Математика и её приложения: ЖИМО. 2008. Выпуск 1 (5). С. 11 – 20.

УДК 519.72

Ю. В. Косолапов[1],

Оценка уровня понимания информации в канале с перехватом

Ключевые слова: канал с перехватом, метод Озарова – Вайнера, обобщенные веса.

Получена верхняя оценка зависимости уровня понимания перехватчика от уровня перехвата данных при комплексной защите информации в канале с перехватом одного типа. Рассмотрены особенности построения защитных кодов для канала с перехватом рассматриваемого типа.

We find the upper bound of understanding level for one type of wire-tap channel. Also we consider some aspects of constructing security factor codes.

1. Введение и постановка задачи

А. Д. Вайнером в [11] рассмотрена схема организации связи, в которой при определенных условиях гарантируется конфиденциальность передаваемой информации без использования секретных ключей шифрования. В этой схеме два легитимных пользователя соединены каналом передачи данных K_1 — главным каналом, а перехватчик считывает данные через канал K_2 — канал перехвата. Гарантией конфиденциальности информации, передаваемой по каналу K_1, является не наличие у легитимных пользователей общего секретного ключа, а то, что $Cap(K_1) > Cap(K_2)$, где $Cap(K)$ — емкость канала K, определяемая как наибольшее количество единиц информации, которое можно передать по этому каналу за единицу времени [6]. В этом случае говорят, что *защитная емкость* $Cap_s = Cap(K_1) - Cap(K_2)$ канала с перехватом положительна [9]. Основная идея метода обеспечения конфиденциальности передаваемой по каналу K_1 информации заключается в использовании помехоустойчивых кодов. Для произвольных каналов K_1 и K_2 вычисление защитной емкости является нерешенной к настоящему времени задачей [9]; изучены свойства лишь частных случаев такой схемы связи.

В работе [8] А. Д. Вайнером и Л. Ю. Озаровым рассмотрен случай схемы канала с перехватом, когда K_1 — канал без помех, а K_2 — канал со стираниями $BEC(\varepsilon)$, где ε — доля стираний. Метод защиты информации в такой системе связи основывается на построении факторного кода по некоторому базовому линейному коду. Впоследствии идея этого метода была применена в работе [9] для защиты информации в более общей схеме связи — в случае, когда главный канал K_1 является некоторым дискретным

[1] Южный Федеральный Университет; E-mail: itaim@mail.ru.

каналом без памяти DMC, вносящим помехи. Однако в [9] был исследован не общий метод защиты, а метод, основанный на использовании слабоплотных кодов, впервые рассмотренных в [7], и связь между свойствами базового кода и свойствами защитного факторного кода установлена только для слабоплотных кодов. Особое внимание в [9] уделено построению быстрого декодера защитного кода. В большинстве работ, посвященных построению защитных кодов и оценке их свойств, основное внимание отводится поиску условий, при которых гарантируется совершенная защита, то есть когда злоумышленник не получает из перехваченных данных никакой информации о переданном сообщении. Отметим, что модель канала с перехватом рассматривается при решении различных прикладных задач. В частности, в [3] рассматривается модель канала с перехватом в контексте защиты информации в многоканальных беспроводных системах связи с псевдослучайной перестройкой рабочей частоты.

В [1] введено понятие уровня понимания перехватчиком полученных данных. Следует отметить, что ненулевой уровень понимания перехватчика (т. е. в случае, когда перехватчик обладает некоторой информацией о передаваемых сообщениях) не всегда может свидетельствовать о наличии приемлемого способа раскрытия (взлома) системы защиты. В этом случае можно говорить, что полученная информация обладает малой ценностью [5]. В связи с этим представляется интересным изучение общей зависимости уровня понимания перехватчика от уровня перехвата данных. Мощные результаты в этом направлении были получены в [10] для схемы связи, рассмотренной в [8], в которой канал K_1 не вносит помех.

В настоящей работе исследуется способ защиты информации в канале с перехватом, когда в канале K_1 есть помехи. Получена верхняя оценка зависимости уровня понимания перехватчика от уровня перехвата при использовании факторных защитных кодов, построенных на основе произвольных базовых линейных кодов. В работе также рассмотрены некоторые особенности построения защитных кодов.

2. Необходимые сведения из теории кодирования

В настоящей работе рассматриваются линейные помехоустойчивые (n, k)-коды над полем F_2, где n — длина кода, k — его размерность. Для удобства введем следующее обозначение. Пусть $A_{k\times n}$ — матрица из k строк и n столбцов, $\gamma \subset \{1; \ldots; n\}$. Через A_γ будем обозначать матрицу, составленную из столбцов матрицы $A_{k\times n}$ с номерами из γ, записанных в естественном порядке. Приведем определение весовой иерархии кода из [10]. Пусть C — линейный (n, k)-код над полем F_2, C' — его подкод. Носителем C' называется множество

$$\chi(C') = \{i : \exists\ (x_1, \ldots, x_n) \in C',\ x_i \neq 0\},$$

а весом подкода C' называется мощность его носителя $wt(C') = |\chi(C')|$. Обозначим через $X_{C,i}$ множество всех подкодов размерности i кода C.

Число $d_i = \min\{wt(C') \,|\, C' \in X_{C,i}\}$ называется i-м обобщенным весом Хемминга кода C, а упорядоченное множество $GW_C = \{d_1; d_2; \ldots; d_k\}$ называется весовой иерархией кода C. Весовая иерархия дуального кода вычисляется по формуле

$$GW_{C^\perp} = \{1; \ldots; n\} \setminus \{n+1-d_1; \ldots; n+1-d_k\}.$$

Весовую иерархию кода C можно интерпретировать следующим образом. Пусть $G_{k\times n}$ — порождающая матрица кода C, $\mathbf{S}$ — множество невырожденных матриц над полем F_2 размерности $k \times k$, $\Gamma = \{S \cdot G_{k\times n} \,|\, S \in \mathbf{S}\}$. Пусть $\tau_c (\subset \{1; 2; \ldots; n\})$ — множество попарно различных номеров такое, что $d_i \le |\tau_c| < d_{i+1}$; $\tau = \{1; 2; \ldots; n\} \setminus \tau_c$, $|\tau| = |\mu|$. Тогда

$$\forall G\ (\in \Gamma),\ \forall \tau,\ |\tau| = \mu:\ \ \mathrm{rank}\,(G_\tau) \ge k - i.$$

При этом

$$\exists G\ (\in \Gamma),\ \exists \tau,\ |\tau| = \mu:\ \ \mathrm{rank}\,(G_\tau) = k - i. \tag{1}$$

3. Общая схема защиты информации в канале с перехватом

Рассмотрим способ защиты информации в канале с перехватом, впервые предложенный в [11]. Пусть C' — (n, l)-код, $G'_{l\times n}$ — его порождающая матрица, $H'_{(n-l)\times n}$ — проверочная матрица. Рассмотрим множество линейно независимых векторов множества $F_2^n \setminus C'$:

$$\{\overline{h}_1; \ldots; \overline{h}_{n-l}\}. \tag{2}$$

Зафиксируем в наборе (2) произвольные k векторов:

$$k \le (n - l). \tag{3}$$

Пусть $G^*_{k\times n}$ — матрица, составленная из этих векторов. Рассмотрим матрицу вида:

$$G_{(k+l)\times n} = \begin{pmatrix} G^*_{k\times n} \\ G'_{l\times n} \end{pmatrix}. \tag{4}$$

Матрица (4) является кодовой матрицей защитного $(n, k + l)$-кода C. Кодирование вектора $\overline{m}$ длины k выполняется по формуле:

$$(\overline{m}||\overline{v}) \cdot G_{(k+l)\times n} = \overline{c},$$

где $\overline{v}$ — случайный двоичный вектор длины l. В случае, когда главный канал без помех, декодирование принятого вектора осуществляется умножением его на проверочную матрицу кода C'. Если же в главном канале

имеются помехи, то эта схема декодирования не подходит. Один их способов борьбы с помехами в главном канале с использованием слабоплотных кодов рассмотрен в [9]. В настоящей работе для защиты информации в случае, когда главный канал вносит помехи, предлагается использовать схему защиты, рассмотренную [11] с тем уточнением, что в формуле (3) должно быть строгое неравенство $k < (n - l)$. В этом случае защитный $(n, k + l)$-код C является линейным помехоустойчиым кодом, и его можно использовать для борьбы с помехами в главном канале. Пусть $\overline{c}$ — кодовое слово кода C, $\overline{e}$ — вектор ошибок, который способен исправить код C. Так как главный канал вносит помехи, то приемник из канала получит вектор $\overline{c}' = \overline{c} + \overline{e}$. Декодирование осуществляется в два этапа. На первом этапе приемник с помощью известного алгоритма декодирования кода C декодирует принятый вектор $\overline{c}'$ в кодовое слово $\overline{c}$. На втором этапе вектор $\overline{c}^T$ умножается справа на проверочную матрицу базового кода C':

$$H'_{(n-l)\times n} \cdot \overline{c}^T = \overline{m}^T. \tag{5}$$

Действительно,

$$H'_{(n-l)\times n} \cdot \overline{c}^T = H'_{(n-l)\times n}(G^*_{k\times n})^T \overline{m}.$$

Так как $\mathrm{Im}(G^*_{k\times n}) \cap C' = \emptyset$, то для $\overline{m}_1 \neq \overline{m}_2$, $\overline{m}_1, \overline{m}_2 \in F_2^k$, выполняется неравенство $(G^*_{k\times n})^T \overline{m}_1 \neq (G^*_{k\times n})^T \overline{m}_2$. Следовательно,

$$\mathrm{rank}\,(H'_{(n-l)\times n}(G^*_{k\times n})^T) = k.$$

А значит, всегда можно подобрать такую проверочную матрицу базового кода C', которая при умножении на матрицу $(G^*_{k\times n})^T$ давала бы единичную. Будем полагать, что матрица $H'_{(n-l)\times n}$ обладает этим свойством.

Отметим, что не для любого линейного кода, построенного по предлагаемой выше схеме построения защитного кода существует алгоритм быстрого декодирования. Некоторые особенности практического построения защитных кодов рассмотрены в разделе 6.

4. Математическая модель канала

В [1] исследована математическая модель защищенного $EWT^{Inf}(\varepsilon)$-канала передачи информации, рассмотренного в [8]. В этой модели главный канал не вносит помех, а канал перехвата является каналом со стираниями. Приведем краткое описание математической модели этого канала. Пусть $A^{(k)}$, $B^{(k)}$ и $T^{(k)}$ — математические модели источника, приемника и перехватчика соответственно, которые в качестве алфавитов используют векторы длины k над полем F_2, C — двоичный (n, k)-код. Математическая модель описывается пятеркой

$$EWT^{Inf}(\varepsilon) = \left(A^{(k)},\ B^{(k)},\ T^{(k)},\ \Sigma_0^{(c)},\ \Sigma_{BEC(\varepsilon)}^{(c)}\right), \tag{6}$$

где $\Sigma_0^{(c)}$ — математическая модель главного канала передачи информации с входными и выходными словами длины k над полем F_2, а математическая модель $\Sigma_{BEC(\varepsilon)}^{(c)}$ описывает канал перехвата информации, ε — доля перехвата данных. Код C называется (λ, δ)-защитным [1], если выполняются следующие условия:

$$1)\ \frac{n-k}{n} \le \lambda; \quad 2)\ \delta(\varepsilon, C) \le \delta.$$

Функция $\delta(\varepsilon, C)$ называется уровнем понимания перехватчиком полученных данных и определяется следующим образом:

$$\delta(\varepsilon, C) = \max_{\Delta:|\Delta|\le\lceil n(1-\varepsilon)\rceil} \left\{ \frac{H(A^{(k)}) - H(A^{(k)}|T_\Delta^{(k)})}{k} \right\},$$

где $T_\Delta^{(k)}$ — математическая модель перехватчика информации, располагающего $\Delta \in [1, \ldots, n]$ перехваченными позициями кодового слова, а $H(A^{(k)}|T_\Delta^{(k)})$ — условная энтропия:

$$H(A^{(k)}|T_\Delta^{(k)}) = \sum_{\overline{s}' \in F_2^k} \sum_{\overline{s} \in F_2^k} p(\overline{s}) \cdot p_\Delta(\overline{s}|\overline{s}') \log_2(p_\Delta(\overline{s}|\overline{s}')).$$

В [1] показано, что факторный защитный $(n, k+l)$-код C, построенный по базовому $(n, l)-$коду C', является (λ, δ)-защитным, если $\lambda = \frac{n-k}{n}$ и

$$\delta = 1 + k^{-1} \sum_{\overline{s}' \in F_2^k} \sum_{\overline{s} \in F_2^k} \frac{p_{\lceil n(1-\varepsilon)\rceil}(\overline{s}|\overline{s}') \log_2(p_{\lceil n(1-\varepsilon)\rceil}(\overline{s}|\overline{s}'))}{2^k}. \qquad (7)$$

При этом переходные вероятности $p_{\lceil n(1-\varepsilon)\rceil}(\overline{s}|\overline{s}')$ канала $\Sigma_{BEC(\varepsilon)}^{(c)}$ при условии перехвата $\lceil n(1-\varepsilon)\rceil$ символов вычисляются по формуле:

$$p(\overline{s}|\overline{s}')_{\lceil n(1-\varepsilon)\rceil} = \sum_{\overline{x} \in \varphi(\overline{s})} \sum_{\overline{z} \in \{\Sigma_{BEC(\varepsilon)}^{(n)}(\overline{x})\}:\, d(\overline{z},\overline{x}) = \lfloor n \cdot \varepsilon \rfloor} \frac{2^{-l} \cdot \left(C_n^{\lceil n(1-\varepsilon)\rceil}\right)^{-1}}{|N(\overline{z}, C)|}, \qquad (8)$$

где $\varphi(\cdot)$ — многозначный кодер Озарова – Вайнера, $\Sigma_{BEC(\varepsilon)}^{(n)}$ — модель канала перехвата данных, входными символами которого являются двоичные слова длиной n (кодовые слова кода C), а выходными — слова длины n над алфавитом $F_2 \cup \{*\}$ (перехваченные кодовые слова); $\{\Sigma_{BEC(\varepsilon)}^{(n)}(\overline{x})\}$ — множество возможных векторов на выходе канала при условии, если на входе вектор $\overline{x}$; $d(\overline{z}, \overline{x})$ — Хэммингово расстояние; $N(\overline{z}, C)$ — список претендентов на информационное сообщение, полученный декодером перехватчика.

Рассмотрим более общую модель канала (6), когда главный канал вносит помехи. Пусть $\Sigma_{N(\Upsilon)}^{(n)}$ — математическая модель главного незащищенного канала, вносящего помехи по закону Υ, $D_{N(\Upsilon)}$ — декодер кода

C, исправляющий ошибки. Тогда математическая модель схемы связи с перехватом и помехами в главном канале описывается пятеркой

$$WT^{Inf}(\varepsilon, \Upsilon) = \left(A^{(k)},\ B^{(k)},\ T^{(k)},\ \Sigma^{(c)}_{N(\Upsilon)},\ \Sigma^{(c)}_{BEC(\varepsilon)}\right). \tag{9}$$

Важной характеристикой кода C при использовании его в качестве защитного в канале с моделью (9) является вероятность ошибочного декодирования P_e при использовании декодера $D_{N(\Upsilon)}$. Эта вероятность зависит от кода C, используемого декодера $D_{N(\Upsilon)}$ и от закона распределения помех Υ в главном канале. Поэтому можно считать, что $P_e = P_e(C, D_{N(\Upsilon)}, \Upsilon)$.

Будем говорить, что (n, k)-код C является (λ, δ, p)-защитным, если выполняются условия:

$$1)\ \frac{n-k}{n} \le \lambda;\quad 2)\ \delta(\varepsilon, C) \le \delta;\quad 3)\ P_e(C, D_{N(\Upsilon)}, \Upsilon) \le p.$$

Отметим, что вероятность ошибки декодирования не зависит от уровня перехвата, так как перехватчик пассивно считывает передаваемые данные. Нахождение вероятности ошибки декодирования для различных кодов является отдельной областью для исследования свойств кодов и соответствующих декодеров. Интересные результаты в этом направлении получены, например, в [2], где, в частности, с помощью имитационного моделирования исследованы декодеры ряда помехоустойчивых кодов и рассмотрены основные способы снижения вероятности ошибки декодирования. Далее будем полагать, что для кода C при заданном законе распределения помех известна вероятность ошибки декодирования $P_e(C, D_{N(\Upsilon)}, \Upsilon)$.

5. Верхняя оценка зависимости уровня понимания от уровня перехвата

Пусть C — защитный $(n, k+l)$-код, построенный по описанной в третьем разделе схеме, $\overline{c}$ — кодовое слово, соответствующее сообщению $\overline{m}$. Предположим, что перехватчик в ходе подслушивания получил вектор $\overline{z}$, состоящий из перехваченных и неперехваченных символов вектора $\overline{c}$, τ — множество неперехваченных позиций, $\tau^c = \{1; 2; \ldots; n\} \setminus \tau$, $|\tau| = \mu$. Перепишем уравнение (5) в виде: $H'_\tau \cdot \overline{z}^T_\tau + H'_{\tau^c} \cdot \overline{z}^T_{\tau^c} = \overline{m}^T$. Перехватчику необходимо восстановить $\overline{m}^T$. Так как вектор $\overline{m}_{\tau^c} = H'_{\tau^c} \cdot \overline{z}^T_{\tau^c}$ известен, то перехватчику необходимо перебрать все *допустимые* векторы

$$\overline{m}_\tau = H'_\tau \cdot \overline{z}^T_\tau. \tag{10}$$

Следующая лемма позволяет оценить мощность списка $N(\overline{z}, C)$.

Лемма. *Пусть C — факторный защитный $(n, k+l)$-код, построенный по базовому (n, l)-коду C', τ — множество неперехваченных позиций кодового вектора $\overline{c}$, $\tau^c = \{1; 2; \ldots; n\} \setminus \tau$, $|\tau| = \mu$. Тогда*

$$N(\overline{z}, C) \ge \min\{2^{\pi_1 + \pi_2 - \mu}, 2^k\},$$

где $\pi_1 = \operatorname{rank}(H'_\tau)$, $\pi_2 = \operatorname{rank}(G_\tau)$.

Доказательство. Так как матрица H'_τ имеет размерность $(n-l)\times\mu$ и ее ранг равен π_1, то H'_τ может быть рассмотрена как проверочная матрица некоторого кода размерности $(\mu-\pi_1)$ и длины μ. Следовательно, пространство всех векторов длины μ можно разбить на $2^\mu/2^{\mu-\pi_1}=2^{\pi_1}$ классов эквивалентности, где каждый класс соответствует некоторому вектору-синдрому длины π_1, т. е. $N(\overline{z},C)=2^{\pi_1}$. Но так как в схеме защитного кодирования, рассмотренной выше, вектор $\overline{z}^T_\tau$ является частью кодового вектора кода C, то мощность списка $N(\overline{z},C)$ также зависит и от мощности множества $N(\overline{z}^T_\tau)$ всех допустимых векторов $\overline{z}^T_\tau$. Очевидно, что $|N(\overline{z}^T_\tau)|=2^{\pi_2}$. Поэтому множество $N(\overline{z}^T_\tau)$ может распасться, как минимум, на $2^{\pi_2}/2^{\mu-\pi_1}=2^{\pi_2-\mu+\pi_1}$ подмножеств, соответствующих различным векторам-синдромам. Следовательно,

$$|N(\overline{z},C)|\geq 2^{\pi_1+\pi_2-\mu}. \tag{11}$$

Так как уровень мощности списка $N(\overline{z},C)$ не может быть больше 2^k, то формулу (11) можно переписать в виде

$$|N(\overline{z},C)|\geq \min\{2^{\pi_1+\pi_2-\mu},2^k\}. \tag{12}$$

■

В лемме рассмотрен случай, когда мощность списка претендентов оценивается исходя из того, что известны позиции перехвата. Наиболее интересным в задаче защиты от перехвата является случай, когда известно только количество перехватываемых символов. Введем следующее обозначение:

$$N_\mu(C)=\min_{\overline{z}:|\tau|=\mu}\{|N(\overline{z},C)|\}.$$

Заметим, что $N_\mu(C)\leq 2^k$. Покажем, как, используя весовые иерархии кодов C и $C'^\perp$, можно оценить величину $N_\mu(C)$ снизу. Введем обозначения:

$$GW_{C'^\perp}=\{d_1(C'^\perp);\, d_2(C'^\perp);\,\ldots;\, d_l(C'^\perp)\},$$

$$GW_C=\{d_1(C);\, d_2(C);\,\ldots;\, d_{n-(k+l)}(C)\}.$$

Теорема 1. *Рассмотрим факторный защитный $(n,k+l)$-код C и базовый (n,l)-код C'. Пусть $G_{(k+l)\times n}$ — порождающая матрица кода C, $H'_{(n-l)\times n}$ — проверочная матрица кода C', $n-\mu$ — число перехватываемых позиций, а r_1 и r_2 — такие числа, что*

$$d_{r_1}(C'^\perp)\leq n-\mu<d_{r_1+1}(C'^\perp), \tag{13}$$

$$d_{r_2}(C)\leq n-\mu<d_{r_2+1}(C). \tag{14}$$

Тогда

$$N_\mu(C)\geq\min\{2^{r_1+r_2-\mu},2^k\}. \tag{15}$$

Доказательство. Введем обозначения $t_1 = \min_{|\tau_1|=\mu}\{\operatorname{rank}(H'_{\tau_1})\}$ и $t_2 = \min_{|\tau_2|=\mu}\{\operatorname{rank}(G_{\tau_2})\}$. Тогда из леммы и определения $N_\mu(C)$ следует, что

$$N_\mu(C) \geq \min\{2^{t_1+t_2-\mu}, 2^k\}.$$

Рассмотрим выражение $t_1 = \min_{|\tau_1|=\mu}\{\operatorname{rank}(H'_{\tau_1})\}$. Из (1) следует, что $t_1 = k - r_1$, где r_1 определяется из двойного неравенства (13). Аналогично с помощью (14) оценивается величина t_2. Отсюда получаем (15). ■

Теорема 2. *Рассмотрим факторный защитный $(n, k+l)$-код C и базовый (n,l)-код C'. Пусть $n-\mu$ — число перехватываемых позиций,*

$$N_\mu(C)_{inf} = \min\{2^{r_1+r_2-\mu}, 2^k\},$$

$$\delta = 1 - k^{-1}\log_2(N_\mu(C)_{inf}),$$

$$P_e(C, \Upsilon, D_{N(\Upsilon)}) \leq p.$$

Тогда код C является $(\frac{n-k}{n}, \delta, p)$-защитным.

Доказательство. Выполнение ограничений для избыточности и вероятности ошибочного декодирования следует из определения защитного кода и условия теоремы. Покажем, что $\delta(\varepsilon, C) \leq \delta$. Подставив $N_\mu(C)_{inf}$ в (8) вместо $N(\overline{z}, C)$, получим переходные вероятности в канале перехвата информации:

$$p(\overline{s}|\overline{s}')_{n-\mu} = (N_\mu(C)_{inf})^{-1}.$$

Подставив значение переходной вероятности в формулу (7), получим максимально возможный уровень понимания при перехвате $n-\mu$ символов:

$$\delta = 1 + k^{-1}\sum_{\overline{s}'\in F_2^k}\sum_{\overline{s}\in F_2^k}\frac{(N_\mu(C)_{inf})^{-1}\log_2(N_\mu(C)_{inf})^{-1}}{2^k}.$$

Учитывая то, что все сообщения $\overline{s}$ и $\overline{s}'$ равновероятны, а так же то, что вероятности $p(\overline{s}|\overline{s}')_{n-\mu}$ отличны от нуля только для $N_\mu(C)_{inf}$ векторов $\overline{s}'$ при каждом $\overline{s}$, получим $\delta = 1 - k^{-1}\log_2(N_\mu(C)_{inf})$. Таким образом, защитный код C является $(\frac{n-k}{n}, \delta, p)$-защитным. ■

6. Особенности построения защитных кодов

Задача построения (λ, δ, ρ)-защитного факторного кода преследует две цели — защита от помех в главном канале и защита от несанкционированного доступа в канале перехвата. Рассмотрим некоторые способы построения защитных кодов. Первый способ заключается в непосредственном применении техники, описанной в третьем разделе, где защитный код C строится по базовому коду C'. Однако код C, построенный этим способом,

не всегда может быть применен на практике, так как для него в общем случае неизвестны алгоритм быстрого декодирования и весовая иерархия. Для устранения этих недостатков первого способа можно, например, оценить весовую иерархию защитного кода экспериментально, а для возможности быстрого декодирования можно воспользоваться различными способами комбинирования кодов. Покажем, например, как, используя технику комбинирования кодов можно построить защитный код по первому способу. Рассмотрим конструкцию $|u|u+v|$, которая используется для построения кода по известным двум кодам [4]. Пусть C_1 и C_2 — линейные коды длины $n = n_1 = n_2$, размерности k_1 и k_2 и с минимальным кодовым расстоянием d_1 и d_2 соответственно; G_1 и G_2 — соответствующие порождающие матрицы. Пусть для кода C_2 известен быстрый декодер D_2, а для кода C_1 известна весовая иерархия. Рассмотрим порождающую матрицу кода $C = |C_1|C_1 + C_2|$:

$$G = \begin{pmatrix} G_1 & G_1 \\ 0 & G_2 \end{pmatrix}. \tag{16}$$

Код C имеет параметры $(2n, k_1 + k_2, d)$, где минимальное кодовое расстояние этого кода равно $d = \min\{2d_1, d_2\}$ [4]. Если в задаче построения защитного кода в качестве базового кода выбрать код с порождающей матрицей

$$G_{1,1} = (G_1||G_1), \tag{17}$$

то для оценки уровня понимания достаточно экспериментально оценить только весовую иерархию кода C, так как для кода с порождающей матрицей (17) весовая иерархия легко вычисляется по весовой иерархии кода C_1. А для восстановления информационного сообщения можно воспользоваться следующей теоремой.

Теорема 3. *Пусть C — код с порождающей матрицей* (16), $\overline{c} \in C$, $\overline{x} = \overline{c} + \overline{e}$, $wt(\overline{e}) \le \lfloor (d-1)/2 \rfloor$, $\overline{x} = (\overline{x}_1||\overline{x}_2)$, $\overline{c} = (\overline{c}_1||\overline{c}_1 + \overline{c}_2)$. *Тогда*

$$\overline{c}_2 = D_2(\overline{x}_1 + \overline{x}_2).$$

Доказательство. Так как вектор ошибок можно представить в виде $\overline{e} = (\overline{e}_1||\overline{e}_2)$, $|\overline{e}_1| = |\overline{e}_2| = n$, то справедливы равенства: $\overline{x}_1 = \overline{c}_1 + \overline{e}_1$ и $\overline{x}_2 = \overline{c}_1 + \overline{c}_2 + \overline{e}_2$. Рассмотрим вектор $\overline{x}_3 = \overline{x}_1 + \overline{x}_2 = \overline{c}_2 + \overline{e}_1 + \overline{e}_2$. Так как $wt(\overline{e}_1 + \overline{e}_2) \le wt(\overline{e}_1) + wt(\overline{e}_2) = wt(\overline{e}) \le \lfloor (d_2 - 1)/2 \rfloor$, то $\overline{c}_2 = D_2(\overline{x}_3)$. ■

Второй способ заключается в том, что в качестве защитного кода выбирается помехоустойчивый код C с *известным* быстрым алгоритмом декодирования. В качестве базового выбирается код C' с порождающей матрицей, составленной из части порождающей матрицы кода C. Недостатком этого способа является то, что для базового кода неизвестна весовая иерархия. Как и в первом случае, ее можно оценить экспериментально. В

частных случаях, когда для факторного и базового кода известна весовая иерархия, можно получить теоретическую оценку уровня понимания. Например, если в качестве защитного кода выбрать код Рида – Маллера m-го порядка, а в качестве его подкода (базового кода) выбрать код $(m-1)$-го порядка, то оценивать экспериментально весовые иерархии нет необходимости, так как для этих кодов известны теоретические оценки [10].

7. Заключение

При практической реализации схемы Озарова – Вайнера защиты информации в канале с перехватом возникает проблема исследования зависимости уровня понимания перехватчика от уровня перехвата данных. В настоящей работе в случае, когда главный канал вносит помехи, а канал перехвата есть канал со стираниями, получена верхняя оценка такой зависимости. Рассмотрены особенности построения удобных для практической реализации защитных кодов.

Список использованной литературы

1. *Деундяк В. М., Косолапов Ю. В.* Математическая модель канала с перехватом второго типа // Изв. вузов. Северо-Кавказский регион. Естественные науки. – 2008. – № 3. – С. 3–8.
2. *Деундяк В. М., Могилевская Н. С.* Методы оценки применимости помехоустойчивого кодирования в каналах связи: Учеб. пособие. – Ростов н/Д: Издательский центр ДГТУ, 2007. – 86 с.
3. *Косолапов Ю. В.* О применении схемы Озарова – Вайнера для защиты информации в беспроводных многоканальных системах передачи данных // Информационное противодействие угрозам терроризма: Научно-практический журнал. – 2007. – № 10. – С. 112–120.
4. *Морелос-Сарагоса Р.* Искусство помехоустойчивого кодирования. Методы алгоритмы, применение. – М.: Техносфера, 2006. – 320 с.
5. *Шанкин Г. П.* Ценность информации. Вопросы теории и приложений. – М.: Филоматис, 2004. – 128 с.
6. *Яглом А. М., Яглом И. М.* Вероятность и информация. – М.: Наука, 1973. – 512 с.
7. *Gallager R. G.* Low-density parity-check codes. – Cambridge: MA–MIT Press, 1963. – 90 p.
8. *Ozarow L. Y., Wyner A. D.* Wire-tap channel II // AT&T Bell labs Tech. J. – 1984. – Vol. 3. – P. 2135–2157.
9. *Thangaraj A., Dihidar S., Calderbank A. R., McLaughlin S., Merolla J.* Applications of LDPC codes to wiretap channel // arXiv:cs/0411003v3 [cs.IT]. – 29 Jan. 2007. – 30 p.
10. *Wei V. K.* Generalized Hamming weights for linear codes // IEEE Transactions on information theory. – 1991. – Vol. 37. – № 5.– P. 1412–1418.
11. *Wyner A. D.* Wire-tap channel // Bell System Technical Journal. – 1975. – Vol. 54. – № 8. – P. 1355–1387.

Поступила в редакцию 17.11.2008.