ЗАЩИТА ИНФОРМАЦИИ ПОСРЕДСТВОМ НИЗКОСКОРОСТНОГО И КРИПТОГРАФИЧЕСКОГО КОДИРОВАНИЯ

А.И. Митюхин, В.Л. Николаенко

Как известно, обнаружение и анализ скрытных сигналов в канале с перехватом оказывается затрудненным при использовании низкоскоростного помехоустойчивого кодирования информации. Если в качестве кодовых псевдослучайных последовательностей (ПСП) применять слова с минимально возможным спектральным отличием, достигается высокая степень энергетической скрытности. Обеспечение повышенных показателей скрытности (не только энергетической) требует введения второй ступени защиты — криптокодирования информационного потока. Здесь также желательно использовать кодовые (ключевые) структуры, обладающие равномерным энергетическим спектром. В этом случае, в занимаемом сигналами частотном диапазоне, следует ожидать отсутствия характерных спектральных точек, по которым наиболее вероятно обнаружение и декодирование скрываемого полезного сигнала. На практике целесообразно применять методы скрытности, соответствующие необходимым целям. Компромисс между сложностью, стоимостью и требуемой степенью защиты информации, а также назначение системы и условия ее применения проводят к разным вариантам соотношения низкоскоростного помехоустойчивого и криптокодирования.

В сообщении приводятся результаты экспериментального исследования двухступенчатой системы кодирования информации. В качестве криптоалфавита использовались символы клавиатуры компьютера. Ключевые последовательности длиной n=(8, 16, 32) представляли собой случайные последовательности изображений q-ичных символов. Длины ключевых последовательностей выбиралась значительно меньше длины ПСП. Ключевые последовательности образовывали сравнительно

большое множество слов с заданными корреляционными свойствами. Например, сравнительно легко было получено множество, включающее 128 последовательностей системы 8-символьных ключей с пиковым значением бокового лепестка взаимно-корреляционной функции не превышающим значения 0,33. Спектральные свойства, степень равномерности спектра выбранных ключевых последовательностей оценивались формой их автокорреляционной функции.