УДК 004.052.42
Название: Приложение надежного кодирования на основе бент-функций и вейвлет-разложений в системах связи.
Автор: Ряскин Глеб Александрович, Таранов Сергей Владимирович, Мухамеджанов Данияр Давлетович, Университет ИТМО (Федеральное государственное автономное образовательное учреждение высшего образования Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики), Санкт-Петербург, +79110074647.
Научный руководитель: доцент, к.физ-мат.н. Левина Алла Борисовна, Университет ИТМО (Федеральное государственное автономное образовательное учреждение высшего образования Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики), Санкт-Петербург.

Одним из эффективных способов по решению задачи обеспечения высокой достоверности информации при ее передаче является использование теории кодирования и помехоустойчивых кодов. Злоумышленник, осуществляя различные воздействия на аппаратную составляющую кодирующего устройства с целью возникновения искажений информации на некоторых этапах кодирования, управляя и анализируя ошибки, может изменять передаваемую по каналу информацию. Для обеспечения защиты против подобных атак используют надежные коды, которые строятся на нелинейных функциях. В рамках данного исследования в качестве нелинейных функций было предложено использование бент - функций и сплайн-вейвлетное разложение.

Целью работы является разработка схем применения надежных кодов в системах связи на основе вейвлетных разложений и бент-функций для повышения показателей системы защиты от данных атак.

Для достижения цели были поставлены следующие задачи:

- выбор конструкции надежных кодов на основе вейвлетных разложений и бент-функций;
- разработка схемы внедрения выбранной конструкции надежных кодов с точки зрения защиты от атак по сторонним каналам и соответствия требованиям системы связи;
- сравнение характеристик новой схемы по показателям защищенности системы по сравнению с существующими вариантами.

В работе были выбраны несколько конструкций надежных кодов, основанных на бент-функциях и вейвлет разложении с различной степенью мультипликативных элементов, в результате получаем более низкий показатель по максимальной маскировке ошибки, но время, затраченное на кодирование информации, увеличивается. Составлены схемы внедрения в различные системы связи выбранных конструкций. Произведено сравнение с кодами, использующиеся в системах связи, с последующим анализом результатов.

Разработанная схемы надежного сплайн-вейвлетного бент кода при внедрении в системы связи:

- обеспечивает более высокие показатели по защите информации в случае защиты информации от атак по сторонним каналам в сравнении с существующими решениями;
- обладает распределением вероятности обнаружения ошибок близким к равномерному распределению, что позволяет обеспечить защиту от атак по сторонним каналам.
- более высокое время кодирования информации по сравнению с существующими решениями.

Автор	_____	Ряскин Г.А.
Научный руководитель	_____	Левина А.Б.
Декан факультета ФБИТ	_____	Заколдаев Д.А.