Если не предъявляются жесткие требования по температурным и временным параметрам, то предпочтение отдают простым схемам ГШ на шумовых диодах. Схема ГШ на диоде 2Г401В представлена на рис. 2, d. Указанный генератор обладает равномерным спектром шумов в полосе частот 100 – 10000 Гц.

Для зашумления экранов линий связи разговорного тракта используется схема подключения ГШ, представленная на рис. 2, b, для зашумления корпуса аппаратуры используется схема подключения ГШ, представленная на рис. 2, e, а для зашумления незадействованных линий связи используется схема подключения ГШ, представленная на рис. 2, c.

IV Выводы

Для эффективной активной защиты каналов телефонной связи в качестве простейших устройств с невысокими метрологическими характеристиками может быть рекомендован аналоговый ГШ на шумовом диоде типа 2Г401В с зашумлением цепей экранов линий связи, корпуса аппаратуры, незадействованных линий связи и сети электропитания.

Литература: ***1.*** *«Справочник по теоретическим основам радиоэлектроники» под ред.Кривицкого Б. Х. в 2-х ч, т.1, т.2. – М.: «Энергия», 1977.* ***2.*** *Тетерич Н. М. «Генераторы шума и измерение шумовых характеристик». – М.: «Энергия», 1968.* ***3.*** *Алексеев А. И. «Теория применения псевдослучайных сигналов». – М.: Наука, 1969*

УДК 621.391:519.2

НЕЛИНЕЙНОЕ СЛУЧАЙНОЕ КОДИРОВАНИЕ В СИСТЕМАХ ПЕРЕДАЧИ ИНФОРМАЦИИ ПО КАНАЛУ СВЯЗИ С ОТВОДОМ

Антон Алексейчук, Сергей Гришаков
СФ СБ Украины в составе ВИТИ НТУУ "КПИ"

Аннотация: **Получены неасимптотические границы вероятности оптимального приема сообщений в отводном канале системы передачи информации со случайным кодированием, построенной на основе произвольной устойчивой функции над конечной абелевой группой. Описаны алгоритмы случайного кодирования и декодирования сообщений в основном канале с использованием нелинейных систематических кодов. Рассмотрен пример системы передачи со случайным кодированием, построенной на основе кодов Препараты.**

Summary: **Non-asymptotically bounds for the probability of optimal messages decoding in the wiretap channel of a information transmission system with random coding by a arbitrary resilient function over an Abelian group, are obtained. Algorithms of random messages coding and decoding in main channel which use non-linear systhematic codes, are described. An example of the information transmission system with random coding by Preparata codes is considered.**

Ключевые слова: **Криптографическая защита информации, случайное кодирование, отводной канал, устойчивая функция, нелинейный систематический код, код Препараты.**

I Введение

Концепция отводного канала, основанная на теоретико-информационной модели системы передачи дискретных сообщений по "каналу связи с подслушиванием" ("wire-tap channel") была впервые предложена в [1] и в дальнейшем получила развитие в [2 – 8] и ряде других работ. В настоящее время эта концепция охватывает широкий круг теоретических и прикладных задач в областях криптографии и стеганографии [6 – 10], позволяя строить унифицированные математические модели вероятностно-криптографических систем [11] и решать, в определенной степени, едиными общими методами различные по своей прикладной направленности криптографические задачи.

В рамках классической концепции отводного канала, в последние годы заметное развитие получило направление, имеющее своей задачей разработку математических основ теории кодовой защиты информации [5], включающей, в том числе, методы построения неасимптотических оценок стойкости и практически эффективных алгоритмов кодирования-декодирования сообщений в системах передачи информации по каналу связи с отводом [3, 4, 12 – 17]. Наиболее подробно изученный класс таких систем составляют системы передачи с линейным случайным кодированием в двоичном симметричном канале, являющиеся традиционным объектом исследования в теории кодовой защиты [1, 3 – 5].

Вероятностные характеристики эффективности систем со случайным кодированием, построенных на основе произвольных равновероятных функций, изучались в [12, 18 – 20] (в случае двоичного симметричного отводного канала) и [16, 17, 21] (для модели отводного канала с аддитивным шумом, распределенным на конечной абелевой группе). Целью настоящей статьи является продолжение указанных исследований, в частности, построение аналитических оценок стойкости и алгоритмов кодирования-декодирования сообщений в системах передачи со случайным кодированием, основанном на устойчивых функциях [22], включая системы со случайным кодированием нелинейными систематическими кодами над произвольной конечной абелевой группой.

II Определения основных понятий и некоторые вспомогательные результаты

Пусть F – конечная абелева группа порядка $q \geq 2$, σ: $F^n \to F^k$ – равновероятная функция, $1 < k < n$. Для любого $s \in F^k$ положим $C_s = \sigma^{-1}(s)$; в силу равновероятности σ имеем $|C_s| = q^{n-k}$, $s \in F^k$.

Запишем векторы, принадлежащие множеству C_s, в виде прямоугольной таблицы размера $q^{n-k} \times n$. Согласно определению [21, стр. 319], C_s называется *ортогональной таблицей с n ограничениями*, q *уровнями*, *силы t и индекса* λ, если для любых $1 \leq j_1 < \ldots < j_t \leq n$ каждый вектор, принадлежащий группе F^t, встречается в столбцах с номерами $j_1, \ldots, j_t$ таблицы C_s ровно λ раз. Множество всех ортогональных таблиц над группой F с указанными параметрами n, q, t и λ обозначим через $OA_\lambda(t, n, q)$.

Функция σ: $F^n \to F^k$ называется *t-устойчивой* [22], если для любого $s \in F^k$ элементы множества C_s образуют ортогональную таблицу силы t: $C_s \in OA_\lambda(t, n, q)$, где $\lambda = q^{n-k-t}$.

Изучению различных свойств и способов построения устойчивых функций посвящено большое число публикаций (см., например, [24 – 26]). Данное выше определение выражает одно из известных (эквивалентных друг другу) характеристических свойств устойчивых функций [24]. Приведем необходимый для дальнейшего результат, устанавливающий критерий t-устойчивости функции σ в терминах дуальных расстояний кодов C_s, $s \in F^k$.

Напомним [27, стр. 108], что кодом длины n над абелевой группой F называется произвольное подмножество C множества F^n. Для любого кода $C \subseteq F^n$ мощности M положим

$$B_i(C) = M^{-1}\#\{(x, y) \in C^2 : \|x - y\| = i\},\ i \in \overline{0, n}, \tag{1}$$

$$B_i'(C) = M^{-2} \sum_{\substack{x \in F^n: \\ \|x\| = i}} \left| \hat{I}_C(x) \right|^2,\ i \in \overline{0, n}, \tag{2}$$

где $\|x\|$ обозначает вес Хэмминга (число ненулевых координат) произвольного вектора $x \in F^n$, I_C – индикатор множества C: $I_C(x) = 1$, если $x \in F^n$, $I_C(x) = 0$, если $x \in F^n \backslash C$;

$$\hat{I}_C(x) = \sum_{y \in C} \chi_y(x),\ x \in F^n \tag{3}$$

есть преобразование Фурье функции I_C (символом χ_y обозначен комплексный характер группы F^n, соответствующий элементу $y \in F^n$ при фиксированном изоморфизме группы F^n в ее группу характеров) [28]. Упорядоченные наборы чисел вида (1) и (2) называются соответственно *спектром расстояний* и *дуальным спектром расстояний* кода C [23, 27]. Непосредственно из равенств (1) – (3) следует, что для любого кода $C \subseteq F^n$

$$B_0(C) = B_0'(C) = 1. \tag{4}$$

Наименьшее натуральное $d' = d'(C)$, удовлетворяющее условию $B_{d'}'(C) \neq 0$, называется *дуальным расстоянием* кода C.

Известно [27, стр. 58], что код $C \subseteq F^n$ является ортогональной таблицей силы t в том и только том случае, когда его дуальное расстояние $d'(C)$ не меньше, чем $t + 1$. Отсюда на основании определения t-устойчивой функции вытекает следующее утверждение.

Утверждение 1 [25]**.** Функция σ: $F^n \to F^k$ является t-устойчивой тогда и только тогда, когда для любых $i \in \overline{1,t}$ и $s \in F^k$ выполняется равенство $B_i'(C_s) = 0$, где $C_s = \sigma^{-1}(s)$.

В [25] предложен способ построения устойчивых функций по нелинейным систематическим кодам над полем из двух элементов ($F = (\mathbf{GF}(2), +)$). Этот способ легко обобщается на случай систематического кода над произвольной конечной абелевой группой F. Пусть $C \subseteq F^n$ – систематический код, первые $n - k$ символов которого являются информационными (по определению это означает, что каждый вектор длины $n - k$ над группой Fвстречается ровно один раз в первых $n - k$ столбцах таблицы, составленной из слов кода C). Введем в рассмотрение множества

$$C_s = C + (0, s),\ s \in F^k, \tag{5}$$

где $(0, s)$ – вектор длины n, первые $n - k$ координат которого равны 0. Нетрудно видеть, что множества вида (5) образуют дизъюнктное объединение группы F^n, и для любого $s \in F^k$ выполняется равенство

$$d'(C_s) = d'(C). \tag{6}$$

Зададим функцию σ: $F^n \to F^k$, полагая $\sigma(x) = s$, где $s \in F^k$, в том и только том случае, когда $x \in C_s$. Тогда на основании утверждения 1 и равенств (5), (6) функция σ является t-устойчивой при $t = d'(C) - 1$.

Конкретные примеры устойчивых функций, построенных в соответствии с описанным выше способом по нелинейным двоичным кодам, можно найти в [25, 26].

III Устойчивые функции в системах передачи информации со случайным кодированием

Рассмотрим стандартную математическую модель системы передачи информации по каналу связи с отводом, состоящую из безызбыточного источника дискретных сообщений в алфавите F и двух статистически независимых каналов с общим входом [1, 2]. Предположим, что первый (основной) канал, предназначенный для передачи сообщений источника законному получателю информации, не имеет помех, а второй (отводной) канал, контролируемый противником, является q-ичным симметричным каналом с входным алфавитом F. Для данных натуральных k и n ($1 < k < n$) зафиксируем равновероятную функцию σ: $F^n \to F^k$ и рассмотрим случайное кодирование источника, при котором для передачи произвольного информационного сообщения $s \in F^k$ используется вектор $x \in F^n$, выбираемый случайно и равновероятно во множестве $C_s = \sigma^{-1}(s)$. Поскольку основной канал не имеет помех, то законный получатель однозначно восстановит сообщение s, вычисляя его по формуле $s = \sigma(x)$. В отводном канале вектор x искажается и преобразуется в вектор $y = x + \xi$, где ξ – случайный вектор, распределенный на группе F^n по закону

$$P\{\xi = a\} = x(\Delta)^{n-\|a\|}\, y(\Delta)^{\|a\|},\ a \in F^n, \tag{7}$$

где $x(\Delta) = q^{-1}(1 + (q-1)\Delta)$, $y(\Delta) = q^{-1}(1 - \Delta)$, $\Delta \in [0, 1]$.

Для любого отображения (декодера отводного канала) δ: $F^n \to F^k$ обозначим через $\pi(\sigma; \delta) = P\{\delta(y) = s\}$ вероятность правильного приема сообщений в отводе с помощью декодера δ: $F^n \to F^k$. При $\delta = \sigma$ будем писать $\pi(\sigma)$ вместо $\pi(\sigma; \sigma)$. Следуя [12], примем в качестве показателя стойкости защиты информации в отводном канале вероятность $\pi^*(\sigma) = \pi(\sigma; \delta^*)$ правильного декодирования сообщений *оптимальным декодером* δ^*: $F^n \to F^k$, который определяется согласно следующему условию: $\pi(\sigma; \delta^*) \geq \pi(\sigma; \delta)$ для любого δ: $F^n \to F^k$.

Вероятностные характеристики эффективности систем передачи информации со случайным кодированием в канале с аддитивным шумом, распределенным на конечной абелевой группе, исследованы в [16, 17, 21]. В частности, в [17] показано, что при выполнении условия (7) для любой равновероятной функции σ: $F^n \to F^k$ и произвольного декодера δ: $F^n \to F^k$ выполняется равенство

$$\pi(\sigma; \delta) = q^{-2n} \sum_{s \in F^k} \sum_{a \in F^n} \Delta^{\|a\|}\, \hat{I}_{\sigma,s}(a)\overline{\hat{I}_{\delta,s}(a)}, \tag{8}$$

где $I_{\sigma,s}$ и $I_{\delta,s}$ – индикаторы множеств $\sigma^{-1}(s)$ и $\delta^{-1}(s)$ соответственно, $s \in F^k$, $\hat{I}_{\sigma,s}$, $\hat{I}_{\delta,s}$ – преобразования

Фурье указанных функций, и $\overline{\hat{I}_{\delta,s}(a)}$ обозначает число, комплексно-сопряженное к $\hat{I}_{\delta,s}(a)$.

Докажем следующее утверждение, устанавливающее аналитические границы стойкости защиты информации в отводном канале системы передачи со случайным кодированием, построенной на основе устойчивой функции σ.

Утверждение 2. Пусть σ: $F^n \to F^k$ является t-устойчивой функцией, и распределение вероятностей случайного вектора ξ искажений в отводе имеет вид (7). Тогда справедливы соотношения

$$\pi(\sigma) = q^{-k} \sum_{s \in F^k} q^{-k} \Big(1 + \sum_{t+1 \le i \le n} B_i'(C_s)\Delta^i\Big), \tag{9}$$

$$q^{-k} \le \pi(\sigma) \le \pi^*(\sigma) \le q^{-k} + \Delta^{\frac{t+1}{2}} (\pi(\sigma) - q^{-k})^{1/2}, \tag{10}$$

где $(B_i'(C_s)\colon\ i \in \overline{0,n})$ – дуальный спектр расстояний кода $C_s = \sigma^{-1}(s), s \in F^k$.

Доказательство. Равенство (9) следует непосредственно из соотношений (2), (4), (8) и утверждения 1. Убедимся в справедливости верхней границы (10) (нижняя граница очевидна в силу определения оптимального декодера δ^* и формулы (9)).

Выделяя во внутренней сумме в правой части равенства (8) слагаемое, соответствующее значению $a = 0$ и используя равенства $\hat{I}_{\sigma,s}(a) = 0, 1 \le \|a\| \le t$ (см. утверждение 1 и формулу (2)), получим

$$\pi(\sigma;\delta) = q^{-2n} \sum_{s \in F^k} \hat{I}_{\sigma,s}(0)\overline{\hat{I}_{\delta,s}(0)} + q^{-2n} \sum_{s \in F^k} \sum_{\substack{a \in F^n: \\ \|a\| \ge t+1}} \Delta^{\|a\|} \hat{I}_{\sigma,s}(a)\overline{\hat{I}_{\delta,s}(a)} =$$

$$= q^{-k} + q^{-2n} \sum_{s \in F^k} \sum_{\substack{a \in F^n: \\ \|a\| \ge t+1}} (\Delta^{\frac{1}{2}\|a\|} \hat{I}_{\sigma,s}(a))\overline{(\Delta^{\frac{1}{2}\|a\|} \hat{I}_{\delta,s}(a))},$$

откуда в силу неравенства Коши-Буняковского следует, что

$$\pi(\sigma;\delta) \le q^{-k} + q^{-2n} \Big(\sum_{s \in F^k} \sum_{\substack{a \in F^n: \\ \|a\| \ge t+1}} \Delta^{\|a\|} \Big|\hat{I}_{\sigma,s}(a)\Big|^2\Big)^{1/2} \Big(\sum_{s \in F^k} \sum_{\substack{a \in F^n: \\ \|a\| \ge t+1}} \Delta^{\|a\|} \Big|\hat{I}_{\delta,s}(a)\Big|^2\Big)^{1/2}. \tag{11}$$

Используя равенство Парсеваля [28], оценим сверху второй сомножитель в выражении (11) следующим образом:

$$\Big(\sum_{s \in F^k} \sum_{\substack{a \in F^n: \\ \|a\| \ge t+1}} \Delta^{\|a\|} \Big|\hat{I}_{\delta,s}(a)\Big|^2\Big)^{1/2} \le \Delta^{\frac{t+1}{2}} \Big(\sum_{s \in F^k} \sum_{\substack{a \in F^n: \\ \|a\| \ge t+1}} \Big|\hat{I}_{\delta,s}(a)\Big|^2\Big)^{1/2} \le \Delta^{\frac{t+1}{2}} \Big(\sum_{s \in F^k} \sum_{a \in F^n} \Big|\hat{I}_{\delta,s}(a)\Big|^2\Big)^{1/2} =$$

$$= \Delta^{\frac{t+1}{2}} \Big(q^n \sum_{s \in F^k} \sum_{a \in F^n} \Big|I_{\delta,s}(a)\Big|^2\Big)^{1/2} = q^n \Delta^{\frac{t+1}{2}}.$$

Отсюда на основании неравенства (11) и соотношений (2), (9) получим, что

$$\pi(\sigma;\delta) \le q^{-k} + \Delta^{\frac{t+1}{2}} \Big(q^{-2n} \sum_{s \in F^k} \sum_{\substack{a \in F^n: \\ \|a\| \ge t+1}} \Delta^{\|a\|} \Big|\hat{I}_{\sigma,s}(a)\Big|^2\Big)^{1/2} = q^{-k} + \Delta^{\frac{t+1}{2}} (\pi(\sigma) - q^{-k})^{1/2}.$$

Утверждение доказано.

Непосредственно из соотношений (9), (10) вытекает следующий результат.

Следствие 1. При выполнении условия утверждения 2 для вероятности $\pi^*(\sigma)$ справедливы оценки

$$q^{-k} \le \pi^*(\sigma) \le q^{-k} + \Delta^{t+1}.$$

IV Случайное кодирование нелинейным систематическим кодом в q-ичном симметричном канале

Применим полученные выше результаты к оценке стойкости систем со случайным кодированием, построенных на основе нелинейных систематических кодов над абелевой группой F.

Рассмотрим систематический код $C \subseteq F^n$ мощности q^{n-k}, информационные символы которого имеют номера $1, 2, \ldots, n-k$, где $1 < k < n$, и обозначим через σ устойчивую функцию, соответствующую коду C (см. п. II). Заметим, что, поскольку коды C_s ($s \in F^k$) вида (5) отличаются друг от друга сдвигами в группе F^n, то они имеют одинаковые спектры расстояний, и следовательно (в силу тождества Мак-Вильямс [23]), одинаковые дуальные спектры расстояний. Отсюда на основании утверждений 1, 2 получаем такое утверждение.

Следствие 2. Пусть функция $\sigma\colon F^n \to F^k$ построена по систематическому коду $C \subseteq F^n$ мощности q^{n-k}, d' – дуальное расстояние кода C. Тогда при выполнении условия (7) для вероятности $\pi^*(\sigma)$ оптимального приема сообщений в отводном канале системы передачи со случайным кодированием, построенной на основе функции σ, имеют место следующие оценки:

$$\pi(\sigma) \le \pi^*(\sigma) \le q^{-k} + \Delta^{\frac{t+1}{2}} (\pi(\sigma) - q^{-k})^{1/2}, \tag{12}$$

где

$$\pi(\sigma) = q^{-k} (1 + \sum_{i=d'}^{n} B_i'(C) \Delta^i), \tag{13}$$

($B_i'(C)\colon i \in \overline{0, n}$) – дуальный спектр расстояний кода C.

Рассмотрим подробнее возможные способы построения практически эффективных алгоритмов случайного кодирования и декодирования (в основном канале) сообщений в системах передачи информации с нелинейным случайным кодированием.

Пусть $\sigma\colon F^n \to F^k$ – устойчивая функция, соответствующая систематическому коду $C \subseteq F^n$ мощности q^{n-k}. Обозначим через $f(t)$ k-мерный вектор над группой F, состоящий из проверочных символов кодового слова $(t, f(t)) \in C$, информационные символы которого определяются вектором $t \in F^{n-k}$. Заметим, что на основании равенства (5) каждый вектор $x \in F^n$ допускает единственное представление в виде

$$x = (t, f(t)) + (0, s) = (t, s + f(t)),\ t \in F^{n-k},\ s \in F^k. \tag{14}$$

Отсюда следует, что *случайное кодирование информационного сообщения $s \in F^k$ с использованием кода C* может быть реализовано путем вычисления значения x по формуле (14), где t представляет собой случайный равновероятный вектор длины $n - k$ над группой F. При этом *декодирование сообщения* $x = (x_1, x_2)$, где $x_1 \in F^{n-k}$, $x_2 \in F^k$, *законным получателем* осуществляется в соответствии с равенством $s = \sigma(x) = x_2 - f(x_1)$.

Ясно, что трудоемкость описанных процедур кодирования-декодирования сообщений определяется сложностью вычисления значений функции $f\colon F^{n-k} \to F^k$ (проверочных символов по информационным символам кода C). Важно отметить, что эффективность алгоритмов случайного кодирования или декодирования сообщений нелинейным систематическим кодом (над полем из двух элементов) можно существенно повысить в случае, когда исходный двоичный код C обладает "эффективно вычислимым" линейным представлением над подходящим конечным коммутативным кольцом [29]. Впервые такое представление было построено в [30] для кода Кердока; в [29, 31, 32] получены аналогичные представления кодов Препараты и некоторых других нелинейных двоичных кодов, превосходящих, в ряде случаев, по своей корректирующей способности известные линейные коды с теми же параметрами.

С целью иллюстрации изложенных выше результатов на конкретном примере нелинейных двоичных кодов, рассмотрим последовательность кодов Препараты ($\Pi_m\colon m = 4, 6, \ldots$). Для каждого четного $m \ge 4$ код Π_m имеет длину $n = 2^m$, мощность 2^{n-2m}, дуальное расстояние $d' = 2^{m-1} - 2^{(m-2)/2}$ и является нелинейным систематическим кодом [23, стр. 454]. Отсюда на основании утверждения 1 вытекает, что этому коду соответствует $(d'-1)$-усточивая функция $\sigma_m\colon F^n \to F^k$, где $k = 2m$. Дуальный спектр расстояний кода Π_m (см. табл. 1) совпадает со спектром расстояний кода Кердока длины $n = 2^m$ [23, стр. 440].

Таблица 1 – Дуальный спектр расстояний кода Препараты

i	$B_i'(\Pi_m)$
0	1
$2^{m-1}-2^{(m-2)/2}$	$2^m(2^{m-1}-1)$
2^{m-1}	$2^{m+1}-2$
$2^{m-1}+2^{(m-2)/2}$	$2^m(2^{m-1}-1)$
2^m	1

В табл. 2 приведены (полученные с использованием соотношений (12), (13) и данных табл. 1) результаты расчетов границ вероятности $\pi^*(\sigma_m)$ оптимального приема сообщений в отводном канале системы передачи со случайным кодированием, построенной на основе кода Π_m при $m = 4, 6$, и различных значениях вероятности $p = \frac{1}{2}(1-\Delta)$ искажения символа в отводном (двоичном симметричном) канале. Для сравнения в таблице указаны также значения вероятности

$$\pi(H_m) = \frac{1}{2^m}\left(1+(2^m-1)\Delta^{2^{m-1}}\right),\ \Delta = 1-2p,$$

оптимального декодирования сообщений в отводном канале системы передачи со случайным кодированием кодом Хэмминга H_m с параметрами $(2^m - 1,\ 2^m - m - 1)$ [3]. Через $R(\Pi_m) = \frac{m}{2^{m-1}}$ и $R(H_m) = \frac{m}{2^m-1}$ обозначены скорости передачи кодов Π_m и H_m соответственно.

Таблица 2 – Характристики эффективности систем передачи информации со случайным кодированием кодами Препараты и Хэмминга

p	$m = 4$				
	Нижняя граница (12)	Верхняя граница (12)	$\pi(H_m)$	$R(\Pi_m)$	$R(H_m)$
0,01	0,8515	0,8704	0,8601	0,5000	0,2667
0,02	0,7238	0,7546	0,7388	0,5000	0,2667
0,10	0,1853	0,2220	0,2198	0,5000	0,2667
0,20	0,0289	0,0381	0,0782	0,5000	0,2667
p	$m = 6$				
	Нижняя граница (12)	Верхняя граница (12)	$\pi(H_m)$	$R(\Pi_m)$	$R(H_m)$
0,01	0,5256	0,5465	0,5313	0,1857	0,0952
0,02	0,2745	0,2959	0,2822	0,1857	0,0952
0,10	0,0014	0,0017	0,0164	0,1857	0,0952
0,20	0,0002	0,0002	0,0156	0,1857	0,0952

Как видно из табл. 2, при относительно малой вероятности искажения в отводном канале ($p \le 0{,}02$) и равных (с точностью до 1) длинах кодовых слов коды Хэмминга и Препараты обеспечивают примерно одинаковую стойкость защиты информации в отводе. С ухудшением отводного канала ($p \ge 0{,}1$) и увеличением длины кодового слова стойкость защиты информации кодами Препараты оказывается существенно выше по сравнению со стойкостью, обеспечиваемой при применении кодов Хэмминга (на 1 меньшей длины). Так, при $m = 6$, $p = 0{,}1$ вероятность $\pi^*(\sigma_m)$ почти на порядок мешьше вероятности $\pi(H_m)$. При этом во всех случаях код Препараты Π_m имеет практически в два раза большую по сравнению с кодом Хэмминга H_m скорость передачи.

V Выводы

Одним из новых, перспективных направлений теории кодовой защиты информации является разработка методов построения и анализа эффективности систем передачи со случайным кодированием, основанном на

устойчивых функциях. Как следует из результатов [25, 26], случайное кодирование с использованием устойчивых функций включает в себя, в качестве частных случаев, способ случайного кодирования сообщений линейными кодами [1, 3 – 5], а также описанный выше способ случайного кодирования с помощью нелинейных систематических кодов (над произвольной конечной абелевой группой F).

Стойкость защиты информации в отводном канале системы передачи со случайным кодированием, построенной на основе t-устойчивой функции, существенно зависит от параметра t (см. утверждение 2 и следствия 1, 2). При этом задача оптимизации стойкости (характеризуемой вероятностью $\pi^*(\sigma)$ оптимального приема сообщений в отводе) при заданных качестве отводного канала и скорости передачи информации законному получателю тесно связана с известной в криптографии проблемой максимизации коэффициента t устойчивости функции $\sigma: F^n \to F^k$ при фиксированном отношении k/n [26].

Использование в системах со случайным кодированием нелинейных систематических кодов, имеющих “большие” дуальное расстояние и скорость передачи и обладающих “эффективно вычислимыми” линейными представлениями над коммутативными кольцами [29 – 32] (в частности, кодов Препараты), позволяет при определенных условиях повысить эффективность указанных систем по сравнению с эффективностью аналогичных систем передачи со случайным кодированием линейными блоковыми кодами.

Литература: ***1.*** *Wyner A. D. The Wire-Tap Channel // Bell System Techn. J. – 1975. – V. 54. - № 8. – P. 1355 – 1388.* ***2.*** *Csiszar I., Korner J. Broadcast Channels with Confidential Messages // IEEE Trans. Inform. Theory. – 1978. – V. 24. – № 3. – P. 339 – 348.* ***3.*** *Коржик В. И., Яковлев В .А. Неасимптотические оценки кодового зашумления одного канала // Проблемы передачи информации. – 1981.– Т.17.– В.4.– С.11 – 18.* ***4****. Коржик В. И., Яковлев В .А. Пропускная способность канала связи с внутренним случайным кодированием // Проблемы передачи информации. – 1992. – Т. 28. – В. 4. – С. 24 – 34.* ***5.*** *Горицкий В. М. Вероятностная криптография в системах защиты информации: кодовая защита // Электроника и связь. – 1998. – В. 5. – С. 140 – 145.* ***6.*** *Maurer U. M., Massey J .L. Perfect local randomness in pseudo-random sequences // Advances in Cryptology – CRYPTO' 89, Proceedings. – Springer Verlag, 1990. – P. 110-112.* ***7.*** *Чисар И. Почти независимость случайных величин и пропускная способность криптостойкого канала // Проблемы передачи информации. – 1996. – Т. 32. – В. 1. – С. 48-57.* ***8.*** *Bennet C. H., Brassard G., Maurer U. M. Generalized privacy amplifications // IEEE Trans. Inform. Theory. – 1995. – V. 41. – № 6. – P. 1915-1923.* ***9.*** *Ahlswede R., Csiszar I. Common randomness in information theory and cryptography – Part 1: Secret sharing // IEEE Trans. Inform. Theory. – 1993. – V. 39. – № 4. – P. 1121 – 1132.* ***10.*** *Korjik V., Morales-Luna G. Information hiding though noisy channels // IH' 2001, Proceedings. – Springer Verlag, 2001. – P. 42 – 50.* ***11.*** *Алексейчук А. Математическая модель и задачи анализа стойкости вероятностно-криптографических систем в системах защиты информации // Захист інформації. – 2001. – № 3. – С. 5-12.* ***12.*** *Иванов В. А. О методе случайного кодирования // Дискретная математика. – 1999. – Т. 11. – В. 3. – С. 99 – 108.* ***13.*** *Алексейчук А. Н. Оценки эффективности кодовой защиты дискретных сообщений с использованием линейных кодов с большим дуальным расстоянием // Реєстрація, зберігання і обробка даних. – 2001. – Т. 3 – № 2. – С. 99 – 106.* ***14.*** *Алексейчук А. Н., Дроздовский Т. А., Сергиенко Ю. В. Система передачи информации со случайным кодированием, построенная на основе кодов Рида-Соломона // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Вып. 6. – К.: 2003. – С. 84-89.* ***15.*** *Алексейчук А. Н., Сергиенко Ю. В. Оценки стойкости и способ реализации кодовой защиты дискретных сообщений с использованием каскадных кодов // Электронное моделирование. – 2003. – Т. 25. – № 5. – С. 33-44.* ***16.*** *Алексейчук А. Н. Случайное кодирование в канале связи с аддитивным шумом, распределенным на конечной абелевой группе // Захист інформації. – 2002.– № 3.– С. 7 – 16.* ***17.*** *Алексейчук А. Н. Оптимальное случайное кодирование равновероятных сообщений в q-ичном симметричном канале // Захист інформації. – 2002. – № 4. – С. 49 – 58.* ***18.*** *Иванов В. А. Об использовании случайных кодов в алгоритмах защиты информации // Обозрение прикл. и промышл. матем.– 2001.– Т. 8. – вып. 3.– С.613-614.* ***19.*** *Ошкин И. Б., Проскурин Г. В. Нижние оценки различения подмножеств единичного куба // Проблемы передачи информации. – 1994. – Т. 30. – В. 3. – С. 15-22.* ***20.*** *Пазизин С. В. О характеристиках случайных блоковых кодов, порождающих ошибки // Обозрение прикл. и промышл. матем.– 2000.– Т. 7. – вып. 2.– С.520 – 521.* ***21.*** *Алексейчук А. Н. Вероятность правильного декодирования как функция канала групповой вероятностно-криптографической системы // Збірник наукових праць ІПМЕ НАН України. – 2004. – Вып. 21 (в печати).* ***22.*** *Bennet C. H., Brassard G., Robert J.-M. Privacy amplifications by public discussion // SIAM J. Comput. – 1988. – V. 17. – P. 210 – 229.* ***23.*** *Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки: Пер. с англ. – М.: Связь, 1979. – 743 с.* ***24.*** *Stinson D. R. Resilient functions and large sets of orthogonal arrays // Congressus Numer. – 1993. – V. 92. – P. 105-110.* ***25.*** *Stinson D. R., Massey J. L. An infinite class of countrexamples to a conjecture concerning non-linear resilient functions // J.*

Cryptology. – 1995. – № 8. – P. 167-173. ***26.*** *Bierbrauer J., Gopalakrishnan K., Stinson D. R. Orthogonal arrays, resilient functions, error correcting codes and linear programming bounds // Advances in Cryptology – CRYPTO' 94, Proceedings. – Springer Verlag, 1994. – P. 247-256.* ***27.*** *Дельсарт Ф. Алгебраический подход к схемам отношений теории кодирования. – М.: Мир, 1976. – 134 с.* ***28.*** *Зиновьев В. А., Эриксон Т. О Фурье-инвариантных разбиениях конечных абелевых групп и тождестве Мак-Вильямс для групповых кодов // Проблемы передачи информации. – 1996.– Т. 32.– Вып. 1. – С.137 – 143.* ***29.*** *Кузьмин А. С., Нечаев А. А. Линейно представимые коды и код Кердока над произвольным полем Галуа характеристики 2 // Успехи матем. наук – 1994. – Т. 49. – № 5. – С. 165 – 166.* ***30.*** *Нечаев А. А. Код Кердока в циклической форме // Дискретная математика. – 1989. – Т. 1. – Вып. 4. – С. 123-139.* ***31.*** *Hammous A. R., Kumar P. V., Calderbrank A. R., Sloane N. J. A., Sole P. The Z_4-linearity of Kerdock, Preparata, Goethals and related codes // Bull. Amer. Math. Soc. – 1993. – V. 29. – №. 2. – P. 218-222.* ***32.*** *Кузьмин А. С., Нечаев А. А. Построение помехоустойчивых кодов с использованием линейных рекуррент над кольцами Галуа // Успехи матем. наук – 1992. – Т. 47. – № 5. – С. 183 – 184.*

УДК 681.321;322:621.395

АНАЛІЗ ПРОБЛЕМИ РОЗПОДІЛУ ВИТРАТ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Володимир Кононович, Микола Тардаскін, Тетяна Тардаскіна*

Одеський регіональний центр технічного захисту інформації ВАТ "Укртелеком",
**Одеська національна академія зв'язку*

Анотація: **Розглядаються проблеми розподілу засобів інформаційної безпеки по елементам інформаційно-телекомунікаційних систем, формулюється задача оптимізації витрат на інформаційну безпеку.**

Summary: **The problem of information security devices distribution on the elements of information telecommunication systems is considered and the task of optimization expenses for information security is formulated.**

Ключові слова: **Інформаційна безпека, автоматизовані системи, інформаційно-телекомунікаційні системи, загрози, послуги та механізми безпеки, функціональний профіль захисту.**

І Вступ

З розширенням ролі інформаційно-телекомунікаційних систем в роботі органів державного управління, в обробці електронних документів, в освіті, бізнесі та інших сферах інформаційної діяльності зростає увага до інформаційної безпеки. Вдосконалення сучасних мереж, як загального користування, так спеціальних і корпоративних здійснюється в умовах підвищення вимог до надійності функціонування зв'язку, сталості та інформаційної безпеки телекомунікаційних мереж, якості та безпеки телекомунікаційних послуг. Актуальною стає задача побудови "довіреного" телекомунікаційного середовища. За методами побудови серед систем забезпечення інформаційної безпеки виділяються накладені, тобто побудовані "поверх" існуючих систем [1, 2], та вбудовані як підсистеми захисту інформаційних ресурсів. Приміром, в АТМ-мережах рекомендуються до застосування три основні механізми захисту інформації: шифрування інформації з метою збереження її конфіденційності, автентифікації аспектів інформаційної взаємодії, контроль цілісності й незмінності даних при передаванні та зберіганні [3]. Міжнародні рекомендації щодо нових телекомунікаційних технологій включають вбудовані підсистеми інформаційної безпеки [4, 5].

При виборі функціонального профілю захисту інформаційно-телекомунікаційних систем або частин їх декомпозиції є актуальною задача оптимального розподілу послуг та механізмів безпеки поміж елементами інформаційно-телекомунікаційної системи. Необхідне використання механізмів захисту, які підвищують загальний рівень безпеки телекомунікаційної мережі й дозволяють дати більш високу гарантію відносно окремих вузлів і мереж у цілому.

Метою даної роботи є аналіз проблем оптимального розподілу послуг і механізмів безпеки в інформаційно-телекомунікаційних системах та пошук методів зниження загальних витрат на інформаційну безпеку.