ЗАЩИТА ИНФОРМАЦИИ В ШИРОКОВЕЩАТЕЛЬНОМ КАНАЛЕ НА ОСНОВЕ СМЕЖНЫХ КЛАССОВ РЕШЕТЧАТЫХ КОДОВ С.Б. Саломатин, М.А. Алисеенко, В.В. Панькова

Защита информации в широковещательном канале от перехвата предполагает организацию схемы передачи данных с заданной скоростью и решения задачи восстановления информации из перехваченных сообщений нелегитимным пользователем [1, 2]. При этом предполагается, что перехватчик обладает неограниченными вычислительными способностями.

Схема защиты. Схема использует свойства смежных классов модулярных решетчатых кодов. В процессе кодирования сообщение отображается на смежный класс кода, а в канал передается случайная точка в пределах смежного класса.

Варианты случайного кодирования. Рассматриваются многомерные модулярные решетки обобщенных кодов конечных полей. Модели декодеров соответствуют схемам декодирования по критерию максимального правдоподобия и решению задачи CVP – поиска ближайшего вектора.

Статистический анализ процессов декодирования сигналов без использования случайности и случайного кодирования с использованием смежных классов показывает, что рандомизация алгоритмов передачи снижает эффективность приемника-анализатора в канале перехвата.

Литература

1. Semantically Secure Lattice Codes for the Gaussian Wiretap Channel/ C. Ling [et al.] // IEEE Transactions On Information Theory. – 2014. – Vol. 60, no 10.

2. Zamir R., Nazer B., Kochman Y. Lattice Coding for Signals and Networks: A Structured Coding Approach to Quantization, Modulation abd Multi-user Information Theory. – Cambridge University Press, 2014.