ОТЗЫВ

официального оппонента на диссертацию 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», представленную на соискание ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность, технические науки

Актуальность избранной темы

Доступность разделяемого телекоммуникационными системами ресурса является важным фактором, определяющим необходимые способности нарушителя информационной безопасности для реализации им угрозы. Системы спутниковой связи (ССС) являются традиционным объектом атаки со стороны нарушителей, характеризующихся различающимися мотивами, потенциалами и целями, что объясняется использованием ССС как системами двойного назначения, редкими обновлениями аппаратуры ССС, а также повышением рыночной доступности радиоизмерительной аппаратуры и вычислительных ресурсов.

Обеспечение безопасности информации, передаваемой по радиолиниям телекоммуникационных систем, без применения криптографических средств защиты информации является в настоящее время предметом многих исследований. Несмотря на это терминологический аппарат в области некриптографических средств для радиосистем является существенно менее зрелым, чем для ставших традиционными для многих приложений криптографических средств защиты информации.

Одним из наиболее популярных направлений исследований по развитию подходов и средств защиты информации среди «некриптографических» стало повышение скрытности функционирования телекоммуникационной системы.

Выявленное автором противоречие в практике, заключающееся в невозможности обеспечения требуемого уровня структурной скрытности ортогональных кодовых последовательностей, используемых в современных ССС с кодовым разделением каналов, обусловило соответствующие исследования. В результате автором выявлено и противоречие в теории, обусловившее исследования по его разрешению путем разработки метода противодействия угрозе подмены сообщений для ССС с кодовым разделением каналов на основе синтеза, формирования и стохастического применения ансамблей многофазных ортогональных кодовых последовательностей (АМФОКП).

Целью диссертационной работы Студеникина А.В. 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. В связи с этим диссертация, выполненная на тему «Метод противодействия угрозе подмены сообщений для систем спутниковой связи с кодовым разделением каналов на основе стохастического применения ансамблей многофазных ортогональных кодовых последовательностей», является **актуальной** и представляет значительный теоретический и практический интерес.

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертации

Научные результаты, положения, выводы и рекомендации, изложенные в диссертации, обоснованы в ходе, как теоретических исследований, так и при проведении вычислительных экспериментов и создании алгоритмов обработки информации. Это подтверждается их апробацией на четырёх международных и одиннадцати всероссийских научных конференциях, которые достаточно полно излагают ключевые результаты исследования, а также внедрением результатов

работы в образовательную и научно-практическую деятельность, что подтверждается актами реализации.

Научная новизна результатов, научных положений выводов и рекомендаций и их значимость

В диссертации получен ряд новых научных результатов, к основным из которых можно отнести следующие:

1. Модель противодействия угрозе подмены сообщений в ССС с кодовым разделением каналов на основе синхронного генерирования и стохастического применения АМФОКП, отличающийся 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 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 комплексных чисел.

3. Принцип построения и техническое решение генератора псевдослучайных АМФОКП для стохастического средства защиты информации ССС 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.

Новизна результатов, положений, выводов и рекомендаций, сформулированных в диссертации, подтверждается: отсутствием в доступной литературе работ с аналогичными научными и техническими решениями; положительными отзывами специалистов на опубликованные статьи, доклады, представленные на конференциях; наличием патентов и свидетельств о государственной регистрации программ для ЭВМ.

Теоретическая и практическая ценность результатов исследования

Теоретическая ценность исследования, считаю, что заключается в развитии методологии исследований подходов и методов некриптографической защиты информации в радиолиниях телекоммуникационных систем, теории сигналов за счет разработки научно-методического аппарата синтеза АМФОКП требуемых размерностей, получения аналитических зависимостей для расчета показателя структурной скрытности радиосигналов.

Практическая ценность работы заключается в разработке структуры генератора псевдослучайных АМФОКП и его алгоритма функционирования, способного формировать АМФОКП с изменяющейся структурой на основе собственных векторов эрмитовых матриц в соответствии с набором псевдослучайных комплексных чисел.

Достоверность научных результатов, научных положений, выводов и рекомендаций, сформулированных в диссертации

Достоверность полученных в диссертационной работе результатов подтверждается корректным использованием и непротиворечивостью фундаментальным положениям теории моделирования, теории информации, непротиворечивостью полученных результатов с общепринятыми подходами к анализу и синтезу сигналов, подтверждением теоретических выводов и положений полученными результатами имитационного моделирования.

Оценка содержания диссертации и автореферата

Диссертационная работа выполнена автором с достаточно полным анализом известных подходов к построению и анализу некриптографических средств защиты информации, используемых для решения задач данного класса, корректной постановкой и декомпозицией задач, их обоснованным и последовательным решением.

Полученные научные результаты соответствуют следующим пунктам паспорта научной специальности:

п. 9. «Модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем, позволяющие получать оценки показателей информационной безопасности»;

п. 15. «Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности».

Замечания по диссертации и автореферату

1. Во введении диссертации утверждается, что «Технология OFDM по своей сути более устойчива к вредным явлениям межсимвольной интерференции и многолучевого замирания», однако при моделировании рассматривается только модель АБГШ, и обоснование такого выбора не приведено.
2. Во введении диссертации имеют место терминологические неточности «обеспечить защиту информации», «решения задачи безопасности информации», «проблему защиты от несанкционированного доступа к информационному тракту», «расшифровки структуры сигнала».
3. В автореферате отсутствует формальное описание угрозы, не определены возможности нарушителя, что затрудняет сопоставление цели и результата исследования.
4. Во введении диссертации упоминаются гипотезы, однако в тексте отсутствует их явное представление.
5. В разделе **1.2** диссертации **Анализ угроз информационной безопасности систем спутниковой связи** опирается на недостаточное количество источников.
6. В диссертации показана связь «скрытности» с «защищенностью от подмены», однако, считаю, что недостаточно убедительно, например, не учтены известные методы аутентификации и проверки подлинности сообщений.

7. Описанная в разделе 2.2 диссертации «Модель угрозы подмены» нуждается в пояснениях.

8. В диссертации в выражении (2.2), описывающем вероятность разведки структуры сигнала, фигурирует вероятность раскрытия смысла передаваемой информации, что требует пояснения.

9. В диссертации не приведены оценки сложности разработанных автором алгоритмов, что затрудняет оценивание значимости результатов.

10. В диссертации на странице 174 фигурирует отношение «Pс/Pш = 0 дБ». Считаю необходимым пояснение о полосе частот, в которой осуществлялось измерение мощностей, а также причины использования такого соотношения, а не «энергия бита/спектральная плотность мощности шума.

Указанные замечания не являются критическими и не снижают значимости результатов исследований, представленных в диссертации.

Заключение о соответствии диссертации критериям, установленным Положением о присуждении ученых степеней в ЮФУ для кандидатских диссертаций

В соответствии с п. 2.1 диссертация «Метод противодействия угрозе подмены сообщений для систем спутниковой связи с кодовым разделением каналов на основе стохастического применения ансамблей многофазных ортогональных кодовых последовательностей» является научно-квалификационной работой, в которой на основании выполненных автором исследований изложены новые научно обоснованные технические решения и разработки, направленные на повышение защищённости информации в системах спутниковой связи.

В соответствии с п. 2.2 диссертация подготовлена в виде рукописи, написана автором самостоятельно, структурирована и обладает внутренним единством. Работа содержит научные результаты и положения, выдвигаемые для публичной защиты, и свидетельствует о личном вкладе автора диссертации в науку.

Анализ опубликованных работ показал, что все научные результаты принадлежат диссертанту.

В работе имеются сведения о внедрении результатов диссертационного исследования в научно-практических исследованиях ООО «Инфоком-С» при создании новых и совершенствовании существующих методов и алгоритмов скрытного информационного обмена в беспроводных системах передачи данных в системе комплексной безопасности распределенных объектов, а также в учебный процесс ФГАОУ ВО «Северо-Кавказский федеральный университет».

В соответствии с п. 2.3, 2.4 основные научные результаты диссертации достаточно полно отражены в 14 научных работах, в том числе 5 статьях в изданиях, рекомендованных ВАК, в 9 статьях в материалах конференций, а также в 4 патентах на изобретение и 3 свидетельствах о государственной регистрации программ для ЭВМ.

В соответствии с п. 2.10 диссертация содержит ссылки на источники использованных материалов и на работы других авторов.

Диссертация соответствует специальности 2.3.6. Методы и системы защиты информации, информационная безопасность, технические науки.

Содержание автореферата отражает основные положения диссертации.

ВЫВОД. Диссертация 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» является самостоятельно выполненной и законченной научно-квалификационной работой, имеющей научную и практическую ценность. Работа соответствует требованиям п. 2.1-2.4, 2.9, 2.10 «Положения о присуждении ученых степеней в ЮФУ», предъявляемым к кандидатским диссертациям, а ее автор, Студеникин Андрей Владимирович, заслуживает присуждения ему ученой степени кандидата

технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность, технические науки.

Официальный оппонент
Начальник 31 кафедры (защиты информации
от несанкционированного доступа)
Краснодарского высшего военного училища
кандидат технических наук, доцент В.А. Головской

Головской Василий Андреевич, кандидат технических наук, доцент.
Кандидатская диссертация защищена по специальности 20.02.25 Военная электроника, аппаратура комплексов военного назначения.
Наименование организации: Федеральное государственное казенное военное образовательное учреждение высшего образования «Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С.М. Штеменко» Министерства обороны Российской Федерации.
Должность: начальник 31 кафедры (защиты информации от несанкционированного доступа).
Почтовый адрес (рабочий): Российская Федерация, 350063, г. Краснодар, ул. Красина, 4.
Телефон рабочий: +7 (861) 258-10-30, e-mail: kvvu@mil.ru, веб-сайт: https://kvvu.mil.ru/

Подпись Головского Василия Андреевича «ЗАВЕРЯЮ».
Врио помощника начальника училища по СВ и БЗС – начальника строевого отдела М.Мирный