УДК 621.391:519.2

НЕАСИМПТОТИЧЕСКИЕ ОЦЕНКИ ЭФФЕКТИВНОСТИ СЛУЧАЙНОГО КОДИРОВАНИЯ В СИСТЕМЕ ПЕРЕДАЧИ ИНФОРМАЦИИ ПО ДВОИЧНОМУ СИММЕТРИЧНОМУ КАНАЛУ СВЯЗИ С ОТВОДОМ

А.Н. АЛЕКСЕЙЧУК, С.В. ГРИШАКОВ

Исследована эффективность случайного кодирования при многократной передаче безизбыточных сообщений по двоичному симметричному каналу связи с отводом. Получены неасимптотические оценки надежности восстановления сообщений законным получателем информации и стойкости их защиты в отводном канале.

ВВЕДЕНИЕ

Математическая модель системы передачи информации по каналу связи с отводом предложена в [1] и в дальнейшем изучалась в [2–11] и ряде других работ. В настоящее время эта модель широко используется при разработке алгоритмических методов защиты информации от утечки по побочным каналам связи, квантово-криптографических протоколов распределения ключей, схем разделения секрета, а также при решении других криптографических задач [10, 11].

Традиционная система передачи информации по каналу связи с отводом состоит из двух статистически независимых каналов связи с общим входом. Выход одного (основного) канала наблюдает законный получатель, а выход другого (отводного) канала — противник. Для повышения стойкости защиты информации в отводном канале применяют случайное кодирование, при котором входные сообщения преобразуются в дискретные сигналы, выбираемые случайно и равновероятно из подходящих конечных множеств. В большинстве доступных публикаций, посвященных исследованию эффективности случайного кодирования, рассматривается случай, в котором основной канал связи является идеальным (не имеет помех), а отводной — двоичным симметричным каналом или каналом со стиранием [3, 5–11]. В частности, в [8, 9] были исследованы асимптотические свойства характеристик эффективности случайного кодирования при многократной передаче безизбыточного случайного сообщения по идеальному основному и двоичному симметричному отводному каналам связи, а также получены асимптотические оценки минимального количества передач, необходимого для восстановления противником переданного сообщения с заданной надежностью. Вместе с тем, асимптотический вид оценок, полученных в [8, 9], не позволяет применять их непосредственно к системам со случайным кодированием кодами фиксированной длины.

Цель работы — исследовать эффективность случайного кодирования при многократной передаче сообщений по неидеальному основному каналу связи. В работе получены неасимптотические оценки вероятности правильного восстановления сообщений законным получателем и, соответственно, противником. Показано, что при определенных соотношениях между параметрами линейных кодов, применяемых для случайного кодирования, и вероятностями искажений в основном и отводном каналах можно обеспечить надежный прием сообщений законным получателем при высокой практической стойкости их защиты в отводе, используя сравнительно небольшое число передач.

ПОСТАНОВКА ЗАДАЧИ И ОСНОВНЫЕ РЕЗУЛЬТАТЫ

Рассмотрим систему передачи информации по каналу связи с отводом, состоящую из источника и двух статистически независимых каналов связи с общим входом: основного канала — от источника к законному получателю, и отводного канала — от источника к противнику [1, 2]. Предположим, что основной канал является двоичным симметричным каналом с вероятностью ошибки p_1, а отводной — двоичным симметричным каналом с вероятностью ошибки p_2, где $0 < p_1 < p_2 < 0{,}5$. Источник вырабатывает случайное сообщение S с равномерным распределением на множестве $V_k = \{0,1\}^k$, для передачи которого отправитель выбирает сюръективное линейное отображение $\sigma : V_n \to V_k$ и генерирует t независимых случайных векторов $X_1, ..., X_t$ с равномерным распределением на множестве $C_s = \sigma^{-1}(s)$, где $s \in V_k$ — значение случайного вектора S. Затем последовательность $X_1, ..., X_t$ передается по основному и отводному каналам связи. При этом она искажается и в основном канале преобразовывается в случайную последовательность $Y_1, ..., Y_t$, а в отводном канале — в случайную последовательность $Z_1, ..., Z_t$. Необходимо получить оценки вероятности правильного восстановления сообщения S по каждой из указанных последовательностей в предположении, что декодеры основного и отводного каналов строятся на основе тех или иных практически реализуемых алгоритмов.

Предположим, что законный получатель информации применяет следующий алгоритм декодирования по методу максимума правдоподобия.

Алгоритм 1. Пусть $y = y_1, ..., y_t$ — наблюдаемая реализация случайной последовательности $Y_1, ..., Y_t$. Тогда получатель находит последовательность $\sigma(y) = \sigma(y_1), ..., \sigma(y_t)$ и выбирает в качестве оценки искомого значения случайного вектора S произвольный элемент $s^* = s^*(y)$ с наибольшей частотой встречаемости в последовательности $\sigma(y)$.

Если противнику известен некоторый критерий отбраковки ложных значений сообщения S (например, S является ключом симметричной криптосистемы, и существует возможность его опробования), то алгоритм 1 можно модифицировать следующим образом.

Алгоритм 2. Пусть $z = z_1, ..., z_t$ — наблюдаемая реализация случайной последовательности $Z_1, ..., Z_t$. Тогда противник находит последовательность $\sigma(z) = \sigma(z_1),..., \sigma(z_t)$, составляет список ее членов, расположенных в порядке убывания их частот, и опробует в указанном порядке (до первого успеха) векторы из списка.

Обозначим $\lambda_1 = \lambda_1(t, p_1)$ и $\lambda_2 = \lambda_2(t, p_2)$ вероятности правильного восстановления сообщения S с использованием алгоритмов 1 и 2 соответственно. Для того, чтобы привести оценки параметров λ_1, λ_2, введем ряд дополнительных обозначений.

Обозначим C линейный $(n, n-k)$-код, равный ядру отображения σ. Для любого $p \in [0, 1]$ положим

$$\pi(C_s; p) = \sum_{u \in C_s} p^{\|u\|} (1-p)^{n-\|u\|}, \qquad (1)$$

где $C_s = \sigma^{-1}(s)$ — смежный класс (СК) кода C, соответствующий вектору $s \in V_k$;

$$\pi_0(C; p) = \pi(C_0; p),\ \pi_1(C; p) = \max\{\pi(C_s; p) : s \in V_k \setminus \{0\}\}. \qquad (2)$$

Отметим, что на основании тождества Мак-Вильямс [12]

$$\pi(C_s; p) = 2^{-k} \sum_{u \in C^{\perp}} (-1)^{au} \Delta^{\|u\|},\ s \in V_k, \qquad (3)$$

где $C^{\perp}$ — код, дуальный к C; a — произвольный вектор, принадлежащий СК C_s; au — булево скалярное произведение векторов $a, u \in V_n$, $\Delta = 1 - 2p$. Отсюда непосредственно следует, что $\pi_1(C; p) < \pi_0(C; p)$ для любого $0 < p < 0{,}5$.

Утверждение 1. Справедливы неравенства

$$\lambda_1(t, p_1) \geq 1 - 2^k \exp\left\{-\frac{t}{2}(\pi_0(C; p_1) - \pi_1(C; p_1))^2\right\}, \qquad (4)$$

$$\lambda_2(t, p_2) \leq 1 - (1 - \pi_0(C; p_2))^t. \qquad (5)$$

Доказательство. Как следует из описания алгоритма 2, вероятность его успешного завершения не превосходит вероятности события, состоящего в том, что случайный вектор S присутствует в последовательности $\sigma(Z)$. Последнее равносильно тому, что хотя бы один из векторов искажений, переводящих слово X_i в слово Z_i в отводном канале, принадлежит коду C, $i = \overline{1, t}$. Отсюда вытекает справедливость неравенства (5).

Докажем неравенство (4). Обозначим P_s условное распределение вероятностей на множестве значений случайной последовательности $Y = Y_1, ..., Y_t$ при условии $S = s$; $n_s(Y)$ — частоту появления вектора s в последовательности $\sigma(Y)$. Справедливо равенство

$$\lambda_1(t, p_1) = 2^{-k} \sum_{s \in V_k} P_s\{s^*(Y) = s\}\,. \qquad (6)$$

Заметим теперь, что для любого $s \in V_k$ событие $\{s^*(Y) \neq s\}$ влечет событие $\bigcup_{s' \neq s} \{n_{s'}(Y) > n_s(Y)\}$. Следовательно, для любого $A > 0$ выполняются следующие неравенства:

$$P_s\{s^*(Y) \neq s\} \le P_s\left(\bigcup_{s' \neq s} \{n_{s'}(Y) > n_s(Y)\}\right) \le$$

$$\le P_s\{n_s(Y) \le A\} + \sum_{s' \neq s} P_s\{n_{s'}(Y) > A\}\,. \qquad (7)$$

Далее, при выполнении условия $S = s$ случайная величина $n_s(Y)$ имеет биномиальное распределение с параметрами $(t, \pi_0(C; p_1))$, а случайная величина $n_{s'}(Y)$ — биномиальное распределение с параметрами $(t, \pi(C_{s \oplus s'}; p_1))$. Следовательно, в силу неравенств для вероятностей больших уклонений [13] при выполнении условия

$$\pi_1(C; p_1) < At^{-1} < \pi_0(C; p_1) \qquad (8)$$

для любых $s, s' \in V_k$, $s' \neq s$, справедливы следующие неравенства:

$$P_s\{n_s(Y) \le A\} \le \exp\{-2t(At^{-1} - \pi_0(C; p_1))^2\}\,, \qquad (9)$$

$$P_s\{n_{s'}(Y) > A\} \le \exp\{-2t(At^{-1} - \pi(C_{s \oplus s'}; p_1))^2\}\,. \qquad (10)$$

Подставляя оценки (9), (10) в формулу (7) и принимая во внимание второе соотношение (2), получим, что при выполнении условия (8)

$$P_s\{s^*(Y) \neq s\} \le \exp\{-2t(At^{-1} - \pi_0(C; p_1))^2\} +$$

$$+ (2^k - 1)\exp\{-2t(At^{-1} - \pi_1(C; p_1))^2\}\,. \qquad (11)$$

Наконец, полагая в формуле (11) $At^{-1} = \frac{1}{2}(\pi_0(C; p_1) + \pi_1(C; p_1))$, на основании равенства (6) получим соотношение

$$\lambda_1(t, p_1) \ge 1 - 2^k \exp\left\{-2t\left(\frac{\pi_0(C; p_1) - \pi_1(C; p_1)}{2}\right)^2\right\},$$

которое равносильно неравенству (4).

Утверждение доказано.

Отметим, что соотношения (4), (5) справедливы для любого линейного $(n, n-k)$-кода C. Чтобы оценивать с их помощью эффективность систем со случайным кодированием, построенных на основе конкретных кодов, необходимо иметь пригодные для практических вычислений границы парамет-

ров (2). Ряд таких границ, вытекающих, в основном, из результатов работ [7, 14–16], содержит следующее утверждение.

Утверждение 2. Пусть C — произвольный линейный $(n, n-k)$-код с минимальным расстоянием d и дуальным расстоянием d'. Тогда для любого $0 < p < 0{,}5$ справедливы следующие неравенства:

$$\pi_0(C; p) \le 2^{-k}(1 + (2^k - 1)\Delta^{d'}), \tag{12}$$

$$\pi_0(C; p) \le 2^{-\frac{kp}{1-p}}, \tag{13}$$

$$\pi_0(C; p) \le 2^{-k} + (1-\widetilde{p})^{-n}\begin{pmatrix}\left\lceil \frac{n}{2} \right\rceil + l \\ l\end{pmatrix}^{-1} \sum_{i=2l+1}^{n} \binom{n}{i} \widetilde{p}^{\,i}(1-\widetilde{p})^{n-i}, \tag{14}$$

где

$$\Delta = 1 - 2p,\ l = \left\lfloor \frac{d'-1}{2} \right\rfloor,\ \widetilde{p} = \frac{1-2p}{2(1-p)}. \tag{15}$$

Кроме того, справедливо неравенство

$$\pi_0(C; p) - \pi_1(C; p) \ge 2(1-p)^n \frac{\Delta^{n-k+1}}{1 + \Delta^{n-k+1}}, \tag{16}$$

а при условии $d \ge 3$ — неравенство

$$\pi_0(C; p) - \pi_1(C; p) \ge \Delta^{\frac{n+1}{2}}. \tag{17}$$

Обе границы (12), (17) достигаются, если C является кодом Хэмминга.

Доказательство. Справедливость оценки (12) и ее достижимость для кодов Хэмминга доказаны в [7]. Неравенство (13) следует из формулы

$$\pi_0(C; p) = (1-p)^n + P_{\text{но}}(C), \tag{18}$$

где

$$P_{\text{но}}(C; p) = \sum_{x \in C \setminus \{0\}} p^{\|x\|}(1-p)^{n-\|x\|} \tag{19}$$

есть вероятность необнаружения ошибки кодом C, и соотношения

$$P_{\text{но}}(C; p) \le \left(2^{-n} \mid C \mid\right)^{\frac{p}{1-p}} - (1-p)^n,$$

полученного в работе [16].

Для доказательства формулы (14) воспользуемся неравенством [15]

$$P_{\text{но}}(G; \widetilde{p}) \le \begin{pmatrix}\left\lceil \frac{n}{2} \right\rceil + l \\ l\end{pmatrix}^{-1} \sum_{i=2l+1}^{n} \binom{n}{i} \widetilde{p}^{\,i}(1-\widetilde{p})^{n-i},\ 0 < \widetilde{p} < 0{,}5 \tag{20}$$

справедливым для любого двоичного линейного кода G длины n, исправляющего l ошибок. Полагая в формуле (20) $G = C^{\perp}$, при выполнении (15) получим следующее неравенство:

$$P_{\text{но}}(C^{\perp};\widetilde{p}) \le \left(\begin{matrix}\left\lceil \frac{n}{2} \right\rceil + l \\ l\end{matrix}\right)^{-1} \sum_{i=2l+1}^{n} \binom{n}{i} \widetilde{p}^{\,i} (1-\widetilde{p})^{n-i}. \qquad (21)$$

Далее, согласно формуле (3) при $s=0$, выполняется равенство $\pi_0(C;p) = 2^{-k} \sum_{x\in C^{\perp}} \Delta^{\|x\|}$. Следовательно,

$$\pi_0(C;p) = 2^{-k} + \sum_{x\in C^{\perp}\setminus\{0\}} \Delta^{\|x\|} = 2^{-k} + \sum_{x\in C^{\perp}\setminus\{0\}} \left(\frac{\widetilde{p}}{1-\widetilde{p}}\right)^{\|x\|} =$$

$$= 2^{-k} + (1-\widetilde{p})^{-n} \sum_{x\in C^{\perp}\setminus\{0\}} \widetilde{p}^{\,\|x\|} (1-\widetilde{p})^{n-\|x\|} = 2^{-k} + (1-\widetilde{p})^{-n} P_{\text{но}}(C^{\perp};\widetilde{p}). \qquad (22)$$

Подставляя оценку (21) в формулу (22), получим неравенство (14).

Для доказательства неравенства (16) воспользуемся следующей оценкой [14]:

$$\frac{\pi_0(C;p)}{\pi_1(C;p)} \ge \frac{1+\Delta^{n-k+1}}{1-\Delta^{n-k+1}}. \qquad (23)$$

На основании (23) справедливы соотношения

$$\pi_0(C;p) - \pi_1(C;p) \ge \pi_0(C;p)\left(1 - \frac{1-\Delta^{n-k+1}}{1+\Delta^{n-k+1}}\right) = 2\pi_0(C;p)\frac{\Delta^{n-k+1}}{1+\Delta^{n-k+1}},$$

из которых в силу неравенства $\pi_0(C;p) \ge (1-p)^n$, вытекающего из формулы (18), следует оценка (16).

Убедимся, наконец, в справедливости неравенства (17). Зафиксируем элемент $s \in V_k$ такой, что $\pi_1(C;p) = \pi(C_s;p)$, и вектор $a \in C_s$. Обозначим

$$G = C^{\perp},\ G_0 = \{u \in G : ua = 0\},\ G_1 = \{u \in G : ua = 1\}.$$

На основании формулы (3) и неравенства между средним арифметическим и средним геометрическим справедливы соотношения

$$\pi_0(C;p) - \pi_1(C;p) = 2^{-k} \sum_{u\in G} \Delta^{\|u\|} - 2^{-k} \sum_{u\in G} (-1)^{au} \Delta^{\|u\|} =$$

$$= 2^{-(k-1)} \sum_{u\in G_1} \Delta^{\|u\|} \ge \Delta^{\,2^{-(k-1)} \sum_{u\in G_1} \|u\|}.$$

Следовательно, для обоснования оценки (17) достаточно показать, что при $d \ge 3$ выполняется следующее неравенство:

$$2^{-(k-1)} \sum_{u\in G_1} \| u \| \le \frac{n+1}{2}. \qquad (24)$$

Для любого $H \in \{G, G_0, G_1\}$ обозначим $s_i(H) = |\{u = (u_1,...,u_n) \in$ $\in H : u_i = 1\}|$, $i = \overline{1,n}$. Заметим, что

$$2^{-(k-1)} \sum_{x \in G_1} \| u \| = 2^{-(k-1)} \sum_{i=1}^{n} s_i(G_1). \qquad (25)$$

При этом, поскольку G и G_0 являются линейными кодами размерности k и $k-1$ соответственно, а G_1 — смежным классом кода G_0, то

$$s_i(G) \in \{0, 2^{k-1}\},\ s_i(G_0) \in \{0, 2^{k-2}\},\ s_i(G_1) \in \{0, 2^{k-2}, 2^{k-1}\},\ i = \overline{1,n}. \quad (26)$$

Предположим, что существует два различных значения $i, j \in \{1, 2, \dots, n\}$ таких, что $s_i(G_1) = s_j(G_1) = 2^{k-1}$. Тогда $s_i(G_0) =$ $= s_j(G_0) = 0$, согласно первым двум соотношениям (26). Следовательно, для любого слова $u = (u_1,...,u_n) \in G$ выполняется равенство $u_i = u_j$. Но в таком случае дуальное расстояние кода G (равное минимальному расстоянию d кода $C = G^{\perp}$) не превосходит 2, что противоречит условию утверждения.

Итак, существует не более одного значения $i \in \{1, 2, ..., n\}$, для которого $s_i(G_1) = 2^{k-1}$. Для остальных же значений $j \neq i$ в силу третьего соотношения (26) $s_j(G_1) \le 2^{k-2}$. Отсюда следует, что $2^{-(k-1)} \sum_{i=1}^{n} s_i(G) \le$ $\le 2^{-(k-1)}(2^{k-1} + 2^{k-2}(n-1)) = \frac{n+1}{2}$, из чего следует, что на основании формулы (25) справедливо неравенство (24), что и требовалось доказать.

Достижимость оценки (17) для $(n, n-k)$-кода Хэмминга C, $n = 2^k - 1$, вытекает из следующих равенств [3]:

$$\pi_0(C; p) = 2^{-k}(1 + (2^k - 1)\Delta^{2^{k-1}}),\ \pi_1(C; p) = 2^{-k}(1 - \Delta^{2^{k-1}}).$$

Утверждение доказано.

ЧИСЛЕННЫЕ ОЦЕНКИ ХАРАКТЕРИСТИК ЭФФЕКТИВНОСТИ СИСТЕМ ПЕРЕДАЧИ ИНФОРМАЦИИ ПО КАНАЛУ СВЯЗИ С ОТВОДОМ

Для сравнения полученных оценок были проведены численные расчеты значений в правых частях неравенств (12)–(14), (16), (17). Расчеты проводились для различных линейных кодов C, имеющих длину от нескольких десятков до нескольких сотен битов.

В качестве типового примера, иллюстрирующего полученные результаты, приведем оценки параметров $-\log_2(\pi_0(C; p_1) - \pi_1(C; p_1))$ и $-\log_2 \pi_0(C; p_2)$, рассчитанные для двух линейных кодов $C = G^{\perp}$ (табл. 1).

В табл. 1 после символа G указаны значения параметров n, k и d', равных соответственно длине, размерности и минимальному расстоянию кода G; символ «–» показывает, что соответствующая верхняя граница параметра $\pi_0(C; p_2)$ является тривиальной, то есть превосходит число 1.

Таблица 1. Оценки вероятности правильного восстановления сообщений в основном и отводном каналах

Код $G(63,45,7)$				
p_1	10^{-2}	10^{-4}		10^{-8}
Неравенство (16)	1,217	0,012		$1{,}2 \cdot 10^{-6}$
Неравенство (17)	0,933	0,009		$0{,}9 \cdot 10^{-6}$
p_2	0,1	0,2	0,3	0,4
Неравенство (12)	2,253	5,159	9,253	16,253
Неравенство (13)	5,000	11,250	19,286	30,000
Неравенство (14)	–	–	–	–
Код $G(256,27,106)$				
p_1	10^{-2}	10^{-4}		10^{-8}
Неравенство (16)	9,429	0,071		$0{,}7 \cdot 10^{-5}$
Неравенство (17)	3,745	0,037		$0{,}4 \cdot 10^{-5}$
p_2	0,1	0,2	0,3	0,4
Неравенство (12)	26,990	27,000	27,000	27,000
Неравенство (13)	3,000	6,750	11,571	18,000
Неравенство (14)	–	–	27,000	27,000

Как видно из табл. 1, неравенство (17) в обоих случаях доставляет более точное приближение параметра $\pi_0(C; p_1) - \pi_1(C; p_1)$ по сравнению с формулой (16). Для первого из указанных кодов (имеющего относительно большую скорость передачи $k/n = 45/63$) более точную аппроксимацию параметра $\pi_0(C; p_2)$ обеспечивает оценка (13), а для второго (имеющего относительно малую скорость $k/n = 27/256$) — оценка (12). При этом во втором случае значения $\pi_0(C; p_2)$ быстро приближаются к экстремальному значению 2^{-k} с ростом p_2 (например, при $p_2 = 0{,}1$ значение параметра $\pi_0(C; p_2)$ заключено в пределах от 2^{-27} до $2^{-26{,}990}$). Аналогичное поведение верхних границ (12)–(14) наблюдается для ряда других линейных кодов C, имеющих достаточно большие длину и дуальное расстояние.

В табл. 2 приведены численные значения параметров, характеризующих эффективность систем со случайным кодированием кодами $C_i = G_i^{\perp}$, $i = \overline{1,7}$. Как и в табл. 1, тут после символа G_i указаны значения параметров n, k и d', равных соответственно длине, размерности и минимальному расстоянию кода G_i, $i = \overline{1,7}$.

Таблица 2. Оценки эффективности систем передачи информации по каналу связи с отводом

Код $G(63,45,7)$												
p_1	10^{-2}				10^{-4}				10^{-8}			
t	245				68				67			
p_2	0,1	0,2	0,3	0,4	0,1	0,2	0,3	0,4	0,1	0,2	0,3	0,4
$\hat{\lambda}_2(t,p_2)$	0,0006	3,39	11,35	22,06	0,18	5,18	13,20	23,91	0,18	5,20	13,22	23,93
Код $G_2(63,51,5)$												
p_1	10^{-2}				10^{-4}				10^{-8}			
t	275				77				76			
p_2	0,1	0,2	0,3	0,4	0,1	0,2	0,3	0,4	0,1	0,2	0,3	0,4
$\hat{\lambda}_2(t,p_2)$	0,006	4,67	13,75	25,90	0,35	6,49	15,59	27,73	0,36	6,51	15,61	27,75
Код $G_3(256,203,84)$												
p_1	10^{-2}				10^{-4}				10^{-8}			
t	51440				302				287			
p_2	0,1	0,2	0,3	0,4	0,1	0,2	0,3	0,4	0,1	0,2	0,3	0,4
$\hat{\lambda}_2(t,p_2)$	11,39	46,25	95,39	179,39	18,80	53,67	102,80	186,80	18,88	53,74	102,88	186,87
Код $G_4(256,229,106)$												
p_1	10^{-2}				10^{-4}				10^{-8}			
t	57923				340				323			
p_2	0,1	0,2	0,3	0,4	0,1	0,2	0,3	0,4	0,1	0,2	0,3	0,4
$\hat{\lambda}_2(t,p_2)$	18,30	62,30	124,30	213,18	25,71	69,71	131,71	220,59	25,79	69,78	131,79	220,66
Код $G_5(255,247,3)$												
p_1	10^{-2}				10^{-4}				10^{-8}			
t	61162				366				348			
p_2	0,1	0,2	0,3	0,4	0,1	0,2	0,3	0,4	0,1	0,2	0,3	0,4
$\hat{\lambda}_2(t,p_2)$	11,54	45,85	89,96	148,77	18,93	53,23	97,34	156,15	19,00	53,31	97,41	156,22
Код $G_6(256,53,84)$												
p_1	10^{-2}				10^{-4}				10^{-8}			
t	14043				83				79			
p_2	0,1	0,2	0,3	0,4	0,1	0,2	0,3	0,4	0,1	0,2	0,3	0,4
$\hat{\lambda}_2(t,p_2)$	13,26	39,22	39,22	39,22	20,67	46,62	46,62	46,62	20,73	46,70	46,70	46,70
Код $G_7(256,27,106)$												
p_1	10^{-2}				10^{-4}				10^{-8}			
t	7560				45				43			
p_2	0,1	0,2	0,3	0,4	0,1	0,2	0,3	0,4	0,1	0,2	0,3	0,4
$\hat{\lambda}_2(t,p_2)$	14,11	14,12	14,12	14,12	21,50	21,51	21,51	21,51	21,56	21,57	21,57	21,57

При этом G_1 и G_2 являются кодами Боуза-Чоудхури-Хоквингема, а G_5 — кодом Хэмминга [12]. Параметры остальных линейных кодов взяты из таблиц, приведенных в [17] (отметим, что G_1 и G_7 совпадают с кодами, указанными в табл. 1). Символы p_1 и p_2 в табл. 2 обозначают вероятности ошибок в основном и в отводном каналах связи соответственно, а параметры $t = t(p_1)$ и $\hat{\lambda}_2(t, p_2)$ определяются следующим образом.

Обозначим $\mu_1(C; p_1)$ наибольшее из двух значений в правых частях неравенств (16) и (17) соответственно при $\Delta = 1 - 2p_1$; $\mu_2(C; p_2)$ — наименьшее из трех значений в правых частях неравенств (12), (13), (14) соответственно при $p = p_2$. Тогда t есть наименьшее натуральное число, удовлетворяющее условию

$$1 - 2^k \exp\left\{-\frac{t}{2}\mu_1(C; p_1)^2\right\} \geq 0{,}9, \tag{27}$$

а значение $\hat{\lambda}_2(t, p_2)$ определяется по формуле

$$\hat{\lambda}_2(t, p_2) = -\log_2(1 - (1 - \mu_2(C; p_2))^t), \tag{28}$$

где $C = G_i^{\perp}$, $i = \overline{1,7}$. Отметим, что на основании неравенств (4) и (27) вероятность правильного восстановления сообщения S законным получателем рассматриваемой системы передачи информации по каналу связи с отводом не меньше $0{,}9$. При этом, согласно формулам (5) и (28), вероятность правильного восстановления этого сообщения противником не превосходит $2^{-\hat{\lambda}_2(t, p_2)}$.

ВЫВОДЫ

В целом, полученные результаты позволяют сделать вывод о том, что при заметном отличии между вероятностями ошибок в основном и отводном каналах можно обеспечить достаточно надежный прием сообщений законным получателем при высокой практической стойкости их защиты в отводном канале, используя сравнительно умеренное число передач t. Так, в системе со случайным кодированием кодом $C_4 = G_4^{\perp}$ и вероятностями ошибок $p_1 = 0{,}01$, $p_2 = 0{,}3$ для передачи сообщения S длины 229 бит достаточно сформировать случайную последовательность $X_1, ..., X_t$, состоящую из $t = 57923$ слов, каждое из которых имеет длину 256 битов. Законный получатель, используя алгоритм 1, сможет восстановить S с вероятностью не менее $0{,}9$, в то время как противник, применяющий более надежный алгоритм 2, сумеет восстановить S с вероятностью не более чем $2^{-124{,}3}$ (при этом вероятность угадывания сообщения S равна 2^{-229}).

Уменьшить значения параметра t удается лишь за счет снижения скорости передачи информации. Например, в системе со случайным кодированием кодом $C_6 = G_6^{\perp}$ при тех же значениях p_1 и p_2 для передачи сообщения S длины 53 бита достаточно положить $t = 14043$. При этом законный

получатель восстановит переданное сообщение с вероятностью не менее $0{,}9$, в то время как противник — с вероятностью не более $2^{-39{,}22}$ (табл. 2). Для повышения скорости передачи информации (при заданных границах надежности ее приема в основном канале связи и стойкости защиты — в отводном) следует, по-видимому, использовать отличные от рассмотренного выше способы случайного кодирования.

ЛИТЕРАТУРА

1. *Wyner A.D.* The wire-tap channel // Bell System Technical Journal. — 1975. — **54**. — № 8. — P. 1355–1388.
2. *Csiszar I.*, *Korner J.* Broadcast channels with confidential messages // IEEE Transactions on Information Theory. — 1978. — **24**, № 3. — P. 339–348.
3. *Коржик В.И.*, *Яковлев В.А.* Неасимптотические оценки кодового зашумления одного канала // Проблемы передачи информации. — 1981. — Т. 17. — Вып. 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. — Вып. 4. — С. 24–34.
5. *Яковлев В.А.* Границы для оценки неопределенности в системе передачи со случайным кодированием // Радиотехника. — 1996. — № 12. — С. 58–63.
6. *Иванов В.А.* О методе случайного кодирования // Дискретная математика. — 1999. — Т. 11. — Вып. 3. — С. 99–108.
7. *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.
8. *Иванов В.А.* Асимптотические характеристики критериев проверки гипотез по случайно преобразованной выборке // Тр. по дискретной математике: в 11 т. Т. 5. — М.: Физматлит, 2002. — С. 61–72.
9. *Иванов В.А.* Статистические методы оценки эффективности кодового зашумления // Тр. по дискретной математике: в 11 т. Т. 6. — М.: Физматлит, 2002. — С. 48–63.
10. *Алексейчук А.Н.*, *Гришаков С.В.* Нелинейное случайное кодирование в системах передачи информации по каналу связи с отводом // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. — 2004. — Вип. 8. — С. 133–140.
11. *Thangaraj A.*, *Dihidar S.*, *Calderbank A.R.*, *McLaughlin S.*, *Merolla J.-M.* Capacity achiving codes for the wire-tap channel with applications to quantum key distribution. — http://eprint.arXiv:cs.IT/0411003v1.
12. *Мак-Вильямс Ф.Дж.*, *Слоэн Н.Дж.А.* Теория кодов, исправляющих ошибки: пер. с англ. — М.: Связь, 1979. — 743 с.
13. *Ширяев А.Н.* Вероятность. — М.: Наука, 1989. — 638 с.
14. *Sullivan D.* A fundamental inequality between the probabilities of binary subgroups and cosets // IEEE Transactions on Information Theory. — 1967. — **13**, № 1. — P. 91–94.
15. *Kasami T.*, *Klove T.*, *Lin S.* Linear block codes for error detection // IEEE Transactions on Information Theory. — 1983. — **29**, № 1. — P. 131–136.
16. *Ashikhmin A., Gohen G., Krivelevich M., Litsyn S.* Bounds on distance distributions in codes of known size // IEEE Transactions on Information Theory. — 2005. — **51**, № 1. — P. 250–258.
17. *Влэдуц С.Г.*, *Ногин Д.Ю.*, *Цфасман М.А.* Алгеброгеометрические коды. Основные понятия. — М.: МЦНМО, 2003. — 504 с.

Поступила 09.10.2009