ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

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

1. Актуальность темы диссертационного исследования

Системы спутниковой связи играют важнейшую роль в жизни и деятельности современного общества, поскольку обеспечивают связью, в том числе в тех случаях, когда другие телекоммуникационные системы являются недоступными в силу географической удаленности или сложных метеорологических условий, а также по причине малонаселенности.

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 передаваемых в ней сообщений достаточно вероятна, и может быть реализована злоумышленниками с помощью стандартного оборудования при низких материальных затратах.

С учетом того, что большинство коммерческих спутниковых систем спроектированы и используются без защиты данных от угрозы подмены сообщений, то решение задачи повышения защищённости информационного обмена в системах спутниковой связи от угрозы подмены сообщений имеет важное значение.

Поскольку этапу непосредственной реализации угрозы подмены сообщений предшествует этап радиотехнической разведки, то успешность его осуществления будет во многом зависеть от скрытности системы спутниковой связи. Скрытность беспроводных системах передачи информации может быть обеспечена за счет энергетической и структурной

скрытности используемых в них сигналов-переносчиков информации, а также информационной скрытности передаваемого сообщения.

Наибольшую сложность при комплексном решении задачи обеспечения скрытности системы спутниковой связи с кодовым разделением каналов, из всех видов скрытности представляет задача обеспечения структурной скрытности используемых в системе передачи информации сигналов-переносчиков информации. Это связано с тем, что они должны обеспечивать условие ортогональности, а также должны удовлетворять предъявлять требованиям, предъявляемым к их спектральным и корреляционным характеристикам. С учетом того, что количество известных ортогональных кодовых последовательностей требуемой размерности, удовлетворяющих данным требованиям, невелико, то они обладают низкой структурной скрытностью. Известные алгоритмы и методы получения ортогональных и квазиортогональных кодовых последовательностей имеют ограничения по количеству синтезируемых ансамблей ортогональных кодовых последовательностей, а устройства их формирования имеют ограничения, связанные прежде всего с тем, что позволяют генерировать в основном двоичные последовательности.

С учетом изложенного отмечаю, что научная задача разработки метода противодействия угрозе подмены сообщений для систем спутниковой связи с кодовым разделением каналов на основе синтеза, формирования и стохастического применения увеличенного количества ансамблей многофазных ортогональных кодовых последовательностей является **актуальной.**

2. Оценка достоверности полученных результатов и новизны диссертационного исследования

Достоверность результатов и обоснованность научных положений и основных выводов диссертационной работы подтверждается методологической строгостью применения математического аппарата. Эффективность разработанных методов и алгоритмов подтверждена экспериментально путём компьютерного моделирования. 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. Новизна генератора ансамблей многофазных ортогональных кодовых последовательностей (АМФОКП) и системы спутниковой связи с кодовым разделением каналов (ССС с КРК) со стохастическим средством защиты информации, подтверждается имеющимися у автора диссертационной работы патентами на изобретения.

Научная новизна диссертационной работы заключается в следующем:

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 заключается в развитии стохастических методов защиты информации в ССС с КРК на основе повышения структурной скрытности сигналов 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 для случая стохастического применения АМФОКП, представляемых собственными векторами эрмитовых матриц.

Практическая ценность работы:

- 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 сообщений, передаваемых в ССС с КРК, на основе формирования и стохастического применения АМФОКП. В случае использования разработанного алгоритма противодействия угрозе подмены сообщений за счет стохастического применения неповторяющихся АМФОКП происходит преобразование исходной информации и её передача в канал связи с помощью 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 ансамблей дискретных ортогональных многоуровневых сигналов (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 собственных векторов (СВ) эрмитовых матриц (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.

3. Оценка содержания диссертации, степени ее завершенности, подтверждение публикаций автора

Содержание и структура диссертации Студеникина А.В. соответствует теме, целям и задачам исследования. В диссертации текст, рисунки и таблицы оформлены в соответствии с ГОСТ.

Во введении обосновывается актуальность темы, формулируются цель исследования, научная задача исследования, определяются объект и предмет исследования, практическая ценность и научная новизна результатов, излагаются научные положения, выдвигаемые на защиту.

В первой главе содержится анализ существующих подходов к повышению защищенности существующих ССС с КРК, обоснована целесообразность противодействия угрозе подмены сообщений в них за счет

увеличения структурной скрытности используемых ансамблей ортогональных кодовых последовательностей (АОКП). 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.

С учетом выявленных противоречий в практике и теории сформулирована научная задача исследования и основные задачи исследования, дана характеристика положений, выдвигаемых на защиту.

Во второй главе автор диссертационной работы аргументированно обосновал, возможность снижения вероятности разведки структуры сигнала $P_{\text{разв.}}$ за счет снижения вероятности раскрытия структуры сигнала при условии его обнаружения $P_{\text{стр.}}$, что позволило ему предложить эффективный механизм противодействия угрозе подмены сообщений в ССС с КРК.

В результате автором предложена усовершенствованная модель противодействия угрозе подмены сообщений в ССС с КРК на основе синхронного генерирования и стохастического применения АМФОКП размерностей $N = 128, 256$, позволяющая повысить показатель их структурной скрытности.

Разработанная модель противодействия угрозе подмены сообщений в процессе сеанса связи при передаче каждого информационного бита в ССС с КРК предполагает использование уникальной неповторяющейся структуры ортогональных кодовых последовательностей.

Автором 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 $A_{\text{треб.}} \geq 4{,}54 \cdot 10^{12}$.

Считаю, что положение 1, заключающееся в том, что «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» автором доказано.

В третьей главе автором 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 в ССС с КРК, при их стохастическом применении.

Модель АМФОКП основана на использовании множества наборов собственных векторов эрмитовых матриц, которые в каждом конкретном случае вычисляются в соответствии с набором значений модулей и аргументов диагональных коэффициентов ЭМ. Используя различные наборы исходных данных, присваиваемых диагональным коэффициентам ЭМ в соответствии с разработанным алгоритмом синтеза, определяются различные по своей структуре АМФОКП в количестве, превышающем требуемое значение $A_{\text{треб.}} \geq 4{,}54 \cdot 10^{12}$ для размерностей $N = 128, 256$.

Автором 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.

Для оценки структурной скрытности АМФОКП, применяемых в ССС с КРК, автором проведен расчет их количества, которое может быть получено на основе разработанной модели и алгоритма синтеза.

В соответствии с полученными результатами автором найдено абсолютное значение прироста структурной скрытности ΔS АМФОКП (для

случаев изменения фаз элементов кодовых последовательностей на углы $\Delta\varphi_i = 1°, \Delta\varphi_i = 18°$).

Считаю, что положение 2, заключающееся в том, что «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 эрмитовой матрицы $n = 128$, 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» автором доказано.

В четвертой главе автором диссертационной работы 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, генератор псевдослучайных АМФОКП, устройство синхронизации и буферный накопитель, которые имеют техническую возможность сформировать необходимое количество кодовых последовательностей для последующего стохастического применения. В разделе предложена структура генератора псевдослучайных АМФОКП.

Автором разработан и подробно описан алгоритм формирования АМФОКП. Данный алгоритм позволяет из наборов последовательностей, формируемых генератором псевдослучайных комплексных чисел, получить наборы различных псевдослучайных АМФОКП.

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

Считаю, что положение 3, заключающееся в том, что «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» автором доказано.

В заключении формулируются выводы, основные результаты работы и рекомендации.

В приложениях приводятся программы синтеза ансамблей многофазных ортогональных кодовых последовательностей на основе собственных векторов эрмитовых матриц, результаты эксперимента по решению задач синтеза ансамблей многофазных ортогональных кодовых последовательностей размерности $N = 4$, акты о внедрении диссертационной работы.

Достоинствами диссертационной работы являются:

1. Диссертация представляет собой законченную, логически выстроенную и выполненную на хорошем уровне научно-квалификационную работу.

2. Модель противодействия угрозе подмены сообщений в ССС с КРК на основе стохастического применения АМФОКП, модель АМФОКП и алгоритм синтеза их увеличенного количества для ССС с КРК получены автором лично.

3. Автореферат в полной мере отражает основное содержание диссертации.

4. Основные результаты диссертации подтверждены научными публикациями необходимого уровня, в том числе патентами на изобретения и свидетельствами о регистрации программ для ЭВМ.

Основные положения диссертации опубликованы в 14 научных печатных работах в том числе: 5 – в ведущих рецензируемых научных журналах, входящих в перечень ВАК РФ (из них 1 категории К1, 3 категории К2, 1 категории К3), 9 – в материалах конференций и других изданиях. Получено 4 патента на изобретение, 3 свидетельства о государственной регистрации программ для ЭВМ. Результаты работы прошли апробацию на научных конференциях различного уровня.

4. Соответствие специальности

Выполненное соискателем научное исследование соответствует паспорту специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность» по пунктам 9. «Модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем, позволяющие получать оценки показателей информационной безопасности» и 15. «Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности».

5. Замечания по диссертационной работе

1. Для проверки случайности чисел используется до 15 параметров и до 200 тестов. В диссертационной работе не проведена проверка случайности для комплексных чисел.

2. В диссертационном исследовании автором приведены расчеты показателя структурной скрытности для фазового сдвига равного $\Delta\varphi = 1°$.

Возникает вопрос в практической реализуемости такой системы спутниковой связи с кодовым разделением каналов.

3. Из текста диссертации не совсем понятен вид последовательностей вырабатываемых генератор ансамблей многофазных ортогональных последовательностей, структура которого представлена на рисунке 4.2.

4. В алгоритме формирования АМФОКП, представленном на рисунке 4.3, не учтена процедура вывода полученного ансамбля ортогональных кодовых последовательностей.

5. Разработанная программная модель ССС с КРК, содержащая генератор АМФОКП для стохастического средства защиты информации, позволяет провести исследование характеристик рассматриваемой системы только для одного вида помех, и не учитывает все существующие в канале спутниковой связи их виды, а также эффекты, возникающие при использовании спутников-ретрансляторов.

6. Имеются стилистические ошибки и описки в диссертации, а также достаточно субъективное и вольное толкование отдельных известных общеизвестных терминов и математических символов.

Отмеченные недостатки в целом не влияют на общую положительную оценку главных научных и практических результатов диссертационного исследования.

9. Заключение о соответствии диссертации критериям

Диссертационная работа Студеникина А.В. представляет собой законченную научно-квалификационную работу, посвящённую решению актуальной задачи, имеющей важное значение в области совершенствования методов и систем защиты информации применительно к системам спутниковой связи. Диссертация обладает научной новизной, имеет теоретическую значимость и практическую ценность. Полученные результаты в полной мере отражены в авторских публикациях. Автореферат полностью отражает содержание диссертации.

Диссертация отвечает требованиям, установленным «Положением о присуждении ученых степеней в федеральном государственном автономном образовательном учреждении высшего образования «Южный федеральный университет» (в действующей редакции) и предъявляемым к диссертациям на соискание учёной степени кандидата наук, а автор, Студеникин Андрей Владимирович заслуживает присвоения ему ученой степени кандидата технических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность», технические науки.

Официальный оппонент
Доктор технических наук (05.13.10 – «Управление в социальных и экономических системах»), доцент, заведующий кафедрой информационных технологий и систем безопасности, Федеральное государственное бюджетное образовательное учреждение высшего образования «Российский государственный гидрометеорологический университет», г. Санкт-Петербург,
Лепешкин Олег Михайлович

192007, г. Санкт-Петербург, ул. Воронежская, д. 79
Тел. служ.: +7(812) 372-50-92, e-mail: rshu@rshu.ru

«25» декабря 2025 г. О.М. Лепешкин

Подпись О.М. Лепешкина заверяю:
Нач. управления кадров Л.В.