$$P(\boldsymbol{Y}|\boldsymbol{X}^s) = P(\boldsymbol{Y} - \boldsymbol{X}^s = \boldsymbol{n}) = P(\boldsymbol{n}),$$

где $\{\boldsymbol{n}\}$ – множество преднамеренных шумовых векторов, $P(\boldsymbol{n})$ – вероятности векторов шума. Выражение $\{\boldsymbol{Y} - \boldsymbol{X}^s\}$ – это множество $\{d_x\}$ расстояний Хемминга между словом $\boldsymbol{Y}$ на входе декодера и всеми словами кода. С позиции теории кодирования d_x показывает, сколько символов в слове надо исказить, чтобы перевести одно разрешенное для передачи кодовое слово в другое разрешенное. Тогда вычисление функции max $P(\boldsymbol{Y}|\boldsymbol{X}^s)$ сводится к нахождению опорного кодового вектора $\boldsymbol{X}^s$ ближайшего по расстоянию Хемминга к принятому вектору $\boldsymbol{Y}$ (на выходе канала). Если использовать пространственную интерпретацию кода как множество точек (векторов) *N*-мерной решетки, то вероятность того, что точка $\boldsymbol{X}^s$ совпадет с точкой $\boldsymbol{Y}$, увеличивается с уменьшением евклидова расстояния. Степень близости точек $\boldsymbol{X}^s$ и $\boldsymbol{Y}$ в пространстве размерностью N легко вычисляется с помощью скалярного произведения

$$\langle \boldsymbol{Y}|\boldsymbol{X}^s\rangle = \sum_{i=1}^{N} y(i)\, x^s(i) \qquad (3)$$

векторов, описывающих точки. Эта операция лежит в основе декодирования по основному каналу. Из проведенного анализа следует, что для успешного перехвата информации по каналу подслушивания необходимо иметь априорные знания об основных параметрах кода, в частности, мощности множества $\{\boldsymbol{X}\}$ и переходных вероятностях канала. Задача декодирования еще более усложняется, когда шум используется с целью маскирования информации. Тогда декодирование должно выполняться по вектору наблюдения $\boldsymbol{Y} = \boldsymbol{X} + \boldsymbol{n}$. Отсутствие точной информации об алгебраической структуре кода $\boldsymbol{X}$ и множестве случайных векторов $\{\boldsymbol{n}\}$ в канале с подслушиванием не позволяет перехватчику декодировать сигнал $\boldsymbol{Y}$ по алгоритму (3). Решение задачи перехвата на основе многоканальной обработки по (3) и перебором последовательностей $\boldsymbol{X}$ и $\boldsymbol{n}$ потребует значительных вычислительных, временных и технических ресурсов.

Список использованных источников.

1. Митюхин, А.И. Корреляционные спектры и кодовые расстояния мажоритарных последовательностей/А.И. Митюхин, П.Н. Якубенко// Доклады БГУИР. – 2015. № 4 (90). − С. 5–9.

ЗАЩИТА ИНФОРМАЦИИ НА ОСНОВЕ НИЗКОСКОРОСТНОГО КОДИРОВАНИЯ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Шлома К.Н.

Митюхин А. И. – доцент каф. ФМД

Анализируется один из основных сервисов информационной безопасности – помехоустойчивое кодирование и защита информации от несанкционированного доступа в радиоэлектронных системах. Рассматривается система кодирования информации с использованием множества неприводимых полиномов над полем $GF(2)$ в каналах с гауссовским шумом. Дана оценка возможных временных затрат декодирования при приеме кодированных данных в условиях априорной неопределенности.

Для обеспечения информационной безопасности при передаче данных используются помехоустойчивые коды. Защита информации в специальных радиоэлектронных системах гражданского и военного назначения от воздействия непреднамеренных и преднамеренных помех осуществляется посредством низкоскоростного помехоустойчивого кодирования [1]. Кроме защиты информации от ошибок (коррекции информации) в каналах с шумами, такие коды над конечным полем $GF(q)$ обеспечивают определенную степень безопасности информационных комплексов от случайного и несанкционированного доступа к информации. Решение этой задачи основывается на применении множества изменяющихся во времени $[n, k, d]$-кодов

$$\boldsymbol{C} = \{\boldsymbol{C^1}, \dots, \boldsymbol{C^J}, \dots, \boldsymbol{C^L}\}, \boldsymbol{c^j} \in \boldsymbol{C^J}, c^j = (c_1, \dots, c_i \dots, c_n), c_i \in GF(q),$$

где k – размерность *j*-кода, $n = q^k - 1$ – длина *j*-кода, d – минимальное расстояние *j*-кода (характеризует корректирующую способность кода), $\boldsymbol{c}^j$– кодовая последовательность с символами из поля $GF(q)$, $M = q^k$–1 – количество слов *j*-кода (мощность множества), q – простое число (основание кода). Практическая алгебраическая конструкция псевдошумового низкоскоростного $[n, k, d]$-кода основывается на применении неприводимого над полем $GF(2)$ полинома вида

$$h(x) = 1 + h_1 x + \cdots + h_{m-1} x^{m-1} + h_m x^m,$$

где коэффициенты $h_i \in \{0, 1\}$, $k = m$. Число возможных различных неприводимых над полем $GF(2)$ полиномов $h(x)$ степени m определяется по формуле

$$L = \frac{\varphi(n)}{m},$$

где $\varphi(n)$ – тотиент-функция Эйлера. Напомним, если n – простое число, то $\varphi(n) = n - 1$. Для реальных значений степеней m и длин n, т.е. в диапазоне значений $n = 2^7 - 2^{19}$ было рассчитано число полиномов $h(x)$. Соответствующие значения показаны в таблице

Таблица 1. Число неприводимых полиномов над полем $GF(2)$

m=k	7	8	9	10	11	12	13	14	15	16	17	18	19
L	18	16	48	60	176	144	630	756	1800	2048	7710	7776	27954

Пример оценки мощности кода и кодирования источника $[1023, 10, 512]$-кодом. Степень кодирующего полинома $h(x)$ определяется размерностью кода $k = 10$. Существуют таблицы, с помощью которых можно найти все неприводимые над полем $GF(2)$ полиномы степени $2 \le m \le 61$ [2]. Для $m = 10$ имеется 60 полиномов, каждый из которых образует код с числом кодовых слов $M = 2^{10} = 1024$. Суммарное количество слов с законами кодирования $h(x)^j = 1 + \cdots + h_9 x^9 + h_{10} x^{10}$ равно $M_\Sigma = LM = 60 \cdot 1024 = 61440$. Пусть проектируется система с длительностью тактового интервала $\tau = 1$ мкс $\boldsymbol{c}^j$ – последовательности. Период одного кодового слова $T = n\tau = = (2^{10} - 1)1 \cdot 10^{-6}\ c = 1{,}023$ мс. Время формирования всех M_Σ последовательностей составит $T_\Sigma = M_\Sigma T \cong 61440 \times \times 1{,}023$ мс $\cong 63\ c$, т.е. около одного часа. В реальной практике стратегия любой защищаемой системы основывается на ограничении времени t передачи информации, когда $t \ll T_\Sigma$ и использовании значительного числа равновероятных кодовых последовательностей. Перехватчик, даже имея некоторые априорные знания о методах кодирования, должен затратить большое время, соизмеримое со значением T_Σ, на анализ наблюдаемого процесса с целью обнаружения и последующего декодирования сигнала. Задача перехвата усложняется из-за отсутствия априорных данных о структуре и алгоритме использования порождающих полиномов. По этой причине, для обнаружения и декодирования ничего не остается как использовать алгоритмы затратной многоканальной обработки наблюдаемого сигнала, фактически, случайного процесса. В этом случае, оптимальное декодирование на основе стратегии максимального правдоподобия [1], реализуемое в рассматриваемой системе, для перехватывающей стороны становится не возможным. Обработка кодированной информации становится не эффективной, чрезмерно затратной по оборудованию и временному ресурсу.

Список использованных источников

1. Митюхин, А.И. Корреляционные спектры и кодовые расстояния мажоритарных последовательностей/ А.И. Митюхин, П.Н. Якубенко // Доклады БГУИР. – 2015. № 4 (90). – С. 5–9.

2. Ziemer, R. E. Introduction to Digital Communication/R.E. Ziemer, R.L. Peterson // Prentice-Hall, NJ, 2001.