УДК 517.19

В.М. Деундяк, Ю.В. Косолапов

ОБ ОДНОМ МЕТОДЕ СНЯТИЯ НЕОПРЕДЕЛЕННОСТИ В КАНАЛЕ С ПОМЕХАМИ В СЛУЧАЕ ПРИМЕНЕНИЯ КОДОВОГО ЗАШУМЛЕНИЯ

Анализируется метод снятия неопределенности при частичном перехвате данных в канале с помехами, основанный на l-кратном частичном перехвате кодовых слов, соответствующих одному информационному слову. Предполагается, что передаваемые в канал данные защищаются с помощью метода кодового зашумления, основанного на использовании пары линейных кодов $(\tilde{C}, C)$*, где* $C \subset \tilde{C}$*. В качестве меры стойкости выбрана условная энтропия информационного слова после перехвата l частичных кодовых слов. Получено выражение для вычисления меры стойкости кодового зашумления после l перехватов в канале с помехами. В частном случае для кодов Хэмминга и некоторых кодов Рида-Маллера удалось вычислить меру стойкости в зависимости от числа* μ *перехватываемых символов в каждом кодовом слове и количества l наблюдаемых кодовых слов, соответствующих одному информационному слову. В частности, получены минимально необходимые условия для l и* μ*, при выполнении которых за l перехватов полностью снимается неопределенность о закодированном информационном слове.*

Канал с помехами; частичное наблюдение; кодовое зашумление; многократный перехват.

V.M. Deundyak, Yu.V. Kosolapov

ONE METHOD OF REMOVING THE UNCERTAINTY IN THE CHANNEL WITH ERRORS IN THE CASE OF CODE NOISING

Analyzed method of removing uncertainty during partial interception of the data channel interference, based on l-multiplying the partial interception of codewords corresponding to the same information word. It is assumed that the transmitted data is protected in the channel using the code noising method based on the use of a pair of linear codes $(\tilde{C}, C)$ *where* $C \subset \tilde{C}$*. As a measure of resistance selected conditional entropy information word after a partial interception of l codewords. An expression for calculating measures resistance after interceptions channel interference protected code noising. In the particular case of Hamming codes, and some of the Reed-Muller code was possible to calculate a measure of resistance depending on the number* μ *of intercepted symbols in each codeword, and codewords observable quantity l, corresponding to one information word. In particular, we obtain the minimum necessary conditions for l and* μ *under which l for interceptions completely eliminated uncertainty about the information encoded word.*

A channel with errors; partial observation; code noising; multiple interception.

Введение и постановка задачи. В [1] рассмотрена модель перехвата, когда в легитимном бесшумном канале, также называемом главным каналом, наблюдатель по своему усмотрению выбирает для просмотра любые μ координат передаваемого вектора длины n над конечным полем F_q. Такая модель получила название канала с перехватом второго типа, так как ранее в 1975 в [2] была рассмотрена модель перехвата первого типа, в которой наблюдатель перехватывает сообщению полностью, но с помехами, позиции которых наблюдателю неизвестны. В [1] предполагается, что источник информационных слов является случайным и равновероятным, а в качестве показателя защищенности данных при заданном μ естественным образом рассматривается минимальная условная энтропия информационного слова после наблюдения части данных. В силу равновероятности источни-

ка условная энтропия равна логарифму мощности множества претендентов по основанию q при перехвате конкретных μ координат передаваемого вектора. В [1] доказано, что за счет уменьшения длины информационного слова и использования метода случайного кодирования, можно закодировать информационное слово длины k в кодовое слово длины $n(>k)$ так, что найдется такое неотрицательное натуральное μ_0, для которого при условии $\mu \le \mu_0$ множество претендентов на стороне наблюдателя будет совпадать с множеством всех возможных информационных слов длины k, и, таким образом, будет обеспечиваться совершенная защита. Предложенный в [1] метод случайного кодирования обычно реализуется на основе линейных кодов. Такая реализация в отечественной литературе получила название "метода кодового зашумления" [3]. При этом случайные коды, реализующие кодовое зашумление, называются факторными кодами, а линейные коды, на основе которых строится случайный код – базовыми кодами [4]. В случае, когда главный канал не имеет помех, значение μ_0 при использовании метода кодового зашумления полностью определяется свойствами базового кода [1, 5]. Заметим, что возможность обеспечить совершенную защиту при частичном наблюдении данных потенциально позволяет использовать метод кодового зашумления для защиты данных в распределенных системах хранения, где частичное наблюдение моделирует, например, несанкционированный доступ к некоторым серверам, на базе которых организуется распределенное хранилище. Некоторые аспекты построения защиты данных на основе кодового зашумления в распределенных системах рассмотрены в [6, 7].

Отметим, что в работах [1-6], посвященых исследованию модели из [1] и ее модификаций, не рассматривается вопрос о том, как наблюдатель может использовать ненулевую информацию об информационном слове в случае $\mu > \mu_0$, т.е. в случае, когда после перехвата μ координат в кодовом векторе длины n построенное множество претендентов на информационное слово будет меньше по мощности множества всех информационных слов длины k.

В настоящей работе предлагается использовать такую ненулевую информацию для снятия неопределенности в рамках многократного наблюдения. Именно, пусть информационное сообщение M состоит из N информационных слов длины k над полем F_q, а информационное слово $\mathbf{s}$ в сообщении M встречается в $l(\le N)$ разных местах. Пусть также перед передачей в канал сообщение M кодируется с помощью метода кодового зашумления, согласно которому каждое информационное слово длины k заменяется кодовым словом длины n. Если наблюдателю заранее известна структура сообщения M, то есть известно, в каких метах в сообщении содержится интересующее его и неизвестное ему информационное слово $\mathbf{s}$, то он может попытаться перехватить части соответсвующих кодовых слов, передаваемых по главному каналу. Сложность анализа для наблюдателя затрудняется тем, что информационное слово $\mathbf{s}$, в силу специфики кодового зашумления, в разных местах может быть закодировано в разные кодовые слова. Тогда для наблюдателя естественной стратегией представляется построение множества претендентов по каждому перехваченному частичному кодовому слову, а затем пересечение всех этих множеств для сокращения, если удастся, итогового множества претендентов. В [8] для бесшумного главного канала рассмотрен случай, когда $l = 2$, и показано, что для

случая $\mu > \mu_0$ можно провести атаку двукратного перехвата так, что итоговое множество претендентов будет меньше по мощности, чем множество претендентов после первого или второго перехвата в отдельности.

Отметим, что в рамках модели канала с перехватом первого типа вопрос оценки стойкости кодового зашумления к многократному перехвату исследован в [9], где оценивается минимально необходимый объем наблюдаемых данных в двоичном симметричном канале, по которому с заданными вероятностями ошибок первого и второго рода можно методом максимума правдоподобия проверить гипотезу о содержании закодированного случайным кодом сообщения. В [10] результат [9] конкретизирован для факторных кодов.

В настоящей работе рассматривается обобщение метода двукратного перехавата второго типа, рассмотренного в [8], и ставится задача оценки меры стойкости метода кодового зашумления к *l*-кратному частичному перехвату в канале с помехами.

1. Оценка неопределенности при l-кратном частичном перехвате. Пусть F_q – поле Галуа, где $q = p^r$, p – простое число, r – натуральное число; множество $\{1;2;...;n\}$, где $n \in \mathsf{N}$, будем обозначать $\underline{n}$. Пусть τ – произвольное подмножество множества $\underline{n}$, тогда вектор, составленный из значений координат вектора $\mathbf{x} \in \mathsf{F}_q^n$, номера которых принадлежат τ, будем обозначать $\mathbf{x}_\tau$; символом $M_{k\times n}$ будем обозначать матрицу, состоящую из k строк и n столбцов, а матрицу, составленную из столбцов матрицы $M_{k\times n}$, номера которых принадлежат множеству τ, будем обозначать M_τ. Для произвольных матриц $A_{k\times n_1}$ и $B_{k\times n_2}$ запись $(A_{k\times n_1} \mid B_{k\times n_2})$ будет обозначать дописывание матрицы $B_{k\times n_2}$ справа к матрице $A_{k\times n_1}$, а для векторов $\mathbf{a}$ и $\mathbf{b}$ аналогичная запись будет обозначать дописывание к вектору $\mathbf{a}$ вектора $\mathbf{b}$ справа. Для матриц $A_{k_1\times n_1}$ и $B_{k_2\times n_2}$ запись $A_{k_1\times n_1} \circ B_{k_2\times n_2}$ обозначет матрицу:

$$\begin{pmatrix} A_{1_{2\times n_1}} & O_{k_1\times n_2} \\ O_{k_2\times n_1} & B_{k_2\times n_2} \end{pmatrix},$$

где $O_{k\times n}$ – нулевая матрица размера $k\times n$. Рассмотрим линейный (n,k)-код $\tilde{C}(\subseteq \mathsf{F}_q^n)$ и $(n,k-k_1)$-код C, $C \subseteq \tilde{C}$. Пусть $\tilde{G}_{k\times n}$ – порождающая матрица $\tilde{C}$, $\tilde{H}_{(n-k)\times n}$ – проверочная матрица, $G_{k_1\times n}$ и $H_{(n-k_1)\times n}$ – соответственно порождающая и проверочная матрица для C. Так как $C \subseteq \tilde{C}$, то имеет место представление

$$\tilde{G}_{k\times n} = \begin{pmatrix} G_{k_1\times n} \\ G_{k_2\times n} \end{pmatrix},\ H_{(n-k_1)\times n} = \begin{pmatrix} \hat{H}_{k_2\times n} \\ \tilde{H}_{(n-k)\times n} \end{pmatrix}, \qquad (1)$$

где $k_2 = k - k_1$. В соответствии с [4] пару $(\tilde{C}, C)$ будем называть *факторным кодом*, а код C – *базовым кодом*. Отметим, что пара $(\tilde{C}, C)$ подбирается таким образом, чтобы, во-первых, код $\tilde{C}$ обеспечивал защиту от помех в главном канале,

а, во-вторых, чтобы за счет выбора кода C обеспечивалась защиты от наблюдателя, частично перехватывающего данные в главном канале. Предполагается, что частично перехваченные наблюдателем данные не содержат помех, тем самым наблюдатель ставится в наиболее выгодные для него условия.

Кодирование сообщения $\mathbf{s}(\in \mathsf{F}^{k_2})$ факторным кодом $(\tilde{C}, C)$ выполняется по правилу:

$$(\mathbf{v} \mid \mathbf{s})\tilde{G}_{k\times n} = c = \mathbf{v}G_{k_1\times n} + \mathbf{s}G_{k_2\times n}, \tag{2}$$

где $\mathbf{v}(\in \mathsf{F}^{k_1})$ – случайный и равновероятно выбранный вектор. Снятие зашумления с корректного кодового слова $\mathbf{c}$ выполняется по правилу: $\mathbf{s} = \mathbf{c}\hat{H}^T_{k_2\times n}$. Правило (2) задает разбиение: $\tilde{C}/C = \{C_{\mathbf{s}}\}_{\mathbf{s}\in \mathsf{F}^{k_2}}$, где $C_{\mathbf{s}} = \mathbf{s}G_{k_2\times n} + C$.

Пусть $\mathbf{S}^{k_2}$ – случайный вектор, моделирующий информационные сообщения, который принимает значения из $\mathsf{F}_{\mathrm{q}}^{k_2}$ случайно и равновероятно, $\mathbf{X}^n$ – случайный вектор, моделирующий кодовые словам кода $\tilde{C}$ и принимающий значения случайно и равновероятно, $\mathbf{Z}^{\mathrm{n}}_{\tau}$ – случайный вектор, моделирующий наблюдаемые значения, где $\tau(\subseteq \underline{n})$ – множество наблюдаемых координат. Неопределенность наблюдателя при перехвате координат из множества τ обозначим $\Delta_\tau(\tilde{C}, C)$ и будем считать, как и в [1], что $\Delta_\tau(\tilde{C}, C) = H(\mathbf{S}^{k_2} \mid \mathbf{Z}^n_\tau)$.

Лемма 1. *Пусть* $(\tilde{C}, C)$ *– факторный код,* $H_{n-k_1\times n}$ *— проверочная матрица вида* (1) *кода* C, $\tau(\subseteq \underline{n})$ *– подмножество наблюдаемых координат,* $\bar{\tau} = \underline{n} \setminus \tau$ *– подмножество ненаблюдаемых координат. Тогда*

$$\Delta_\tau(\tilde{C}, C) = rank(H_{\bar{\tau}}) - rank(\tilde{H}_{\bar{\tau}}). \tag{3}$$

Доказательство. Пусть $\mathbf{z}^{\mathrm{n}}_{\tau}$ – наблюдаемое значение в канале. Тогда

$$H(\mathbf{S}^{k_2} \mid \mathbf{z}^n_\tau) + H(\mathbf{X}^n_{\bar{\tau}} \mid \mathbf{S}^{k_2}, \mathbf{z}^n_\tau) = H(\mathbf{X}^n_{\bar{\tau}} \mid \mathbf{z}^n_\tau) + H(\mathbf{S}^{k_2} \mid \mathbf{X}^n_{\bar{\tau}}, \mathbf{z}^n_\tau).$$

Так как $H(\mathbf{S}^{k_2} \mid \mathbf{X}^n_{\bar{\tau}}, \mathbf{z}^n_\tau) = 0$, то

$$H(\mathbf{S}^{k_2} \mid \mathbf{z}^n_\tau) = H(\mathbf{X}^n_{\bar{\tau}} \mid \mathbf{z}^n_\tau) - H(\mathbf{X}^n_{\bar{\tau}} \mid \mathbf{S}^{k_2}, \mathbf{z}^n_\tau). \tag{4}$$

Несложно видеть, что $H(\mathbf{X}^n_{\bar{\tau}} \mid \mathbf{z}^n_\tau) = n - |\tau| - rank(\tilde{H}_{\bar{\tau}})$, а $H(\mathbf{X}^n_{\bar{\tau}} \mid \mathbf{S}^{k_2}, \mathbf{z}^n_\tau)$ определяется как размерность пространства решений системы уравнений:

$$\begin{pmatrix} \hat{H}_{\bar{\tau}} \\ \tilde{H}_{\bar{\tau}} \end{pmatrix} \mathbf{X}^{nT}_{\bar{\tau}} = \begin{bmatrix} \mathbf{S}^{k_2 T} - \hat{H}_\tau \mathbf{z}^{nT}_\tau \\ -\tilde{H}_\tau \mathbf{z}^{nT}_\tau \end{bmatrix}. \tag{5}$$

Поэтому $H(\mathbf{X}^n_{\bar{\tau}} \mid \mathbf{S}^{k_2}, \mathbf{z}^n_\tau) = n - |\tau| - rank(H_{\bar{\tau}})$ и из (4) $H(\mathbf{S}^{k_2} \mid \mathbf{z}^n_\tau) = rank(H_{\bar{\tau}}) - rank(\tilde{H}_{\bar{\tau}})$. Так как $H(\mathbf{S}^{k_2} \mid \mathbf{z}^n_\tau)$ не зависит от значений координат, то получаем (3). Лемма доказана.

Пусть наблюдатель имеет возможность из потока наблюдаемых кодовых слов выделить l таких кодовых слов $\mathbf{x}(1),...,\mathbf{x}(l)$, которые соответствуют одному информационному сообщению $\mathbf{s}$. Таким образом, $\mathbf{x}(1),...,\mathbf{x}(l) \in C_{\mathbf{s}}$, где сообщение $\mathbf{s}$ неизвестно наблюдателю. Пусть $\tau_i \subseteq \underline{n}$ – множества координат, значения которых наблюдает перехватчик в кодовых словах $\mathbf{x}(i)$, $i = 1,...,l$ $|\tau_i| = \mu_i$. Другими словами, наблюдателю доступны векторы $\mathbf{z}(i)_{\tau_i} = \mathbf{x}(i)_{\tau_i}$. Выборку $(\mathbf{z}(1)_{\tau_1},...,\mathbf{z}(l)_{\tau_l})$ назовем однородной. Введем для удобства обозначения для подмножеств ненаблюдаемых координат: $\bar{\tau}_i = \underline{n} \setminus \tau_i$, $i = 1,...,l$. По каждому из векторов в отдельности $\mathbf{x}(i)^T_{\tau_i}$ наблюдатель может составить списки претендентов $N(\mathbf{z}(i)^T_{\tau_i})(\subseteq \mathsf{F}_q^{k_2})$. Список претендентов, составленный одновременно по l известным векторам $\mathbf{z}(i)^T_{\tau_i}$, $i = 1,...,l$, будет равен $N(\mathbf{z}(1)^T_{\tau_1},...,\mathbf{z}(l)^T_{\tau_l}) = \bigcap_{i=1}^{l} N(\mathbf{z}(i)^T_{\tau_i})$. Обозначим неопределенность наблюдателя по l наблюдаемым векторам $\mathbf{Z}(i)^n_{\tau_i}$, $i = 1,...,l$ через $\Delta_{\tau_1,...,\tau_l}(\tilde{C}, C)$. Будем считать, что

$$\Delta_{\tau_1,...,\tau_l}(\tilde{C}, C) = H(\mathbf{S}^{k_2} \mid \mathbf{Z}(1)^n_{\tau_1},..., \mathbf{Z}(l)^n_{\tau_l}) = \log_q L_{\tau_1,...,\tau_l}. \quad (6)$$

Для случая, когда при всех $\mu_1 = ... = \mu_l = \mu$, т.е. когда в каждом из l перехватов наблюдатель просматривает фиксированное число μ координат в каждом кодовом слове, ведем определение:

$$\Delta^{(l)}_{\mu}(\tilde{C}, C) = \min_{\tau_i \subset \underline{n}, |\tau_i| = \mu,\, i \in \underline{l}} \{\Delta_{\tau_1,...,\tau_l}(\tilde{C}, C)\}. \quad (7)$$

Теорема 1. *Пусть* $(\tilde{C}, C)$ *– факторный код, проверочная матрица базового кода имеет вид из* (1), τ_1, τ_2 *– подмножества наблюдаемых координат при первом и втором перехвате кодовых слов, соответствующих одному информационному сообщению;* $\bar{\tau}_i = \underline{n} \setminus \tau_i$, $\Delta_i = rank(H_{\bar{\tau}_i})$, $\Delta_{\tau_1 \| \tau_2} = rank\left(H_{\bar{\tau}_1} \mid H_{\bar{\tau}_2}\right)$, $\tilde{\Delta}_i = rank(\tilde{H}_{\bar{\tau}_i})$, $i = 1,2$. *Тогда:*

$$\Delta_{\tau_1,\tau_2}(\tilde{C}, C) = \Delta_1 + \Delta_2 - (\tilde{\Delta}_1 + \tilde{\Delta}_2 + \Delta_{\tau_1 \| \tau_2} - \dim(\mathsf{L}_r(\tilde{H}_{\bar{\tau}_1} \circ \tilde{H}_{\bar{\tau}_2}) \cap \mathsf{L}_r(H_{\bar{\tau}_1} \mid H_{\bar{\tau}_2}))), \quad (8)$$

где $\mathsf{L}_{\mathrm{r}}(\mathrm{M})$ – линейная оболочка, натянутая на строки матрицы M.

Доказательство. Пусть наблюдателю доступны два вектора $\mathbf{z}(1)_{\tau_1} = \mathbf{x}(1)_{\tau_1}$ и $\mathbf{z}(2)_{\tau_2} = \mathbf{x}(2)_{\tau_2}$, где $\mathbf{x}(1), \mathbf{x}(2) \in C_{\mathbf{s}}$ ($C_{\mathbf{s}} \subset \tilde{C}$), $\mathbf{s}(\in \mathsf{F}_q^{k_2})$ – неизвестное наблюдателю информационное сообщение. Заметим, что

$$H(\mathbf{S}^{k_2} \mid \mathbf{z}(1)^n_{\tau_1}, \mathbf{z}(2)^n_{\tau_2}) + H(\mathbf{X}(1)^n_{\bar{\tau}_1}, \mathbf{X}(2)^n_{\bar{\tau}_2} \mid \mathbf{S}^{k_2}, \mathbf{z}(1)^n_{\tau_1}, \mathbf{z}(2)^n_{\tau_2}) =$$

$$= H(\mathbf{X}(1)^n_{\bar{\tau}_1}, \mathbf{X}(2)^n_{\bar{\tau}_2} \mid \mathbf{z}(1)^n_{\tau_1}, \mathbf{z}(2)^n_{\tau_2}) + H(\mathbf{S}^{k_2} \mid \mathbf{X}(1)^n_{\bar{\tau}_1}, \mathbf{X}(2)^n_{\bar{\tau}_2}, \mathbf{z}(1)^n_{\tau_1}, \mathbf{z}(2)^n_{\tau_2}).$$

Так как $H(\mathbf{S}^{k_2} \mid \mathbf{X}(1)^n_{\bar{\tau}_1}, \mathbf{X}(2)^n_{\bar{\tau}_2}, \mathbf{z}(1)^n_{\tau_1}, \mathbf{z}(2)^n_{\tau_2}) = 0$, то

$$H(\mathbf{S}^{k_2} \mid \mathbf{z}(1)^n_{\tau_1}, \mathbf{z}(2)^n_{\tau_2}) = \tag{9}$$

$$= H(\mathbf{X}(1)^n_{\bar{\tau}_1}, \mathbf{X}(2)^n_{\bar{\tau}_2} \mid \mathbf{z}(1)^n_{\tau_1}, \mathbf{z}(2)^n_{\tau_2}) - H(\mathbf{X}(1)^n_{\bar{\tau}_1}, \mathbf{X}(2)^n_{\bar{\tau}_2} \mid \mathbf{S}^{k_2}, \mathbf{z}(1)^n_{\tau_1}, \mathbf{z}(2)^n_{\tau_2}).$$

Учитывая то, что $\mathbf{z}(1)^n_{\tau_1}$ и $\mathbf{z}(2)^n_{\tau_2}$ – части кодовых слов $\mathbf{x}(1)$ и $\mathbf{x}(2)$ соответственно, принадлежащих коду $\tilde{C}$, и то, что $\mathbf{x}(1)$ и $\mathbf{x}(2)$ принадлежат одному смежному классу из фактор-множества $\tilde{C}$ ($\mathbf{x}(1) - \mathbf{x}(2) \in C$), то множество значений вектора неизвестных $(\mathbf{X}(1)^n_{\bar{\tau}_1}, \mathbf{X}(2)^n_{\bar{\tau}_2})$ равно количеству решений системы:

$$\begin{cases} \tilde{H}_{\bar{\tau}_1} \mathbf{X}(1)^{n\,T}_{\bar{\tau}_1} = -\tilde{H}_{\tau_1} \mathbf{z}(1)^{n\,T}_{\tau_1} \\ \tilde{H}_{\bar{\tau}_2} \mathbf{X}(2)^{n\,T}_{\bar{\tau}_2} = -\tilde{H}_{\tau_1} \mathbf{z}(2)^{n\,T}_{\tau_1} \\ H_{(n-k_1)\times n} \mathbf{X}(1)^{nT} - H_{(n-k_1)\times n} \mathbf{X}(2)^{nT} = \mathbf{0}. \end{cases} \tag{10}$$

Так как для $i = 1, 2$ верно $H_{(n-k_1)\times n} \mathbf{X}(i)^{nT} = H_{\bar{\tau}_i} \mathbf{X}(i)^{n\,T}_{\bar{\tau}_i} + H_{\tau_i} \mathbf{z}(i)^{n\,T}_{\tau_i}$, то (10) примет вид:

$$\begin{cases} \tilde{H}_{\bar{\tau}_1} \mathbf{X}(1)^{n\,T}_{\bar{\tau}_1} = -\tilde{H}_{\tau_1} \mathbf{z}(1)^{n\,T}_{\tau_1} \\ \tilde{H}_{\bar{\tau}_2} \mathbf{X}(2)^{n\,T}_{\bar{\tau}_2} = -\tilde{H}_{\tau_1} \mathbf{z}(2)^{n\,T}_{\tau_1} \\ H_{\bar{\tau}_1} \mathbf{X}(1)^{n\,T}_{\bar{\tau}_1} - H_{\bar{\tau}_2} \mathbf{X}(2)^{n\,T}_{\bar{\tau}_2} = -(H_{\tau_1} \mathbf{z}(1)^{n\,T}_{\tau_1} - H_{\tau_2} \mathbf{z}(2)^{n\,T}_{\tau_2}). \end{cases} \tag{11}$$

Поскольку все решения системы (11) равноправны, то

$$H(\mathbf{X}(1)^n_{\bar{\tau}_1}, \mathbf{X}(2)^n_{\bar{\tau}_2} \mid \mathbf{z}(1)^n_{\tau_1}, \mathbf{z}(2)^n_{\tau_2}) = \tag{12}$$

$$2n - (|\tau_1| + |\tau_2|) - (\tilde{\Delta}_1 + \tilde{\Delta}_2 + \Delta_{\tau_1 \| \tau_2} - \dim(\mathsf{L}_r(\tilde{H}_{\bar{\tau}_1} \circ \tilde{H}_{\bar{\tau}_2}) \cap \mathsf{L}_r(H_{\bar{\tau}_1} \mid H_{\bar{\tau}_2}))).$$

Отметим, что случайные величины $\mathbf{S}^{k_2}$, $\mathbf{X}^n$ и $\mathbf{Z}^n_\tau$ образуют марковскую цепь. Тогда

$$H(\mathbf{X}(1)^n_{\bar{\tau}_1}, \mathbf{X}(2)^n_{\bar{\tau}_2} \mid \mathbf{S}^{k_2}, \mathbf{z}(1)^n_{\tau_1}, \mathbf{z}(2)^n_{\tau_2}) = H(\mathbf{X}(1)^n_{\bar{\tau}_1} \mid \mathbf{S}^{k_2}, \mathbf{z}(1)^n_{\tau_1}) + H(\mathbf{X}(2)^n_{\bar{\tau}_2} \mid \mathbf{S}^{k_2}, \mathbf{z}(2)^n_{\tau_2}).$$

В соответствии с (5) получим:

$$H(\mathbf{X}(1)^n_{\bar{\tau}_1}, \mathbf{X}(2)^n_{\bar{\tau}_2} \mid \mathbf{S}^{k_2}, \mathbf{z}(1)^n_{\tau_1}, \mathbf{z}(2)^n_{\tau_2}) = 2n - (|\tau_1| + |\tau_2|) - (rank(H_{\bar{\tau}_1}) + rank(H_{\bar{\tau}_2})). \tag{13}$$

Таким образом, подставляя в (9) выражения (12) и (13), получим:

$$H(\mathbf{S}^{k_2} \mid \mathbf{z}(1)^n_{\tau_1}, \mathbf{z}(2)^n_{\tau_2}) = \Delta_1 + \Delta_2 - (\tilde{\Delta}_1 + \tilde{\Delta}_2 + \Delta_{\tau_1 \| \tau_2} - \dim(\mathsf{L}_r(\tilde{H}_{\bar{\tau}_1} \circ \tilde{H}_{\bar{\tau}_2}) \cap \mathsf{L}_r(H_{\bar{\tau}_1} \mid H_{\bar{\tau}_2}))).$$

Так как $H(\mathbf{S}^{k_2} \mid \mathbf{z}(1)^n_{\tau_1}, \mathbf{z}(2)^n_{\tau_2})$ не зависит от значений координат с номерами из $\bar{\tau}_1$ и $\bar{\tau}_2$, то $H(\mathbf{S}^{k_2} \mid \mathbf{Z}(1)^n_{\tau_1}, \mathbf{Z}(2)^n_{\tau_2}) = H(\mathbf{S}^{k_2} \mid \mathbf{z}(1)^n_{\tau_1}, \mathbf{z}(2)^n_{\tau_2})$. Тогда из определения (6) следует (8). Теорема доказана.

Для $t(>)1$, в общем случае, различных матриц $A^{(1)}, ..., A^{(t)}$, имеющих одинаковое количество строк, символом $\mathrm{A}^{(1)} \| ... \| \mathrm{A}^{(t)}$ обозначим матрицу вида:

$$\begin{pmatrix} A^{(1)} & A^{(2)} & O & \dots & O & O \\ \dots & \dots & \dots & \dots & \dots & \dots \\ O & O & \dots & O & A^{(t-1)} & A^{(t)} \end{pmatrix}.$$

Следующая теорема является обобщением теоремы 1 на случай l-кратного перехвата и в работе она формулируется без доказательства.

Теорема 2. *Пусть* $(\tilde{C}, C)$ *– факторный код, проверочная матрица базового кода имеет вид из* (1), $\tau_1,...,\tau_l$ *– подмножества координат при* l *перехватах кодовых слов, соответствующих одному информационному сообщению;* $\bar{\tau}_i = \underline{n} \setminus \tau_i$, $\Delta_i = rank(H_{\bar{\tau}_i})$, $\Delta_{1\|..\|l} = rank\left(H_{\bar{\tau}_1} \| ... \| H_{\bar{\tau}_l}\right)$, $\tilde{\Delta}_i = rank(\tilde{H}_{\bar{\tau}_i})$, $i = 1,...,l$. *Тогда:*

$$\Delta_{\tau_1,...,\tau_l}(\tilde{C}, C) = \sum_{i=1}^{l}\Delta_i - (\sum_{i=1}^{l}\tilde{\Delta}_i + \Delta_{1\|..\|l} - \dim(\mathsf{L}_r(\tilde{H}_{\bar{\tau}_1} \circ ... \circ \tilde{H}_{\bar{\tau}_l}) \cap \mathsf{L}_r(H_{\bar{\tau}_1} \| ... \| H_{\bar{\tau}_l}))). \quad (14)$$

Вычисление неопределенности при l-кратном перехвате в случае применения кода Хэмминга и кода Рида-Маллера. Рассмотрим частный случай применения теоремы 2. Пусть главный канал без помех, $\tilde{C} = \mathsf{F}_q^n$, $k = n$, $k_2 = n - k_1$, $\tilde{H}_{0\times n} = \mathbf{0}(\in \mathsf{F}_q^n)$ и $\mu_1 = ... = \mu_l = \mu$. Можно показать, что

$$\Delta_{\tau_1,...,\tau_l}(\mathsf{F}_q^n, C) = \dim\left(\bigcap_{i=1}^{l}\mathsf{L}_c(H_{\bar{\tau}_i})\right), \quad (15)$$

где $\mathsf{L}_c(M)$ – линейная оболочка, натянутая на столбцы матрицы M. Введем обозначение для множества подматриц из $H_{k\times n}$: $\mathsf{H}(\mu) = \{H_\omega : \omega \subset \underline{n}, |\omega| = \mu\}$. Для фиксированного l рассмотрим последовательность чисел:

$$\tilde{k}_i^{(l)} = \min_{\chi \subset \mathsf{H}(i):|\chi|=l}\left\{\dim\left(\bigcap_{j=1}^{l}\mathsf{L}_c(H_{\omega_{i_j}})\right) : H_{\omega_{i_j}} \in \chi\right\}, \quad (16)$$

Из (7) и (16) можно показать, что $\Delta_\mu^{(l)}(\mathsf{F}_q^n, C) = \tilde{k}_{n-\mu}^{(l)}$. Далее приводится оценка $\Delta_\mu^{(l)}(\mathsf{F}_q^n, C)$ для $q = 2$, когда C является кодом Хэмминга или кодом Рида-Маллера.

Применение кода Хэмминга.

Лемма 2. *Пусть* C *–* $(n, k, 3)$ *– код Хэмминга,* $n = 2^r - 1$, $k = 2^r - r - 1$, $r \in \mathsf{N}$. *Тогда* $\tilde{k}_{n-\mu}^{(2)} = 0$, $\tilde{k}_{n-\mu}^{(1)} > 0$, $\tilde{k}_{n-\mu+1}^{(2)} > 0$ *при* $\mu = 2^r - 2^{\lfloor r/2 \rfloor}$.

Даказательство. Так как проверочная матрица $H_{(n-k)\times n}$ кода Хэмминга в качестве столбцов содержит все ненулевые векторы длины $n - k = r$, то в проверочной матрице найдутся два таких непересекающихся множества номеров столбцов $\bar{\tau}_1$ и $\bar{\tau}_2$, $|\bar{\tau}_1| = |\bar{\tau}_2| = 2^{\lfloor (n-k)/2 \rfloor} - 1$, что в столбцах с номерами из $\bar{\tau}_1$ нижние $\lfloor (n-k)/2 \rfloor$ элементов нулевые, а в $\bar{\tau}_2$ верхние $\lfloor (n-k)/2 \rfloor$ элементов нулевые. Следовательно $\mathsf{L}(H_{\bar{\tau}_1}) \cap \mathsf{L}(H_{\bar{\tau}_2}) = \mathbf{0}$. Обозначим $\tau_i = \underline{n} \setminus \{\bar{\tau}_i\}$, $i = 1, 2$.

Из (15) следует, что $\Delta_{\tau_1,\tau_2}(\mathsf{F}_2^n, C) = 0$ и $\tilde{k}_{n-\mu}^{(2)} = 0$. Предположим, что $\tilde{k}_{n-\mu}^{(1)} = 0$. Тогда существовало бы множество номеров τ мощности $n - 2^{\lfloor (n-k)/2 \rfloor} + 1$, $\tau \subset \underline{n}$, наблюдение значений которых давало бы полную информацию о закодированном сообщении. Но это предположение противоречит необходимому условию для полного снятия неопределенности. Предположим теперь, что $\tilde{k}_{n-\mu+1}^{(2)} = 0$. Тогда найдутся два таких непересекающихся множества $\bar{\tau}_1$ и $\bar{\tau}_2$, $|\bar{\tau}_1| = |\bar{\tau}_2| = 2^{\lfloor (n-k)/2 \rfloor}$, что $\mathsf{L}(H_{\bar{\tau}_1}) \cap \mathsf{L}(H_{\bar{\tau}_2}) = \mathbf{0}$. Отсюда следует, что $\dim\left(\mathsf{L}(H_{\bar{\tau}_1}) + \mathsf{L}(H_{\bar{\tau}_2})\right) = \dim\left(\mathsf{L}(H_{\bar{\tau}_1})\right) + \dim\left(\mathsf{L}(H_{\bar{\tau}_2})\right)$. Так как проверочная матрица кода Хэмминга не содержит нулевых столбцов, то $\dim \mathsf{L}(H_{\bar{\tau}_i}) \geq \lfloor (n-k)/2 \rfloor + 1$, $i = 1, 2$. Отсюда получаем, что

$$\dim\left(\mathsf{L}(H_{\bar{\tau}_1}) + \mathsf{L}(H_{\bar{\tau}_2})\right) \geq 2 \cdot \lfloor (n-k)/2 \rfloor + 2 \geq (n-k) + 1.$$

Это противоречит тому, что ранг проверочной матрицы кода равен $(n-k)$. Лемма доказана.

Лемма 3. *Пусть* C – $(n, k, 3)$*-код Хэмминга,* $n = 2^r - 1$, $k = 2^r - r - 1$, $r \in \mathsf{N}$. *Тогда* $\tilde{k}_{n-\mu}^{(4)} = 0$ *при* $\mu = 2^r - 2^{\lfloor r/2 \rfloor + 1}$, $n - k \geq 4$.

Доказательство. Пусть $\bar{\tau}_1$ и $\bar{\tau}_2$, $|\bar{\tau}_1| = |\bar{\tau}_2| = 2^{\lfloor (n-k)/2 \rfloor} - 1$, такие множества номеров, что в столбцах с номерами из $\bar{\tau}_1$ нижние $\lfloor (n-k)/2 \rfloor$ элементов нулевые, а в $\bar{\tau}_2$ верхние $\lfloor (n-k)/2 \rfloor$ элементов нулевые. Пусть g – номер столбца, верхние $\lfloor (n-k)/2 \rfloor$ и нижние $\lfloor (n-k)/2 \rfloor$ элементы которого единичные; по построению имеем $g \notin \bar{\tau}_i$, $i = 1, 2$. Пусть $\mathbf{e}$ – вектор длины $\lfloor (n-k)/2 \rfloor$, все элементы которого единичные. Тогда

$$H_{\{g\}} = \begin{cases} (\mathbf{e}, \mathbf{e})^T, & \textit{если k четное;} \\ (\mathbf{e}, 0, \mathbf{e})^T, & \textit{иначе.} \end{cases}$$

Без потери общности, предположим, что k – нечетное. Пусть $\bar{\tau}'_i$ – множество номеров тех столбцов матрицы $H_{(n-k)\times n}$, которые получаются всевозможными линейными комбинациями столбцов с номерами из множества $\bar{\tau}_i \cup \{g\}$, $i = 1, 2$. Так как в матрице $H_{(n-k)\times n}$ нет нулевых столбцов, то $|\bar{\tau}'_i| = 2^{\lfloor (n-k)/2 \rfloor + 1} - 1$. Получим

$$\mathsf{L}_c(H_{\bar{\tau}'_1}) \cap \mathsf{L}_c(H_{\bar{\tau}'_2}) = \{\mathbf{0}^{\mathrm{T}} (\in \mathsf{F}_2^{n-k}); (\mathbf{e}, 0, \mathbf{e})^{\mathrm{T}}; (\mathbf{0} (\in \mathsf{F}_2^{\lfloor (n-k)/2 \rfloor}), 0, \mathbf{e})^{\mathrm{T}}; (\mathbf{e}, 0, \mathbf{0} (\in \mathsf{F}_2^{\lfloor (n-k)/2 \rfloor}))^{\mathrm{T}}\}.$$

Отметим, что $\dim\left(\mathsf{L}(H_{\bar{\tau}'_1}) \cap \mathsf{L}(H_{\bar{\tau}'_2})\right) = 2$. Пусть $\mathbf{e}' (\in \mathsf{F}_2^{\lfloor (n-k)/2 \rfloor})$ – не равен нулевому вектору и отличается в одной позции от вектора $\mathbf{e}$. Так как проверочная матрица кода Хэмминга содержит все ненулевые векторы высоты

$(n-k)$, то существует такой номер $h \in \underline{n} \setminus \left(\bar{\tau}'_1 \cup \bar{\tau}'_2\right)$, что столбец с номером h имеет вид: $H_{\{h\}} = (\mathbf{e}', 0, \mathbf{e}')^T$. По аналогии с множествами $\bar{\tau}'_i$, $i = 1, 2$, построим $\bar{\tau}''_i$ по множествам $\bar{\tau}_i \cup \{h\}$, $i = 1, 2$. Очевидно, что $|\bar{\tau}''_i| = 2^{\lfloor (n-k)/2 \rfloor + 1} - 1$. Тогда $\mathsf{L}(H_{\bar{\tau}''_1}) \cap \mathsf{L}(H_{\bar{\tau}''_2}) = \{\mathbf{0}^T (\in \mathsf{F}_2^{n-k}); (\mathbf{e}', 0, \mathbf{e}')^T; (\mathbf{0} (\in \mathsf{F}_2^{\lfloor (n-k)/2 \rfloor}), 0, \mathbf{e}')^T; (\mathbf{e}', 0, \mathbf{0} (\in \mathsf{F}_2^{\lfloor (n-k)/2 \rfloor}))^T\}$.

Откуда, $\mathsf{L}_c(H_{\bar{\tau}_1}) \cap \mathsf{L}_c(H_{\bar{\tau}_2}) \cap \mathsf{L}(H_{\bar{\tau}''_1}) \cap \mathsf{L}(H_{\bar{\tau}''_2}) = \mathbf{0}^T$. Поэтому $\tilde{k}^{(4)}_{n-\mu} = 0$ при $\mu = 2^r - 2^{\lfloor r/2 \rfloor + 1}$. Лемма доказана.

Пусть F_q^n – линейное векторное пространство, $\{i_1; \ldots; i_m\} \subseteq \{1; \ldots; n\}$. Обозначим символом $V_{i_1, \ldots, i_m}$ – подпространство пространства F_q^n размерности $n-m$, векторы которого на координатах из множества $\{i_1; \ldots; i_m\}$ нулевые.

Лемма 4. *Пусть* $0 \le s \le n$. *Тогда* $\bigcap_{\{i_1; \ldots; i_{n-s}\} \subseteq \{1; \ldots; n\}} V_{i_1, \ldots, i_{n-s}} = \mathbf{0} (\in \mathsf{F}_q^n)$.

Доказательство. Предположим, что

$$\mathbf{a} = (a_1, \ldots, a_n) \in \bigcap\nolimits_{\{i_1; \ldots; i_{n-s}\} \subseteq \{1; \ldots; n\}} V_{i_1, \ldots, i_{n-s}}, \ \mathbf{a} \neq (0, \ldots, 0).$$

Без потери общности предположим, что $a_1 \neq 0$. Но это противоречит тому, среди всех подпространств вида $V_{i_1, \ldots, i_m}$ есть подпространства, где $i_1 = 1$. Лемма доказана.

Лемма 5. *Пусть* C – $(n, k, 3)$-*код Хэмминга,* $n = 2^r - 1$, $k = 2^r - r - 1$, $r \in \mathsf{N}$, $\mu = 2^{r-1}$. *Тогда* $\tilde{k}^{(l)}_{n-\mu} = \max\{0; r - l\}$, $l \in \mathsf{N}$.

Доказательство. По условию, $\mu = 2^{r-1}$, следовательно $n - \mu = 2^{r-1} - 1$. Заметим, что если среди столбцов матрицы $H_{(n-k) \times n}$ выбрать все столбцы с i-й нулевой координатой, $i = 1, \ldots, r$, то таких столбцов в каждой выборке будет $2^{r-1} - 1$, и подпространство, порожденное этими столбцами, будет совпадать с V_i. Если же выбрать произвольные $2^{r-1} - 1$ столбцов так, что все координаты могут быть ненулевыми, то размерность подпространства, порожденного таким столбцами, будет равна r. Таким образом, такой набор столбцов не снижает размерности пересечения подпространств. Следовательно, при нахождении $\tilde{k}^{(i)}_{n-\mu}$ необходимо выбирать $2^{r-1} - 1$ столбцов, порождающих V_i, $i = 1, \ldots, r$. По предыдущей лемме получаем, что $\tilde{k}^{(r)}_{n-\mu} = 0$. Покажем, что $\tilde{k}^{(r-1)}_{n-\mu} \ge 1$. Пусть $L_1, \ldots, L_{r-1}$ – различные подпространства размерности $r-1$ в F_q^r. Пусть $\mathbf{e}_i = (\varepsilon_{i,1}, \ldots, \varepsilon_{i,r}), i = 1, \ldots, r-1$ – векторы такие, что $\mathsf{L}(\mathbf{e}_i) = L_i^{\perp}$. Тогда пересечением подпространств $L_1, \ldots, L_{r-1}$ будет пространство решений однородной системы уравнений: $(\mathbf{e}_1^T, \ldots, \mathbf{e}_{r-1}^T)^T \mathbf{x}^T = \mathbf{0}^T \in \mathsf{F}_2^r$. Так как ранг системы не превосходит $r-1$ и число неизвестных равно r, то размерность

пространства решений будет не меньше 1. Следовательно, $\tilde{k}_{n-\mu}^{(r-1)} \geq 1$. Таким образом, минимальное количество подпространств размерности $r-1$, которые в пересечении дают нулевое подпространство, равно r. Учитывая это, а также то, что при нахождении $\tilde{k}_{n-\mu}^{(i)}$ необходимо выбирать $2^{r-1}-1$ столбцов, порождающих V_i, $i=1,...,r$, получим, что при $0 \leq j \leq r-1$ справедливо равенство: $\tilde{k}_{n-\mu}^{(j+1)} - \tilde{k}_{n-\mu}^{(j)} = 1.$ Лемма доказана.

Лемма 6. *Пусть* C $-(n,k,3)$*-код Хэмминга,* $n = 2^r - 1$, $k = 2^r - r - 1$, $r \in \mathbb{N}$. *Тогда* $\tilde{k}_{n-\mu}^{l} = k$ *при* $\mu < 2^{r-1}$ *для любого* $l \in \mathbb{N}$.

Доказательство. Известно, что для кода Хэмминга C справедливо равенство $d(C^{\perp}) = 2^{r-1}$. Если $\mu \leq 2^{r-1} - 1 < 2^{r-1}$, то любой первый перехват μ символов не несет никакой информации об информационном сообщении, а любой повтороный перехват μ символов обладает нулевой ценностью. Таким образом, любой l-кратный перехват в этом случае не возволяет снизить неопределенность наблюдателя ниже чем k. Лемма доказана.

Теорема 3. *Пусть* C $-(n,k,3)$*-код Хэмминга,* $n = 2^r - 1$, $k = 2^r - r - 1$, $r \in \mathbb{N}$. *Тогда:*

$$\Delta_{\mu}^{(l)}(\mathbb{F}_2^n, C)\begin{cases} = r, & \mu < d(C^{\perp})(= 2^{r-1}) \\ = \max\{0, r-l\}, & \mu = 2^{r-1} \\ = 0, & \mu = 2^r - 2^{\lfloor r/2 \rfloor}, l \geq 2 \\ > 0, & \mu = 2^r - 2^{\lfloor r/2 \rfloor}, l < 2 \\ = 0, & \mu = 2^r - 2^{\lfloor r/2 \rfloor + 1}, n-k \geq 4, l \geq 4 \\ > 0, & \mu = 2^r - 2^{\lfloor r/2 \rfloor} - 1, l \leq 2 \\ = 0, & \mu = n. \end{cases}$$

Доказательство теоремы следует из лемм 6, 5, 2 и 3.

Применение кода Рида-Маллера $\mathrm{R}(m-2,m)$**.** Пусть базовый код C – код Рида-Маллера $\mathrm{R}(m-2,m)$ с проверочной матрицей $H_{(m+1)\times(2^m-1)}$. Рассмотрим наборы $V_i^{(1)}$ $(i = 2,...,m+1)$ столбцов матрицы $H_{(m+1)\times(2^m-1)}$, содержащих столбцы, у которых первая координата имеет значение 1, координата с номером i имеет нулевое значение, а остальные координаты принимают произвольные значения из $\mathbb{F}_2$. Из вида матрицы $H_{(m+1)\times(2^m-1)}$ имеем, что $|V_i^{(1)}| = 2^{m-1}$ и таких наборов будет m штук. Не сложно видеть, что $V_i^{(1)} \cap V_{1,i} = \varnothing$, $V_i^{(1)} \oplus V_{1,i} = V_i$. Другими словами, $V_i^{(1)} = (1,0,...,0)^T + V_i$. Более того, $\mathrm{L}(V_i^{(1)}) = V_i$, $\dim(\mathrm{L}(V_i^{(1)})) = \dim(V_i) = m$. Таким образом, $\bigcap_{i=2}^{m+1} V_i^{(1)} = \{\mathbf{0}^T; (1,0,0,...,0)^T\}$. Рассмотрим набор V', состоящий из всех столбцов $H_{(m+1)\times(2^m-1)}$, содержащих две единицы. По множеству V' по-

строим множество V'', содержащее V' и столбцы матрицы $H_{(m+1)\times(2^m-1)}$, являющиеся линейными комбинациями столбцов из V'. Так как первая координата у всех столбцов матрицы $\mathrm{H}_{(\mathrm{m}+1)\times(2^{\mathrm{m}}-1)}$ равна единице, то любой столбец этой матрицы, содержащий четное число единиц, является суммой нечетного числа столбцов из V'. Заметим, что $|V'|=m$, $|V''|=\sum_{i \bmod 2=1, i\le m} C_m^i$; а так как $\sum_{i=0}^{m}(-1)^i C_m^i = 0$ и $\sum_{i=0}^{m} C_m^i = 2^m$, то $|V''|=2^{m-1}$. Отметим, что $\dim \mathsf{L}(V'') = m$. По построению V'', имеем $\mathsf{L}(V'') = \mathsf{L}(V')$. Выше отмечалось, что суммы любого нечетного количества векторов из V' дают вектор четного веса. Но сумма любого четного количества векторов из V' также даст вектор четного веса. Поэтому $\mathsf{L}(V'')$ – это подпространство пространства F_2^{m+1}, содержащее векторы четного веса. Отсюда следует, что $(1,0,...,0)^T \notin \mathsf{L}(V'')$ и

$$\bigcap_{i=2}^{m+1} V_i^{(1)} \bigcap V'' = \{\mathbf{0}^T\}. \qquad (17)$$

Лемма 7. *Пусть* C *– код* $\mathsf{R}(m-1,m)$, $m \in \mathsf{N}$, $H_{(m+1)\times 2^m}$ *– его проверочная матрица. Любой набор из* 2^{m-1} *столбцов матрицы* $H_{(m+1)\times 2^m}$ *имеет ранг либо* m*, либо* $m+1$.

Доказательство. Выше показано, что имеются наборы $V_i^{(1)}$ $(i = 2,...,m+1)$ из 2^{m-1} столбцов ранга m. Набор ранга $m+1$ может быть получен из любого набора $V_i^{(1)}$ $(i = 2,...,m+1)$ заменой любого вектора из $V_i^{(1)}$ вектор, у которого i-ая координата не равна 0. Покажем, что набор из 2^{m-1} столбцов не может иметь ранг $m-1$ и менее. Это следует из того, что набор из 2^{m-1} столбцов матрицы $H_{(m+1)\times 2^m}$ не образует подпространство. Поэтому линейная оболочка, натянутая на эти столбцы, содержит более 2^{m-1} векторов. Следовательно, размерность подпространства не менее m. Лемма доказана.

Для вычисления $\tilde{k}_{2^{m-1}}^{(l)}$ естественно выбирать наборы, ранг которых равен m, так как наборы ранга $m+1$ пользы не несут (размерность пересечения не уменьшается). Пусть $L_1,...,L_m$ – различные подпространства размерности m в пространстве F_2^{m+1}. Пусть $\mathbf{e}_i = (\varepsilon_{i,1},...,\varepsilon_{i,m+1}), i = 1,...,m$ – векторы такие, что $\mathsf{L}(\mathbf{e}_i) = L_i^{\perp}$. Тогда пересечением подпространств $L_1,...,L_{r-1}$ будет пространство решений однородной системы уравнений: $(\mathbf{e}_1^T,...,\mathbf{e}_m^T)^T \mathbf{x}^T = \mathbf{0}^T \in \mathsf{F}_2^{m+1}$. Ранг этой системы не более m. А так как число неизвестных равно $m+1$, то размерность пространства решений будет не меньше 1. Поэтому $\tilde{k}_{2^{m-1}}^{(l)} = 0,$ при $l \ge m+1$. Таким образом, справедлива

Теорема 4. *Пусть* C *– код Рида-Маллера* $\mathrm{R}(m-1,m)$, $m \in \mathbb{N}$. *Тогда* $\Delta_{\mu}^{(l)}(\mathrm{F}_2^n, C) = m+1$ *для всех* $l \in \mathbb{N}$, *если* $\mu < 2^{m-1}$, *и* $\Delta_{\mu}^{(l)}(\mathrm{F}_2^n, C) = 0$, *при* $l \geq m+1$ *и* $\mu \geq 2^{m-1}$.

Выводы. Таким образом, впервые получено выражение для вычисления меры стойкости кодового зашумления после l частичных перехватов в канале с помехами. В частном случае, когда канал не имеет помех, для базовых кодов Хэмминга и некоторых кодов Рида-Маллера удалось вычислить меру стойкости кодового зашумления в зависимости от числа μ перехватываемых символов в каждом кодовом слове и количества l наблюдаемых кодовых слов, соответствующих одному информационному слову. В частности, получены условия на полное снятие неопределенности для рассмотренных кодов. Отметим, что вычисление меры стойкости на основе полученного выражения для произвольных кодов представляется задачей трудной, хотя и очень актуальной с прикладной точки зрения.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Ozarov H., Wyner A. D.* Wire-Tap Channel II // BLTj, 63. – 1984. – P. 2135-2157.
2. *Wyner A. D.* The wire-tap channel // Bell System Technical Journal. – 1975. – Vol. 54, № 8. – P. 1355-1387.
3. *Яковлев В.А.* Защита информации на основе кодового зашумления / Под ред. В.И. Коржика. – СПб., 1993.
4. *Деундяк В.М., Косолапов Ю.В.* Математическая модель канала с перехватом второго типа // Известия высших учебных заведений, Северо-Кавказский регион, серия Естественные науки. – 2008. – № 3 (145). – С. 3-8.
5. *Wei V.K.* Generalized Hamming Weights for Linear Codes // IEEE Transactions on information theory. – 1991. – Vol. 37, № 5. – P. 1412-1418.
6. *Arunkumar Subramanian, Steven W. McLaughlin.* MDS codes on the erasure-erasure wiretap channel // arXv:0902.3286v1 [cs.IT]. – 19 Feb. 2009. – P. 1-4.
7. *Косолапов Ю.В., Никулин В.Э.* Способ организации распределенного хранилища, устойчивого к частичной утечке данных // Материалы XIII Междунар. научно-практ. конф. "ИБ-2013".Ч. I. – Таганрог: Изд-во ЮФУ, 2013. – С. 186-191.
8. *Газарян Ю.О., Винничук И.И., Косолапов Ю.В.* Стойкость кодового зашумления в рамках модели многократного частичного наблюдения кодовых сообщений // В сб. "Материалы XII Междунар. научно-практ. конф. ”Информационная безопасность". Ч. 3. – Таганрог: ЮФУ, 2012. – С. 258-263.
9. *Иванов В.А.* Статистические методы оценки эффективности кодового зашумления // Труды по дискр. мат. – М.: Физматлит, 2002. – Т. 6. – С. 48-63.
10. *Деундяк В.М., Косолапов Ю.В.* О стойкости кодового зашумления к статистическому анализу наблюдаемых данных многократного повторения // Моделирование и анализ информационных систем. – 2012. – Т. 19, № 4. – С. 110-127.

Статью рекомендовал к опубликованию к.т.н. Н.С. Могилевская.

Деундяк Владимир Михайлович – Южный федеральный университет; e-mail: vlade@math.rsu.ru; 344006, Ростов-на-Дону, ул. Большая Садовая, 105/42; тел.: 88632339861; кафедра АДМ; ст. научный сотрудник; к.ф.-м.н.; доцент.

Косолапов Юрий Владимирович – e-mail: taim@mail.ru; тел.: 89061833020; кафедра АДМ; к.т.н.; доцент.

Deundyak Vladimir Mikhailovich – South Federal University; e-mail: vlade@math.rsu.ru; 105/42, Bol'shaya Sadovaya street, Rosot-on-Don, 344006, Russia; phone: +78632339861; senior scientist; cand. of phis.-math. sc.; associate professor.

Kosolapov Jury Vladimirovich – e-mail: itaim@mail.ru; phone: +79061833020; cand. of eng. sc.; associate professor.