УДК 681.3.06

СИСТЕМЫ ОРТОГОНАЛЬНЫХ БИФАЗНЫХ СИГНАЛОВ НА ОСНОВЕ БЕНТ-ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Соколов А.В., Барабанов Н.А.

Одесский национальный политехнический университет
65044, Украина, Одесса, пр-т Шевченко, 1.
radiosquid@gmail.com

СИСТЕМИ ОРТОГОНАЛЬНИХ БІФАЗНИХ СИГНАЛІВ НА ОСНОВІ БЕНТ-ПОСЛІДОВНОСТЕЙ

Соколов А.В., Барабанов М.О.

Одеський національний політехнічний університет
65044, Україна, Одеса, пр-т Шевченка, 1.
radiosquid@gmail.com

SYSTEMS OF ORTHOGONAL BIPHASIC SIGNALS ON THE BASIS OF BENT-SEQUENCES

Sokolov A.V., Barabanov N.A.

Odessa National Polytechnic University,
ave. Shevchenko, 1, Odessa, Ukraine, 65044
radiosquid@gmail.com

Аннотация. Проблема построения систем ортогональных бифазных сигналов, обладающих хорошими авто- и взаимокорреляционными свойствами, является актуальной для технологии CDMA, которая лежит в основе третьего, четвертого и пятого поколений мобильной связи. Известные методы построения ортогональных систем бифазных сигналов (на основе функций Уолша, на основе совершенных двоичных решеток) позволяют синтезировать лишь небольшое, с криптографической точки зрения, число систем, обладающих хорошими апериодическими корреляционными свойствами, что затрудняет реализацию концепции оперативной смены рабочего ансамбля сигналов в целях защиты информации. В данной статье предложен метод синтеза ортогональных систем бифазных сигналов на основе полного класса бент-последовательностей и регулярного оператора диадного сдвига. Мощность построенного множества ортогональных систем составляет $J = 5\,425\,430\,528$. Проведенные исследования зависимости вероятности ошибки от апериодических корреляционных свойств построенных систем сигналов позволили подтвердить их высокую эффективность как в плане помехоустойчивости, так и с точки зрения защиты информации.

Ключевые слова: система ортогональных бифазных сигналов, бент-последовательность, диадный сдвиг, производная система сигналов.

Анотація. Проблема побудови систем ортогональних біфазних сигналів, що володіють хорошими авто- і взаємокореляційними властивостями, є актуальною для технології CDMA, яка лежить в основі третього, четвертого і п'ятого поколінь мобільного зв'язку. Відомі методи побудови ортогональних систем біфазних сигналів (на основі функцій Уолша, на основі досконалих двійкових решіток) дозволяють синтезувати лише невелике, з криптографічної точки зору, число систем, що володіють хорошими аперіодичними кореляційними властивостями, що ускладнює реалізацію концепції оперативної зміни робочого ансамблю сигналів з метою захисту інформації. У даній статті запропонований метод синтезу ортогональних систем біфазних сигналів на основі повного класу бент-послідовностей і регулярного оператора діадного зсуву. Потужність побудованої множини ортогональних систем становить $J = 5\,425\,430\,528$. Проведені дослідження залежності ймовірності

помилки від аперіодичних кореляційних властивостей побудованих систем сигналів дозволили підтвердити їх високу ефективність, як в плані завадостійкості, так і з точки зору захисту інформації.

Ключові слова: система ортогональних біфазних сигналів, бент-послідовність, діадний зсув, похідна система сигналів.

Abstract. The problem of constructing of orthogonal systems of biphasic signals having good auto and intercorrelation properties is relevant for the CDMA technology, which is the basis of the third, fourth and fifth generations of mobile communication. Known methods for constructing orthogonal systems of biphasic signals (based on Walsh functions, on the basis of perfect binary arrays) allows to synthesize only small from cryptographic point of view numbers of systems that have good aperiodic correlation properties, making it difficult to implement the concept of operational change of working ensemble of signals in order to protect the information. In this paper, we propose a method of synthesis of orthogonal systems of biphasic signals based on complete class of bent-sequences and regular operator of dyadic shift. The volume of constructed sets of orthogonal systems is $J = 5425430\,528$. Research of the depending of error probability from aperiodic correlation properties of the constructed systems of signals allowed to confirm their high efficiency, both in terms of noise immunity, and from the point of view of information security.

Key words: system of orthogonal biphasic signals, bent sequence, dyadic shift, derived signal system.

Ортогональные системы сигналов, основанные на функциях Уолша, получили широкое распространение в современных системах связи, а также при решении задач защиты информации. Ортогональность функций Уолша позволяет использовать их в технологии кодового разделения каналов CDMA (Code Division Multiple Access) [1], где каждому пользователю выделяется одна из функций Уолша в качестве кода расширения, тем самым, позволяя свести корреляцию между пользователями к нулю (в рамках одной базовой станции) [2]. Тем не менее, в технологии CDMA все подвижные станции являются синхронными по режиму работы только в рамках одной базовой станции, в то время как по отношению к подвижным станциям другой базовой станции — являются асинхронными. Данный факт диктует необходимость применения в системах CDMA сигналов с хорошими апериодическими авто- и взаимокорреляционными свойствами.

Известно достаточно много различных определений систем функций Уолша, самым распространенным из которых является их определение через матрицу Адамара [1,3], которая определяется следующим рекуррентным соотношением

$$\mathbf{A}_{L+1} = \begin{bmatrix} \mathbf{A}_L & \mathbf{A}_L \\ \mathbf{A}_L & -\mathbf{A}_L \end{bmatrix}, \tag{1}$$

где $\mathbf{A}_1 = 1$.

В качестве кодовых последовательностей системы Уолша можно брать строки или столбцы матрицы Адамара. Таким образом объем системы сигналов равен порядку матрицы $J = L$.

Рассмотрим, например, матрицу Адамара четвертого порядка $L = 4$, которая может быть построена в соответствии с рекуррентной формулой (1)

$$\mathbf{A}_4 = \begin{bmatrix} + & + & + & + \\ + & - & + & - \\ + & + & - & - \\ + & - & - & + \end{bmatrix}. \tag{2}$$

Ясно, что число блоков в представленных последовательностях Уолша (строках или столбцах матрицы (2)) изменяется от 1 до L и не соответствует оптимальному числу блоков $\mu_0 \simeq N/2$, что, в соответствии с гипотезой [3] определяет плохие апериодические авто- и взаимокорреляционные свойства данной системы сигналов.

Для преодоления данного недостатка на практике используются производные системы сигналов на основе функций Уолша.

Определение 1 [3]. Производным сигналом называется сигнал, который получается в результате перемножения двух сигналов – производящего и исходного.

Система, составленная из производных сигналов, называется производной. Для того, чтобы улучшить апериодические корреляционные свойства системы сигналов, производящий сигнал выбирают так, чтобы его апериодические авто- и взаимокорреляционные функции (ААКФ и АВКФ)

$$R_{i,k}(\tau)=\begin{cases}\dfrac{1}{n}\displaystyle\sum_{\nu=\tau}^{n-1}\omega_{i,\nu}\omega_{k,\nu-\tau}, & \text{для } \tau\geq 0;\\ \dfrac{1}{n}\displaystyle\sum_{\nu=0}^{n+\tau-1}\omega_{i,\nu}\omega_{k,\nu-\tau}, & \text{для } \tau<0,\end{cases} \tag{3}$$

были наилучшими (минимаксными).

На практике в качестве производящих сигналов применяются сегменты M-последовательностей, например, в стандарте CDMA применяются система сигналов Уолша порядка $N=64$ и сегменты M-последовательностей периода $n=2^{15}-1$ в качестве производящей последовательности [2].

Тем не менее, в связи с бурным развитием технологии CDMA и ее повсеместным внедрением в практические системы связи помимо вопроса синтеза ортогональных систем сигналов с хорошими апериодическими авто- и взаимокорреляционными свойствами органично встает вопрос о построении регулярных правил синтеза больших множеств таких систем, в частности в целях улучшения защиты информации при реализации концепции оперативной смены ансамбля сигналов по псевдослучайному закону.

В [4] рассмотрены методы построения ортогональных систем бифазных сигналов на основе совершенных двоичных решеток, которые позволили построить $J=688128$ различных ортогональных бифазных систем сигналов. Однако, при реализации концепции оперативной смены ансамбля сигналов практический интерес может представлять дальнейшее увеличение числа доступных систем сигналов.

Целью настоящей статьи *является разработка метода синтеза ортогональных бифазных систем сигналов на основе полного класса бент-последовательностей длины* $N=64$.

Как показали проведенные исследования, для решения задачи построения больших бифазных ортогональных систем сигналов с хорошими корреляционными свойствами могут быть использованы такие совершенные алгебраические конструкции как бент-последовательности.

Определение 2 [5]. Бинарная последовательность $\mathbf{B}=[b_0,b_1,\cdots,b_i,\cdots,b_{n-1}]$, где коэффициенты $b_i\in\pm 1$, четной длины $n=N^2$, называется бент-последовательностью (БП), если она имеет равномерный по модулю спектр Уолша-Адамара, который представим в матричной форме

$$\mathbf{W}_B(\omega)=\mathbf{B}\cdot\mathbf{A}_L=\pm 2^{N/2},\ \ \omega=\overline{0,n-1}, \tag{4}$$

где $\mathbf{A}(n)$ — матрица Уолша-Адамара порядка $L=N$.

Регулярный метод синтеза бент-последовательностей длины $N=16$ разработаны в [5], полная мощность класса составляет $J_{bent16}=896$ последовательностей, среди которых $J_{PBA}=384$ совершенные двоичные решетки СДР [4]. Метод синтеза полного класса бент-последовательностей длины $N=64$, основанный на свойствах преобразования Рида-Маллера, приведен в [6]. Мощность полного класса составляет $J_{bent64}=5\,425\,430\,528$.

Известен регулярный метод построения ортогональных матриц на основе регулярного оператора диадного сдвига [7], который строится по рекуррентному правилу:

$$\mathbf{Diad}(N) = \begin{bmatrix} \mathbf{Diad}(N/2), & \mathbf{Diad}(N/2)+N/2 \\ \mathbf{Diad}(N/2)+N/2, & \mathbf{Diad}(N/2) \end{bmatrix}, \quad (5)$$

где $\mathbf{Diad}(2) = \begin{bmatrix} 1, & 2 \\ 2, & 1 \end{bmatrix}$.

Таким образом, каждая бент-последовательность под действием оператора диадного сдвига (5) определяет ортогональную матрицу, строки и столбцы которой, соответственно, являются системой бифазных ортогональных векторов. При этом объем таких систем сигналов определяется количеством существующих бент-последовательностей.

Пусть, например, задана бент-последовательность длины $N = 64$

$$B = \begin{Bmatrix} +++-+--+++--++++++-+--++--+++ \\ +--++-+-++--++++-++--+-+--++---- \end{Bmatrix}, \quad (6)$$

на основе которой с помощью оператора диадного сдвига (5) может быть построена ортогональная матрица, представленная на рис. 1.

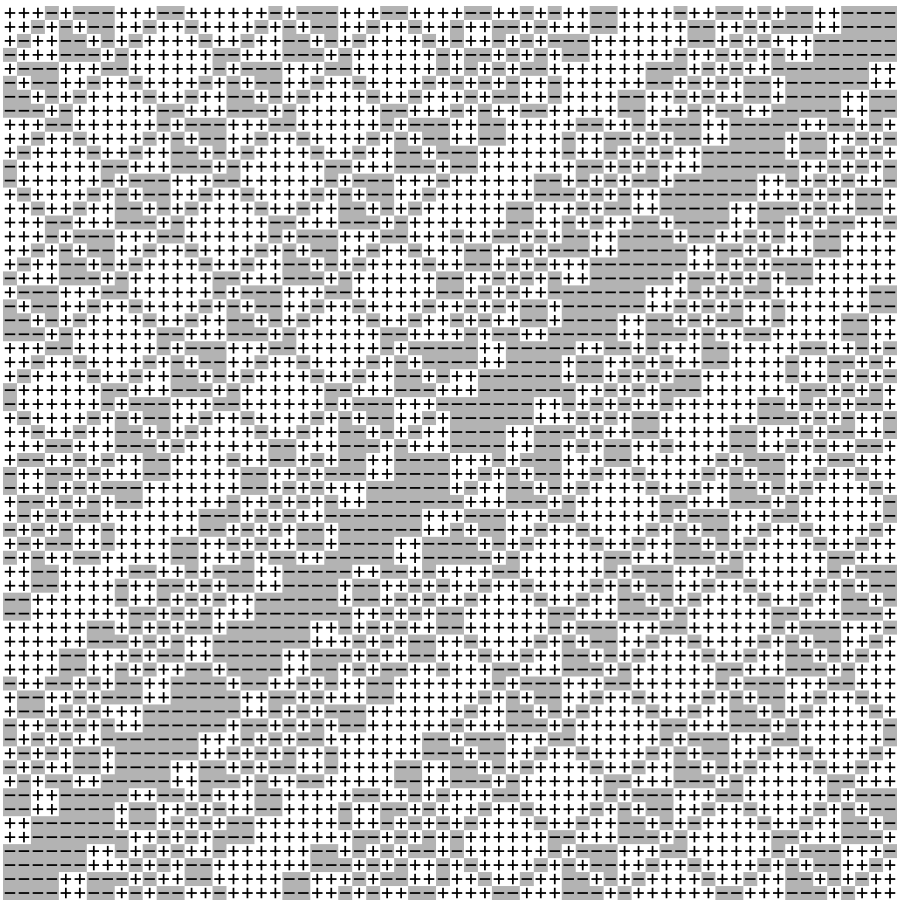

Рисунок 1 – Ортогональная матрица на основе бент-последовательности (6)

Для того, чтобы провести сравнительный анализ построенной системы ортогональных сигналов, на рис. 2 приведен график зависимости вероятности ошибки P_e от взаимокорреляционных свойств сигналов для построенной системы на основе бент-последовательности, а также систем сигналов на основе функций Уолша и СДР, где по оси абсцисс отложено отношение сигнал/взаимная помеха q.

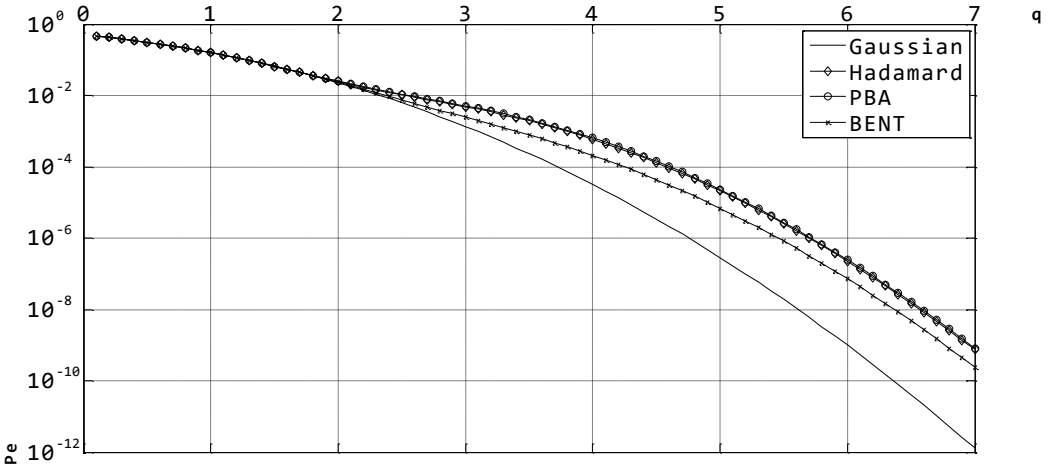

Рисунок 2 – График зависимости вероятности ошибки
от взаимокорреляционных свойств оригинальных систем сигналов

Анализ данных рис. 2 показывает, что системы на основе бент-последовательностей и регулярного оператора диадного сдвига обладают лучшей помехоустойчивостью, нежели оригинальные системы на основе функций Уолша или совершенных двоичных решеток.

Ясно, что для системы сигналов (рис. 1) может быть построена производная система сигналов. Пусть задана производящая последовательность, как сегмент *M*-последовательности длины N, построенной на основе генераторного полинома $f(x) = x^{15} + x + 1$, тогда как исходное состояние регистра сдвига с обратной связью $\alpha_i = \{100010011010111\}$. Найденный сегмент производящей последовательности может быть представлен в бинарном виде с помощью однозначного отображения $"0" \to "+1", "1" \to "-1"$.

График зависимости вероятности ошибки от отношения сигнал/взаимная помеха для производной системы на основе бент-последовательности, а также производных систем на основе последовательностей Уолша и совершенных двоичных решеток приведен на рис. 3.

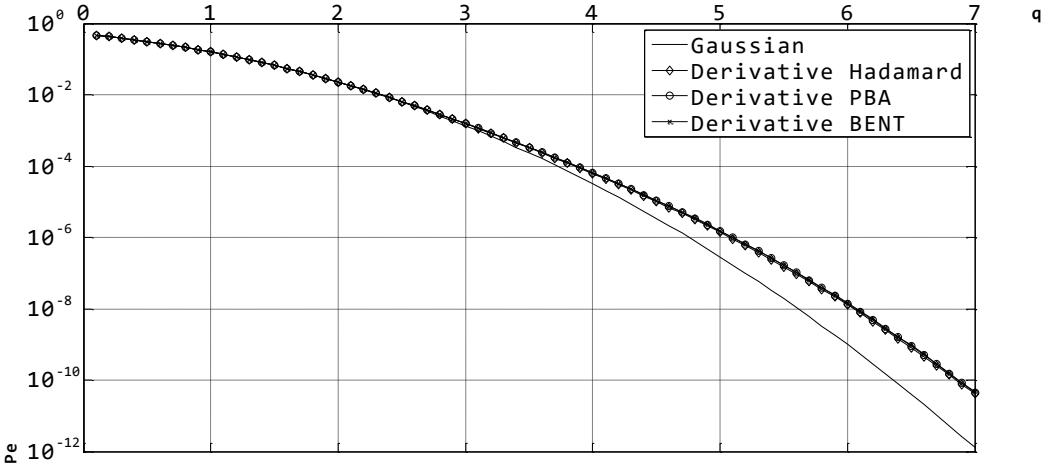

Рисунок 3 – График зависимости вероятности ошибки
от взаимокорреляционных свойств производных систем сигналов

Анализ данных (рис. 3) показывает практически одинаковую эффективность использования производных систем сигналов на основе бент-последовательностей, совершенных двоичных решеток и матриц Адамара. Таким образом, для увеличения числа доступных ортогональных систем бифазных сигналов, данные классы могут быть объединены, что приведет к увеличению общего числа уровней защиты.

В табл. 1 приведены данные сравнительного анализа параметров корреляционных свойств и мощностей систем бифазных ортогональных сигналов на основе различных совершенных алгебраических конструкций:

– $\max\{R_{\text{ААКФ}}\}$ — максимальное значение среди всех значений апериодических автокорреляционных функций сигналов системы;

– $\max\{R_{\text{АВКФ}}\}$ — максимальное значение среди всех значений апериодических взаимокорреляционных функций сигналов системы;

– σ^2 – дисперсия;

– γ – коэффициент эксцесса;

– П – доступное количество производных сигналов.

Таблица 1 – Сравнительный анализ типовых значений основных параметров

№ п/п	Система бифазных сигналов	Параметры				
		$\max\{R_{\text{ААКФ}}\}$	$\max\{R_{\text{АВКФ}}\}$	σ^2	γ	Мощность, J
1	Ортогональные системы на основе функций Уолша-Адамара	63	63	0,0066	19,3090	1
2	Производные ортогональные системы на основе функций Уолша-Адамара	17	26	0,0078	0,8662	$1\cdot$П
3	Ортогональные системы на основе СДР	16	57	0,0077	17,8953	688 128
4	Производные ортогональные системы на основе СДР	20	29	0,0078	0,9503	688 128$\cdot$П
5	Ортогональные системы на основе бент-последовательностей	19	46	0,0077	5,2342	5 425 430 528
6	Производные ортогональные системы на основе бент-последовательностей	22	30	0,0078	0,9856	5425430 528$\cdot$П

Анализ данных табл. 1 показывает высокую эффективность использования бент-последовательностей и регулярного оператора диадного сдвига для конструирования больших множеств бифазных ортогональных систем сигналов.

В заключение можно сказать следующее:

1. Предложен метод синтеза систем бифазных ортогональных сигналов на основе бент-последовательностей и регулярного оператора диадного сдвига. При этом, мощность множества составляет $J = 5425430\,528$. Выборочное изучение построенных систем сигналов показывает их хорошие апериодические авто- и взаимокорреляционные свойства.

2. Установлено, что на основе построенных ортогональных систем на основе бент-последовательностей могут быть получены производные ортогональные системы сигналов, что позволит еще более существенно увеличить мощность множества построенных ортогональных систем. Данный аспект может быть использован в целях защиты информации для реализации концепции оперативной смены рабочего ансамбля сигналов.

3. Проведенное моделирование зависимости вероятности ошибки от корреляционных свойств используемой системы сигналов показывает более высокую эффективность использования бент-последовательностей для построения ортогональных преобразований, нежели другие известные методы. Для производных систем сигналов, значения вероятности возникновения ошибки является практически сходным с известными методами, тем не менее бент-последовательности обеспечивают намного большую (в ~7884 раза по отношению к системе на основе совершенных двоичных решеток) мощность множества доступных систем сигналов.

Таким образом, бент-последовательности являются перспективным классом совершенных алгебраических конструкций с точки зрения построения ортогональных систем сигналов для технологии CDMA.

ЛИТЕРАТУРА:

1. Wysocki B. J. Modified Walsh-Hadamard Sequences for DS CDMA Wireless Systems / B.J. Wysocki, T.A. Wysocki. – Int. J. Adapt. Control Signal Process, 2002. – Vol. 16. – P. 589–602.
2. Peterson, K.G. Sequences For OFDM and Multi-code CDMA: two problems in algebraic Coding Theory // Sequences and their applications. Seta 2001. Second Int. Conference (Bergen, Norway, May 13–17, 2001). Proc. Berlin: Springer, 2002. – P.46–71.
3. Варакин Л.Е. Системы связи с шумоподобными сигналами / Варакин Л.Е. – М.: Радио и связь, 1985. – 384 с.
4. Мазурков М.И. Классы минимаксных бифазных сигналов на основе совершенных двоичных решеток / М.И. Мазурков, В.Я. Чечельницкий, М.Ю. Герасименко // Известия высших учебных заведений. Радиоэлектроника. – 2006. – Т. 49. – N 10. – С. 25–38.
5. Мазурков М.И. Регулярные правила построения полного класса бент-последовательностей длины 16 / М.И. Мазурков, А.В. Соколов // Труды Одес. нац. политехн. ун-та. – Одесса, 2013. – № 1 (40).
6. Qingshu, Meng A novel algorithm enumerating bent functions / Qingshu Meng, Min Yang, Huanguo Zhang, Jingsong Cui // Discrete Mathematics. – Volume 308, Issue 23, 2008. – P. 5576–5584.
7. Мазурков М.И. Быстрые ортогональные преобразования на основе бент-последовательностей / М.И. Мазурков, А.В. Соколов // Інформатика та математичні методи в моделюванні. – Одеса, 2014. – №1. – С.5–13.

REFERENCES:

1. Wysocki, B. J. Modified Walsh-Hadamard Sequences for DS CDMA Wireless Systems / B.J. Wysocki, T.A. Wysocki. – Int. J. Adapt. Control Signal Process, 2002. – Vol. 16. – P. 589–602.
2. Peterson, K.G. Sequences For OFDM and Multi-code CDMA: two problems in algebraic Coding Theory // Sequences and their applications. Seta 2001. Second Int. Conference (Bergen, Norway, May 13–17, 2001). Proc. Berlin: Springer, 2002. – P.46–71.
3. Varakin, L.E. Communication system with noise-like signals / Varakin L.E. – M.: Radio i svjaz`, 1985. – 384 s.
4. Mazurkov, M.I. Classes of minimax bi-phase signals based on perfect binary arrays / M.I. Mazurkov, V.JA. Chechel`nickijj, M.JU. Gerasimenko // Izvestija vysshikh uchebnykh zavedenijj. Radioehlektronika. – 2006. – T. 49. – N 10. – S. 25–38.
5. Mazurkov, M.I. The regular rules of full class of bent sequences of length 16 construction / M.I. Mazurkov, A.V. Sokolov // Trudy Odes. nac. politekhn. un-ta. – Odessa, 2013. – N1 (40).
6. Qingshu, Meng A novel algorithm enumerating bent functions / Qingshu Meng, Min Yang, Huanguo Zhang, Jingsong Cui // Discrete Mathematics. – Volume 308, Issue 23, 2008. – P. 5576–5584.
7. Mazurkov, M.I. Fast orthogonal transforms based on bent-sequences / M.I. Mazurkov, A.V. Sokolov // Informatika ta matematichns metodi v modeljuvannss. – Odesa, 2014. – N 1. – P. 5–13.