ЗАЩИТА ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ ТАБЛИЦЫ ДЕКОДИРОВАНИЯ

А.И. Митюхин, В.А. Томин

Рассматривается решение задачи зашиты информации на основе кодирования цифровой информации с использованием кодов с расширением спектра. Известно, при расширении спектра сигнала с равномерным распределением энергии, уменьшается его спектральная плотность мощности и тем самым обеспечивается энергетическая скрытность передачи закодированной информации [1]. Наряду с открытым широкополосным кодированием предлагается осуществлять дополнительное кодирование, основанное на алгебраических свойствах и особенностях низкоскоростных кодов. Для этого можно применить алгебраическую операцию разложения группы на смежные классы по подгруппе. В теории кодирования эта операция определяет построение таблицы декодирования кода с расширением спектра. Информации ставится в соответствие номер смежного класса. Далее закодированные данные передаются по двоично-симметричному каналу (ДСК) с шумом. В качестве ключей используются случайно выбираемые шумовые векторы, отражаемые операцией разложения группы на смежные классы подгруппы. Порядок группы определяет значность кода. Для повышения надежности информационной системы предлагается шумовые векторы дополнительно кодировать с помощью апериодической псевдослучайной последовательности, например, М-последовательности. Длительность последовательности соизмерима с временем сеанса связи. Кроме того, структура полиномов над полем Галуа, генерирующая псевдослучайную последовательность, может меняться через заранее выбранный промежуток времени. Уполномоченный пользователь системы использует декодер, работающий по синдромному алгоритму. При этом используется теорема о связи формы синдрома и номера соответствующего смежного класса [2]. В случае обнаружения активной работы системы, несанкционированный доступ к информации усложняется из-за необходимости проведения значительных вычислительных операций на основе поэлементного сравнения входного процесса ДСК с векторами смежных классов. Стойкость рассматриваемого алгоритма зависит от параметров открытого кода (значности, размерности и минимального расстояния), а также количества вариантов разложения исходного открытого кода на смежные классы по параметру, характеризующему избыточность кода. Представлены оценки сложности несанкционированного декодирования с использование энтропийного подхода.

Литература

1. Ипатов В. Широкополосные системы и кодовое разделение сигналов. Принципы и приложения. – Москва: Техносфера, 2007.

2. Митюхин А. И. Прикладная теория информации. – Минск: БГУИР, 2018.