соответствующей строки минус единица;

2. Все остальные элементы матрицы строятся по рекурсивной формуле:

$P(i, j) \cdot P = (i-1, j-1) + P(i-1, j)$, *где* $i = \overline{3, n}$, $j = \overline{2, m}$, *причем n и m – целые числа.*» [47].

«Основная идея предложенного метода кодирования на основе матрицы Паскаля заключается в следующем. Пусть имеется некоторое множество S_1, состоящее из всех неотрицательных десятичных целых чисел. Необходимо найти преобразование этого множества во множество двоичных слов (обозначим его S_2), причём длина и вес этих слов могут быть переменными, кроме этого, должно быть найдено и обратное преобразование» [47].

3.5.1 Формирования двоичного кода передаваемых данных с помощью матрично-алгоритмического кодирования

Код, передаваемого числа формируется за «счет построения пути на поле матрицы Паскаля по определенному правилу, которое задается уравнением формирования кода числа N, которое является телеметрическим показателем и задается уравнением вида:

$$N = \sum_{k=1}^{i} x_k a_{i,j},$$

где

$$x_k = \begin{cases} 1, \textit{при } f = true \\ 0, \textit{при } f = false \end{cases}$$

k - число бит в кодовой последовательности передаваемых телеметрических данных, G- некоторое условие, связанное со значениями матричного числа $a_{i,j}$ и некоторого числа Q. Условие G и число Q задают правило формирования значения, текущего бита кода x_k. Выбор правила и связанного с ним условия G влияет на переходы на числовом поле матрицы и определяют искомую кодовую последовательность» [49].

«Предложенная схема кодирования обеспечивает получение битов кода x_k и включает в себя отдельные шаги по применению правила φ и анализа

условий f . В качестве шаговой операции предлагается использовать операцию последовательного вычитания из исходного кодируемого числа вначале и затем из остатков вычитания матричных чисел и оценки получаемых разностей» [49].

«Переходы осуществляются следующим образом» [47]:

1. «На первом шаге выбирается такой столбец матрицы, чтобы его номер совпадал со значением веса кодируемого числа» [46]. Далее в выбранном столбце подбирается матричное число наиболее близкое по значению к искомому. Так как оно положительное, то в первый разряд кода числа записывается 1 и делается переход на матричное число $N(i-1, j-1)$.

3. На следующем переходе из полученного остатка ΔA_1 вычитается матричное число $N(i-2, j-1)$. Если результат отрицательный, то делается переход вверх по столбцу на матричное число $N(i-2, j-1)$ и в код числа записывается 0.

Процесс кодирования завершается, как только разность между последним остатком и последним выбранным матричным числом станет равной нулю. Последовательность вычитаний приводит к последовательности матричных чисел, которые образуют путь на поле матрицы и представляют собой разложение кодируемого числа на сумму чисел.

При использовании такого подхода обеспечивается биективность кодирования и декодирования из-за того, что структура матрицы Паскаля имеет строго фиксированную организацию и все пути в ней являются уникальными.

В этом проявляется свойство взаимо однозначности кодирования – количество формируемых путей из одной стартовой позиции фиксирован и не один путь не повторяет другие.

Время кодирования определяется как суммарное время перехода от одного числа матрицы к другому плюс время вычитания и плюс время сравнения [52]:

$$T = t_{пер.} + t_{выч.} + t_{ср.}.$$

3.5.2 Алгоритм декодирования кода с заданным весом

При формировании маршрута процедуры поиска матричного числа, удовлетворяющего условию G на каждом его отрезке разложения исходного числа, необходимо учитывать, что матричные числа привязаны к своим координатам (*i*,*j*), где индекс *i* - номер строки матрицы, а второй индекс j – номер столбца (вес), и последние могут менять свои значения. «Положение матричного

числа в матрице и его «маркировка» единицей в кодовой комбинации происходит с помощью использования двух индексов $i, j - x_j^i$» [49].

«Верхний индекс i обозначает номера шагов маршрута, и он является непрерывным $(N = 1, 2, 3, ...)$. Нижний индекс j связан с весом кодируемого числа в процессе кодирования, т.е. путём вычитания из исходного числа матричных чисел, вес должен уменьшаться, как и длина пути в матрице. Неизменность веса (значение j) означает, что отрезок пути проходит по столбцу вверх, а так как длина пути (в количестве шагов - бит) известна заранее (задаётся вес), то значения верхнего или нижнего индексов, или они оба, на каждом шаге уменьшаются» [47].

«Нумерация нижних индексов начинается с первой стоящей справа единицы в коде числа и уменьшение веса (числа единиц в коде) означает смену столбца с уменьшением значения строки» [49].

«При декодировании нижний индекс формируется путём сплошной нумерации всех единиц кода справа налево (пропускаются нули)» [48].

Предлагается «определять индекс j - бита в коде по формуле:

$$j = i - z(0),$$

где i - номер i - ой позиции единицы по нумерации в верхней строке, $z(0)$ - количество нулей справа от j - ой позиции, на которой стоит единица.

Время декодирования прямо пропорционально и равно весу кода W, умноженному на время вычисления координат j для случая появления в коде единицы плюс время, необходимое для выполнения операции сложения чисел по полученным координатам» [49].

Ниже приводятся данные, характеризующие свойства матричного кодирования для оценки возможностей использования его на практике.

«Объем памяти для хранения матрицы кодирования:

$$V = (n-1) \times \left(\frac{n \times (n-1)}{2} - \frac{(n-W) \times (n-W-1)}{2}\right).$$

Максимальная длина матричного кода:

$$n = \log_2 C_{n-1}^{g}, \text{ где } g = \left[\frac{n-1}{2}\right].$$

Максимально представимое число:

$$\max M_j^i = \max C_{n-1}^{\left\lceil \frac{n-1}{2} \right\rceil}.$$

Диапазон представления кодируемых чисел:

$$C_{L-2}^{W-1} < M < C_{n-1}^{W-1}.$$

Количество кодируемых чисел длиной L с весом W:

$$K = C_{L-1}^{W-1}.$$

Скорость кода:

$$R' = \left\lfloor \frac{\log C_{L-1}^{W-1}}{L} \right\rfloor$$ [48, 49]».

3.6 Обнаружение искажений в передаваемых данных на основе использования кодов с переменным весом

Система передачи-приема данных в общем случае включает три составные части: подсистему отправителя, на стороне которой находится матричный кодер, защумленный дискретный канал передачи данных, приемник, который имеет декодер. Кодер отправителя формирует данные в виде целых двоичных чисел заданного веса и передает их в канал, в котором действуют шумы и помехи. В приемнике имеется декодер, обрабатывающий полученные данные алгоритмом декодирования и обнаруживает ошибки с указанием местоположений этих ошибок.

Рассмотрим процесс, происходящий на обеих сторонах канала, при этом для удобства будем называть исходные данные прообразом, а принятые данные его образом. Согласно алгоритму матричного кодирования [48], прообраз данных формируется с построением пути на поле чисел двоичным кодом с необходимым числом единиц.

Согласно этому алгоритму необходимо сначала выбрать стартовую позицию – стартовое число начала формируемого пути. Для этого в матрице Паскаля требуется подобрать такое число, которое удовлетворяет условию:

$$N_M(i, w) \le N_{исх.} \le N_M(i+1, w), \qquad (3.3)$$

где $N_{исх.}$ - это число подлежащее кодированию с заданным весом. Для поиска этого стартового числа ($N_{ст.}$) необходимо сначала выбрать столбец матрицы, номер которого совпадает со значением веса, которым должно обладать кодируемое число. Для этого нужно просмотреть все числа столбца, который удовлетворяет неравенству 3.3. После этого реализуется процесс кодирования числа $N_{исх.}$, реализованный в виде программного приложения, которое входит в состав средств у отправителя. Структура этих средств представлена на рисунке 3.2.

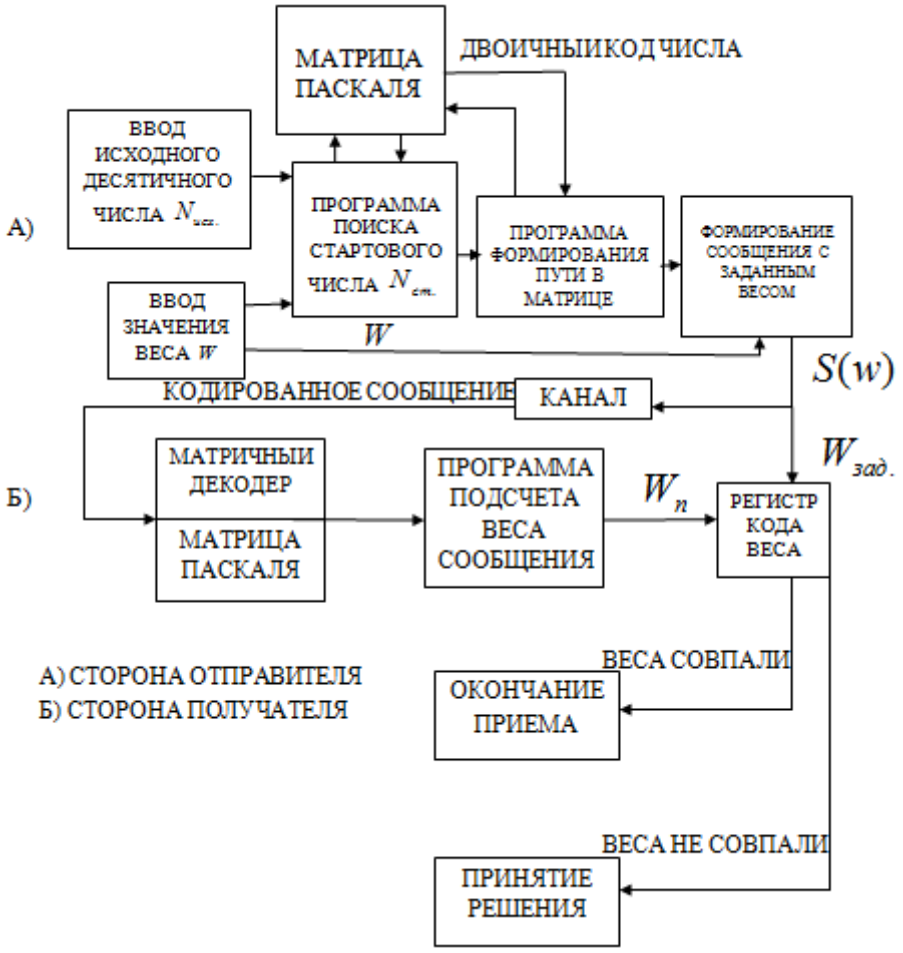

Рисунок 3.2 Подсистема обеспечения целостности данных на основе кодов с переменным весом

Это будет свидетельство факта обнаружения ошибки. Для того, чтобы это сделать необходимо, чтобы в состав средств у получателя входила матрица Паскаля, матричный декодер, программа подсчета единиц (веса) полученных данных, методика и дополнительные средства по определению достоверного восстановления прообраза данных. В случае отсутствия матрицы Паскаля считается, что у получателя есть программа ее быстрого формирования по

столбцу, с равным любому заданному весу до строки, в которой находится стартовое число построения данных – кодового пути.

В случае несовпадения весов проводится вторая проверка, которая заключается в просмотре чисел по столбцу матрицы Паскаля с номером, равным декодированному весу, и если совпадения нет, то проверка может продолжаться в междустроковом интервале, границы которого определяются стартовым числом и следующим числом матрицы Паскаля по порядку возрастания «столбцовой» координаты. Например, в столбце № 2 матрицы Паскаля соседние матричные числа 6 и 10 заключают между собой числа - 7, 8, 9, которых в матрице нет. С их помощью можно посмотреть наличие и соответствие им полученных и построенных декодером десятичных чисел. Отметим, что с помощью матрицы Паскаля кодирование произвольных натуральных десятичных чисел осуществляется таким образом, что ее числа используются для поиска стартового числа, с которого начинается формироваться путь на поле чисел самой матрицы, и после этого ими - для формирования пути.

После установления факта наличия прообраза числа в матрице Паскаля сеанс передачи-приема данных в матрице заканчивается. Недостатком этого варианта является необходимость просмотра этих неявно скрытых диапазонов чисел, которые в отдельных случаях могут быть достаточно большими.

Если веса отправленного и полученного кодов данных не совпадают, и нет возможности повторной отправки из-за ограничения времени для более высокой достоверности, требуется, чтобы у получателя имелся прообраз данных. С этой целью предлагается следующий вариант обработки данных со стороны получателя.

Известно, что все двоичные числа имеют свой вес, то есть характеризуются этим параметром, и по которому их можно разбить на множества чисел, каждое из которых имеет одинаковый вес для всех относящихся к нему чисел. Структурирование этих множеств привело к построению матриц треугольного вида, в которых числа упорядочены по возрастанию, а сама организация матриц представляет собой таблицу в виде столбцов и строк, причем в первом столбце находятся по порядку увеличения их значений нечетные числа, а в других, начиная со второго четные числа. Подход к организации этих матриц получен в [48], а пример их группирования для весов $W = 2$ u $W = 3$ представлен на рисунке 3.3.

$w = 2$

№	НОМЕРА ПОДМАТРИЦ						
	1	2	3	4	5	6	7
1	3	6	12	24	48	96	192
2	5	10	20	40	80	160	
3	9	18	36	72	144		
4	17	34	68	136			
5	33	66	132				
6	65	130					

$w = 3$

№	НОМЕРА МАТРИЦ					
	1	2	3	4	5	6
1	7	14	28	56	112	224
2	11	22	44	88	176	
3	13	26	52	104	208	
4	19	38	76	152		
5	21	42	84	168		
6	25	50	100	200		
7	35	70	140			
8	37	74	148			
9	41	82	164			
10	49	98	196			
11	67	134				
12	69	138				
13	73	146				
14	81	162				
15	97	194				

Рисунок 3.3 Организация таблиц десятичных чисел с весами $W = 2, W = 3$

Заполнение таблиц происходит по строкам, причем числа строк и столбцов образуются из исходного числа, находящегося в первом столбце путем их умножения на двойку, начиная с числа первого столбца, которое называется числом, образующим строки (ЧОС). В такой таблице, имеющей треугольный характер, все числа одного веса упорядочены и имеют координаты. Этому способствует разделение матрицы на подматрицы, количество которых фиксировано. Такая организация позволяет указать местоположение числа с заданным весом, задавая его координаты в виде вектора $T = (w, N_{иос}, N_{n/m})$, где w - вес матрицы числа, $N_{иос}$ - номер ЧОС, то есть, номер строки, в которой она находится, $N_{n/m}$ - номер подматрицы его содержащее.

Таким образом, на пересечении строки ЧОС и номера подматрицы (номер столбца, который ее содержит) находятся необходимые координаты кодируемого числа. Возможность указания координат чисел с заданным весом в соответствующей таблице позволяет определить прообраз передаваемого числа, выбрать его и установить его достоверность для случая, когда полученное число

восстанавливается методом матричного декодирования. Отсюда появляются два способа получения достоверности передачи данных, включающего в себя:

1. Матричное декодирование и поиск полученного образа путем просмотра его точного совпадения или близкого соответствия по мажоритарному принципу в столбце матрицы Паскаля с номером передаваемого веса;
2. Вместе с весом числа передаются координаты прообраза в таблице с этим же весом. В этом случае появляется дополнительная избыточность, которая увеличивает длину декодируемых данных.

В первом случае затрачивается время на восстановление матричного кода и последующее его сравнение с прообразом в матрице Паскаля. Во втором случае требуется время на выборку таблицы с переданным весом и поиск в ней по указанным координатам местоположения прообраза.

Если же образ кода и прообраза не совпадают, то в этом случае принимается решение о сравнении числа, найденного в матрице Паскаля после декодирования, и числа, найденного в матрице с заданным весом. Если ни одно из сравнений не получило полного соответствия, то в этом случае из двух выбранных чисел выбирается то, которое является ближайшим, то есть образ отличается от прообраза на меньшее количество битовых несовпадений. Такой подход к декодированию и обнаружению местоположения ошибок относится к комбинаторному подходу, который в настоящее время считается особенно эффективным.

Отдельно отметим, что смысл контроля, как указывалось выше, состоит в поэлементном сравнении веса в отправленном коде и весом в полученном коде числа. Если веса не совпадают, то принимаемая комбинация блокируется и требуется передача снова. На практике в этом случае пользуются кодами с повторениями, которые позволяют обнаруживать ошибки любой кратности.

Однако такие коды обладают высокой избыточностью, и для полного обеспечения достоверности получаемых данных используют кратность повторений (но не более трех). В нашем случае, также возможно, использовать подход с повторением для обнаружения ошибок в принятом коде числа. Для этого нужно кодировать передаваемое число с другим весом и после его получения и декодирования сравнить с тем же числом, принятым ранее. Преимуществом этого приема является то, что повторение кодированных данных может осуществляться кодом с наименьшей длиной среди всех равных ему по величине чисел, но с другим весом, что в итоге уменьшает избыточность на стадии обнаружения ошибок.

Отдельно рассмотрим вариант повторения отправки кода числа, когда у первых отправленных данных вес меньше чем в повторении. То есть в первом сообщении число единиц меньше, чем во втором. Однако на практике вероятность ошибки в переходе $0 \to 1$ меньше чем $1 \to 0$, хотя и наиболее уязвимыми при передаче по зашумленному каналу считаются сигналы низкого уровня, которые представляют собой коды нулей. Поэтому коды с меньшим весом имеют большую вероятность того, что у них имеется искажение данных.

Таким образом, отправитель формирует данные в виде потока целых неотрицательных чисел заданного веса, причем коды чисел состоят из веса числа, для которого отводится число бит равных максимальному значению веса чисел в диапазоне множества возможных, исходя из размеров телеметрических данных. Вторая часть кода представляет собой любое закодированное целое число, либо его номер в множестве чисел (таблице) заданного веса. Структура такого кода представлена ниже:

Вес числа	Число N (номер)

Очевидно, что максимальное количество бит определяет максимальный вес числа, заданного в двоичном коде - $l_{чис.}$. Тогда длина кодовой последовательности будет определяться как $L = L_{чис.} + L_{вес.}$, где $L_{чис.}$ - при матричном кодировании равен $L_{чис.} = \log_2 N + 1$, а длина веса будет определяться как $Lx_{вес.} = \log(\log_2 N + 1)$.

Рассмотрим пример: $N = 43$. При $W = 3, L = 8\,бит$ код будет иметь длину равную $L_{код} = 3 + log8 = 6\,бит$, максимальное значение при $N_{\max} = 1024$ длина кода будет равна $L = \log 1024 + \log 10 \approx 14\,бит$. В случае, если вес самого числа отправляется с его координатами вместе с весом, то избыточность будет выражаться в длине передаваемых данных.

Приведем пример построения данных, с использованием координат прообраза передаваемого числа. Пусть $N = 31$, то его табличные координаты в таблице с весом $W = 5$, с номером в столбце ЧОС 1. Тогда сообщение о передаче прообраза, а именно $N = 31$ будет выглядеть, как $M_a = (5,1,1)$ - третья координата подматрицы матрицы с весом $W = 5$, указывает на первый столбец, так как число нечетное и для них выделен только первый столбец.

Дополнительная избыточность в виде координатных позиций служит для контроля правильности полученных данных и в принципе является частью нумерационного кодирования, то есть расширением части данных, которые

следует за весом. Тогда само число передавать не нужно. Передавать нужно только вес плюс три координаты, вес обнаружения факта ошибки и координаты ее местоположения. Схема организации декодирования для рассмотренного варианта представлена на рисунке 3.4.

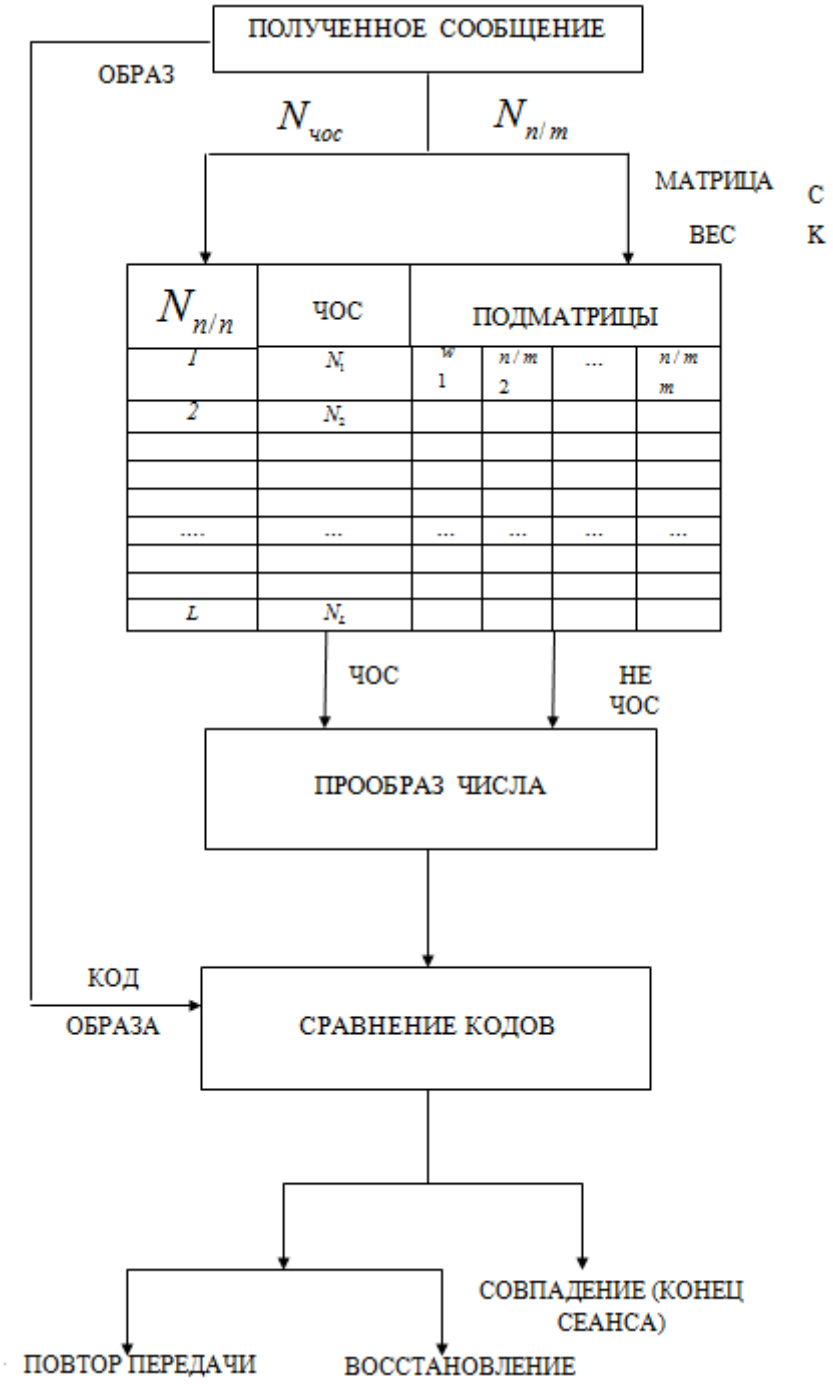

Рисунок 3.4 Обработка данных на стороне получателя

Алгоритм декодирования данных с ошибкой по способу использования данных из матрицы Паскаля и матрицы чисел с фиксированными весами представлен на рисунке 3.5.

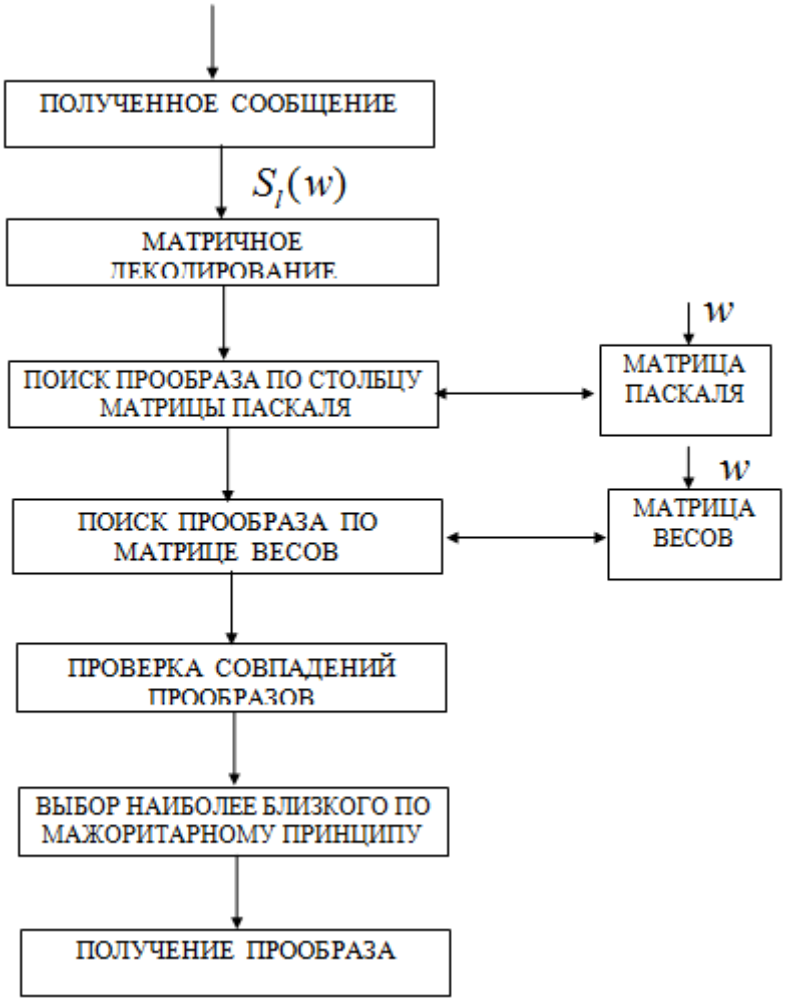

Рисунок 3.5 Алгоритм поиска прообраза данных по двум матрицам

Исходя из вышеизложенного, следует вывод об эффективности описанного метода применительно к высокоскоростным каналам передачи данных, поскольку разработанный метод кодирования целого числа с помощью матрицы Паскаля позволяет быстро и эффективно по прообразу восстановить его при отправке по зашумленному каналу, на который воздействуют различные помехи.

3.7.1 Определение координат кодируемых чисел в матрицах весов

«Процедура определения порядкового номера ЧОС в матрице опирается на разбиения двоичного эквивалента десятичного числа M_{10} с заданным весом W на фрагменты числа, которые образуются по следующему правилу: исходный двоичный код сдвигается влево до тех пор, пока на его крайней левой позиции не появится единица, при этом эта единица и стоящая справа последовательность нулей отбрасывается. Исходный двоичный код уменьшается по длине. После

сдвига полученный фрагмент подвергается обработке с учетом веса числа (матрицы) и веса фрагмента по формуле:

$$p_i = C_{l-2}^{w-1}, \qquad (3.4)$$

где p_i - порядковый номер фрагмента, l - длина фрагмента в битах, $i = \overline{1;q}, q -$ число формируемых фрагментов в процессе разбиения числа N_2» [50].

Окончательно порядковый номер ЧОС определяется по формуле:

$$p = \sum_{l=1}^{q} p_i + 1.$$

Пример. Пусть $M_{10} = 45, M_2 = 101101, l = 6, w = 4.$

1 шаг. Произведем расчет $p_1 = C_{l-2}^{w-1} = C_{6-2}^{4-1} = C_4^3 = 4$. «Осуществляем сдвиг двоичного кода M_2 влево на 2 позиции и получаем первый фрагмент числа $M_2^1 = 1101, l = 4, w = 3$ » [51].

2 шаг. Вычисляем $p_2 = C_{4-2}^{3-1} = 1$. «Производим сдвиг двоичного кода M_2^1 влево и формируем второй фрагмент $M_2^2 = 101, l = 3, w = 2$» [46].

3 шаг. Вычисляем $p_3 = C_1^1 = 1$.

4 шаг. Окончательно

$$p = \sum_{1}^{3} p_i + 1 = 4 + 1 + 1 + 1 = 7.$$

Поскольку «ЧОСы расположены в вектор-столбце в порядке возрастания их значений» [49], следовательно, значения их порядковых номеров также должны увеличиваться. Достаточно очевидно, что «чем больше нулей в двоичном коде, причем, даже если единицы расположены на младших разрядах, то тем меньше будет фрагментов разбиений, при этом они создают меньшую суммирующую составляющую» [50].

3.7.2 Определение порядкового номера числа, образующего строку, внутри подматрицы

Представляет практический интерес определение порядкового номера ЧОС в подматрице, которой он принадлежит. В основу способа вычисления порядкового номера ЧОС в подматрице ($N_{ЧОС_{n/m}}$) положено представление ЧОС в двоичном виде и проведение пошагового процесса вычисления биномиальных коэффициентов с учетом основных параметров двоичных кодов – веса кода и веса последовательности.

Для этого необходимо произвести расчет количества элементов во всех подматрицах, в которых находится искомый ЧОС. На каждом шаге требуется контролировать количество «просчитанных ЧОС», так чтобы оно не превысило значения порядкового номера ЧОС в самой матрице $n_{ЧОС}$. Отсюда требуется предварительно знать количество ЧОС - $n_{ЧОС}$ в подматрице.

Пошаговая операция определения количества ЧОС в каждой подматрице имеет вид:

$$n_{ЧОС_{n/m}} = C^{w-2}_{N_{n/m+}+w-3},$$

где w – вес ЧОС, $N_{n/m}$ – номер подматрицы в матрице.

Номер подматрицы $N_{n/m}$ для заданного ЧОС – $M_{ЧОС}$ в матрице определяется следующим образом:

$$N_{n/m} = [\log_2 M_{ЧОС}] - (w-2),$$

где $M_{ЧОС}$ – рассматриваемое ЧОС.

В целом процедура вычисления номера ЧОС в подматрице $N_{ЧОС_{n/m}}$ носит циклический характер и представлена алгоритмом на рисунке 3.10. При переходе к очередным подматрицам, подсчитанное количество ЧОС в рассмотренных ранее подматрицах, суммируется и на каждом шаге цикла обработки одной подматрицы осуществляется проверка на превышение текущего значения количества ЧОС - S_i значению порядкового номера ЧОС в матрице, т.е. идет проверка $S_i < N_{ЧОС_М}$.

Если в результате проверки условие выполняется, то процесс подсчета количества ЧОС продолжается по формуле $S_{i+1} = S_{i-1} + S_i$. В противном случае выполняется получение результата по формуле $N_{ЧОС_{n/m}} = N_{ЧОС_М} - S_i$. Алгоритм определения номера ЧОС в подматрице представлен на рисунке 3.6.

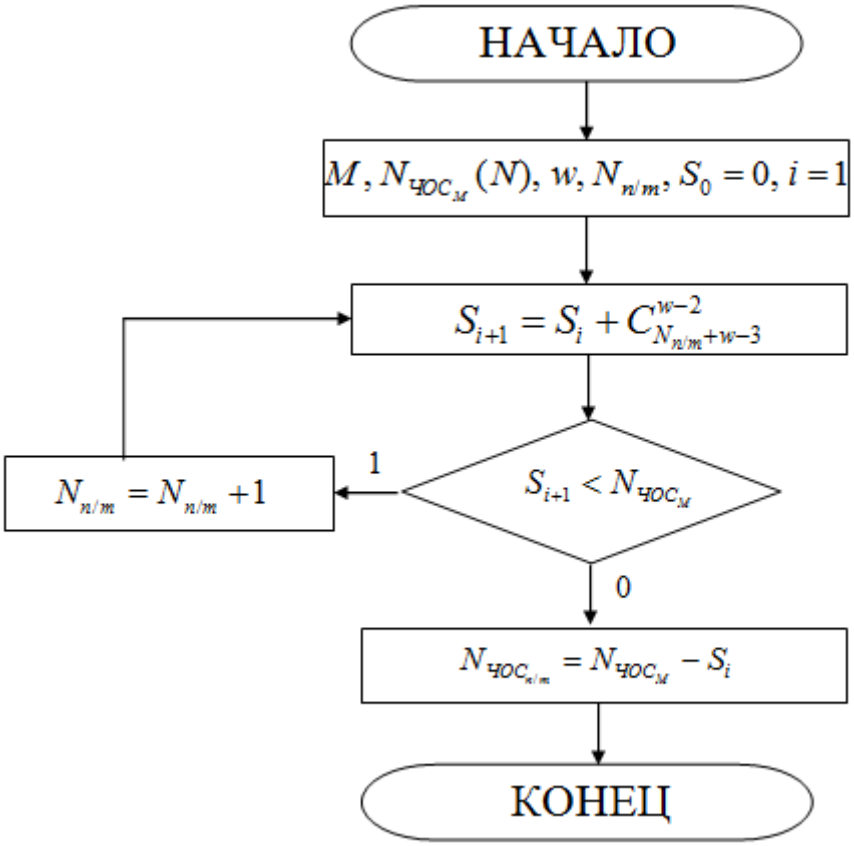

Рисунок 3.6 Алгоритм определения номера ЧОС в подматрице

Пример. Пусть $M_{10} = 25, M_2 = 11001, l = 6, w = 3.$ Определим местоположение ЧОС $M = 25$ в подматрице (номер $N_{ЧОС_M}$ предварительно определен по выражению (3.4), поэтому эти вычисления опускаются) [48, 50].

1 цикл: задаем номер подматрицы $N_{n/m} = 1, S_0 = 0$. Вычисляем S_1.

$$S_1 = C^{w-2}_{N_{n/m}+w-3} = C^{3-2}_{1+3-3} = 1;$$
$$S = S_0 + S_1 = 1.$$
$$S < N_{ЧОС_M} \rightarrow 1 < 6.$$

2 цикл: $N_{n/m} = 2$.

$$S_2 = C^{3-2}_{2+3-3} = 2;$$
$$S = S_1 + S_2 = 1 + 2 = 3.$$
$$S < N_{ЧОС_M} \rightarrow 3 < 6.$$

3 цикл: $N_{n/m} = 3$.

$$S_2 = C_{3+3-3}^{3-2} = 3;$$
$$S = S_1 + S_2 + S_3 = 3 + 3 = 6.$$
$$6 = 6.$$

Условие не выполняется, следовательно, номер ЧОС - $M_{10} = 25$ в третьей подматрице равен:

$$N_{ЧОС_{n/m}} = N_{ЧОС_m} - S = 6 - 3 = 3.$$

3.8 Выводы по третьей главе

1. Рассмотрены известные модели каналов передачи данных, и показано, что они носят числовой потоковый параметрический характер в пакетной форме. Установлено, что модели с достаточной точностью отражают специфику зашумленных каналов передачи данных и основным требованием к ним являются требование высокого быстродействия, вызванное ограниченностью времени сеанса обмена телеметрическими данными и временными затратами на выполнение процедур обнаружения ошибок в закодированных данных и восстановления их с заданной достоверностью.

2. Обосновано применение кодов с переменным весом в виде эффективного быстрого средства обнаружения и исправления ошибок. Коды с переменным весом позволяют быстро и эффективно обнаруживать любые одиночные ошибки (в том числе одиночные ошибки различной кратности). Преимуществом кодов с переменным весом является эффективность их использования в современных каналах передачи данных при условии быстрой генерации двоичными кодами чисел с переменными весами.

3. Предложен эффективный численный метод вычисления веса целого десятичного числа (с помощью которых кодируются телеметрические данные) и определение позиций единиц, который может быть применен для идентификации получаемых образов данных, представленных кодами переменного веса на этапе декодирования на стороне получателя.

4. Для построения генератора кодов с переменными весами предложено использовать матрично-алгоритмический подход к кодированию целых чисел на основе использования матрицы Паскаля. Исходными данными для генерации являются: задаваемый вес исходного числа и само число, при этом вес определяется выбором номера столбца матрицы Паскаля, а получение двоичного

кода происходит в процессе формирования пути на поле чисел матрицы по введенному правилу.

5. Разработаны новые удобные формы представления алгоритмов матрично-алгоритмического кодирования и декодирования в виде специальных матричных диаграмм, которые позволяют эффективно работать с числами матрицы Паскаля и данными, представленными кодами с переменным весом. Разработана процедура и средства обнаружения фактов искажений целостности данных, вызванных канальными помехами и влиянием внешней среды. Представлен процесс восстановления этих данных с высокой достоверностью на основе применения матриц Паскаля для генерации кодовых данных и матриц чисел с фиксированными весами для получения их прообраза за счет быстрых матричных вычислений.

ГЛАВА 4. РАЗРАБОТКА ПОДСИСТЕМЫ ОЦЕНКИ РИСКА ВОЗНИКНОВЕНИЯ ПОВТОРНЫХ ОШИБОК, ВЫЗВАННЫХ СБОЯМИ ПРИЕМНОЙ АППАРАТУРЫ И ПРОГРАММНЫХ СРЕДСТВ

Из-за длительной эксплуатации и удаленности приемника СППД, невозможности проведения постоянных регламентных, профилактических и ремонтных работ надежность корректного функционирования приемной аппаратуры ухудшается, что приводит к возникновениям неисправностей и ошибок в ней при обработке полученных данных. Не учет этих отрицательно действующих факторов может привести к неточностям в управлении событиями в СППД и вызвать неправильную ответную реакцию, а также утерять надежную связь с центром управления.

В четвертой главе разработана математическая модель подсистемы оценки риска повторных ошибок, вызванных сбоями приемной аппаратуры и программных средств. Отличительной особенностью разработанной математической модели от известных является использование в рисковой системе сигмовидной функции Гомперца [52, 53], позволяющей учитывать угрозы нарушения целостности данных, возникающих на начальной и завершающей стадиях обмена данными. В известных моделях оценки риска возникновения повторных ошибок используется распределение Вейбула [54-57], которое в недостаточной степени учитывает группирование ошибок на начальных и конечных стадиях сеанса обмена данными. В случае применения сигмовидной функции Гомперца появляется возможность учитывать указанные обстоятельства, что позволяет обнаруживать местоположения пачек ошибок, наибольшую вероятность присутствия этих ошибок на интервале сеанса обмена данными, а также сократить время на поиск местоположения сгруппированных ошибок и высвобождает время для проведения дополнительных мероприятий по восстановлению переданных данных с необходимой точностью.

4.1 Разработка подсистемы оценки риска возникновения повторных ошибок, вызванных сбоями приемной аппаратуры и программных средств

Определим набор параметров, который необходимо учесть при разработке математической модели подсистемы оценки риска повторного возникновения ошибок в пакетах данных после их поступления в приемное устройство СППД, а именно:

- полноту данных;
- управляемость процессами контроля и выявления возникновения повторных ошибок в передаваемых пакетах данных;
- агрегируемость данных (возможность перехода от единичных параметров к комплексным или интегральным).

Разработана структурная схема функционирования системы обеспечения целостности данных, в основе которой лежат взаимодействующие между собой подсистемы обнаружения признаков несанкционированного доступа, подсистемы обеспечения целостности телеметрических данных на основе кодов с переменным весом, подсистемы оценки риска повторных ошибок, вызванных сбоями приемной аппаратуры и программных средств. Структурная схема функционирования системы обеспечения целостности данных (СОЦД) представлена на рисунке 4.1.

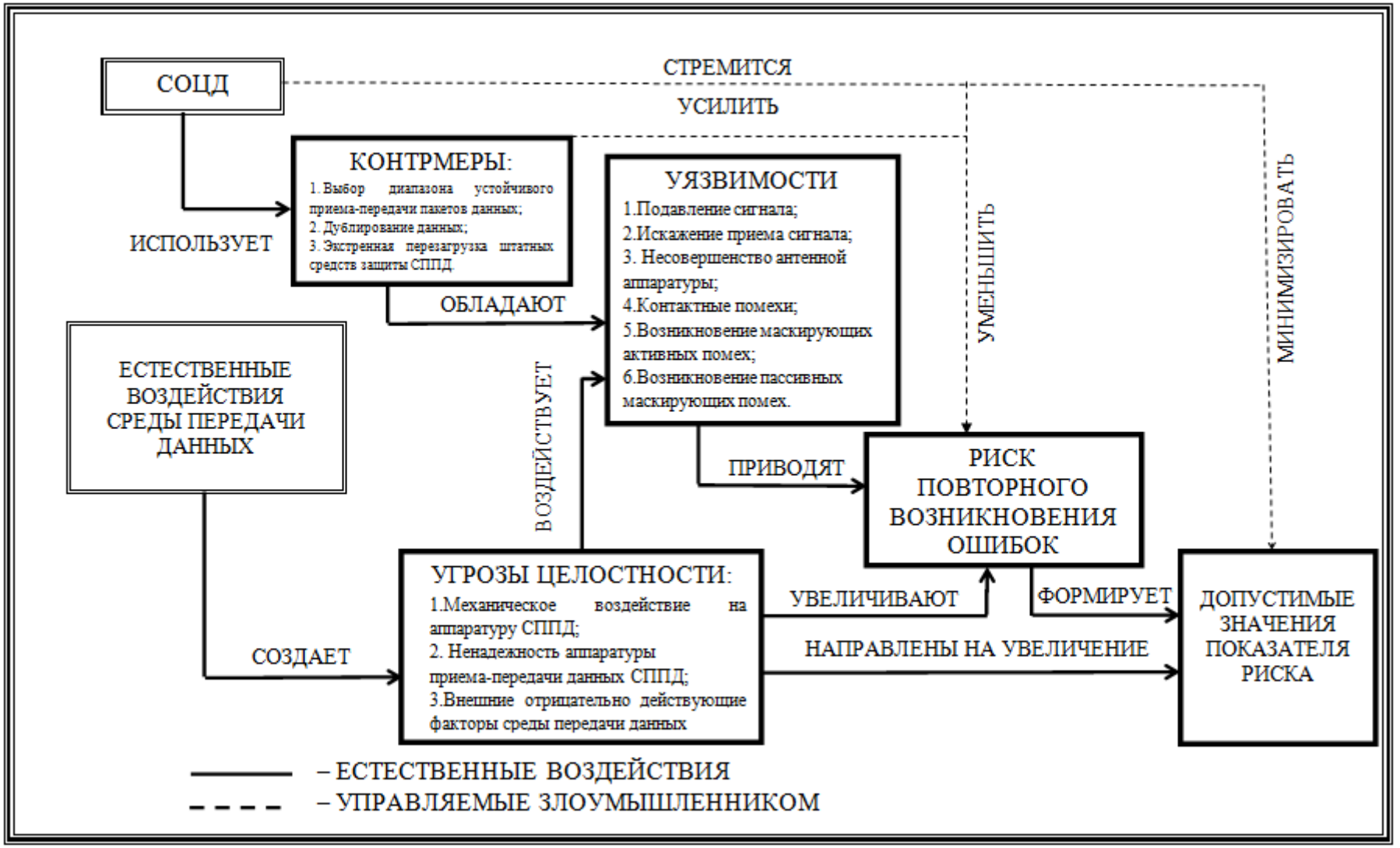

Рисунок 4.1 Структурная схема функционирования СОЦД

Для качественного и эффективного противодействия угрозам нарушения целостности данных СОЦД использует контрмеры, а именно [58, 59]:

- в автоматическом режиме осуществляет выбор устойчивого диапазона передачи-приема данных;

- дублирует поступившие данные;

- производит экстренную перезагрузку средств защиты в случае возникновения нештатной ситуации.

Следует отметить, что используемые контрмеры обладают рядом значительных уязвимостей, а именно, в случае подавления (искажения**)** принимаемого сигнала штатные средства защиты не способны необходимым образом противостоять дестабилизующему фактору, который воздействует на приёмное устройство СППД, в результате чего возникает вероятность программно-аппаратной ошибки, появление которой в канале передачи данных может привести к нарушению целостности пакета данных.

СППД при работе в сложных условиях подвержена воздействию среды передачи данных (оптоволоконные линии, радиолинии, линии спутниковой связи), которая при длительной эксплуатации может в условиях невозможности проведения ремонтно-профилактических работ привести к сбоям и отказам оборудования [60-63]. Критерием эффективности является снижение показателя риска нарушения целостности защищаемых данных. Представим модель подсистемы оценки риска повторного возникновения обнаруживаемых ошибок в пакетах данных в виде следующей трехуровневой структуры (рисунок 4.2).

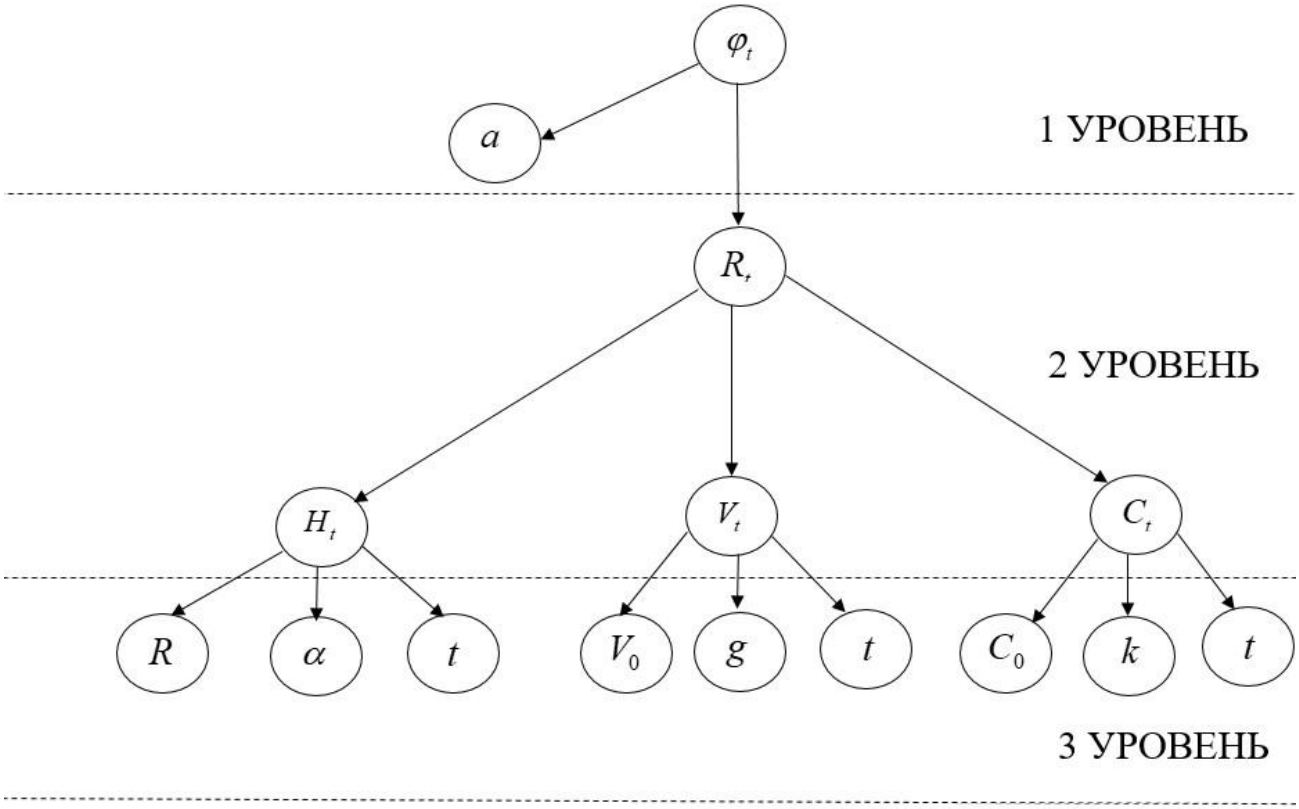

Рисунок 4.2 Структура трехуровневой модели подсистемы оценки риска повторного возникновения ошибок

На рисунке представлена структура трехуровневой модели подсистемы оценки риска повторного возникновения ошибок на стадии обработки. На нижнем (третьем) уровне располагаются параметры управления, являющимися входными «параметрами для приведения моделирования, а именно: коэффициент моделирования $R > 0$, параметр управления риском $\alpha > 0$, начальное состояние уязвимости системы $V_0 > 0$, параметр управления уязвимостью $g > 0$, начальное состояние резерва мощности $C_0 > 0$, параметр управления резервом $k > 0$» [53].

На среднем (втором) уровне расположены следующие параметры модели, а именно: «Риск нарушения целостности данных, описываемый функцией Гомперца H_t», «Уязвимость СОЦД V_t», «Резервная мощность СОЦД C_t», «Риск повторного возникновения ошибок R_t» [53].

На первом уровне расположена функциональная зависимость φ_t, которая определяет компромисс между средним риском в системе и начальными скоростями роста резерва и уменьшения уязвимости системы.

Для построения соответствующих функциональных зависимостей использованы следующие параметры [53]:

1. Риск нарушения целостности данных, описываемый функцией Гомперца H_t:

$$H_t = R \cdot e^{\alpha \cdot t}, \tag{4.1}$$

где коэффициент моделирования $R > 0$, параметр управления риском $\alpha > 0$.

Выбор функции Гомперца обусловлен необходимостью описания интенсивного роста повторного возникновения, как единичных ошибок, так и их комбинаций на начальной и завершающей стадиях функционирования СППД.

2. Уязвимость СОЦД V_t:

$$V_t = \frac{V_0}{1 + t \cdot g}, \tag{4.2}$$

где начальное состояние уязвимости системы $V_0 > 0$, параметр управления уязвимостью $g > 0$.

3. Резервная мощность СОЦД C_t, определяемая как:

$$C_t = C_0 + k \cdot t, \tag{4.3}$$

где начальное состояние резерва мощности $C_0 > 0$, параметр управления резервом $k > 0$.

Риск повторного возникновения ошибки с учетом представленных выше выражений (4.1) – (4.3) определяется следующим образом [52, 53]:

$$R_t = \frac{H_t \cdot V_t}{C_t}. \tag{4.4}$$

На рисунке 4.3 представлена функция риска повторного возникновения ошибок после исправления нарушений целостности, полученная в результате экспериментов по формуле (4.4).

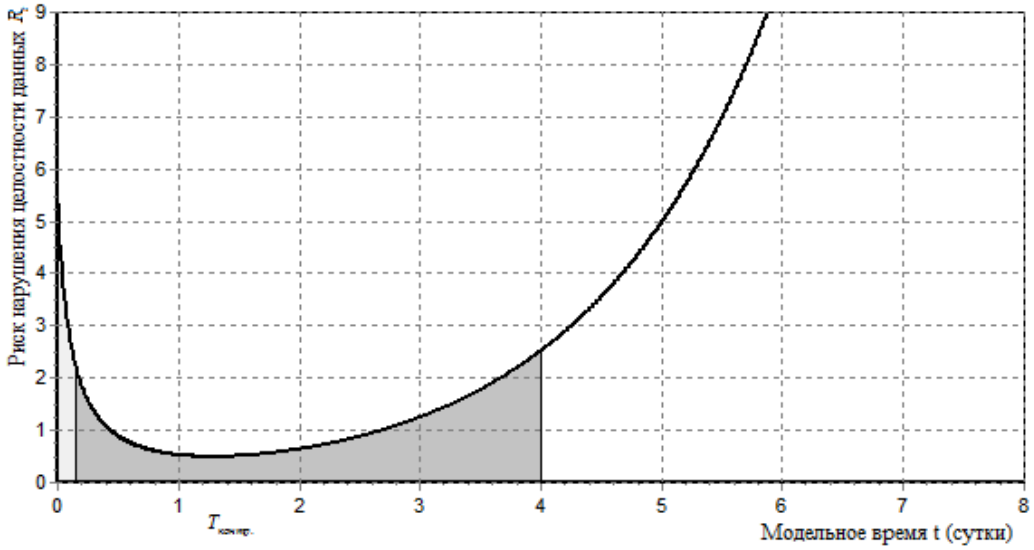

Рисунок 4.3 Риск повторного возникновения ошибок

Функция риска, которая определена выражением (4.4), обеспечивает наличие экстремума на соответствующем графике (рисунок 4.4). В результате анализа рисунка 4.4 следует вывод, что во временном диапазоне $T_{\text{контр.}}$ риск повторного возникновения ошибки принимает допустимые для своего показателя значения. На практике корректное время сеансовой работы СППД составляет ограниченное время, установленное стандартами, после окончания которого, происходит перезагрузка штатных средств защиты.

Функциональная зависимость φ_t, определяющая допустимые значения риска нарушения целостности, задается выражением: [53]

$$\varphi_t = k \cdot g \cdot t + R_t \cdot a, \tag{4.5}$$

где коэффициенты моделирования $k > 0$, $g > 0$, параметр управления $\alpha > 0$.

В случае роста уязвимости и снижения резерва мощности функциональная зависимость, определяющая допустимые значения риска повторного возникновения обнаруженной ошибки, примет вид [53]:

$$\varphi_t = k \cdot g \cdot t + \frac{a}{t} \cdot \int_0^T R_t \, dt. \tag{4.6}$$

На рисунке 4.4 показан график, иллюстрирующий характер поведения компромисса между средним риском в системе и начальными скоростями роста резерва и уменьшения уязвимости системы (4.6).

Рисунок 4.4 Функциональная зависимость φ_t

При работе СППД в течение сформированного временного диапазона (рисунок 4.3) построенная система оценки рисков способна определить критические значения вероятности нарушения целостности передаваемых данных.

В работе предложена структура СОЦД на основании комплексного подхода к обеспечению целостности передаваемых данных, которая служит основой для проведения имитационного моделирования и получения результатов оценки интенсивностей поступивших пакетов данных, интенсивностей принятых к обработке пакетов данных, интенсивностей, находящихся в очереди и ожидающих обработки пакетов данных. На рисунке 4.5 представлена предложенная в настоящей работе структурная схема СОЦД.

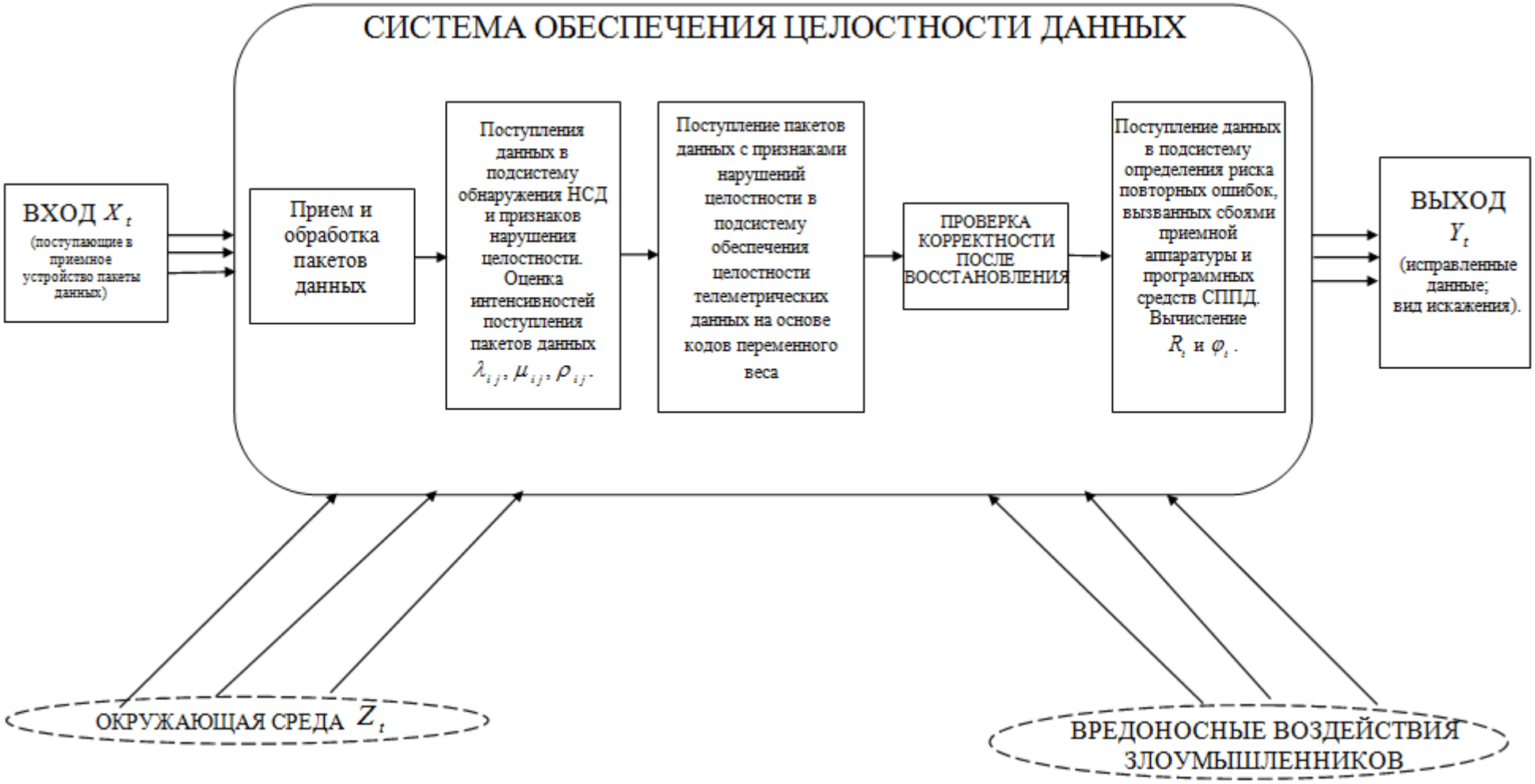

Рисунок 4.5 Структурная схема системы обеспечения целостности данных

Для имитационного моделирования использовался язык программирования C# и среда разработки программного обеспечения Visual Studio 2013. Оценка интенсивности поступивших в систему пакетов данных λ_t, оценка интенсивности принятых к обработке пакетов данных μ_t, оценка интенсивности, находящихся в очереди и ожидающих обработки пакетов данных ρ_t, определены при фиксированном значении компенсатора $I\left(Q_t = k\right)$ и модельном времени t (время моделирования измеряется в минутах). В результате проведения имитационного моделирования получены графики оценок соответствующих интенсивностей (рисунок 4.6). На рисунке 4.6 представлен разработанный пользовательский интерфейс. Из графиков на рисунке 4.6 видно, что пакеты данных поступают в систему с определенной периодичностью без существенных отклонений на протяжении заданного времени моделирования. Это означает, что система полностью справляется с поступающим потоком данных, и при их увеличении работает без каких-либо сбоев и задержек.

Полученные в результате имитационного моделирования функциональные зависимости сходны с графиками функции Бесселя (канонические решения дифференциального уравнения Бесселя), которые применяются при обработке различных сигналов [64-67]. Выявленное сходство позволяет сделать вывод о том, что система с достаточной точностью способна имитировать работу реальной СППД, при этом разработанное программное обеспечение позволяет исследовать различные штатные и нештатные режимы работы СППД, изменяя условия прохождения пакетов данных по трактам СППД с учетом отрицательного воздействия факторов внутренней и внешней среды. Также с его помощью можно вводить различные временные и количественные ограничения, способствующие более детальному изучению свойств реальной аппаратуры при поступлении на приёмное устройство СППД значительного количества пакетов данных.

Для моделирования разработанной системы оценки рисков повторного возникновения ошибок использовалась среда разработки DELPHI 7 и язык программирования Pascal. На рисунке 4.7 представлен пользовательский интерфейс разработанного программного обеспечения.

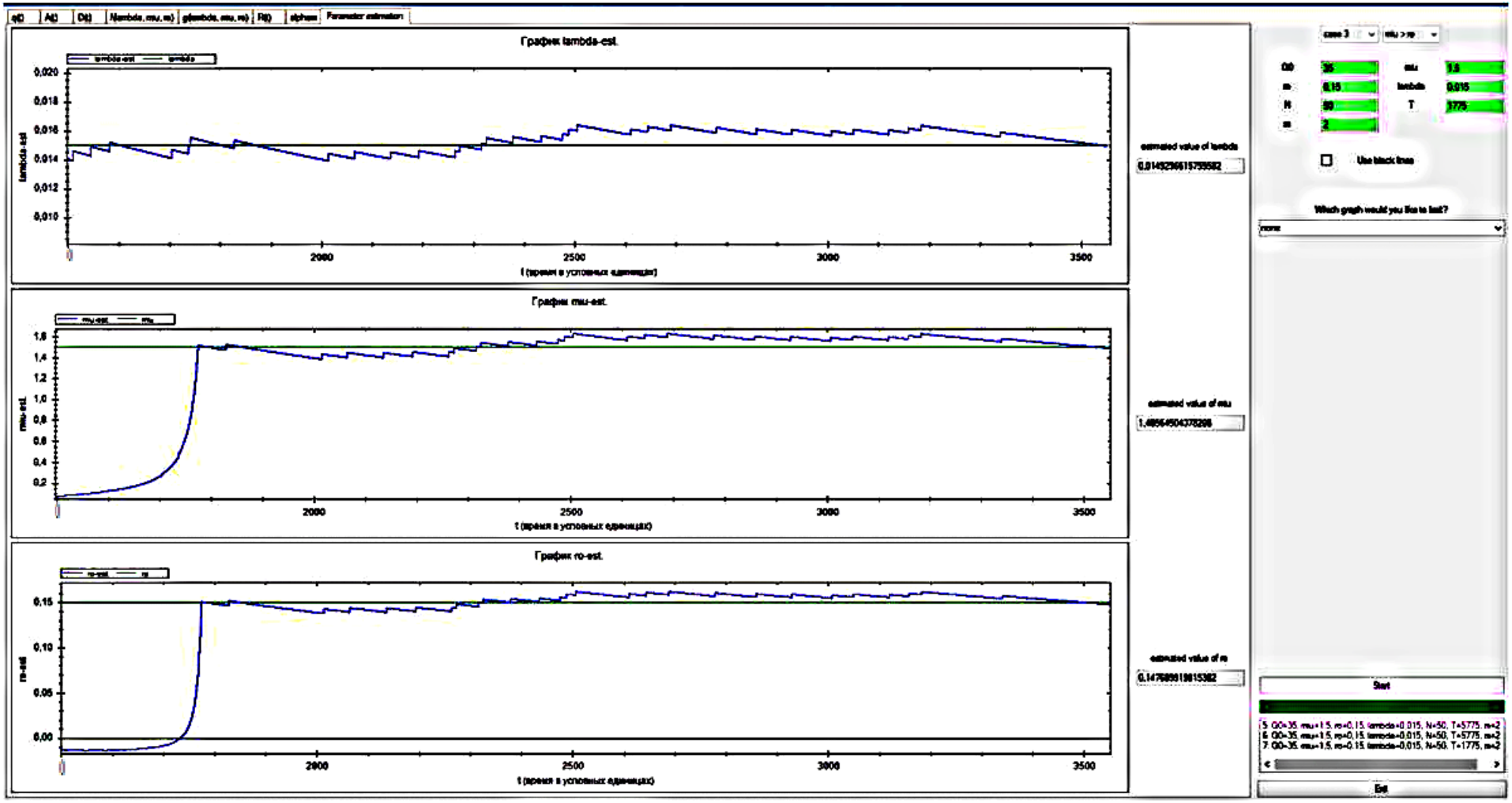

Рисунок 4.6 Пользовательский интерфейс разработанного программного обеспечения

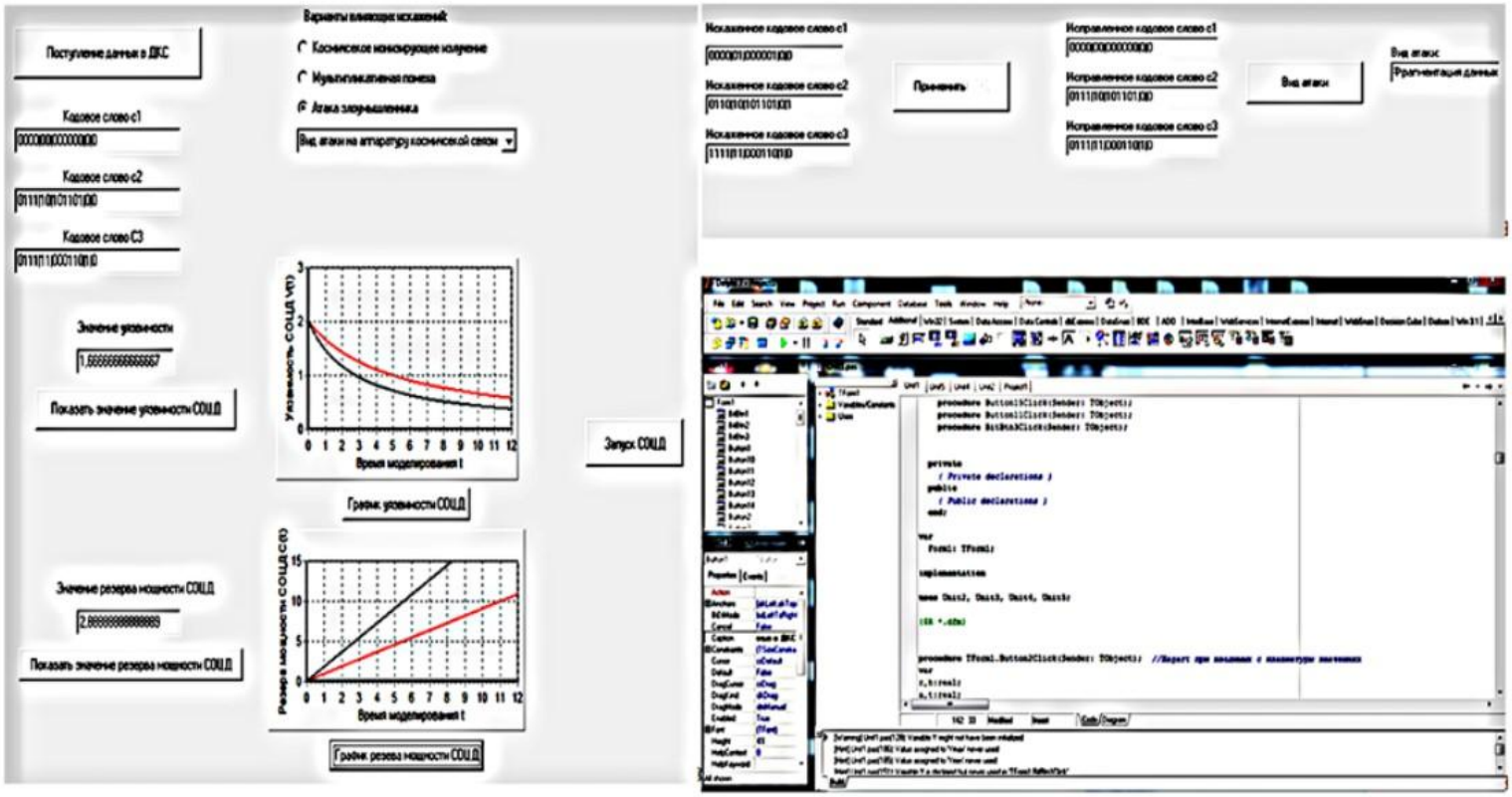

Рисунок 4.7 Пользовательский интерфейс разработанного программного обеспечения

Для запуска программы необходимо активировать кнопку «поступление данных в ДКС», после чего происходит формирование кодовых последовательностей, которые подаются на вход СОЦД. В результате воздействия (атаки) злоумышленника происходит нарушение целостности принимаемых данных. В программе предусмотрено приложение, которое предупреждает о нарушении целостности, поступивших в СОЦД пакетов данных. На рисунке 4.7 в окнах Chart1 и Chart2 построены кривые, иллюстрирующие рост уязвимости и снижение резерва мощности СОЦД при приеме искаженных данных (черным цветом обозначены допустимые значения, а красным – значения при приеме искаженных данных). При активации кнопки «запуск СОЦД» происходит вывод искаженных кодовых последовательностей. Обнаружение и исправление ошибок осуществляется при помощи кодов с переменным весом (для исправления ошибочных символов необходимо активировать кнопку «применить»). После этого происходит определение вида искажения и исправление нарушений целостности данных.

При разработке соответствующего программного приложения учитывается возможность увеличения числа угроз нарушения целостности данных и вероятность возникновения, как единичных аддитивных ошибок различной кратности, так и их комбинаций. Алгоритм работы разработанного программного приложения представлен на рисунке 4.8.

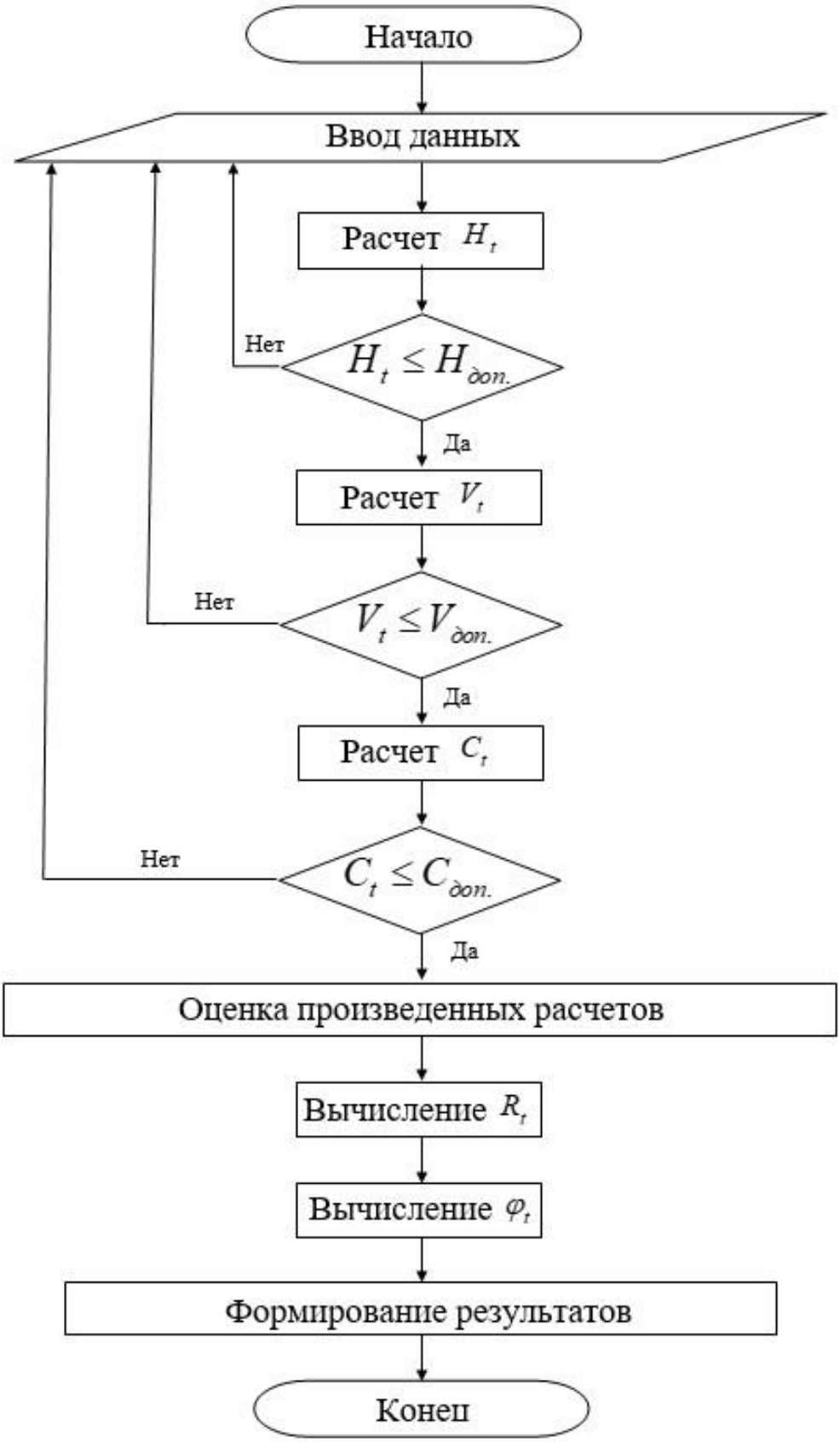

Рисунок 4.8 Блок-схема алгоритма работы подсистемы оценки риска повторных ошибок, вызванных сбоями приемной аппаратуры и программных средств СППД

Рассмотрим примерную методику применения разработанного алгоритма на практике:

1. На начальном этапе работы алгоритма определяются входные данные: параметры управления и начальные состояния уязвимости и резерва мощности СОЦД.

2. Производится расчет риска нарушения целостности данных, описываемого функцией Гомперца. Для его расчета необходимо задать соответствующий коэффициент и параметр управления.

3. Рассчитывается уязвимость СОЦД: задается начальное состояние и соответствующий параметр управления.

4. Вычисляется резерв мощности СОЦД (определяется начальное состояние), а также осуществляется оценка произведенных расчетов.

5. Производится вычисление риска повторного возникновения ошибок;

6. На завершающей стадии работы алгоритма осуществляется расчет значений построенных функциональных зависимостей, для чего задаются соответствующие коэффициенты и параметры управления. Затем формируются соответствующие результаты произведенных расчетов, а также построение графических решений.

Разработанная программа для проведения имитационного моделирования выводит на экран результаты численного моделирования в виде графиков. На рисунке 4.9 представлен пример пользовательского интерфейса, управляющего программой, реализующей имитационную модель СОЦД, согласно методике, изложенной выше.

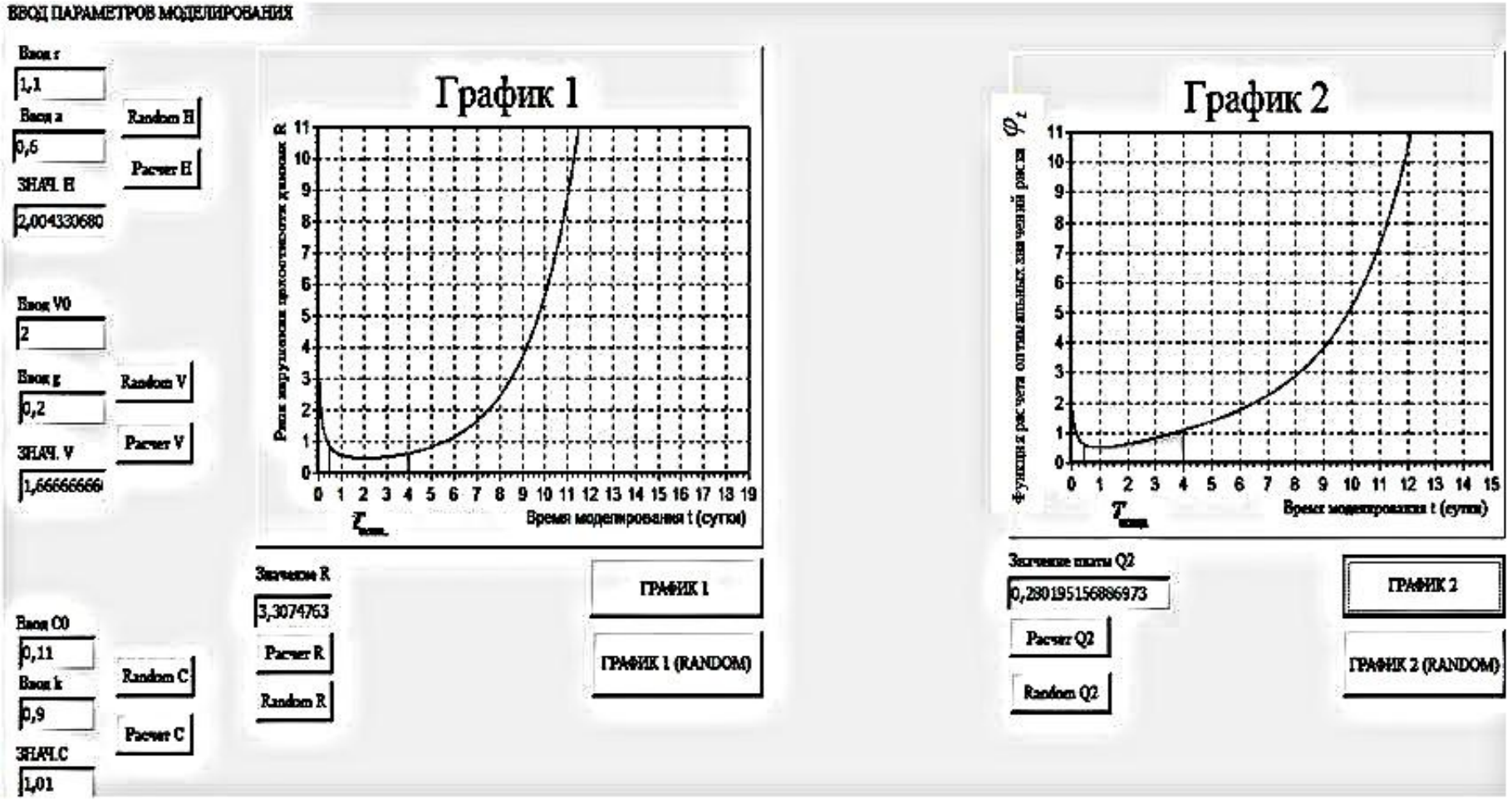

Рисунок 4.9 Пример пользовательского интерфейса разработанного программного обеспечения

Имитационное моделирование производилось в среде разработки Delphi 7 на языке программирования C#. Модель реализована с использованием принципов объектно-ориентированного программирования.

В случае увеличения риска возникновения повторных ошибок в имитационной модели предусмотрено выработка данных, предупреждающая о росте возможных угроз. Такая система указывает на необходимость предпринять контрмеры, например, осуществить экстренную перезагрузку системы [68-73]. Пример подобной ситуации представлен на рисунке 4.10.

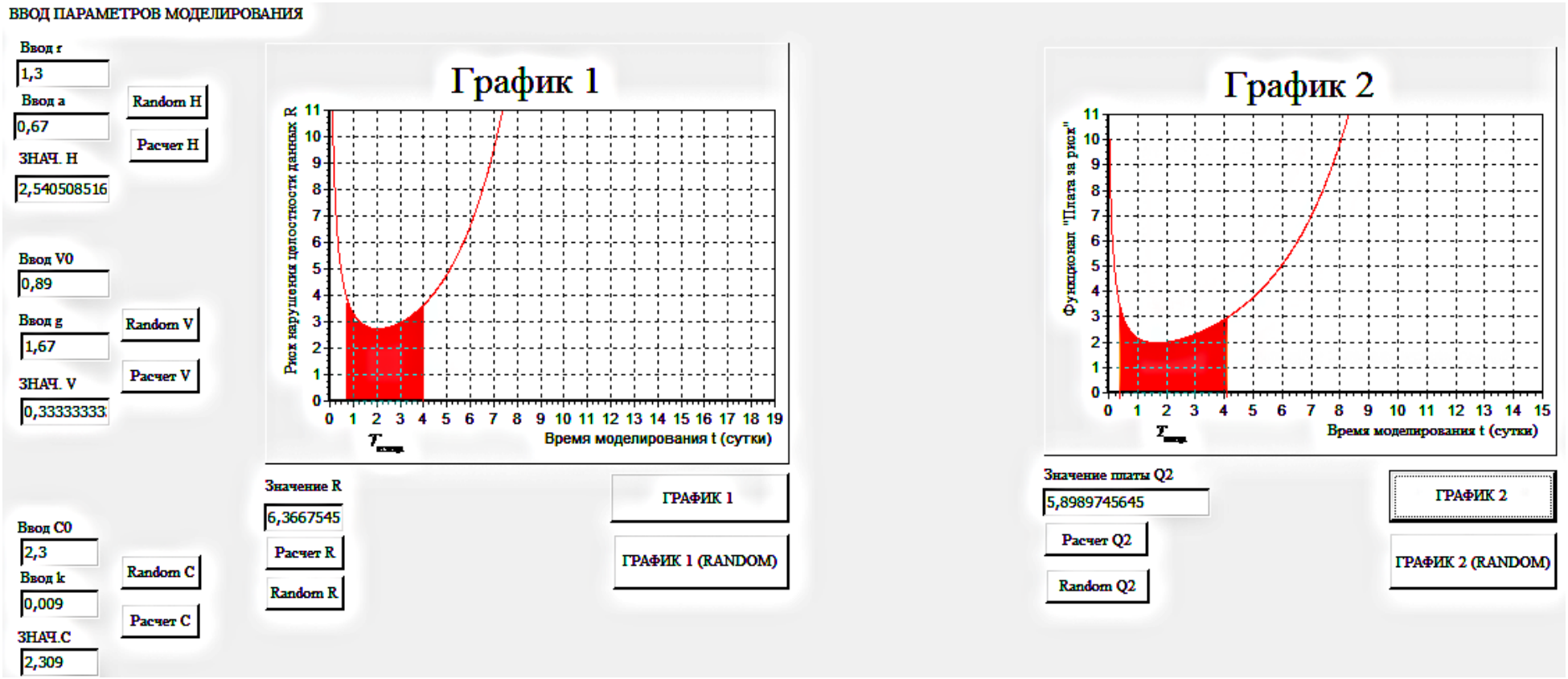

Рисунок 4.10 Пример пользовательского интерфейса разработанного программного обеспечения, реализующего имитационную модель СОЦД в нештатной ситуации

В результате возникновения подобной ситуации, система контроля возможных событий указывает на увеличение риска возникновения повторных ошибок. В случае нарушения целостности данных возможно их экстренное восстановление. Однако этот процесс является достаточно затратным и не всегда позволяет полностью восстановить исходные данные [73-78]. Известны случаи [78-87], когда процесс экстренного восстановления данных приводит к техническим сбоям на физическом уровне. При помощи разработанного программного обеспечения становится возможным, с достаточной точностью, спрогнозировать риск повторного возникновения ошибок и нарушений целостности данных, что позволяет использовать процедуру экстренного восстановления лишь в крайних случаях.

Отметим, что в интерфейсе программы моделирования предусмотрены два варианта ввода данных: ручной ввод значений коэффициентов, параметров управления и начальных состояний уязвимости и резерва СОЦД; использование генератора псевдослучайных чисел, который задает значения этих параметров автоматически.

Ввод параметров управления и начальных состояний уязвимости и резерва СОЦД производится в соответствующие окна (edt1, edt2, edt4, edt5, edt7, edt 8). При нажатии на кнопки «Расчет H» («Random H»), «Расчет V» («Random V»), «Расчет C» («Random C») осуществляется вычисление значений риска нарушения целостности данных, описываемого функцией Гомперца, уязвимости и резерва мощности СОЦД. В соответствующих окнах отображаются результаты произведенных вычислений (edt3, edt6, edt9). При активации кнопки «Расчет R» («Random R») производится вычисление значения риска нарушения целостности данных, в соответствующем окне (edt10) отображается результат вычисления.

После последовательно проделанных операций переходим к построению графического решения задачи построения оценки риска нарушения целостности данных. Для этого необходимо активировать кнопку «График 1» («График 1 (Random)»). В соответствующем окне (cht1) будет построен график функции риска нарушения целостности данных.

Для расчета значения функциональных зависимостей необходимо активировать кнопку «Расчет Q2» («Расчет Q2 (Random)»). В соответствующем окне (edt11) отобразится результат произведенного вычисления. При моделировании ситуации, в которой риск нарушения

целостности данных превышает критические для своего показателя значения, в программе предусмотрена система оповещения (построенные графики приобретают красный цвет).

Полнота разработанных предложений позволяет отразить в достаточной мере характеристики и особенности наземных СППД, которые необходимы для решения поставленной задачи и проведения вычислительного эксперимента. Точность разработанной модели СОЦД обеспечивает приемлемое совпадение реальных [88-92] и найденных показателей риска нарушения целостности данных. Модель качественно и достаточно точно описывает характеристики СППД, которые важны для анализа, прогнозирования и последующего вычисления риска повторного возникновения ошибок в передаваемой дискретной информации. Разработанная программа позволяет предсказать с достаточной точностью результаты вычислительного эксперимента и облегчает контроль их правильности.

Приведем основные результаты, достигнутые при помощи разработанного программного приложения:

- разработанный программный комплекс, позволяет осуществлять численное моделирование процесса прогнозирования риска нарушения целостности данных при их обработке в СППД, при этом, **точность прогнозирования повышается на 9 процентов**. На рисунке 4.11 представлены результаты статистических экспериментов, а на рисунке 4.12 соответствующая диаграмма.

- при помощи предложенного подхода с применением численного метода градиентного спуска получены оценки следующих параметров: оценка интенсивности поступивших в систему пакетов данных, оценка интенсивности принятых к обработке пакетов данных, а также оценка интенсивности, находящихся в очереди и ожидающих обработки пакетов данных, циркулирующих в СППД;

- установлено, что **скорость обработки пакетов данных увеличивается на 12 процентов**. На рисунке 4.13 представлены результаты статистических экспериментов, а на рисунке 4.14 соответствующая диаграмма.

Приложение 1. Таблица значений точности прогнозирования риска нарушения целостности данных

Порядковый номер эксперимента	Точность прогнозирования риска нарушения целостности данных при использовании стандартных методов обеспечения целостности	Точность прогнозирования риска нарушения целостности данных, полученная в результате применения разработанных методов и алгоритмов
1	0,7981	0,8638
2	0,7814	0,8614
3	0,7921	0,8588
4	0,7751	0,8678
5	0,7721	0,8612
6	0,7988	0,8645
7	0,7758	0,8696
8	0,7837	0,8678
9	0,7915	0,8601
10	0,7814	0,8658
11	0,7833	0,8601
12	0,7945	0,8636
13	0,7845	0,8616
14	0,7833	0,8611
15	0,7894	0,8687
16	0,7836	0,8621
17	0,7947	0,8673
18	0,7885	0,8623
19	0,7974	0,8663
20	0,7811	0,8661
21	0,7823	0,8612
...	...	...
50	0,7977	0,8665

Рисунок 4.11 Таблица статистических расчетов №1

Приложение 2. Диаграмма значений точности прогнозирования риска нарушения целостности данных

Рисунок 4.12 Диаграмма произведенных статистических расчетов №2

Приложение 3. Таблица значений скорости обработки данных

Порядковый номер эксперимента	Скорость обработки данных при использовании стандартных методов и алгоритмов обеспечения целостности (Мбит/с)	Скорость обработки данных при использовании разработанных методов и алгоритмов (Мбит/с)
1	4,0456	4,0912
2	4,0412	4,0931
3	4,0459	4,0966
4	4,0741	4,0974
5	4,0631	4,0932
6	4,0573	4,0912
7	4,0612	4,0902
8	4,0426	4,0918
9	4,0873	4,0914
10	4,0651	4,0994
11	4,0741	4,0914
12	4,0645	4,0948
13	4,0624	4,0987
14	4,0796	4,0988
15	4,0645	4,0912
16	4,0742	4,0914
17	4,0756	4,0952
18	4,0625	4,0913
19	4,0756	4,0987
20	4,0656	4,0915
21	4,0795	4,0979
...	...	...
50	4,0651	4,0941

Рисунок 4.13 Таблица статистических расчетов №3

Приложение 4. Диаграмма значений скорости обработки данных

Рисунок 4.14 Диаграмма произведенных статистических расчетов №4

Разработанный подход может быть применен как комплексное средство, направленное на обеспечение целостности телеметрических данных в СППД. Разработанное программное обеспечение способно с достаточной точностью анализировать и прогнозировать риск возникновения повторных ошибок, вызванных средой передачи данных и сбоями приемной аппаратуры СППД. Исходя из вышеизложенного, следует вывод, что разработанный комплексный подход по обеспечению целостности передаваемой информации в СППД может быть интегрирован в штатные средства контроля целостности (в блок контроля целостности поступающих данных) в виде дополнительного программного средства.

4.2 Выводы по четвертой главе

1. Произведенный анализ показал, что в существующих моделях оценки риска возникновения повторных ошибок используется распределение Вейбула, которое в недостаточной степени учитывает группирование ошибок на начальных и конечных стадиях сеанса передачи-приема данных. Для сокращения времени обработки и восстановления искаженных данных предложено использовать сигмовидную функцию Гомперца. Применение сигмовидной функции Гомперца позволяет учитывать указанные обстоятельства, что дает возможность для обнаружения местоположения пачек ошибок, вычислять наибольшую вероятность присутствия этих ошибок на интервале проведения сеанса передачи-приема данных.

2. Исследования показали, что после приема данных имеется риск повторного возникновения ошибок в результате сбоев в приемной аппаратуре СППД и/или в программах их обработки. С этой целью разработана математическая модель подсистемы оценки этого риска, построены функциональные зависимости, позволяющие произвести расчет допустимых значений риска нарушения целостности данных в СППД, разработан алгоритм и методика проведения моделирования.

4. Разработано программное приложение на основе комплексного подхода по обеспечению целостности передаваемой информации, которое позволяет проводить на предварительной стадии проектирования системы надежной передачи телеметрических данных анализ режимов с возможными нарушениями целостности данных и оценивать их риски. При определенной адаптации программное приложение может быть интегрировано в штатные

средства контроля целостности (в блок контроля целостности поступающих данных) в виде дополнительного программного ресурса.

5. Приведены результаты статистических экспериментов по оценке рисков возникновения повторных ошибок за заданный период времени, представлены соответствующие диаграммы. Результаты указали на возможность использования дополнительных средств фиксации фактов несанкционированного доступа, обнаружения вторичных ошибок и восстановление данных в случае искажений.

ЗАКЛЮЧЕНИЕ

В диссертационной работе решалась важная для теории и практики задача обеспечения целостности данных в системах обмена дискретной информацией. В целом решение задачи обеспечения целостности носит комплексный характер и включает выделение трех подзадач: подзадачу обнаружения признаков несанкционированного доступа (вмешательства) в систему передачи-приема данных, подзадачу обнаружения факта искажения данных, которые они получили от отрицательных воздействий среды их передачи, и подзадачу оценки риска возникновения повторных ошибок.

Существует достаточно много способов и средств решения этих задач, большинство из которых дают результаты в конкретных условиях их применения. В работе использован комбинированный подход, суть которого состоит в том, чтобы успешно интегрировать методы решения трех подзадач для создания единых средств построения обеспечения целостности данных и использования их на практике. В условиях среды передачи информации телеметрические данные подвержены воздействиям множества отрицательных как внешних, так и внутренних факторов, причем искажения могут быть вызваны сбоями программно-аппаратных средств обработки данных.

Получены следующие основные результаты:

- представлена классификация СППД, анализ которой показал, что СППД имеет сложную информационную структуру, для которой требуется использовать наиболее эффективные методы обеспечения целостности данных. Также в процессе анализа выявлено, что используемые на практике существующие методы обеспечения целостности имеют ряд существенных недостатков, что не позволяет обеспечивать необходимый уровень безопасности передаваемой дискретной информации;

- предложена концептуальная модель системы передачи-приема данных, которая представлена множеством компонентов и связей между ними, определяющих ее смысловую структуру и позволяющую на ее основе создавать модели систем обеспечения целостности передаваемых данных с учетом различных видов атак злоумышленников и сбоев оборудования;

- произведен анализ наиболее известных угроз нарушения безопасности данных, циркулирующих в СППД. Представлены известные модели целостности, их достоинства и недостатки. Основным недостатком является сложность и большие временные затраты на обнаружение

нарушений целостности и контроль надежности аппаратуры передачи – приёма данных;

- выполнен анализ нарушений целостности данных при их передаче по дискретным каналам СППД. Полученная в результате анализа информация, позволила определить подход к построению подсистемы обнаружения признаков несанкционированного доступа за счет использования временного признакового параметра – задержки поступления пакетов, нарушения порядка следования пакетов в очереди, влияния изменения веса пакета и самой очереди;

- разработан подход к обнаружению признаков несанкционированного доступа к СППД на основе аппарата теории массового обслуживания с использованием индикаторных функций и их компенсаторов. С помощью него можно определять факт нарушения целостности в передаваемых пакетах данных, оценивая значения интенсивностей поступивших пакетов данных, интенсивностей принятых к обработке пакетов данных и интенсивностей, находящихся в очереди и ожидающих обработки пакетов данных, и учета отклонений этих значений от интенсивностей, заданных протоколами телеметрии;

- построены математические модели оценки интенсивности входных пакетов данных, поступающих для обработки в СППД, интенсивности пакетов данных, находящихся в очереди и ожидающих обслуживания при фиксированном значении компенсатора $I\left(Q_t = k\right)$ и заданного модельного времени t, которые позволяют установить тот факт, что обслуживание (обработка) пакетов данных происходит без существенных отклонений в течение заданного времени моделирования;

- предложен вариант эффективного использования численного метода градиентного спуска для решения стохастических интегральных уравнений, применительно к индикаторным функциям и их компенсаторам для использования в подсистеме обнаружения признаков несанкционированного доступа к СППД. Отличительной особенностью этого метода является его использование для подготовки таблиц заранее вычисленных значений интенсивностей поступивших пакетов данных, интенсивностей принятых к обработке пакетов данных, интенсивностей, находящихся в очереди и ожидающих обработки пакетов данных, что позволяет существенно ускорить процесс обработки пакетов на этом отрезке времени;

- рассмотрены известные модели каналов передачи данных, и показано, что они носят числовой потоковый параметрический характер в пакетной форме. Установлено, что модели с достаточной точностью отражают специфику зашумленных каналов передачи данных и основным требованием к ним являются требование высокого быстродействия, вызванное ограниченностью времени сеанса обмена телеметрическими данными и временными затратами на выполнение процедур обнаружения ошибок в закодированных данных и восстановления их с заданной достоверностью;

- обосновано применение кодов с переменным весом в виде эффективного быстрого средства обнаружения и исправления ошибок. Коды с переменным весом позволяют быстро и эффективно обнаруживать любые одиночные ошибки (в том числе одиночные ошибки различной кратности). Преимуществом кодов с переменным весом является эффективность их использования в современных каналах передачи данных при условии быстрой генерации двоичными кодами чисел с переменными весами;

- предложен эффективный численный метод вычисления веса целого десятичного числа, (с помощью которых кодируются телеметрические данные) и определение позиций единиц, который может быть применен для идентификации получаемых образов данных, представленных кодами переменного веса на этапе декодирования на стороне получателя;

- предложно использовать матрично-алгоритмический подход к кодированию целых чисел на основе использования матрицы Паскаля. Исходными данными для генерации являются: задаваемый вес исходного числа и само число, при этом вес определяется выбором номера столбца матрицы Паскаля, а получение двоичного кода происходит в процессе формирования пути на поле чисел матрицы по введенному правилу;

- разработаны новые удобные формы представления алгоритмов матрично-алгоритмического кодирования и декодирования в виде специальных матричных диаграмм, которые позволяют эффективно работать с числами матрицы Паскаля и данными, представленными кодами с переменным весом. Разработана процедура и средства обнаружения фактов искажений целостности данных, вызванных канальными помехами и влиянием внешней среды. Представлен процесс восстановления этих данных с высокой достоверностью на основе применения матриц Паскаля для генерации кодовых данных и матриц чисел с фиксированными весами для получения их прообраза за счет быстрых матричных вычислений;

- разработана математическая модель подсистемы оценки риска возникновения повторных ошибок, построены функциональные зависимости, позволяющие произвести расчет допустимых значений риска нарушения целостности данных в СППД, разработан алгоритм и методика проведения моделирования;

- разработано программное приложение, на основе комплексного подхода по обеспечению целостности передаваемой информации, которое позволяет проводить на предварительной стадии проектирования системы надежной передачи телеметрических данных анализ режимов с возможными нарушениями целостности данных и оценивать их риски. При определенной адаптации программное приложение может быть интегрировано в штатные средства контроля целостности (в блок контроля целостности поступающих данных) в виде дополнительного программного ресурса;

- приведены результаты статистических экспериментов по оценке рисков возникновения повторных ошибок за заданный период времени, установлено, что **точность прогнозирования риска возникновения повторных ошибок повышается на 9 процентов, а скорость обработки пакетов данных увеличивается на 12 процентов,** представлены соответствующие диаграммы. Результаты указали на возможность использования дополнительных средств фиксации фактов несанкционированного доступа, обнаружения вторичных ошибок и восстановление данных в случае искажений.

Цель и задачи, поставленные в диссертации, а именно обеспечение целостности данных в информационных системах обмена дискретной информацией достигнуты.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ГЛОНАСС: принципы построения и функционирования / Р. В. Бакитько [и др.]; под общ. ред. А. И. Перова, В. И. Харисова. 3-е изд., перераб. и доп. М.: Радиотехника, 2005. 688 с.
2. Иванов А. В., Комраков Д. В. Анализ работы автономной системы контроля целостности навигационных данных в навигационных комплексах наземных подвижных объектов с помощью статистического компьютерного моделирования // Техника радио. 2016. №2 (29). С. 63–72.
3. Диченко С.А. Контроль и обеспечение целостности информациии в системах хранения данных // Наукоемкие технологии в космических исследованиях Земли. 2019. Т. 11. №1. С. 49-57.
4. Коржик Ф. М. Финк Л. М. Помехоустойчивое кодирование дискретных данных в каналах со случайной структурой // Связь. — 1975. — Р. 272.
5. Харкевич А.А. Борьба с помехами // Москва: Государственное издательство физико-математической литературы – 1963. -Р.345.
6. Верзунов Г.В. Бортовая обработка сигналов: перспективы и проблемы. Технологии и средства. – Спец. вып. – 2007. – С. 52–58.
7. Иванов А.В., Комраков Д.В. Алгоритм работы автономной системы контроля целостности навигационных данных спутниковых радионавигационных систем // Техника радиосвязи. 2018. Вып. 4 (39). С. 54–60.
8. Васильев В.И. Системы связи [Текст]: учеб. пособие для втузов / В.И. Васильев, А.П. Буркин, В.А. Свириденко – М.: Высшая школа, 1987 – 280 с.:ил.
9. Мордухович Л.Г., Степанов А.П. Системы радио. Уч. пособие для вузов. М.: Радио и связь, 1997.
10. Системы связи: учебное пособие для студентов (курсантов) вузов / С. И. Макаренко, В. И. Сапожников, Г. И. Захаренко, В. Е. Федосеев; под общ. ред. С. И. Макаренко. - Воронеж, издание ВАИУ, 2011. – 285с.: ил.
11. Wang Z. Karpovsky M. G. Algebraic manipulation detection codes and their applications for design of secure cryptographic devices // On-Line Testing Symposium (IOLTS), 2011 IEEE 17th International / IEEE. — 2011. — Pp. 234–239.
12. Кларк Дж. мл. Кодирование с исправлением ошибок в системах цифровой: Пер. с англ. / Дж. Кларк, мл., Дж. Кейн – М.: Радио и связь, 1987. – 392 с.: ил.

13. Муханова Аягоз, Ревнивых Александр Владимирович, Федотов Анатолий Михайлович Классификация угроз и уязвимостей информационной безопасности в корпоративных системах // Вестник НГУ. Серия: Информационные технологии. 2013. №2. URL: https://cyberleninka.ru/article/n/klassifikatsiya-ugroz-i-uyazvimostey-informatsionnoy-bezopasnosti-v-korporativnyh-sistemah.
14. Передача дискретных сообщений [Текст]: учебник для вузов / В.П. Шувалов [и др.]; под ред. В.П. Шувалова. – М.: Радио и связь, 1990, - 464 с.: ил.
15. Голиков А. М. Основы информационной безопасности: учебное пособие / А. М. Голиков. — Москва: ТУСУР, 2007. — 201 с. — ISBN 978-5-868889-467-1. — Текст: электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/10927.
16. Иванов Александр Васильевич, Негуляева Анастасия Петровна, Москвитин Сергей Петрович Автономный контроль целостности навигационных данных спутниковых радионавигационных систем методами сравнения и невязок // Вестник ТГТУ. 2016. №3. URL: https://cyberleninka.ru/article/n/avtonomnyy-kontrol-tselostnosti-navigatsionnyh-dannyh-sputnikovyh-radionavigatsionnyh-sistem-metodami-sravneniya-i-nevyazok.
17. MacKay D. J. C. Information Theory, Inference, and Learning Algorithms / D. J. C. MacKay. — Cambridge : Cambridge University Press, 2003.
18. Савинов Ю.Г., Тихоненко А.А., Пронин В.И., Щукин А.Н. Семимартингальная модель СМО с произвольным временем ожидания «нетерпеливых» заявок // Ученые записки УлГУ. Сер. Математика и информационные технологии. УлГУ. Электрон. журн., 2019, № 2, с.81-88.
19. Кирпичников А.П., Флакс Д.Б., Валеева Л.Р. Системы массового обслуживания с ограниченным временем пребывания заявки в системе // Актуальные проблемы гуманитарных и естественных наук. 2015. №6-1. URL: https://cyberleninka.ru/article/n/sistemy-massovogo-obsluzhivaniya-s-ogranichennym-vremenem-prebyvaniya-zayavki-v-sisteme.
20. Кузнецов Н.А. Имитационное моделирование системы массового обслуживания с размножением заявок в очередях [Текст] / Н.А.Кузнецов, А.А.Мозоль // T-COMM. Телекоммуникации и транспорт:-2019.-№11-с.32-37.
21. Щербаков А.Ю. Введение в теорию и практику компьютерной безопасности. – М.: издатель Молгачева С.В., 2001. - 352 с.

22. Белинский Д.В. Анализ помех и типовых ошибок в каналах связи при приеме данных // Наукоемкие технологии в космических исследованиях Земли. 2011.
23. Р. Морелос-Сарагоса Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. / Р. Морелос-Сарагоса. — М. : Техносфера, 2005.
24. Методы обеспечения целостности информации на основе вейвлетных преобразований для защиты средств хранения информации: диссертация кандидата технических наук: 05.13.19 / Таранов Сергей Владимирович; [Место защиты: С.-Петерб. гос. ун-т телекоммуникаций им. М.А. Бонч-Бруевича]. - Санкт-Петербург, 2018. - 163 с. : ил.
25. Клейнрок Л. Теория массового обслуживания. Пер. с англ. – М.: Машиностроение, 1979. – 432 с.
26. ГОСТ Р56096-2014 Система передачи космических данных и информации. Пакетная телеметрия (Переиздание), ГОСТ Р от 09 сентября 2014 года №56096-2014.
27. Аунг Хла Мо Моделирование системы массового обслуживания порта Янгон // ГИАБ. 2010. №12. URL: https://cyberleninka.ru/article/n/modelirovanie-sistemy-massovogo-obsluzhivaniya-porta-yangon.
28. Орлов Александр Иванович, Шаров Валерий Дмитриевич Выявление отклонений в контроллинге (на примере мониторинга уровня безопасности полетов) // Научный журнал КубГАУ. 2014. №95. URL: https://cyberleninka.ru/article/n/vyyavlenie-otkloneniy-v-kontrollinge-na-primere-monitoringa-urovnya-bezopasnosti-poletov.
29. Kepaptsoglou K., Karlaftis M. Transit Route Network Design Problem: Review. J. Transp. Eng. August 2009. 491 – 505.
30. Кирпичников А.П., Флакс Д.Б., Валеева Л.Р. Системы массового обслуживания с ограниченным временем пребывания заявки в системе // Актуальные проблемы гуманитарных и естественных наук. 2015. №6-1. URL: https://cyberleninka.ru/article/n/sistemy-massovogo-obsluzhivaniya-s-ogranichennym-vremenem-prebyvaniya-zayavki-v-sisteme.
31. Филиппенко И. В. Математическая модель систем радиочастотной идентификации с кодовым разделением каналов // ВЕЖПТ. 2011. №3 (53). URL: https://cyberleninka.ru/article/n/matematicheskaya-model-sistem-radiochastotnoy-identifikatsii-s-kodovym-razdeleniem-kanalov

32. Фадеева Л. Н., Лебедев А. В., Теория вероятностей и математическая статистика: учебное пособие. - 2-е изд., перераб. и доп. - М.: Эксмо, 2010. - 496 с. – (Новое экономическое образование).
33. Н.Б. Ипкаев (АО «Российские космические системы»). Анализ результатов космического эксперимента по передаче расширенного альманаха в ЦИКА ГЛОНАСС (2015. Т. 2. Вып. 1).
34. Иванов В.А., Ручинская Е.В. Методика определения эффективности различных режимов движения ОТС для сближения в космосе // Вестник МГТУ им. Н.Э. Баумана. Сер. «Машиностроение». 2009. №4 (77). С. 45-77.
35. Отчет «Надежность и качество измерительной аппаратуры, разработанной НПО ИТ и изготовленной серийными заводами в 1992–2012 гг.».
36. Савенкова Н.П. Численные методы в математическом моделировании: Учебное пособие / Н.П. Савенкова, О.Г. Проворова, А.Ю. Мокин. - М.: Инфра-М, 2018. - 256 с.
37. Калиткин Н.Н. Численные методы: В 2 кн. Кн. 2. Методы математической физики: Учебник / Н.Н. Калиткин. - М.: Academia, 2018. - 48 с.
38. Косарев В.П. Численные методы линейной алгебры: Учебное пособие / В.П. Косарев, Т.Т. Андрющенко. - СПб.: Лань П, 2016. - 496 с.
39. Самарский А.А. Численные методы решения обратных задач математической физики / А.А. Самарский, П.Н. Вабищевич. - М.: ЛКИ, 2015. - 480 с.
40. Радиотехнические системы передачи информации: Учеб. пособие для вузов / Под ред. В.В. Калмыкова. – М.: Радио и связь, 1990. – 304 с.
41. Радиоэлектронное оборудование [Текст]: учебник для вузов ВВС / В. А.Ефимов [и др.]; - М.: ВВИА им. проф. Н.Е. Жуковского, 2004, - 228 с.: ил. - Библиогр.: с. 227-228.
42. Нефедов В. И. Основы радиоэлектроники и связи [Текст]: учебник для вузов / В. И. Нефедов — 2-е изд., прераб. и доп. — М.: Высш. шк., 2002, - 510 с.: ил.
43. Мозоль А.А. Полуэмпирический способ определения зоны покрытия базовой станции системы подвижной радиосвязи [Текст] / А.А. Мозоль, В.А. Головской // Вестник Воронежского института МВД России. – 2014. – №3. – С. 30–40.

44. Клод Шеннон. Теория информации. Математическая теория связи // Издательство иностранной литературы – 1963. – Р.211.
45. Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки, перевод с англ. И.И. Грушко, В.А. Зиновьева. // Под редакцией Л.А. Бассалыго. Москва. «Связь», - 1979.-744 с.
46. Эндрюс Дж. Теория разбиений, перевод с англ. Б.С. Стечкина. // Главная редакция физико-математической. Москва «Наука», - 1982.- 256 с.
47. Смагин А.А., Леонтьев М.Ю. Программа определения веса целого десятичного числа. Свидетельство о государственной регистрации № №2013610552 в реестре программ для ЭВМ от 09.01.2013.
48. Смагин А.А. Модели разбиений. Ульяновск: УлГУ, 2013.-207с.
49. Смикун Петр Иванович. Исследование вопросов построения и разработка матричных многофункциональных систем обнаружения ошибок и защиты данных : диссертация кандидата технических наук: 05.13.18 / Смикун Петр Иванович; [Место защиты: Ульян. гос. ун-т]. - Ульяновск, 2011. - 175 с. : ил.
50. Чугунков И.В. Методы и средства оценки качества генераторов псевдо случайных последовательностей, ориентированных на решение задач защиты информации: Учебное пособие. М.: НИЯУ МИФИ, 2012. – 236 с.
51. Р.Грэхем, Д.Кнут, О.Паташник. Конкретная математика. Москва. «Мир»,-1998.- 703с.
52. Кузнецов Н.А. Метод построения нелинейного вейвлетного кода для обеспечения целостности данных в каналах связи // TComm: Телекоммуникации и транспорт. 2021. Том 15. №2. С. 26-32.
53. Кузнецов Н.А. Модель автоматизированной системы оптимизации параметров управления рисками в терминах угроз, уязвимостей и резервов [Текст]//Н.А.Кузнецов, А.А.Мозоль// Вестник Воронежского института МВД России. – 2019. – №3. – С.14–21.
54. Тихов Михаил Сергеевич, Агеев Вячеслав Владимирович, Бородина Татьяна Сергеевна Оценивание параметров распределения Вейбулла по случайно цензурированным выборкам // Вестник ННГУ. 2010. №4. URL: https://cyberleninka.ru/article/n/otsenivanie-parametrov-raspredeleniya-veybulla-po-sluchayno-tsenzurirovannym-vyborkam (дата обращения: 24.04.2021).
55. Ярмошенко И. В. Использование свойств логнормального распределения при анализе результатов радоновых обследований / И. В. Ярмошенко, М. В. Жуковский, И. А. Кирдин // Актуальные проблемы

ограничения облучения населения от природных источников ионизирующего излучения. Радон – 2000: материалы научно-практической конференции (18–20 апреля 2000 г.) – М., 2000. – С. 17–20.
56. ГОСТ 11. 009–73. Прикладная статистика: Правила определения оценок и доверительных границ для параметров логарифмического нормального распределения. – М.: Изд-во стандартов, 1980.
57. ГОСТ 11. 007–74. Прикладная статистика: Правила определения оценок и доверительных границ для параметров распределения Вейбулла. – М. : Изд-во стандартов, 1980.
58. Методы нелинейного кодирования для повышения достоверности обработки информации автореферат диссертация кандидата технических наук: 05.13.01 / Алексеев Максим Олегович; [Место защиты: С.-Петерб. ин-т информатики и автоматизации РАН]. - Санкт-Петербург, 2015.
59. Спутниковая связь и вещание: Справочник.2 изд., перераб. и доп. Под ред. Л.Я. Кантора. М.: Радио и связь, 1988.
60. А. Иванов Военные системы спутниковой связи// Военное обозрение [Офиц. сайт]. URL: https://topwar.ru/36729-voennye-sistemy-sputnikovoy-svyazi.html.
61. Рош Р.Д. Принципы построения спутниковой системы персональной связи «Одиссей». Экспресс-информация. Серия «Передача информацией», № 5, 1994.
62. Мелентьев О. Г. Теоретические аспекты передачи данных по каналам с группирующимися ошибками; Горячая Линия - Телеком - , 2007. - 232 с.
63. Бутов А.А., Волков М.А., Макаров В.П., Орлов А.И., Шаров В.Д. Автоматизированная система прогнозирования и предотвращения авиационных происшествий при организации и производстве воздушных перевозок // Известия Самарского научного центра Российской академии наук, 2012, том 14, № 4-2, с. 380-385.
64. Пономаренко А. В. Разработка модельной реализации функций Бесселя из стандарта LSB // Труды ИСП РАН. 2006. №. URL: https://cyberleninka.ru/article/n/razrabotka-modelnoy-realizatsii-funktsiy-besselya-iz-standarta-lsb (дата обращения: 03.04.2022).
65. Бейтмен Г., Эрдейи А. Высшие трансцендентные функции. Т. 2. Функции Бесселя, функции параболического цилиндра, ортогональные многочлены. - М.: Наука, 1966г. - 296с.

66. G.N. Watson A treatise on the theory of Bessel functions. 1945. (Имеется перевод: Ватсон Г.Н. Теория бесселевых функций: Пер. со 2-го англ.изд. / Авт.предисл. В.С. Берман. - М.: ИЛ, 1949г. - 798с.)
67. Кузьмин Р.О. Бесселевы функции. - Л.-М.: ГТТИ, 1933г. - 152с.
68. Рекомендации и отчеты МККР. Т. 4. Ч. 1. Фиксированная спутниковая служба. – Дубровник,1986. – 560 с.
69. Бабков В.Ю. Сотовые системы мобильной радиосвязи / В.Ю. Бабков. - СПб.: BHV, 2013. - 432 с.
70. Андреев В.А. Направляющие системы электросвязи. В 2 тт. Т. 2. Проектирование, строительство и техническая эксплуатация / В.А. Андреев, Э.Л. Портнов и др. - М.: ГЛТ, 2010. - 424 с.
71. Весоловский К. Системы подвижной радиосвязи / К. Весоловский. - М.: ГЛТ, 2006. - 536 с.
72. Комашинский В.И. Системы подвижной радиосвязи с пакетной передачей информации. Основы моделирования. / В.И. Комашинский, А.В. Максимов. - М.: ГЛТ , 2007. - 176 с.
73. Н. М. Василега, В. Н. Крищук, А. В. Неласая Восстановление данных в информационных системах // Радіоелектроніка, інформатика, управління. 1999. №2. URL: https://cyberleninka.ru/article/n/vosstanovlenie-dannyh-v-informatsionnyh-sistemah.
74. Соколинский Л.Б., Цымблер М.Л. Принципы реализации системы управления файлами в параллельной СУБД Омега для МВС-100 // Вестник ЧелГУ. 1999. №2. URL: https://cyberleninka.ru/article/n/printsipy-realizatsii-sistemy-upravleniya-faylami-v-parallelnoy-subd-omega-dlya-mvs-100.
75. Дергачёва Е.В. /Роль информационного противоборства в современных условиях. Информатика и вычислительная техника. - М.: Москва, 2002. - 188 с.
76. А.Гультяев Восстановление данных / Алексей Гультяев. - М.: Питер, 2006. - 384 с.
77. Уточка Р. А., Фадин А. А., Шахалов И. Ю. Проблемные вопросы гарантированного уничтожения информации на носителях с полупроводниковой энергонезависимой перезаписываемой памятью // Вестник МГТУ им. Н.Э. Баумана. Серия «Приборостроение». 2011. №SPEC. URL: https://cyberleninka.ru/article/n/problemnye-voprosy-garantirovannogo-unichtozheniya-informatsii-na-nositelyah-s-poluprovodnikovoy-energonezavisimoy.

78. Портнов Э.Л. Направляющие системы электросвязи. В 2-х т. Т. 2. Проектирование, строительство и техническая эксплуатация: Учебник для вузов / Э.Л. Портнов. - М.: Гор. линия-Телеком, 2010. - 424 с.
79. Скляров О.К. Волоконно-оптические сети и системы связи: Учебное пособие / О.К. Скляров. - СПб.: Лань, 2010. - 272 с.
80. Тоискин В.С. Системы документальной электросвязи: Учебное пособие / В.С. Тоискин, А.П. Жук. - М.: ИЦ РИОР, Инфра-М, 2011. - 352 с.
81. Шарангович С.Н. Многоволновые оптические системы связи: Учебное пособие / С.Н. Шарангович. - СПб.: Лань, 2019. - 120 с.
82. Макаренко Сергей Иванович Описательная модель сети связи специального назначения // Системы управления, связи и безопасности. 2017. №2. URL: https://cyberleninka.ru/article/n/opisatelnaya-model-seti-svyazi-spetsialnogo-naznacheniya.
83. Макаренко Сергей Иванович Подавление сетецентрических систем управления радиоэлектронными информационно-техническими воздействиями // Системы управления, связи и безопасности. 2017. №4. URL: https://cyberleninka.ru/article/n/podavlenie-setetsentricheskih-sistem-upravleniya-radioelektronnymi-informatsionno-tehnicheskimi-vozdeystviyami.
84. Галл Р.Д. Точность местоопределения наземных источников, использующих геостационарные ретрансляторы // Известия вузов России. Радиоэлектроника. 2020. №6. URL: https://cyberleninka.ru/article/n/tochnost-mestoopredeleniya-nazemnyh-istochnikov-ispolzuyuschih-geostatsionarnye-retranslyatory (дата обращения: 03.06.2022).
85. Бурлянд В.А., Володарская В.Е., Яроцкий А.В. Советская радиотехника и электросвязь в датах.- М.: Связь, 1975.- 191с.
86. Карпов Сергей Сергеевич, Рябинин Юрий Евгеньевич, Финько Олег Анатольевич Обеспечение целостности данных, передаваемых по каналам связи виртуальных частных сетей // Вопросы кибербезопасности. 2021. №4 (44). URL: https://cyberleninka.ru/article/n/obespechenie-tselostnosti-dannyh-peredavaemyh-po-kanalam-svyazi-virtualnyh-chastnyh-setey.
87. Тронин Вадим Георгиевич, Галныкина Ксения Сергеевна, Стенина Анна Сергеевна Математические методы анализа рисков в инновационных проектах // Вестник УлГТУ. 2015. №1 (69). URL: https://cyberleninka.ru/article/n/matematicheskie-metody-analiza-riskov-v-innovatsionnyh-proektah.

88. Быков А. А., Порфирьев Б. Н. Об анализе риска, концепциях и классификации рисков // Проблемы анализа риска. 2006. №4. URL: https://cyberleninka.ru/article/n/ob-analize-riska-kontseptsiyah-i-klassifikatsii-riskov.
89. Данильченко Анна Владимировна Управление рисками // Молодой исследователь Дона. 2017. №6 (9). URL: https://cyberleninka.ru/article/n/upravlenie-riskami-4).
90. Октаева Е. В. Математические модели и методы оценки рисков / Е. В. Октаева. — Текст : // Молодой ученый. — 2016. — № 15 (119). — С. 310-313.
91. Слабинский С. В. Особенности оценки рисков в производственной деятельности промышленных предприятий [Электронный ресурс]. — Режим доступа: http://science-bsea.narod.ru
92. Уродовских В. Н. Управление рисками предприятия: Учеб. пособие. — М.: ВЗФЭИ, 2009. — 130 с.