ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 519.7

СВОЙСТВА КОМПОНЕНТ НЕКОТОРЫХ КЛАССОВ ВЕКТОРНЫХ БУЛЕВЫХ ФУНКЦИЙ[1]

И. А. Панкратова

Национальный исследовательский Томский государственный университет, г. Томск, Россия

В классе обратимых векторных булевых функций от n переменных с координатными функциями, существенно зависящими от всех переменных, рассматриваются подклассы $\mathcal{K}_n$ и $\mathcal{K}'_n$. Функции этих классов получены с помощью n независимых транспозиций соответственно из тождественной подстановки и из подстановки, каждая координатная функция которой существенно зависит от одной переменной. Приводятся некоторые свойства компонент функций из этих классов.

Ключевые слова: *векторная булева функция, обратимые функции, нелинейность векторной булевой функции, компонентная алгебраическая иммунность.*

DOI 10.17223/20710410/44/1

PROPERTIES OF COMPONENTS FOR SOME CLASSES OF VECTORIAL BOOLEAN FUNCTIONS

I. A. Pankratova

National Research Tomsk State University, Tomsk, Russia

E-mail: pank@mail.tsu.ru

In the class of invertible vectorial Boolean functions in n variables with coordinate functions depending on all variables, we consider the subclasses $\mathcal{K}_n$ and $\mathcal{K}'_n$, where the functions are obtained using n independent transpositions, respectively, from the identity permutation and from the permutation with coordinate functions essentially dependent on exactly one variable. We show that, for any $F = (f_1 \dots f_n) \in \mathcal{K}_n \cup \mathcal{K}'_n$ and $i \in \{1, \dots, n\}$, the coordinate function f_i has a single linear variable, each component function vF with vector $v \in \mathbb{F}_2^n$ of a weight greater than 1 has no fictitious and linear variables , the nonlinearity N_F, the degree $\deg F$, and the component algebraic immunity $\mathrm{AI}_{\mathrm{comp}}(F)$ are 2, $n-1$, and 2 respectively.

Keywords: *vectorial Boolean functions, invertible functions, nonlinearity, component algebraic immunity.*

[1]Работа поддержана грантом РФФИ, проект № 17-01-00354.

Введение

Векторные булевы функции широко используются при построении симметричных и асимметричных криптосистем [1 – 3]. К этим функциям предъявляются различные требования: они должны быть обратимы, обладать хорошими криптографическими свойствами, допускать компактное представление, быстро вычисляться. Один из способов удовлетворить последним двум требованиям — ограничение на число существенных переменных координатных функций. В [1, 4] описаны методы получения обратимых векторных булевых функций от n переменных, каждая координата которых существенно зависит ровно от k переменных, $k < n$. Отправной точкой для этих методов служат функции от k переменных, каждая координата которых существенно зависит от всех переменных. В данной работе рассматриваются два класса таких функций — $\mathcal{K}_n$ и $\mathcal{K}'_n$, устанавливаются некоторые криптографические свойства функций в них, в том числе значения для их нелинейности, степени и компонентной алгебраической иммунности.

1. Описание классов $\mathcal{K}_n$ и $\mathcal{K}'_n$

Для $n \in \mathbb{N}$ рассмотрим обратимые векторные булевы функции $F = (f_1 \dots f_n)$ на $\mathbb{F}_2^n$, такие, что координатные функции $f_i : \mathbb{F}_2^n \to \mathbb{F}_2$, $i = 1, \dots, n$, существенно зависят от всех переменных $x_1, \dots, x_n$; обозначим класс таких функций $\mathcal{F}_n$. В [5] предложен алгоритм 1 построения некоторой такой функции, который состоит в следующем: стартуя с тождественной подстановки $G : \mathbb{F}_2^n \to \mathbb{F}_2^n$, на i-м шаге, $i = 1, \dots, n$, выбираем множество $M_i = \{a, b\}$, где $a, b \in \mathbb{F}_2^n$, a и b отличаются только в i-й координате (соседние по ней) и не принадлежат M_j для $j < i$, и меняем местами значения $G(a)$ и $G(b)$. Таким образом, по построению, $M_i \cap M_j = \varnothing$ для всех $i, j = 1, \dots, n$, $i \neq j$, и для любого $a = a_1 \dots a_n \in \mathbb{F}_2^n$ имеет место

$$f_i(a) = \begin{cases} a_i \oplus 1, & \text{если } a \in M_i, \\ a_i & \text{иначе.} \end{cases} \tag{1}$$

Обозначим класс функций, которые можно получить алгоритмом 1 (при всевозможных способах выбора пар a, b), через $\mathcal{K}_n$. В [5] доказано, что $\mathcal{K}_n \neq \varnothing$ для всех $n > 2$; в [6] описаны некоторые свойства координат функций из $\mathcal{K}_n$.

Для любой рассматриваемой далее функции $F \in \mathcal{K}_n$ и любого $i \in \{1, \dots, n\}$ под M_i подразумевается та пара векторов в $\mathbb{F}_2^n$, соседних по i-й координате, которую алгоритм 1 выбирает на своём i-м шаге.

В [5] предложена модификация алгоритма 1 построения функций из класса $\mathcal{K}_n$, состоящая в том, что отправной точкой алгоритма является не обязательно тождественная подстановка G, а такая, что каждая координатная функция существенно зависит ровно от одной переменной, т. е. $G(x) = (g_1(x) \dots g_n(x))$, $x = x_1 \dots x_n$, $g_i = x_{j_i}^{\sigma_i}$, где $\{j_1, \dots, j_n\} = \{1, \dots, n\}$, $\sigma_i \in \{0, 1\}$ и $x_i^0 = \overline{x_i}$, $x_i^1 = x_i$, $i = 1, \dots, n$. Будем называть эту модификацию алгоритмом $1'$, а класс функций, которые можно таким образом получить, обозначим $\mathcal{K}'_n$.

В [4, утверждение 1] доказано, что обратимых функций на $\mathbb{F}_2^n$, каждая координатная функция которых существенно зависит от двух переменных, не существует ни при каких $n \in \mathbb{N}$. Таким образом, $\mathcal{F}_2 = \varnothing$, следовательно, $\mathcal{K}_2 = \mathcal{K}'_2 = \varnothing$ ввиду $\mathcal{K}_n \subseteq \mathcal{K}'_n \subseteq \mathcal{F}_n$.

Основные результаты данной работы относятся к свойствам компонент (линейных комбинаций координат) функций из классов $\mathcal{K}_n$ и $\mathcal{K}'_n$.

2. Свойства функций класса $\mathcal{K}_n$

Определение 1. Переменная x_i называется *линейной* (или *фиктивной*) для булевой функции $f(x)$, если $f(a) \neq f(b)$ (или соответственно $f(a) = f(b)$) для каждой пары (a, b) соседних по i-й координате векторов.

Утверждение 1. Пусть $F = (f_1 \dots f_n) \in \mathcal{K}_n$. Тогда для каждого $i = 1, \dots, n$ функция f_i имеет единственную линейную переменную — x_i.

Доказательство. Пусть $a, b \in \mathbb{F}_2^n$ — произвольные соседние по i-й координате векторы. Поскольку множество M_i содержит два соседних по i-й координате вектора, имеет место $a, b \in M_i$ или $a, b \notin M_i$. Отсюда ввиду $a_i \neq b_i$ и (1) имеем $f_i(a) \neq f_i(b)$. Значит, x_i — линейная переменная функции f_i.

Для $k \neq i$ выберем соседние по k-й координате векторы $c, d \in M_k$. Тогда $c, d \notin M_i$ ввиду $M_i \cap M_k = \varnothing$. Получим $f_i(c) = c_i = d_i = f_i(d)$. Следовательно, x_k не является линейной переменной для f_i. ■

Пусть $v = (v_1 \dots v_n) \in (\mathbb{F}_2^n)^* = \mathbb{F}_2^n \setminus \{00 \dots 0\}$. *Компонентой функции* $F = (f_1 \dots f_n)$ называется скалярное произведение $vF : \mathbb{F}_2^n \to \mathbb{F}_2$, $vF(x) = \bigoplus\limits_{i=1}^{n} v_i f_i(x) = \bigoplus\limits_{v_i=1} f_i(x)$. Через $\mathrm{w}(v)$ обозначим вес вектора v (количество единиц в нём).

Лемма 1. Пусть $M = \{a_1, a_2, \dots, a_{2k}\} \subseteq \mathbb{F}_2^n$, $k \geqslant 2$ и векторы a_{2i-1}, a_{2i} соседние по j_i-й координате, $i = 1, \dots, k$, $1 \leqslant j_1 < j_2 < \dots < j_k \leqslant n$. Тогда для любого $i \in \{1, \dots, n\}$ множество M нельзя разбить на пары векторов, соседних по i-й координате.

Доказательство. Заметим, что два соседних по j_i-й координате вектора имеют вид $x0y, x1y$ для некоторых $x \in \mathbb{F}_2^{j_i - 1}$, $y \in \mathbb{F}_2^{n - j_i}$. Тогда сумма по модулю 2 всех векторов из M равна $b = e_{j_1} \oplus e_{j_2} \oplus \dots \oplus e_{j_k}$, где e_t — булев вектор длины n и веса 1, имеющий 1 в t-й координате.

Если множество M можно разбить на k пар векторов, соседних по i-й координате, то

$$\bigoplus_{j=1}^{2k} a_j = \begin{cases} e_i, & \text{если } k \text{ нечётное}, \\ 00 \dots 0, & \text{если } k \text{ чётное}, \end{cases}$$

что противоречит равенству $\bigoplus\limits_{j=1}^{2k} a_j = b$ при $k \geqslant 2$. ■

Утверждение 2. Пусть $F = (f_1 \dots f_n) \in \mathcal{K}_n$. Тогда для каждого $v = v_1 \dots v_n \in \in \mathbb{F}_2^n$, такого, что $\mathrm{w}(v) \geqslant 2$, компонентная функция vF не имеет фиктивных и линейных переменных.

Доказательство. Обозначим $V = \{k : v_k = 1\}$, $M = \bigcup\limits_{k \in V} M_k$. Тогда по построению функции F для любого $a = a_1 \dots a_n \in \mathbb{F}_2^n$ имеет место

$$vF(a) = \begin{cases} \bigoplus\limits_{k \in V} a_k \oplus 1, & \text{если } a \in M, \\ \bigoplus\limits_{k \in V} a_k, & \text{если } a \notin M. \end{cases}$$

Докажем, что для любого $i = 1, \dots, n$ переменная x_i не является ни фиктивной, ни линейной для функции vF, т. е. найдутся соседние по i-й координате векторы a, b, такие, что $vF(a) \neq vF(b)$, и найдутся соседние по i-й координате векторы c, d, такие, что $vF(c) = vF(d)$.

С л у ч а й 1: $v_i = 1$. Выберем $a, b \in M_i \subseteq M$. Тогда

$$vF(a) = \bigoplus_{k\in V} a_k \oplus 1 = \bigoplus_{k\in V\setminus\{i\}} a_k \oplus a_i \oplus 1,$$
$$vF(b) = \bigoplus_{k\in V} b_k \oplus 1 = \bigoplus_{k\in V\setminus\{i\}} b_k \oplus b_i \oplus 1 = \bigoplus_{k\in V\setminus\{i\}} a_k \oplus a_i \neq vF(a),$$

последнее равенство здесь верно ввиду того, что a и b соседние по i-й координате.

Заметим, что множество M есть объединение векторов, образующих пары, соседние по координатам с номерами из V. По лемме 1 множество M нельзя разбить на пары векторов, соседних по i-й координате; другими словами, найдётся такой вектор $c \in M$, что соседний ему по i-й координате вектор d не принадлежит M. Получим

$$vF(c) = \bigoplus_{k\in V} c_k \oplus 1 = \bigoplus_{k\in V\setminus\{i\}} c_k \oplus c_i \oplus 1,$$
$$vF(d) = \bigoplus_{k\in V} d_k = \bigoplus_{k\in V\setminus\{i\}} d_k \oplus d_i = \bigoplus_{k\in V\setminus\{i\}} c_k \oplus c_i \oplus 1 = vF(c).$$

С л у ч а й 2: $v_i = 0$. В этом случае пары векторов a, b и c, d меняются местами, а именно: для $c, d \in M_i \not\subseteq M$ получим

$$vF(c) = \bigoplus_{k\in V} c_k, \quad vF(d) = \bigoplus_{k\in V} d_k = \bigoplus_{k\in V} c_k = vF(c).$$

Выберем соседние по i-й координате векторы a, b так, чтобы $a \in M$, $b \notin M$; запишем

$$vF(a) = \bigoplus_{k\in V} a_k \oplus 1, \quad vF(b) = \bigoplus_{k\in V} b_k = \bigoplus_{k\in V} a_k \neq vF(a).$$

Утверждение доказано. ■

3. Свойства функций класса $\mathcal{K}'_n$

Утверждение 3. Пусть $F = (f_1 \dots f_n) \in \mathcal{K}'_n$ и F получена алгоритмом $1'$ из начальной подстановки $G(x) = (x_{j_1}^{\sigma_1} \dots x_{j_n}^{\sigma_n})$. Тогда f_i имеет единственную линейную переменную — x_{j_i}, $i = 1, \dots, n$.

Доказательство. Рассуждения аналогичны приведённым в доказательстве утверждения 1. Для любого $a = a_1 \dots a_n \in \mathbb{F}_2^n$ имеет место

$$f_i(a) = \begin{cases} a_{j_i}^{\sigma_i} \oplus 1, & \text{если } a \in M_{j_i}, \\ a_{j_i}^{\sigma_i} & \text{иначе.} \end{cases}$$

Тогда для всех пар (a, b) соседних по j_i-й координате векторов получаем $a, b \in M_{j_i}$ или $a, b \notin M_{j_i}$, отсюда x_{j_i} — линейная переменная функции f_i; для соседних по j_k-й координате векторов $c, d \in M_{j_k}$ при $k \neq i$ получим $f_i(c) = f_i(d)$, значит, x_{j_k} не является линейной переменной для f_i. ■

Утверждение 4. Пусть $F = (f_1 \dots f_n) \in \mathcal{K}'_n$. Тогда для всех $v = v_1 \dots v_n \in \mathbb{F}_2^n$, таких, что $\mathrm{w}(v) > 2$, компонентная функция vF не имеет фиктивных и линейных переменных.

Доказательство. Аналогично доказательству утверждения 2, только в качестве множества M выберем $M = \bigcup\limits_{k\in V} M_{j_k}$, где $G = (x_{j_1}^{\sigma_1} \dots x_{j_n}^{\sigma_n})$ — начальная подстановка в алгоритме $1'$, из которой получена функция F. ■

Очевидно, что $\mathcal{K}_n \subseteq \mathcal{K}'_n$; в [5] доказано, что алгоритм $1'$ (и, тем более, алгоритм 1) не обладает свойством полноты в том смысле, что существуют функции класса $\mathcal{F}_n$, которые невозможно получить с его помощью. В [6] приведены экспериментальные данные для мощности $|\mathcal{K}_n|$ при $n = 3, \ldots, 6$.

Обозначим $\mathrm{d}(f, g)$ расстояние между булевыми функциями f и g от n переменных: $\mathrm{d}(f, g) = |\{a \in \mathbb{F}_2^n : f(a) \neq g(a)\}|$.

Утверждение 5. $|\mathcal{K}'_n| = 2^n\, n!|\mathcal{K}_n|$.

Доказательство. Поскольку $\mathcal{K}'_2 = \mathcal{K}_2 = \varnothing$, считаем, что $n > 2$.

Множество возможных начальных подстановок алгоритма $1'$ вида $G = \left(x_{j_1}^{\sigma_1} \ldots x_{j_n}^{\sigma_n}\right)$ образует группу Джевонса, порядок которой равен $2^n\, n!$ [7, с. 129]. Для доказательства утверждения надо показать, что алгоритм $1'$, стартуя с разных начальных подстановок, не получит одинаковых функций класса $\mathcal{K}'_n$.

Пусть $F_1, F_2 \in \mathcal{K}'_n$, F_1 получена из подстановки $G_1 = \left(x_{j_1}^{\sigma_1} \ldots x_{j_n}^{\sigma_n}\right)$, F_2 — из подстановки $G_2 = \left(x_{t_1}^{\delta_1} \ldots x_{t_n}^{\delta_n}\right)$ и $G_1 \neq G_2$, т. е. $j_i \neq t_i$ или $\sigma_i \neq \delta_i$ для некоторого $i \in \{1, \ldots, n\}$.

Предположим, что $F_1 = F_2$. По утверждению 3, i-я координата F_1 имеет единственную линейную переменную x_{j_i}, i-я координата F_2 — единственную линейную переменную x_{t_i}, следовательно, $j_i = t_i$, $i = 1, \ldots, n$.

По построению в алгоритме $1'$, для f_{1i} (i-й координаты функции F_1) имеем $\mathrm{d}(f_{1i}, x_{j_i}^{\sigma_i}) = 2$, для f_{2i} (i-й координаты функции F_2) — $\mathrm{d}(f_{2i}, x_{j_i}^{\delta_i}) = 2$. В случае $F_1 = F_2$ и $\sigma_i \neq \delta_i$ получаем $f_{1i} = f_{2i}$ и $\mathrm{d}(f_{1i}, x_{j_i}) = \mathrm{d}(f_{1i}, \bar{x}_{j_i}) = 2$. По неравенству треугольника

$$2^n = \mathrm{d}(x_{j_i}, \bar{x}_{j_i}) \leqslant \mathrm{d}(f_{1i}, x_{j_i}) + \mathrm{d}(f_{1i}, \bar{x}_{j_i}) = 4,$$

что невозможно при $n > 2$. ■

Приведём, следуя [8], определения некоторых криптографических характеристик векторных булевых функций $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$.

Определение 2. *Нелинейностью функции* $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ называется минимальная нелинейность её компонент:

$$N_F = \min_{v \in (\mathbb{F}_2^m)^*} N_{vF} = \min_{v \in (\mathbb{F}_2^m)^*} \mathrm{d}(vF, \mathcal{A}_n) = \min_{v \in (\mathbb{F}_2^m)^*} \min_{g \in \mathcal{A}_n} \mathrm{d}(vF, g),$$

где $\mathcal{A}_n = \{ax \oplus b : a \in \mathbb{F}_2^n, b \in \mathbb{F}_2\}$ — класс всех аффинных функций от n переменных.

Степень функции F — максимальная степень её компонент (совпадает с максимальной степенью координатных функций):

$$\deg F = \max_{v \in (\mathbb{F}_2^m)^*} \deg vF.$$

Аннигилятором булевой функции $f(x)$ называется булева функция $g(x) \neq \mathrm{const}\, 0$, такая, что $f(x)g(x) = \mathrm{const}\, 0$; класс всех аннигиляторов функции f обозначается $\mathrm{AN}(f)$; алгебраическая иммунность функции f — минимальная степень среди всех аннигиляторов функций f и $f \oplus 1$:

$$\mathrm{AI}(f) = \min_{g \in \mathrm{AN}(f) \cup \mathrm{AN}(f \oplus 1)} \deg g.$$

Компонентная алгебраическая иммунность функции F — минимальная алгебраическая иммунность её компонент:

$$\mathrm{AI}_{\mathrm{comp}}(F) = \min_{v \in (\mathbb{F}_2^m)^*} \mathrm{AI}(vF).$$

Утверждение 6. Для функции $F \in \mathcal{K}'_n$ выполняются следующие свойства:

1) $N_F = 2$;
2) $\deg F = n - 1$;
3) $\mathrm{AI}_{\mathrm{comp}}(F) = 2$;
4) если $v \in \mathbb{F}_2^n$ и $\mathrm{w}(v) \leqslant 2^{n-3}$, то нелинейность компонентной функции vF равна $N_{vF} = 2\mathrm{w}(v)$; в частности, это верно для любого v при $n \geqslant 6$; для всех $v \neq 11111$ при $n = 5$ и т. д.

Доказательство.

1) В [6] доказано, что $N_{f_i} = 2$ для всех координат f_i функции F, поэтому $N_F \leqslant 2$; $N_F \neq 0$, так как по утверждению 4 компонентные функции vF не имеют линейных и фиктивных переменных, следовательно, не являются аффинными; $N_F \neq 1$, так как все компонентные функции обратимой функции F являются уравновешенными [8, Proposition 2], т. е. имеют вес 2^{n-1} — чётное число при $n > 1$, вес функций класса $\mathcal{A}_n$ также чётный, а две функции чётного веса не могут отличаться друг от друга на одном наборе.

2) Следует из доказанного в [6] равенства $\deg f_i = n - 1$ для $i = 1, \ldots, n$.

3) В [6] доказано, что $\mathrm{AI}(f_i) = 2$, $i = 1, \ldots, n$. Докажем, что $\mathrm{AI}(vF) \neq 1$ для всех $v \in (\mathbb{F}_2^n)^*$. Предположим противное: для функции $h \in \{vF, vF \oplus 1\}$ существует аннигилятор $g \in \mathcal{A}_n$. Ввиду уравновешенности функций h и g и равенства $gh = \mathrm{const}\, 0$ получаем, что $h = \overline{g}$, т. е. $h \in \mathcal{A}_n$, что неверно.

4) По построению $\mathrm{d}(vF, vx) = \left| \bigcup\limits_{v_k=1} M_{j_k} \right| = 2\mathrm{w}(v)$, где $vx = \bigoplus\limits_{i=1}^{n} v_i x_i$ и $G = (x_{j_1}^{\sigma_1} \ldots x_{j_n}^{\sigma_n})$ — начальная подстановка в алгоритме $1'$, из которой получена функция F. Поэтому $N_{vF} \leqslant 2\mathrm{w}(v)$. Предположим, что существует функция $g \in \mathcal{A}_n$, $g \neq vx$, такая, что $\mathrm{d}(g, vF) < 2\mathrm{w}(v)$. По неравенству треугольника получим

$$2^{n-1} = \mathrm{d}(g, vx) \leqslant \mathrm{d}(g, vF) + \mathrm{d}(vF, vx) < 2\mathrm{w}(v) + 2\mathrm{w}(v) = 4\mathrm{w}(v),$$

что неверно при $\mathrm{w}(v) \leqslant 2^{n-3}$.

Утверждение доказано. ■

Замечание 1. Эксперименты показывают, что равенство $N_{vF} = 2\mathrm{w}(v)$ выполняется и для $n = 5$ и $v = 11111$.

Автор выражает благодарность Е. Е. Трифоновой и Н. М. Киселевой, чьи компьютерные эксперименты помогли сформулировать свойства функций класса $\mathcal{K}'_n$.

ЛИТЕРАТУРА

1. *Agibalov G. P.* Substitution block ciphers with functional keys // Прикладная дискретная математика. 2017. № 38. С. 57–65.
2. *Agibalov G. P. and Pankratova I. A.* Asymmetric cryptosystems on Boolean functions // Прикладная дискретная математика. 2018. № 40. С. 23–33.
3. *Agibalov G. P.* ElGamal cryptosystems on Boolean functions // Прикладная дискретная математика. 2018. № 42. С. 57–65.
4. *Панкратова И. А.* Об обратимости векторных булевых функций // Прикладная дискретная математика. Приложение. 2015. № 8. С. 35–37.
5. *Pankratova I. A.* Construction of invertible vectorial Boolean functions with coordinates depending on given number of variables // Материалы Междунар. науч. конгресса по информатике: Информационные системы и технологии. Республика Беларусь, Минск, 24–27 окт. 2016. Минск: БГУ, 2016. С. 519–521.

6. *Карпова Л. А., Панкратова И. А.* Свойства координатных функций одного класса подстановок на $\mathbb{F}_2^n$ // Прикладная дискретная математика. Приложение. 2017. № 10. С. 38–40.
7. *Логачев О. А., Сальников А. А., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004.
8. *Carlet C.* Vectorial Boolean Functions for Cryptography. Cambridge: Cambridge University Press, 2010. 93 p.

REFERENCES

1. *Agibalov G. P.* Substitution block ciphers with functional keys. Prikladnaya Diskretnaya Matematika, 2017, no. 38, pp. 57–65.
2. *Agibalov G. P. and Pankratova I. A.* Asymmetric cryptosystems on Boolean functions. Prikladnaya Diskretnaya Matematika, 2018, no. 40, pp. 23–33.
3. *Agibalov G. P.* ElGamal cryptosystems on Boolean functions. Prikladnaya Diskretnaya Matematika, 2018, no. 42, pp. 57–65.
4. *Pankratova I. A.* Ob obratimosti vektornykh bulevykh funktsiy [On the invertibility of vector Boolean functions]. Prikladnaya Diskretnaya Matematika. Prilozhenie, 2015, no. 8, pp. 35–37. (in Russian)
5. *Pankratova I. A.* Construction of invertible vectorial Boolean functions with coordinates depending on given number of variables. Proc. CSIST'16, Minsk, BSU Publ., 2016, pp. 519–521.
6. *Karpova L. A. and Pankratova I. A.* Svoystva koordinatnykh funktsiy odnogo klassa podstanovok na $\mathbb{F}_2^n$ [Properties of coordinate functions for a class of permutations on $\mathbb{F}_2^n$]. Prikladnaya Diskretnaya Matematika. Prilozhenie, 2017, no. 10, pp. 38–40. (in Russian)
7. *Logachev O. A., Sal'nikov A. A., and Yashchenko V. V.* Bulevy funktsii v teorii kodirovaniya i kriptologii [Boolean Functions in Coding Theory and Cryptology]. Moscow, MCCME Publ., 2004, 472 p. (in Russian)
8. *Carlet C.* Vectorial Boolean Functions for Cryptography. Cambridge: Cambridge University Press, 2010. 93 p.