Экз. № 1

УТВЕРЖДАЮ
Заместитель начальника 4 ЦНИИ
Минобороны России по научной работе
кандидат технических наук

В.В. Шкарбань

«19» января 2026 г.

ОТЗЫВ
на автореферат диссертации Студеникина Андрея Владимировича «Метод противодействия угрозе подмены сообщений для систем спутниковой связи с кодовым разделением каналов на основе стохастического применения ансамблей многофазных ортогональных кодовых последовательностей», представленной на соискание учёной степени кандидата технических наук по специальности 2.3.6 –«Методы и системы защиты информации, информационная безопасность»

Актуальность темы исследования. Перспективные высокоскоростные системы беспроводной связи, такие как 5G/6G, Wi-Fi и др., в своей основе используют технологию многостанционного доступа с кодовым разделением каналов. Анализ работ, посвящённых данному вопросу, 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 и конфиденциальности при передаче информации.

При этом анализ работ в данной области показывает, что среди различных видов множественного доступа в системах спутниковой связи широко распространён доступ с кодовым разделением каналов и прямым расширением спектра (DS-CDMA).

Спутниковые системы связи в силу специфики функционирования с высокой степенью подвержены угрозе подмены сообщений.

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

В исследованиях, направленных на повышение защищённости информации от подмены 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 $S_{треб.}$ 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 автор использует, предложенную Каневским З.М., Литвиненко В.П., Макаровым Г.В., структурную скрытность, которая определяется мощностью A (число 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 $S_{треб.} \geq 43$ ДИЗ, а используемые в них известные АОКП Уолша, Стиффлера и др., которые влияют на этот показатель, не удовлетворяют требованию по их количеству. Также имеет место применение ограниченного числа известных ансамблей ортогональных кодовых последовательностей, используемых в ССС с КРК, в связи с чем устройства их формирования имеют недостаточные возможности по формированию многофазных сигналов, что требует их доработки.

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 $S_{треб.} \geq 43$ ДИЗ, достаточный для противодействия угрозе подмены сообщений.

Для разрешения данного противоречия в работе проанализированы известные методы синтеза АОКП. В результате было установлено, что известные методы синтеза АОКП не позволяют разрешить выявленное ранее противоречие в практике, поскольку количество синтезируемых с их помощью АОКП ограничено.

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

С учётом данных обстоятельств сделан вывод о том, что научная задача по разработке 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**.

Целью исследования является повышение защищённости ССС с КРК по показателю структурной скрытности за счёт стохастического применения ансамблей многофазных ортогональных кодовых последовательностей с изменяющейся структурой.

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 $S_{треб.} \geq 43$ ДИЗ, отличается от известных тем, что при передаче каждого информационного бита используется уникальная неповторяющаяся структура многофазной ортогональной кодовой последовательности синхронно изменяемая на приёмной 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.

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 приёмной 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 ССС с КРК, 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 счёт синтеза, генерации и стохастического применения АМФОКП, описываемых ортогональными базисами пространства комплексных чисел C^n, а также в получении

аналитических зависимостей для расчёта показателя структурной скрытности при применении АМФОКП, представляемых собственными векторами (СВ) ЭМ.

Практическая ценность работы состоит в следующем:

– Разработанные технические решения по повышению защищённости информации, 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 счёт 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 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.

– Структура и алгоритм функционирования генератора псевдослучайных АМФОКП, 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 ЭВМ в пакете Matlab SIMULINK, 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 для ССС с КРК, использующего 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 научно-технических конференциях.

Внедрение результатов исследования проведено в ООО «Инфоком-С» при проведении научно-практических исследований по созданию новых и совершенствованию существующих методов и алгоритмов скрытого информационного обмена в беспроводных системах передачи данных в системе комплексной безопасности распределённых объектов на базе программной платформы «Дарвис» с целью повышения скрытности от деструктивных воздействий на информацию, передаваемую в беспроводных каналах связи; в учебном процессе ФГ АОУ ВО «Северо-Кавказский федеральный университет», а также в ходе выполнения 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.

Вместе с тем по результатам рассмотрения автореферата диссертации, следует отметить следующие **недостатки**:

– в автореферате не указано на основании чего выбрано требуемое значение показателя структурной скрытности сигнала $S_{треб.} \geq 43$ ДИЗ;

– в автореферате не раскрыто назначение и механизм использования функций автокорреляции $R_i(\tau)$ и взаимокорреляции $R_{ij}(\tau)$ при реализации алгоритма синтеза увеличенного количества АМФОКП (рисунок 5), что затрудняет верификацию данного алгоритма;

– в автореферате не раскрыто понятие модулей диагональных коэффициентов эрмитовой матрицы с точки зрения физических параметров радиосигнала.

Отмеченные недостатки не снижают общей положительной оценки, научной и практической значимости диссертационной работы и связаны, первую очередь, с ограниченным объёмом автореферата диссертации.

Тема диссертационной работы и содержание автореферата соответствуют специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность», так как поставленная в работе цель научных исследований направлена на повышение защищённости систем спутниковой связи с кодовым разделением каналов от угрозы подмены сообщений, что значительно повышает безопасность информации, передаваемой по спутниковым каналам связи.

По материалам, изложенным в автореферате, можно судить о том, что диссертация Студеникина А.В. является самостоятельным завершённым научным трудом, в котором решена актуальная научная проблема, имеющая важное прикладное значение по разработке метода противодействия угрозе подмены сообщений для систем спутниковой связи с кодовым разделением каналов на основе синтеза, формирования и стохастического применения ансамблей многофазных ортогональных кодовых последовательностей.

Вывод.

Диссертационная работа Студеникина А.В. отвечает критериям действующего «Положения о присуждении учёных степеней» (Постановление Правительства РФ от 24.09.2013 г. № 842), предъявляемым к кандидатским диссертациям, а её автор, Студеникин Андрей Владимирович, заслуживает присуждения учёной степени кандидата технических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность».

Отзыв обсужден и одобрен на заседании НТС 7 научно-исследовательского управления 4 ЦНИИ Минобороны России 15 января 2026 г., протокол №1/26.

Начальник 7 научно-исследовательского управления
доктор технических наук, доцент Н.И. Шахов

«15» января 2026 г.

Начальник 72 научно-исследовательского отдела
кандидат технических наук С.В. Поликарпов

«15» января 2026 г.

Научный сотрудник 72 научно-исследовательского отдела А.В. Ржавин

«15» января 2026 г.

Сведения о лицах, представивших отзыв:
Шкарбань Владимир Викторович, кандидат технических наук;
Шахов Николай Иванович, доктор технических наук, доцент;
Поликарпов Сергей Викторович, кандидат технических наук;
Ржавин Андрей Викторович.
e-mail организации: 4cnii@mil.ru
Полное название организации: Федеральное государственное бюджетное учреждение «4 Центральный научно-исследовательский институт» Министерства обороны Российской Федерации.
Почтовый адрес: 141090, Московская обл., г. Королёв, мкр. Юбилейный, ул. Тихонравова, 29