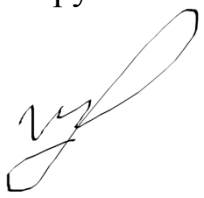
На правах рукописи



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

Автореферат
диссертации на соискание ученой степени
кандидата технических наук

Ульяновск – 2022

Работа выполнена на кафедре телекоммуникационных технологий и сетей ФГБОУ ВО «Ульяновский государственный университет»

Научный руководитель: Смагин Алексей Аркадьевич – доктор технических наук, профессор

Официальные оппоненты: Воловач Владимир Иванович – доктор технических наук, доцент, ФГБОУ ВО «Поволжский государственный университет сервиса», кафедра информационного и электронного сервиса, заведующий кафедрой

Иванов Александр Куприянович – доктор технических наук, доцент, Федеральный научно-производственный центр Акционерное общество «Научно производственное объединение «Марс», комплексный научно-исследовательский отдел-1, главный научный сотрудник

Ведущая организация: ФГБОУ ВО «Ульяновский государственный технический университет»

Защита состоится «21» сентября 2022 г. в «12:00» часов на заседании диссертационного совета Д 212.278.02, созданного на базе федерального государственного бюджетного образовательного учреждения высшего образования «Ульяновский государственный университет» по адресу 432017, г. Ульяновск, ул. Набережная реки Свияги, д. 106, корпус 1, ауд.703.

С диссертацией и авторефератом можно ознакомиться в научной библиотеке ФГБОУ ВО «Ульяновский государственный университет» и на сайте ВУЗа — https://www.ulsu.ru, с авторефератом — на сайте Высшей аттестационной комиссии при Министерстве науки и высшего образования Российской Федерации — https://vak.minobrnauki.gov.ru.

Отзывы на автореферат в двух экземплярах, заверенные печатью, просим направлять по адресу: 432017, г. Ульяновск, ул. Л. Толстого, д. 42, УлГУ, отдел подготовки кадров высшей квалификации.

Автореферат разослан «____» _____ 2022 г.

Учёный секретарь
диссертационного совета Волков Максим Анатольевич

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность работы.

На практике большое распространение получили системы удаленного доступа, которые имеют важное народно-хозяйственное значение для обеспечения обмена данными между центрами управления и удаленными объектами[1,2,3]. 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[4,5,6]. К этим системам предъявляются повышенные требования к обеспечению целостности передаваемых данных, защиты от несанкционированного доступа, обнаружению и исправлению ошибок, вызванных средой передачи данных и сбоями приемной аппаратуры.

Применяемая аппаратура является достаточно уязвимой в условиях динамической и быстро изменяющейся обстановки. Помехи и шумы среды передачи данных, злоумышленники наносят ущерб сеансу обмена данными, вызывая потери информации, получение искаженной информации, подмену информации, недопустимую задержку при получении информации, необходимость ее повторной передачи[7,8].

Под целостностью данных понимается неискаженное их представление в СППД, причем строго соблюдается отношение биективности между отправленными и получаемыми кодами. Обменом являются телеметрические данные, представляющие числовые данные контрольно-измерительной и управляющей аппаратуры СППД. Разработка средств обеспечения

---

[1] Весоловский К. Системы подвижной радиосвязи / К. Весоловский. - М.: ГЛТ, 2006. - 536 с.

[2] 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.

[3] 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.

[4] Комашинский В.И. Системы подвижной радиосвязи с пакетной передачей информации. Основы моделирования. / В.И. Комашинский, А.В. Максимов. - М.: ГЛТ , 2007. - 176 с.

[5] Иванов А.В., Негуляева А.П., Москвитин С.П. Автономный контроль целостности навигационных данных спутниковых радионавигационных систем методами сравнения и невязок // Вестник ТГТУ. 2016. №3.

[6] 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.

[7] 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.

[8] 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.

целостности передаваемых данных обусловлена увеличением их объемов, необходимостью совершенствования способов и средств обнаружения признаков несанкционированного доступа, искажениями передаваемых данных, вызванных средой передачи данных, и появлением новых видов угроз со стороны злоумышленников.

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 обеспечения 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, построенная 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, с возможностью 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, использующая 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.

Теоретиечская и практическая значимость. Теоретическая значимость результатов проведенных исследований состоит в том, что предложен подход к моделированию системы передачи-приема данных с использованием математического аппарата теории массового обслуживания, в которой пакеты передаваемых данных отождествляются с заявками, очереди заявок – с потоком пакетов, использована модель одноканальной системы массового обслуживания с простейшим потоком заявок. Применение этого подхода позволяет диагностировать признак несанкционированного доступа к системе передачи-приема данных как отклонения временных параметров доставки пакетов, интерпретируемые как задержки получателю из-за вмешательства злоумышленников. Практическая значимость результатов проведенных исследований состоит в создании системы компьютерного и имитационного моделирования на базе разработанных математических моделей, реализующих их алгоритмов и численных методов получения многозначных кодов, применение которых позволило решить основную задачу диссертации - обеспечение целостности передаваемых данных в условиях несанкционированного доступа и воздействия отрицательно действующих внутренних и внешних факторов

среды передачи данных и сбоями приемной аппаратуры систем передачи-приема данных, что позволяет на практике проводить предварительные исследования надежности и готовности систем для работы в реальных условиях.

Апробация результатов. Основные результаты диссертации обсуждались и докладывались на следующих конференциях и семинарах:

- XXIII Всероссийская межведомственная научно-техническая конференция школы-семинара «Информационная безопасность – актуальная проблема современности» Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С.М.Штеменко Министерства обороны Российской Федерации, г. Краснодар, 22.09.2021- 03.10.2021 (открытая секция);

-- Всероссийская научно-практическая конференция «Траектории взаимодействия в развитии цифровых навыков», УлГПУ им. Н.И. Ульянова, г. Ульяновск, 25.12.2021;

Международная научно-техническая конференция «Перспективные информационные технологии» г. Самара, 18.04.2022 - 21.04.2022;

- Совместные научные семинары кафедры телекоммуникационных технологий и сетей УлГУ и НИТИ им. С.П. Капицы (2021 – 2022 гг.);

- Научном семинаре 23 кафедры 2 факультета Краснодарского высшего военного орденов Жукова и Октябрьской Революции Краснознаменного училища имени генерала армии С.М.Штеменко Министерства обороны Российской Федерации, г. Краснодар, 22.02.2022 г.**;**

Публикации. 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.

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

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

СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность и научная новизна диссертации, сформулированы цель и задачи исследования, представлены основные положения, выносимые на защиту, и отражен личный вклад автора.

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. Первая глава диссертации состоит из трех разделов.

В первом разделе 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.

Во втором разделе предложена концептуальная модель СППД, 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. Разработанная структурно-функциональная модель СППД учитывает состав операций, их связь, переходы, возможные риски возникновения сбоев, отказов оборудования, постороннего вмешательства, необходимые доработки в случае некорректного функционирования СППД, а также время, затрачиваемое на оценку параметров показателей, с помощью которых анализируется состояние СППД.

В третьем разделе произведен анализ наиболее известных уязвимостей и угроз нарушения безопасности данных, циркулирующих в СППД. Представлены известные модели целостности, их достоинства и недостатки. Основным недостатком являются большие временные затраты на обнаружение нарушений целостности и контроль надежности аппаратуры передачи – приёма 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. Разработана математическая модель подсистемы обнаружения признаков несанкционированного доступа к СППД на основе аппарата теории массового обслуживания с применением эффективных методов аппроксимации, точечных процессов, индикаторных функций и их компенсаторов в семимартингальном описании. С применением модифицированного метода градиентного спуска произведены вычисления значений интенсивностей поступивших пакетов данных, интенсивностей принятых к обработке пакетов данных, интенсивностей, находящихся в очереди и ожидающих обработки пакетов данных. Вторая глава состоит из четырех разделов.

В первом разделе представлены основные процедуры по выявлению угроз нарушения целостности данных в СППД, рассмотрены способы получения информации о состоянии СППД. В результате анализа сделан вывод, что при разработке дополнительных средств обеспечения целостности данных, необходимо учитывать влияние дестабилизирующих факторов

среды передачи данных, сложность устройства реальной аппаратуры (оборудования) СППД, а также модификации основных видов атак злоумышленников.

Во втором разделе рассмотрены основные методы обеспечения целостности данных в СППД, приведены их основные достоинства и недостатки. Эффективным методом обеспечения целостности данных является вычисление контрольных сумм с помощью кодов обнаруживающих и исправляющих ошибки, а также хэш-функций [9] . Преимуществом помехоустойчивых кодов перед применением хэш-сумм является возможность локализации места возникновения ошибок и возможность их непосредственного исправления. Поэтому целесообразно разрабатывать помехоустойчивые коды с заданной корректирующей способностью, что и производится в исследовании. Сделан вывод, что использование представленных методов обеспечения целостности данных (как по отдельности, так в совокупности) в условиях динамической и быстро изменяющейся обстановки не позволяет обеспечить необходимый уровень защищенности информации, циркулирующей в СППД. Следовательно, возникает насущная необходимость в разработке дополнительных программно-аппаратных средств, способных обеспечивать своевременное обнаружение и исправление нарушений целостности передаваемых данных.

В третьем разделе предложен подход к моделированию СППД с использованием математического аппарата теории массового обслуживания, в которой пакеты передаваемых данных отождествляются с заявками, очереди заявок – с потоком пакетов, использована модель одноканальной системы массового обслуживания с интенсивностью обслуживания λ и простейшим потоком заявок. Применение этого подхода позволило диагностировать признак несанкционированного доступа к СППД, как отклонения временных параметров доставки пакетов. Фиксация этого факта осуществлялась по значениям интенсивностей поступивших пакетов данных, интенсивностей принятых к обработке пакетов данных и интенсивностей, находящихся в очереди и ожидающих обработки пакетов данных, величины которых устанавливаются протоколами передачи телеметрии.

В результате несанкционированного доступа к СППД и отрицательно действующих факторов среды передачи данных возникает вероятность сбоев в работе программно-аппаратных средств СППД. Находящиеся в приемном устройстве пакеты данных, поступают в буферную память системы, формируют очередь и отправляются в подсистему обнаружения признаков несанкционированного доступа к СППД, построенной на основе аппарата теории массового обслуживания (ТМО), в которой происходит анализ информации о состоянии очереди и оценка интенсивностей поступивших пакетов данных, интенсивностей принятых к обработке пакетов данных и

[9] Харкевич А.А. Борьба с помехами//Москва: Государственное издательство физико-математической литературы – 1963.-Р.345 с.

интенсивностей, находящихся в очереди и ожидающих обработки пакетов данных.

Структура передаваемых телеметрических данных рассмотрена, как сочетание самих данных в виде пакета, согласно Госстандарту телеметрии пакетной передачи информации ГОСТ Р 56096-2014 [10]. 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.

Установлена адекватность компонентов между параметрами модели системы массового обслуживания (СМО) и СППД: требование интерпретируется, 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 заявок рассматривается как последовательность пакетов данных. Под операцией кодирования интерпретируется точечный процесс. Продолжительность обслуживания заявок рассматривается как моменты времени, связанные с поступлениями пакетов, определяемым своим компенсатором. Семимартингальное (траекторное) описание СМО (в терминах считающих процессов и их компенсаторов) позволяет 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.

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 использованы соответствующие интенсивности поступивших пакетов данных, интенсивности принятых к обработке пакетов данных и интенсивности, находящихся в очереди и ожидающих обработки пакетов данных, которые позволили эффективно обнаруживать в реальном канале пакеты данных с признаками нарушения целостности.

Уравнение системы массового обслуживания представлено в следующем виде:

$$Q_t = Q_0 + A_t + R_t - D_t, \qquad (1)$$

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.

[10] ГОСТ Р56096-2014 Система передачи космических данных и информации. Пакетная телеметрия (Переиздание), ГОСТ Р от 09 сентября 2014 года №56096-2014.

Точечные процессы A_t , D_t , R_t $(t \geq 0)$ определены своими компенсаторами (предсказуемый возрастающий случайный процесс). В результате получены следующие соотношения:

$$A_t = \lambda \cdot t, \tag{2}$$

$$D_t = \int_0^t \mu \cdot Q_s \, ds, \tag{3}$$

$$R_t = \int_0^t \rho \cdot Q_s \, ds, \tag{4}$$

где λ – интенсивность поступивших 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 $t = s$, $\lambda, \mu, \rho > 0$.

Для оценивания параметров модели в семимартингальном описании, использовались следующие соотношения:

$$\begin{cases} \left(A_t\right)_{0 \leq s \leq t}, \\ \left(X_t^0\right)_{0 \leq s \leq t}, \\ \left(X_t^m\right)_{0 \leq s \leq t}, \end{cases} \tag{5}$$

$$X_t^0 = \int_0^t I\left(Q_s = 0\right) ds, \tag{6}$$

$$X_t^m = \int_0^t I\left(Q_s = m\right) ds, \; m \geq 1, \tag{7}$$

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

Несмещенной состоятельной оценкой для интенсивности поступивших в систему пакетов данных λ является:

$$\lambda_t = \frac{A_t}{t}. \tag{8}$$

Воспользовавшись неравенством Чебышева, которое утверждает, что случайная величина в основном принимает значения, близкие к своему среднему, получено следующее выражение:

$$\forall \varepsilon > 0 \;\; P\left\{\left|\frac{A_t}{t} - \lambda\right| > \varepsilon\right\} < \frac{D\left(A_t / t\right)}{\varepsilon^2}, \tag{9}$$

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

Индикаторная функция $I\left(Q_t = k\right)$, $k \geq 0$ представлена в виде:

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

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

Для выражения параметров λ, μ, ρ произведен расчет компенсаторов найденных индикаторов. Для индикаторной функции $I\left(Q_s=0\right)$ компенсатор определен выражением:

$$I\left(Q_t=0\right)=I\left(Q_0=0\right)-\lambda\int_0^t I\left(Q_s=0\right)ds+\mu\int_0^t I\left(Q_s=1\right)ds. \qquad (10)$$

Для индикаторной функции $I\left(Q_s=k\right)$ компенсатор определен выражением:

$$\begin{aligned} I\left(Q_t=k\right)&=I\left(Q_0=0\right)k+\lambda\int_0^t I\left(Q_s=k-1\right)ds+\rho\left(k-1\right)\int_0^t I\left(Q_s=k-1\right)ds-\\ &-\left(\lambda-\mu\cdot k+\rho\cdot k\right)\int_0^t I\left(Q_s=k\right)ds+\mu\left(k+1\right)\int_0^t I\left(Q_s=k+1\right)ds. \end{aligned} \qquad (11)$$

Обозначены локальные времена:

$$\lambda\int_0^t I\left(Q_s=0\right)ds=X_t^k,\quad k=0,1,2,\ldots\ . \qquad (12)$$

Получена система:

$$\begin{cases} a^{(1)}=\dfrac{\lambda}{\mu}\cdot a^{(0)},\\ a^{(2)}=\dfrac{\lambda+\rho}{2\cdot\mu}\cdot a^{(1)},\\ a^{(3)}=\dfrac{\lambda+2\cdot\rho}{3\cdot\mu}\cdot a^{(2)},\\ a^{(4)}=\dfrac{\lambda+3\cdot\rho}{4\cdot\mu}\cdot a^{(3)}. \end{cases} \qquad (13)$$

В результате анализа полученной системы (13) сделан вывод, что каждый последующий аппроксимирующий коэффициент $a^{(k)}$ находится рекуррентно. Получено выражение:

$$a^{(k)}=\frac{\left(k-1\right)!\cdot\lambda\cdot a^{(0)}\rho^{(k-1)}\prod_{i=1}^{k-1}\left(1+\dfrac{\lambda}{i\cdot\rho}\right)}{k!\cdot\mu^{(k)}}=\frac{\lambda\cdot a^{(0)}\rho^{(k-1)}\prod_{i=1}^{k-1}\left(1+\dfrac{\lambda}{i\cdot\rho}\right)}{k\cdot\mu^{(k)}}. \qquad (14)$$

Установлено, что разность

$$1-a^{(0)}=\sum_{k=1}^{\infty}a^{(k)}=\sum_{k=1}^{\infty}\frac{\lambda\cdot a^{(0)}\rho^{(k-1)}\prod_{i=1}^{k-1}\left(1+\dfrac{\lambda}{i\cdot\rho}\right)}{k\cdot\mu^{(k)}}. \qquad (15)$$

Применен метод аппроксимации к выражению (15), получено следующее выражение:

$$\sum_{k=1}^{\infty}\frac{\lambda\cdot a^{(0)}\rho^{(k-1)}\prod_{i=1}^{k-1}\left(1+\frac{\lambda}{i\cdot\rho}\right)}{k\cdot\mu^{(k)}}=c(\lambda,\mu,\rho), \quad (16)$$

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 уравнения (16) выражено $a^{(0)}$, получено следующее:

$$a^{(0)}=\left(1+\frac{\lambda}{\mu}\cdot c(\lambda,\mu,\rho)\right)^{-1}. \quad (17)$$

В нулевом приближении $a^{(0)}=\left(1+\frac{\lambda}{\mu}\right)^{-1}$. Из уравнения (17) выражена оценка параметра интенсивности принятых к обработке пакетов данных μ_t:

$$\mu_t=\frac{\lambda\cdot a^{(0)}}{1-a^{(0)}}. \quad (18)$$

Воспользовавшись процедурами аппроксимации, установлено, что $\frac{1}{2}\cdot\left(\frac{\rho}{\mu}\right)\cdot\left(1+\frac{\lambda}{\rho}\right)\sim\frac{\rho}{2\cdot\mu}$ и из приближения $a^{(0)}=\left(1+\frac{\lambda}{\mu}\cdot\left(1+\frac{\rho}{2\cdot\mu}\right)\right)^{-1}$ выражена оценка, поступивших в очередь и ожидающих обслуживания пакетов данных ρ_t:

$$\rho_t=\frac{2\cdot\mu^{(2)}}{\lambda\cdot a^{(0)}}\cdot\left(1-a^{(0)}-\frac{\lambda}{\mu}\cdot a^{(0)}\right). \quad (19)$$

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

$$\begin{cases}\lambda_t=\frac{A_t}{t},\\ \mu_t=\frac{\lambda\cdot a^{(0)}}{1-a^{(0)}},\\ \rho_t=\left(\frac{m\cdot\lambda^{(m)}\cdot a^{(m)}}{\lambda\cdot a^{(0)}}\right)^{\frac{1}{m-1}},\end{cases} \quad (20)$$

где

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

Алгоритм функционирования построенной подсистемы обнаружения признаков несанкционированного доступа к СППД на основе аппарата ТМО представлен на рис. 1.

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.

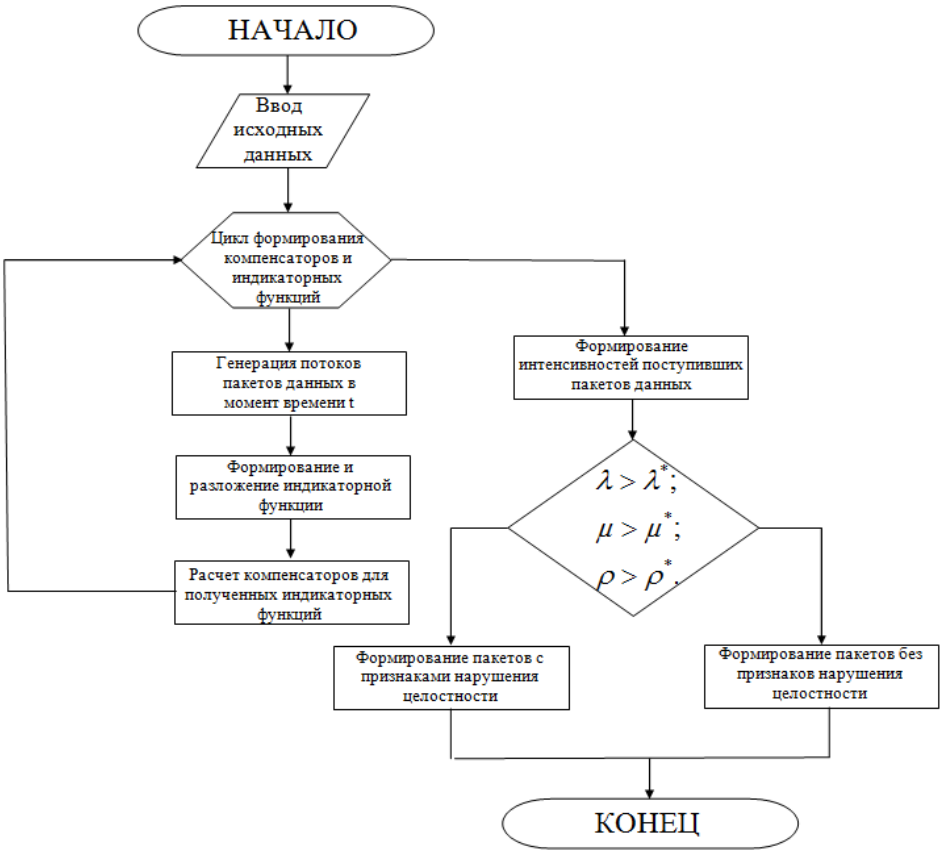


Рис. 1. Алгоритм функционирования разработанной подсистемы обнаружения признаков несанкционированного доступа

Граф состояний подсистемы обнаружения признаков несанкционированного доступа к СППД представлен на рис. 2.

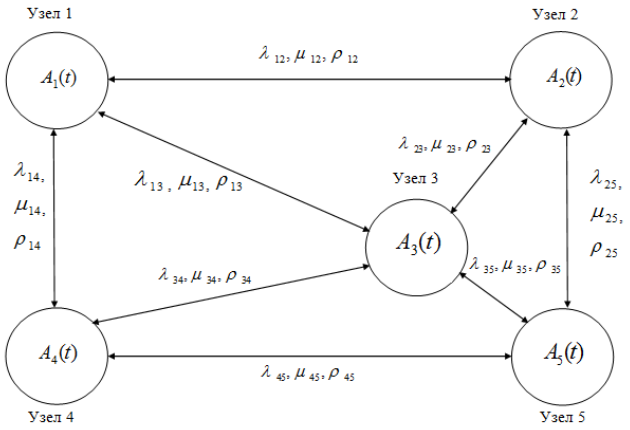


Рис. 2. Граф состояний подсистемы обнаружения признаков несанкционированного доступа к СППД

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 пакетов данных, интенсивностями принятых к обработке пакетов данных, интенсивностями, находящихся в очереди и ожидающих обработки пакетов данных.

На рис. 3, 4, 5 показаны зависимости оценок λ_t , μ_t и ρ_t от модельного времени t (время моделирования измеряется в минутах) при фиксированном значении компенсатора процесса $I\left(Q_t = k\right)$.

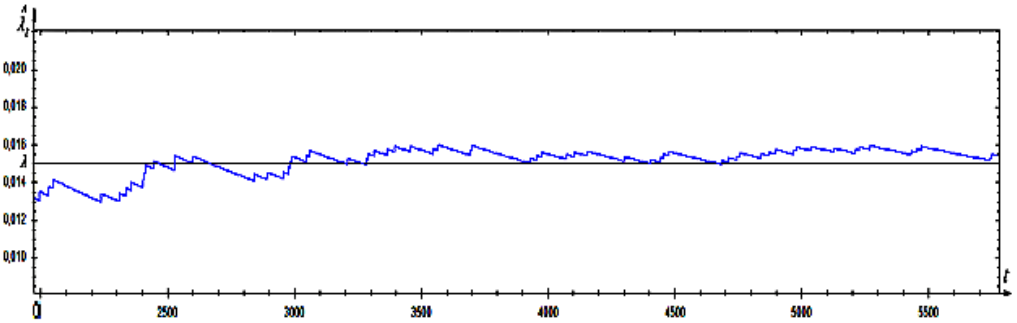


Рис. 3. График оценки интенсивности поступивших пакетов данных в СППД λ_t

На рис. 3 представлен график оценки интенсивности поступивших в систему пакетов данных. Из анализа графика сделан вывод, что при помощи выражений (1) – (8) произведена оценка интенсивности поступивших в систему пакетов при фиксированном значении компенсатора $I\left(Q_t = k\right)$ и модельном времени t.

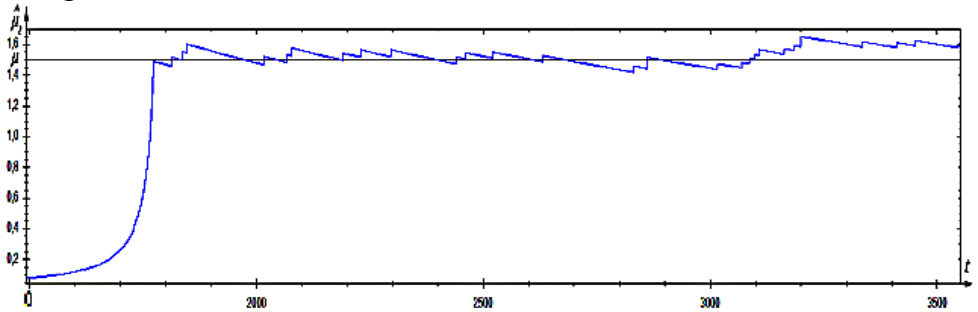


Рис. 4. График оценки интенсивности принятых к обработке пакетов данных μ_t

На рис. 4 представлен график оценки интенсивности принятых к обработке пакетов данных. Из анализа графика следует вывод, что с использованием выражений (9) – (18), получена оценка интенсивности принятых к обработке пакетов данных при фиксированном значении компенсатора $I\left(Q_t = k\right)$ и модельном времени t . Использование формул (9) – (18), позволило установить тот факт, что обслуживание пакетов данных

происходит без существенных отклонений в течение заданного времени моделирования.

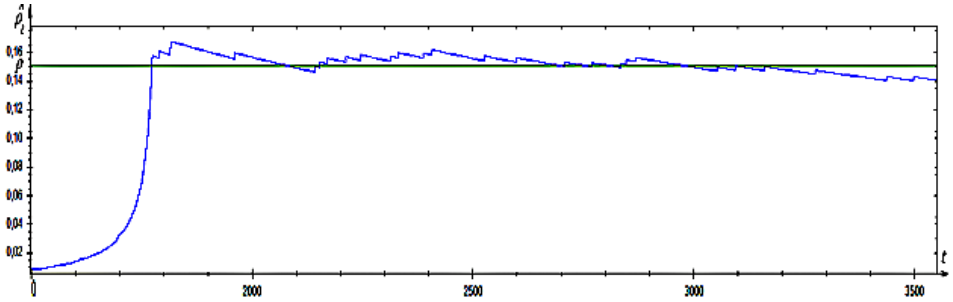


Рис. 5. График оценки интенсивности, находящихся в очереди и ожидающих обработки пакетов данных ρ_t

На рис. 5 представлен график оценки интенсивности, находящихся в очереди и ожидающих обработки пакетов данных. Из графика сделан вывод, что использование выражений (9) – (20) позволило произвести моделирование для оценки интенсивности, находящихся в очереди и ожидающих обработки пакетов данных, при фиксированном значении компенсатора и модельном времени t.

Разработан подход к обнаружению признаков несанкционированного доступа к СППД на основе аппарата ТМО с использованием индикаторных функций и их компенсаторов. С помощью него определяется факт несанкционированного доступа к СППД 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.

В четвертом разделе предложен вариант эффективного применения модификации 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 является применение этого метода для подготовки готовых таблиц заранее вычисленных значений интенсивностей поступивших пакетов данных, интенсивностей принятых к обработке пакетов данных, интенсивностей, находящихся в очереди и ожидающих обработки пакетов данных для учета отклонений этих значений от интенсивностей, заданных протоколами телеметрии, что позволило существенно ускорить процесс обработки пакетов на выбранном отрезке времени. При расчете значений интенсивностей с использованием модификации численного метода градиентного спуска 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.

В третьей главе диссертации рассмотрены известные модели каналов передачи данных, произведен сравнительный анализ используемых приемов и средств обнаружения и исправления ошибок в пакетах данных при передаче по СППД. Рассмотрен подход к обнаружению и исправлению ошибок на основе применения кодов с фиксированными весами. Третья глава диссертации состоит из десяти разделов.

В первом разделе 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 является 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.

Во втором разделе рассмотрен состав передаваемой телеметрической информации. Основной единицей телеметрической информации являются числовые данные о контролируемых или наблюдаемых объектах, расположенных на больших расстояниях от получателя, из которых формируются передаваемые данные по каналу передачи данных. 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.

В третьем разделе 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[11]. Преимуществом кодов с переменным весом является эффективность их использования в современных каналах передачи данных при условии быстрой генерации двоичными кодами чисел с переменными весами.

В четвертом разделе определены параметры двоичных кодов с переменным весом, рассмотрены существующие способы подсчета единиц в двоичном коде, выявлены основные недостатки рассмотренных подходов. 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. Рассмотрены способы реализации метода, который может быть реализован программным путем и аппаратным способом. Представлена схема получения единицы двоичного числа на текущем шаге рекурсии.

[11] Смагин А.А. Модели разбиений. Ульяновск: УлГУ, 2013.-207 с.

В пятом разделе представлен алгоритмический подход генерации двоичных кодов целых чисел с переменным весом. 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. Отмечено, что такой подход представляет двухуровневый процесс кодирования данных, включающий попеременное обращение к матричным числам и дугам наложенного графа.

В шестом разделе представлен процесс формирования двоичного кода передаваемых данных с помощью матрично-алгоритмического кодирования. При использовании такого подхода обеспечивается биективность кодирования и декодирования из-за того, что структура матрицы имеет строго фиксированную организацию и все пути в ней являются уникальными.

В седьмом разделе представлен алгоритм декодирования кода с заданным весом. Приведены данные, характеризующие свойства матричного кодирования, для оценки возможностей использования разработанного алгоритма на практике.

В восьмом разделе 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. Структура этих средств, реализующая на практике подсистему обеспечения целостности данных на основе кодов с переменным весом, представлена на рис.6.

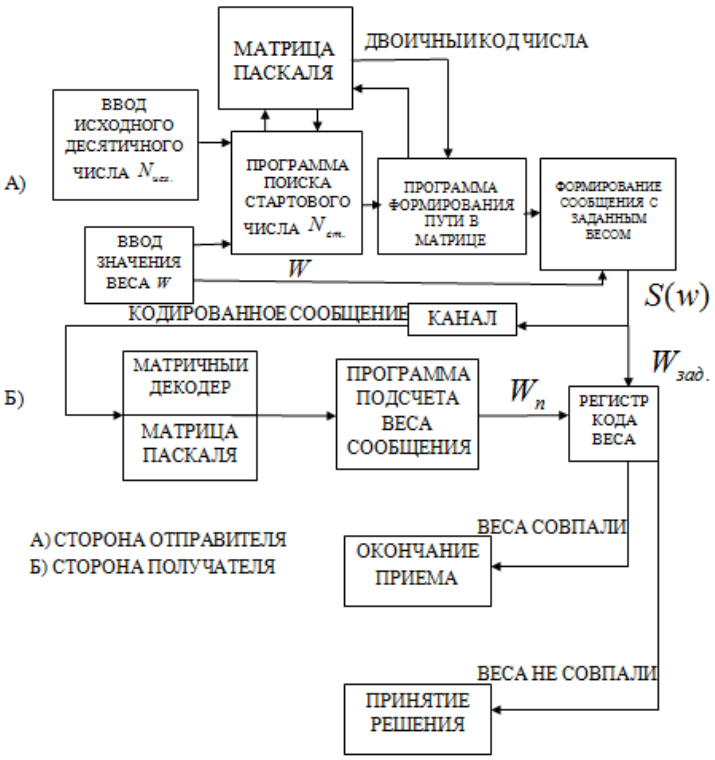


Рис. 6. Подсистема обеспечения целостности данных на основе кодов с переменным весом

В девятом разделе представлена процедура определения координат кодируемых чисел в матрицах весов, которая 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:

$$p_i = C_{l-2}^{w-1},$$

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.

В десятом разделе производится определение порядкового номера числа, образующего строку (ЧОС), внутри подматрицы. 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. Представлены пошаговая процедура определения количества ЧОС в каждой подматрице и алгоритм определения номера ЧОС.

В четвертой главе главе разработана математическая модель подсистемы оценки риска повторных ошибок, вызванных сбоями приемной аппаратуры и программных средств СППД. 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 которой позволяет обнаруживать местоположения пачек ошибок, вычислять наибольшую вероятность присутствия этих ошибок на интервале проведения сеанса передачи-приема данных. Определен набор параметров, который необходимо учитывать при разработке математической модели подсистемы оценки риска повторного возникновения ошибок в пакетах данных после их поступления в приемное устройство СППД, а именно:

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

Разработана структурная схема функционирования системы обеспечения целостности данных (СОЦД), в основе которой лежат взаимодействующие между собой подсистемы обнаружения признаков

несанкционированного доступа к СППД, подсистемы обеспечения целостности телеметрических данных на основе кодов с переменным весом, подсистемы оценки риска повторных ошибок, вызванных сбоями приемной аппаратуры и программных средств).

Для построения соответствующих функциональных зависимостей использованы следующие параметры:

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

$$H_t = R \cdot e^{\alpha \cdot t}, \tag{21}$$

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:

$$V_t = \frac{V_0}{1 + t \cdot g}, \tag{22}$$

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

3. Резервная мощность СОЦД C_t:

$$C_t = C_0 + k \cdot t, \tag{23}$$

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

Риск повторного возникновения ошибки с учетом представленных выше выражений (21) – (23) определен следующим образом:

$$R_t = \frac{H_t \cdot V_t}{C_t}. \tag{24}$$

Функциональная зависимость φ_t, определяющая допустимые значения риска нарушения целостности, задана выражением:

$$\varphi_t = k \cdot g \cdot t + R_t \cdot a, \tag{25}$$

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

В результате роста уязвимости и снижения резерва мощности функциональная зависимость, определяющая допустимые значения риска повторного возникновения обнаруженной ошибки с учетом формул (24)-(25), принимает вид:

$$\varphi_t = k \cdot g \cdot t + \frac{a}{t} \cdot \int_0^T R_t \, dt. \tag{26}$$

На рис. 7 показан график функциональной зависимости φ_t, иллюстрирующий характер поведения компромисса между средним риском в системе и начальными скоростями роста резерва и уменьшения уязвимости системы.

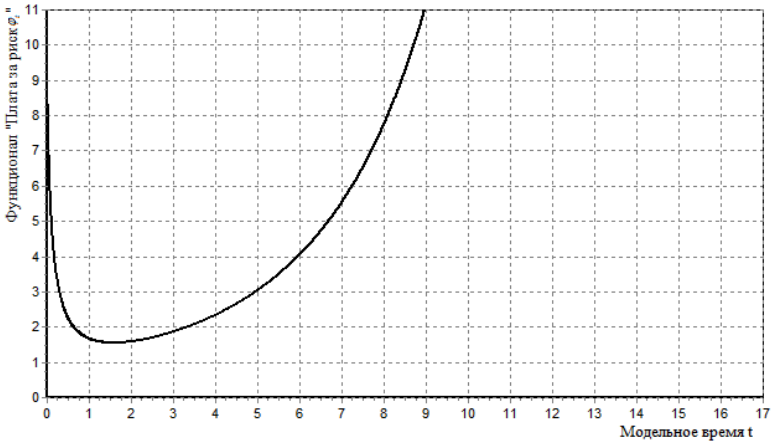


Рис. 7. Функциональная зависимость φ_t

При разработке соответствующего программного приложения учитывалась 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 рис. 8.

Рис. 8. Блок-схема алгоритма работы подсистемы оценки риска повторных ошибок, вызванных сбоями приемной аппаратуры и программных средств СППД

Разработанна программа для проведения имитационного моделирования, которая выводит на экран результаты численного моделирования в виде графиков.

Приведены 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. Представлены результаты статистических экспериментов в виде соответствующей диаграммы.

- 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. Представлены результаты статистических экспериментов в виде соответствующей диаграммы.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ И ВЫВОДЫ

1. Разработан 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. Разработана математическая модель обнаружения признаков несанкционированного доступа к системе передачи-приема данных, которая 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. Организовано эффективное применение кодов с переменным весом, позволяющих 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, с возможностью 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. Разработана математическая модель определения риска повторных ошибок, вызванных сбоями приемной аппаратуры, использующая для оценки риска нарушения целостности сигмовидную функцию Гомперца, которая позволяет описывать с более высокой точностью угрозы нарушения целостности данных на начальной и завершающей стадиях функционирования системы передачи-приема данных.

5. Разработан 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.

СПИСОК ПУБЛИКАЦИЙ ПО ТЕМЕ ДИССЕРТАЦИИ

Работы, опубликованные в рецензируемых журналах, рекомендованных ВАК Министерства науки и высшего образования РФ:

1. Кузнецов Н.А., Мозоль А.А. Модель автоматизированной системы оптимизации параметров управления рисками в терминах угроз, уязвимостей и резервов // Вестник Воронежского института МВД России. - 2019. - №3. - С. 73-79.

2. Кузнецов Н.А., Мозоль А.А. Имитационное моделирование системы массового обслуживания с размножением сообщений в очередях // Т-COMM. Телекоммуникации и транспорт. - 2019. - №11. - С. 32-37.

3. Кузнецов Н.А. Метод построения нелинейного вейвлетного кода для обеспечения целостности данных в каналах связи // Т-COMM. Телекоммуникации и транспорт. - 2021. - №2. - С. 26-31.

4. Кузнецов Н.А. Метод оптимизации системы обеспечения целостности данных в дискретных каналах связи в условиях воздействия алгебраических манипуляций // Информация и космос. - 2021. - №1. - С. 104-111.

Публикации в иных изданиях:

5. Кузнецов Н.А. Рыскин С.В., Батяй А.Н., Мильчевич В.Я. Модели мультивариантных случайных блужданий//Сборник научных трудов «Проблемы обороноспособности и безопасности». Выпуск 19. М.:ФГБНУ «Экспертно-аналитический центр» Минобрнауки России, 2018.

6. Кузнецов Н.А., Батяй А.Н., Попова Ю.Н., Рыскин С.В., Соколовский Е.П. Имитационное моделирование системы оптимизации параметров управления рисками//Сборник научных трудов «Проблемы обороноспособности и безопасности». Выпуск 20. М.:ФГБНУ «Экспертно-аналитический центр» Минобрнауки России, 2018.

7. Кузнецов Н.А. Рыскин С.В., Батяй А.Н., Мильчевич В.Я. Имитационное моделирование систем оценивания характеристик СМО с размножением заявок в очередях//Сборник научных трудов «Проблемы обороноспособности и безопасности». Выпуск 19. М.:ФГБНУ «Экспертно-аналитический центр» Минобрнауки России, 2018.

Научное издание

Кузнецов Николай Алексеевич

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата технических наук
«разработка алгоритмов и моделирование обеспечения целостности данных в информационных системах обмена дискретной информацией»

05.13.18 – Математическое моделирование,
численные методы и комплексы программ (технические науки)