# АЛГОРИТМ КОДИРОВАНИЯ ИНФОРМАЦИИ В ЗАШУМЛЕННОМ ШИРОКОВЕЩАТЕЛЬНОМ КАНАЛЕ

А.И. Митюхин, А.В. Цык

Рассматривается алгоритм кодирования информации, позволяющий повысить уровень информационной безопасности системы передачи данных на основе информационного подхода. Представлен анализ оптимальных возможностей помехоустойчивых кодов при их применении в зашумленном широковещательном канале. Такой преднамеренно ухудшенный широковещательный канал описывается заданными переходными характеристиками (шумом). В качестве связной модели использовался двоичный симметричный канал. Сущность алгоритма основывается на применении основного уравнения помехоустойчивого кодирования [1] для формирования информационной неопределенности в канале перехвата. Предлагается в процесс кодирования ввести дополнительный этап преобразования источника информации. Данное преобразование формирует взаимно однозначное соответствие между векторами сообщений и синдромами. В этом случае размер анализа в канале перехвата определяется не разрешенным подпространством кода, а размером полного евклидова пространства, зависимым от длины кода. При этом дополнительное кодирование характеризуется свойством апериодичности, что важно, при решении задач минимизации информации в канале перехвата [2]. Кроме того, из-за воздействия шума, ошибки в принятом сигнале увеличивают неопределенность передаваемого сообщения в канале перехвата. В исследованиях основное уравнение кодирования задавалось в виде произведения порождающего и проверочных полиномов соответствующих степеней с коэффициентами над двоичным полем Галуа. В качестве исходного кода использовался симплексный m-код. Так как этот код дуален коду Хэмминга (относится к классу высокоскоростных), вычислительные затраты на анализ входного процесса в канале перехвата резко возрастают с увеличением длины кода. С использованием программного приложения MATLAB проводилась экспериментальная оценка вычислительных (программных) затрат на декодирование по стратегии максимального правдоподобия [3]. Например, для сравнительно малой длины кода, равной 31, вычислительная сложность анализа сводится к проведению более 2 млрд сравнений двоичных векторов по mod 2 на один входной сигнал (кодовое слово). Такой же вычислительный порядок необходим для выполнения операций сложений при нахождении коэффициентов корреляции, по множеству значений которых выносится решение о входном сигнале. Обеспечение требуемой информационной определенности приема информации в канале перехвата за реальное время передачи кодированного сигнала с высокой тактовой частотой чипов кода становится технически сложно реализуемым.

**Литература**

1. Митюхин А.И. Прикладная теория информации. Минск, БГУИР, 2018. 168 с.

2. Smart N. Cryptografhy: An Introduction. McGraw-Hill, 2003. 436 p.

2. Mac Willams F.J., Sloane N.J.A. The Theory of Error-Correcting Codes. Oxford, 1977. 762 p.