

ОТЗЫВ **на автореферат диссертации**

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

Актуальность диссертационного исследования обусловлена тем, что она посвящена защите современных систем спутниковой связи (ССС) с кодовым разделением каналов (КРК) от угрозы подмены сообщений. Угроза подмены сообщений обусловлена свойствами известных ортогональных кодовых последовательностей, применяемыми в них.

Например, в спутниковой компоненте Международной подвижной электросвязи ИМТ-2000 используются коды Уолша-Адамара длиной 128 и 256 битов. Регулярная структура применяемого кода не может обеспечить безопасность передаваемой информации на протяжении длительного времени, поскольку вероятность подмены сообщения при использовании известных ортогональных кодовых последовательностей значительно возрастает. При применении шифрования для защиты сообщений возрастают временные задержки, обусловленные выполнением криптографических преобразований.

Ключевой проблемой в данном случае является задача защиты информации от угрозы подмены сообщений, поскольку известные ортогональные кодовые последовательности не позволяют обеспечить их требуемую структурную скрытность при применении в СССР с КРК. Поскольку данная задача в настоящее время решена не полностью, то диссертационное исследование актуально, поскольку в нем разработан метод противодействия угрозе подмены сообщений в СССР с КРК, который позволяет на основе синтеза, формирования и стохастического применения увеличенного количества ансамблей многофазных ортогональных кодовых последовательностей (АМФОКП) решить данную задачу.

Научная новизна диссертационного исследования заключается в следующем:

1. Разработанная модель противодействия угрозе подмены сообщений в СССР 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 (СВ) эрмитовых матриц (ЭМ) в соответствии с задаваемым набором псевдослучайных комплексных чисел.

Теоретическая значимость полученных результатов 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 СВ ЭМ.

Практическая ценность полученных результатов состоит в том, что 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. 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.

Замечания и рекомендации:

1. На стр. 16 автореферата отмечено, что в диссертации разработана программная модель системы спутниковой связи с кодовым разделением каналов на основе стохастического применения ансамблей многофазных ортогональных кодовых последовательностей, однако сама модель в автореферате не представлена, что затрудняет понимание её новизны и практической значимости.

2. Из материалов автореферата не ясно каким образом для обоснования противоречия в практике определен требуемый уровень структурной скрытности $S_{\text{треб.}} \geq 43$ ДИЗ, достаточный для противодействия угрозе подмены сообщений в рассматриваемой системе связи.

Выводы:

Несмотря на указанные замечания диссертационное исследование соответствует необходимому научно-техническому уровню и отвечает критериям специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность».

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» удовлетворяет требованиям, установленным «Положением о присуждении учёных 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.

Кандидат технических наук, доцент, доцент департамента информатики, управления и технологий института цифрового образования Государственного автономного образовательного учреждения высшего образования города Москвы «Московский городской педагогический университет»

Сахнюк П.А. 

13.01.2026

Сахнюк Павел Анатольевич, кандидат технических наук, доцент, доцент департамента информатики, управления и технологий института цифрового образования Государственного автономного образовательного учреждения высшего образования города Москвы «Московский городской педагогический университет», научная специальность: 20.02.25 «Военная электроника, системы и средства опознавания, аппаратура комплексов военного назначения»

Подпись Павла Анатольевича Сахнюка заверяю

специальном  

Адрес: 129594, Москва, ул. Шереметьевская, 28

Сайт: <https://www.mgpu.ru/obrazovanie/institutes/ide/>

Телефон: 8(495) 618 61 52

E-mail: ide@mgpu.ru