



Общероссийский математический портал

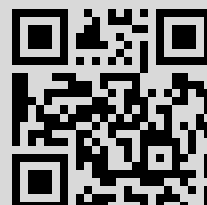
А. В. Соколов, И. В. Цевух, О существовании бинарных С-кодов длины $N = 32$ с заданным значением пик-фактора спектра Уолша–Адамара, *ПФМТ*, 2017, выпуск 2(31), 91–95

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 178.136.56.65

23 сентября 2017 г., 15:21:26



УДК 510.644

О СУЩЕСТВОВАНИИ БИНАРНЫХ С-КОДОВ ДЛИНЫ $N = 32$ С ЗАДАННЫМ ЗНАЧЕНИЕМ ПИК-ФАКТОРА СПЕКТРА УОЛША – АДАМАРА

А.В. Соколов, И.В. Цевух

Одесский национальный политехнический университет

ON THE EXISTENCE OF BINARY C-CODES OF LENGTH $N = 32$ WITH A PREDETERMINED VALUE OF PAPR OF WALSH – HADAMARD SPECTRUM

A.V. Sokolov, I.V. Tsevukh

Odessa National Polytechnic University

Проведена спектральная классификация последовательностей длины $N = 32$ в соответствии со структурой и пик-фактором их спектра Уолша – Адамара в результате чего выделено 40 различных видов спектральных наборов. Рассчитаны предельно достижимые мощности С-кодов с заданным значением пик-фактора. Учитывая взаимосвязь пик-фактора спектра Уолша – Адамара и расстояния нелинейности двоичной последовательности длины $N = 32$, установлены мощности классов данных последовательностей, обладающих заданным значением расстояния нелинейности.

Ключевые слова: преобразование Уолша – Адамара, пик-фактор, расстояние нелинейности.

The spectral classification of sequences of length $N = 32$ in accordance with the structure and the value of the PAPR (Peak-to-Average Power Ratio) of Walsh – Hadamard spectrum resulting in 40 different spectral sets was performed. The maximal achievable cardinality of C-codes with a predetermined value of PAPR was calculated. Taking into account the interconnection between PAPR value of the Walsh – Hadamard spectrum and nonlinearity distance of binary sequence of length $N = 32$, the cardinalities of classes of sequences with a determined value of nonlinearity distance were found.

Keywords: Walsh – Hadamard transform, PAPR, nonlinearity distance.

Памяти д.т.н, проф.
Михаила Ивановича Мазуркова

Введение

Дальнейшее развитие беспроводных сетей передачи данных, в частности, четвертого и пятого поколений во многом связывают с совершенствованием и развитием технологии кодового разделения каналов CDMA. В качестве своего базиса технология кодового разделения каналов использует систему ортогональных функций, в роли которых могут выступать специально подобранные кодовые последовательности.

Одной из перспективных модификаций технологии CDMA является MC-CDMA (Multi Code Code Division Multiple Access), где в качестве набора ортогональных функций выступают функции Уолша [1].

В системе MC-CDMA вектор бинарных данных $B = (b_i)$, $i = 0, N - 1$ подвергается ортогональному преобразованию. Каждый бит данных b_i изменяет знак одной из N ортогональных функций дискретного времени $h_i(t)$, а выход является суммой этих N модулированных функций. Тогда передаваемый сигнал представляет собой спектр Уолша – Адамара последовательности B

$$S_B(t) = \sum_{i=0}^{N-1} b_i h_i(t).$$

Таким образом, выходной сигнал можно представить как произведение вектора B , составленного из бит данных, поступивших от каждого пользователя и матрицы Адамара H

$$S = BH,$$

где матрица Адамара H формируется в соответствии со следующим рекуррентным правилом [2]

$$H_{2^k} = \begin{bmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{bmatrix}, \quad H_1 = [1].$$

Обладая многочисленными преимуществами, такими как высокая помехоустойчивость, гибкость распределения пропускной способности системы среди абонентов, экономичность и хорошая электромагнитная совместимость, технология MC-CDMA не лишена недостатков. Один из самых значимых недостатков технологии MC-CDMA заключается в высоких значениях пик-фактора применяемых в ней сигналов. Данное обстоятельство приводит к неэффективному использованию мощности передатчика, нелинейным искажениям и, как следствие, удорожанию стоимости применяемого оборудования при снижении потенциально достижимой помехоустойчивости.

Пик-фактор применяемых в системе сигналов определяется величиной пиковых значений трансформант Уолша – Адамара [3]

$$\kappa = \frac{P_{\max}}{P_{cp}} = \frac{1}{N} \max_t \left\{ |S_B(t)|^2 \right\}, \quad (0.1)$$

где P_{\max} – пиковая мощность сигнала $S_B(t)$; P_{cp} – средняя мощность сигнала $S_B(t)$; N – длина сигнала $S_B(t)$.

В настоящий момент предложено значительное количество методов борьбы с высоким значением пик-фактора сигналов, представляющих собой трансформанты преобразования Уолша – Адамара, однако, наиболее перспективным является метод, основанный на использовании строго обоснованного математического аппарата, который позволяет снизить значения пик-фактора – применение С-кодов.

1 С-код

Определение 1.1 [3]. С-кодом, или кодом постоянной амплитуды называется множество кодовых слов, обладающих заданным, фиксированным для каждого кодового слова значением пик-фактора κ .

Применение С-кода сводится к замене подаваемых на вход кодера сообщений b_j длины m на такие последовательности c_i длины n , которые обладали бы наименьшим значением пик-фактора κ (рисунок 1.1).

Одним из возможных базисов для построения С-кодов являются бент-последовательности, обладающие равномерным по модулю спектром Уолша – Адамара. Тем не менее, бент-последовательности существуют только для длин $N = 2^k$, $k = 2, 4, 6, 8, \dots$ [4], в то время как практика использования технологии MC-CDMA требует большего ассортимента различных длин сигналов и, соответственно, реализуемого числа кодовых каналов.

В работах [5]–[7] построены полные множества векторов длин $N = 20$, $N = 24$ и $N = 28$, обладающих минимальным значением пик-фактора. В работе [8] разработан регулярный метод синтеза последовательностей длины $N = 32$, обладающих минимальным значением пик-фактора.

Тем не менее, с практической точки зрения, востребованными оказываются кодовые слова С-кода, гарантированно обладающие значением пик-фактора, не превосходящим некоторую заданную величину, что диктует необходимость исследования возможности построения С-кодов с заданным значением пик-фактора $\kappa \leq \kappa_0$.

Целью настоящей статьи является исследование возможности построения С-кодов длины $N = 32$ наибольшей возможной мощности при заданном значении пик-фактора κ_0 .

Изучение характеристик полного кода длины $N = 32$ сопряжено со значительными вычислительными трудностями, т. к. подразумевает рассмотрение множества из $J = 2^{32} = 4\,294\,967\,296$ элементов. Данное обстоятельство диктует необходимость разработки конструктивного метода исследования возможных значений пик-фактора.

2 Полином Жегалкина

Одной из лучших теоретических баз для построения такого метода является математический аппарат полиномов Жегалкина (алгебраической нормальной формы).

Рассмотрим двоичную последовательность длины $N = 32$

$$T = \{t_0, t_1, \dots, t_{31}\}, t_i \in \{0, 1\}, i = 0, 1, \dots, N - 1, \quad (2.1)$$

например,

$$T = \{11110000011001111101001101111110\}. \quad (2.2)$$

Определение 2.1 [9]. Полиномом Жегалкина $\Phi(x_1, x_2, \dots, x_k)$ или алгебраической нормальной формой (АНФ) последовательности T называется многочлен $k \leq \log_2 N$ переменных с коэффициентами $a_i \in \{0, 1\}$, где в качестве умножения принята операция конъюнкции, а в качестве сложения – операция суммирования по модулю 2

$$\Phi(x_1, x_2, \dots, x_k) = \bigoplus_{i=0}^{N-1} a_i X_i^s,$$

где X_i^s – термы полинома Жегалкина степени $s = wt\{X\}$; wt – вес Хэмминга.

Рассмотрим все возможные термы для последовательностей T длины $N = 32$

$$\begin{aligned} X_0 &= \{00000\} \quad 0 & X_1 &= \{00001\} \quad x_5 \\ X_2 &= \{00010\} \quad x_4 & X_3 &= \{00011\} \quad x_4 x_5 \\ X_4 &= \{00100\} \quad x_3 & X_5 &= \{00101\} \quad x_3 x_5 \\ X_6 &= \{00110\} \quad x_3 x_4 & X_7 &= \{00111\} \quad x_3 x_4 x_5 \\ X_8 &= \{01000\} \quad x_2 & X_9 &= \{01001\} \quad x_2 x_5 \\ X_{10} &= \{01010\} \quad x_2 x_4 & X_{11} &= \{01011\} \quad x_2 x_4 x_5 \\ X_{12} &= \{01100\} \quad x_2 x_3 & X_{13} &= \{01101\} \quad x_2 x_3 x_5 \\ X_{14} &= \{01110\} \quad x_2 x_3 x_4 & X_{15} &= \{01111\} \quad x_2 x_3 x_4 x_5 \\ X_{16} &= \{10000\} \quad x_1 & X_{17} &= \{10001\} \quad x_1 x_5 \end{aligned}$$

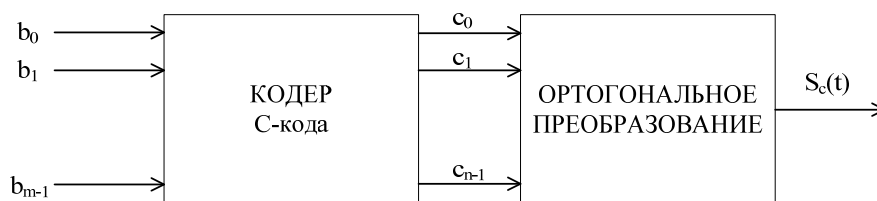


Рисунок 1.1 – Схема кодера С-кода

$$\begin{aligned}
 X_{18} &= \{10010\} x_1 x_4 & X_{19} &= \{10011\} x_1 x_4 x_5 \\
 X_{20} &= \{10100\} x_1 x_3 & X_{21} &= \{10101\} x_1 x_3 x_5 \\
 X_{22} &= \{10110\} x_1 x_3 x_4 & X_{23} &= \{10111\} x_1 x_3 x_4 x_5 \\
 X_{24} &= \{11000\} x_1 x_2 & X_{25} &= \{11001\} x_1 x_2 x_5 \\
 X_{26} &= \{11010\} x_1 x_2 x_4 & X_{27} &= \{11011\} x_1 x_2 x_4 x_5 \\
 X_{28} &= \{11100\} x_1 x_2 x_3 & X_{29} &= \{11101\} x_1 x_2 x_3 x_5 \\
 X_{30} &= \{11110\} x_1 x_2 x_3 x_4 & X_{31} &= \{11111\} x_1 x_2 x_3 x_4 x_5
 \end{aligned}
 \tag{2.3}$$

Коэффициенты $a_i = \{a_0, a_1, \dots, a_{N-1}\}$ могут быть найдены путем выполнения преобразования Рида – Маллера, т. е. путем умножения исходной последовательности T (2.1) на матрицу Рида – Маллера A_v , которую можно определить с помощью следующего рекуррентного правила

$$A_0 = [1], A_v = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \otimes A_{v-1} = \begin{bmatrix} A_{v-1} & 0 \\ A_{v-1} & A_{v-1} \end{bmatrix},$$

где \otimes – произведение Кронекера.

Для нашего примера коэффициенты преобразования Рида – Маллера будут иметь вид

$$\begin{aligned}
 \{a_i\} &= T \cdot A_{32} = \\
 &= \{10001000111010010011000100101110\},
 \end{aligned}$$

тогда полином Жегалкина будет иметь вид

$$\begin{aligned}
 \varphi &= 1 + x_3 + x_4 + x_1 x_4 + x_2 x_4 + x_3 x_4 + \\
 &+ x_1 x_2 x_3 x_4 + x_2 x_5 + x_1 x_2 x_5 + x_1 x_2 x_3 x_5 + \\
 &+ x_2 x_4 x_5 + x_3 x_4 x_5 + x_1 x_3 x_4 x_5 + x_2 x_3 x_4 x_5.
 \end{aligned}$$

Подставляя в полученный полином значения X_i , в точности получаем исходную последовательность T .

3 Метод исследования значений пик-фактора

Метод исследования значений пик-фактора основан на следующем предположении:

Предположение. Суммирование булевой функции с любой аффинной булевой функцией не меняет структуру её спектра, а лишь приводит к перестановке или знаковому кодированию его элементов.

На основе данного предположения запишем метод поиска различных спектральных структур для векторов длины 32 в виде шагов.

Шаг 1. Рассмотрим последовательность $\{a_i\}$ коэффициентов АНФ булевой функции пяти переменных. Учитывая (2.3), обнулیم такие позиции в ней, которые соответствуют аффинным

функциям (таблица 3.1). В таблице 3.1 приняты следующие обозначения: **0** – обнуленное значение, **?** – значение, изменяемое в процессе поиска.

Шаг 2. Производим последовательное изменение оставшихся позиций, придавая им значения 0 или 1.

В случае длины исходной последовательности $N = 32$ на данном этапе необходимо рассмотреть $2^{32}/2^6 = 2^{26} = 67\,108\,864$ различные последовательности, что является вычислительно осуществимым.

Шаг 3. Из множества последовательностей, полученных на **Шаге 2**, выбираем такие, которые обладают различной спектральной структурой.

Результаты использования предложенного метода относительно последовательностей длины $N = 32$ приведены в таблице 3.2 в виде спектральной классификации, где для каждого возможного набора рассчитаны значения пик-фактора k в соответствии с (0.1).

Отметим, что значение пик-фактора последовательностей напрямую связано с уровнем их нелинейности, который является ключевой характеристикой при использовании той или иной последовательности в криптографических приложениях.

Основным критерием, по которому производится исследование нелинейных свойств двоичных последовательностей длины $N = 2^k$ является расстояние нелинейности, которое определяется как степень удаления данной последовательности от аффинного кода $\{A_j\}$ [10]

$$N_f = \text{dist}(T, A_j), \quad j = 1, 2^{k+1}$$

С другой стороны известно, что расстояние нелинейности произвольной бинарной последовательности T длины $N = 2^k$ определяется через её спектральные коэффициенты преобразования Уолша – Адамара с помощью следующего соотношения

$$N_f = 2^{k-1} - \frac{1}{2} \max_{v \in Z_2^k} |S_T(v)|. \tag{3.1}$$

Таким образом, каждый сконструированный С-код можно рассматривать как множество кодовых слов, обладающих заданным значением нелинейности, определяемым в соответствии с (3.1). Значения нелинейности N_f для каждого класса последовательностей указаны в таблице 3.2.

Таблица 3.1 – Позиции аффинных термов в последовательности длины $N = 32$

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
0	0	0	?	0	?	?	?	0	?	?	?	?	?	?	?	0	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?
0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Таблица 3.2 – Возможные спектральные структуры векторов длины $N = 32$

№ п/п	№ класса	Набор	Пик-фактор κ	N_f	Мощность
1	1.1.	{32(1), 0(31)}	32	0	64
2	2.1.	{30(1), 2(31)}	28.125	1	2 048
3	3.1.	{28(1), 4(15), 0(16)}	24.5	2	31 744
4	4.1.	{26(1), 6(7), 2(24)}	21.125	3	317 440
5	5.1.	{24(1), 8(7), 0(24)}	18	4	79 360
6	5.2.	{24(1), 8(3), 4(16), 0(12)}	18	4	2 222 080
7	6.1.	{22(1), 10(3), 6(4), 2(24)}	15.125	5	2 222 080
8	6.2.	{22(1), 10(1), 6(10), 2(20)}	15.125	5	10 665 984
9	7.1.	{20(1), 12(3), 4(12), 0(16)}	12.5	6	1 111 040
10	7.2.	{20(1), 8(6), 4(15), 0(10)}	12.5	6	28 442 624
11	7.3.	{20(1), 12(1), 4(30)}	12.5	6	1 777 664
12	7.4.	{20(1), 12(1), 8(4), 4(14), 0(12)}	12.5	6	26 664 960
13	8.1.	{18(1), 14(3), 2(28)}	10.125	7	317 440
14	8.2.	{18(1), 14(1), 10(2), 6(6), 2(22)}	10.125	7	26 664 960
15	8.3.	{18(1), 10(3), 6(9), 2(19)}	10.125	7	142 213 120
16	8.4.	{18(1), 10(1), 6(15), 2(15)}	10.125	7	28 442 624
17	8.5.	{18(1), 14(1), 6(12), 2(18)}	10.125	7	17 776 640
18	9.1.	{16(1), 12(2), 8(4), 4(14), 0(11)}	8	8	213 319 680
19	9.2.	{16(2), 12(2), 4(14), 0(14)}	8	8	3 809 280
20	9.3.	{16(2), 8(4), 4(16), 0(10)}	8	8	19 998 720
21	9.4.	{16(2), 8(8), 0(22)}	8	8	1 666 560
22	9.5.	{16(4), 0(28)}	8	8	9 920
23	9.6.	{16(1), 12(1), 8(6), 4(15), 0(9)}	8	8	284 426 240
24	9.7.	{16(1), 8(12), 0(19)}	8	8	17 776 640
25	9.8.	{16(1), 8(8), 4(16), 0(7)}	8	8	106 659 840
26	10.1.	{14(3), 10(1), 6(7), 2(21)}	6.125	9	20 316 160
27	10.2.	{14(2), 10(4), 6(4), 2(22)}	6.125	9	26 664 960
28	10.3.	{14(2), 10(2), 6(10), 2(18)}	6.125	9	319 979 520
29	10.4.	{14(1), 10(5), 6(7), 2(19)}	6.125	9	426 639 360
30	10.5.	{14(1), 10(3), 6(13), 2(15)}	6.125	9	568 852 480
31	11.1.	{12(4), 8(4), 4(12), 0(12)}	4.5	10	115 548 160
32	11.2.	{12(4), 4(28)}	4.5	10	31 744 000
33	11.3.	{12(6), 4(10), 0(16)}	4.5	10	888 832
34	11.4.	{12(3), 8(6), 4(13), 0(10)}	4.5	10	426 639 360
35	11.5.	{12(2), 8(8), 4(14), 0(8)}	4.5	10	666 624 000
36	11.6.	{12(1), 8(10), 4(15), 0(6)}	4.5	10	170 655 744
37	12.1.	{10(6), 6(10), 2(16)}	3.125	11	449 748 992
38	12.2.	{10(4), 6(16), 2(12)}	3.125	11	106 659 840
39	13.1.	{8(12), 4(16), 0(4)}	2	12	13 332 480
40	13.2.	{8(16), 0(16)}	2	12	14 054 656
Всего:			4294967296 = 2^{32}		

Таблица 3.3 – Максимально возможные мощности С-кодов длины $N = 32$

κ_0	2	3.125	4.5	6.125	8
J_1	27 387 136	556 408 832	1 412 100 096	1 362 452 480	647 666 880
J_{\max}	27 387 136	583 795 968	1 995 896 064	3 358 348 544	4 006 015 424
κ_0	10.125	12.5	15.125	18	21.125
J_1	215 414 784	57996288	12888064	2301 440	317 440
J_{\max}	4 221 430 208	4 279 426 496	4 292 314 560	4 294 616 000	4 294 933 440
κ_0	24.5	28.125	32	–	–
J_1	31 744	2 048	64	–	–
J_{\max}	4 294 965 184	4 294 967 232	4 294 967 296	–	–

В таблице 3.2 для представления спектральных наборов принята следующая форма: число перед круглыми скобками характеризует абсолютное значение спектрального коэффициента, тогда как число в круглых скобках показывает, сколько раз он встречается в спектральном векторе. Например, найдем спектр последовательности (2.2)

$$S_T = H_{32}T =$$

$$= \begin{Bmatrix} -8 & 4 & 4 & 8 & -8 & 4 & -4 & 0 \\ 4 & 0 & 0 & -12 & -12 & 0 & -8 & -4 \\ 4 & 0 & 0 & 4 & -4 & -8 & 0 & 4 \\ 0 & -4 & -4 & 0 & -8 & 4 & 12 & 0 \end{Bmatrix},$$

что исходя из принятой нотации соответствует спектральному набору $\{12(3), 8(6), 4(13), 0(10)\}$ и величине пик-фактора $\kappa = 4.5$.

Изучение данных таблицы 3.2 позволяет рассчитать предельные мощности С-кодов с длиной кодового слова $N = 32$ и заданным значением пик-фактора $\kappa \leq \kappa_0$, которые принципиально могут быть построены для некоторого заданного значения пик-фактора κ_0 . В таблице 3.3 приведены максимально возможные мощности С-кодов длины $N = 32$, которые могут быть построены.

В таблице 3.3 под J_1 понимается количество последовательностей длины $N = 32$, которые обладают заданным уровнем пик-фактора κ_0 , тогда как под J_{\max} понимается количество последовательностей, которые обладают уровнем пик-фактора не ниже, чем величина κ_0 . Таким образом, J_{\max} является границей мощности С-кода длины $N = 32$ для каждого заданного значения κ .

Заключение

Отметим основные результаты проведенных исследований:

- предложен алгоритм спектральной классификации последовательностей длины $N = 32$, основанный на использовании свойств коэффициентов АНФ и позволяющий сократить перебор множества исследуемых последовательностей в 64 раза;
- проведена спектральная классификация полного множества последовательностей длины $N = 32$, в результате чего рассчитаны теоретически предельно достижимые мощности С-кодов с заданным значением пик-фактора κ_0 ;
- определены мощности множеств последовательностей длины $N = 32$, обладающих заданным значением расстояния нелинейности N_f .

Таким образом, изложенные в статье результаты определяют мощности С-кодов длины

$N = 32$, которые принципиально могут быть сконструированы и применены в технологии МС-CDMA, а также мощности множеств последовательностей данной длины, обладающие заданным расстоянием нелинейности, которые применимы в криптографических приложениях, например, при синтезе псевдослучайных ключевых последовательностей или S-блоков подставки.

ЛИТЕРАТУРА

1. Бакулин, М.Г. Технология OFDM / М.Г. Бакулин, В.Б. Крейнделин, А.М. Шлома, А.П. Шумов. – М.: Горячая линия – Телеком, 2016. – 352 с.
2. Мазурков, М.И. Системы широкополосной радиосвязи / М.И. Мазурков // Одесса: Наука и Техника. – 2010. – 340 с.
3. Paterson, K.G. Sequences For OFDM and Multi-code CDMA: two problems in algebraic coding theory / K.G. Paterson // Sequences and their applications. Seta 2001. Second Int. Conference (Bergen, Norway, May 13–17, 2001). Proc. Berlin: Springer, 2002. – P. 46–71.
4. Токарева, Н.Н. Бенг-функции: результаты и приложения. Обзор работ / Н.Н. Токарева // Прикладная дискретная математика. – Томск, 2009. – Сер. № 1 (3). – С. 15–37.
5. Соколов, А.В. Конструктивный метод синтеза последовательностей длины $N = 20$ с оптимальным спектром Уолша – Адамара / А.В. Соколов. – Научные труды ОНАС им. АС Попова, 2015. – № 2. – С. 118–126.
6. Sokolov, A.V. Regular synthesis method of the sequences of length $N = 24$ with optimal PAPR of Walsh-Hadamard spectrum / A.V. Sokolov // – Far East Journal of Electronics and Communications. – 2016. – Vol. 16, № 2. – P. 459–469.
7. Соколов, А.В. Нескінченні сімейства послідовностей Пелі з оптимальним пик-фактором спектра Уолша – Адамара / А.В. Соколов, О.О. Гаркуша. – Наукові праці ОНАЗ ім. О.С. Попова. – 2016. – № 2. – С. 163–169.
8. Мазурков, М.И. Рекуррентные методы синтеза последовательностей с оптимальным пик-фактором спектра Уолша – Адамара / М.И. Мазурков, А.В. Соколов // Информатика и математические методы в моделировании. – 2015. – Т. 5, № 4. – С. 203–209.
9. Ростовцев, А.Г. Криптография и защита информации / А.Г. Ростовцев. – СПб.: Мир и Семья. – 2002.
10. Соколов, А.В. Новые методы синтеза нелинейных преобразований современных шифров / А.В. Соколов. – Lap Lambert Academic Publishing, Germany, 2015. – 100 с.

Поступила в редакцию 24.02.17.