УДК 681.3.06

**Ю.В. СТАСЕВ, А.А. КУЗНЕЦОВ, А.А. ЮКАЛЬЧУК**

***Харьковский университет Воздушных Сил, Украина***

# РАЗРАБОТКА И ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИ СТОЙКИХ БУЛЕВЫХ ФУНКЦИЙ

Рассматриваются методы построения криптографически стойких булевых функций, основанные на применении развитого аппарата булевой алгебры. Исследуются криптографические свойства сформированных высоко нелинейных булевых функций.

**криптографически стойкие булевы функции, булева алгебра**

## Постановка проблемы в общем виде и анализ литературы

Построение современных алгоритмов криптографической обработки информации связывают с многократным (итеративным) применением простых и хорошо изученных криптографических примитивов: блоков линейного рассеивания и нелинейных блоков подстановки (S-блоков) [1 – 3].

Наиболее обоснованным подходом к построению нелинейных блоков подстановки является развитый аппарат булевой алгебры, применение которого позволяет представить узлы нелинейных замен в виде набора специальным образом подобранных булевых функций [4, 5]. В работах [6, 7] предложен метод построения булевых функций стремящихся по показателю нелинейности к верхней границе. **Целью статьи** является исследование криптографических свойств сформированных таким образом булевых функций.

## Критерии и показатели эффективности криптографических функций

Основными показателями стойкости булевых функций являются сбалансированность, нелинейность, корреляционный иммунитет, критерий распространения (строгий лавинный критерий) и алгебраическая степень. Введем основные термины и определения [4, 5].

*Булевой функцией* $f$ от $n$ переменных является функция, осуществляющая отображение из поля $GF(2^n)$ всех двоичных векторов $x = (x_1, \ldots, x_n)$ длины $n$ в поле $GF(2)$. Обычно булевы функции представляются в алгебраической нормальной форме и рассматриваются как сумма произведений составляющих координат. Поле $GF(2^n)$ состоит из $2^n$ векторов $\alpha_i$: $\alpha_0 = (0,\ldots,0,0)$, $\alpha_1 = (0,...,0,1)$,..., $\alpha_{2^n-1} = (1,...,1,1)$, $\alpha_i \in V_n$, где $V_n$ – векторное пространство в $GF(2^n)$. Последовательность функции $f$ является *сбалансированной*, если ее (0,1)-последовательность ((1,–1)-последовательность) содержит одинаковое количество нулей и единиц (единиц и минус единиц). Функция $f$ является сбалансированной, если сбалансирована ее последовательность.

*Аффинной функцией* $f$ называется функция вида $f = a_1x_1 \oplus \ldots \oplus a_nx_n \oplus c$, где $a_j, c \in GF(2)$, $j = 1, 2, ..., n$. Функция $f$ называется *линейной*, если $c = 0$.

*Весом Хэмминга* вектора $\alpha$ ((0,1)-последовательности $\alpha$), обозначаемым как $W(\alpha)$, является количество единиц в векторе (последовательности).

*Расстоянием Хэмминга* $d(f,g)$ между последовательностями двух функций $f$ и $g$ является количество позиций, в которых различны последовательности этих функций.

*Нелинейность функции* $N_f$ – минимальное расстояние Хэмминга $N_f$ между функцией $f$ и всеми

аффинными функциями над $GF(2^n)$:

$$N_f = min\ \{d(f,\varphi)\},$$

где $\varphi$ - множество аффинных функций.

Для произвольной функции $f$ нелинейность $N_f$ над $GF(2^n)$ может достигать:

$$N_f \le 2^{n-1} - 2^{n/2-1}.$$

Предельный показатель нелинейности для сбалансированных функций:

$$N_f \ge 2^{4t-1} - 2^{2t-1} - 2^t,\ n = 4t. \qquad (1)$$

Функция $f$ обладает *корреляционным иммунитетом* порядка $k$, если выходная последовательность функции $y \in Y$ статистически не зависит от любого подмножества из $k$ входных координат:

$$\forall \{x_1, \ldots, x_k\}\ P(y \in Y / \{x_1, \ldots, x_k\} \in X) = P(y \in Y).$$

Эквивалентное определение корреляционного иммунитета в терминах преобразования Уолша [4, 5]: функция $f$ над полем $GF(2^n)$ имеет корреляционный иммунитет порядка $k$, $КИ(k)$, если ее преобразование Уолша удовлетворяет равенству $F(\omega) = 0$ для всех $\omega \in V_n$ таких, что $1 \le W(\omega) \le k$:

$$\forall \omega \in V_n,\ F(\omega) = 0,\ \ КИ(f) = k.$$

*Преобразование Уолша* $F(\omega)$ функции $f$ над полем $GF(2^n)$ определяется как принимающая действительные значения функция

$$F(\omega) = 2^{-n} \sum\nolimits_x (-1)^{f(x) \oplus \langle \omega, x \rangle},$$

где $\omega \in V_n$, $f(x)$, $\langle \omega, x \rangle \in N$ ($\langle \omega, x \rangle$ – скалярное произведение $w_1x_1 \oplus \ldots \oplus w_nx_n$) .

Функция $f$ над полем $GF(2^n)$ удовлетворяет:

– *критерию распространения относительно вектора* $\alpha$, $КР(\alpha)$, если функция $f(x) \oplus f(x \oplus \alpha)$ является сбалансированной, $x \in V_n$, где $x = (x_1, x_2, \ldots, x_n)$:

$$P(f(x) = f(x \oplus \alpha)) = 0{,}5;$$

– *критерию распространения степени* $k$, $КР(k)$, если удовлетворяется критерий распространения относительно всех векторов $\alpha \in V_n$ при $1 \le W(\alpha) \le k$:

$$P(f(x) = f(x \oplus \alpha)) = 0{,}5; \quad \forall \alpha : 1 \le W(\alpha) \le k.$$

*Алгебраическая степень* $deg(f)$ является степенью самого длинного слагаемого функции, представленной в алгебраической нормальной форме.

*Коэффициент корреляции* функции со множеством всех аффинных функций определяется как

$$c_i(f, L_w) = 2^{-n} \sum_x (-1)^{f(x)} (-1)^{wx} = 2^{-n}\ \hat{F}(w).$$

Функция $f$ над $GF(2^n)$ называется бент-функцией, если

$$2^{-n/2} \sum_{x \in V_n} (-1)^{f(x) \oplus \langle \beta, x \rangle} = \pm 1$$

для всех $\beta \in V_n$.

К дополнительным показателям эффективности относят следующие.

*Коэффициент равномерной минимизации корреляции*

$$k_{рм} = \frac{k_{гр}}{r \cdot c_{ср}},$$

где $k_{гр}$ – граничный коэффициент корреляции; $r$ – удельный вес ненулевых значений коэффициентов корреляции; $c_{ср}$ – среднее значение коэффициента корреляции;

$$r = \left| \frac{B}{2^n} - 2^{n-1} \right|; \qquad c_{ср} = \frac{\sum_{i=1}^{2^n} c_i}{2^n};$$

$$k_{гр} = \begin{cases} \dfrac{\left|1 - 2^n\right| \cdot (c_n + c_{n+2})}{2}, & n - четное; \\ \left|1 - 2^n\right| \cdot c_n, & n - нечетное. \end{cases}$$

где $B$ – число ненулевых значений коэффициентов корреляции; $c_i$ – значение коэффициента корреляции; $c_n$ – коэффициент корреляции бент-функции над $V_n$; $c_{n+2}$ – коэффициент корреляции бент-функции над $V_{n+2}$.

*Абсолютное значение корреляции функции:*

$$C_f = max\ |c(f, \ell_i)|,\ \ell_i \in L,$$

где $\ell_i$, $L$ – линейная функция и множество всех линейных функций, соответственно.

## Исследование свойств высоконелинейных булевых функций

В работах [6, 7] предложен метод построения булевых функций стремящихся по показателю нелинейности к верхней границе (1). Проведем исследо-

вания криптографических свойств булевых функций, сформированных с использованием предложенного метода, сравним с известными методами (рис. 1).

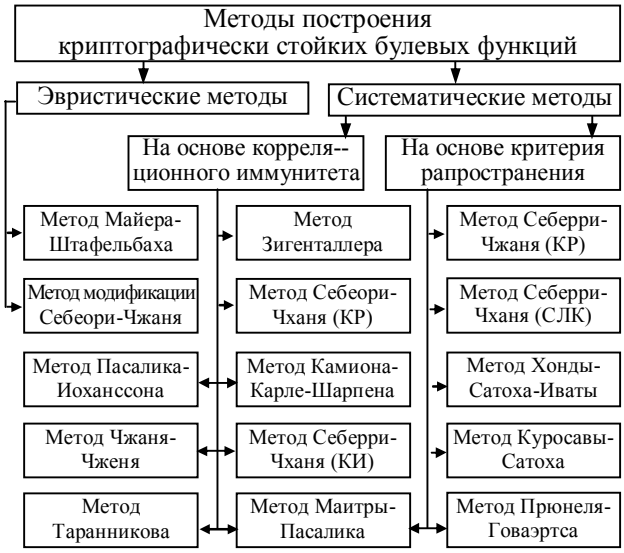


Рис. 1. Методы построения высоко нелинейных булевых функций

В качестве прототипа разработанного метода использовался эвристический метод модификации высоко нелинейных последовательностей. В табл. 1. представлены показатели стойкости функций, полученных при использовании разработанного метода и метода-прототипа.

Таблица 1

Показатели стойкости функций

| | Метод модификации | Разраб. метод |
|---|---|---|
| $N_f$ | $N_f \geq 2^{4t-1} - 2^{2t-1} - 2^t$, $n = 4t$ | $N_f \geq 2^{n-1} - 2^{n/2}$ |
| $KP(k)$ | не обсуждается | $KP(1)$ |
| $deg(f)$ | не обсуждается | $n - 1$ |

Как видно из приведенной таблицы, основным преимуществом разработанного метода является то, что при сохранении основного показателя стойкости – высокой нелинейности, удается построить булевы функции, удовлетворяющие критерию распространения степени 1 и обладающие максимально достижимой для сбалансированных функций алгебраической степенью ($n - 1$).

В табл. 2 приведены сравнительные характеристики нелинейности разработанного и известных методов (построенных на основе концепции критерия распространения).

Таблица 2

Сравнительные характеристики нелинейности

| | $V_4$ | $V_6$ | $V_8$ | $V_{10}$ | $V_{12}$ | $V_{14}$ | $V_{16}$ |
|---|---|---|---|---|---|---|---|
| Верхняя граница | 4 | 26 | 118 | 494 | 2014 | 8126 | 32638 |
| Разработанный метод | 4 | 26 | 116 | 492 | 2010 | 8120 | 32624 |
| Наилучшие известные методы | 4 | 24 | 112 | 480 | 1984 | 8064 | 32512 |

Приведенные данные свидетельствуют, что среди методов, основанных на концепции критерия распространения, разработанный метод достигает наивысшей нелинейности и стремится к верхней границе.

Высокая нелинейность свидетельствует о высокой степени замешивания данных, что определяет стойкость преобразований.

На рис. 2 приведены сравнительные характеристики алгебраической степени функций разработанного и известных методов (построенных на основе концепции критерия распространения).

Как видно из приведенных данных, разработанный метод и метод Куросавы-Сатоха достигают верхней границы алгебраической степени и по данному показателю являются более предпочтительными, чем остальные методы.

Для полноты сравнения проведем исследования нелинейности и алгебраической степени функций, построенных в соответствии с разработанным методом и наиболее известными методами, построенными на основе концепции корреляционного иммунитета (табл. 3) над $V_8$. Отметим, что для корреляционно-иммунных функций справедливо неравенство:

$$k + deg(f) \leq n - 1, \qquad (2)$$

где $k$ – степень корреляционного иммунитета. Таким образом, при фиксированном $n$ разработчики корреляционно-иммунных функций всегда вынуждены искать компромисс между алгебраической степенью и степенью корреляционного иммунитета.

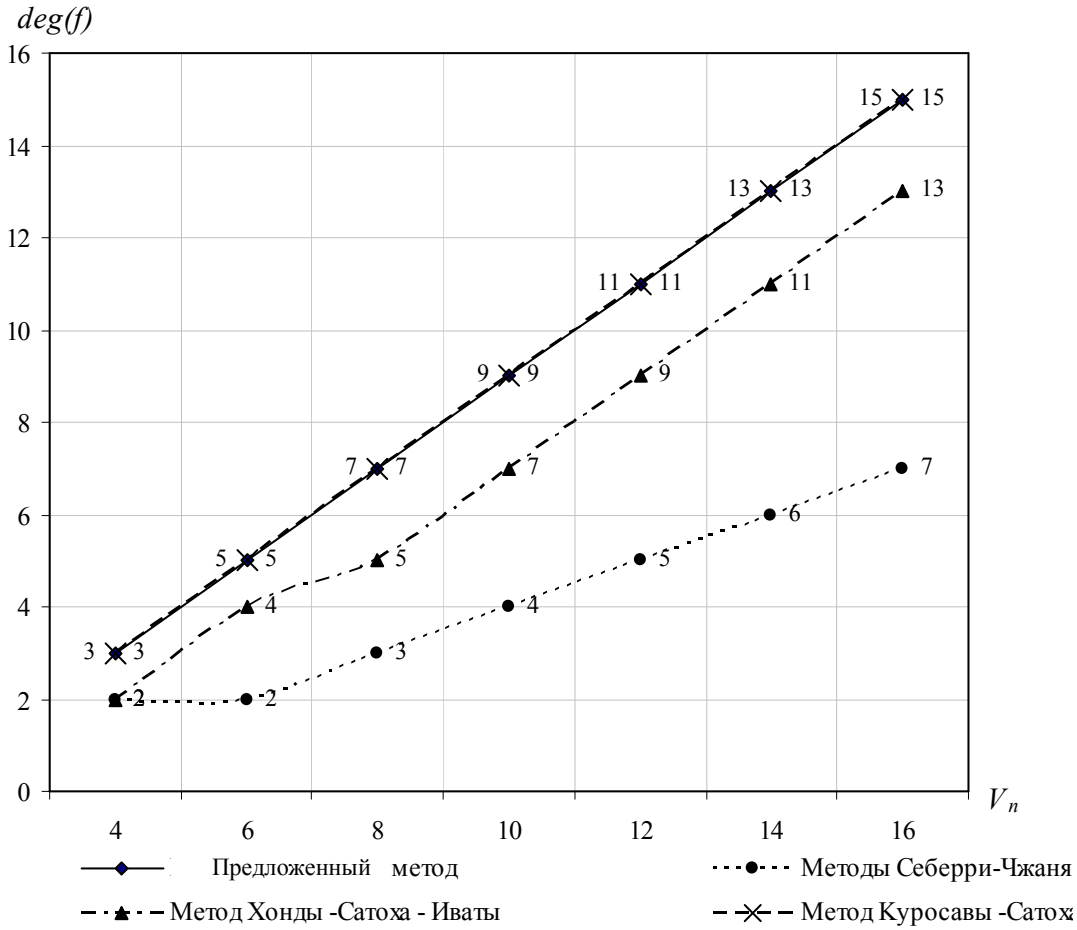


Рис. 2. Алгебраическая степень формируемых функций

Таблица 3

Сравнительные характеристики нелинейности и алгебраической степени

| | Нелинейность, $N_f$ | Алгебраическая степень, $deg(f)$ |
|---|---|---|
| Разработанный метод | 116 | 7 ($KP(1)$) |
| Метод Кларка | 116<br>112 | 7 ($k = 0$)<br>5 ($k = 2$) |
| Метод Кавута | 116<br>114 | 7 ($k = 0$)<br>7 ($k = 0$) |
| Метод Станича – Сунга | 112 | |
| Метод Карле – Шарпена | 112 | |
| Метод Маитры | 116 | |
| Метод Маити – Йоханссона | 116 | 6 ($k = 1$) |
| Метод Чжаня – Чженя | $\geq 112$ | |

Как видно из приведенной таблицы, корреляционно-иммунные функции также имеют высокие показатели стойкости. Отличительной их чертой является то, что максимально достижимого на сегодняшний день значения нелинейности ($N_f = 116$ при $N_{max} = 118$ для сбалансированных функций) и верхней границы алгебраической степени $deg(f) = 7$ они могут достичь, в соответствии с выражением (2), только в том случае, если степень корреляционного иммунитета будет равна $k = 0$. В этом случае, строго говоря, мы не можем говорить о корреляционно-имунных функциях как таковых. В целом можно заключить, что разработанный метод по таким показателям, как нелинейность и алгебраическая степень, не уступает корреляционно-иммунным функциям и имеет перед ними преимущество в терминах характеристик распространения.

В табл. 4 представлена комплексная оценка сравнения комбинированного метода и известных методов для случая $n = 8$ (построенных на основе концепции критерия распространения).

Рассмотрим также дополнительные показатели стойкости. Коэффициент равномерной минимиза-

ции корреляции $k_{рм}$ и абсолютное значение корреляции $C_f$ определяют спектральные свойства функций и отражают их корреляционные свойства. Коэффициент равномерной минимизации корреляции определяет, во сколько раз, по сравнению с бент-функцией [4, 5], ухудшилась равномерность спектра функции. Абсолютное значение корреляции функции, как следует из названия, определяет значение максимальной корреляции функции с некоторой аффинной функцией.

На рис. 3 – 8 представлены спектральные свойства бент-функций, функций, построенных в соответствии с предлагаемым и известными методами построения нелинейных булевых функций, а также функций, используемых в блоках подстановок симметричных шифров (СШ).

Таблица 4

Граничные показатели стойкости функций

| | Нелинейность, $N_f$ | Степень критерия распространения, $KP(k)$ | Алгебраическая степень, $deg(f)$ |
|---|---|---|---|
| Разработанный метод | 116 ($N_{max} = 118$) | $KP(1)$ | 7 ($deg_{max} = 7$ ) |
| Метод Себерри – Чжаня (*КР*) | 112 | $KP(5)$ | 3 |
| Метод Себерри – Чжаня (*СЛК*) | 112 | $KP(1)$ | 3 |
| Метод Хонды – Сатоха – Иваты | не обсуждается | $KP(2)$ | 5 |
| Метод Куросавы – Сатоха | 112 | $KP(1)$ | 7 |

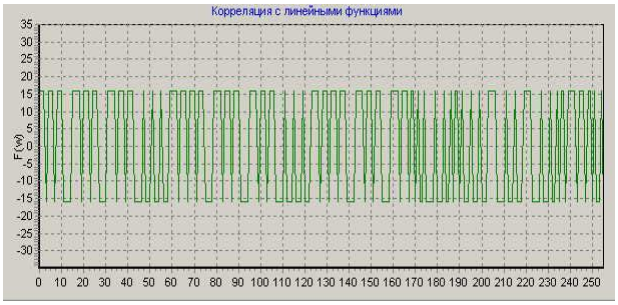


Рис.3. Спектральные свойства бент-функции

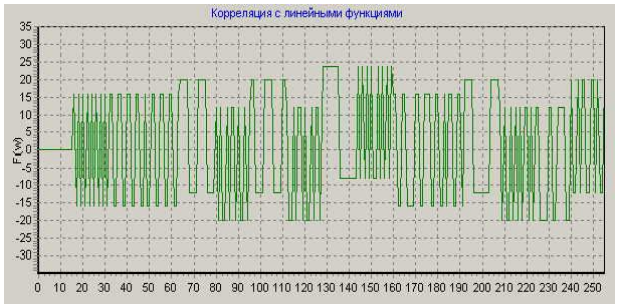


Рис. 4. Спектральные свойства функции, построенной в соответствии с разработанным методом


Рис. 5. Спектральные свойства функции, построенной в соответствии с методом Себерри – Чжаня (*СЛК*)

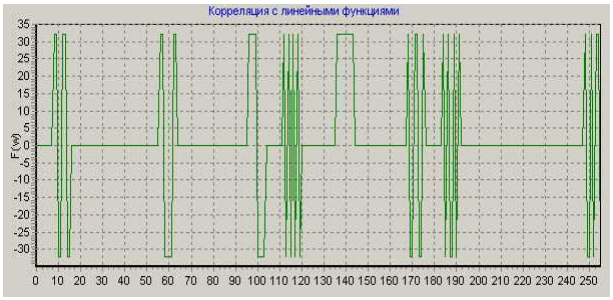


Рис. 6. Спектральные свойства функции, построенной в соответствии с методом Себерри – Чжаня (*КИ*)

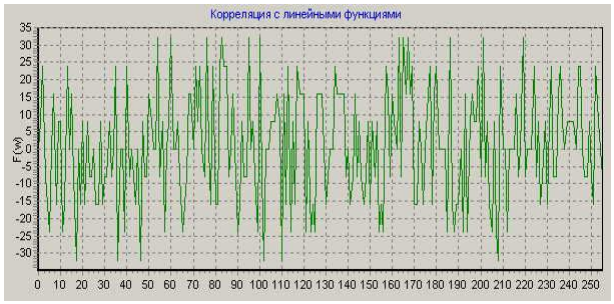


Рис. 7. Спектральные свойства функции, используемой в блоке подстановки СШ Sober t-32, Turing

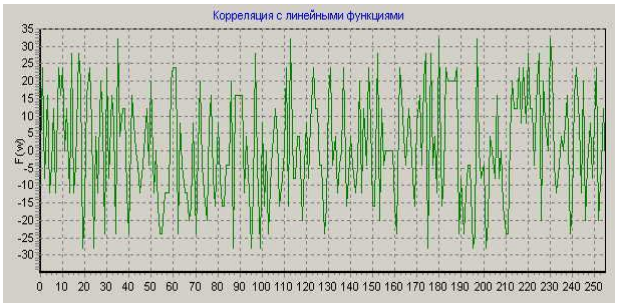


Рис. 8. Спектральные свойства функции, используемой в блоке подстановки СШ Rijendael

Таблица 5

Дополнительные показатели стойкости нелинейных функций

| | $N_f$ | $deg(f)$ | $k_{рм}$ | $C_f$ |
|---|---|---|---|---|
| Бент-функция | 120 | 4 | 1 | 0.0625 |
| Разработанный метод | 116 | 7 | 1,0678 | 0,09375 |
| Метод Себерри – Чжаня (*КР*) | 112 | 3 | 1,9893 | 0,125 |
| Метод Себерри – Чжаня (*СЛК*) | 112 | 3 | 1.3434 | 0,125 |
| Метод Себерри – Чжаня (*КИ*) | 112 | 4 | 1,9882 | 0,125 |
| Функции в СШ Sober t-32, Turing | 112 | 6 | 1,2348 | 0,125 |
| Функции в СШ AES Rijndael | 112 | 7 | 1,1847 | 0,125 |

В табл. 5 представлены дополнительные показатели стойкости бент-функций, функций, построенных в соответствии с предлагаемым и известными методами построения нелинейных булевых функций, а также функций, используемых в блоках подстановок СШ.

Приведенные данные показывают, что разработанный метод имеет наивысшие показатели нелинейности и алгебраической степени: все известные методы уступают по нелинейности и только метод Куросавы – Сатоха имеет аналогичную алгебраическую степень, проигрывая при этом разработанному методу по нелинейности. Значительно более высокую степень критерия распространения, в отличие от разработанного метода, имеет метод Себерри – Чжаня (*КР*), однако он уступает по нелинейности и имеет критически низкую алгебраическую степень. Обсуждая дополнительные показатели стойкости, можно отметить, что функции, полученные в соответствии с разработанным методом, имеют наилучшие спектральные характеристики: их коэффициенты корреляции наиболее равномерно минимизированы, абсолютные значения корреляции имеют наинизшие значения по сравнению с функциями, построенными согласно известных методов. На основе проведенных исследований можно сделать **вывод** о том, что функции, построенные в соответствии с разработанным методом построения, имеют высокие показатели стойкости и превосходят по данным показателям известные функции.

## Литература

1. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – М.: Изд-во стандартов, 1989. – 20 с.

2. National Institute of Standards and Technology, “FIPS-46-3: Data Encryption Standard.” Oct. 1999. – [Электр. ресурс]. – Режим доступа: http://csrc.nist.gov/publications/fips.

3. National Institute of Standards and Technology, “FIPS-197: Advanced Encryption Standard.” Nov. 2001. – [Электр. ресурс]. – Режим доступа: //csrc.nist.gov/publications/fips.

4. Fuller J., Millan W. On linear redundancy in S-boxes // Proceedings of Fast Software Encryption – FSE’03 (T. Johansson, ed.), Lecture Notes in Computer Science, Springer-Verlag, 2003. – [Электр. ресурс]. – Режим доступа: http://eprint.iacr.org/2002/111.

5. Maier W., Staffelbach O. Nonlinearity criteria for cryptographic functions // Advances in Cryptology – EUROCRYPT’89, vol.434, Lecture Notes in Computer Science, Springer-Verlag, 1990. – P. 549-562.

6. Кузнецов А.А., Избенко Ю.А., Юкальчук А.А. Теоретическое обоснование возможности разработки комбинированного метода построения высоко нелинейных булевых функций // Вісник НТУ “ХПІ”: Збірник наукових праць. – Х.: НТУ “ХПІ”, 2004. – № 19. – С. 115-120.

7. Кузнецов О.О., Ізбенко Ю.А., Юкальчук А.А. Метод побудови високо нелінійних булевих функцій // IV НТК молодих вчених Харківського військового університету 16-17 квітня 2004 р. – Х.: ХВУ, 2004. – С. 60.

*Поступила в редакцию 27.01.2006*

**Рецензент:** д-р техн. наук, проф. В.И. Долгов, Харьковский национальный университет радиоэлектроники.