Вестн. Сам. гос. техн. ун-та. Сер. Физ.-мат. науки. 2014. № 4 (37). С. 178–186
ISSN: 2310-7081 (online), 1991-8615 (print) doi: http://dx.doi.org/10.14498/vsgtu1309

# Информатика

УДК 519.728

## О КОДАХ АУТЕНТИФИКАЦИИ НА ОСНОВЕ ОРТОГОНАЛЬНЫХ ТАБЛИЦ

***С. М. Рацеев***[1], ***О. И. Череватенко***[2]

[1] Ульяновский государственный университет,
Россия, 432017, Ульяновск, ул. Л. Толстого, 42.
[2] Ульяновский государственный педагогический университет имени И. Н. Ульянова,
Россия, 432063, Ульяновск, пл. 100-летия со дня рождения В. И. Ленина, 4.

**Аннотация**

Исследуются коды аутентификации, стойкие к имитации и подмене сообщений. Особо выделен случай, когда вероятности имитации и подмены достигают нижних границ. Такие коды аутентификации называются оптимальными. Приводятся конструкции оптимальных кодов аутентификации на основе ортогональных таблиц. Рассматривается случай оптимальных кодов аутентификации с необязательно равномерным распределением на множестве ключей.

**Ключевые слова:** код аутентификации, имитация сообщения, хеш-функция.

**doi:** http://dx.doi.org/10.14498/vsgtu1309

Пусть $h : K \times X \to Y$ — ключевая криптографическая хеш-функция, где $X$ — конечное множество сообщений, $K$ — конечное множество ключей, $Y$ — конечное множество сверток. Напомним, что *кодом аутентификации* (без сокрытия) называется четверка $(X, K, Y, h)$, для которой $Y = \bigcup_{k \in K} h_k(X)$.

Заметим, что потенциальный противник может осуществлять не только пассивные действия относительно передаваемых по каналу связи сообщений,



**Образец для цитирования**
Рацеев С. М., Череватенко О. И. О кодах аутентификации на основе ортогональных таблиц // *Вестн. Сам. гос. техн. ун-та. Сер. Физ.-мат. науки*, 2014. № 4 (37). С. 178–186. doi: 10.14498/vsgtu1309.

**Сведения об авторах**
*Сергей Михайлович Рацеев* (к.ф.-м.н., доц.; RatseevSM@mail.ru; автор, ведущий переписку), доцент, каф. информационной безопасности и теории управления.
*Ольга Ивановна Череватенко* (к.ф.-м.н., доц.; chai@pisem.net), доцент, каф. высшей математики.

которые заключаются, например, в подслушивании или перехвате сообщений, но также и активные атаки, заключающиеся в *имитации* или *подмене* сообщения.

Пусть канал связи готов к работе и на приеме установлены действующие ключи $k \in K$, но в данный момент времени никакого сообщения вида $(x, y)$, где $y = h_k(x)$, не передается. Тогда в этом случае противником может быть предпринята попытка имитации сообщения некоторой парой $(x, y) \in X \times Y$.

Рассмотрим вероятностное пространство $(\Omega = K, F_K, P_K)$. Зафиксируем $(x, y) \in X \times Y$. Обозначим через $K(x, y)$ следующее множество:

$$K(x, y) = \{k \in K \mid h_k(x) = y\}.$$

Под обозначением $K(x, y)$ будем также понимать событие из алгебры событий $F_K$, заключающееся в том, что при случайном выборе ключа $k \in K$ будет выполнено равенство $h_k(x) = y$. Тогда событию $K(x, y)$ будут благоприятствовать все элементы из множества $K(x, y)$, и только они. Поэтому

$$P(K(x, y)) = \sum_{k \in K(x,y)} P_K(k).$$

Поскольку противник имеет возможность выбора $(x, y) \in X \times Y$, его шансы на успех имитации сообщения выражаются такой величиной:

$$P_{\text{im}} = \max_{(x,y) \in X \times Y} P(K(x, y)).$$

Если же в данный момент передается некоторое сообщение вместе со своей сверткой $(x, y) \in X \times Y$, $y = h_k(x)$, то противник может заменить его на $(\widetilde{x}, \widetilde{y}) \in X \times Y$, $\widetilde{x} \neq x$. При этом он будет рассчитывать на то, что на действующем ключе $k$ при проверке будет выполнено равенство $\widetilde{y} = h_k(\widetilde{x})$. Чем больше вероятность этого события, тем успешнее будет попытка подмены. Пусть «$K(\widetilde{x}, \widetilde{y}) \mid K(x, y)$» — событие, заключающееся в попытке подмены сообщения $(x, y)$ сообщением $(\widetilde{x}, \widetilde{y})$. Применяя теорему о произведении вероятностей, получаем

$$P(K(\widetilde{x}, \widetilde{y}) \mid K(x, y)) = \frac{P(K(x, y) \cap K(\widetilde{x}, \widetilde{y}))}{P(K(x, y))}.$$

Тогда вероятность успеха подмены сообщения будет вычисляться по следующей формуле:

$$P_{\text{subst}} = \max_{\substack{x, \widetilde{x} \in X,\ y, \widetilde{y} \in Y \\ x \neq \widetilde{x}}} P(K(\widetilde{x}, \widetilde{y}) \mid K(x, y)).$$

Теорема 1 [1]. *Для любого кода аутентификации $(X, K, Y, h)$ справедливы следующие утверждения*:

(*i*) $P_{\text{im}} \geqslant 1/|Y|$, *причем нижняя граница достигается тогда и только тогда, когда для любой пары $(x, y) \in X \times Y$ выполнено равенство*

$$P(K(x, y)) = 1/|Y|;$$

(*ii*) $P_{\text{subst}} \geqslant 1/|Y|$, *причем нижняя граница достигается тогда и только тогда, когда для любых* $x, \widetilde{x} \in X$, $x \neq \widetilde{x}$, $y, \widetilde{y} \in Y$ *выполнено равенство*

$$P(K(\widetilde{x}, \widetilde{y}) \mid K(x, y)) = 1/|Y|;$$

(*iii*) $P_{\text{im}}$ *и* $P_{\text{subst}}$ *одновременно достигают нижней границы тогда и только тогда, когда для любых* $x, \widetilde{x} \in X$, $x \neq \widetilde{x}$, $y, \widetilde{y} \in Y$ *выполнено равенство*

$$P(K(x, y) \ \cap \ K(\widetilde{x}, \widetilde{y})) = 1/|Y|^2.$$

Напомним несколько определений. *Латинским квадратом* $s$-того порядка над множеством $Y = \{y_1, \ldots, y_s\}$ называется таблица размера $s \times s$, заполненная элементами множества $Y$ таким образом, что в каждой строке и в каждом столбце каждый элемент встречается ровно один раз.

Две матрицы $A = (a_{ij})$ и $B = (b_{ij})$ над множеством $Y = \{y_1, ..., y_s\}$ называются *ортогональными*, если все упорядоченные пары $(a_{ij}, b_{ij})$ различны.

*Ортогональной таблицей* $OA(s, n)$ над множеством $Y = \{y_1, \ldots, y_s\}$ называется матрица размера $s^2 \times n$ над множеством $Y$ с тем условием, что для любых двух столбцов данной матрицы каждая из пар $(y_i, y_j) \in Y \times Y$ встречается ровно один раз. Существование ортогональной таблицы $OA(s, n)$ над множеством $Y$ эквивалентно существованию $n$ попарно ортогональных квадратных матриц порядка $s$ над множеством $Y$ [2].

Хорошо известно, что если число $s$ является степенью некоторого простого числа, то в этом случае существуют $s - 1$ попарно ортогональных латинских квадрата, или, что то же самое, $s + 1$ ортогональных матриц [3]: для этого достаточно рассмотреть многочлены $f_\alpha(x, y) = \alpha x + y$ над полем $GF(s)$ при ненулевых $\alpha$.

Большой интерес представляют коды аутентификации со свойством

$$P_{\text{im}} = P_{\text{subst}} = 1/|Y|.$$

Такие коды называются *оптимальными.* Для описания таких кодов используется понятие ортогональной таблицы.

Теорема 2 [1]. *Пусть код аутентификации* $(X, K, Y, h)$ *является оптимальным. Тогда верны следующие утверждения*:

(*i*) $|K| \geqslant |Y|^2$;

(*ii*) $|K| = |Y|^2$ *тогда и только тогда, когда табличное задание хеш-функции* $h$ *представляет собой ортогональную таблицу* $OA(|Y|, |X|)$ *над* $Y$ *и распределение вероятностей* $P_K$ *является равномерным.*

Следствие 1. *Пусть для кода аутентификации* $(X, K, Y, h)$ *выполнено равенство* $|K| = |Y|^2$. *Код аутентификации* $(X, K, Y, h)$ *является оптимальным тогда и только тогда, когда выполнены следующие условия*:

(*i*) *табличное задание хеш-функции* $h$ *представляет собой ортогональную таблицу* $OA(|Y|, |X|)$;

(*ii*) *распределение вероятностей на множестве* $K$ *равномерно.*

Пусть $(X, K, Y, h)$ — код аутентификации, $|X| = n$, $K = \{k_1, \ldots, k_r\}$, с распределением вероятностей $P_K$ на множестве ключей $K$ и табличным заданием хеш-функции $A$ размера $r \times n$ над множеством $Y$. При этом строки матрицы $A$ пронумерованы элементами множества $K$, а столбцы — элементами множества $X$. Пусть также для некоторого другого ключевого множества $\widetilde{K}$, $|\widetilde{K}| \geqslant |K|$, с распределением вероятностей $P_{\widetilde{K}}$ найдется такое разбиение на $r$ непустых непересекающиеся подмножеств

$$\widetilde{K} = K_1 \cup K_2 \cup \cdots \cup K_r, \tag{1}$$

для которого выполнены равенства

$$P_{\widetilde{K}}(K_i) = \sum_{k \in K_i} P_{\widetilde{K}}(k) = P_K(k_i), \quad i = 1, \ldots, r. \tag{2}$$

Построим код аутентификации $(X, \widetilde{K}, Y, \widetilde{h})$. Как видно, для данного кода остается задать хеш-функцию $\widetilde{h}$. Зададим ее таблично следующим образом: $j$-тую строку матрицы $A$ продублируем $|K_j|$ раз, $j = 1, \ldots, r$, и из всех полученных (продублированных) строк составим матрицу $B$. Матрица $B$ и будет табличным заданием хеш-функции $\widetilde{h}$.

Предложение 1. *Вероятности успехов имитации и успехов подмены для кодов аутентификации* $(X, K, Y, h)$ *и* $(X, \widetilde{K}, Y, \widetilde{h})$ *соответственно равны, в частности, из оптимальности одного кода аутентификации следует оптимальность другого.*

*Доказательство.* Следующие равенства

$$P(K(x, y)) = P(\widetilde{K}(x, y)), \quad P(K(\widetilde{x}, \widetilde{y}) \mid K(x, y)) = P(\widetilde{K}(\widetilde{x}, \widetilde{y}) \mid \widetilde{K}(x, y))$$

выполняются, так как для любых $x$, $\widetilde{x} \in X$, $x \neq \widetilde{x}$, $y$, $\widetilde{y} \in Y$, $i = 1, \ldots, r$

$$k_i \in K(x, y) \Leftrightarrow K_i \subseteq \widetilde{K}(x, y). \quad \square$$

Данное утверждение показывает, что оптимальные коды можно строить не только для случая, когда $P_K$ равномерно. Пусть

$$K = K_1 \cup K_2 \cup \cdots \cup K_{s^2} \tag{3}$$

— разбиение множества $K$ на непустые непересекающиеся подмножества с условием

$$P_K(K_i) = \sum_{k \in K_i} P_K(k) = \frac{1}{s^2}, \quad i = 1, \ldots, s^2. \tag{4}$$

Пусть также для чисел $s$ и $n$ существует ортогональная таблица $OA(s, n)$ над некоторым множеством $Y = \{y_1, ..., y_s\}$. Построим из данной таблицы (как

и до предложения 1) матрицу $B$ размера $|K| \times n$, которая будет таблично представлять хеш-функцию $h : K \times X \to Y$, где $X = \{x_1, \ldots, x_n\}$ — некоторое множество открытых текстов.

Предложение 2. *Полученный код аутентификации будет являться оптимальным.*

*Доказательство* следует из предложения 1 и следствия 1.

Пример. Пусть $X = \{x_1, x_2, x_3\}$, $Y = \{0, 1\}$, $K = \{k_1, \ldots, k_7\}$ и распределение вероятностей на множестве $K$ имеет вид

| $K$ | $k_1$ | $k_2$ | $k_3$ | $k_4$ | $k_5$ | $k_6$ | $k_7$ |
|---|---|---|---|---|---|---|---|
| $P_K$ | 1/16 | 3/16 | 1/20 | 1/10 | 1/10 | 1/4 | 1/4 |

.

В этом случае существует разбиение вида (3) с условием (4):

$$K_1 = \{k_1, k_2\}, \quad K_2 = \{k_3, k_4, k_5\}, \quad K_3 = \{k_6\}, \quad K_4 = \{k_7\},$$

$$P_K(K_1) = P_K(K_2) = P_K(K_3) = P_K(K_4) = 1/4.$$

Составим ортогональную таблицу $OA(2, 3)$ над $Y$, а на ее основе построим матрицу $B$, которая будет являться табличным представлением хеш-функции $h$:

$OA(2,3)$ :

| | | |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

,

$B$ :

| $K \diagdown X$ | $x_1$ | $x_2$ | $x_3$ |
|---|---|---|---|
| $k_1$ | 0 | 0 | 0 |
| $k_2$ | 0 | 0 | 0 |
| $k_3$ | 0 | 1 | 1 |
| $k_4$ | 0 | 1 | 1 |
| $k_5$ | 0 | 1 | 1 |
| $k_6$ | 1 | 0 | 1 |
| $k_7$ | 1 | 1 | 0 |

.

Из предложения 2 следует, что полученный код аутентификации является оптимальным, причем

$$P_{\text{im}} = P_{\text{subst}} = 1/2.$$

Заметим, что недостатком данной математической модели кода аутентификации является ограничения, накладываемые на мощности множеств $X$ и $K$. Рассмотрим математическую модель кода аутентификации без этих ограничений, введенную в работе [4], которая является аналогом математической модели шифров замены с ограниченным и неограниченным ключом, введенную А. Ю. Зубовым в работе [5] и позволяющую строить совершенные имитостойкие шифры [6, 7].

Пусть $U$, $V$ — соответственно конечные множества возможных кодвеличин и кодобозначений (как аналогия шифрвеличин и шифробозначений в модели шифра замены с неограниченным ключом [5]). Перед выработкой кода аутентификации сообщение $x \in X$ предварительно представляется в виде

последовательности кодвеличин, которые в процессе выработки кода аутентификации заменяются на кодобозначения. Пусть также имеются конечное множество ключей $K$ и ключевая хеш-функция $h : K \times U \to V$. Процесс выработки кода аутентификации для сообщения $x = u_1 \dots u_l$ на ключе $k_1 \dots k_l$ заключается в замене каждой кодвеличины $u_i$ на кодобозначение $v_i$ в соответствии с ключом $k_i$, $i = 1, \dots, l$. *Опорным кодом* кода аутентификации назовем совокупность $\Delta_H^0 = (U, K, V, h)$, для которой $V = \bigcup_{k \in K} h_k(U)$.

*$l$-той степенью опорного кода* $\Delta_H^0$ назовем совокупность

$$\Delta_H^l = (U^l, K^l, V^l, h^{(l)}),$$

где $U^l$, $K^l$, $V^l$ — декартовы степени соответствующих множеств $U$, $K$, $V$; множество $h^{(l)}$ состоит из отображений

$$h_{\overline{k}} : U^l \to V^l, \quad \overline{k} \in K^l,$$

таких, что для любых $\overline{u} = u_1 \dots u_l \in U^l$, $\overline{k} = k_1 \dots k_l \in K^l$ выполнено равенство

$$h_{\overline{k}}(\overline{u}) = h_{k_1}(u_1) \dots h_{k_l}(u_l) = v_1 \dots v_l \in V^l.$$

*Кодом аутентификации с неограниченным ключом* назовем семейство

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

где $\psi_c$ — случайный генератор ключевого потока.

Будем говорить, что код аутентификации с неограниченным ключом $\Delta_H$ является *оптимальным*, если оптимальным является код $\Delta_H^l$ для любого $l \in \mathbb{N}$.

Теорема 3 [4]. *Пусть для кода аутентификации $\Delta_H$ выполнены следующие условия*:

(*i*) $|K| = |V|^2$;

(*ii*) *для любых $u_1$, $u_2 \in U$, $v_1$, $v_2 \in V$ существует, и притом единственный, ключ $k \in K$, для которого $h_k(u_1) = v_1$ и $h_k(u_2) = v_2$*;

(*iii*) *распределение вероятностей на множестве $K$ равномерно.*

*Тогда код аутентификации $\Delta_H$ является оптимальным.*

Следствие 2. *Пусть для кода аутентификации $\Delta_H$ выполнено равенство $|K| = |V|^2$. Тогда $\Delta_H$ является оптимальным, тогда и только тогда, когда выполнены следующие условия*:

(*i*) *для любых $u_1$, $u_2 \in U$, $v_1$, $v_2 \in V$ существует, и притом единственный, ключ $k \in K$ такой, что $h_k(u_1) = v_1$, $h_k(u_2) = v_2$*;

(*ii*) *распределение вероятностей на множестве $K$ равномерно.*

Для кода аутентификации $\Delta_H^l$, $l \in \mathbb{N}$, обозначим через $P_{\text{im}}^l$ вероятность успеха имитации, а через $P_{\text{subst}}^l(s)$ — вероятность успеха подмены в сообщении ровно $s$ пар элементов вида $(u_i, v_i) \in U \times V$, где $v_i = h_{k_i}(u_i)$. Тогда, если код аутентификации $\Delta_H$ является оптимальным, то

$$P_{\text{im}}^l = 1/|V|^l, \qquad P_{\text{subst}}^l(s) = 1/|V|^s,$$

то есть $P^l_{\text{im}} \to 0$ при $l \to \infty$, $P^l_{\text{subst}}(s) \to 0$ при $s \to \infty$.

Пусть $\Delta_H$ — некоторый код аутентификации с неограниченным ключом с опорным кодом $\Delta^0_H = (U, K, V, h)$, $|U| = n$, $|V| = s$, $|K| = r$, распределением вероятностей $P_K$ для случайного генератора $\psi_c$ и табличным заданием хеш-функции $A$ размера $r \times n$ над множеством $V$ для кода $\Delta^0_H$. Пусть также для некоторого ключевого множества $\widetilde{K}$, $|\widetilde{K}| = \widetilde{r}$, $\widetilde{r} \geqslant r$, имеется случайный генератор $\widetilde{\psi}_c$ с распределением вероятностей $P_{\widetilde{K}}$ и условием, что найдется разбиение множества $\widetilde{K}$ на $r$ частей вида (1) с условием (2). Построим код аутентификации с неограниченным ключом $\widetilde{\Delta}_H$ со случайным генератором $\widetilde{\psi}_c$ и опорным кодом $\widetilde{\Delta}^0_H = (U, \widetilde{K}, V, \widetilde{h})$ со значениями $U$ и $V$, как и в опорном коде $\Delta^0_H$. Определим хеш-функцию $\widetilde{h}$ с помощью табличного представления $B$ размера $\widetilde{r} \times n$ над множеством $V$, в которой строки пронумерованы элементами множества $\widetilde{K}$, а столбцы — элементами множества $U$ следующим образом: $j$-тую строку матрицы $A$ продублируем $|K_j|$ раз, $j = 1, \ldots, r$, и из всех полученных (продублированных) строк составим матрицу $B$, которая и будет представлять хеш-функцию $\widetilde{h}$.

Предложение 3. *Вероятности успехов имитации и успехов подмены для кодов аутентификации $\Delta_H$ и $\widetilde{\Delta}_H$ соответственно равны, в частности, из оптимальности одного кода аутентификации следует оптимальность другого.*

*Доказательство* следует из предложения 1.

Пусть имеется разбиение (3) с условием (4). Пусть также для чисел $s$ и $n$ существует ортогональная таблица $OA(s, n)$ над множеством $V = \{v_1, \ldots, v_s\}$. Построим из данной таблицы матрицу $B$ размера $s^2 \times n$, которая будет таблично представлять хеш-функцию $h : K \times U \to V$.

Предложение 4. *Полученный код аутентификации $\Delta_H$ будет являться оптимальным.*

*Доказательство* следует из предложения 2.

**ORCID**
**Sergey Ratseev:** http://orcid.org/0000-0003-4995-9418
**Olga Cherevatenko:** http://orcid.org/0000-0003-3931-9425

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Черемушкин А. В. *Криптографические протоколы. Основные свойства и уязвимости.* М.: Академия, 2009. 272 с.
2. Холл М. *Комбинаторика.* М.: Мир, 1970. 424 с.
3. Bose R. S. On the applications of the properties of Galois fields to the problems of construction of Hyper–Graeco–Latin square // *Indian J. Stat*, 1938. vol. 4, no. 3. pp. 323–338.
4. Рацеев С. М. Об оптимальных кодах аутентификации // *Системы и средства информ.*, 2013. Т. 23, № 1 («Проблемы информационной безопасности и надежности систем информатики»). С. 53–57.
5. Зубов А. Ю. *Криптографические методы защиты информации. Совершенные шифры.* М.: Гелиос АРВ, 2005. 192 с.

6. Рацеев С. М. О совершенных имитостойких шифрах // *ПДМ*, 2012. № 3. С. 41–46.
7. Рацеев С. М. О совершенных имитостойких шифрах замены с неограниченным ключом // *Вестн. СамГУ. Естественнонаучн. сер.*, 2013. № 9/1(110). С. 42–48.

Поступила в редакцию 31/III/2014;
в окончательном варианте — 17/VI/2014;
принята в печать — 27/VIII/2014.

**Vestn. Samar. Gos. Techn. Un-ta. Ser. Fiz.-mat. nauki**
**[J. Samara State Tech. Univ., Ser. Phys. & Math. Sci.] 2014. Issue 4 (37). Pp. 178–186**

**ISSN: 2310-7081 (online), 1991-8615 (print)** **doi:** http://dx.doi.org/10.14498/vsgtu1309

**MSC: 68P25, 94A60**

# ON AUTHENTICATION CODES BASED ON ORTHOGONAL TABLES

***S. M. Ratseev*[1], *O. I. Cherevatenko*[2]**

[1] Ulyanovsk State University,
42, L. Tolstoy st., Ulyanovsk, 432017, Russian Federation.
[2] Ulyanovsk State I. N. Ulyanov Pedagogical University,
4, Ploshchad' 100-letiya so dnya rozhdeniya V. I. Lenina,
Ulyanovsk, 432063, Russian Federation.

**Abstract**

The authentication codes resistant to messages imitation and substitution are investigated. The case when the probabilities of imitation and substitution reach the lower limits has been highlighted. Such authentication codes are called optimal. We study constructions of optimal authentication codes based on orthogonal tables. The case of optimal authentication codes with optional uniform distribution on the set of keys is studied.

**Keywords:** authentication code, message imitation, hash function.

**doi:** http://dx.doi.org/10.14498/vsgtu1309

**ORCID**
**Sergey Ratseev:** http://orcid.org/0000-0003-4995-9418
**Olga Cherevatenko:** http://orcid.org/0000-0003-3931-9425



**How to cite Reference**
Ratseev S. M., Cherevatenko O. I. On authentication codes based on orthogonal tables, *Vestn. Samar. Gos. Tekhn. Univ., Ser. Fiz.-Mat. Nauki* [J. Samara State Tech. Univ., Ser. Phys. & Math. Sci.], 2014, no. 4 (37), pp. 178–186. doi: 10.14498/vsgtu1309. (In Russian)

**Authors Details**
*Sergey M. Ratseev* (Cand. Phys. & Math. Sci.; RatseevSM@mail.ru; Corresponding Author), Associate Professor, Dept. of Information Security & Control Theory.
*Olga I. Cherevatenko* (Cand. Phys. & Math. Sci.; chai@pisem.net), Associate Professor, Dept. of Higher Mathematics.

## REFERENCES


1. Cheremushkin A. V. *Kriptograficheskie protokoly. Osnovnye svoistva i uiazvimosti* [Cryptographic Protocols: Basic Properties and Vulnerability]. Moscow, Akademiia, 2009, 272 pp. (In Russian)
2. Holl M. *Combinatorial Theory*. New York, John Wiley & Sons, Inc., 1988, xvii+440 pp.. doi: 10.1002/9781118032862.
3. Bose R. S. On the applications of the properties of Galois fields to the problems of construction of Hyper–Graeco–Latin square, *Indian J. Stat*, 1938, vol. 4, no. 3, pp. 323–338.
4. Ratseev S. M. On optimal authentication code, *Sistemy i Sredstva Inform.*, 2013, vol. 23, no. 1, pp. 53–57 (In Russian).
5. Zubov A. Iy. *Kriptograficheskie metody zashchity informatsii. Sovershennye shifry* [Cryptographic Metho ds of Information Security. Perfect Ciphers]. Moscow, Gelios ARV, 2005, 192 pp. (In Russian)
6. Ratseev S. M. About perfect imitation resistant ciphers, *Prikl. Diskr. Mat.*, 2012, no. 3, pp. 41–46 (In Russian).
7. Ratseev S. M. On perfect imitation resistant ciphers of substitution with unbounded key, *Vestnik SamGU. Estestvenno-Nauchnaya Ser.*, 2013, no. 9/1(110), pp. 42–48 (In Russian).


Received 31/III/2014;
received in revised form 17/VI/2014;
accepted 27/VIII/2014.