MSC 94A60

О ПОСТРОЕНИИ СОВЕРШЕННЫХ ШИФРОВ ЗАМЕНЫ С НЕОГРАНИЧЕННЫМ КЛЮЧОМ

С.М. Рацеев, Н.П. Панов

Ульяновский государственный университет,
ул. Льва Толстого, 42, Ульяновск, 432017, Россия, e-mail: RatseevSM@mail.ru

Аннотация. Исследуется задача построения совершенных шифров по фиксированному набору параметров.

Ключевые слова: криптография, информация, шифр, совершенный шифр.

К. Шеннон в 40-х годах 20-го века ввел понятие совершенного шифра, обеспечивающего наилучшую защиту открытых текстов. Такой шифр не дает криптоаналитику никакой дополнительной информации об открытом тексте па основе перехваченной криптограммы. Данные шифры используются в тех случаях, когда наиболее важна секретность передаваемой информации. В настоящей работе исследуется задача построения совершенных шифров замены с неограниченным ключом но фиксированному набору параметров.

Все необходимые определения можно найти в работах [1, 2]. Пусть U — конечное множество возможных «шифрвеличин», V — конечное множество возможных «шифробозначений». Пусть также имеются r ($r > 1$) инъективных отображений из U в V. Пронумеруем данные отображения: E_1, E_2,..., E_r. Данные отображения называются простыми заменами. Обозначим $\mathbb{N}_r = \{1, 2, ..., r\}$. Опорным шифром замены назовем совокупность $\Sigma = (U, \mathbb{N}_r, V, E, D)$, для которой выполнены следующие свойства:

1) для любых $u \in U$ и $j \in \mathbb{N}_r$ выполнено равенство $D_j(E_j(u)) = u$;

2) $V = \bigcup_{j\in\mathbb{N}_r} E_j(U)$.

При этом $E = \{E_1, ..., E_r\}$, $D = \{D_1, ..., D_r\}$, $D_j : E_j(U) \to U$, $j \in \mathbb{N}_r$.

l-ой степенью опорного шифра Σ назовем совокупность

$$\Sigma^l = (U^l, \mathbb{N}_r^l, V^l, E^{(l)}, D^{(l)})\,,$$

где $U^l, \mathbb{N}_r^l, V^l$ — декартовы степени соответствующих множеств U, $\mathbb{N}_r$, V. Множество $E^{(l)}$ состоит из отображений $E_{\overline{j}} : U^l \to V^l$, $\overline{j} \in \mathbb{N}_r^l$, таких что для любых $\overline{u} = u_1...u_l \in U^l$, $\overline{j} = j_1...j_l \in \mathbb{N}_r^l$ выполнено равенство

$$E_{\overline{j}}(\overline{u}) = E_{j_1}(u_1)...E_{j_l}(u_l) = v_1...v_l \in V^l\,,$$

а множество $D^{(l)}$ состоит из отображений $D_{\overline{j}} : E_{\overline{j}}(U^l) \to U^l$, $\overline{j} \in \mathbb{N}_r^l$, таких что для любых $\overline{v} = v_1...v_l \in V^l$, $\overline{j} = j_1...j_l \in \mathbb{N}_r^l$ выполнено равенство

$$D_{\overline{j}}(\overline{v}) = D_{j_1}(v_1)...D_{j_l}(v_l) = u_1...u_l \in U^l\,.$$

Отметим такой важный момент. В ряде случаев не всякое слово длины l в алфавите U может появиться в открытом тексте. Поэтому обозначим через $U^{(l)}$ подмножество всех таких слов во множестве U^l, появление которых в открытом тексте имеет ненулевую вероятность:

$$U^{(l)} = \{\overline{u} \in U^l \mid P_{U^l}(\overline{u}) > 0\}\,.$$

Тогда

$$V^{(l)} = \bigcup_{\overline{\jmath} \in \mathbb{N}_r^l} E_{\overline{\jmath}}(U^{(l)})\,.$$

Пусть ψ_c — случайный генератор ключевого потока, который для любого натурального числа l вырабатывает случайный ключевой поток $j_1 \ldots j_l$, где все $j_i \in \mathbb{N}_r$. Обозначим через Σ_H^l следующую совокупность величин:

$$\Sigma_H^l = (U^{(l)}, \mathbb{N}_r^l, V^{(l)}, E^{(l)}, D^{(l)}, P(U^{(l)}), P(\mathbb{N}_r^l))\,.$$

Шифром замены с неограниченным ключом назовем семейство

$$\Sigma_H = (\Sigma_H^l,\ l \in \mathbb{N};\ \psi_c)\,.$$

При этом независимые и не содержащие нулевых вероятностей распределения $P(U^{(l)})$ и $P(\mathbb{N}_r^l)$ индуцируют распределения вероятностей на множестве $V^{(l)}$:

$$P_{V^{(l)}}(\overline{v}) = \sum_{\substack{(\overline{u},\overline{\jmath}) \in U^{(l)} \cdot \mathbb{N}_r^l \\ E_{\overline{\jmath}}(\overline{u}) = \overline{v}}} P_{U^{(l)}}(\overline{u}) \cdot P_{\mathbb{N}_r^l}(\overline{\jmath}).$$

Также определим условные вероятности $P_{U^{(l)}|V^{(l)}}(\overline{u}|\overline{v})$ и $P_{V^{(l)}|U^{(l)}}(\overline{v}|\overline{u})$:

$$P_{V^{(l)}|U^{(l)}}(\overline{v}|\overline{u}) = \sum_{\overline{\jmath} \in \mathbb{N}_r^l(\overline{u},\overline{v})} P_{\mathbb{N}_r^l}(\overline{\jmath}), \qquad P_{U^{(l)}|V^{(l)}}(\overline{u}|\overline{v}) = \frac{P_{U^{(l)}}(\overline{u}) \cdot P_{V^{(l)}|U^{(l)}}(\overline{v}|\overline{u})}{P_{V^{(l)}}(\overline{v})},$$

где $\mathbb{N}_r^l(\overline{u},\overline{v}) = \{\overline{\jmath} \in \mathbb{N}_r^l \mid E_{\overline{\jmath}}(\overline{u}) = \overline{v}\}$.

Говорят, что шифр Σ_H является совершенным, если для любого натурального l и для любых $\overline{u} \in U^{(l)}$, $\overline{v} \in V^{(l)}$ выполнено равенство $P_{U^{(l)}|V^{(l)}}(\overline{u}|\overline{v}) = P_{U^{(l)}}(\overline{u})$.

Предложение 1 [2]. *Для шифра Σ_H следующие условия эквивалентны:*
(i) *для любого $l \in \mathbb{N}$ и любых $\overline{u} \in U^{(l)}$, $\overline{v} \in V^{(l)}$ выполнено равенство $P_{U^{(l)}|V^{(l)}}(\overline{u}|\overline{v}) = P_{U^{(l)}}(\overline{u})$;*
(ii) *для любого $l \in \mathbb{N}$ и любых $\overline{u} \in U^{(l)}$, $\overline{v} \in V^{(l)}$ выполнено равенство $P_{V^{(l)}|U^{(l)}}(\overline{v}|\overline{u}) = P_{V^{(l)}}(\overline{v})$;*
(iii) *для любого $l \in \mathbb{N}$ и любых $\overline{u}_1, \overline{u}_2 \in U^{(l)}$, $\overline{v} \in V^{(l)}$ выполнено равенство $P_{V^{(l)}|U^{(l)}}(\overline{v}|\overline{u}_1) = P_{V^{(l)}|U^{(l)}}(\overline{v}|\overline{u}_2)$.*

Предложение 2 [2]. *Пусть шифр замены с неограниченным ключом Σ_H является совершенным. Тогда для данного шифра будут выиолиеиы следующие свойства:*

(i) *для любого натурального числа* l *и любых* $\overline{u} \in U^{(l)}$, $\overline{v} \in V^{(l)}$ *найдется такой ключевой поток* $\overline{j} \in \mathbb{N}_r^l$, что $E_{\overline{j}}(\overline{u}) = \overline{v}$;

(ii) *для любого натурального числа* l *справедливо двойное неравенство*

$$|U^{(l)}| \leq |V^{(l)}| \leq |\mathbb{N}_r^l| = r^l.$$

Теорема 1 (достаточные условия совершенности шифра Σ_H [3]). *Пусть шифр замены* Σ_H *обладает следующими условиями:*

(i) *правила зашифрования* E_1, E_2,..., E_r *шифра* Σ_H *обладают тем свойством, что для любых* $u \in U$, $v \in V$ *найдется, и притом единственный, элемент* $j = j(u, v) \in \mathbb{N}_r$, *такой что* $E_j(u) = v$;

(ii) *распределение вероятностей* $P(\mathbb{N}_r)$ *является равномерным.*

Тогда шифр Σ_H *является совершенным, причем для любого* $l \in \mathbb{N}$ *выполнено равенство* $|V^{(l)}| = r^l$ *и распределение вероятностей* $P(V^{(l)})$ *будет являться равномерным.*

Теорема 2 [2]. *Пусть для шифра* Σ_H *выполнено равенство:* $|U| = |\mathbb{N}_r| = |V|$. *Шифр* Σ_H *является совершенным тогда и только тогда, когда выполнены следующие условия:*

(i) *правила зашифрования* E_1, E_2,..., E_r *шифра* Σ_H *обладают тем свойством, что для любых* $u \in U$, $v \in V$ *найдется, и притом единственный, элемент* $j = j(u, v) \in \mathbb{N}_r$, *такой что* $E_j(u) = v$;

(ii) *распределение вероятностей* $P(\mathbb{N}_r)$ *является равномерным.*

Приведем также критерий совершенных шифров замены с неограниченным ключом в классе шифров с равномерным распределением вероятностей на множестве $\mathbb{N}_r$.

Теорема 3 [4]. *Пусть для шифра* Σ_H *выполнены неравенства* $|U| \leq |V| \leq |\mathbb{N}_r|$ *и распределение вероятностей* $P(\mathbb{N}_r)$ *является равномерным. Шифр* Σ_H *является совершенным тогда и только тогда, когда выполнены следующие условия:*

(i) *для любых* $u \in U$ *и* $v \in V$ *найдется такое* $j \in \mathbb{N}_r$, *что* $E_j(u) = v$;

(ii) *для любых* $u_1, u_2 \in U$, $v \in V$ *выполнено равенство* $|\mathbb{N}_r(u_1, v)| = |\mathbb{N}_r(u_2, v)|$.

Рассмотрим задачу построения совершенного шифра Σ_H по заданному множеству «шифрвеличин» U и множеству $\mathbb{N}_r$ с распределением вероятностей $P(\mathbb{N}_r)$: по заданным U, $\mathbb{N}_r$, $P(\mathbb{N}_r)$ требуется определить, найдутся ли такие V, E, D, для которых шифр Σ_H являлся бы совершенным.

Теорема 4. *Для заданных* U, $|U| = n$, $\mathbb{N}_r$, $P(\mathbb{N}_r)$ *существует совершенный шифр* Σ_H *тогда и только тогда, когда найдется такое натуральное число* s *и* n *разбиений множества* $\mathbb{N}_r$

$$\begin{array}{lll}
\mathbb{N}_r = K_{11} \cup K_{12} \cup ... \cup K_{1s}, & K_{1i} \cap K_{1j} = \varnothing, & 1 \leq i < j \leq s, \\
\mathbb{N}_r = K_{21} \cup K_{22} \cup ... \cup K_{2s}, & K_{2i} \cap K_{2j} = \varnothing, & 1 \leq i < j \leq s, \\
 & ... & \\
\mathbb{N}_r = K_{n1} \cup K_{n2} \cup ... \cup K_{ns}, & K_{ni} \cap K_{nj} = \varnothing, & 1 \leq i < j \leq s,
\end{array} \qquad (1)$$

для которых выполнены следующие условия:

1) $K_{it} \cap K_{jt} = \emptyset$, $1 \le i < j \le n$, $t = 1, ..., s$;

2) *для любых* $1 \le i < j \le n$, $t = 1, ..., s$ *выполнено равенство*

$$\sum_{k \in K_{it}} P_{\mathbb{N}_r}(k) = \sum_{k \in K_{jt}} P_{\mathbb{N}_r}(k).$$

□ Достаточность. Пусть для U, $\mathbb{N}_r$, $P(\mathbb{N}_r)$, найдется такое s и n таких разбиений (1), для которых выполнены условия 1), 2). Пусть $V = \{v_1, ..., v_s\}$ — некоторое множество «шифробозначений», где s — число непустых частей из (1). Составим матрицу зашифрования размера $r \times n$ для опорного шифра, где строки пронумерованы элементами множества $\mathbb{N}_r$, а столбцы — элементами множества U, следующим образом. В i-м столбце ($i = 1, ..., n$) данной матрицы в строках, пронумерованных элементами множества K_{ij}, поставим элемент v_j, $j = 1, ..., s$. Условие 1) в этом случае гарантирует, что все простые замены E_j, $j \in \mathbb{N}_r$, полученного шифра являются инъективными отображениями. А из условия 2) следует, что для любого $t = 1, ..., s$ и любых $1 \le i < j \le n$ будут выполнены равенства

$$P_{V|U}(v_t|u_i) = \sum_{k \in K_{it}} P_{\mathbb{N}_r}(k) = \sum_{k \in K_{jt}} P_{\mathbb{N}_r}(k) = P_{V|U}(v_t|u_j)\,.$$

Поэтому, учитывая предложение 1, полученный опорный шифр Σ будет являться совершенным по Шеннону.

Покажем, что для любого $l \in \mathbb{N}$ шифр Σ_H^l является совершенным по Шеннону. Зафиксируем некоторое натуральное l. Пусть $\overline{a} = a_1...a_l \in U^{(l)}$, $\overline{b} = b_1...b_l \in U^{(l)}$, $\overline{v} = v_1...v_l \in V^{(l)}$. Тогда

$$P_{V^{(l)}|U^{(l)}}(\overline{v}|\overline{a}) = \prod_{i=1}^{l} P_{V|U}(v_i|a_i) = \prod_{i=1}^{l} P_{V|U}(v_i|b_i) = P_{V^{(l)}|U^{(l)}}(\overline{v}|\overline{b})\,.$$

Поэтому из предложения 1 следует, что шифр Σ_H^l является совершенным по Шеннону.

Необходимость. Пусть для заданных U, $\mathbb{N}_r$, $P(\mathbb{N}_r)$ существует совершенный шифр Σ_H со множеством «шифробозначений» $V = \{v_1, ..., v_s\}$. Обозначим для данного шифра

$$K_{it} = \{j \in \mathbb{N}_r \mid E_j(u_i) = v_t\}\,, \quad i = 1, ..., n, \quad t = 1, ..., s\,.$$

Понятно, что

$$P_{V|U}(v_t|u_i) = \sum_{j \in K_{it}} P_{\mathbb{N}_r}(j)\,.$$

Из предложений 1 и 2 следует, что для множеств K_{it} будут выполнены равенства (1) и условия 1), 2). ■

Следствие 1. *Пусть для заданных* U, $\mathbb{N}_r$, $P(\mathbb{N}_r)$ *существует совершенный шифр. Тогда для любого множества «шифрвеличин»* $\widetilde{U}$, $|\widetilde{U}| \le |U|$, *и для заданных* $\mathbb{N}_r$, $P(\mathbb{N}_r)$ *существует совершенный шифр* Σ_H.

Следствие 2. *Для заданных U, $|U| = n$, $\mathbb{N}_r$, $P(\mathbb{N}_r)$, V, $|V| = s$, существует совершенный шифр Σ_H тогда и только тогда, когда найдется n таких разбиений (1), для которых выполнены условия 1 и 2 предыдущей теоремы.*

Следствие 3. *Для заданных V, $|V| = s$, $\mathbb{N}_r$, $P(\mathbb{N}_r)$ существует совершенный шифр Σ_H тогда и только тогда, когда найдется такое n и такие разбиения (1), для которых выполнены условия 1 и 2 предыдущей теоремы.*

Следствие 4. *Для заданных $\mathbb{N}_r$, $P(\mathbb{N}_r)$ существует совершенный шифр Σ_H тогда и только тогда, когда найдутся такие n и s, $n \leq s$, и такие разбиения (1), для которых выполнены условия 1 и 2 предыдущей теоремы.*

Пример. Пусть $U = \{u_1, u_2\}$, $\mathbb{N}_4 = \{1, 2, 3, 4\}$ и распределение вероятностей на множестве $\mathbb{N}_4$ имеет вид

$\mathbb{N}_4$	1	2	3	4
$P(\mathbb{N}_4)$	2/7	1/7	3/7	1/7

В этом случае можно построить два разбиения множества $\mathbb{N}_4$ вида

$$\begin{array}{lcccccc} \mathbb{N}_4 & = & \{1,2\} & \cup & \{3\} & \cup & \{4\}, \\ \mathbb{N}_4 & = & \{3\} & \cup & \{1,4\} & \cup & \{2\} \end{array}$$

с условиями

$$P_{\mathbb{N}_4}(1) + P_{\mathbb{N}_4}(2) = P_{\mathbb{N}_4}(3),$$

$$P_{\mathbb{N}_4}(3) = P_{\mathbb{N}_4}(1) + P_{\mathbb{N}_4}(4),$$

$$P_{\mathbb{N}_4}(4) = P_{\mathbb{N}_4}(2).$$

По теореме 4 для данных U, $\mathbb{N}_4$, $P(\mathbb{N}_4)$ можно построить совершенный шифр Σ_H. Пусть $V = \{v_1, v_2, v_3\}$. Составим матрицу зашифрования следующим образом:

$\mathbb{N}_4 \diagdown U$	u_1	u_2
1	v_1	v_2
2	v_1	v_3
3	v_2	v_1
4	v_3	v_2

Тогда полученный шифр Σ_H будет являться совершенным.

Рассмотрим теперь такой несложный критерий.

Предложение 3. *Для заданных U и V можно построить совершенный шифр Σ_H тогда и только тогда, когда $|U| \leq |V|$.*

□ Если шифр Σ_H является совершенным, то неравенство $|U| \leq |V|$ следует из предложения 2.

Обратно, пусть для U и V выполнено неравенство $|U| \leq |V|$. Обозначим $r = |V|$, $n = |U|$. Составим матрицу A порядка $r \times n$ над множеством V следующим образом:

в каждом столбце матрицы A каждый элемент множества V встречается ровно один раз, а в каждой строке нет повторяющихся элементов (напомним, что такая матрица называется латинским прямоугольником и построить его можно, например, так: каждый следующий столбец является циклическим сдвигом на одну позицию предыдущего столбца). Пусть матрица A будет матрицей зашифрования опорного шифра для шифра Σ_H, а распределение вероятностей на множестве $\mathbb{N}_r$ равномерно. Тогда из теоремы 1 следует, что шифр Σ_H является совершенным. ■

Пусть $(\Omega = \mathbb{N}_r, F_{\mathbb{N}_r}, P_{\mathbb{N}_r})$ — вероятностное пространство. Зафиксируем $v \in V$. Обозначим через $\mathbb{N}_r(v)$ следующее множество:

$$\mathbb{N}_r(v) = \{j \in \mathbb{N}_r \mid v \in E_j(U)\}\,.$$

Под обозначением $\mathbb{N}_r(v)$ будем также понимать событие $(\mathbb{N}_r(v) \in F_{\mathbb{N}_r})$, заключающееся в том, что при случайном выборе элемента $j \in \mathbb{N}_r$ «шифробозначение» v можно расшифровать правилом расшифрования D_j: $v \in E_j(U)$. Тогда событию $\mathbb{N}_r(v)$ будут благоприятствовать все элементы из множества $\mathbb{N}_r(v)$, и только они. Поэтому

$$P(\mathbb{N}_r(v)) = \sum_{j\in\mathbb{N}_r(v)} P_{\mathbb{N}_r}(j)\,.$$

Если канал связи готов к работе и на приеме установлены действующие ключи, но в данный момент времени никакого сообщения не передается, то в этом случае противником может быть предпринята попытка имитации сообщения. Тогда вероятность успеха имитации каждого символа передаваемого сообщения определяется следующим образом:

$$P_{\text{im}} = \max_{v\in V} P(\mathbb{N}_r(v))\,.$$

Если же в данный момент передается некоторое сообщение, то противник может заменить некоторые символы этого сообщения, например некоторый символ $v \in V$ на $\widetilde{v} \in V$, отличный от v. При этом он будет рассчитывать на то, что на действующем ключе «шифробозначение» $\widetilde{v}$ будет успешно расшифровано. Пусть «$\mathbb{N}_r(\widetilde{v}) \mid \mathbb{N}_r(v)$» — событие, заключающееся в попытке подмены «шифробозначения» v «шифробозначением» $\widetilde{v}$. Применяя теорему о произведении вероятностей, получаем, что

$$P(\mathbb{N}_r(\widetilde{v}) \mid \mathbb{N}_r(v)) = \frac{P(\mathbb{N}_r(v)\ \cap\ \mathbb{N}_r(\widetilde{v}))}{P(\mathbb{N}_r(v))} = \frac{\sum_{j\in\mathbb{N}_r(v,\widetilde{v})} P_{\mathbb{N}_r}(j)}{\sum_{j\in\mathbb{N}_r(v)} P_{\mathbb{N}_r}(j)}\,,$$

где $\mathbb{N}_r(v,\widetilde{v}) = \mathbb{N}_r(v) \cap \mathbb{N}_r(\widetilde{v})$. Тогда вероятность успеха подмены «шифробозначения» будет вычисляться по следующей формуле:

$$P_{\text{podm}} = \max_{\substack{v,\widetilde{v}\in V,\\ v\neq\widetilde{v}}} P(\mathbb{N}_r(\widetilde{v}) \mid \mathbb{N}_r(v))\,.$$

Теорема 5 [2]. *Для шифра Σ_H справедливы неравенства*

$$P_{\text{im}} \geq \frac{|U|}{|V|}, \quad P_{\text{podm}} \geq \frac{|U|-1}{|V|-1}\,.$$

При этом $P_{\mathrm{im}} = |U|/|V|$ *тогда и только тогда, когда для любого* $v \in V$ *выполнено равенство* $P(K(v)) = |U|/|V|$. *Также* $P_{\mathrm{podm}} = (|U|-1)/(|V|-1)$ *тогда и только тогда, когда для любых* $v, \widetilde{v} \in V$, $v \neq \widetilde{v}$, *выполнено равенство*

$$P(K(\widetilde{v}) \mid K(v)) = (|U|-1)/(|V|-1)\,.$$

Далее везде предполагается, что для любого натурального l выполнены равенства $U^{(l)} = U^l$, $V^{(l)} = V^l$. Обозначим через P^l_{im} вероятность успеха имитации сообщения для шифра Σ^l_H, а через $P^l_{\mathrm{podm}}(s)$ — вероятность успеха подмены в сообщении длины l ровно s символов для шифра Σ^l_H, где $s \leq l$. Из определения вероятностей P_{im} и P_{podm} следуют такие равенства:

$$P^l_{\mathrm{im}} = (P_{\mathrm{im}})^l\,, \quad P^l_{\mathrm{podm}}(s) = (P_{\mathrm{podm}})^s\,.$$

Предложение 4. *Пусть для шифра* Σ_H *(с матрицей зашифрования опорного шифра из теоремы 4) выполнены равенства (1) и условия 1 и 2 теоремы 4. Тогда*

$$P^l_{\mathrm{im}} = \left(n \cdot \max_{1 \leq i \leq s} \sum_{k \in K_{1i}} P_{\mathbb{N}_r}(k)\right)^l,$$

$$P^l_{\mathrm{podm}}(t) = \left(\frac{1}{n} \cdot \max_{\substack{1 \leq i,j \leq s\\ i \neq j}} \frac{\sum_{k \in K_i \cap K_j} P_{\mathbb{N}_r}(k)}{\sum_{k \in K_{1i}} P_{\mathbb{N}_r}(k)}\right)^t,$$

где

$$K_i = \bigcup_{j=1}^{n} K_{ji}\,, \quad i = 1, ..., s\,.$$

□ Пусть $V = \{v_1, ..., v_s\}$, $1 \leq i \leq s$. Тогда из условий 1 и 2 теоремы 4 следуют такие равенства:

$$P(\mathbb{N}_r(v_i)) = \sum_{k \in K_{1i} \cup \ldots \cup K_{ni}} P_{\mathbb{N}_r}(k) = n \cdot \left(\sum_{k \in K_{1i}} P_{\mathbb{N}_r}(k)\right),$$

поэтому

$$P_{\mathrm{im}} = n \cdot \max_{1 \leq i \leq s} \sum_{k \in K_{1i}} P_{\mathbb{N}_r}(k)\,.$$

Далее, пусть $1 \leq i, j \leq s$, $i \neq j$. Тогда

$$P(\mathbb{N}_r(v_j) \mid \mathbb{N}_r(v_i)) = \frac{\sum_{k \in K_i \cap K_j} P_{\mathbb{N}_r}(k)}{\sum_{k \in K_i} P_{\mathbb{N}_r}(k)} = \frac{\sum_{k \in K_i \cap K_j} P_{\mathbb{N}_r}(k)}{n \cdot \left(\sum_{k \in K_{1i}} P_{\mathbb{N}_r}(k)\right)},$$

поэтому

$$P_{\mathrm{podm}} = \frac{1}{n} \cdot \max_{\substack{1 \leq i,j \leq s,\\ i \neq j}} \frac{\sum_{k \in K_i \cap K_j} P_{\mathbb{N}_r}(k)}{\sum_{k \in K_{1i}} P_{\mathbb{N}_r}(k)}\,. \quad \blacksquare$$

Предложение 5. *Пусть для шифра* Σ_H *выполнены равенства* (1) *и условия* 1 *и* 2 *теоремы* 4. *Для шифра* Σ_H *достигаются нижние границы для вероятностей имитации и подмены*

$$P^l_{\text{im}} = \left(\frac{n}{s}\right)^l, \quad P^l_{\text{podm}}(t) = \left(\frac{n-1}{s-1}\right)^t,$$

где $n = |U|$, $s = |V|$, *тогда и только тогда, когда для любых* $1 \leq i < j \leq s$ *выполнены следующие равенства:*

$$\sum_{k \in K_{1i}} P_{\mathbb{N}_r}(k) = \frac{1}{s}, \qquad \sum_{k \in K_i \cap K_j} P_{\mathbb{N}_r}(k) = \frac{n(n-1)}{s(s-1)}.$$

□ Доказательство следует из теоремы 5 и предложения 4. ■

Литература

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии / М.: Гелиос АРВ, 2005. – 480 с.
2. Зубов А.Ю. Криптографические методы защиты информации. Совершенные шифры / М.: Гелиос АРВ, 2005. – 192 с.
3. Рацеев С.М. О совершенных имитостойких шифрах // Прикладная дискретная математика. – 2012. – 17; №3. – С.41-47.
4. Рацеев С.М. О совершенных имитостойких шифрах замены с неограниченным ключом // Вестник Самарского государственного университета. Естественнонаучная серия. – 2013. – 110;№9/1. – С.42-48.

ON CONSTRUCTIONS OF PERFECT CODES OF SUBSTITUTION WITH UNBOUNDED KEY

S.M. Ratseev, N.P. Panov

Ulyanovsk State University,
Lev Tolstoy St., 42, Ulyanovsk, 432017, Russia, e-mail: RatseevSM@mail.ru

Abstract. The problem of constructing perfect codes on a fixed set of parameters is studied.

Key words: cryptography, information, code, perfect code.