УДК 519.7

С.М. Рацеев, А.М. Иванцов

О НЕКОТОРЫХ СВОЙСТВАХ КРИПТОГРАФИЧЕСКИХ ХЕШ-ФУНКЦИЙ

Рацеев Сергей Михайлович, *доктор физико-математических наук, доцент, окончил механико-математический факультет Ульяновского государственного университета. Профессор кафедры «Информационная безопасность и теория управления» УлГУ. Имеет статьи, учебные пособия в области криптографических методов защиты информации, PI-алгебр. [e-mail: ratseevsm@mail.ru].*

Иванцов Андрей Михайлович, *кандидат технических наук, доцент, окончил Ленинградское высшее военное инженерное училище связи, Военную академию связи, очную адъюнктуру Военной академии связи. Доцент кафедры «Информационная безопасность и теория управления» УлГУ. Имеет статьи, учебные пособия в области защиты информации. [e-mail: iwanzow@mail.ru].*

Аннотация

В работе исследуются бесключевые и ключевые хеш-функции. Для бесключевых хеш-функций одним из дополнительных требований является условие равномерности распределения значений хеш-функции при случайном равновероятном выборе значений аргументов. Приводится обоснование этого требования на примере конечного множества сообщений с использованием понятия сбалансированных функций. В работе показано, что в этом случае вероятность факта необнаружения изменения сообщения (файла) не превышает обратной величины мощности образов хеш-функции. Для современных хеш-функций с длиной хеш-значений 256–512 бит это означает, что такая вероятность ничтожно мала. Также приводятся недавние результаты о кодах аутентификации без сокрытия, стойких 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: хеш-функция, код аутентификации, имитация сообщения.

doi: 10.35752/1991-2927-2019-2-56-53-58

ON SOME PROPERTIES OF CRYPTOGRAPHIC HASH FUNCTIONS

Sergei Mikhailovich Ratseev, *Doctor of Sciences in Physics and Mathematics, Associate Professor; graduated from the Faculty of Mechanics and Mathematics of Ulyanovsk State University; Professor of the Department of Information Security and Control Theory of Ulyanovsk State University; an author of articles, textbooks in the field of cryptographic methods of information protection, PI-algebras. e-mail: ratseevsm@mail.ru.*

Andrei Mikhailovich Ivantsov, *Candidate of Science in Engineering; graduated from the Leningrad Higher Military Engineering School of Communications; graduated from the Military Academy of Communications; a postgraduate from the Military Academy of Communications; Associate Professor of the Department of Information Security and Control Theory of Ulyanovsk State University; an author of articles, textbooks in the field of information security. e-mail: iwanzow@mail.ru.*

Abstract

The article deals with hash functions with and without secret key. For the hash functions without a secret key, a condition of uniform distribution of hash functions values with a random equiprobable choice of argument values is one of the additional requirements. The rationale of this requirement is given on the example of a finite set of messages using the concept of the balanced functions. Authors demonstrate that the probability of the fact of nondetection of the message (or file) change does not exceed the reciprocal power value of hash function images. For modern hash functions with length of hash values of 256–512 bits, it means that such probability is slim to none. The paper is also survey of recent results of investigations on authentication codes resistant to imitation and substitution messages. 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.

Key words: hash function, authentication code, message simulation.

Введение

В криптографии особо выделяются два типа криптографических хеш-функций – ключевые (задаваемые ключом) и бесключевые (не зависящие от ключа). Хеш-функции, не зависящие от ключа, называют *кодами обнаружения ошибок* (modification detection code – MDC). Напомним, что основными требованиями, которые предъявляются к криптографическим хеш-функциям, не зависящим от ключа, должны быть следующие: практическая эффективность, сложность вычисления прообразов, устойчивость к коллизиям, устойчивость к нахождению второго прообраза. Ключевые хеш-функции имеют другое содержание, нежели бесключевые. Их применяют в системах с симметричными ключами и доверяющими друг другу сторонами. Данные функции называют к*одами аутентификации сообщений* (message authentication code – MAC). Ключевые хеш-функции предназначены для обеспечения невозможности для противника создавать новые или модифицировать передаваемые сообщения.

Хеш-функции, не зависящие от ключа

Пользователи некоторой сети или компьютерной системы должны быть уверены в подлинности приходящих в их адрес сообщений или хранимых файлов. Один из методов проверки целостности хранимого файла состоит в вычислении его «контрольной суммы», которая должна содержаться в защищенном от противника месте [1]. В случае, когда владелец файла желает убедиться в том, что он не подвергался изменению, необходимо вычислить вновь контрольную сумму для своего файла и сравнить результат с исходным значением. Несовпадение будет свидетельствовать о нарушении целостности. В качестве контрольной суммы удобно использовать значение некоторой бесключевой хеш-функции, которое обычно называется кодом обнаружения ошибок.

Хеш-функцией называют всякую легко вычисляемую функцию $h: X \to Y$. Значение хеш-функции называется ее *сверткой*.

При этом важным требованием, предъявляемым к хеш-функциям, является *равномерность* распределения их значений при случайном равновероятном выборе значений аргументов.

Поясним важность данного требования на примере. Для этого напомним понятие сбалансированного отображения. Пусть X, Y – некоторые конечные множества. Отображение $h: X \to Y$ называется *сбалансированным*, если для любых $y_1, y_2 \in Y$ мощности полных прообразов элементов y_1 и y_2 совпадают: $\left|h^{-1}(y_1)\right| = \left|h^{-1}(y_2)\right|$. Это означает, что если h является сбалансированным отображением, то для любого фиксированного $y \in Y$ верно равенство $|h^{-1}(y)| = \frac{|X|}{|Y|}$. Пусть A – некоторый конечный алфавит, в котором записываются сообщения (как правило, $A = \{0,1\}$), A^* – множество всех конечных слов в алфавите A, $X \subseteq A^*$ – некоторое множество открытых текстов, $Y = V_m$ – множество двоичных векторов длины m.

Предложение 1. *Пусть множество X конечно и распределение $P(X)$ равномерно. Тогда условие равномерности распределения значений хеш-функции при случайном выборе значений аргументов эквивалентно сбалансированности отображения h.*

Доказательство. Заметим, что распределение вероятностей $P(X)$ естественным образом индуцирует распределение вероятностей $P(Y)$ следующим образом. Пусть $y \in Y$. Тогда $P(y) = \sum_{x \in h^{-1}(y)} P(x)$. Так как распределение $P(X)$ равномерно, то $P(y) = \sum_{x \in h^{-1}(y)} P(x) = \frac{\left|h^{-1}(y)\right|}{|X|}$. Пусть отображение h сбалансированно. Тогда $P(y) = \frac{\left|h^{-1}(y)\right|}{|X|} = \frac{1}{|Y|}$, $y \in Y$. Обратно, пусть распределение $P(Y)$ равномерно. Тогда $\frac{1}{|Y|} = P(y) = \frac{\left|h^{-1}(y)\right|}{|X|}$, откуда $\left|h^{-1}(y)\right| = \frac{|X|}{|Y|}$. Предложение доказано.

Пусть $h: X \to Y$ – некоторая хеш-функция (со свойством равномерности распределения значений), $|X| < +\infty$, $x \in X$. В качестве x может быть некоторое сообщение, некоторые данные на компьютере и т. д. Для того чтобы контролировать целостность данных x, можно поступить следующим образом. Вычислим значение $y = h(x)$, и данные будем хранить или передавать в виде пары (x, y).

Предположим, что данные (x, y) были каким-либо случайным образом изменены. Пусть на приемном конце получена одна из следующих пар: (x', y), (x, y'), (x', y'), где $x' \in X, y' \in Y, x \neq x', y \neq y'$.

Вычислим вероятность того, что данные были изменены, но этот факт остался незамеченным.

1. Рассмотрим вариант (x',y). Вычислим вероятность того, что $h(x')=y$, т. е. с какой вероятностью факт изменения данных в сообщении x не будет обнаружен.

Так как в данном случае значение y фиксировано, а изменилось только $x \in X$, то пространством элементарных исходов будет являться множество $X\backslash\{x\}$. Событию $h(x')=y$ благоприятствуют такие элементарные исходы $x' \in X\backslash\{x\}$, при которых $h(x')=y$. Всего таких исходов $|h^{-1}(y)|-1$. В силу сбалансированности отображения h имеем такое равенство:

$$\left|h^{-1}(y)\right|-1=\frac{|X|}{|Y|}-1.$$

Следовательно,

$$P\left(h(x')=y\right)=\frac{\left|h^{-1}(y)\right|-1}{|X|-1}=$$

$$\frac{|X|-|Y|}{|Y|\cdot\left(|X|-1\right)}\le\frac{|X|-|Y|}{|Y|\cdot\left(|X|-|Y|\right)}=\frac{1}{|Y|}.$$

Таким образом, $P\left(h(x')=y\right)\le\frac{1}{|Y|}$.

2. Рассмотрим случай (x,y'). Так как $y\neq y'$, то $h(x)\neq y'$. Следовательно, $P(h(x)=y')=0$.

3. Остался случай (x',y'). Вычислим вероятность события, при котором $h(x')=y'$. Пространством элементарных исходов будет такое множество: $X\backslash\{x\}\times Y\backslash\{y\}$. Пусть B – матрица над множеством $\{0,1\}$ размером $(|X|-1)\times(|Y|-1)$, в которой строки занумерованы элементами множества $X\backslash\{x\}$, а столбцы – элементами множества $Y\backslash\{y\}$. В каждой клетке с номером $(x',y')\in X\backslash\{x\}\times Y\backslash\{y\}$ поставим единицу, если $h(x')=y'$, иначе 0. Очевидно, что в каждой строке данной матрицы будет не более одной единицы, поэтому количество пар (x',y'), для которых $h(x')=y'$, не превосходит $|X|-1$. Следовательно,

$$P\left(h(x')=y'\right)\le\frac{|X|-1}{\left(|X|-1\right)\cdot\left(|Y|-1\right)}=\frac{1}{|Y|-1}.$$

Таким образом, если, например, m = 256 (длина свертки), то из рассмотренных выше трех случаев видно, что вероятность не обнаружить изменения данных не превышает числа $\frac{1}{2^{256}-1}$. Важную роль для получения такой оценки сыграло свойство равномерности распределения значений хеш-функции при случайном выборе значений аргументов.

Коды аутентификации

Рассмотрим теперь хеш-функции, задаваемые ключом. Как правило, такие функции рассматривают в терминах теории кодирования как обобщение кодов, обнаруживающих ошибки, и называют кодами аутентификации [2]. При этом понятие кода аутентификации является более широким. Оно охватывает различные случаи кодирования сообщений: не только те, в которых сообщение передается в открытом виде и к нему дописывается код аутентичности сообщения, но и те, в которых обеспечивается сокрытие самого сообщения. Имеется большое многообразие систем аутентификации информации. С ними можно ознакомиться в работах [1–6]. Мы ограничимся рассмотрением понятием кода аутентификации без сокрытия, которое сводится к понятию ключевой хеш-функции.

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

Заметим, что потенциальный противник может осуществлять не только пассивные действия относительно передаваемых по каналу связи сообщений, 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 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 $P\left(K(x,y)\right)=\sum_{k\in K(x,y)}P_K(k)$. Поскольку противник имеет возможность выбора $(x,y)\in X\times Y$ его шансы на успех имитации сообщения выражаются такой величиной: $P_{im}=\max_{(x,y)\in X\times Y}P(K(x,y))$.

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

$$P\left(K\left(x',y'\right)|K\left(x,y\right)\right)=\frac{P\left(K\left(x,y\right)\cap K\left(x',y'\right)\right)}{P\left(K\left(x,y\right)\right)}.$$

Тогда вероятность успеха подмены сообщения будет вычисляться по следующей формуле:

$$P_{podm}=\max_{x,x'\in X,x\neq x',y,y'\in Y}P(K(x',y')|K(x,y)).$$

Теорема 1 [2]. *Для любого кода аутентификации* (X,K,Y,h), $|Y|=s$ *справедливы следующие утверждения:*

1. $P_{im}\geq 1/s$ *причем нижняя граница достигается тогда и только тогда, когда для всех* $(x,y)\in X\times Y$ *выполнено равенство* $P(K(x,y))=1/s$.
2. $P_{podm}\geq 1/s$ *причем нижняя граница достигается тогда и только тогда, когда для любых* $x,x'\in X; x\neq x'; y,y'\in Y$ *выполнено равенство* $P(K(x',y')|K(x,y))=1/s$.
3. P_{im} и P_{podm} *одновременно достигают нижней границы тогда и только тогда, когда для любых* $x,x'\in X; x\neq x'; y,y'\in Y$ *выполнено равенство* $P((K(x,y)\cap(K(x',y'))=1/s^2$.

Напомним, что *ортогональной таблицей* $OA(s,n,\lambda)$ над множеством $Y=\{y_1,\ldots,y_s\}$ называется матрица порядка $\lambda s^2\times n$ над множеством Y с тем условием, что для любых двух столбцов данной матрицы каждая из пар $(x_i,y_i)\in X\times Y$ встречается ровно в λ строках.

Большой интерес представляют коды аутентификации со свойством $P_{im}=P_{podm}=1/|Y|$. Такие коды аутентификации называются *оптимальными*. Для описания оптимальных кодов аутентификации используются ортогональные таблицы.

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

1. $|K|\geq n(s-1)+1$.
2. $|K|=n(s-1)+1$ *тогда и только тогда, когда табличное задание хеш-функции* h *представляет собой ортогональную таблицу* $OA(s,n,\lambda)$ *при* $\lambda=\frac{n(s-1)+1}{s^2}$ *и распределение вероятностей* $P(K)$ *является равномерным.*

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

1. *Табличное задание хеш-функции* h *представляет собой ортогональную таблицу* $OA\left(s,n,\frac{n(s-1)+1}{s^2}\right)$.
2. *Распределение вероятностей на множестве* K *равномерно.*

Рассмотрим алгоритм создания ортогональной таблицы на основе работ [2, 7]. Пусть $F=GF(q)$ – конечное поле из q элементов, $q=p^n$ – степень простого числа p, F^d – векторное пространство размерности d, $d\geq 2$ над полем F. Пусть M – подмножество в F^d, состоящее из попарно линейно независимых векторов над F. Например, множество M можно построить следующим образом. Рассмотрим следующие подмножества в

$$F^d: M_i=\{(0,\ldots,0,1,x_{i+1},\ldots,x_d)\ |x_j\in F, j=i+1,\ldots,d\}, i=1,\ldots,d.$$

Тогда в качестве M возьмем множество $M=\bigcup_{i=1}^{d}M_i$.

Заметим, что $|M|=1+q+\ldots+q^{d-1}=\frac{q^d-1}{q-1}$.

Пусть A – матрица порядка $|F^d|\times|M|$ над F. Пронумеруем строки матрицы A элементами множества F^d, а столбцы – элементами множества M. В матрице A на пересечении строки с номером $x=(x_1,\ldots,x_d)\in F^d$ и столбца с номером $y=(y_1,\ldots,y_d)\in M$ поставим элемент $\sum_{i=1}^{d}x_iy_i\in F$.

Предложение 2 [7]. *Полученная матрица* A *является ортогональной таблицей* $OA(q,|M|,q^{d-2})$ *над* F.

Предложение 3 [7]. *Пусть табличное задание хеш-функции* $h:K\times X\to Y$ *представляет собой построенную выше матрицу* A *и распределение вероятностей на множестве ключей* K *равномерно. Тогда код аутентификации* (X,K,Y,h) *является оптимальным.*

Заметим, что оптимальные коды можно строить не только для случая, когда $P(K)$ равномерно [8]. Пусть (X,K,Y,h) – некоторый код аутентификации, в котором $|X|=n$, $K=\{k_1,\ldots,k_r\}$ 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 K', $|K'|\geq|K|$, с распределением вероятностей $P(K')$ найдется такое разбиение на r непустых непересекающихся подмножеств $K'=K_1\cup K_2\cup\ldots\cup K_r$, для которого выполнены равенства:

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

Построим код аутентификации (X, K', Y, h'). Как видно, для данного кода остается задать хеш-функцию h'. Зададим ее таблично следующим образом: j-ю 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 h'.

Предложение 4 [8]. *Вероятности успехов имитации и успехов подмены для кодов аутентификации (X, K, Y, h) и (X, K', Y, h') соответственно равны, в частности, из оптимальности одного кода аутентификации следует оптимальность другого.*

Данное предложение показывает, что оптимальные коды можно строить не только для случая, когда $P(K)$ равномерно. Пусть $K = K_1 \cup K_2 \cup \ldots \cup K_{s^2}$ – разбиение множества K на непустые непересекающиеся подмножества с условием, что

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

Пусть также для чисел s и n существует ортогональная таблица $OA(s, n)$ над некоторым множеством $Y = \{y_1, \ldots, y_s\}$. Построим из данной таблицы (как и до предложения 4) 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 5 [8]. *Полученный код аутентификации будет являться оптимальным.*

Заметим также, что оптимальные коды аутентификации можно строить на основе конечных полей [9].

Заключение

Хеш-функции играют важную роль в криптографии и используются во многих приложениях, например, электронной подписи, аутентификации и обеспечения целостности данных. Если бесключевая хеш-функция используется для контроля целостности информации, то, как показано выше, важно, чтобы выполнялось условие равномерности распределения ее значений при случайном равновероятном выборе значений аргументов. Что касается ключевых хеш-функций, заметим, что некоторые конструкции оптимальных кодов аутентификации тесно связаны с конструкциями совершенных имитостойких шифров [9, 10]. Такие шифры обеспечивают наилучшую защиту открытых текстов, и они не дают криптоаналитику никакой дополнительной информации об открытом тексте на основе перехваченного шифрованного сообщения. Так как длины ключей совершенных шифров и оптимальных кодов аутентификации не меньше длин передаваемых сообщений, то данные шифры и коды аутентификации целесообразно использовать в исключительно важных случаях.

СПИСОК ЛИТЕРАТУРЫ

1. Зубов А.Ю. Математика кодов аутентификации. – М. : Гелиос АРВ, 2007. – 480 с.

2. Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости. – М. : Издательский центр «Академия», 2009. – 272 с.

3. Мао В. Современная криптография: теория и практика. – М. : Вильямс, 2005. – 768 с.

4. Столлингс В. Криптография и защита сетей: принципы и практика : – М. : Вильямс, 2001. – 672 с.

5. Фергюсон Н., Шнайер Б. Практическая криптография. – М. : Вильямс, 2005. – 424 с.

6. Prenel B. Cryptographic primitives for information authentication – state of the art. Lecture Notes in Computer Science. 1998. Vol. 1528. pp. 49–104.

7. Рацеев С.М., Череватенко О.И. Об оптимальных кодах аутентификации на основе конечных полей // Научные ведомости БелГУ. Сер. Математика. Физика. – 2017. – № 13 (262). – С. 38–41.

8. Рацеев С.М., Череватенко О.И. О кодах аутентификации на основе ортогональных таблиц // Вестник СамГТУ. Сер. Физ.-мат. науки. – 2014. – № 4 (37). – С. 178–186.

9. О применении конечных полей в некоторых совершенных криптосистемах / С.М. Рацеев, Е.Е. Беспалова, П.В. Буранкина, М.А. Гусарова // Вестник СибГУТИ. – 2017. – № 4. – С. 35–44.

10. Рацеев С.М. Некоторые обобщения теории Шеннона о совершенных шифрах // Вестник ЮУрГУ. Сер. Математическое моделирование и программирование. – 2015. – № 1 (8). – С. 111–127.

REFERENCES

1. Zubov A.Iu. *Matematika kodov autentifikatsii* [Authentication Codes Mathematics]. Moscow, Gelios ARV Publ., 2007. 480 p.

2. Cheremushkin A.V. *Kriptograficheskie protokoly. Osnovnye svoistva i uiazvimosti* [Cryptographic Protocols: Basic Properties and Vulnerability]. Moscow, 'Akademiya' Publ., 2009. 272 .

3. Mao V. *Sovremennaia kriptografiia: teoriia i praktika* [Modern Cryptography: Theory and Practice]. Moscow, Williams Publ., 2005. 768 p.

4. Stallings W. *Kriptografiia i zashchita setei: printsipy i praktika. Per. s angl.* [Cryptography and Network Security: Principles and Practice. Translated from Engl.]. Moscow, Williams Publ., 2001. 672 p.

5. Ferguson N., Shneier B. *Prakticheskaia kriptografiia* [Practical Cryptography]. Moscow, Williams, 2005. 424 p.

6. Prenel B. Cryptographic Primitives for Information Authentication – State of the Art. *Lecture Notes in Computer Science*, 1998, vol. 1528, pp. 49–104.

7. Ratseev S.M., Cherevatenko O.I. Ob optimalnykh kodakh autentifikatsii na osnove konechnykh polei [On Optimal Authentification Codes Based on Galois Fields].

Nauchnye vedomosti Belgorodskogo gosudarstvennogo universiteta. Matematika. Fizika [Proc. of Belgorod State University. Series Mathematics and Physics], 2017, no. 13 (262), pp. 38–41.

8. Ratseev S.M., Cherevatenko O.I. O kodakh autentifikatsii na osnove ortogonalnykh tablits [On Authentication Codes Based on Orthogonal Tables]. *Vestnik Samarskogo gosudarstvennogo tekhnicheskogo universiteta. Ser. Fiz. mat. nauki.* [Journal of Samara State Technical University. Ser. Physical and Mathematical Sciences], 2014, no. 4 (37), pp. 178–186.

9. Ratseev S.M., Bespalova E.E., Burankina P.V., Gusarova M.A. O primenenii konechnykh polei v nekotorykh sovershennykh kriptosistemakh [On Application of Finite Fields in Some Perfect Cryptosystems]. *Vestnik SibGUTI* [Proc. of the Siberian State University of Telecommunications and Information Science], 2017, no. 4, pp. 35–44.

10. Ratseev S.M. Nekotorye obobshcheniia teorii Shennona o sovershennykh shifrakh [Some Generalizations of Shannon's Theory of Perfect Ciphers]. *Vestnik Yuzhno-Uralskogo gosudarstvennogo universiteta. Ser. Matematicheskoe modelirovanie i programmirovanie* [Bulletin of the South Ural State University. Series: Mathematical Modelling, Programming and Computer Software], 2015, no. 1 (8), pp. 111–127.