На правах рукописи

Студеникин Андрей Владимирович

МЕТОД ПРОТИВОДЕЙСТВИЯ УГРОЗЕ ПОДМЕНЫ СООБЩЕНИЙ ДЛЯ СИСТЕМ СПУТНИКОВОЙ СВЯЗИ С КОДОВЫМ РАЗДЕЛЕНИЕМ КАНАЛОВ НА ОСНОВЕ СТОХАСТИЧЕСКОГО ПРИМЕНЕНИЯ АНСАМБЛЕЙ МНОГОФАЗНЫХ ОРТОГОНАЛЬНЫХ КОДОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Специальность 2.3.6 –
«Методы и системы защиты информации, информационная безопасность»

АВТОРЕФЕРАТ
диссертации на соискание учёной степени
кандидата технических наук

Ставрополь – 2025

Работа выполнена в ФГАОУ ВО «Северо-Кавказский федеральный университет» на кафедре организации и технологии защиты информации факультета математики и компьютерных наук имени профессора Н.И. Червякова.

Научный руководитель: **Жук Александр Павлович,**

кандидат технических наук, профессор

Официальные оппоненты: **Лепешкин Олег Михайлович,**

доктор технических наук, доцент,
ФГБОУ ВО «Российский государственный гидрометеорологический университет», г. Санкт-Петербург, заведующий кафедрой информационных технологий и систем безопасности

Головской Василий Андреевич,

кандидат технических наук, доцент,
ФГКВОУ ВО «Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С.М. Штеменко» МО РФ, г. Краснодар,
начальник кафедры защиты информации от несанкционированного доступа

Защита состоится «19» февраля 2026 г. в 14:00 на заседании диссертационного совета ЮФУ801.02.10 Федерального государственного автономного образовательного учреждения высшего образования «Южный федеральный университет» по адресу: Ростовская обл., г. Таганрог, ул. Шевченко, 2, «Точка кипения» ИТА ЮФУ.

С диссертацией можно ознакомиться в Зональной научной библиотеке им. Ю.А. Жданова Южного федерального университета по адресу: г. Ростов-на-Дону, ул. Зорге, 21 Ж и на сайте: https://hub.sfedu.ru/diss/show/1347324/.

Отзыв в 2-х экз. *(с указанием ФИО (полностью), ученой степени со специальностью, звания, организации, подразделения, должности, адреса, телефона, e-mail, даты)* с заверенной подписью рецензента и печатью учреждения просим направлять ученому секретарю диссертационного совета ЮФУ801.02.10 по адресу: 347922, Ростовская обл., г. Таганрог, пер. Некрасовский, 44, к. 302, а также в формате pdf – на e-mail: uaishukova@sfedu.ru.

Автореферат разослан «___» декабря 2025 г.

Учёный секретарь
диссертационного совета
ЮФУ801.02.10,
кандидат технических наук, доцент Ищукова Е.А.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Совершенствованию систем передачи информации с технологией многостанционного доступа с кодовым разделением каналов (КРК) посвящено большое количество работ Л.Е. Варакина, В.И. Борисова, В.Б. Пестрякова, В.П. Ипатова, В.М. Зинчука, А.Е. Лимарева, Е.М. Сухарева, Н.Н. Залогина, В.В. Кислова и др., поскольку они составляют основу перспективных высокоскоростных систем, таких как 5G/6G, Wi-Fi и др. Анализ работ показывает, что методы доступа к спектру с несколькими несущими, включая мультиплексирование с ортогональным частотным разделением (OFDM) и множественный доступ с кодовым разделением с несколькими несущими (MC-CDMA), имеют ряд существенных преимуществ по сравнению с системами с одной несущей по помехозащищённости, эффективности использования спектра частот, конфиденциальности при передаче сообщений и другие.

Системы спутниковой связи (ССС) представляют собой специфическую разновидность беспроводных систем передачи информации, обеспечивающих глобальное информационное взаимодействие между собой, в которых передача информации осуществляется через искусственные спутники Земли.

Анализ работ в данной области показал, что среди многообразия видов множественного доступа в системах спутниковой связи (FDMA, TDMA, CDMA), доступ с кодовым разделением каналов и прямым расширением спектра (CDMA-DS) является достаточно распространенным.

Поскольку система спутниковой связи является беспроводной, то в силу специфики её функционирования угроза подмены сообщений может быть реализована в ней с высокой степенью вероятности.

В диссертационной работе предложен метод, предназначенный для противодействия угрозе подмены сообщений в системах ССС с КРК, в основе которого лежит стохастическое использование ансамблей многофазных ортогональных кодовых последовательностей (АМФОКП).

Степень разработанности темы. В исследованиях, направленных на повышение защищённости информации в ССС, предлагается применять кодовые последовательности с динамически изменяющейся структурой. Такой подход обеспечивает необходимый уровень структурной скрытности при стохастическом применении необходимого количества ансамблей ортогональных кодовых последовательностей (АОКП), при условии, что они удовлетворяют требованиям по спектральным и корреляционным свойствам.

В диссертационной работе автором обосновано, что в качестве сменяемых последовательностей для достижения требуемого показателя структурной скрытности $S_{\text{треб.}}$ целесообразно использовать АМФОКП, поскольку они имеют преимущество по их количеству, по сравнению с количеством двоичных ортогональных кодовых последовательностей, что очень важно при их стохастическом применении в ССС с КРК.

Для оценки показателя структурной скрытности сигналов S авторами З.М. Каневским, В.П. Литвиненко, Г.В. Макаровым предложено использовать структурную скрытность, которая определяется мощностью A (числом элементов) множества X возможных сменяемых параметров сигнала, измеряемую числом двоичных измерений (ДИЗ), которые необходимо провести для раскрытия структуры сигнала.

Оценка структурной скрытности кодовых последовательностей,

применяемых в существующих ССС с КРК, показала, что они не удовлетворяют требуемому значению $S_{\text{треб.}} \geq 43$ ДИЗ, а используемые в них известные АОКП Уолша, Стиффлера и др., которые влияют на этот показатель, не удовлетворяют требованию по их количеству. Также установлено, что по причине применения ограниченного числа известных ансамблей ортогональных кодовых последовательностей, используемых в ССС с КРК, устройства их формирования имеют недостаточные возможности, которые необходимо расширить с учетом обеспечения возможности формирования многофазных сигналов.

По этим причинам выявлено **противоречие в практике**, которое заключается в том, что используемые в настоящее время в ССС с КРК ортогональные кодовые последовательности не позволяют обеспечить требуемый уровень их структурной скрытности $S_{\text{треб.}} \geq 43$ ДИЗ, достаточный для противодействия угрозе подмены сообщений.

Для разрешения данного противоречия в работе проанализированы известные методы синтеза АОКП, позволяющие получить их увеличенное количество, которое при их стохастическом применении в ССС с КРК обеспечвает необходимый уровень их структурной скрытности $S_{\text{треб.}} \geq 43$ ДИЗ.

В результате анализа было установлено, что известные методы синтеза АОКП, обеспечивающие необходимый уровень их структурной скрытности, не позволяют разрешить выявленное ранее противоречие в практике, поскольку количество синтезируемых АОКП известными методами ограничено.

В связи с этим выявлено **противоречие в теории**, которое заключается в том, что что известные методы синтеза не позволяют получить АОКП в количестве, обеспечивающем требуемое значение их структурной скрытности Sтреб. ≥ 43 ДИЗ при стохастическом применении в ССС с КРК.

С учетом данных обстоятельств сделан вывод о том, что задача разработки метода противодействия угрозе подмены сообщений для ССС с КРК на основе синтеза, формирования и стохастического применения увеличенного количества ансамблей многофазных ортогональных кодовых последовательностей является **актуальной**.

Объектом исследования является система спутниковой связи с кодовым разделением каналов.

Предметом исследования является метод противодействия угрозе подмены сообщений для систем спутниковой связи с кодовым разделением каналов.

Целью исследований является повышение защищенности систем спутниковой связи с кодовым разделением каналов по показателю структурной скрытности за счет стохастического применения ансамблей многофазных ортогональных кодовых последовательностей с изменяющейся структурой.

Научная задача исследования заключается в разработке метода противодействия угрозе подмены сообщений для ССС с КРК на основе синтеза, формирования и стохастического применения АМФОКП.

Основные задачи исследования:

1. Разработать модель противодействия угрозе подмены сообщений в ССС с КРК на основе синхронного генерирования и стохастического применения АМФОКП размерностей $N = 128, 256$.

2. Разработать модель и алгоритм синтеза АМФОКП размерностей $N = 128, 256$, в количестве, обеспечивающем при стохастическом применении в ССС с КРК требуемый уровень их структурной скрытности $S_{\text{треб.}} \geq 43$ ДИЗ.

3. Разработать принцип построения и техническое решение стохастического средства защиты информации для ССС с КРК.

Методология и методы исследования работы составляют стохастические методы защиты информации, теория систем сигналов, теория вероятностей и математической статистики, математическое моделирование, сравнение и эксперимент.

Положения, выносимые на защиту:

1. Разработанная модель противодействия угрозе подмены сообщений в ССС с КРК на основе синхронного генерирования и стохастического применения АМФОКП обеспечивает повышение структурной скрытности выше требуемого значения $S_{\text{треб.}} \geq 43$ ДИЗ, отличается от известных тем, что при передаче каждого информационного бита используется уникальная неповторяющаяся структура многофазной ортогональной кодовой последовательности синхронно изменяемая на приемной и передающей сторонах.

2. Разработанная модель АМФОКП требуемых размерностей $N = 128, 256$ и алгоритм их синтеза, по сравнению с известной моделью ансамблей дискретных ортогональных многоуровневых сигналов (АДОМУС), позволяют увеличить выигрыш в структурной скрытности АМФОКП. Получаемые АМФОКП имеют прирост структурной скрытности по отношению к структурной скрытности АДОМУС, который лежит в пределах от 2,5 до 101,31% для порядка эрмитовой матрицы (ЭМ) $n = 128$, и в пределах от 2,32 до 101,02% для порядка ЭМ $n = 256$. Данный выигрыш обеспечивается при условии, что фаза каждого диагонального коэффициента эрмитовой матрицы изменяется на угол $\Delta\varphi_i = 18^{\circ}$ и, соответственно $\Delta\varphi_i = 1^{\circ}$. Значение структурной скрытности АМФОКП для $\Delta\varphi_i = 90^{\circ}$ также находится выше требуемого значения структурной скрытности $S_{\text{треб.}} \geq 43$ ДИЗ для $N = 128, 256$, что позволяет их использовать в существующих ССС с КРК.

3. Полученные принцип построения и техническое решение генератора псевдослучайных АМФОКП для стохастического средства защиты информации ССС с КРК, в отличие от известных, обеспечивают генерацию ансамблей многофазных ортогональных кодовых последовательностей, описываемых комплексными числами.

Научная новизна:

1. Разработанная модель противодействия угрозе подмены сообщений в ССС с КРК, отличающаяся от известных тем, что при передаче каждого информационного бита используется уникальная неповторяющаяся структура ансамбля многофазных ортогональных кодовых последовательностей синхронно изменяемых на приемной и передающей сторонах.

2. Модель АМФОКП требуемых размерностей $N = 128, 256$ и алгоритм их синтеза которые, в отличие от известных, основаны на рассмотрении множества эрмитовых матриц порядка $(n \times n)$, элементы которых являются комплексными числами и задают все возможные ортогональные базисы пространства C^n – комплексных чисел.

3. Принцип построения и техническое решение генератора псевдослучайных АМФОКП для стохастического средства защиты информации системы спутниковой связи с кодовым разделением каналов, позволяющие, в отличие от известных, генерировать псевдослучайные АМФОКП на основе собственных векторов эрмитовых матриц в соответствии с задаваемым набором псевдослучайных комплексных чисел.

Теоретическая значимость работы заключается в развитии стохастических методов защиты информации в ССС с КРК на основе повышения структурной скрытности за счет синтеза, генерации и стохастического применения АМФОКП, описываемых ортогональными базисами пространства комплексных чисел C^n, а также в получении аналитических зависимостей для расчета показателя структурной скрытности при применении АМФОКП, представляемых собственными векторами (СВ) ЭМ.

Практическая ценность работы состоит в следующем:

- Разработанные технические решения по повышению защищённости информации, защищённые патентами на изобретения и свидетельствами на регистрацию программ для ЭВМ, реализующие предложенные алгоритмы, обеспечивают реализацию модели и алгоритма противодействия угрозе подмены передаваемых в ССС с КРК сообщений на основе формирования и стохастического применения АМФОКП. В случае использования разработанного алгоритма противодействия угрозе подмены сообщений за счет стохастического применения неповторяющихся псевдослучайных АМФОКП происходит преобразование исходной информации и её передача в канал связи с помощью стохастическим образом изменяющихся ансамблей ортогональных кодовых последовательностей для передачи каждого информационного символа, что обеспечивает повышение их структурной скрытности. Получаемые АМФОКП имеют прирост структурной скрытности по отношению к структурной скрытности АДОМУС, который лежит в пределах от 2,5 до 101,31% для порядка матрицы $n = 128$, и в пределах от 2,32 до 101,02% для порядка матрицы $n = 256$, который соответственно обеспечивается при допустимых значениях фаз каждого диагонального коэффициента ЭМ $\Delta\varphi_i = 18^\circ$ и $\Delta\varphi_i = 1^\circ$. Величина структурной скрытности АМФОКП для $\Delta\varphi_i = 90^\circ$ также находится выше требуемого значения структурной скрытности $S_{\text{треб.}} \geq 43$ ДИЗ для $N = 128, 256$, что позволяет их использовать в существующих ССС с КРК.
- Структура и алгоритм функционирования генератора псевдослучайных АМФОКП, защищённые патентами на изобретения и свидетельствами на регистрацию программ для ЭВМ, позволяют формировать АМФОКП с изменяющейся структурой на основе СВ ЭМ в соответствии с набором псевдослучайных комплексных чисел, поступающих на вход генератора, и могут быть применены для усовершенствования стохастического средства защиты информации в ССС с КРК.
- Разработанное программное обеспечение для ПЭВМ в пакете Matlab SIMULINK, защищённое свидетельством о государственной регистрации программы для ЭВМ позволяет выполнять исследования процесса передачи информации в модели ССС с КРК на основе стохастического применения АМФОКП при изменении отношения сигнал/шум в канале связи.
- Даны рекомендации по использованию компьютерной модели ССС с КРК в пакете Matlab SIMULINK, реализующей модель противодействия угрозе подмены сообщений на основе применения стохастического средства защиты информации.

Степень достоверности результатов диссертационного исследования обеспечивается методологической строгостью применения математического аппарата. Эффективность разработанных методов и алгоритмов подтверждена экспериментально путём компьютерного моделирования в программных средах Matlab и Matlab SIMULINK. Все ключевые положения, ограничения и

допущения, использованные в работе, соответствуют опубликованным научным данным в рамках исследуемой тематики. Экспериментальные данные, полученные в ходе исследования, согласуются с частными результатами авторитетных работ в данной области. Техническая новизна генератора АМФОКП и ССС с КРК, использующих стохастическое средство защиты информации, подтверждается имеющимися у автора патентами на изобретения.

Апробация результатов диссертационного исследования. Основные положения и результаты диссертации обсуждались и получили положительную оценку на всероссийских и международных НТК, в том числе: IX Всероссийской НТК «Студенческая наука для развития информационного общества» (Ставрополь, 2018 г.); Workshop on computer science and information technologies 21thCSIT'2019 (Vienna, Austria, 2019г.); II Всероссийской научной конференции (с приглашением зарубежных ученых) «Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации» (Ставрополь, 2020г.); Международной НПК «Глобальные тенденции и перспективы цифровизации экономики, образования и науки – 2021» (Ставрополь, 2021г.); Всероссийской НТК «Теория и практика обеспечения информационной безопасности» (Москва, 2021г.); Всероссийской конференции «Радиоэлектронные устройства и системы для инфокоммуникационных технологий - РЭУС-2022» (Москва, 2022г.); XLI Всероссийской НТК «Проблемы эффективности и безопасности функционирования сложных технических и информационных систем» (Серпухов, 2022г.); IV Всероссийской НПК «Социотехнические и гуманитарные аспекты информационной безопасности» (Пятигорск, 2023г.) и др.

Внедрение результатов исследования проведено в ООО «Инфоком-С» в научно-практических исследованиях по созданию новых и совершенствованию существующих методов и алгоритмов скрытного информационного обмена в беспроводных системах передачи данных в системе комплексной безопасности распределенных объектов на базе программной платформы «Дарвис» с целью повышения скрытности от деструктивных воздействий информации, передаваемых в беспроводных каналах связи; в учебный процесс ФГАОУ ВО «Северо-Кавказский федеральный университет», а также выполнением работ по гранту «Грант-ИБ» № 29/2020 от 14.10.2020 г. РТУ МИРЭА.

Публикации. Основные положения диссертации опубликованы в 14 научных печатных работах в том числе: 5 – в ведущих рецензируемых научных журналах, входящих в перечень ВАК РФ, 9 – в материалах конференций и других изданиях. Получено 4 патента на изобретение, 3 свидетельства о государственной регистрации программ для ЭВМ.

Личный вклад автора. Все результаты, представленные в исследовании, были получены при личном участии автора. Основной вклад автора включает следующие аспекты: 1) разработка модели противодействия угрозе подмены сообщений в ССС с КРК на основе стохастического применения АМФОКП; 2) разработка модели АМФОКП и алгоритма синтеза их увеличенного количества для ССС с КРК; 3) разработка структуры и алгоритма функционирования генератора псевдослучайных АМФОКП для стохастического средства защиты информации (в соавторстве); 4) разработка программной модели защищённой ССС с КРК со стохастическим применением АМФОКП (в соавторстве).

Структура и объем работы. Объём диссертационной работы составляет

247 страниц основного содержания. Материал сопровождается 81 иллюстрацией и 15 таблицами. Структура исследования включает введение, четыре раздела, заключение, список из 145 использованных источников и три приложения.

СОДЕРЖАНИЕ РАБОТЫ

Во введении данной работы обоснована актуальность темы, проанализированы текущие исследования и выявлены проблемные области в защите спутниковой связи от угроз подмены сообщений. Определены объект, предмет, цель и задачи исследования. Описаны новизна, практическая ценность, апробация и внедрение результатов, а также представлены основные защищаемые положения и общая структура диссертации.

В первой главе последовательно проведен анализ функционирования существующих ССС с КРК, проанализированы пути повышения защищенности ССС с КРК, обоснована целесообразность противодействия угрозе подмены сообщений в них за счет увеличения структурной скрытности используемых АОКП с изменяющейся структурой. С учетом сделанных выводов определены задачи исследования, обоснована необходимость разработки метода противодействия угрозе подмены сообщений в ССС с КРК на основе синтеза, формирования и стохастического применения АОКП.

Обоснована необходимость усовершенствования процесса защиты информации в ССС с КРК на основе увеличения структурной скрытности АОКП, которая подразумевает под собой степень затруднения определения злоумышленником структуры информационного сигнала при попытке реализации угрозы подмены сообщений.

Анализ результатов расчетов показателя структурной скрытности в зависимости от базы сигнала, представленный на рисунке 1 и рисунке 2, свидетельствует о том, что известные последовательности Уолша и M-последовательности, используемые в ССС с КРК, обладают низкой структурной скрытностью, которая значительно ниже $S_{\text{треб.}} \geq 43$ ДИЗ.

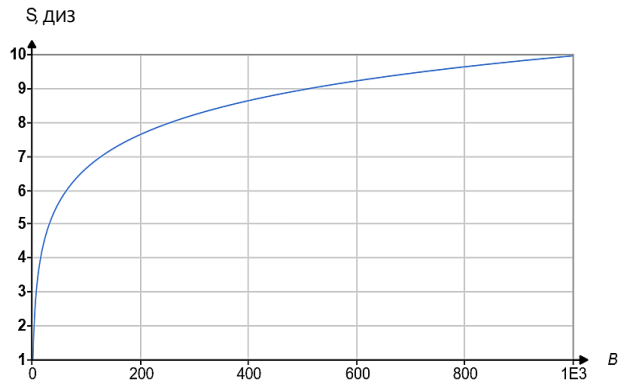

Рисунок 1 – График зависимости структурной последовательностей Уолша $S_{\text{Уолша}}$ от базы B

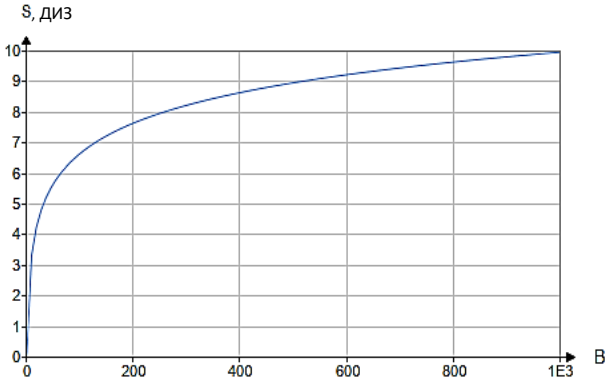

Рисунок 2 – График зависимости структурной скрытности M-последовательностей S_M от базы B

Проведен анализ известных ортогональных кодовых последовательностей, а также определены параметры их структурной скрытности для баз $B = 128$ и $B = 256$. Графическая интерпретация результатов анализа приведена на рисунке 3.

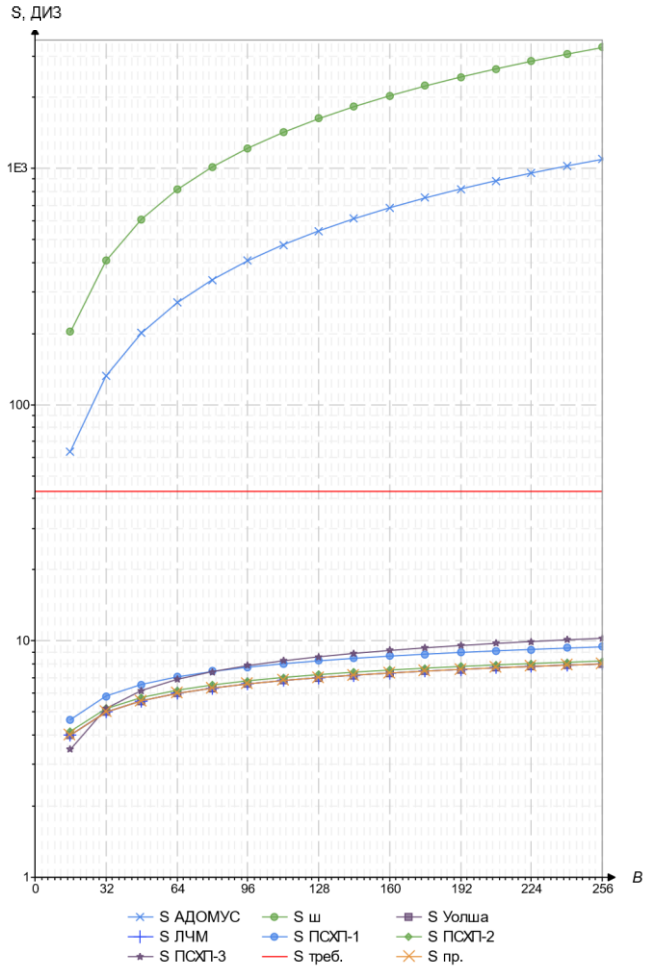

Рисунок 3 – Значения структурной скрытности S известных ортогональных кодовых последовательностей для баз $B = 128$ и $B = 256$

Анализ значений структурной скрытности известных ортогональных кодовых последовательностей для баз $B = 128$ и $B = 256$ показал, что их структурная скрытность не достигает требуемого значения $S_{\text{треб.}} \geq 43$ ДИЗ, за исключением многопозиционных ансамблей дискретных ортогональных многоуровневых сигналов $S_{\text{АДОМУС}}$ при базе сигнала $B > 10$ и многопозиционной импульсной последовательности на основе реализации шума $S_{\text{Ш}}$ при базе сигнала $B > 4$.

При этом установлено, что что многопозиционные АДОМУС в ССС с КРК, использоваться не могут, поскольку они являются многоуровневыми и обладают низкой помехоустойчивостью, что неприемлемо для спутниковых радиолиний, а практическая реализация информационного обмена на базе случайного процесса затруднительна, ввиду невозможности обеспечения устойчивой синхронизации приемной и передающей частей аппаратуры, а также сложности генерации идентичных кодовых последовательностей в цифровом виде на основе аналогового случайного процесса на приемной и передающей сторонах ССС с КРК.

Таким образом, известные методы построения АОКП по показателю структурной скрытности не позволяют обеспечить её требуемое значение $S_{\text{треб.}} \geq 43$ ДИЗ.

С учетом выявленных противоречий в практике и теории сформулирована научная задача, заключающаяся в разработке метода противодействия угрозе подмены сообщений для ССС с КРК на основе синтеза, формирования и стохастического применения АМФОКП, который включает в себя:

– модель противодействия угрозе подмены сообщений в ССС с КРК на основе стохастического применения АМФОКП;

– модель АМФОКП и алгоритм синтеза их увеличенного количества для стохастического применения в ССС с КРК, обеспечивающие требуемый уровень их структурной скрытности;

– принцип построения и техническое решение стохастического средства защиты информации для ССС с КРК.

Во второй главе решена первая основная задача исследования. В ней разработана модель противодействия угрозе подмены сообщений в ССС с КРК на основе синхронного генерирования и стохастического применения АМФОКП размерностей $N = 128,256$, которая позволяет повысить показатель их структурной скрытности, что обеспечивает эффективное противодействие угрозе подмены сообщений в ССС с КРК. Разработанная модель противодействия угрозе подмены сообщений, представленная на рисунке 4, состоит из 14 этапов и позволяет в процессе передачи информации реализовать стохастическое применение АМФОКП синхронно на передающей и приемной сторонах.

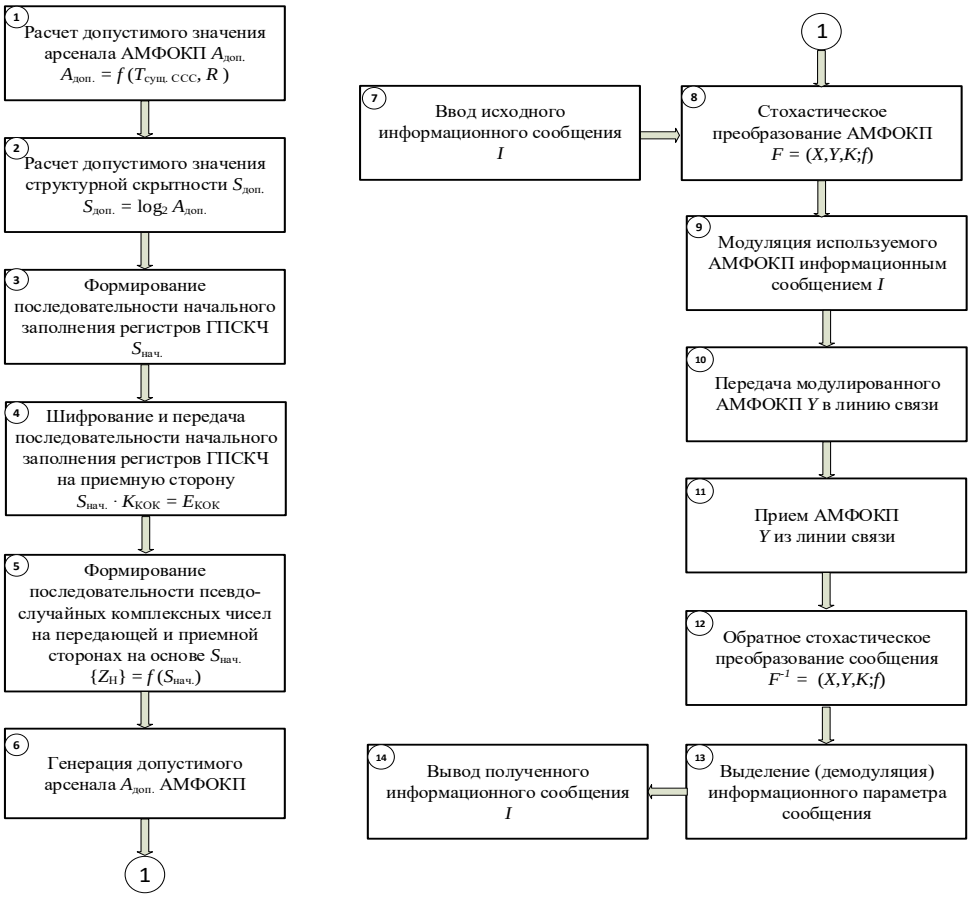

Рисунок 4 – Модель противодействия угрозе подмены сообщений в ССС с КРК

Применение разработанной модели противодействия угрозе подмены сообщений позволяет в процессе сеанса связи при передаче каждого информационного бита использовать уникальную неповторяющуюся структуру ортогональных кодовых последовательностей, за счет чего обеспечивается требуемое значение структурной скрытности АМФОКП, применяемых в ССС с КРК.

В данном разделе определено, что для того, чтобы ансамбли

ортогональных кодовых последовательностей обеспечивали требуемое значение структурной скрытности $S_{\text{треб.}} \geq 43$ ДИЗ, необходимо разработать алгоритм синтеза АМФОКП, обеспечивающий получение требуемого их количества $A_{\text{треб.}} \geq 4{,}54 \cdot 10^{12}$.

В третьей главе решена вторая основная задача исследования – разработана модель АМФОКП и алгоритм синтеза их требуемого количества $A_{\text{треб.}} \geq 4{,}54 \cdot 10^{12}$, обеспечивающих требуемый уровень их структурной скрытности $S_{\text{треб.}} \geq 43$ ДИЗ при стохастическом применении в ССС с КРК.

Модель АМФОКП основана на использовании множества наборов СВ ЭМ, которые вычисляются в соответствии с задаваемым набором значений модулей и аргументов диагональных коэффициентов ЭМ. Используя различные наборы диагональных коэффициентов ЭМ, в соответствии с разработанным алгоритмом синтеза, определяются различные по своей структуре ансамбли ортогональных кодовых последовательностей в количестве, превышающем их требуемое значение $A_{\text{треб.}} \geq 4{,}54 \cdot 10^{12}$ для размерностей $N = 128, 256$.

С учетом того, что наибольшие возможности по охватываемому объему ортогональных базисов имеет подход, основанный на рассмотрении СВ ЭМ вида (1), их СВ выбраны в качестве моделей АМФОКП.

$$A = \begin{pmatrix} d_{1,1} & a_{1,2} \cdot e^{j\varphi_{1,2}} & \cdots & a_{1,m-1} \cdot e^{j\varphi_{1,m-1}} & a_{1,m} \cdot e^{j\varphi_{1,m}} \\ a_{2,1} \cdot e^{-j\varphi_{2,1}} & d_{2,1} & \cdots & a_{2,m-1} \cdot e^{j\varphi_{2,m-1}} & a_{2,m} \cdot e^{j\varphi_{2,m}} \\ a_{3,1} \cdot e^{-j\varphi_{3,1}} & a_{3,2} \cdot e^{-j\varphi_{3,2}} & \cdots & a_{3,m-1} \cdot e^{j\varphi_{3,m-1}} & a_{3,m} \cdot e^{j\varphi_{3,m}} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{n-1,1} \cdot e^{-j\varphi_{n-1,1}} & a_{n-1,2} \cdot e^{-j\varphi_{n-1,2}} & \cdots & a_{n-1,m-1} \cdot e^{-j\varphi_{n-1,m-1}} & a_{n-1,m} \cdot e^{j\varphi_{n-1,m}} \\ a_{n,1} \cdot e^{-j\varphi_{n,1}} & a_{n,2} \cdot e^{-j\varphi_{n,2}} & \cdots & a_{n,m-1} \cdot e^{-j\phi_{n,m-1}} & d_{n,m} \end{pmatrix}, \quad (1)$$

где $a_{k,i} \cdot e^{-j\varphi_{k,i}} = a_{i,k} \cdot e^{j\varphi_{i,k}}$ – диагональные коэффициенты ЭМ являются комплексно-сопряженными числами, $d_{1,1} \ldots d_{n,m}$ – коэффициенты главной диагонали ЭМ, которые всегда вещественные числа $k = 1, 2, \ldots, n, i = 1, 2, \ldots, m$.

В работе рассмотрены бидиагональные ЭМ, у которых отличны от нуля главная диагональ и ближайшие к ней, расположенные выше и ниже неё, следующего вида

$$A = \begin{pmatrix} d_{1,1} & a_{1,2} \cdot e^{j\cdot\varphi_{1,2}} & 0 & 0 \\ a_{2,1} \cdot e^{-j\cdot\varphi_{2,1}} & d_{2,2} & a_{2,3} \cdot e^{j\cdot\varphi_{2,3}} & 0 \\ 0 & a_{3,2} \cdot e^{-j\cdot\varphi_{3,2}} & d_{3,3} & a_{3,4} \cdot e^{j\cdot\varphi_{3,4}} \\ 0 & 0 & a_{4,3} \cdot e^{-j\cdot\varphi_{4,3}} & d_{4,4} \end{pmatrix}. \quad (2)$$

Для бидиагональной ЭМ 4-го порядка вида (2) система её СВ описывается выражением

$$\overline{\mathrm{X}} = \begin{pmatrix} x_{1,1} \cdot e^{j\cdot\psi_{1,1}} & x_{1,2} \cdot e^{j\cdot\psi_{1,2}} & x_{1,3} \cdot e^{j\cdot\psi_{1,3}} & x_{1,4} \cdot e^{j\cdot\psi_{1,4}} \\ x_{2,1} \cdot e^{j\cdot\psi_{2,1}} & x_{2,2} \cdot e^{j\cdot\psi_{2,2}} & x_{2,3} \cdot e^{j\cdot\psi_{2,3}} & x_{2,4} \cdot e^{j\cdot\psi_{2,4}} \\ x_{3,1} \cdot e^{j\cdot\psi_{3,1}} & x_{3,2} \cdot e^{j\cdot\psi_{3,2}} & x_{3,3} \cdot e^{j\cdot\psi_{3,3}} & x_{3,4} \cdot e^{j\cdot\psi_{3,4}} \\ x_{4,1} \cdot e^{j\cdot\psi_{4,1}} & x_{4,2} \cdot e^{j\cdot\psi_{4,2}} & x_{4,3} \cdot e^{j\cdot\psi_{4,3}} & x_{4,4} \cdot e^{j\cdot\psi_{4,4}} \end{pmatrix}, \quad (3)$$

где $x_{k,i}$ – модули координат СВ ЭМ, а $\psi_{k,i}$ – аргументы координат СВ ЭМ, $n = 1, \ldots, 4,\ m = 1, \ldots, 4$.

Предложены аналитические выражения и утверждения, определяющие зависимость модулей и аргументов координат СВ ЭМ от значений модулей и аргументов её диагональных коэффициентов, на основе которых разработан алгоритм синтеза увеличенного количества АМФОКП, представленный на рисунке 5, включающий в себя семь этапов.

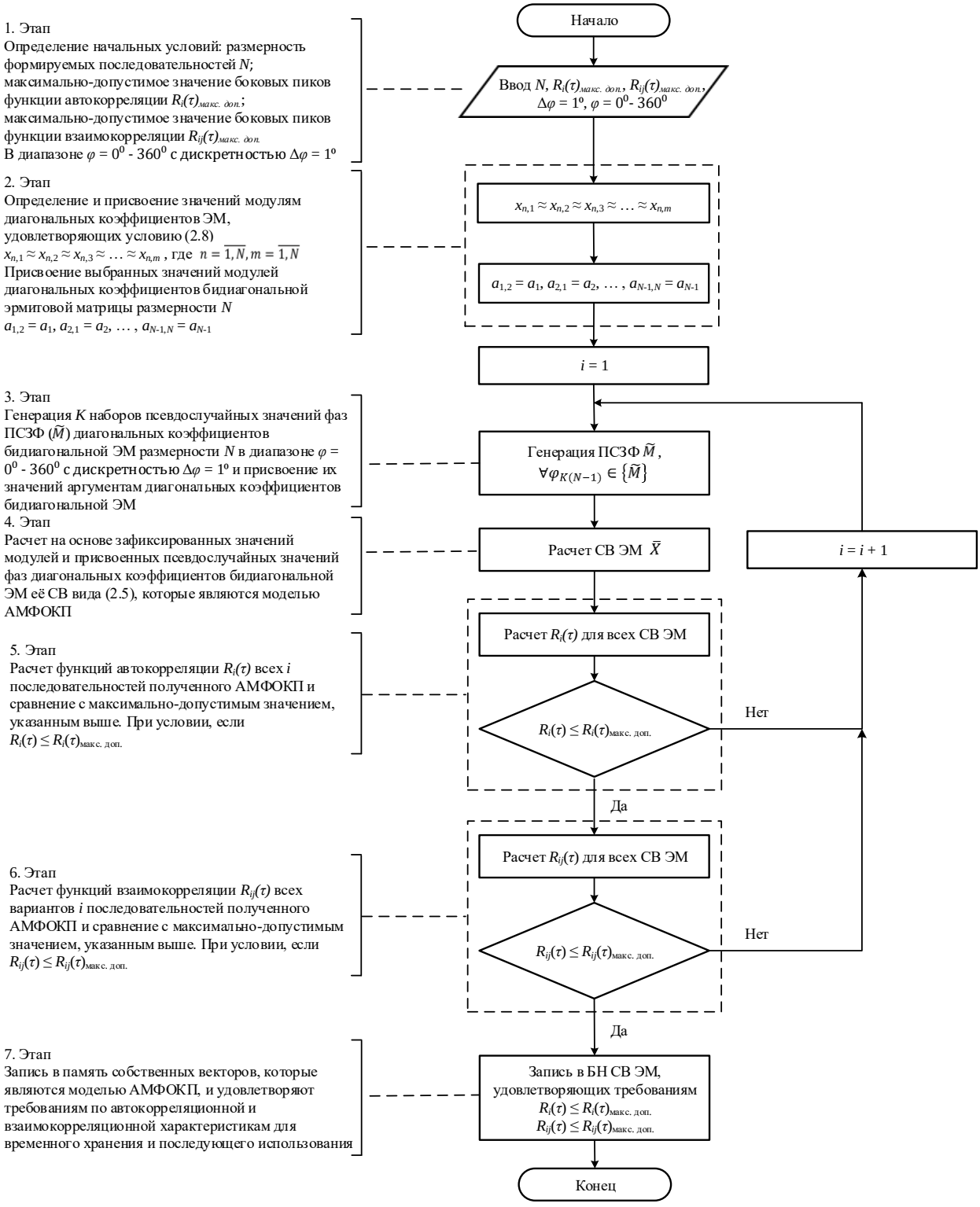

Рисунок 5 – Алгоритм синтеза увеличенного количества АМФОКП

Для оценки структурной скрытности АМФОКП, применяемых в ССС с

КРК, в работе проведен расчет их количества, которое может быть получено на основе разработанной модели и алгоритма синтеза, с последующим стохастическим использованием в процессе информационного обмена.

Для оценки структурной скрытности АМФОКП в диссертационной работе выведено математическое выражение для расчета числа возможных фазовых значений, принимаемых диагональными элементами бидиагональной ЭМ N −го порядка

$$Q = \prod_{i=1}^{N-1} K_i, \tag{4}$$

где $K_i = \frac{360^\circ}{\Delta\varphi_i}$ − количество используемых фаз рассматриваемого i −го диагонального коэффициента $A_i = a_i \cdot e^{j\varphi_i}$ бидиагональной ЭМ A, $\Delta\varphi_i$ − величина угла изменения фазы i −го диагонального коэффициента бидиагональной ЭМ, N- порядок ЭМ.

Сравнительный анализ количества АМФОКП и АДОМУС, представленный в таблице 1, показал, что АМФОКП обладают преимуществами по сравнению с известными АДОМУС по числу получаемых ансамблей ортогональных кодовых последовательностей при допустимых значениях фаз каждого элемента АМФОКП $\Delta\varphi_i = 18^\circ$ и $\Delta\varphi_i = 1^\circ$

Таблица 1 – Сравнительный анализ количества АМФОКП и АДОМУС для порядков матрицы $N = 128, 256$

Порядок матрицы, N	Количество АМФОКП при $\Delta\varphi_i = 1°$, Q	Количество АМФОКП при $\Delta\varphi_i = 18°$, Q	Количество АДОМУС, Q
128	$6{,}46 \cdot 10^{324}$	$1{,}70 \cdot 10^{165}$	$1{,}59 \cdot 10^{161}$
256	$5{,}37 \cdot 10^{651}$	$5{,}43 \cdot 10^{331}$	$1{,}62 \cdot 10^{324}$

С учетом количества АМФОКП Q при условии, что фаза каждого элемента кодовой последовательности может изменяться на угол $\Delta\varphi = 1°$, для заданного значения N проведен расчёт их структурной скрытности S_Q по формуле

$$S_Q = \log_2 Q = \log_2 \prod_{i=1}^{N-1} K_i = (N-1) \cdot \log_2 K. \tag{5}$$

В таблице 2 приведены показатели структурных скрытностей АМФОКП $S_{\text{АМФОКП}}$ при $\Delta\varphi_i = 1°$, $\Delta\varphi_i = 18°$, $\Delta\varphi_i = 90°$ и АДОМУС $S_{\text{АДОМУС}}$

Таблица 2 – Сравнительный анализ структурных скрытностей АМФОКП $S_{\text{АМФОКП}}$ и АДОМУС $S_{\text{АДОМУС}}$

Порядок матрицы, N	Структурная скрытность АДОМУС, $S_{\text{АДОМУС}}$	Структурная скрытность АМФОКП, $S_{\text{АМФОКП}}$ при $\Delta\varphi_i = 1°$	Структурная скрытность АМФОКП, $S_{\text{АМФОКП}}$ при $\Delta\varphi_i = 18°$	Структурная скрытность АМФОКП, $S_{\text{АМФОКП}}$ при $\Delta\varphi_i = 90°$
128	535,5	1078	548,88	254
256	1077	2165	1102	510

По результатам полученных значений структурной скрытности S, представленных в таблице 2, построены графики зависимостей структурных скрытностей АДОМУС и АМФОКП (для случаев изменения фазового сдвига между элементами кодовой последовательности на углы $\Delta\varphi_i = 1°$, $\Delta\varphi_i = 18°$ и $\Delta\varphi_i = 90°$) от длины последовательностей L, представленные на рисунке 6.

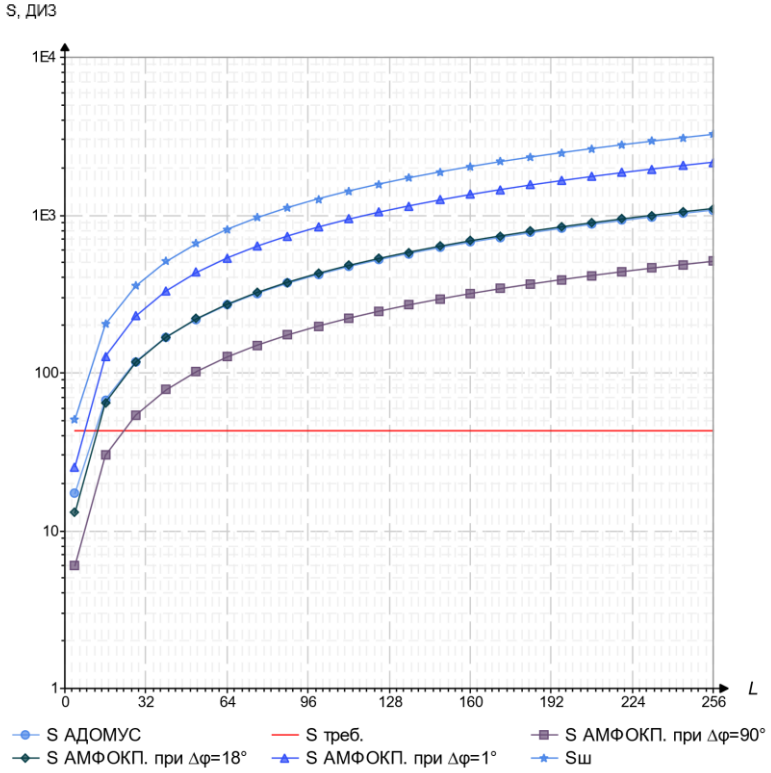

Рисунок 6 – Графики зависимостей структурной скрытности АДОМУС и АМФОКП, получаемых при изменении фазового сдвига между элементами кодовой последовательности на углы $\Delta\varphi_i = 1°$, $\Delta\varphi_i = 18°$, и $\Delta\varphi_i = 90°$ от длины последовательностей L

В соответствии с полученными результатами найдено абсолютное значение прироста структурной скрытности ΔS АМФОКП (для случаев изменения фазового сдвига между элементами кодовых последовательностей на углы $\Delta\varphi_i = 1°$, $\Delta\varphi_i = 18°$) по сравнению со структурной скрытностью АДОМУС $S_{\text{АДОМУС}}$.

Расчет абсолютного значения прироста структурной скрытности выполнен по следующей формуле

$$\Delta S = S_{\text{АМФОКП}} - S_{\text{АДОМУС}}. \quad (6)$$

Расчет абсолютного значения прироста структурной скрытности АМФОКП σ_S, выраженной в процентах, (для случаев изменения фазового сдвига между элементами кодовых последовательностей на углы $\Delta\varphi_i = 1°$, $\Delta\varphi_i = 18°$) по сравнению со структурной скрытностью АДОМУС $S_{\text{АДОМУС}}$ произведен по формуле

$$\sigma_S = \frac{\Delta S}{S_{\text{АДОМУС}}} \cdot 100\%, \quad (7)$$

где $\Delta S -$ абсолютное значение прироста структурной скрытности АМФОКП по сравнению со структурной скрытностью АДОМУС, $S_{\text{АДОМУС}} -$ структурная скрытность АДОМУС.

В таблице 3 представлены результаты расчетов прироста структурной скрытности АМФОКП к структурной скрытности АДОМУС σ_S, выраженной в процентах, для матриц порядков $N = 128, 256$ фазового сдвига между элементами кодовых последовательностей на углы $\Delta\varphi_i = 1°, \Delta\varphi_i = 18°$.

Таблица 3 – Значения прироста структурной скрытности АМФОКП к структурной скрытности АДОМУС σ_S при изменении фазового сдвига между элементами кодовых последовательностей на углы $\Delta\varphi_i = 1°, \Delta\varphi_i = 18°$

Порядок матрицы, N	σ_S при $\Delta\varphi_i = 1°$, %	σ_S при $\Delta\varphi_i = 18°$, %
128	101,31	2,5
256	101,02	2,32

В работе предложены аналитические выражения для расчета структурной скрытности АМФОКП, формируемых на основе СВ бидиагональных ЭМ, при различных значениях фазового сдвига между элементами кодовых последовательностей. Полученные АМФОКП на основе разработанных модели и алгоритма их синтеза, демонстрируют увеличение уровня структурной скрытности относительно аналогичного параметра АДОМУС, при этом величина прироста находится в интервале от 2,5 до 101,31% для $n = 128$, и в интервале от 2,32 до 101,02% для $n = 256$.

Значение структурной скрытности АМФОКП при изменении фазового сдвига между элементами кодовых последовательностей на угол $\Delta\varphi_i = 90^{\circ}$ также находится выше требуемого значения структурной скрытности $S_{\text{треб.}} \geq 43$ ДИЗ для $N = 128$ и $N = 256$, что позволяет их применять в существующих ССС с КРК.

Выявленные преимущества АМФОКП по показателю структурной скрытности доказывают целесообразность их применения, в современных ССС с КРК для противодействия угрозе подмены сообщений.

В четвертой главе решена третья основная задача исследования – разработаны принцип построения и техническое решение по противодействию угрозе подмены сообщений в ССС с КРК.

Принцип защиты информации от угрозы подмены сообщений в ССС с КРК заключается в том, что каждый информационный символ каждого информационного канала передается при помощи уникальной реализации АМФОКП размерностей $N = 128, 256$ с неповторяющейся структурой, изменяющейся по одинаковому закону на передающей и приемной стороне. Техническое решение предложено в виде стохастического средства защиты информации, включающее генератор псевдослучайных комплексных чисел (ГПСКЧ), генератор псевдослучайных АМФОКП, устройство синхронизации и буферный накопитель, которые имеют техническую возможность сформировать необходимое множество кодовых последовательностей и осуществить их стохастическое использование.

С учетом того, что АМФОКП представляют собой ансамбли ортогональных кодовых последовательностей, которые получаются путем моделирования на основе использования СВ ЭМ в данном разделе предложена структура генератора псевдослучайных АМФОКП, представленная на рисунке 7.

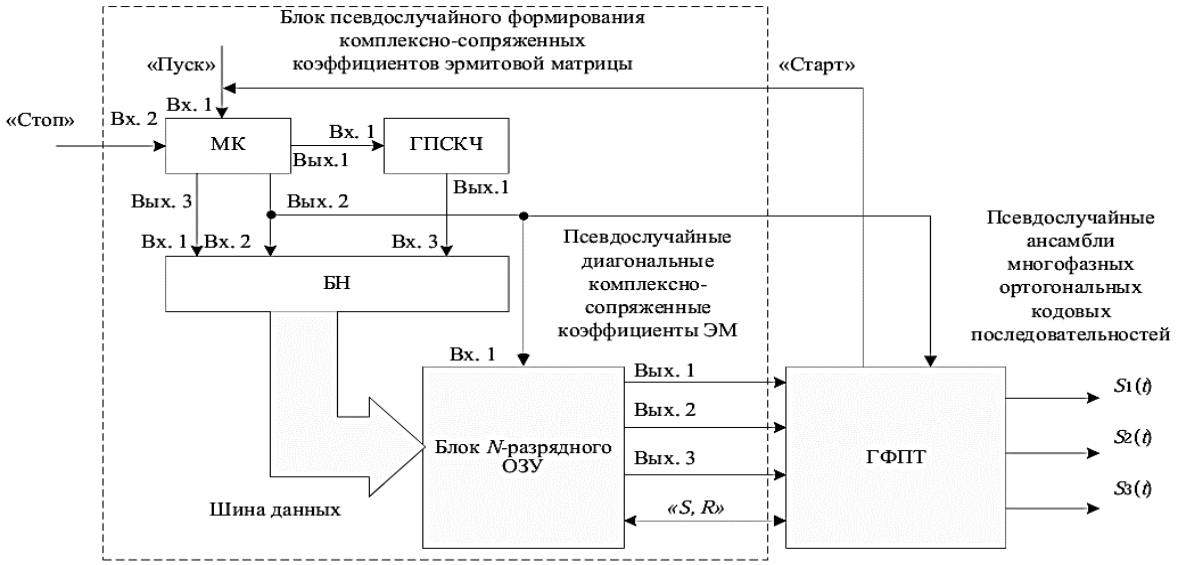

Рисунок 7 – Структура генератора псевдослучайных АМФОКП

В предлагаемом генераторе исходная структура генератора функций Попенко-Турко (ГФПТ) дополнена блоком псевдослучайного формирования комплексно-сопряженных коэффициентов ЭМ, состоящим из микроконтроллера (МК), ГПСКЧ, блока накопителя (БН), блока N – разрядного (N – разрядность генерируемых ГПСКЧ псевдослучайных комплексно-сопряженных коэффициентов ЭМ) оперативного запоминающего устройства (ОЗУ). Временные диаграммы работы генератора АМФОКП представлены в диссертационной работе.

Алгоритм формирования АМФОКП состоит из одиннадцати этапов, подробно описанных в диссертационной работе.

Таким образом, разработанные структура генератора псевдослучайных АМФОКП и алгоритм их формирования позволяют из наборов последовательностей псевдослучайных комплексных чисел, задаваемых ГПСКЧ, получить наборы различных псевдослучайных АМФОКП, вариант которых представлен на рисунке 8.

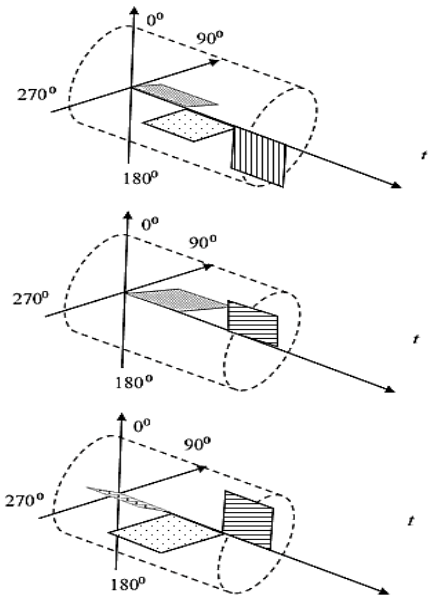

Рисунок 8 – Временные диаграммы АМФОКП на выходе ГПСКЧ

Для обоснования реализуемости разработанных моделей, алгоритмов и технических решений создана программная модель ССС с КРК, содержащая генератор АМФОКП для стохастического средства защиты информации, в среде Matlab SIMULINK.

Модель СПИ с КРК на основе стохастического применения АМФОКП состоит из передающей части, приемной части и канала связи, подробно описанных в диссертации. Временные осциллограммы работы модели ССС с КРК представлены на рисунке 9.

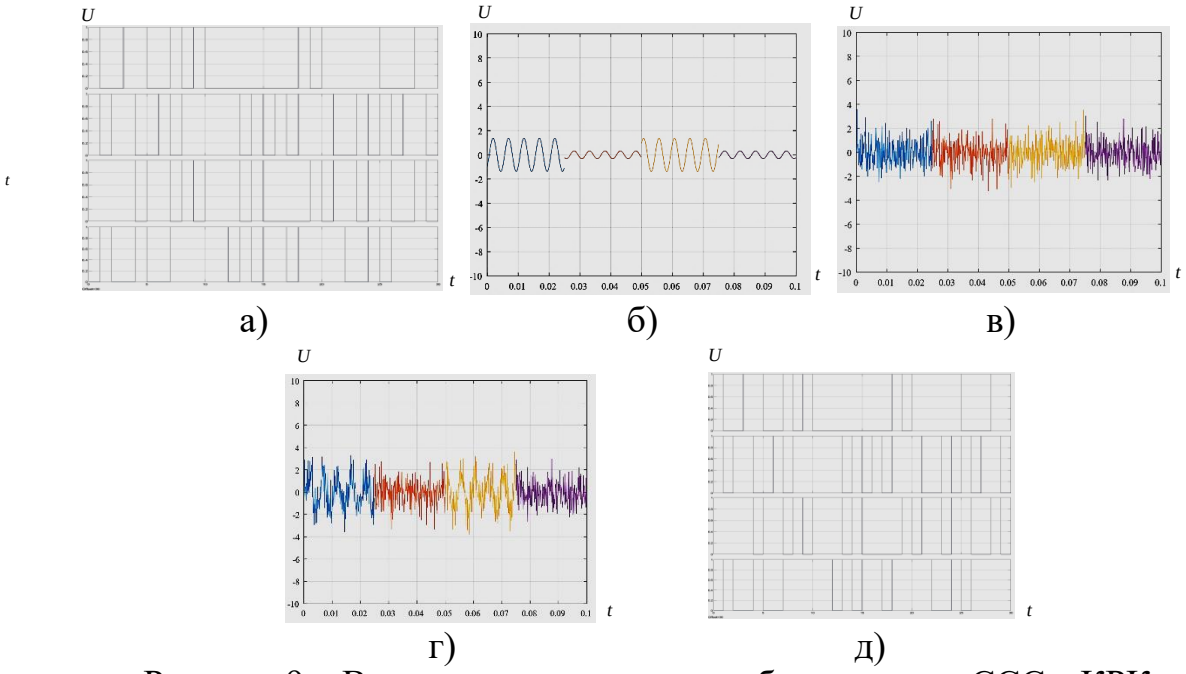

Рисунок 9 – Временные диаграммы работы модели ССС с КРК

На осциллограмме а) показаны информационные последовательности 1-4 перед подачей их на входы блоков модуляторов 1-4 передающей части. На осциллограмме б) показан сигнал на выходе передатчика. На осциллограмме в) показана визуализация помехи типа «Белый шум» в канале связи. На осциллограмме г) показана визуализация сигнала с помехой типа «Белый шум» в канале связи на входе приемного устройства ССС с КРК. На осциллограмме д) показаны информационные последовательности 1-4 на выходе приемника ССС с КРК. Как видно из осциллограмм а) и д) исходные информационные последовательности и принятые последовательности идентичны. Результаты исследования программной модели ССС с КРК доказывают возможность её практической осуществимости, а также корректность алгоритма её работы.

ЗАКЛЮЧЕНИЕ

В заключении систематизированы ключевые научные и прикладные результаты исследования, отражающие вклад диссертационного исследования в развитие рассматриваемой предметной области, обозначены перспективные направления для последующего развития полученных результатов, сформулированы итоговые выводы.

В процессе работы были получены следующие результаты:

1. Разработанная модель противодействия угрозе подмены сообщений в ССС с КРК на основе синхронного генерирования и стохастического применения АМФОКП обеспечивает повышение их структурной скрытности выше требуемого значения $S_{\text{треб.}} \geq 43$ ДИЗ, отличается от известных тем, что при передаче каждого информационного бита используется уникальная неповторяющаяся структура многофазной ортогональной кодовой последовательности синхронно изменяемая на приемной и передающей сторонах.

2. Разработанная модель АМФОКП требуемых размерностей $N = 128, 256$ и алгоритм их синтеза, по сравнению с известной моделью АДОМУС, позволяют увеличить выигрыш в структурной скрытности

АМФОКП. Получаемые АМФОКП имеют прирост структурной скрытности по отношению к структурной скрытности АДОМУС, который лежит в пределах от 2,5 до 101,31% для порядка матрицы $n = 128$, и в пределах от 2,32 до 101,02% для порядка матрицы $n = 256$. Данный выигрыш обеспечивается при условии, что фазовый сдвиг между элементами кодовой последовательности изменяется на угол $\Delta\varphi_i = 18^{\circ}$ и, соответственно $\Delta\varphi_i = 1^{\circ}$. Значение структурной скрытности АМФОКП для фазового сдвига между элементами кодовой последовательности $\Delta\varphi_i = 90^{\circ}$ также находится выше требуемого значения структурной скрытности $S_{\text{треб.}} \geq 43$ ДИЗ для $N = 128, 256$, что позволяет их использовать в существующих ССС с КРК.

3. Полученные принцип построения и техническое решение генератора псевдослучайных АМФОКП для стохастического средства защиты информации ССС с КРК, в отличие от известных, обеспечивают генерацию ансамблей многофазных ортогональных кодовых последовательностей, описываемых комплексными числами.

Решение поставленных задач исследования подтвердило достижение его цели. На основе полученных данных обозначены направления для дальнейшего развития исследований.

СПИСОК ПУБЛИКАЦИЙ ПО ТЕМЕ ДИССЕРТАЦИИ

Статьи в научных изданиях, входящих в Перечень ВАК

1. Жук, А. П. Алгоритм и устройство формирования ансамблей псевдослучайных ортогональных последовательностей для систем передачи информации с кодовым разделением каналов / А. П. Жук, А. В. Студеникин, Е. П. Жук // Системы управления, связи и безопасности. – 2020. – № 3. – С. 1-21. – DOI 10.24411/2410-9916-2020-10301. (К1)

2. Студеникин, А. В. Моделирование дискретных ортогональных кодовых последовательностей для систем передачи информации / А. В. Студеникин, А. П. Жук // Наукоемкие технологии в космических исследованиях Земли. – 2021. – Т. 13, № 1. – С. 36-43. – DOI 10.36724/2409-5419-2021-13-1-36-43. (К2)

3. Жук, А. П. Алгоритм синтеза ансамблей многофазных ортогональных кодовых последовательностей для защищенной системы передачи информации с кодовым разделением каналов / А. П. Жук, А. В. Студеникин, Д. Е. Белов // Телекоммуникации. – 2021. – № 10. – С. 21-30. – DOI 10.31044/1684-2588-2021-0-10-21-30. (К2)

4. Студеникин, А. В. Алгоритм скрытного информационного обмена в системах передачи информации с кодовым разделением каналов на основе хаотического применения ортогональных кодовых последовательностей / А. В. Студеникин // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2021. – № 11. – С. 102-107. – DOI 10.37882/2223-2966.2021.11.31. (К3)

5. Жук, А. П. Оценка структурной скрытности ансамблей многофазных ортогональных кодовых последовательностей / А. П. Жук, А. В. Студеникин, И. В. Макаров, А. А. Беседин // Телекоммуникации. – 2024. – № 3. – С. 13-21. – DOI 10.31044/1684-2588-2024-0-3-13-21. (К2)

Публикации в сборниках трудов конференций

6. Zhuk, A. P. Improved Method of Formation of an Increased Number of Binary Quasi-Orthogonal Code Sequence Systems with the Required Statistical and Correlation Characteristics / A. P. Zhuk, D. V. Orel, I. A. Kalmykov, A. V. Studenikin // Proceedings of the 21st International Workshop on Computer Science and Information Technologies (CSIT 2019). – Atlantis Highlights in Computer Sciences, 2019. – Vol. 3. – P. 209-214. – DOI 10.2991/csit-19.2019.36.

7. Студеникин, А. В. Программная модель синтеза увеличенных объемов систем дискретных ортогональных кодовых последовательностей / А. В. Студеникин, А. П. Жук, Е. С. Тран // Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации : сборник докладов II Всероссийской научной конференции (с приглашением зарубежных ученых), Ставрополь, 30 ноября 2020 года. – Ставрополь: Северо-Кавказский федеральный университет, 2020. – С. 227-232.

8. Жук, А. П. Универсальный формирователь дискретных ортогональных последовательностей / А. П. Жук, А. В. Студеникин, Е. П. Жук // Радиоэлектронные устройства и системы для инфокоммуникационных технологий - РЭУС-2020, Москва, 27–29 мая 2020 года. – Москва: Российское научно-техническое общество радиотехники, электроники и связи им. А.С. Попова, 2020. – С. 46-48.

9. Студеникин, А. В. Математическое моделирование ансамблей дискретных ортогональных последовательностей / А. В. Студеникин, А. П. Жук, Е. П. Жук // Инновационные векторы цифровизации экономики и образования в регионах России : Сборник научных статей по материалам Всероссийской научно-практической конференции, Ставрополь, 10–11 марта 2021 года. – Ставрополь: Издательство "АГРУС", 2021. – С. 714-717.

10. Студеникин, А. В. Экспериментальное моделирование защищенного информационного обмена в системе передачи информации с кодовым разделением каналов / А. В. Студеникин, А. П. Жук // Глобальные тенденции и перспективы цифровизации экономики, образования и науки : сборник материалов Международной научно-практической конференции, Ставрополь, 19–20 мая 2021 года. – Ставрополь: Издательство "АГРУС", 2021. – С. 572-577.

11. Студеникин, А. В. Моделирование системы передачи информации с кодовым разделением каналов на основе хаотического применения ортогональных кодовых последовательностей / А. В. Студеникин // Проблемы передачи информации в инфокоммуникационных системах : Сборник докладов и тезисов XI Всероссийской научно-практической конференции , Волгоград, 28 мая 2021 года / Редколлегия: Е.С. Семенов (пред.) [и др.]. – Волгоград: Волгоградский государственный университет, 2021. – С. 98-101.

12. Студеникин, А. В. Метод защиты информации в системах связи с кодовым разделением каналов на основе хаотического применения ортогональных кодовых последовательностей / А. В. Студеникин // Теория и практика обеспечения информационной безопасности : Сборник научных трудов по материалам всероссийской научно-теоретической конференции, Москва, 03 декабря 2021 года. – Москва: Московский технический университет связи и информатики, 2021. – С. 303-310.

13. Студеникин, А. В. Исследование угроз и методов защиты информации в сетях когнитивного радио / А. В. Студеникин, А. П. Жук // Теория и практика

обеспечения информационной безопасности : Сборник научных трудов по материалам всероссийской научно-теоретической конференции, Москва, 03 декабря 2021 года. – Москва: Московский технический университет связи и информатики, 2021. – С. 298-302.

14. Алгоритм повышения структурной скрытности систем передачи информации с кодовым разделением каналов / А. П. Жук, А. В. Студеникин, А. В. Кузин, Д. А. Лебедев // Радиоэлектронные устройства и системы для инфокоммуникационных технологий ("РЭУС-2022") : Доклады Всероссийской конференции (с международным участием), Москва, 08–10 июня 2022 года. Том Выпуск: LXXVII. – Москва: Российское научно-техническое общество радиотехники, электроники и связи им. А.С. Попова, 2022. – С. 175-180.

Патенты на изобретения

15. Патент № 2780418 C1 Российская Федерация, МПК H04B 7/216. Система передачи информации с применением стохастических ортогональных кодов : № 2021129144 : заявл. 06.10.2021 : опубл. 22.09.2022 / А. П. Жук, Н. Э. Степанян, А. В. Студеникин, О. П. Малофей, А. О. Малофей, В. А. Кучуков ; заявитель Федеральное государственное автономное образовательное учреждение высшего образования "Северо-Кавказский федеральный университет".

16. Патент № 2773107 C1 Российская Федерация, МПК G06F 1/02, G06F 7/58. Устройство формирования стохастических ортогональных кодов : № 2021117997 : заявл. 21.06.2021 : опубл. 30.05.2022 / А. П. Жук, Н. Э. Степанян, А. В. Студеникин, О. П. Малофей, А. О. Малофей, В. А. Кучуков ; заявитель Федеральное государственное автономное образовательное учреждение высшего образования "Северо-Кавказский федеральный университет".

17. Патент № 2801172 C1 Российская Федерация, МПК H04B 7/216, H04J 11/00, H04L 9/26. Система непрерывной передачи информации ансамблями стохастических ортогональных кодов : № 2022132306 : заявл. 09.12.2022 : опубл. 02.08.2023 / А. П. Жук, Н. Э. Степанян, А. В. Студеникин, О. П. Малофей, Д. Е. Белов, Е. С. Тран ; заявитель Федеральное государственное автономное образовательное учреждение высшего образования "Северо-Кавказский федеральный университет".

18. Патент № 2787561 C1 Российская Федерация, МПК G06F 1/02, H04J 13/12. Формирователь ансамблей стохастических ортогональных кодов с отсутствующей временной задержкой : № 2022111972 : заявл. 04.05.2022 : опубл. 10.01.2023 / А. П. Жук, Н. Э. Степанян, А. В. Студеникин, О. П. Малофей, В. А. Кучуков ; заявитель Федеральное государственное автономное образовательное учреждение высшего образования "Северо-Кавказский федеральный университет".

Свидетельства о государственной регистрации программ для ЭВМ

19. Свидетельство о государственной регистрации программы для ЭВМ № 2020665609 Российская Федерация. Программа генерации стохастических ортогональных сигналов "Stochastic orthogonal signal generator (SOSG)" : № 2020664575 : заявл. 20.11.2020 : опубл. 27.11.2020 / С. Ю. Сухоруков, А. П. Жук, Е. С. Тран, Я. В. Шуляк, Е. П. Жук, А. В. Студеникин ; заявитель Федеральное

государственное автономное образовательное учреждение высшего образования «Северо-Кавказский федеральный университет».

20. Свидетельство о государственной регистрации программы для ЭВМ № 2021661193 Российская Федерация. Генератор стохастических ортогональных кодовых последовательностей : № 2021619557 : заявл. 21.06.2021 : опубл. 07.07.2021 / А. П. Жук, Е. С. Тран, А. В. Студеникин, Я. В. Шуляк, А. А. Апурин ; заявитель Федеральное государственное автономное образовательное учреждение высшего образования «Северо-Кавказский федеральный университет».

21. Свидетельство о государственной регистрации программы для ЭВМ № 2023682120 Российская Федерация. Модель системы передачи информации с кодовым разделением каналов на основе псевдослучайного применения ортогональных кодовых последовательностей : № 2023681642 : заявл. 20.10.2023 : опубл. 23.10.2023 / И. В. Макаров, А. П. Жук, А. В. Студеникин ; заявитель Федеральное государственное автономное образовательное учреждение высшего образования «Северо-Кавказский федеральный университет».

Личный вклад автора в работы, выполненные в соавторстве

В [1] предложен алгоритм формирования ансамблей псевдослучайных ортогональных последовательностей для систем передачи информации с кодовым разделением каналов, в [2] проведено исследование характеристик известных ансамблей и нового ансамбля дискретных ортогональных кодовых последовательностей, в [3] предложен алгоритм синтеза АМФОКП, [5] предложено аналитическое выражение для определения количества вариантов возможных значений фаз АМФОКП, в [6] проведен анализ свойств функций преобразования для метода синтеза двоичных квазиортогональных кодовых последовательностей, в [7] выполнен модуль расчета корреляционной энтропии ансамблей стохастических дискретных ортогональных последовательностей, в [8] разработан принцип функционирования универсального формирователя дискретных ортогональных последовательностей, в [9] проведен анализ свойств СВ ЭМ, в [10] выполнена обработка и анализ результатов экспериментального моделирования защищенного информационного обмена, в [12] проведен анализ известных методов защиты информации в беспроводных сетях от известных угроз, в [13] проведен анализ методов защиты информации в сетях когнитивного радио, в [14] предложен алгоритм целенаправленного отбора АМОКП, в [15] разработана структура стохастического преобразователя системы передачи информации, в [16] разработан блок управляемого инвертирования устройства формирования стохастических ортогональных кодов, в [17] предложена структура устройства контроля ансамблей многофазных ортогональных кодовых последовательностей, в [18] предложен блок памяти стохастических ортогональных кодов, в [19] разработана подпрограмма для расчета статистических показателей ансамблей дискретных ортогональных сигналов, в [20] разработан интерфейс программы, написание части кода, в [21] разработан алгоритм функционирования программы, написание части кода.

Студеникин Андрей Владимирович
МЕТОД ПРОТИВОДЕЙСТВИЯ УГРОЗЕ ПОДМЕНЫ СООБЩЕНИЙ ДЛЯ СИСТЕМ СПУТНИКОВОЙ СВЯЗИ С КОДОВЫМ РАЗДЕЛЕНИЕМ КАНАЛОВ НА ОСНОВЕ СТОХАСТИЧЕСКОГО ПРИМЕНЕНИЯ АНСАМБЛЕЙ МНОГОФАЗНЫХ ОРТОГОНАЛЬНЫХ КОДОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ.
Автореф. дис. на соискание учёной степени канд. тех. наук