ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)

УДК 004.056.55

М.И. Мазурков, д-р техн. наук, проф.,
Н.А. Барабанов, инженер,
А.В. Соколов, магистр,
Одес. нац. политехн. ун-т

ГЕНЕРАТОР КЛЮЧЕВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ОСНОВЕ ДУАЛЬНЫХ ПАР БЕНТ-ФУНКЦИЙ

М.І. Мазурков, М.О. Барабанов, А.В. Соколов. **Генератор ключових послідовностей на основі дуальних пар бент-функцій.** Пропонується конструкція генератора псевдовипадкових послідовностей на основі високонелінійних булевих бент-функцій, який може бути використаний для генерації високоякісних ключів блокових шифрів в якості елемента алгоритмів потокового шифрування і для інших застосувань сучасної криптографії. Показано, що побудований генератор має практично важливі криптографічні і стохастичні властивості.
Ключові слова: генератор ключових послідовностей, бент-функція, алгоритм потокового шифрування.

М.И. Мазурков, Н.А. Барабанов, А.В. Соколов. **Генератор ключевых последовательностей на основе дуальных пар бент-функций.** Предлагается конструкция генератора псевдослучайных последовательностей на основе высоконелинейных булевых бент-функций, который может быть использован для генерации высококачественных ключей блочных шифров в качестве элемента алгоритмов поточного шифрования и для других приложений современной криптографии. Показано, что построенный генератор обладает практически важными криптографическими и стохастическими свойствами.
Ключевые слова: генератор ключевых последовательностей, бент-функция, алгоритм поточного шифрования.

M.I. Mazurkov, N.A. Barabanov, A.V. Sokolov. **The key sequences generator based on bent functions dual couples.** The design of pseudo-random sequence generator based on highly nonlinear Boolean bent functions is proposed . The generator can be used to generate high-quality block ciphers keys, as a part of the stream encryption algorithms and in other applications of modern cryptography. It is shown that the constructed generator has practically important cryptographic and stochastic properties.
Keywords: key sequences generator, bent function, stream encryption algorithm.

Генераторы псевдослучайных ключевых последовательностей (ГПКП) являются основным элементом многих современных криптографических систем, определяющим криптостойкость и быстродействие современных устройств криптографического преобразования информации. Важную роль ГПКП играют в алгоритмах поточного шифрования (АПШ), генераторах ключей блочных шифров и некоторых криптографических приложениях [1].

Например, ГПКП в АПШ генерирует поток битов z_i, которые используются в качестве псевдослучайной ключевой последовательности $\Gamma = \{z_i\}$ (далее Γ-последовательности). Зашифрованное сообщение $y_1, y_2, ..., y_i, ..., y_k$ и исходное $x_1, x_2, ..., x_i, ..., x_k$ связаны с Γ-последовательностью соотношениями, однозначно определяющими операцию шифрования и дешифрования [1],

$$\begin{cases} y_i = x_i \oplus z_i \\ x_i = y_i \oplus z_i \end{cases}, \quad i = \overline{1,k}\,. \tag{1}$$

При этом свойства ГПКП полностью определяют криптостойкость и скоростные характеристики АПШ. Таким образом, построение высококачественного и скоростного ГПКП фактически эквивалентно построению высококачественного и скоростного АПШ.

Одним из наиболее эффективных методов генерации Γ-последовательностей является применение математического аппарата булевых функций [2], что позволяет дифференцирован-

ный выбор структурных элементов ГПКП, соответствующих тем или иным криптографическим и стохастическим свойствам. Наилучшие булевы функции для построения ГПКП — широко известные бент-функции от n переменных [2].

Бинарная, т.е. полученная в результате однозначного преобразования между двоичным и бинарным кодом $0 \leftrightarrow +$, $1 \leftrightarrow -$, последовательность $\mathbf{B}$ называется бент-функцией, если ее спектр Уолша-Адамара равномерно распределен по модулю [3]

$$\mathbf{W}_B(\omega) = \mathbf{BA} = \{\pm 2^{n/2}\},\ \omega = \overline{0, 2^n - 1}, \tag{2}$$

где $\mathbf{A}$ — матрица Уолша-Адамара порядка 2^n [3].

Применение бент-функций позволяет максимально эффективно противостоять атакам, основанным на низкой линейной сложности математического описания ГПКП, а также атаке Берлекэмпа-Мэсси, основанной на раскрытии закона генерации Г-последовательности при известных нескольких ее периодах [4].

Современный подход к формированию Г-последовательностей обычно сводится к использованию регистров сдвига с линейной обратной связью (РСЛОС) для формирования входного сигнала n переменных блока, реализующего булеву бент-функцию $\mathbf{B} = f(x_1, x_2, ..., x_i, ..., x_n)$, выход которого подключен к блоку суммирования по $\mathrm{mod}\,2$. Таким образом, современные АПШ, содержащие ГПКП, основанные на применении свойств булевых бент-функций, можно изобразить схематически (рис. 1) [2].

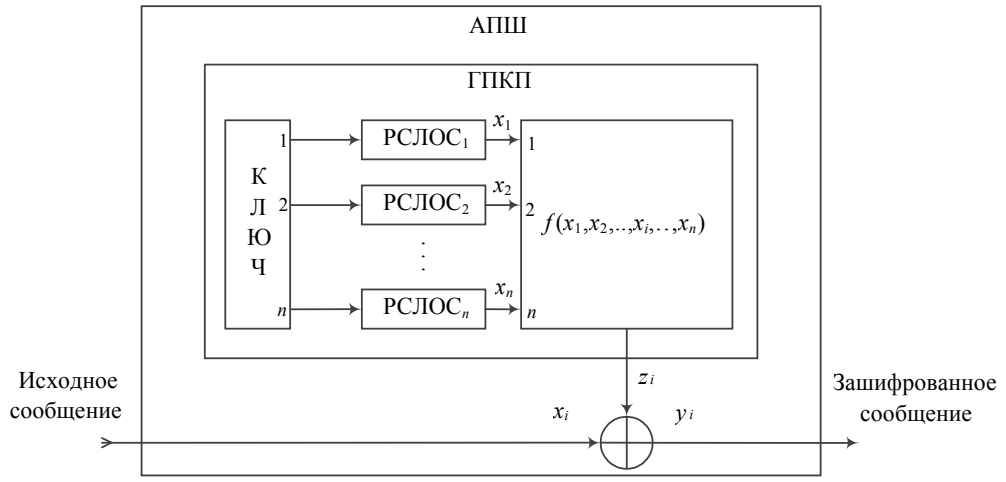


Рис. 1. Схема АПШ, содержащая ГПКП на основе бент-функции $f(x_1, x_2, ..., x_i, ..., x_n)$

Применение подобных АПШ, основанных на свойстве максимальной нелинейности бент-функций [2], позволяет добиться высоких показателей криптографического качества Г-последовательностей, что дает возможность эффективно противостоять атакам линейного криптоанализа, а также атаке Берлекэмпа-Мэсси [2]. Тем не менее, проведенные исследования показали, что стохастические свойства Г-последовательности на выходе ГПКП (рис. 1) неудовлетворительны, что открывает в АПШ возможности для атак частотного криптоанализа. Действительно, пусть в АПШ для построения РСЛОС использованы генераторные полиномы

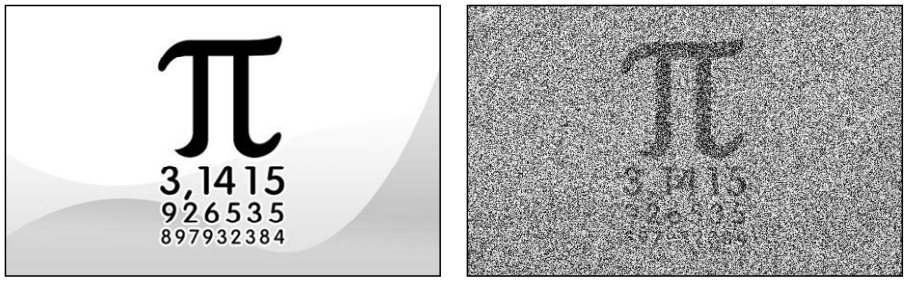
$$\begin{cases} h_1(x) = x^{13} + x^{12} + x^{10} + x^9 + 1, \\ h_2(x) = x^{17} + x^{14} + 1, \\ h_3(x) = x^{19} + x^{18} + x^{17} + x^{14} + 1, \\ h_4(x) = x^{23} + x^{18} + 1 \end{cases} \tag{3}$$

ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)

и булева бент-функция от четырех переменных

$$f(x_1,x_2,x_3,x_4)=x_1+x_2+x_3+x_2x_3+x_4+x_1x_4=\{0110101011000000\}. \quad (4)$$

Приведен пример использования рассмотренного АПШ (см. рисунок 1) для преобразования графического сообщения **M** в виде трехмерной битовой матрицы размера $[450,300,8]$, определяющей цвет (градации серого) пикселей изображения (рис. 2). В соответствии со схемой АПШ и с учетом (3), (4) сформирована Γ-последовательность, далее сформирована ключевая трехмерная битовая матрица **Z** размера $[450,300,8]$ путем последовательного заполнения ее позиций элементами Γ-последовательности. После чего произведено шифрование в соответствии с (1).



а *б*

Рис. 2. Пример использования АПШ [2] для шифрования графического сообщения **M** *: исходное изображение (а), зашифрованное изображение (б)*

Анализ изображений показывает, что недостаточное стохастическое качество генерируемой АПШ Γ-последовательности приводит к недостаточному сокрытию информации, что позволяет несанкционированный доступ к исходному сообщению. И даже по внешнему виду зашифрованного изображения (рис. 2, *б*) возможно получить некоторые сведения об исходном без каких-либо специальных методов криптоанализа.

Изучение принципов работы АПШ [2] позволяет сделать вывод относительно причин столь низкого стохастического качества Γ-последовательности, которые кроются в структурных свойствах применяемых булевых бент-функций $f(x_1,x_2,...,x_i,...,x_n)$.

Нетрудно заметить, что условие (2) приводит к несбалансированной структуре бент-функции, т.е. количество нулевых символов $K^{(0)}$ отличается от количества единичных символов $K^{(1)}$, причем величина разбаланса

$$\Delta=\left|K^{(0)}-K^{(1)}\right|=\mathbf{W}(0)=\pm 2^{n/2}. \quad (5)$$

Поскольку последовательности, генерируемые РСЛОС при достаточно большой длине периода $N=2^{\deg\{h(x)\}}-1$, где $\deg\{h(x)\}$ — степень генераторного первообразного полинома, определяющего закон обратной связи РСЛОС, можно считать сбалансированными, то, учитывая (5), ГПКП (см. рисунок 2) всегда будет генерировать Γ-последовательность, имеющую существенный разбаланс, пропорциональный Δ, что ведет к катастрофическому ухудшению стохастических свойств Γ-последовательности и соответственно АПШ в целом.

Предлагается схема ГПКП, устраняющая влияние разбаланса Δ бент-функций четырех переменных, вес Хэмминга которых может быть $wt_1(f(x_1,x_2,x_3,x_4))=6$ либо $wt_2(f(x_1,x_2,x_3,x_4))=10$. Анализ показывает, что устранение недостатка, связанного с разбалансом Γ-последовательности, генерируемой ГПКП, может лежать в плоскости дихотомического разделения полного класса бент-функций Ψ, мощности $|\Psi|=896$ на подклассы ψ и $\overline{\psi}$, $|\psi|=|\overline{\psi}|=448$ таким образом, чтобы один класс можно было получить из другого путем применения операции отрицания. Другими словами, подкласс $\overline{\psi}$ будет содержать множество дуаль-

ных к множеству ψ бент функций, связанных равенством $\mathbf{W}_{f_{\bar{\psi}}} = 2^{n/2}(-1)^{f_\psi}$. Одновременное применение бент-функций из множества ψ и $\bar{\psi}$ для построения ГПКП приводит к компенсации разбаланса (5) и позволяет получить на выходе Γ-последовательность, свойства которой значительно превосходят свойства Γ-последовательности, генерируемой ГПКП (см. рисунок 1). Исходя из приведенных свойств бент-функций подклассов ψ и $\bar{\psi}$, построен АПШ на основе дуальных пар бент-функций четырех переменных (рис. 3), удовлетворяющий критериям случайности [4].

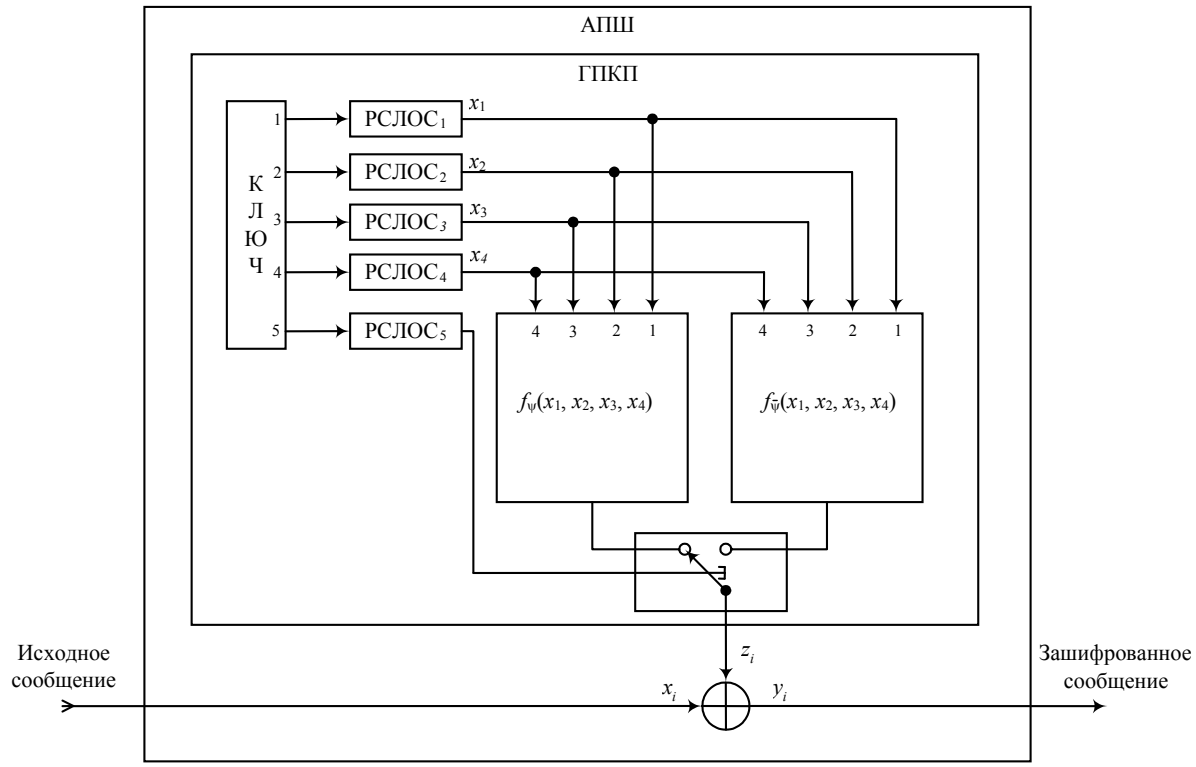


Рис. 3 Схема предлагаемого АПШ на основе дуальной пары бент-функций $\{f_\psi(x_1,x_2,x_3,x_4),\ f_{\bar{\psi}}(x_1,x_2,x_3,x_4)\}$

Шаги работы АПШ.

Шаг 1. Выбор $n+1=5$ различных первообразных полиномов $h_1(x)$, $h_2(x)$, $h_3(x)$, $h_4(x)$, $h_5(x)$ с попарно различными периодами, каждый из которых больше двух.

Шаг 2. Выбор дуальной пары булевых бент-функций $f_\psi(x_1,x_2,x_3,x_4)$ и $f_{\bar{\psi}}(x_1,x_2,x_3,x_4)$ из множества ψ и $\bar{\psi}$, соответственно.

Шаг 3. Задание ключей $K=\{K_1,K_2,K_3,K_4,K_5\}$, где длина каждого элемента ключа $|K_i| = \deg(f_i(x))$, $K_i \neq \{0,0,...,0\}$; число возможных ключей определяется степенями выбранных на Шаге 1 полиномов и может быть масштабировано в зависимости от необходимого числа уровней защищенности

$$|K| = \prod_{i=1}^{n-1}(2^{\deg(h_i(x))}-1). \qquad (6)$$

Шаг 4. Инициализация схемы следующим образом: значения ключа K_i записываются в регистр РСЛОС$_i$; на каждом последующем такте генерируются значения x_1,x_2,x_3,x_4, посту-

ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)

пающие на входы блоков бент-функций $f_{\psi}(x_1,x_2,x_3,x_4)$ и $f_{\bar{\psi}}(x_1,x_2,x_3,x_4)$, выходы которых подключены к ключу, которым управляет РСЛОС$_5$, на каждом такте осуществляющий коммутацию выходов блоков бент-функций в соответствии с законом, определяемым первообразным полиномом $h_5(x)$.

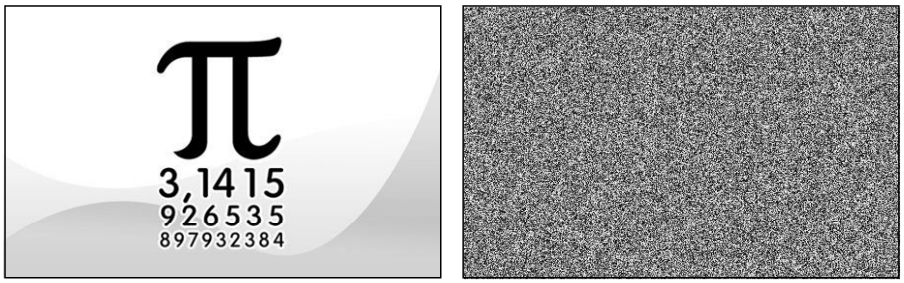
Проведенные исследования предлагаемого АПШ с генераторными полиномами (3) и коммутирующим полиномом

$$h_5(x) = x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^5 + x^4 + x^3 + x^2 + 1, \tag{7}$$

а также бент-функциями

$$\begin{cases} f_{\psi}(x_1,x_2,x_3,x_4) = x_1 + x_2 + x_3 + x_2x_3 + x_4 + x_1x_4 = \{0110101011000000\}; \\ f_{\bar{\psi}}(x_1,x_2,x_3,x_4) = 1 + x_1 + x_1x_2 + x_1x_3 + x_3x_4 = \{1011111010110001\}, \end{cases} \tag{8}$$

показывают, что он удовлетворяет всем стохастическим тестам [4]. На рис. 4 приведен пример шифрования.



а *б*

Рис. 4. Пример использования предлагаемого АПШ для шифрования графических сообщений: исходное изображение (а), зашифрованное изображение (б)

Число уровней защиты Υ разработанного АПШ определяется размером ключа $|K|$ (6), мощностью подклассов бент-функций $|\psi| = |\bar{\psi}| = 448$, а также количеством первообразных генераторных полиномов степени k $|\mathbf{V}_k| = \varphi(2^k - 1)/k$, где φ — фи-функция Эйлера. Таким образом, для рассматриваемого примера число уровней защиты информации определяется соотношением

$$\begin{aligned} \Upsilon = |K| \cdot |\psi| \cdot |\bar{\psi}| \cdot |V_{13}| \cdot |V_{17}| \cdot |V_{19}| \cdot |V_{23}| \cdot |V_{12}| = (2^{13} - 1)(2^{17} - 1)(2^{19} - 1) \times \\ \times (2^{23} - 1)(2^{12} - 1) \cdot 448 \cdot 448 \cdot 630 \cdot 7710 \cdot 27594 \cdot 356960 \cdot 144 \approx 2{,}67 \cdot 10^{49} \approx 2^{165}, \end{aligned} \tag{9}$$

причем, данное значение является легко масштабируемым (управляемым).

При этом ключ состоит из 84 бит исходных состояний РСЛОС, 18 бит для передачи номера применяемой дуальной пары бент-функций и 63 бит для передачи номера используемого генераторного полинома. Итого размер ключа составляет 165 бит при периоде последовательности, который не может быть даже измерен при современном состоянии развития вычислительной техники.

Проведен сравнительный анализ стохастических характеристик [4] предложенного ГПКП для длины гаммы 2^{14} бит (см. таблицу, где знак “+” означает, что данный критерий выполняется, а знак “–” — не выполняется).

Анализ подтверждает высокое криптографическое и стохастическое качество предложенного ГПКП. При этом, в отличие от AES [1,6] и RC4[1], он обладает значительно более простой

аппаратной реализацией, а в отличие от генератора MATLAB (Вихрь Мерсенна) — существенно большим числом уровней защиты.

Сравнительный анализ стохастических характеристик предложенного ГПКП

№ п/п	Критерии качества	Предложенный ГПКП	Генератор [2]	Генератор MATLAB [5]	АПШ RC4 [1]	Алгоритм AES, 10 раундов [6]
1	Сбалансированность	8250/ 8134	10210/ 6174	8143/ 8241	8082/8302	7552/ 8832
2	Случайный внешний вид сигнала	+	+	+	+	+
3	Равномерное распределение гистограммы	+	–	+	+	+
4	Случайное распределение на плоскости	+	–	+	+	–
5	2-х граммное распределение	+	–	+	+	–
6	3-х граммное распределение	+	–	+	+	–
7	4-х граммное распределение	+	–	+	+	–
8	Монотонность	+	+	+	+	+
9	Линейная сложность	+	+	+	+	+
10	Максимальный боковой лепесток битовой АКФ	~0,02	~0,1	~0,02	~0,02	1
11	Спектральный тест	+	–	+	+	–

Основные результаты проведенных исследований:

— получила дальнейшее развитие теория генерации псевдослучайных ключевых последовательностей на основе свойств максимальной нелинейности полного класса бент-функций, в рамках чего разработан новый ГПКП на основе дуальной пары полного класса бент-функций четырех переменных;

— сравнительный анализ стохастических свойств известных ранее ГПКП и разработанного показал высокое качество генерируемых им Г-последовательностей, что в сочетании с существенным числом уровней защиты позволяет рекомендовать его для практического применения в задачах криптографии;

— полученные данные о защищенности АПШ на основе разработанного ГПКП путем шифрования и дешифрования графической информации позволили экспериментально подтвердить его эффективность.

Таким образом, разработанный ГПКП на основе дуальных пар бент-функций может быть рекомендован к использованию в АПШ, генераторах ключей и других приложениях, требующих использования высококачественных Г-последовательностей.

Литература

1. Рябко, Б.Я. Основы современной криптографии и стеганографии / Б.Я. Рябко, А.Н. Фионов. — М.: Горячая линия — Телеком, 2010. — 232 с.
2. Агафонова, И. В. Криптографические свойства нелинейных булевых функций / И.В. Агафонова // Семинар по дискрет. гармон. анализу и геометр. моделированию. — СПб.: DHA & CAGD, 2007. — С. 1—24.
3. Мазурков, М.И. Регулярные правила построения полного класса бент-последовательностей длины 16 / М.И. Мазурков, А.В. Соколов. — Пр. Одес. політехн. ун-ту. — Одеса, 2013. — Вип. 2(41). — С. 227 — 231.
4. Иванов, М.А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей / М.А. Иванов, И.В. Чугунков. — М.: КУДИЦ-ОБРАЗ, 2003. — 240 с.

ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)

5. Matsumoto, M. A 623-dimensionally equidistributed uniform pseudorandom number generator [Electronic resource] / M.Matsumoto. — Hiroshima, 1998. — http://www.math.sci.hiroshima-u.ac.jp/~m-mat/MT/ARTICLES/mt.pdf. — 02.07.2013.
6. FIPS 197. Advanced encryption standard [Electronic resource]. — USA, Maryland: NIST, 2001. — http://csrc.nist.gov/publications/ — 03.10.2012

References

1. Ryabko, B.Ya. Osnovy sovremennoy kriptografii i steganografii [Foundations of modern cryptography and steganography] / B. Ya. Ryabko, A. N. Fionov. — Moscow, 2010. — 232 p.
2. Agafonova, I.V. Kriptograficheskie svoystva nelineynykh bulevykh funktsiy [Cryptographic properties of nonlinear Boolean functions] / I.V. Agafonova // Seminar po diskretnomu garmonicheskomu analizu i geometricheskomu modelirovaniyu [Seminar on Discrete Harmonic Analysis and Geometric Simulation]. — St. Petersburg, 2007. — pp. 1 — 24.
3. Mazurkov, M.I. Regulyarnye pravila postroeniya polnogo klassa bent-posledovatel`nostey dliny 16 [The regular rules of constructing a complete class of bent-sequences of length 16] / M.I. Mazurkov, A.V. Sokolov. — Trudy Odes. nac. politekhn. un-ta [Proc. of Odessa Nat. Polytech. Univ.]. — Odessa, 2013. — #2 (41). — pp. 227 — 231.
4. Ivanov, M.A. Teoriya, primenenie i otsenka kachestva generatorov psevdosluchaynykh posledovatel`nostey [The theory, application and estimation of quality of pseudorandom sequences generators] / M.A. Ivanov, I.V. Chugunkov. — Moscow, 2003. — 240 p.
5. Matsumoto, M. A 623-dimensionally equidistributed uniform pseudorandom number generator [Electronic resource] / M.Matsumoto. — Hiroshima, 1998. — http://www.math.sci.hiroshima-u.ac.jp/~m-mat/MT/ARTICLES/mt.pdf. — 02.07.2013.
6. FIPS 197. Advanced encryption standard [Electronic resource]. — USA, Maryland: NIST, 2001. — http://csrc.nist.gov/publications/ — 03.10.2012

Рецензент д-р техн. наук, проф. Одес. нац. политехн. ун-та Кобозева А.А.

Поступила в редакцию 2 сентября 2013 г.