Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК_____

Литвинов
Валентин Сергеевич

# Обеспечение структурной скрытности радиосигналов на основе стохастических кодовых структур

## АВТОРЕФЕРАТ

на соискание степени магистра технических наук
по специальности 1-39 80 02 «Радиотехника, в том числе системы и устройства радионавигации, радиолокации и телевидения»

_____

Научный руководитель
Карпушкин Эдуард Михайлович
Кандидат технических наук

_____

Минск 2019

# ВВЕДЕНИЕ

В настоящее время кодовые структуры на основе низкоскоростных кодов, обладающие приемлемыми корреляционными свойствами, достаточно глубоко изучены и нашли широкое применение в области радиотехнических систем – например, М-последовательности, коды Голда, коды Касами, ансамбли Уолша и т.д.

Однако указанные кодовые структуры не обладают достаточным уровнем мощности ансамблей для того, чтобы обеспечить криптографический уровень сложности структурной скрытности формируемых радиосигналов, более того, их длина не произвольна, а мощность зависит от длины. Стохастические кодовые структуры на основе классов вычетов позволяют формировать ансамбли с приемлемыми корреляционными свойствами, криптографическим уровнем сложности формируемых ансамблей, зависимых от ключа, и произвольной длиной последовательностей, не влияющей на мощность кодовой структуры, а лишь определяющей её верхнюю границу.

Одним из направлений в области разработки защищённых радиотехнических систем передачи информации является обеспечение структурной скрытности на основе кодовых структур псевдослучайных последовательностей. Данное направление актуально как для систем с одним передатчиком и приёмником, так и для радиосетей с кодовым разделением каналов, и позволяет повысить уровень защищённости передаваемых данных.

## ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

**Целью данной работы** является разработка метода формирования стохастических кодовых структур на основе арифметики в классах вычетов для обеспечения структурной скрытности радиосигналов.

Для достижения целей в работе должны быть решены **задачи** анализа корреляционных свойств и криптографической стойкости стохастических кодовых структур на основе арифметики в классах вычетов.

**Объектом исследования** данной работы являются стохастические кодовые структуры на основе арифметики классов вычетов в простых полях.

Результаты работы по формирования кодовых структур, обеспечивающих структурную скрытность радиосигналов, были опубликованы в сборнике «Системы и средства связи, аппаратура передачи данных, системные и программно-технические решения в сфере навигации» 35-й научно-технической конференции ОАО «Агат-системы управления» в 2018 г. Также результаты разработки алгоритма синтеза псевдослучайной последовательности на основе системы классов вычетов были представлены на конференции БГУИР «55-я юбилейная конференция студентов, магистрантов и аспирантов БГУИР» в 2019 г. Доклад об изделии «Комплекс по обнаружению операторов мультикоптеров» был представлен в штабе ПВО и ВВС в 2019 г.

## КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Для решения поставленных задач и достижения цели диссертационной работы были проведены анализ научной литературы и исследования свойств и характеристик стохастических кодовых структур на основе арифметики в классах вычетов.

В первой главе был проведен анализ существующей научной литературы по теме исследований. Особое внимание было уделено теории чисел, методам формирования псевдослучайных последовательностей и криптографическим алгоритмам.

Во второй главе разрабатывался алгоритм формирования стохастических кодовых структур на основе арифметики в классах вычетов и исследовались их корреляционные свойства в сравнении с псевдослучайными последовательностями Голда.

В третьей главе рассматривались способы криптографического анализа, в частности корреляционного криптоанализа, и критерии криптографической стойкости, а также исследовалась устойчивость стохастических кодовых структур на основе арифметики в классах вычетов корреляционным атакам.

В четвёртой главе были приведены результаты моделирования радиоканала с использованием стохастических кодовых структур на основе арифметики в классах вычетов в среде моделирования *Simulink* и на программно-определяемых модулях.

# ЗАКЛЮЧЕНИЕ

На основании проведённых исследований можно сделать вывод, что стохастические кодовые структуры на основе классов вычетов позволяют формировать ансамбли с приемлемыми корреляционными свойствами, криптографическим уровнем сложности формируемых ансамблей, зависимых от ключа, и произвольной длиной последовательностей, не влияющей на мощность кодовой структуры, а лишь определяющей её верхнюю границу.

Основным недостатком использования стохастических кодовых структур на основе арифметики в классах вычетов является более высокий корреляционный порог последовательностей по сравнению с другими алгоритмами псевдослучайных последовательностей, таких как коды Голда и коды Касами.

Таким образом, в ходе работы были выполнены следующие задачи:

- предложен альтернативный алгоритм формирования стохастических кодовых структур;
- рассмотрен метод оценки криптографической стойкости алгоритма путём выделения статистических свойств корреляционных характеристик последовательностей;
- реализована приёмо-передающая модель с использованием алгоритма на базе программно-определяемого радиомодуля.

**Список опубликованных работ**

I. Бильдюк Д.М., Литвинов В.С. Обеспечение структурной скрытности навигационных данных GPS на основе СКВ-кодов // Системы и средства связи, аппаратура передачи данных, системные и программно-технические решения в сфере навигации, Агат-системы управления, 2018 г. – с.11.

II. Литвинов В.С. Псевдослучайные последовательности на основе системы классов вычетов // 55-я Юбилейная Научная Конференция Аспирантов, Магистрантов и Студентов БГУИР, 2019 г.

III. Наливко П.С., Дворецкий Е.А., Литвинов В.С., Сасковец А.В. Комплекс обнаружения операторов мультикоптеров «Гроза-О» // Конференция штаба ПВО и ВВС, 2019 г.