ISSN 1684–8853

ИНФОРМАЦИОННО-УПРАВЛЯЮЩИЕ СИСТЕМЫ

НАУЧНЫЙ ЖУРНАЛ

5(72)/2014

ISSN 1684-8853

SCIENTIFIC JOURNAL

5(72)/2014

INFORMATSIONNO-UPRAVLIAIUSHCHIE SISTEMY (INFORMATION AND CONTROL SYSTEMS)

REFEREED EDITION

Contact information
The Editorial and Publishing Center, SUAI
67, B. Morskaia, 190000, St. Petersburg, Russia
Website: http://i-us.ru/en, E-mail: ius.spb@gmail.com
Tel.: +7 - 812 494 70 02

The Journal was registered in the Ministry of Press, Broadcasting and Mass Media of the Russian Federation.
Registration Certificate JD № 77-12412 from April, 19, 2002.
Re-registration in the Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications (ROSKOMNADZOR) due to change of the founder: «Information and Control Systems», Ltd., JD № FS77-49181 from March, 30, 2012.

Submitted for publication 02.09.14. Passed for printing 20.10.14. Format $60\times84_{1/8}$.
Offset paper. Phototype SchoolBookC. Offset printing.

Layout original is made at the Editorial and Publishing Center, SUAI.
67, B. Morskaia, 190000, St. Petersburg, Russia
Printed from slides at the Editorial and Publishing Center, SUAI.
67, B. Morskaia, 190000, St. Petersburg, Russia

The journal is distributed by subscription. Subscription can be made in the Editorial and publishing center, SUAI as well as in any post office based on «Rospechat» catalogue:
№ 48060 — annual subscript, № 15385 — semiannual subscript.

ISSN 1684-8853

НАУЧНЫЙ ЖУРНАЛ

5(72)/2014

РЕЦЕНЗИРУЕМОЕ ИЗДАНИЕ

ИНФОРМАЦИОННО-УПРАВЛЯЮЩИЕ СИСТЕМЫ

Учредитель
ООО «Информационно-управляющие системы»

Издатель
Санкт-Петербургский государственный университет аэрокосмического приборостроения

Адрес редакции: 190000, Санкт-Петербург,
Б. Морская ул., д. 67, ГУАП, РИЦ
Тел.: (812) 494-70-02, e-mail: ius.spb@gmail.com, сайт: http://i-us.ru

Журнал зарегистрирован в Министерстве РФ по делам печати, телерадиовещания и средств массовых коммуникаций.
Свидетельство о регистрации ПИ № 77-12412 от 19 апреля 2002 г.
Перерегистрирован в Роскомнадзоре.
Свидетельство о регистрации ПИ № ФС77-49181 от 30 марта 2012 г.

Журнал входит в «Перечень ведущих рецензируемых научных журналов и изданий, в которых должны быть опубликованы основные научные результаты диссертации на соискание ученой степени доктора и кандидата наук».

Сдано в набор 02.09.14. Подписано в печать 20.10.14. Формат 60×84 1/8.
Бумага офсетная. Гарнитура SchoolBookC. Печать офсетная.
Усл. печ. л. 14,4. Уч.-изд. л. 18,1. Тираж 1000 экз. Заказ 533.

Оригинал-макет изготовлен в редакционно-издательском центре ГУАП.
190000, Санкт-Петербург, Б. Морская ул., 67.

Отпечатано с готовых диапозитивов в редакционно-издательском центре ГУАП.
190000, Санкт-Петербург, Б. Морская ул., 67.

Журнал распространяется по подписке. Подписку можно оформить через редакцию, а также в любом отделении связи по каталогу «Роспечать»:
№ 48060 — годовой индекс, № 15385 — полугодовой индекс.

UDC 004.438

REMARKS ON EXTREMAL AND MAXIMUM DETERMINANT MATRICES WITH MODULI OF REAL ENTRIES ≤ 1

N. A. Balonin[a], *Dr. Sc., Tech., Professor, korbendfs@mail.ru*
Jennifer Seberry[b], *PhD, Professor of Computer Science, jennifer_seberry@uow.edu.au*
[a]*Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St., 190000, Saint-Petersburg, Russian Federation*
[b]*Centre for Computer Security Research, EIS, University of Wollongong, NSW, 2522, Australia*

Purpose: *This note discusses quasi-orthogonal matrices which were first highlighted by J. J. Sylvester and later by V. Belevitch, who showed that three level matrices mapped to lossless telephone connections. The goal of this note is to develop a theory of such matrices based on preliminary research results.* ***Methods:*** *Extreme solutions (using the determinant) have been established by minimization of the maximum of the absolute values of the elements of the matrices followed by their subsequent classification.* ***Results:*** *We give the definitions of Balonin–Mironovsky (BM), Balonin–Sergeev (BSM) and Cretan matrices (CM), illustrations for some elementary and some interesting cases, and reveal some new properties of weighing matrices (Balonin–Seberry conjecture). We restrict our attention in this remark to the properties of Cretan matrices depending on their order.* ***Practical relevance:*** *Web addresses are given for other illustrations and other matrices with similar properties. Algorithms to construct Cretan matrices have been implemented in developing software of the research program-complex.*

Keywords *— Hadamard Matrices, Conference Matrices, Weighing Matrices, Constructions, Balonin–Mironovsky Matrices, Balonin–Sergeev Matrices, Cretan Matrices.*

AMS Subject Classification: *05B20; 20B20.*

Definition 1. A real square matrix $\mathbf{X} = (x_{ij})$ of order n is called *quasi-orthogonal* if it satisfies $\mathbf{X}^T\mathbf{X} = \mathbf{X}\mathbf{X}^T = c\mathbf{I}_n$, where $\mathbf{I}_n$ is the $n\times n$ identity matrix and "T" stands for transposition, c is constant real number. In this and future work we will only use quasi-orthogonal to refer to matrices with real elements, a least one entry in each row and column must be 1. Hadamard matrices are the best known of these matrices with entries from the unit disk [1].

Definition 2. An *Hadamard matrix* of order n is an $n\times n$ matrix with elements 1, –1 such, that $\mathbf{H}^T\mathbf{H} = \mathbf{H}\mathbf{H}^T = n\mathbf{I}_n$, where $\mathbf{I}_n$ is the identity matrix.

The Hadamard inequality [2] says, that Hadamard matrices have maximal determinant for the class of matrices with entries from the unit disk (the moduli of the elements is $|x_{ij}| \le 1$ by default). Hadamard matrices can only exist for orders 1, 2 and $n = 4t$, t an integer (the so called *Hadamard conjecture*).

The class of *quasi-orthogonal* matrices with maximal determinant and entries from the unit disk may have a very large set of solutions. Different solutions may give the same maximal determinant. Symmetric conference matrices, a particularly important class of 0, ±1 matrices, are the most well known [3].

Definition 3. A *symmetric conference matrix,* $\mathbf{C}$, is an $n\times n$ matrix with elements 0, +1 or –1, satisfying $\mathbf{C}^T\mathbf{C} = \mathbf{C}\mathbf{C}^T = (n-1)\mathbf{I}_n$.

Conference matrices can only exist if the number $n - 1$ is the sum of two squares. Similar to symmetric conference matrices are quasi-orthogonal matrices $W = W(2t, 2t - m)$ of order $n = 2t$, with elements 0, +1 or –1, satisfying $\mathbf{W}^T\mathbf{W} = \mathbf{W}\mathbf{W}^T = (2t - m)\mathbf{I}_n$. These are called *weighing matrices*. It has been conjectured [4] that for $n = 4t$, there exists a $W = W(4t, 4t - m)$ for all integers $0 \le m \le 4t$.

Definition 4. The values of the entries of the quasi-orthogonal matrix, $\mathbf{X}$, are called *levels*, so Hadamard matrices are two-level matrices and symmetric conference matrices and weighing matrices are three-level matrices. *Quasi-orthogonal* matrices with maximal determinant of odd orders have been discovered to have a larger number of levels [5].

Definition 5. A *Balonin–Mironovsky* [5] matrix, $\mathbf{A}_n$, of order n, is quasi-orthogonal matrix of maximal determinant. In this remark they are called *BM matrices.*

Conjecture (Balonin, [6, 7]): there are only 5 Balonin–Mironovsky matrices $\mathbf{A}_3$, $\mathbf{A}_5$, $\mathbf{A}_7$, $\mathbf{A}_9$, $\mathbf{A}_{11}$ with $\frac{n+1}{2} \pm m$, $m \le 1$, levels.

The 2006 paper [5] gave 5 examples of BM matrices. Order 13 was unresolved. During 2006–2011 Balonin and Sergeev carried out many computer experiments to find the absolute maximum of the determinant of $\mathbf{A}_{13}$.

It was speculated [6] that 13 is a critical order for matrices of odd orders with maximal determinant. Starting from this odd order, the number of levels $k >> \frac{n+1}{2}$. An example of a 6-level (by moduli) matrix of even order was found and called Yura's matrix $\mathbf{Y}_{22}$ [8] (Fig. 1, *a*). A student Yura Balonin found this rare solution using DOS–MatLab [8, 9]. The matrix levels are captured by the colour of the squares.

Order $n = 22$ is special, $n - 1$ is not sum of two squares, and a symmetric three level conference matrix does not exist. The two circulant matrix $\mathbf{Y}_{22}$

based on the sequences $\{-f\ b\ a\ -a\ a\ a\ a\ a\ -a\ a\ -a\}$, $\{a\ a\ -a\ -c\ -a\ a\ d\ a\ e\ a\ -a\}$ has elements with moduli $a = 1$, $b = 0.9802$, $c = 0.7845$, $d = 0.6924$, $e = 0.5299$, $f = 0.3076$. It appears similar to a conference matrix of order 22 because of the small value for f. A non optimal determinant version was also found with $f = 0.0055$.

It was then discovered that there is a 22×22 matrix W(22,20) constructed using Golay sequences which gave det(W(22,20)) > det($\mathbf{Y}_{22}$) (Fig. 1, *b*).

We note that Golay sequences exist which give W($2n$, $2n - 2$) with determinant $(2n - 2)^n$ for orders 4, 6, 10, 18, 22, 34, 42, 54, 66, 82, 102, 106, 130, 162, 258, 262, 322. In the cases 22, 34, 66, 106, 130, 162, 210, 322 there is no corresponding conference matrix [3].

Conjecture I (Balonin–Seberry, 2014): Suppose a W($2n$, $2n - 1$) does not exist. Suppose a W($2n$, $2n - 2$) exists. Then the quasi-orthogonal matrix with maximal determinant is constructed using the W($2n$, $2n - 2$).

Conjecture II (Balonin–Seberry, 2014): Suppose a W($2n$, $2n - 1$) does not exist. Suppose that W($2n$, k) is the weighing matrix with largest k that exists, then W($2n$, k) will give a quasi-orthogonal matrix with near maximal determinant.

For order 58 Balonin found [10] a quasi-orthogonal matrix $\mathbf{Y}_{58}$ with only a few levels and determinant $2 \cdot 10^{50}$, the weighing matrices W(58, k), $k = 54, 55, 56, 57$, do not exist. The weighing matrix W(58,53) has determinant 10^{50}, so conjecture I only applies for W($2n$, $2n - 2$) matrices (Fig. 2, *a*, *b*).

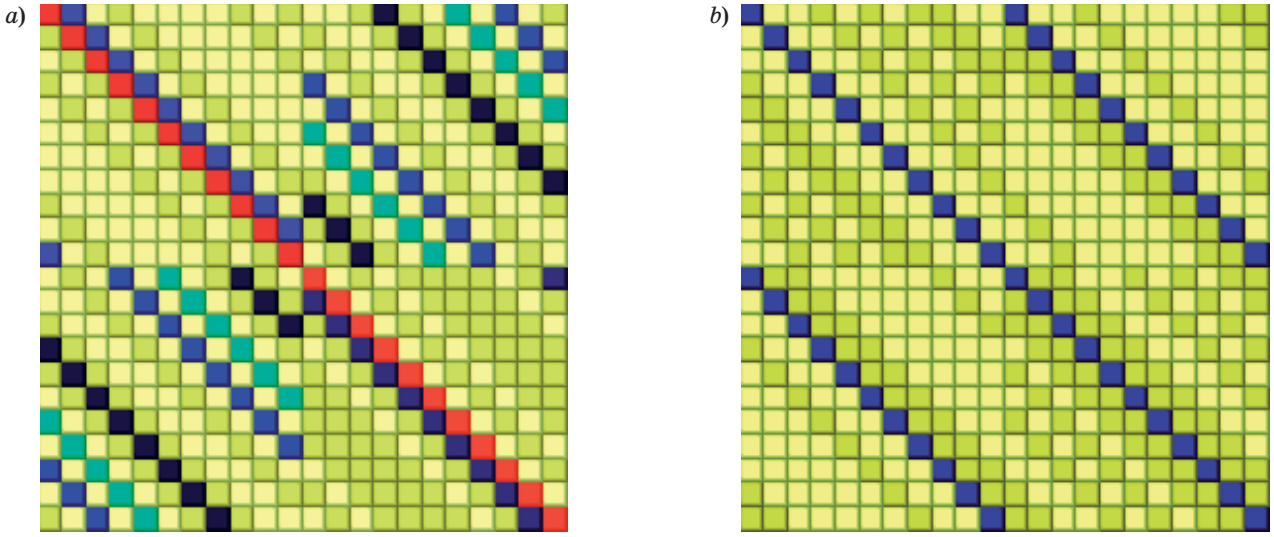


Fig. 1. Yura's matrix $\mathbf{Y}_{22}$ (*a*) and a weighing matrix W(22,20) (*b*)

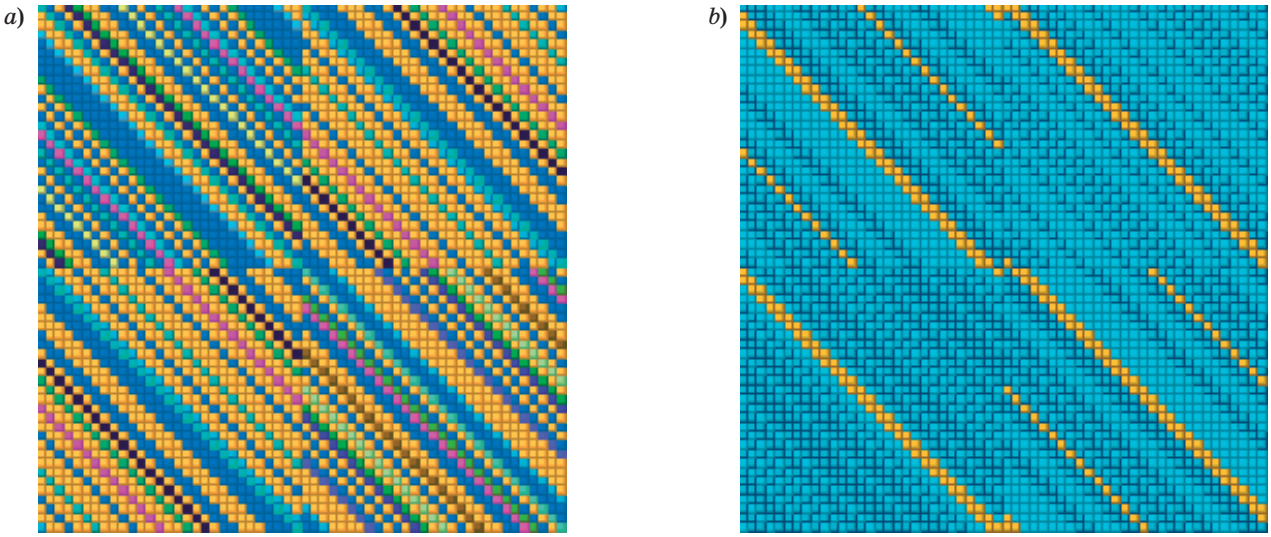


Fig. 2. A low number of levels matrix of order 58 (*a*) and a weighing matrix W(58,53) (*b*)

The absence of a solution with a low number of levels for $n \geq 13$, led Balonin and Sergeev to search for and classify quasi-orthogonal matrices with other properties [5, 6, 11–13].

Definition 6. A quasi-orthogonal matrix with extremal or fixed properties: global or local extremum of the determinant, saddle points, the minimum number of levels, or matrices with fixed numbers of levels is called a *Balonin–Sergeev* matrix. They are called here BSM-matrices.

A Balonin–Mironovsky matrix is a Balonin–Sergeev matrix with the absolute maximum determinant. Balonin–Sergeev matrices with fixed numbers of levels were first mentioned during a conference in Crete, so we will call them *Cretan matrices* (*CM-matrix*).

Definition 7. A *Cretan matrix*, $\mathbf{X}$, of order n, which has indeterminate entries, x_1, x_2, x_3, x_4, ..., x_k is said to have k levels.

It satisfies $\mathbf{X}^T\mathbf{X} = \mathbf{X}\mathbf{X}^T = \omega(n)\mathbf{I}_n$, $\mathbf{I}_n$ the identity matrix, $\omega(n)$ the weight, that give a number of equations, called the *CM-equations*, which make $\mathbf{X}$ quasi-orthogonal when the variables (indeterminates) are replaced by real elements with moduli $|x_{ij}| \leq 1$.

The $\mathbf{X}^T\mathbf{X} = \mathbf{X}\mathbf{X}^T$ have diagonal entries the weight $\omega(n)$ and off diagonal entries 0. *CM-matrices* can be defined by a function $\omega(n)$ or functions $x_1(n)$, $x_2(n)$, $x_3(n)$, $x_4(n)$, ..., $x_k(n)$. We write $CM(n; k; \omega(n);$ determinant) as shorthand.

Notation: When the variable (indeterminate) entries, x_1, x_2, x_3, x_4, ..., x_k occur s_1, s_2, s_3, s_4, ..., s_k times in each row and column, we write $CM(n; k; s_1, s_2, s_3, s_4, ..., s_k; \omega(n);$ determinant) as shorthand.

A review and questions of existence are discussed in [7, 13, 14].

Balonin and Sergeev concluded [7, 13] that the resolution of the question of the existence of quasi-orthogonal matrices and their generalizations discussed here depends on the order [15]:

— for $n = 4t$, t an integer, at least 2 levels, a, $-b$, $|a| = |b|$, are needed;

— for $n = 4t - 1$, at least 2 levels, $a = 1$, $-b$, $b < a$, are needed;

— for $n = 4t - 2$, at least 2 levels, $a = 1$, $-b$, $b < a$, are needed for a two block circulant construction;

— for $n = 4t - 3$, at least 3 levels, $a = 1$, $-b$, c, $b < a, c < a$, are needed.

Definitions and examples of different types of *Cretan matrices* will be discussed in future papers.

Acknowledgements

The authors wish to sincerely thank Tamara Balonina for converting this note into printing format.

References

1. **Seberry J., Yamada M.** Hadamard Matrices, Sequences, and Block Designs. *Contemporary Design Theory*: *A Collection of Surveys*. J. H. Dinitz and D. R. Stinson eds. John Wiley and Sons, Inc., 1992, pp. 431–560.
2. **Hadamard J.** Résolution d'une Question Relative aux Dé terminants. *Bulletin des Sciences Mathématiques*, 1893, vol. 17, pp. 240–246 (In French).
3. **Balonin N. A., Seberry J.** A Review and New Symmetric Conference Matrices. *Informatsionno-upravliaiushchie sistemy*, 2014, no. 4(71), pp. 2–7.
4. **Wallis (Seberry) Jennifer.** Orthogonal (0, 1, –1) matrices. *Proc. of First Australian Conf. on Combinatorial Mathematics*, TUNRA, Newcastle, 1972, pp. 61–84.
5. **Balonin N. A., Mironovsky L. A.** Hadamard Matrices of Odd Order. *Informatsionno-upravliaiushchie sistemy*, 2006, no. 3, pp. 46–50 (In Russian).
6. **Balonin N. A., Sergeev M. B.** M-matrices. *Informatsionno-upravliaiushchie sistemy*, 2011, no. 1, pp. 14–21 (In Russian).
7. **Balonin N. A., Sergeev M. B.** Local Maximum Determinant Matrices. *Informatsionno-upravliaiushchie sistemy*, 2014, no. 1(68), pp. 2–15 (In Russian).
8. **Balonin Yu. N., Sergeev M. B.** M-matrix of 22nd Order. *Informatsionno-upravliaiushchie sistemy*, 2011, no. 5(54), pp. 87–90 (In Russian).
9. **Balonin Yu. N., Sergeev M. B.** The Algorithm and Program for Searching and Studying of M-matrices. *Nauchno-tekhnicheskii vestnik informatsionnykh tekhnologii, mekhaniki i optiki*, 2013, no. 3, pp. 82–86 (In Russian).
10. **Balonin N. A.** Quasi-Orthogonal Matrix with Maximal Determinant, Order 58. Available at: http://mathscinet.ru/catalogue/artifact58 (accessed 15 November 2013).
11. **Balonin N. A.** Existence of Mersenne Matrices of 11th and 19th Orders. *Informatsionno-upravliaiushchie sistemy*, 2013, no. 2, pp. 89–90 (In Russian).
12. **Balonin N. A., Sergeev M. B.** Two Ways to Construct Hadamard-Euler Matrices. *Informatsionno-upravliaiushchie sistemy*, 2013, 1(62), pp. 7–10 (In Russian).
13. **Sergeev A. M.** Generalized Mersenne Matrices and Balonin's Conjecture. *Automatic Control and Computer Sciences*, 2014, vol. 48, no. 4, pp. 214–220.
14. **Balonin N. A., Sergeev M. B.** On the Issue of Existence of Hadamard and Mersenne Matrices. *Informatsionno-upravliaiushchie sistemy*, 2013, no. 5(66), pp. 2–8 (In Russian).
15. **Balonin N. A., Djokovic D. Z., Mironovsky L. A., Seberry Jennifer, Sergeev M. B.** Hadamard Type Matrices Catalogue. Available at: http://mathscinet.ru/catalogue (accessed 25 September 2014).

UDC 519.61:511-33

TWO-CIRCULANT GOLDEN RATIO MATRICES

N. A. Balonin[a]***,*** *Dr. Sc., Tech., Professor, korbendfs@mail.ru*
A. A. Vostrikov[a]***,*** *PhD Tech., Associate Professor, vostricov@mail.ru*
M. B. Sergeev[a]***,*** *Dr. Sc., Tech., Professor, mbse@mail.ru*
[a]*Department of Computing Systems and Networks*
Saint-Petersburg State University of Aerospace Instrumentation,
67, B. Morskaya St., 190000, Saint-Petersburg, Russian Federation

Purpose: *This paper considers two-level quasi-orthogonal matrices, complementing the Mersenne and Euler matrices belonging to the class of Hadamard type matrices, which were first highlighted by J. Hadamard and V. Belevitch. The goal of this note is to develop a theory of such matrices based on preliminary research results. The definitions are provided.* ***Methods:*** *Extreme solutions (using the determinant) have been established by minimization of the absolute values of the elements of the matrices followed their subsequent classification.* ***Results:*** *We give the definitions of a section and a layer of quasi-orthogonal matrices. An example of continuous matrices with varying levels is used to show that the branch of golden ratio matrices is closely associated with the Hadamard and Belevitch matrices. Commentary on the applied aspects of the two-circulant golden ratio matrices and illustrations for some elementary and some interesting cases of Fermat, Mersenne and Euler matrices are provided.* ***Practical relevance:*** *Web addresses are given for other illustrations and other matrices with similar properties. Algorithms to construct golden ratio matrices have been implemented in developing software of the research program-complex.*

Keywords *— Quasi-Orthogonal Matrices, Hadamard Matrices, Belevitch Matrices, Mersenne Matrices, Euler Matrices, Golden Section, Golden Ratio Matrices.*

Introduction

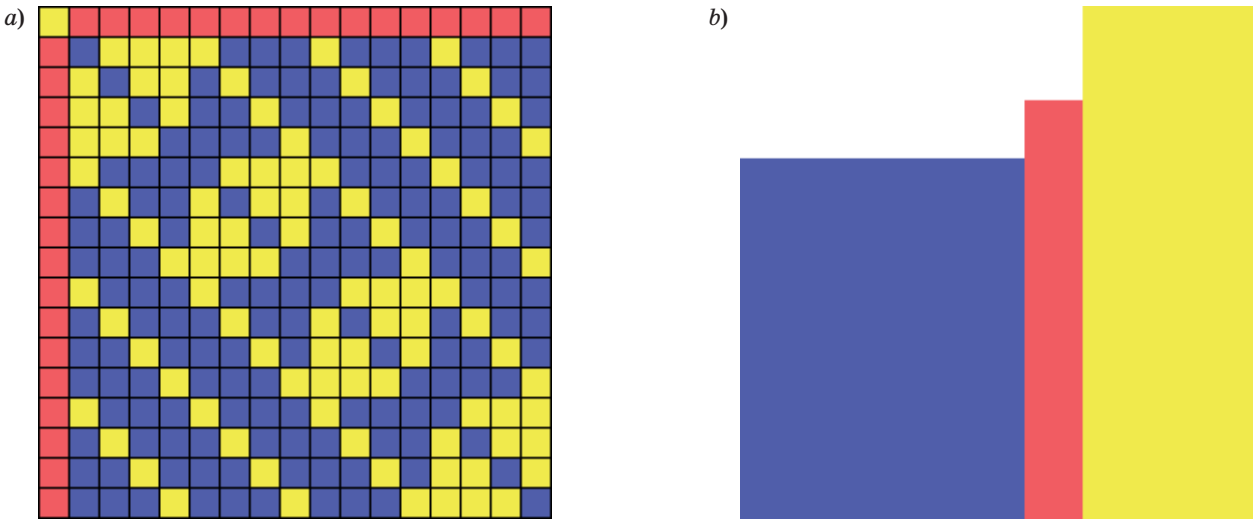
An analysis of *Mersenne* matrix existence [1, 2] has raised the question of quasi-orthogonal matrices belonging to the Hadamard type matrix family [3], the special cases of which are *Belevitch* (C-matrices) [4, 5], *Hadamard* [6, 7], *Mersenne* [8, 9], *Euler* [10], and *Fermat* matrices [11]. The matrices are listed in descending order for $n = 4k - d$, where $d = 0, 1, 2, 3$, $k > 0$ is integer.

A *quasi-orthogonal matrix*, of order n, is a square matrix $\mathbf{A}$, with $|a_{ij}| \le 1$ in each column (and row), with maximum modulus 1, has $\mathbf{A}^{\mathrm{T}}\mathbf{A} = \omega(n)\mathbf{I}$, with $\mathbf{I}$ the identity matrix and $\omega(n)$ is the *weight*.

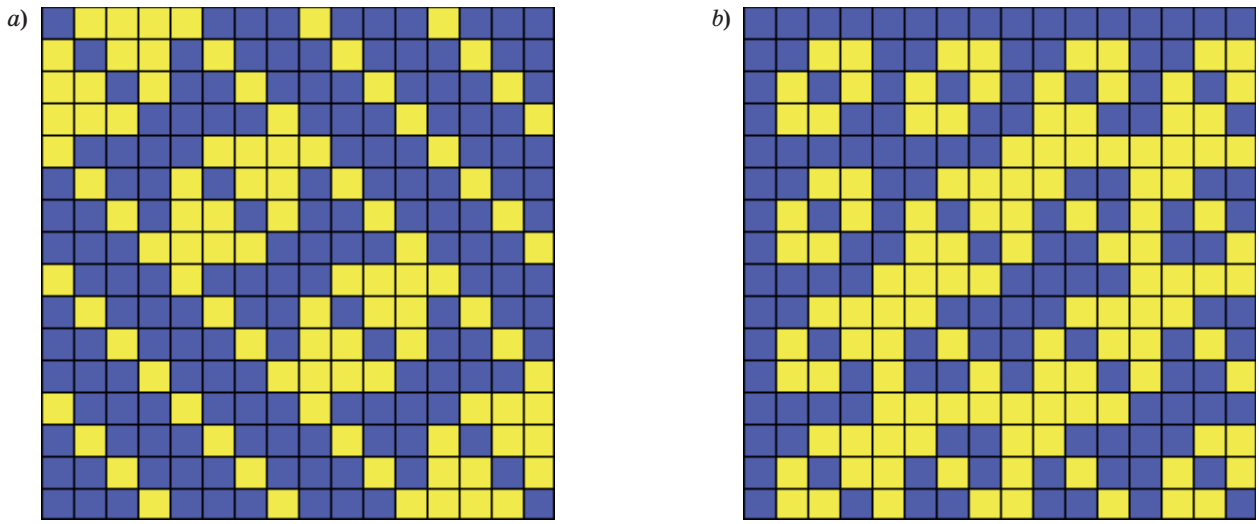
The values of the entries we will call "levels" of the matrix. An Hadamard matrix with entries $\{1, -1\}$ is a two-level matrix. A Mersenne matrix with entries $\{1, -b\}$, $0 < b < 1$ is also a two-level matrix. Now matrices, themselves, can belong to a layer.

Definition 1. In this paper a *matrix layer* is a set of quasi-orthogonal matrices with known functions for entries describing their dependence on $n = 4k - d$ for some d and all possible $k > 0$.

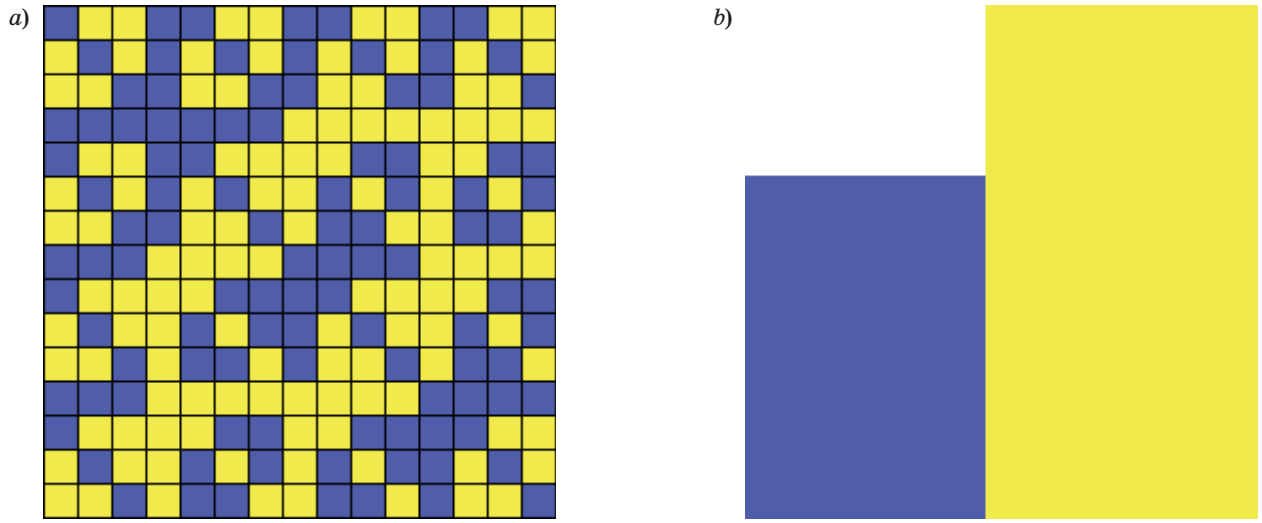
A Mersenne matrix, of order n, has negative entries $-b$, described by some function $b = f(n)$ and determined for all orders $n = 4k - 1$. Any fixed (non-varying) Mersenne matrix belongs to this layer. In the same way, Hadamard and Euler matrices with sizes $n = 4k - d$, $d = 0, 2$, as described in [1–3],



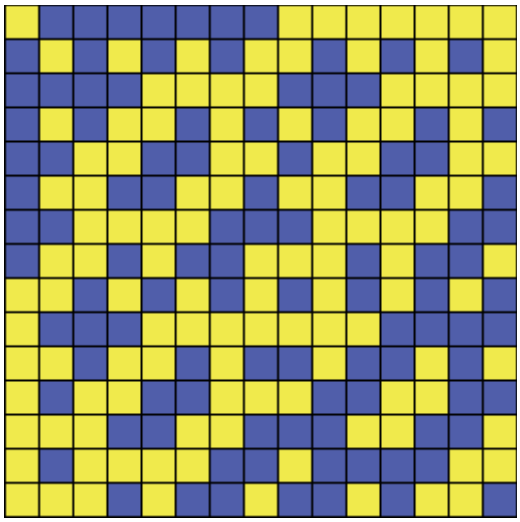
■ ***Fig. 1.*** Fermat matrix $\mathbf{F}_{17}$ (*a*) and histogram of moduli of its elements (*b*)



■ ***Fig. 2.*** Hadamard matrix $\mathbf{H}_{16}$ before (*a*) and after (*b*) normalization



■ ***Fig. 3.*** Mersenne matrix $\mathbf{M}_{15}$ (*a*) and histogram of moduli of its elements (*b*)

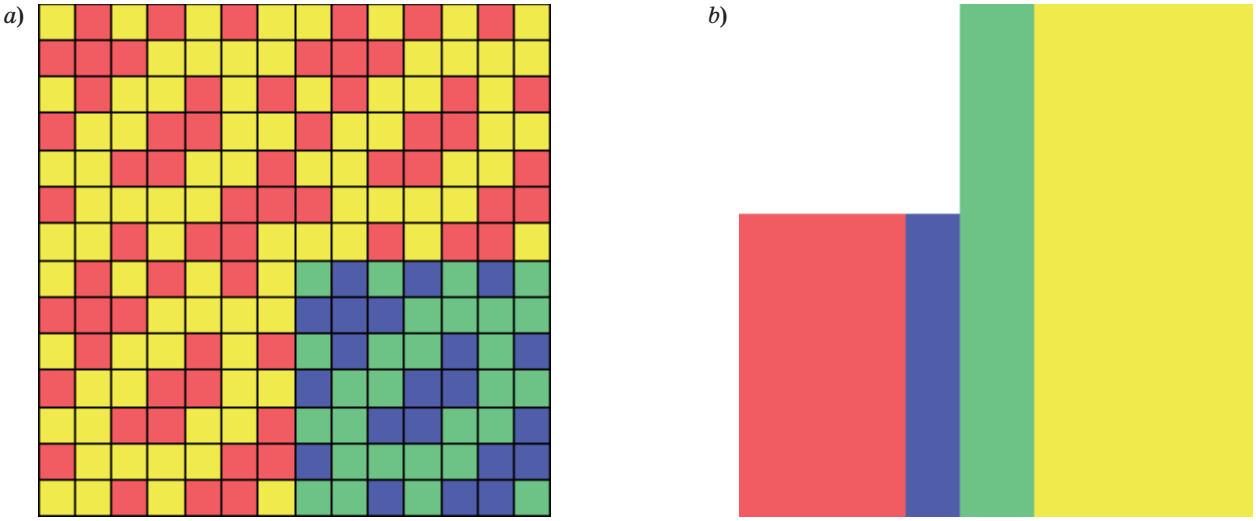


■ ***Fig. 4.*** Normalized Mersenne $\mathbf{M}_{15}$

belong to layers. Fermat matrices [11] do not form such layer, as their level functions are defined within a narrow set of values $n = 2^k + 1$ for even and some odd values of integer k.

Definition 2. In this paper a *section* is a set of quasi-orthogonal matrices of different layers, which depend on $n = 4k - d$ for some k and all possible $d = 0, 1, 2, 3$.

A particular (wider) section can be expanded by Fermat matrices using the same principle — the Fermat matrix (Fig. 1) with size $4k + 1$ can be used to find the corresponding Hadamard matrix (Fig. 2) with size $4k$ (the main order of the section). The Hadamard matrix can then be used to find a Mersenne matrix (Fig. 3, 4) with size $4k - 1$. This last matrix can be used to find an Euler (Fig. 5) matrix with size $4k - 2$ [3].



■ ***Fig. 5.*** Euler matrix $\mathbf{E}_{14}$ (*a*) and histogram of moduli of its elements (*b*)

Matrices with Few Levels

The matrices mentioned above are the manifestation of a mathematical object, described by its layers and sections [3]. The existence of any matrix in a section entails the existence of all other matrices of the same section because these matrices are mutually dependent.

Besides Hadamard matrices with entries $\{1, -1\}$ and similar to them Mersenne matrices with entries $\{1, -b\}$, $0 < b < 1$, there are other matrices with small numbers of levels. The Euler matrix $\mathbf{E}_n$ [3, 11] (shown in Fig. 5) is a square matrix of order $n = 4k - 2$ with entries $\{1, -1, b, -b\}$, where $\mathbf{E}_n^{\mathrm{T}}\mathbf{E}_n = \xi\,\mathbf{I}_n$, $\mathbf{I}_n$ is an identity matrix, $\xi = \dfrac{(n+2)+(n-2)b^2}{2}$, and $b = \dfrac{1}{2}$, when $n = 6$, in other cases $b = \dfrac{q-\sqrt{8q}}{q-8}$, where $q = n + 2$.

The number of levels is an important characteristic of a matrix set. The low number of levels does not guarantee existence of Belevitch matrices (conference matrices) [4, 5], they do not exist for order $n = 4k - 2$, if $n - 1$ is not sum of two squares.

The number of matrix levels increases with the value d in the interval $n = 4k - d$. Hadamard matrices have single level (by modulus of elements) matrices as the elements are 1 or −1. Mersenne matrices are two-level matrices; Euler matrices are four-level matrices. All these matrices have some minimal number of levels guaranteeing their existence for pre chosen orders [3].

Many sets of quasi-orthogonal matrices with low numbers of levels do not belong to a layer, they are special orthogonal per columns (Hadamard type) matrices: conference matrices with three levels of entries {0, 1, −1} are defined for orders shared with the bigger family of four levels Euler matrices. Paley [7] noted that any Hadamard matrix (or quasi-orthogonal matrix respectively) can be used to give matrix of the double size using the Sylvester algorithm. These we call these Sylvester constructions.

In this case, a new matrix branch appears: it does not intersect with any of the previous branches. Paley's observation induces us to study *artifact matrices* from the orthogonal matrix family (the Hadamard family), including the two-circulant *golden ratio matrix*. This is considered in this paper. The golden ratio matrix [13] and the two-circulant *golden ratio matrix* of order 10 lead to G-matrices of orders $n = 10 \cdot 2^k$, these sizes 10, 20, 40, 80, 160, 320, 640, etc. hold a special place in image processing algorithms.

Continuous Matrices

Continuous matrices are different from previously observed section matrices of the orthogonal (Hadamard) family, their level functions depend on more than one argument n. Therefore, for each n they generate not one, but a continuum of quasi-orthogonal matrices, described by a parametric dependence. This possibility follows from the interpretation of orthogonal or quasi-orthogonal matrix as a table of vector projections of the required orthogonal basis. We use optimal to denote matrices with maximal determinant. This allows us to get non-varying matrices for this continuum, known as orthogonal (Hadamard) matrices [6, 7].

Sub-optimal solutions are known for M-matrices [14, 15] with a small number of levels. Fig. 6 shows a continuous M-matrix $\mathbf{M}_{10}$.

$$\mathbf{M}_{10} = \begin{pmatrix} g & a & -c & -c & a & -a & a & b & b & a \\ a & g & a & -c & -c & a & -a & a & b & b \\ -c & a & g & a & -c & b & a & -a & a & b \\ -c & -c & a & g & a & b & b & a & -a & a \\ a & -c & -c & a & g & a & b & b & a & -a \\ -a & a & b & b & a & -g & -a & c & c & -a \\ a & -a & a & b & b & -a & -g & -a & c & c \\ b & a & -a & a & b & c & -a & -g & -a & c \\ b & b & a & -a & a & c & c & -a & -g & -a \\ a & b & b & a & -a & -a & c & c & -a & -g \end{pmatrix}.$$

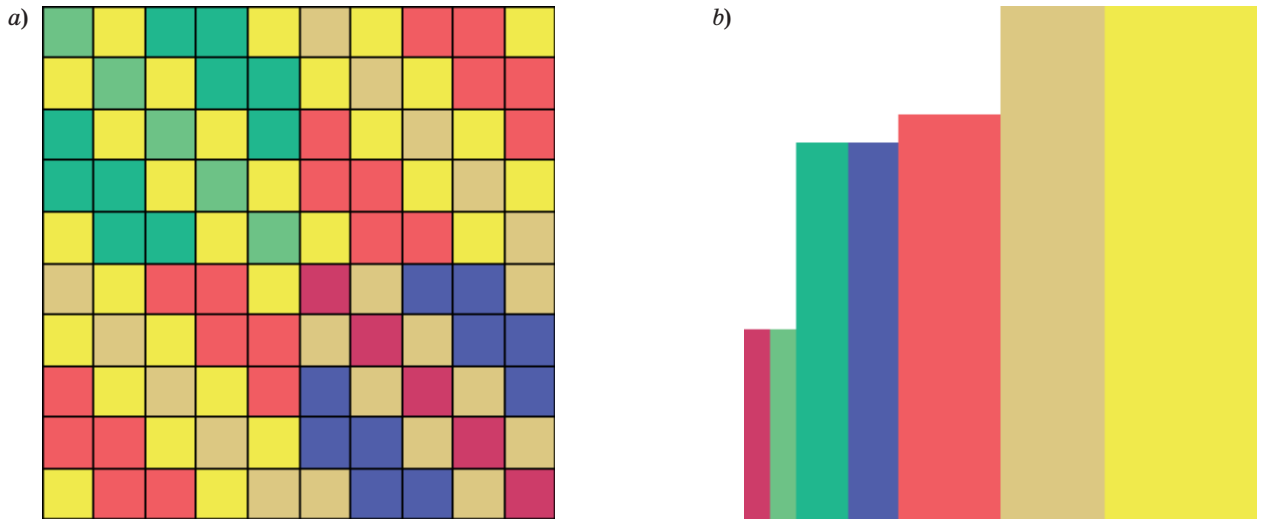
The upper module level from set of levels $a \geq b \geq c \geq g$ is $a = 1$. The second and the third levels depend on the lower level g as $b^2 + 2(b-1) + 2(g-c) + c^2 = 0$, $c = 1/(g+1)$.

The coloured matrix portrait represents the structure and levels of entries — every level has its own colour.

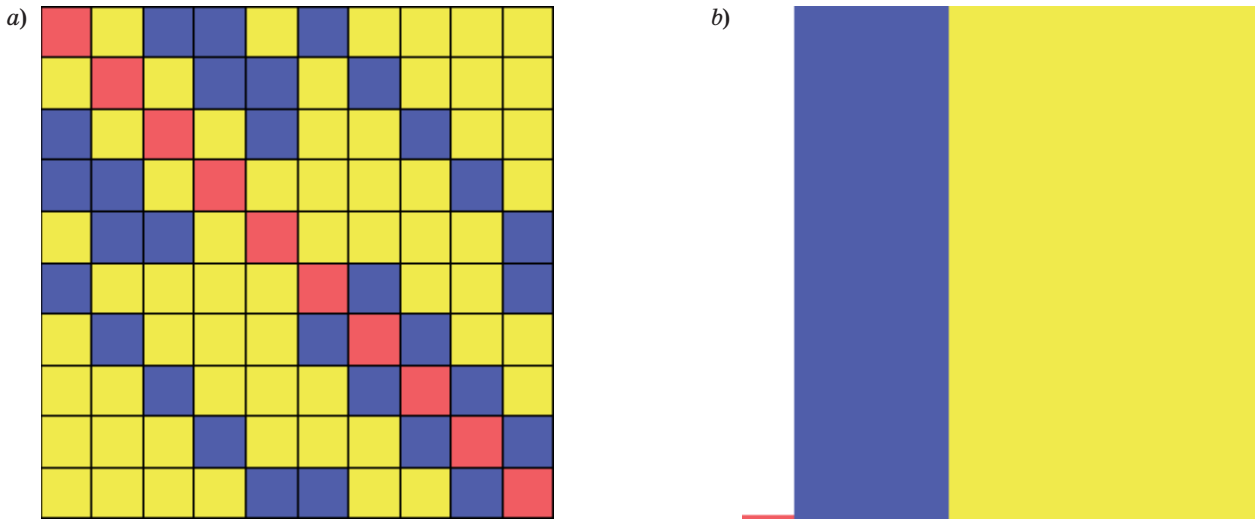
The continuous matrix $\mathbf{M}_{10}$ is a matrix with a low number of changeable levels and is notable by its solutions: two bounds (Fig. 7, 8) of a continuum.

One solution (see Fig. 7) is the two-circulant Belevitch matrix $\mathbf{C}_{10}$ since when $b = c = a = 1$ we have $g = 0$.

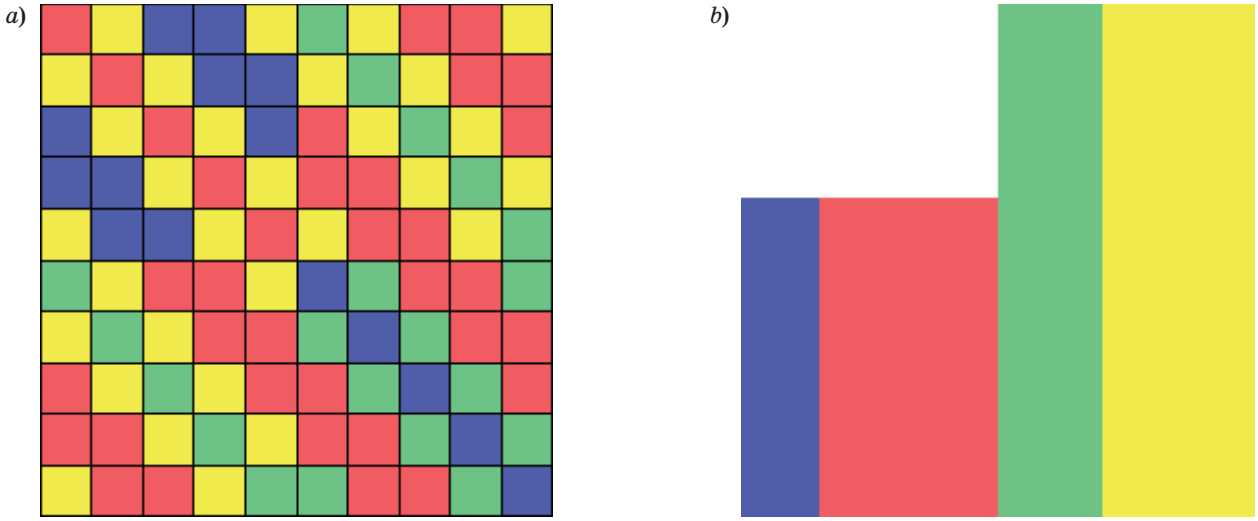
We call the second solution (see Fig. 8), with $b = c = g < a = 1$, as two-circulant *golden ratio matrix* $\mathbf{G}_{10}$.



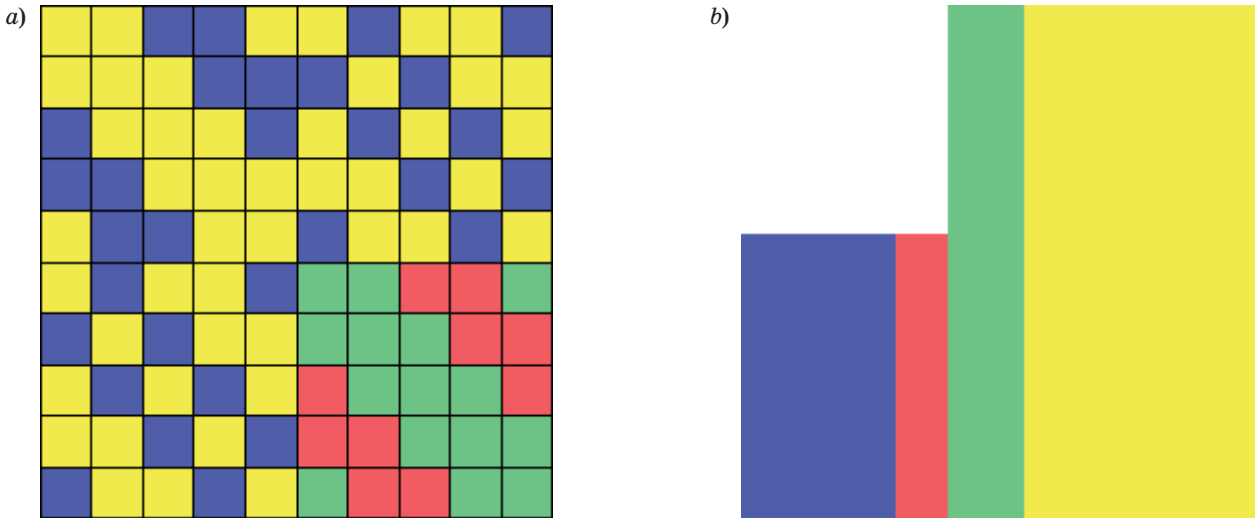
■ ***Fig. 6.*** Portrait of matrix $\mathbf{M}_{10}$ (*a*) and histogram of moduli of its elements (*b*)



■ ***Fig. 7.*** Belevitch matrix $\mathbf{C}_{10}$ (*a*) and histogram of moduli of its elements (*b*)



■ ***Fig. 8.*** Golden ratio matrix $\mathbf{G}_{10}$ (*a*) and histogram of moduli of its elements (*b*)



■ ***Fig. 9.*** Euler matrix $\mathbf{E}_{10}$ (*a*) and histogram of modules of its elements (*b*)

$$\mathbf{G}_{10} = \begin{pmatrix} g & a & -g & -g & a & -a & a & g & g & a \\ a & g & a & -g & -g & a & -a & a & g & g \\ -g & a & g & a & -g & g & a & -a & a & g \\ -g & -g & a & g & a & g & g & a & -a & a \\ a & -g & -g & a & g & a & g & g & a & -a \\ -a & a & g & g & a & -g & -a & g & g & -a \\ a & -a & a & g & g & -a & -g & -a & g & g \\ g & a & -a & a & g & g & -a & -g & -a & g \\ g & g & a & -a & a & g & g & -a & -g & -a \\ a & g & g & a & -a & -a & g & g & -a & -g \end{pmatrix}.$$

It is distinguished by the equation $g^2 + g - 1 = 0$, well known by its irrational roots called the *golden ratio* in the Fibonacci number theory. In this case we are interested in the lower level $g = 0.618...$ that proportional to the inversion of 1.618... . Matrices with such elements were for the first time provided in [13].

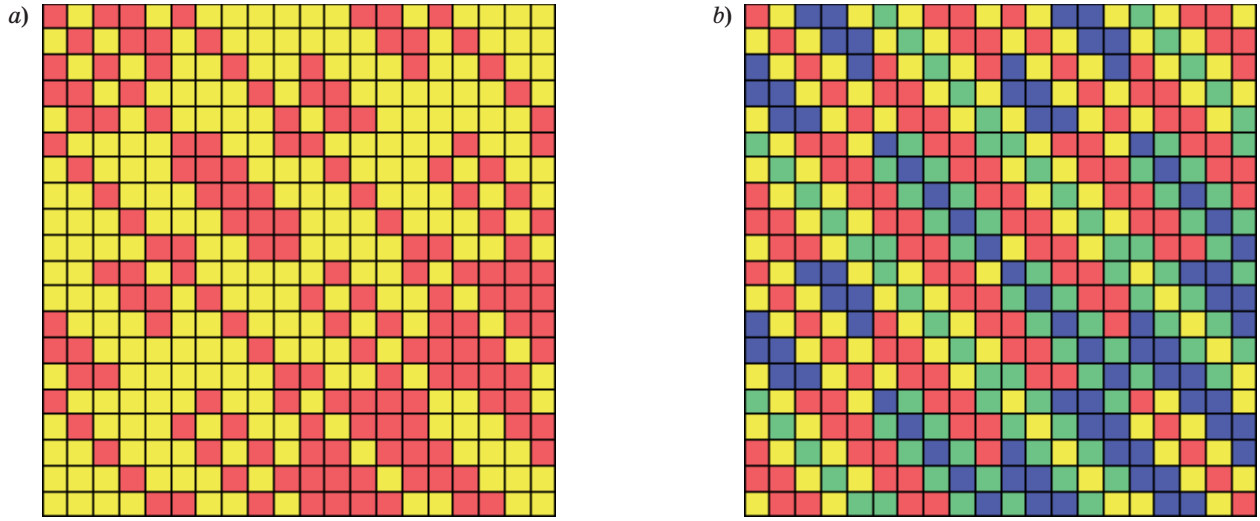
Let's note that histograms for golden ratio matrix $\mathbf{G}_{10}$ and Euler matrix $\mathbf{E}_{10}$ are similar to each other (see Fig. 8, 9), they both are two-level (by modulus) matrices.

Golden ratio matrices

Consequently, all golden ratio matrices are defined on orders $n = 10 \cdot 2^k$.

For them, as for all Hadamard family matrices, matrix $\mathbf{G}_{10}$ is the starting point for the sequence of matrices, found by iterations

$$\mathbf{G}_{2n} = \begin{pmatrix} \mathbf{G}_n & \mathbf{G}_n \\ \mathbf{G}_n & -\mathbf{G}_n \end{pmatrix}.$$



■ ***Fig. 10.*** Hadamard matrix $\mathbf{H}_{20}$ (*a*) and golden ratio matrix $\mathbf{G}_{20}$ (*b*)

The value of modulus level g is constant. This implies, that golden ratio matrices and Hadamard-type matrices are two boundary solutions of a continuum matrix (Fig. 10).

Acknowledgements

The authors would like to acknowledge the great help of Professor Jennifer Seberry with translation and discussion of the content of this paper. The authors also wish to sincerely thank Tamara Balonina for converting this paper into printing format.

Conclusion

This paper describes a golden ratio matrix $\mathbf{G}_{10}$ and sequence of such G-matrices, represented by the example $\mathbf{G}_{20}$. These matrices are closely associated with Belevitch and Hadamard-type matrices, their specific structures and algorithms to find them.

Golden ratio matrices, represented by $\mathbf{G}_{10}$, connect with Belevitch matrices as bounds of continuum. The latter (coexisting with Euler matrices) have no solutions for the orders 22, 34, 58 and so on. So golden ratio matrices do not have a layer by the determination.

The range of application of mathematical models as orthogonal bases is wide [3]. There is a curious idea to use the continuous matrix as a model of phase transformations taking place during the crystallization of cooled alloys [16].

The special boundary points of the continuous matrix can explain the patterns, observed in the tests. The two level golden ratio matrix can be a model reflecting the details of crystal structure [17]. The peculiarities of the quasi-crystal problem are present here — the dichotomy of elements, associated with the golden ratio level and specific orders [18]. Matrix models may be calculated and used to predict the existence of new materials [19].

References

1. **Sergeev A. M.** Generalized Mersenne Matrices and Balonin's Conjecture. *Automatic Control and Computer Sciences*, 2014, vol. 48, no. 4, pp. 214–220.
2. **Balonin N. A., Sergeev M. B.** On the Issue of Existence of Hadamard and Mersenne Matrices. *Informatsionno-upravliaiushchie sistemy*, 2013, no. 5(66), pp. 2–8 (In Russian).
3. **Balonin N. A., Sergeev M. B.** Local Maximum Determinant Matrices. *Informatsionno-upravliaiushchie sistemy*, 2014, no. 1(68), pp. 2–15 (In Russian).
4. **Belevitch V.** Theorem of 2n-terminal Networks with Application to Conference Telephony. *Electr. Commun.*, 1950, vol. 26, pp. 231–244.
5. **Balonin N. A., Seberry J.** A Review and New Symmetric Conference Matrices. *Informatsionno-upravliaiushchie sistemy*, 2014, no. 4(71), pp. 2–7.
6. **Hadamard J.** Résolution d'une Question Relative aux Dé terminants. *Bulletin des Sciences Mathématiques*, 1893, vol. 17, pp. 240–246 (In French).
7. **Paley R. E. A. C.** On Orthogonal Matrices. *Journal of Mathematics and Physics*, 1933, vol. 12, pp. 311–320.
8. **Balonin N. A., Sergeev M. B.** M-matrices. *Informatsionno-upravliaiushchie sistemy*, 2011, no. 1, pp. 14–21 (In Russian).
9. **Balonin N. A., Sergeev M. B., Mironovsky L. A.** Calculation of Hadamard–Mersenne Matrices. *Informatsionno-upravliaiushchie sistemy*, 2012, no. 5(60), pp. 92–94 (In Russian).

10. **Balonin N. A.** Existence of Mersenne Matrices of 11th and 19th Orders. *Informatsionno-upravliaiushchie sistemy*, 2013, no. 2, pp. 89 – 90 (In Russian).
11. **Balonin N. A., Sergeev M. B.** Two Ways to Construct Hadamard–Euler Matrices. *Informatsionno-upravliaiushchie sistemy*, 2013, no. 1(62), pp. 7–10 (In Rusian).
12. **Balonin N. A., Sergeev M. B., Mironovsky L. A.** Calculation of Hadamard-Fermat Matrices. *Informatsionno-upravliaiushchie sistemy*, 2012, no. 6(61), pp. 90–93 (In Russian)
13. **Balonin N. A., Sergeev M. B.** Matrix of Golden Ratio G10. *Informatsionno-upravliaiushchie sistemy*, 2013, no. 6(67), pp. 2–5 (In Russian).
14. **Balonin N. A., Sergeev M. B.** M-matrices. *Informatsionno-upravliaiushchie sistemy*, 2011, no. 1, pp. 14–21 (In Russian).
15. **Balonin Yu. N., Sergeev M. B.** M-matrix of 22nd order. *Informatsionno-upravliaiushchie sistemy*, 2011, no. 5(54), pp. 87–90 (In Russian).
16. **Balonin N. A., Sergeev M. B.** M-matrices and Crystal Structures. *Vestnik Magnitogorskogo gosudarstvennogo tekhnicheskogo universiteta*, 2013, no. 3(43), pp. 58–62 (In Russian).
17. **Shechtman D., Blech I., Gratias D., Cahn J. W.** Metallic Phase with Long-Range Orientational Order and No Translational Symmetry. *Physical Review Letters*, 1984, vol. 53, pp. 1951–1954.
18. **Комаров S. M.** Doubt Crystal. Available at http://elementy.ru/lib/431491 (accessed 30.09.2014) (In Russian).
19. **Balonin Yu. N., Sergeev M. B.** The Algorithm and Program for Searching and Studying of M-matrices. *Nauchno-tekhnicheskii Vestnik Informatsionnykh Tekhnologii, Mekhaniki i Optiki*,, 2013, no. 3, pp. 82–86 (In Russian).

УВАЖАЕМЫЕ АВТОРЫ!

Научные базы данных, включая SCOPUS и Web of Science, обрабатывают данные автоматически. С одной стороны, это ускоряет процесс обработки данных, с другой — различия в транслитерации ФИО, неточные данные о месте работы, области научного знания и т. д. приводят к тому, что в базах оказывается несколько авторских страниц для одного и того же человека. В результате для всех по отдельности считаются индексы цитирования, снижая рейтинг ученого.

Для идентификации авторов в сетях Thomson Reuters проводит регистрацию с присвоением уникального индекса (ID) для каждого из авторов научных публикаций.

Процедура получения ID бесплатна и очень проста: входите на страницу http://www.researcherid.com, слева под надписью «New to ResearcherID?» нажимаете на синюю кнопку «Join Now It's Free» и заполняете короткую анкету. По указанному электронному адресу получаете сообщение с предложением по ссылке заполнить полную регистрационную форму на ORCID. Получаете ID.

УДК 004.8

АССОЦИАТИВНАЯ ИНТЕЛЛЕКТУАЛЬНАЯ МАШИНА С ТРЕМЯ СИГНАЛЬНЫМИ СИСТЕМАМИ

В. Ю. Осипов[a], *доктор техн. наук, профессор*
[a]*Санкт-Петербургский институт информатики и автоматизации РАН, Санкт-Петербург, РФ*

Цель: *расширение функциональных возможностей ассоциативных интеллектуальных машин по обработке динамических сигналов.* ***Методы:*** *для наделения ассоциативных интеллектуальных машин новыми возможностями использованы подходы к построению таких машин с двумя сигнальными системами на основе рекуррентных нейронных сетей с управляемыми синапсами. Применены решения по изменению пространственных характеристик обрабатываемых сигналов и формированию их копий.* ***Результаты:*** *предложено наделять ассоциативную интеллектуальную машину третьей сигнальной системой, позволяющей осуществлять управляемый отрыв нейронной сети этой машины от исполнительных устройств и изменять характеристики выходных сигналов в зависимости от текущих состояний слоев. В интересах этого формируются и обрабатываются параллельно вторые копии сигналов в виде сигнально-шумовых групп единичных образов. Помимо управления пространственными параметрами расходящихся единичных образов, передаваемых от слоя к слою в рекуррентной нейронной сети, рекомендовано управлять пространственной селекцией сходящихся единичных образов. Сформулированы правила такого управления.* ***Практическая значимость:*** *показано, что за счет наличия у ассоциативной интеллектуальной машины третьей сигнальной системы расширяются ее возможности по интеллектуальному взаимодействию с внешним миром. У такой машины появляется возможность сначала все «обдумать», а потом действовать, не выдавая на исполнительные устройства все текущие результаты «мышления». Кроме этого, дополнительная пространственная селекция сигналов позволяет повысить избирательность ассоциативного взаимодействия обрабатываемых сигналов, улучшить их запоминание и извлечение из памяти.*

Ключевые слова *— ассоциативная машина, сигнальная система, интеллектуальная обработка сигналов.*

Введение

Создание высокоинтеллектуальных машин, способных оперативно решать широкий спектр трудно формализуемых творческих задач подобно человеку, является одной из актуальных проблем современности. Наличие таких машин позволит не только облегчить труд человека и повысить его безопасность, но и выйти на новый уровень познавательной, созидательной деятельности в различных сферах и средах. Пока все попытки решения данной проблемы не увенчались успехом. Это обусловлено рядом причин. Среди них — отсутствие полноценных моделей «мышления» машин, а также несовершенство технологий их реализации.

При построении моделей «мышления» машин используют два основных подхода [1]. Первый из них, называемый программно-прагматическим, предусматривает анализ мышления и поведения человека в зависимости от воздействий на него различных сигналов. По результатам этого анализа осуществляют синтез соответствующих моделей в виде программно реализуемых правил. Затем используют разработанные программы для наделения машин интеллектуальностью. Однако получаемые таким образом модели отражают лишь частные случаи «мыслительных» процессов. Фактически машины с таким «интеллектом» решают творческие задачи согласно правилам, которые заложили в них разработчики.

Второй, бионический подход, базируется на анализе реальных биологических процессов, происходящих в мозге живых существ, и построении обучаемых искусственных нейронных сетей, моделирующих его деятельность. В настоящее время известно несколько типов таких сетей [2–4], которые применяют для решения различных частных творческих задач. Особого внимания заслуживают модели, позволяющие обрабатывать информацию в реальном времени. Несмотря на ряд существенных результатов, полученных в последние годы [2, 5, 6], известные нейронные сети как модели искусственного «мозга» по функциональности также пока далеки от совершенства и не обеспечивают для машин широких интеллектуальных возможностей. Кроме того, есть трудности с реализацией интеллектуальных машин на основе рекуррентных нейронных сетей больших размеров. Традиционное программное моделирование их малопригодно из-за высокой вычислительной сложности. Способы аппаратной реализации таких машин требуют дальнейшего развития.

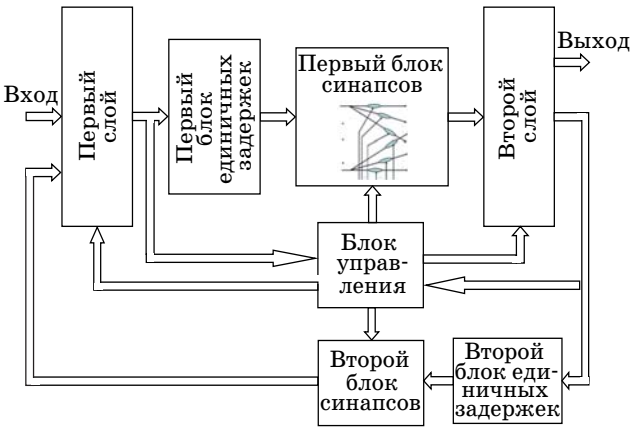
Необходим поиск новых идей и технологий, позволяющих расширить возможности машин по интеллектуальной обработке информации.

В рамках бионического подхода предлагается ассоциативная интеллектуальная машина с тремя сигнальными системами, наделенная новыми свойствами по решению трудно формализуемых творческих задач.

Постановка задачи совершенствования ассоциативной интеллектуальной машины

Опираясь на особенности электрических процессов, протекающих в мозге реальных биологических систем [7, 8], рассмотрим в качестве

прототипа предлагаемого решения ассоциативную интеллектуальную машину (АИМ) с двумя сигнальными системами [9–11]. Ее основу составляет совокупность взаимосвязанных датчиков, двухслойной рекуррентной нейронной сети (РНС) с управляемыми синапсами (рис. 1) и исполнительных устройств. Обратные связи РНС замыкают контуры с временем задержки единичных образов, меньшим времени невосприимчивости нейронов после их возбуждения. Каждый нейрон одного слоя в общем случае связан со всеми нейронами другого слоя и может находиться в трех состояниях: ожидания, возбуждения и невосприимчивости. Из РНС путем управления синапсами могут быть сформированы различные другие сети. В РНС подают групповой сигнал, предварительно разложенный на составляющие. Каждая из них преобразована в последовательность единичных образов (ЕО) с частотой повторения как функции от амплитуды соответствующей составляющей. Групповой сигнал состоит из полезного сигнала, просуммированного с маломощным шумом, и самого этого шума. Полезный сигнал также может быть групповым, состоящим из разных полезных воздействий. Групповой входной сигнал представляют в сети в виде последовательных групповых совокупностей единичных образов (СЕО) в соответствии с предварительно заданными правилами его распознавания с учетом обратных результатов обработки. При передаче от слоя к слою такие СЕО сдвигают вдоль слоев с учетом текущих состояний последних и продвигают эти совокупности вдоль них по заданной (в частности, спиральной) схеме. Также при передаче от слоя к слою СЕО, состоящих из сигнально-шумовых и шумовых групп, формируют копии сигнально-шумовых групп. Формирование этих копий и их обработку осуществляют с учетом изменения форм поперечных сечений расходящихся ЕО и поворотов этих образов вокруг направлений их передачи в зависимости от текущих состояний слоев. Результаты распознавания сигналов запоминают на элементах сети. Причем за счет частичного отражения СЕО от нейронов принимающего слоя частично стирают с синапсов устаревшую информацию [12]. В качестве результатов обработки используют последовательные копии сигнально-шумовых групп ЕО на выходном слое сети после обратного преобразования в соответствующие им исходные сигналы. Однозначное соответствие между входом и выходом сети обеспечивается за счет приоритетности коротких связей между нейронами взаимодействующих слоев. В этой АИМ первая сигнальная система отвечает за формирование «условно-рефлекторных» связей и реакций по результатам воздействия входных сигналов. Она обрабатывает оригинальные групповые сигналы. Вторая сигнальная система реализует саму интеллектуальную обработку информации и оперирует копиями последовательных сигнально-шумовых групп. За счет изменения в РНС форм поперечных сечений расходящихся ЕО и поворотов этих образов вокруг направлений их передачи в зависимости от текущих состояний слоев можно временно отрывать обработку сигналов во второй сигнальной системе от первой. Это позволяет исключить подавление обратных результатов распознавания входным потоком и увеличить глубину обработки сигналов.



■ ***Рис. 1.*** Структурная схема двухслойной РНС с управляемыми синапсами

К недостаткам данной АИМ следует отнести то, что при приеме совокупностей единичных образов в РНС не предусмотрена их управляемая пространственная селекция. Кроме того, в АИМ отсутствует управляемый отрыв РНС от исполнительных устройств. Действия АИМ напрямую отражают все результаты обработки сигналов в РНС, что не желательно, так как не все они должны реализовываться. Не раскрыты правила изменения поперечных сечений расходящихся и сходящихся ЕО в РНС с учетом текущих состояний слоев. Это ограничивает интеллектуальные возможности АИМ и затрудняет ее практическую реализацию.

Необходимо усовершенствовать известную АИМ, расширить ее возможности по интеллектуальной обработке информации.

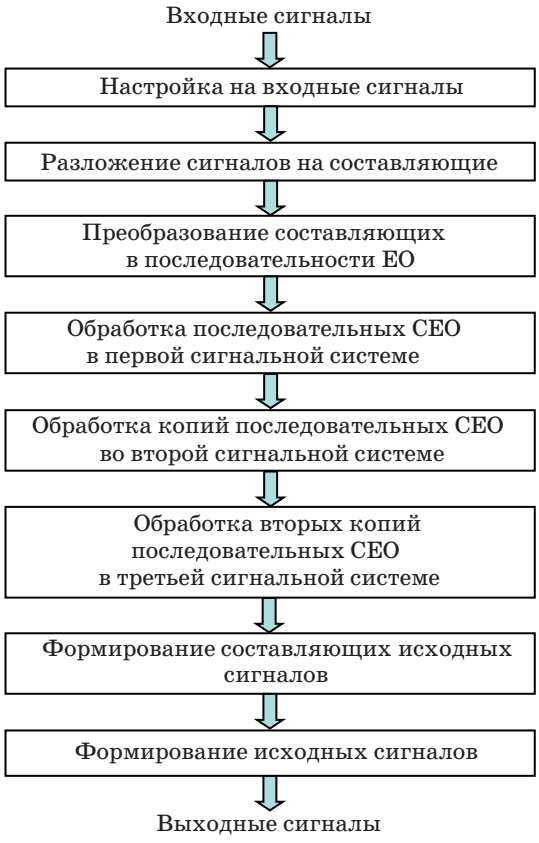
Метод обработки информации

Для расширения возможностей АИМ предлагается наделить ее третьей сигнальной системой и повысить избирательность ассоциативного взаимодействия сигналов в ее РНС в зависимости от текущих состояний слоев. С формальной точки зрения процесс обработки информации в усовершенствованной АИМ с тремя сигнальными системами можно представить в виде схемы обобщенных

действий (рис. 2). Согласно этой схеме, АИМ должна настраиваться на входные сигналы в зависимости от текущих состояний слоев РНС так, чтобы имело место наибольшее их ассоциативное взаимодействие с запомненными сигналами. Основная обработка сигналов в виде копий последовательных совокупностей (сигнально-шумовых групп) ЕО осуществляется во второй сигнальной системе, как и в прототипе. Отличие этой схемы от известных решений в том, что предлагается формировать и обрабатывать в АИМ (в ее третьей сигнальной системе) вторые копии сигнально-шумовых групп ЕО с учетом изменения пространственных параметров расходящихся и сходящихся единичных образов в зависимости от текущих состояний слоев. Это позволяет АИМ сначала все «обдумать», а потом действовать. Причем дополнительно на третью сигнальную систему могут возлагаться функции по формированию ряда самостоятельных устойчивых цепочек сигналов для реализации типовых действий АИМ. В этом случае вторая сигнальная система при необходимости может ограничиваться лишь запуском и прерыванием генерации этих цепочек сигналов (программ действий). Кроме этого, возможность формирования таким образом вторых копий сигналов позволяет со стороны второй сигнальной системы плавно изменять параметры действий АИМ (их масштаб, быстроту, силу). С физической точки зрения это сводится к изменению частот следования ЕО в их последовательностях и, соответственно, амплитуд составляющих исходных сигналов. В результате наличие третьей сигнальной системы в АИМ позволяет существенно расширить ее функциональные возможности, прежде всего, по интеллектуальному взаимодействию с внешним миром. В такой АИМ циклическая обработка сигналов может реализовываться во всех трех сигнальных системах. Причем управляемые циклы в общем случае реализуются внутри каждой сигнальной системы. Управление ими осуществимо также за счет изменения форм и поворотов поперечных сечений расходящихся и сходящихся ЕО.

Заметим, что при формировании первых и вторых копий сигнально-шумовых групп ЕО предлагается учитывать изменения пространственных параметров не только расходящихся, но и сходящихся ЕО. Изменение пространственных параметров сходящихся ЕО успешно применяется в радиальных нейронных сетях [3, 4], однако в РНС с управляемыми синапсами такое применение имеет свою специфику.

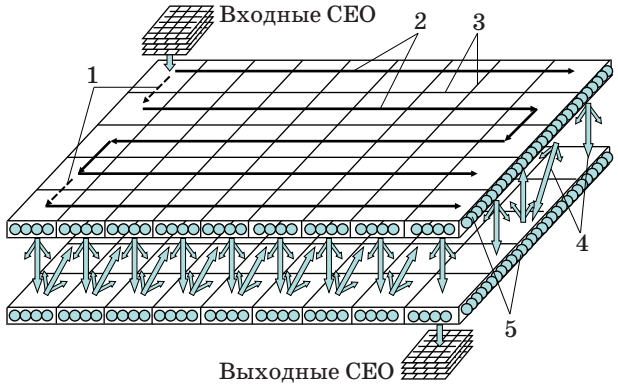
Для пояснения предлагаемого метода рассмотрим особенности РНС АИМ, позволяющие говорить об ее трех сигнальных системах.



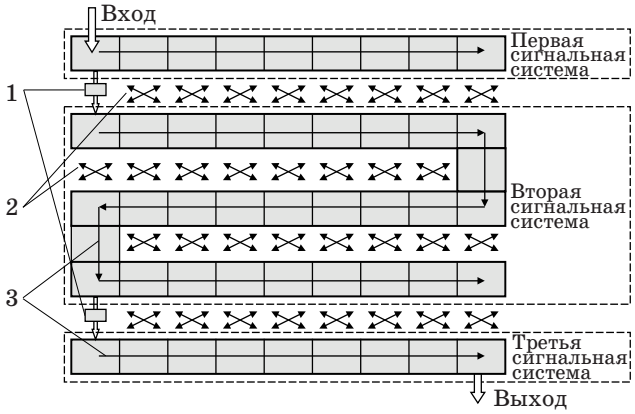
■ ***Рис. 2.*** Схема обработки сигналов в АИМ

Усовершенствованная структура РНС АИМ

Пример логической структуры РНС, в которой слои разбиты на поля, показан на рис. 3. Линии разбивки обозначены цифрой *3*. Сплошными стрелками *2*, *4* отражены направления продвижения СЕО, соответственно, вдоль и между слоями сети. Штрихпунктирными стрелками *1* указаны вспомогательные направления, по которым продвигаются формируемые из основных вспомогательные совокупности, несущие информацию о маломощном шуме, содержащемся



■ ***Рис. 3.*** Структура слоев РНС с тремя сигнальными системами

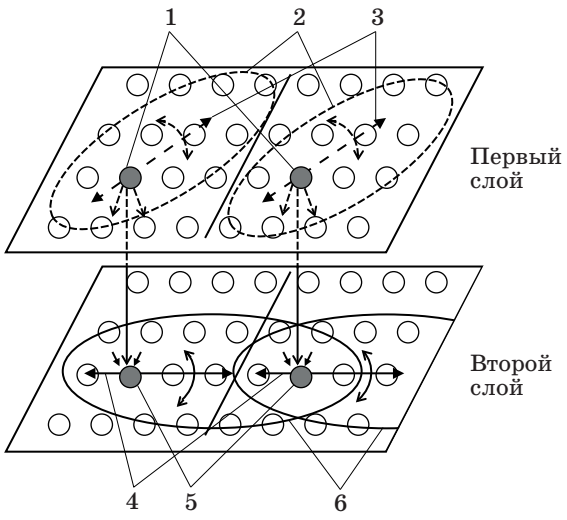


■ ***Рис. 4.*** Структура РНС с тремя сигнальными системами на уровне нейросетевых каналов продвижения СЕО

во входном сигнале. Нейроны первого и второго слоев сети имеют обозначение *5*. Этой структуре можно поставить в соответствие структуру РНС с тремя сигнальными системами на уровне нейросетевых каналов продвижения СЕО (рис. 4). На рис. 4 приняты обозначения: *1* — вспомогательные каналы (фильтры), пропускающие СЕО, относящиеся к маломощному шуму, отраженные на рис. 3 цифрой *1*; *2* — основные ассоциативные взаимодействия ЕО (формы и направления этих взаимодействий можно изменять в зависимости от текущих состояний слоев сети); *3* — направления продвижения СЕО вдоль слоев. Согласно рис. 3 и 4, входные СЕО поступают в первую сигнальную систему РНС АИМ. Она представляет из себя частную рекуррентную двухслойную сеть, связанную вспомогательным каналом и синапсами нейронов со второй частной РНС — второй сигнальной системой. Выделяемые за счет вспомогательного канала СЕО, относящиеся к маломощному шуму, продвигаются некоторое время в одном и том же направлении по первой и второй сигнальным системам. По суммарному времени воздействия на АИМ маломощный шум существенно превышает воздействие на нее полезных сигналов. Это позволяет не только устанавливать и поддерживать прочные ассоциативные связи между первой и второй сигнальными системами, но и стимулировать РНС. Посредством этих связей формируются и обрабатываются во второй сигнальной системе копии полезных сигналов. При этом учитываются изменения форм поперечных сечений расходящихся и сходящихся ЕО, а также повороты их вокруг направлений передачи и приема в зависимости от текущих состояний слоев. Заметим, что в отличие от прототипа дополнительно учитываются текущие параметры сходящихся ЕО. Наличие возможностей изменять параметры расходящихся и сходящихся ЕО в РНС обеспечивает не только развязку между всеми тремя сигнальными системами, но и изменение в широких пределах направлений ассоциативного взаимодействия сигналов в сети (формирование и завершение циклов обработки информации, избирательное запоминание информации, обращение к конкретным ресурсам и вызов из памяти связанных сигналов).

Предлагается преобразовывать в выходные сигналы не все результаты обработки последовательных копий СЕО во второй сигнальной системе, а лишь часть из них. В интересах этого в зависимости от текущих состояний слоев формируются вторые копии последовательных СЕО в третьей частной двухслойной РНС (в третьей сигнальной системе). Из этих копий затем получают соответствующие им исходные сигналы. Это позволяет АИМ при необходимости отрывать «мышление» от непосредственного управления исполнительными устройствами.

Для пояснения возможностей управления ассоциативным взаимодействием сигналов в РНС АИМ за счет изменения пространственных параметров расходящихся и сходящихся ЕО в зависимости от текущих состояний слоев рассмотрим рис. 5, где *1* — нейроны, сформировавшие расходящиеся ЕО с поперечными сечениями *6*; *2* — поперечные сечения сходящихся к нейронам *5* единичных образов; *3*, *4* — оси максимальной протяженности распределения плотности мощности в поперечных сечениях, соответственно, сходящихся и расходящихся ЕО. Из рис. 5 видно, что даже при заданных направленных формах поперечных сечений только за счет их поворотов можно существенно изменять направления ассоциативного взаимодействия сигналов в РНС. За счет же управления формами, придания им, например, многолепесткового вида в зависимости



■ ***Рис. 5.*** Примеры ориентации сглаженных эллиптических форм поперечных сечений расходящихся и сходящихся ЕО

от текущих состояний слоев возможности такого изменения резко возрастают. Причем дополнительный учет управляемой пространственной селекции ЕО при их приеме позволяет расширить внутреннее пространство состояний РНС и, согласно этому, ее возможности по обработке сигналов.

При условии, что пространственные сдвиги СЕО в РНС уже устоялись и фиксированы, наибольшие эффекты ассоциативного взаимодействия сигналов в АИМ могут достигаться в тех случаях, когда поперечные сечения расходящихся и сходящихся ЕО ориентированы, соответственно, на текущие энергетические минимумы принимающего слоя и текущие энергетические максимумы передающего слоя с учетом их удаленности от центров вращения этих сечений. При программной реализации АИМ для построения текущих поперечных сечений расходящихся и сходящихся ЕО в РНС все пространство этих сечений должно быть разбито на сектора. Для этих секторов предлагается определять соответствующие энергетические показатели с учетом удаленности локальных центров. Затем путем нормировки можно найти относительные коэффициенты направленности поперечных сечений для каждого выделенного сектора.

В целом при предлагаемом подходе веса синапсов нейронов рекомендуется определять умножением весовых коэффициентов на функцию ослабления расходящихся ЕО и функцию ослабления сходящихся ЕО. С физической точки зрения реализация такого управления синапсами осуществима за счет изменения их проводимости по соответствующим правилам.

Для выделения из входных сигналов маломощного шума в составе РНС должны присутствовать вспомогательные нейроны с большим временем невосприимчивости нейронов после возбуждения.

Результаты моделирования

В подтверждение справедливости предложенного подхода проводились вычислительные эксперименты, для чего была разработана усовершенствованная модель двухслойной РНС с числом нейронов в каждом слое 2016 единиц. Слои сети разбивались на логические поля размером 3×7 нейронов. Под первую сигнальную систему на каждом слое выделялась одна строка из 16 таких полей, под вторую — три, а под третью — две строки. Имитация выделения из входного сигнала маломощного шума осуществлялась прореживанием последовательных СЕО. Установлено, что дополнительная управляемая пространственная селекция сигналов в РНС предоставляет расширенные возможности по интеллектуальной ассоциативно-адресной обработке разнородной информации. Однако при программной реализации она также требует дополнительных вычислительных ресурсов. Подтверждено, что вторые копии сигналов могут успешно формироваться, как и первые. В случае, когда исключалось формирование вторых копий, вторая сигнальная система функционировала только на себя. При наличии вторых копий результаты обработки сигналов через третью сигнальную систему поступали на выход РНС.

Наличие в составе АИМ третьей сигнальной системы обеспечивает управляемый отрыв РНС от исполнительных устройств, а также плавное изменение параметров выходных воздействий машины. Изменяя форму и (или) поворачивая поперечные сечения расходящихся и сходящихся ЕО при формировании вторых копий сигнально-шумовых групп ЕО в третьей сигнальной системе, можно в широких пределах изменять уровень ассоциативного взаимодействия сигналов и варьировать амплитудами составляющих выходных сигналов. Напомним, что амплитуды этих составляющих являются функциями частот следования ЕО в соответствующих последовательностях.

Заключение

Предложенные решения по наделению АИМ третьей сигнальной системой и управляемой избирательностью взаимодействия сигналов в ее РНС позволяют понять, как могут развиваться процессы глубокой интеллектуальной ассоциативно-адресной обработки информации в таких машинах. Возможность управляемого отрыва второй сигнальной системы от входного потока и от воздействий на исполнительные устройства обеспечивает недостающие условия для полноценной интеллектуальной обработки информации в АИМ. Вторую сигнальную систему в предлагаемой АИМ теперь можно рассматривать как интеллектуальное нейросетевое ядро, принимающее решения не только о том, какие сигналы надо исключать из рассмотрения, но и какие подвергать глубокой обработке. На это ядро возлагаются также функции по выдаче на исполнительные устройства результатов, лишь «требующих» реализации, а не всех, как в прототипе. Формирование таких решений осуществимо путем изменения пространственных параметров ассоциативного взаимодействия сигналов в РНС в зависимости от текущих состояний ее слоев. При этом структура сигналов в предлагаемой АИМ не разрушается. Это обеспечивается, так же как и в прототипе, за счет приоритетности коротких связей между нейронами взаимодействующих слоев. Совместимость всех сигнальных систем в РНС по языку обработки сигналов достигается путем использования вспомогатель-

ных каналов (фильтров), пропускающих СЕО, относящиеся к маломощному шуму.

Разработанный метод обработки информации в АИМ и усовершенствованная структура ее РНС могут быть использованы при создании перспективных интеллектуальных машин. Рекомендуется реализовывать их в аналоговом варианте, позволяющем получить все преимущества параллельной ассоциативно-адресной интеллектуальной обработки различных сигналов.

Литература

1. **Аверкин А. Н., Гаазе-Рапопорт М. Г., Поспелов Д. А.** Толковый словарь по искусственному интеллекту. — М.: Радио и связь, 1992. — 256 с.
2. **Galushkin A. I.** Neural Networks Theory. — Springer-Verlag Berlin Heidelberg, 2007. — 396 p.
3. **Хайкин С.** Нейронные сети: полный курс. 2-е изд.: пер. с англ. — М.: Вильямс, 2006. — 1103 с.
4. **Осовский С.** Нейронные сети для обработки информации / пер. с польского И. Д. Рудницкого. — М.: Финансы и статистика, 2002. — 344 с.
5. **Amari S.** Dreaming of Mathematical Neuroscience for Half a Century // Neural Networks. 2013. N 37. P. 48–51.
6. **Palm G.** Neural Associative Memories and Sparse Coding // Neural Networks. 2013. N 37. P. 165–171.
7. **Альбертс Б.** и др. Молекулярная биология клетки. В 3 т.: пер. с англ. — М.: Мир, 1994. Т. 3. — 504 с.
8. **Физиология** человека / под ред. В. М. Покровского, Г. Ф. Коротько. — М.: Медицина, 2007. — 656 с.
9. **Осипов В. Ю.** Рекуррентная нейронная сеть с двумя сигнальными системами // Информационно-управляющие системы. 2013. № 4. С. 8–15.
10. **Осипов В. Ю.** Ассоциативная интеллектуальная машина с двумя сигнальными системами // Мехатроника, автоматизация, управление. 2013. № 8. С. 17–22.
11. **Осипов В. Ю.** Аналоговые ассоциативные интеллектуальные системы // Тр. СПИИРАН. 2013. Вып. 7(30). С. 141–155.
12. **Осипов В. Ю.** Стирание устаревшей информации в ассоциативных интеллектуальных системах // Мехатроника, автоматизация, управление. 2012. № 3. С. 16–20.

UDC 004.8

Three Signaling Systems Associative Machine

Osipov V. Yu.[a], Dr. Sc., Tech., Professor, Leading Research Fellow, osipov_vasiliy@mail.ru
[a]Saint-Petersburg Institute for Informatics and Automation of RAS, 39, 14 Line, V. O., 199178, Saint-Petersburg, Russian Federation

Purpose: Increasing the functionality of associative intelligent machines for dynamic signal processing. **Methods:** In order to give new features to associative intelligent machines, these machines are constructed with two signaling systems based on recurrent neural networks with operated synapses. Special solutions changed the spatial characteristics of the processed signals and the formation of their copies. **Results:** The idea is to provide an associative intelligent machine with the third signaling system, performing an operated separation of the neural network of this machine from the actuation mechanisms, and to change the output signal characteristics depending on the current states of the layers. This assumes producing and parallel processing of the second copies of the signals in the form of signal-and-noise groups of single images. Besides the control of the spatial parameters of the dispersing single images transferred from one layer to a layer in the recurrent neural network, it is recommended to control the spatial selection of the convergent single images. The rules of such control are formulated. **Practical relevance:** With the third signaling system, an associative intelligent machine has greater capabilities for intellectual interaction with the outer world. Such a machine has a chance to "think" first and act later, without sending all its transitional "thoughts" to the actuation mechanisms. Besides, the additional spatial selection of the signals increases the selectivity of the associative interaction between the processed signals, improving their storage and extraction from the memory.

Keywords — Associative Machine, Signaling System, Intellectual Processing of Signals.

References

1. Averkin A. N., Gaaze-Rapoport M. G., Pospelov D. A. *Tolkovyi slovar' po iskusstvennomu intellektu* [The Explanatory Dictionary on Artificial Intelligence]. Moscow, Radio i sviaz' Publ., 1992. 256 p. (In Russian).
2. Galushkin A. I. *Neural Networks Theory*. Springer-Verlag Berlin Heidelberg, 2007. 396 p.
3. Haykin S. *Neural Networks: A Comprehensive Foundation*. Second ed. Prentice Hall, 1988. 842 p.
4. Osovsky S. *Neironnye seti dlia obrabotki informatsii* [Neural Networks for Processing of Information]. Moscow, Finansy i statistika Publ., 2002. 344 p. (In Russian).
5. Amari S. Dreaming of Mathematical Neuroscience for Half a Century. *Neural Networks*, 2013, no. 37, pp. 48–51.
6. Palm G. Neural Associative Memories and Sparse Coding. *Neural Networks*, 2013, no. 37, pp. 165–171.
7. Alberts B., Bray D., Lewis J., Raff M., Roberts K., Watson J. D. (Eds.). *Molecular Biology of The Cell*. Second ed. New York, Garland Publishing, Inc., 1989. 1219 p.
8. Pokrovsky V. M., Korotko G. F. (Eds.). *Fiziologiia cheloveka* [Human Physiology]. Moscow, Meditsina Publ., 2007. 656 p. (In Russian).
9. Osipov V. Yu. The Recurrent Neural Network with Two Signal System. *Informatsionno-upravliaiushchie sistemy*, 2013, no. 4, pp. 8–15 (In Russian).
10. Osipov V. Yu. Double Signaling Systems Associative Machine. *Mekhatronika, avtomatizatsiia, upravlenie*, 2013, no. 8, pp. 17–22 (In Russian).
11. Osipov V. Yu. The Analog Associative Intelligent Systems. *Trudy SPIIRAN*, 2013, iss. 7(30), pp. 141–155 (In Russian).
12. Osipov V. Yu. Erase Outdated Information in Associative Intelligent Systems. *Mekhatronika, avtomatizatsiia, upravlenie*, 2012, no. 3, pp. 16–20 (In Russian).

УДК 004.931

ОБНАРУЖЕНИЕ И ИДЕНТИФИКАЦИЯ ОПАСНЫХ КОСМИЧЕСКИХ ОБЪЕКТОВ С ИСПОЛЬЗОВАНИЕМ АДАПТИВНЫХ МАТРИЧНЫХ ПРИЕМНИКОВ РАДИОИЗЛУЧЕНИЯ

А. Е. Городецкий[а], *доктор техн. наук, профессор*
И. Л. Тарасова[б], *канд. техн. наук, доцент*
[а]*Санкт-Петербургский государственный политехнический университет, Санкт-Петербург, РФ*
[б]*Институт проблем машиноведения РАН, Санкт-Петербург, РФ*

Цель: *рассмотрение возможности использования адаптивных матричных приемников миллиметрового диапазона при обнаружении и идентификации опасных космических объектов в радиоастрономической локации.* ***Результаты:*** *описаны пути создания адаптивных матричных приемников, основанных на приемниках радиоизлучения миллиметрового диапазона типа HEB (Hot Electron Bolometer). Такие приемники снабжены блоком коммутации, например на тонкопленочных криотронах, устанавливаемым вместе с матрицей HEB в гелиевый криостат. При этом необходимо исключать влияние на работу пикселей токов управления ключами коммутаторов за счет их экранирования. Представлены обобщенная структура адаптивного матричного приемника типа HEB и блок-схема его системы управления, содержащая физически реализуемую HEB-матрицу, виртуальную матрицу, запоминающее устройство, блок управления адаптивного матричного приемника, внешнее запоминающее устройство, блок адаптации, систему автоматического управления радиотелескопом, коммутатор, блок измерения колебаний контррефлектора, блок измерения колебаний главного зеркала, точку измерения колебаний на краю главного зеркала, точку измерения колебаний на краю контррефлектора. Приведен алгоритм работы системы управления адаптивного матричного приемника радиотелескопа в режиме обнаружения опасных космических объектов. Рассмотренные возможности применения адаптивных матричных приемников радиоизлучения миллиметрового диапазона позволяют сделать вывод, что при создании сверхбыстрых адаптивных матричных приемников целесообразно использовать HEB-пиксели и осуществлять необходимый подбор сверхпроводниковых материалов с малым временем электрон-фононного взаимодействия. Решена проблема создания адаптивного матричного приемника миллиметрового диапазона, обеспечивающего оптимальный выбор размеров пикселей матрицы, исходя из угла места, длины волны излучения и ожидаемых параметров опасных космических объектов, и высокую эффективность получения радиоизображений в радиоастрономической локации.* ***Практическая значимость:*** *предложенная система управления адаптивных матричных приемников типа HEB позволяет не только настраивать параметры матрицы для оптимального поиска опасных космических объектов по методу равносигнальной зоны, но и проводить аппаратными средствами эффективную предобработку их изображений, а в ряде случаев — и осуществлять идентификацию их формы.*

Ключевые слова *— матричный приемник, радиолокация, HEB-пиксели, система управления радиотелескопом, опасные космические объекты.*

Введение

Актуальность проблемы обнаружения и идентификации опасных космических объектов (ОКО) после падения Чебаркульского метеорита стала очевидной. Однако до сих пор готовность к защите Земли от астероидной опасности находится на очень низком уровне [1]. Поэтому в последнее время большое внимание уделяется разработке новых методов и средств локации ОКО. Среди них рассматриваются и методы радиоастрономической локации, хотя идея использования радиоастрономических инструментов для обнаружения малоразмерных космических объектов (космического мусора, астероидов или комет) не нова. Подобные задачи решались и решаются в радиолокационной астрономии. Например, на РТ-70 в Евпатории с 1992 г. проводятся с международным участием радиоастрономические и радиофизические эксперименты по изучению планет Солнечной системы, космического мусора; определению параметров движения астероидов, их формы и изображения. В 2005 г. с помощью РТ-70 впервые обнаружены мелкие фрагменты космического мусора на геостационарных орбитах. До 2009 г. РТ-70 два раза в год применялся в рамках проекта «Астероидная опасность» [2].

При использовании больших радиотелескопов миллиметрового диапазона значительно повышается чувствительность и, соответственно, высокое угловое разрешение. В частности, используя известные соотношения и существующие на сегодняшний день типы излучателей и приемников радиоизлучения миллиметрового диапазона, можно получить следующие оценки: объекты радиуса порядка $R = 100$ м можно обнаруживать на расстоянии почти в 3 раза дальше, чем от Земли до Луны, а при $R = 10$ м — почти на двойном расстоянии до Луны [3]. Однако радиоастрономическая локация с такими радиотелескопами неизбежно потребует применения матричных приемников радиоизлучения, что в значительной мере решает проблему поиска объектов узкой диаграммой направленности, так как поле зрения у матричного приемника может быть

значительно больше, чем у точечного. Очевидно, что в этом случае главной проблемой будет поиск объекта на матричном приемнике путем цифровой фильтрации и ряда пространственно-временных преобразований сигналов с выхода матричного приемника. Однако для обеспечения высокой эффективности использования матричных приемников для получения радиоизображений в радиоастрономической локации прежде всего необходимо решить проблему создания адаптивного матричного приемника (АМП) миллиметрового диапазона, обеспечивающего оптимальный выбор размеров пикселей матрицы исходя из угла места, длины волны излучения и ожидаемых параметров ОКО [4].

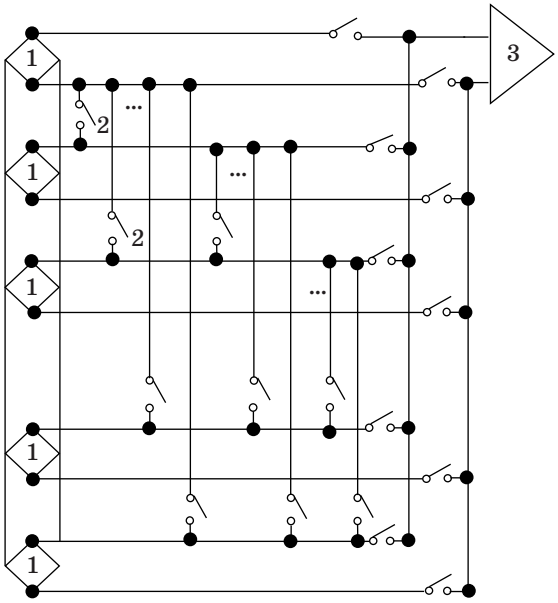
Возможности создания адаптивных матричных приемников

Известны приемники радиоизлучения миллиметрового диапазона типа НЕВ (Hot Electron Bolometer) [5–8], основанные на эффекте электронного разогрева в сверхпроводящих пленках [9]. Они имеют рекордные чувствительность (до $5 \cdot 10^{-14}$ Вт/Гц$^{1/2}$) и быстродействие (до 1 ТГц). Ближайшими их конкурентами являются полупроводниковые детекторы на основе InSb и Ge [10]. Оба имеют чувствительность порядка 10^{-12} Вт/Гц$^{1/2}$ и малое быстродействие (1 МГц для InSb и 200 Гц для Ge). Поэтому в качестве пикселей АМП-излучения целесообразно применять НЕВ болометры (рис. 1).

В работе [10] описываются болометры, использующие тонкие пленки из NbN и MoRe, которые имели время остывания электронной подсистемы 50 пс и 1 нс соответственно. Чувствительная область этих болометров имела размеры 0,1×1 мкм и была интегрирована с планарной широкополосной антенной. Для улучшения согласования с излучением использовалась кремниевая линза, фокусирующая излучение на антенну. Поэтому размер пикселя АМП, использующих указанные болометры, может составлять несколько десятков микрон. При создании сверхбыстрых АМП с указанными пикселями (НЕВ АМП) необходим подбор сверхпроводниковых материалов с малым временем электрон-фононного взаимодействия, а также создание условий для уменьшения времени выхода неравновесных фононов в подложку. Последнее достигается уменьшением толщины сверхпроводящей пленки и при улучшении акустического согласования сверхпроводящей пленки и подложки. Кроме того, при конструировании матрицы из указанных пикселей необходимо, прежде всего, уменьшить взаимовлияние последних за счет выбора оптимального расстояния между пикселями (скважности) и обеспечить наилучшее акустическое согласование сверхпроводящих пленок пикселей с подложкой. Естественно, что НЕВ АМП должен быть снабжен блоком коммутации, например, на тонкопленочных криотронах, устанавливаемым вместе с матрицей НЕВ в гелиевый криостат. При этом необходимо исключить влияние на работу пикселей токов управления ключами коммутаторов за счет их экранирования.

Из представленной на рис. 2 обобщенной структуры НЕВ АМП без блока управления видно, что за счет управления ключами *2* можно на усилителе *3* осуществлять суммирование сигналов с пикселей *1* в любом заданном сочетании. При этом [4] в большинстве случаев с достаточ-

■ ***Рис. 1.*** Чувствительный элемент НЕВ болометра, интегрированного с планарной спиральной антенной



■ ***Рис. 2.*** Структура НЕВ АМП

ной точностью для оценки оптимального размера пикселя $l_{\max}$ матричного приемника может быть использовано выражение

$$l_{\max} = \sqrt{k_z^2 \alpha_1^2 + k_r^2 \alpha_2^2},$$

где α_1 и α_2 — амплитуды колебаний краев главного зеркала и контррефлектора антенны радиотелескопа;

$$k_z = \frac{\sin \psi_1}{\sin \psi_3};$$

$$k_r = \frac{2 \sin \psi_2}{\sin \psi_3}.$$

Здесь ψ_1 — угол падения излучения на край поверхности главного зеркала; ψ_2 — угол падения излучения на край поверхности контррефлектора; ψ_3 — угол падения излучения от края поверхности контррефлектора на фокальную плоскость.

Указанные углы могут быть выражены через параметры антенны [4]. Очевидно, что за минимальный размер пикселя можно принять величину

$$l_{\min} = H,$$

где H — ширина диаграммы направленности антенны в фокальной плоскости, которая зависит от длины волны λ и размера апертуры (раскрыва) антенны d_a [4]:

$$H \approx \lambda / d_a.$$

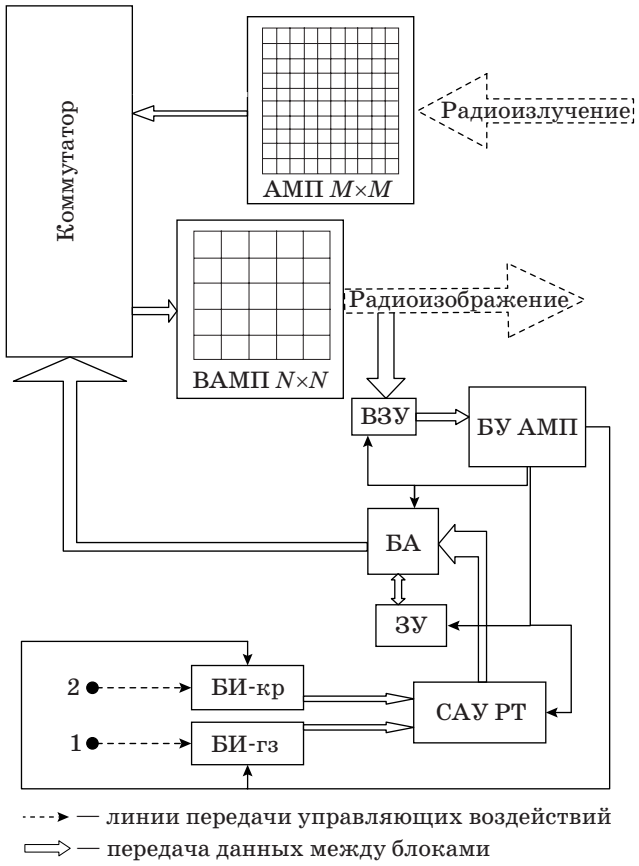
Блок-схема системы управления НЕВ АМП радиотелескопа представлена на рис. 3.

Блок управления АМП предназначен для обеспечения взаимодействия между остальными блоками системы управления. *БИ-гз* и *БИ-кр* измеряют колебания краев главного зеркала и контррефлектора. *ЗУ* предназначено для хранения исходных данных для расчета параметров *ВАМП*, а *ВЗУ* — для записи и хранения информации (сигналов) от *АМП*, который преобразует принимаемое излучение в электрические сигналы. *БА* вычисляет текущие и конечные значения размеров пикселей ВАМП, которые формируются *коммутатором* путем соответствующего объединения пикселей АМП. *САУ РТ* обеспечивает перемещение элементов антенны радиотелескопа по заданной траектории и передачу в БА текущих значений угла места β антенны, а также амплитуд и частот колебаний краев главного зеркала и контррефлектора.

Система управления в режиме настройки оптимальных размеров виртуальных пикселей работает следующим образом.

Блок управления выдает команду в САУ РТ на перемещение элементов антенны радиотелескопа по заданной траектории и команды на начало измерений в БИ-гз и БИ-кр, которые начинают измерять колебания краев главного зеркала и контррефлектора и передавать их в САУ РТ. Периодически САУ РТ вычисляет амплитуды и частоты колебаний краев главного зеркала и контррефлектора и по команде из БУ АМП передает эти величины вместе с измеренной в САУ РТ величиной угла места β антенны в БА.

Последний периодически вычисляет шаги измерения Δt_1 и записи Δt, период T, а также минимальную H, оптимальные l_{opt}, максимальный $l_{\max}$ и текущий l_n размеры пикселей ВАМП, используя исходные данные, получаемые из ЗУ по команде из БУ АМП. После вычислений БА по команде из БУ АМП периодически (с периодом Δt_1) передает вычисленное значение l_n в коммутатор, который коммутирует выходы пикселей



■ ***Рис. 3.*** Блок-схема системы управления НЕВ АМП радиотелескопа: ВАМП — виртуальный АМП; ЗУ — запоминающее устройство; БУ АМП — блок управления АМП; ВЗУ — внешнее запоминающее устройство; БА — блок адаптации; САУ РТ — система автоматического управления радиотелескопом; БИ-кр — блок измерения колебаний контррефлектора; БИ-гз — блок измерения колебаний главного зеркала; *1* — точка измерения колебаний на краю главного зеркала; *2* — точка измерения колебаний на краю контррефлектора

АМП таким образом, чтобы в ВАМП образовалась матрица с размером пикселя l_n. АМП через коммутатор и ВАМП преобразует излучение в радиоизображение, которое в виде электрических сигналов периодически (с периодом T) по команде из БУ АМП записывается в ВЗУ.

В дальнейшем алгоритм работы системы управления изменяется в зависимости от текущего режима работы радиотелескопа.

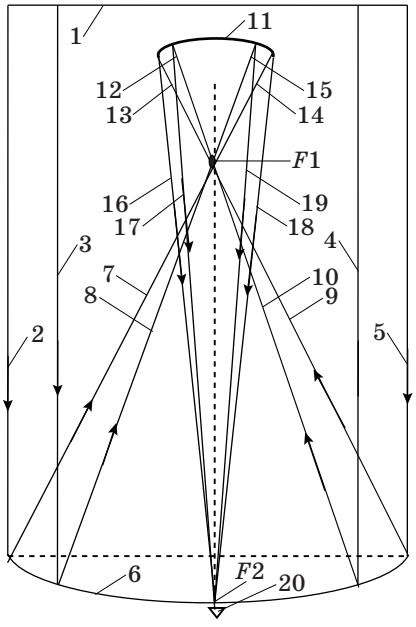
Режим обнаружения опасных космических объектов

Для обеспечения оптимальных параметров радиотелескопов с АМП в режиме радиоастрономической локации целесообразно производить подстройку (адаптацию) размеров пикселей матричных приемников излучения под параметры предполагаемых ОКО. При этом на начальном этапе, до захвата ОКО, устанавливается максимальный размер виртуального пикселя, т. е. все пиксели матрицы объединяются в один и производится сканирование главным зеркалом или контррефлектором антенны. Затем, после захвата ОКО, включается режим сканирования платформы матричного приемника или перископического зеркала и уточнение координат ОКО по методу равносигнальной зоны [11]. После чего размер виртуального пикселя l_n на каждом следующем проходе уменьшают в соответствии с формулой $l_n = (l_0 M)/2^n$, где l_0 — размер пикселя матричного приемника; M — размерность матрицы приемника; n — номер прохода. Процесс сканирования заканчивается либо когда будет $l_n = l_0$, либо когда изображение ОКО будет совершенно неразличимо на фоне помех.

Повысить качество изображения на матрице приемника излучения можно за счет периодической фокусировки зеркальной системы антенны путем адаптации поверхностей главного зеркала и контррефлектора к внешним воздействиям, основными из которых являются угол места и азимут, ветер и температура. В этом случае главное зеркало и контррефлектор должны состоять из щитов, положение которых может регулироваться специальными приводами в САУ [11]. Для уменьшения фазовых искажений при перемещении указанных щитов в согласованное положение следует учитывать длину волны принимаемого излучения [12].

В способе адаптации по измеренным значениям положений щитов главного зеркала [12] для каждого щита строят в компьютере свой аппроксимирующий параболоид таким образом, чтобы фокусное расстояние и положение основания каждого параболоида минимально отличались от соседних и при этом разности между их фокусными расстояниями были кратны длине волны принимаемого антенной радиоизлучения. Затем вычисляют отклонения каждого щита от соответствующего своего аппроксимирующего параболоида и осуществляют их необходимые перемещения. После окончания перемещений щитов главного зеркала измеряют положения каждого щита второго зеркала (контррефлектора), строят в компьютере модель хода лучей, отраженных от щитов главного зеркала в сторону контррефлектора, и положение отражающих поверхностей щитов контррефлектора. Вычисляют рассогласования крайних лучей, отраженных от щитов главного зеркала, с положениями соответствующих краев отражающих поверхностей щитов контррефлектора. Далее с помощью САУ перемещают каждый щит контррефлектора в сторону уменьшения указанных рассогласований таким образом, чтобы положения их фокусов минимально расходились между собой и с положением вторичного фокуса зеркальной системы и (или) с положением приемника излучения при условии, что длины лучей (оптических путей) от первичного фокуса до отражающих поверхностей щитов контррефлектора и расхождения между ними, а также длины лучей (оптических путей) от отражающих поверхностей щитов контррефлектора до вторичного фокуса и расхождения между ними были кратны длине волны принимаемого излучения (рис. 4).

Схема зеркальной системы антенны (см. рис. 4) содержит плоскость *1* фронта принимаемого антенной радиоизлучения; лучи *2–5* принимаемого антенной радиоизлучения, падающего



■ ***Рис. 4.*** Схема хода лучей в зеркальной системе антенны

на главное зеркало; отражающую поверхность *6* главного зеркала; лучи *7–10*, отраженные от щитов главного зеркала до первичного фокуса *F*1; отражающую поверхность *11* контррефлектора; лучи *12–15* от первичного фокуса *F*1 до отражающей поверхности контррефлектора, лучи *16–19* от отражающей поверхности контррефлектора до вторичного фокуса *F*2; приемник *20* радиоизлучения.

Предобработка радиоизображений адаптивным матричным приемником

Использование АМП радиоизлучения позволяет на аппаратном уровне легко производить такие стандартные операции предобработки изображений, как [13]:

— повышение/снижение яркости, т. е. сложение/вычитание значения яркости с некоторым фиксированным значением;

— повышение/снижение контрастности, т. е. соответственно умножение/деление значения яркости на некоторое значение, что приводит к более четким яркостным границам;

— получение негатива за счет простой замены каждого значения на его дополнение;

— бинаризацию, т. е. преобразование изображения к двум тонам по амплитуде;

— изменение положения за счет апертуры фильтра: апертура фильтра — это размер окна (части изображения), с которым фильтр работает непосредственно в данный момент времени; это окно постепенно передвигается по изображению слева направо и сверху вниз на один пиксель (т. е. на следующем шаге фильтр работает с окном, состоящим не только из элементов исходного изображения, но и из элементов, ранее подвергнувшихся преобразованию);

— масштабирование, т. е. изменение размеров пикселей;

— сглаживающую фильтрацию, т. е. нахождение среднеарифметического значения всех элементов рабочего окна изображения (отдельно по каждому из каналов), после чего это среднее значение становится значением среднего элемента (речь идет о нечетной апертуре фильтра; для двумерного случая средним элементом будет средний элемент по горизонтали и вертикали, т. е. центр квадрата);

— медианную фильтрацию, основанную на нахождении медианы — среднего элемента последовательности в результате ее упорядочения по возрастанию/убыванию и присваиванию найденного значения только среднему элементу;

— выделение границ различными методами (Робертса, Лапласа, Уоллеса и др.), в основе которых лежит работа с двумерной апертурой 2×2 либо 3×3.

Кроме того, использование АМП радиоизлучения позволяет легко выделить такие признаки двумерных изображений, как зависимость числа пикселей, попавших в контур изображения от их масштаба за счет изменения размеров виртуальных пикселей. Гармонический анализ этих зависимостей позволяет распознавать форму двумерных объектов. Также представляет интерес получение с помощью коммутации пикселей приемника масок типов двумерных объектов, по максимальному совпадению с которыми можно легко классифицировать изображения ОКО, проектируемые на матрицу с помощью зеркальной системы антенны.

Заключение

Рассмотрены возможности создания АМП радиоизлучения миллиметрового диапазона для обеспечения высокой эффективности получения радиоизображений в радиоастрономической локации. При создании сверхбыстрых АМП целесообразно использовать НЕВ-пиксели и осуществлять необходимый подбор сверхпроводниковых материалов с малым временем электрон-фононного взаимодействия, а также создавать условия для сокращения времени выхода неравновесных фононов в подложку, что происходит при уменьшении толщины сверхпроводящей пленки и улучшении акустического согласования сверхпроводящей пленки и подложки. Кроме того, при конструировании матрицы из указанных пикселей необходимо, прежде всего, уменьшить взаимовлияние последних за счет выбора оптимального расстояния между пикселями (скважности) и обеспечить наилучшее акустическое согласование сверхпроводящих пленок пикселей с подложкой. При этом оптимальный размер пикселя НЕВ АМП должен быть согласован с амплитудами колебаний краев главного зеркала и контррефлектора антенны радиотелескопа.

Предложенная система управления НЕВ АМП позволяет не только настраивать параметры матрицы для оптимального поиска ОКО по методу равносигнальной зоны, но и проводить аппаратными средствами эффективную предобработку изображений ОКО, а в ряде случаев и осуществлять идентификацию формы ОКО.

Эффективность радиовидения с помощью НЕВ АМП можно повысить за счет оптимальной фокусировки антенны и адаптации ее зеркальных поверхностей с учетом длины волны принимаемого излучения.

Литература

1. **Лебедев В. В.** Готовность России к защите Земли от астероидной опасности // Вестник Российской академии наук. 2013. Т. 83. № 9. С. 807–814.
2. **Кисляков А. Г.** Радиоастрономические исследования в миллиметровом и субмиллиметровом диапазонах волн // Успехи физических наук. 1970. Т. 101. Вып. 4. С. 607–653.
3. **Возможности** обнаружения малоразмерных космических объектов радиоастрономическими инструментами миллиметрового диапазона / Н. Ф. Морозов, Д. А. Индейцев, А. Е. Городецкий, В. Г. Курбанов, В. А. Агапов // Антенны. 2013. № 12. С. 56–59.
4. **Адаптивные** матричные приемники миллиметрового диапазона/ А. Е. Городецкий, В. В. Дубаренко, В. Г. Курбанов, А. Ю. Кучмин, В. А. Агапов // Многоликая Вселенная: тез. докл. Всерос. астрономической конф. (ВАК-2013), Санкт-Петербург, 23–27 сентября 2013 г. СПб., 2013. С. 59.
5. **Финкель М. И., Масленников С. И., Гольцман Г. Н.** Супергетеродинные терогерцовые приемники со сверхпроводниковым смесителем на электронном разогреве // Изв. вузов. Радиофизика. 2005. Т. 48. № 10–11. С. 964–970.
6. **Гольцман Г. Н., Лудков Д. Н.** Сверхпроводниковые смесители на горячих электронах терагерцового диапазона и их применение в радиоастрономии // Изв. вузов. Радиофизика. 2003. Т. 46. № 8–9. С. 671–686.
7. **Semenov A., Gol'tsman G. N., Sobolewski R.** Hot-Electron Effect in Superconductors and its Applications for Radiation Sensors // Superconductor Science and Technology. 2002. Vol. 15. P. 1–16.
8. **Dobrovolsky V. N., Sizov F. F.** Room Temperature, or Moder-Ately Cooled, Fast THz Semiconductor Hot Electron Bolometer // Semiconductor Science and Technology. 2007. Vol. 22. P. 103–106.
9. **Гершензон Е. М., Гершензон М. Е., Гольцман Г. Н.** Разогрев квазичастиц в сверхпроводящей пленке, находящейся в резистивном состоянии // Письма в ЖЭТВ. 1981. Т. 34. Вып. 5. С. 281–283.
10. **Быстродействующий** терогерцовый приемник и инфракрасный счетчик одиночных фотонов на эффекте разогрева электронов в сверхпроводниковых тонкопленочных наноструктурах / И. В. Пентин, К. В. Смирнов, Ю. Б. Вахтомин, А. В. Смирнов, Р. В. Ожегов, А. В. Дивочий, Г. Н. Гольцман // Физика, электроника, нанотехнологии: тр. МФТИ. 2011. Т. 3. № 2. С. 38–42.
11. **Пат.** 2319171 РФ, МПК8 G01S13/66. Система автоматического наведения радиотелескопа / А. Е. Городецкий, В. В. Дубаренко, Ю. Н. Артеменко, А. А. Парщиков, В. Г. Гиммельман, Г. С. Кучинский, А. П. Мозгов, А. Ю. Кучмин (РФ). — № 2319171; заявл. 17.07.06; опубл. 10.03.06, Бюл. № 7, ч. 3. — С. 824–825.
12. **Пат.** 2518398 РФ, МПК G 01S. Способ адаптации отражающих поверхностей антенны/ Ю. Н. Артеменко, А. Е. Городецкий, В. В. Дубаренко, А. Ю. Кучмин, И. Л. Тарасова, А. И. Галушкин, В. А. Агапов (РФ). — № 2518398; заявл. 20.10.12; опубл. 10.06.14, Бюл. № 16. — С. 1–10.
13. **Пат.** 987643 СССР, МКИ G 06 K 9/30. Способ выделения признаков для распознавания объектов / Э. И. Панков, И. А. Краснов, П. П. Кузьмин, А. Е. Городецкий, Н. Н. Ляшенко (СССР). — № 3240697/18-24; заявл. 10.12.80; опубл. 07.01.83, Бюл. № 1.

UDC 004.931

Detection and Identification of Dangerous Space Objects Using Adaptive Matrix Radio Receivers

Gorodetskiy A. E.[a], Dr. Sc., Tech., Professor, g27764@yandex.ru
Tarasova I. L.[b], PhD, Tech., Associate Professor, g17265l@yandex.ru
[a] Saint-Petersburg State Polytechnical University, 29, Politekhicheskaia St., 195251, Saint-Petersburg, Russian Federation
[b]Institute of Problems of Mechanical Engineering of RAS, 61, Bol'shoi Pr. V. O., 199178, Saint-Petersburg, Russian Federation

Purpose: Consideration of the possibility to use adaptive millimeter-wave matrix receivers for the detection and identification of dangerous space objects in radio astronomy location. **Results:** The ways to create adaptive matrix receivers are discussed, based on millimeter-wave radio emission receivers of HEB type (Hot Electron Bolometer). These receivers are equipped with a switching unit (for example, on thin-film cryotrons) installed together with the HEB matrix into a helium cryostat. It is also necessary to screen the currents that control the switch keys, so they do not affect the functioning of the pixels. A generalized structure of the adaptive matrix-type HEB receiver is given, along with a block diagram of its control system, containing the physically realizable HEB matrix, the virtual matrix, the storage device, the adaptive matrix receiver control unit, the external storage, the adaptation unit, the radio telescope automatic control unit, the switch, the counter-reflector oscillation measurement unit, the primary mirror oscillation measurement unit, the point of the oscillation measurement on the edge of the primary mirror and the point of the oscillation measurement on the edge of the counter-reflector. An algorithm is given for a radio telescope adaptive matrix receiver in the mode of detecting dangerous space objects. The discussed ways of using adaptive matrix receivers of millimeter-wave radio emission suggest that for creating ultrafast adaptive matrix receivers it is advisable to use HEB pixels and properly select superconducting materials with low electron-phonon interaction. The problem of creating an adaptive millimeter-wave matrix receiver is solved, providing optimal sizing of the matrix pixels (basing on the elevation angle, radiation wavelength and the expected parameters of the dangerous space objects) and high efficiency of getting

radio images in radio astronomy location. **Practical relevance:** The proposed HEB-like adaptive matrix receiver control system helps you not only configure the template for optimal search of dangerous space objects by beam method, but also perform an efficient hardware preprocessing of their images. In some cases, it can help you identify their shape.

Keywords — Matrix Detector, Radar, HEB Pixels, Radio Telescope Control System, Dangerous Space Objects.

References

1. Lebedev V. V. Russia's Willingness to Protect Earth Against Asteroid Danger. *Vestnik Rossiiskoi akademii nauk*, 2013, vol. 83, no. 9, pp. 807–814 (In Russian).
2. Kislyakov A. G. Radio Astronomy Research in Millimeter and Submillimeter Wavelengths. *Uspekhi fizicheskikh nauk*, 1970, vol. 101, no. 4, pp. 607–653 (In Russian).
3. Morozov N. F., Indians D. A., Gorodetskiy A. E., Kurbanov V. G., Agapov V. A. Detection of Small-Size Space Objects Radio Astronomy Instruments of Millimeter Range. *Antenny*, 2013, no. 12, pp. 56–59 (In Russian).
4. Gorodetskiy A. E., Dubarenko V. V., Kurbanov V. G., Kuchmin A. Y., Agapov V. A. Adaptivnye Matrichnye Priemniki Millimetrovogo Diapazona. *Tezisy dokladov Vserossijskoi astronomicheskoi konferentsii "Mnogolikaia Vselennaia" (VAK-2013)* [Proc. of Russian Astronomical Conf. "The Many Faces of the Universe"]. Saint-Petersburg, 2013, p. 59 (In Russian).
5. Finkel M. I., Maslennikov S. I., Gol'tsman G. N. Superheterodyne Teragertsovyi Receivers with Superconducting Mixer on Electronic Heating. *Izvestiia vuzov. Radiophysika*, 2005, vol. 48, no. 10–11, p. 964–970 (In Russian).
6. Gol'tsman G. N., Ludkov D. N. Superconducting Mixers on the Hot Electrons Terahertz Range and their Application in Radio Astronomy. *Izvestiia vuzov. Radiofizika*, 2003, vol. 46, no. 8–9, pp. 671–686 (In Russian).
7. Semenov A., Gol'tsman G. N., Sobolewski R. Hot-Electron Effect in Superconductors and its Applications for Radiation Sensors. *Superconductor Science and Technology*, 2002, vol. 15, pp. 1–16.
8. Dobrovolsky V. N., Sizov F. F. Room Temperature, or Moderately Cooled, Fast THz Semiconductor Hot Electron Bolometer. *Semiconductor Science and Technology*, 2007, vol. 22, pp. 103–106.
9. Gershenzon E. M., Gershenzon M. E., Gol'tsman G. N. Heating of Quasiparticles in a Superconducting Film in the Resistive State. *Pis'ma v ZhETV*, 1981, vol. 34, no. 5, pp. 281–283 (In Russian).
10. Pentin I. V., Smirnov K. V., Vahtomin Y. B., Smirnov A. V., Ozhegov R. V., Divochi A. V., Gol'tsman G. N. Fast Teragertsovyi Receiver and Infrared Counter Single Photons on the Effect of Heating of Electrons in Superconducting Thin-Film Nanostructures. *Fizika*, *elektronika*, *nanotekhnologii. Trudy MFTI*, 2011, vol. 3, no. 2, pp. 38–42 (In Russian).
11. Gorodetskiy A. E., Dubarenko V. V., Artemenko Y. N., Parschikov A. A., Himmelman V. G., Kuchinsky G. S., Mozgov A. P., Kuchmin A. Y. *Sistema avtomaticheskogo navedeniia radioteleskopa* [Controlled Pointing of the Radiotelescope]. Patent RF, no. 2319171, 2006.
12. Artemenko Y. N., Gorodetskiy A. E., Dubarenko V. V., Kuchmin A. Y., Tarasova I. L., Galushkin A. I., Agapov V. A. *Sposob adaptatsii otrazhaiushchikh poverkhnostei antenny* [The Way of Adaptation of Reflecting Surfaces Antenna]. Patent RF, no. 2518398, 2014.
13. Pankov E. I., Krasnov I. A., Kuzmin P. P., Gorodetskiy A. E., Lyashenko N. N. *Sposob vydeleniia priznakov dlia raspoznavaniia ob"ektov* [The Allocation Method of Characteristics for Object Recognition]. Patent USSR, no. 3240697/18–24, 1983.

УДК [519.85+519.71]:681.5

МЕТОД СТРУКТУРНО-ПАРАМЕТРИЧЕСКОЙ АДАПТАЦИИ МНОГОУРОВНЕВЫХ СИСТЕМ ОБРАБОТКИ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ ЛОКАЛЬНЫХ ФУНКЦИОНАЛОВ КАЧЕСТВА

А. В. Назаров[a]***,*** *канд. техн. наук, доцент*
[a]*Военно-космическая академия им. А. Ф. Можайского, Санкт-Петербург, РФ*

Постановка проблемы: *широкий класс прикладных задач связан с перераспределением ограниченных ресурсов иерархических систем так, чтобы обеспечить экстремумы выходным показателям качества при возникновении ограничений на функционалы качества элементов внутренних уровней. В случае большой размерности таких задач возникают методологические проблемы построения оптимальных моделей распределенных систем обработки информации, функционирующих в условиях нестационарных изменений локальных функционалов качества. Целью работы является разработка модели и метода структурно-параметрической адаптации иерархических систем большой размерности на основе локализации изменений функционалов качества структурных элементов.* ***Результаты:*** *применение развитого математического аппарата методов оптимизации в сочетании с алгоритмом обратного распространения ошибки в многослойных MLP-сетях позволило разработать модель адаптации показателей качества системы сбора и обработки измерительной информации к ее структурным и (или) параметрическим изменениям. Сформулирована постановка задачи синтеза многомерной по входу и выходу модели адаптации распределенной системы сбора и обработки измерительной информации. Разработан метод структурно-параметрической адаптации иерархических систем с использованием функционалов качества структурных элементов.* ***Практическая значимость:*** *модель позволяет определить настройки функциональных элементов различных иерархических уровней, исходя из заданного функционала качества всей системы на высшем уровне ее иерархии. Получены зависимости, позволяющие выбрать алгоритм параметрического синтеза модели информационной структуры иерархической системы в зависимости от состояния множества ее элементов.*

Ключевые слова *— адаптация, система сбора и обработки измерительной информации, многопараметрическая оптимизация, нейронные сети, многослойный MLP-классификатор.*

Введение

Для обеспечения эффективного функционирования сложных информационно-управляющих систем необходимо иметь алгоритмы управления, целью которых является такая подстройка или адаптация характеристик элементов систем, чтобы выбранный показатель или свертка показателей качества функционирования достигали экстремального значения. Адаптацией, в соответствии с наиболее распространенным определением Я. З. Цыпкина, будем считать процесс изменения параметров и структуры системы, а возможно, и управляющих воздействий на основе текущей информации с целью достичь определенного, обычно оптимального, состояния системы при начальной неопределенности и изменяющихся условиях функционирования [1, 2]. В статье рассматриваются модель и метод структурно-параметрической адаптации систем с многоуровневой структурой в функциональном, организационном или каком-либо ином плане, формируемой путем последовательного объединения множеств, содержащих более одного параметра. Примером распределенной многоуровневой системы является система сбора и обработки телеметрической информации космических комплексов (ССОИ) [3, 4].

Постановка задачи синтеза модели адаптации многоуровневой системы сбора и обработки информации

Функциональное назначение ССОИ — сбор и анализ измерительной информации о некоторых объектах или процессах. Распределенность ССОИ обусловлена пространственным, временным и функциональным разнесением элементов множеств измерительных преобразователей и элементов предварительной обработки информации по различным уровням иерархии. Задачу синтеза многомерной по входу и выходу модели адаптации к изменяющимся структуре и параметрам ССОИ сформулируем следующим образом.

Дано: 1. Множество функциональных звеньев ССОИ $\mathbf{U}^i = \left(u_1^i, u_2^i, \ldots, u_h^i, \ldots, u_H^i\right)$, $h = \overline{1,H}$, где H — общее число звеньев функциональной схемы сбора и анализа измерительной информации. Функциональные звенья реализуют различные операции, начиная от первичного преобразования физической величины в электрический сигнал и заканчивая операцией вычисления вида состояния наблюдаемого объекта или процесса.

2. Для каждого функционального элемента ССОИ введена скалярная характеристика $P(u)$ как вероятность совместного наступления двух событий: 1) элемент работоспособен и 2) элемент функционирует по целевому назначению

в соответствии с заданными техническими характеристиками. Поскольку часть звеньев ССОИ являются управляемыми элементами, то существует возможность управлять значениями составляющих вектора параметров $\mathbf{P}^i = \left[P\left(u_1^i\right), P\left(u_2^i\right), \ldots, P\left(u_h^i\right), \ldots, P\left(u_H^i\right) \right]^{\mathrm{T}}$, $h = \overline{1, H}$.

3. Вектор Θ структурных характеристик функциональной (информационной) схемы ССОИ, включающий количественные характеристики состава, инцидентности, связности графа рассматриваемой структуры и др. Каждый элемент схемы при реализации информационных процессов в ССОИ связан с множеством других элементов на соседних уровнях иерархии.

4. В качестве весов связей между узлами u графа информационных процессов ССОИ определены веса w_{ij}, с которыми значение функционала элемента $y_i = w_{ij} f(P(u_i))$ влияет на функционалы элементов $y_j = w_{ij} f(P(u_j))$, находящихся на более высоких уровнях иерархии ССОИ. Локальный функционал $f(*)$ осуществляет однозначное отображение множества значений вероятностной характеристики $P(u)$ функционального звена u в единый для всех элементов ССОИ диапазон [0, ..., 1].

5. Входными воздействиями ССОИ являются нелинейные преобразования от вероятностных характеристик физических величин $\left\{\mathbf{X}^i\right\}_{i=1}^{L}$, $i = 1, L$, регистрируемых в определенные моменты времени t_i, $i = \overline{1, L}$ функционирования ССОИ. Так, входными процессами для узлов графа нижнего уровня иерархии модели являются измеряемые физические процессы, характеризуемые функционалом вероятностных характеристик $f(P(\lambda))$ — функционалом вероятности события, заключающегося в том, что свойства измеряемого процесса λ соответствуют статическим и динамическим характеристикам первичных измерительных преобразователей (датчиков).

6. Выходными показателями ССОИ являются множество значений функционалов от показателей качества, упорядоченных в вектор целевых характеристик ССОИ $\left\{d_j^i\right\}_{\substack{j=1 \\ i=1}}^{\substack{n3 \\ L}}$, $j = \overline{1, n_3}$; $i = \overline{1, L}$;

n_3 — количество целевых функционалов качества распределенной многоуровневой ССОИ. Например, $d_i = [f(D_1), f(D_1), \ldots, f(D_N), f(E_1), f(E_2), \ldots, f(E_N), f(T_1), f(T_2), \ldots, f(T_N)]^{\mathrm{T}}$, где $f(D_N)$ — функционал достоверности распознавания вида состояния N-го объекта или процесса; $f(E_N)$ — функционал точности вычислений параметров состояния; $f(T_N)$ — функционал оперативности распознавания вида состояния N-го объекта или процесса.

Найти: 1. Параметры и структуру многомерной модели F информационной структуры ССОИ, позволяющую отображать множество значений вероятностных функционалов $\left\{\mathbf{X}^i\right\}_{i=1}^{L}$, $i = 1, L$ входных характеристик измеряемых процессов во множество $\left\{\mathbf{Z}^i\right\}_{i=1}^{L}$, $i = 1, L$ значений выходных показателей качества ССОИ при ограничениях на значения вероятностных характеристик качества функционирования $f\left(P\left(u_1^i\right)\right), \ldots, f\left(P\left(u_H^i\right)\right)$ функциональных звеньев на промежуточных уровнях иерархии ССОИ.

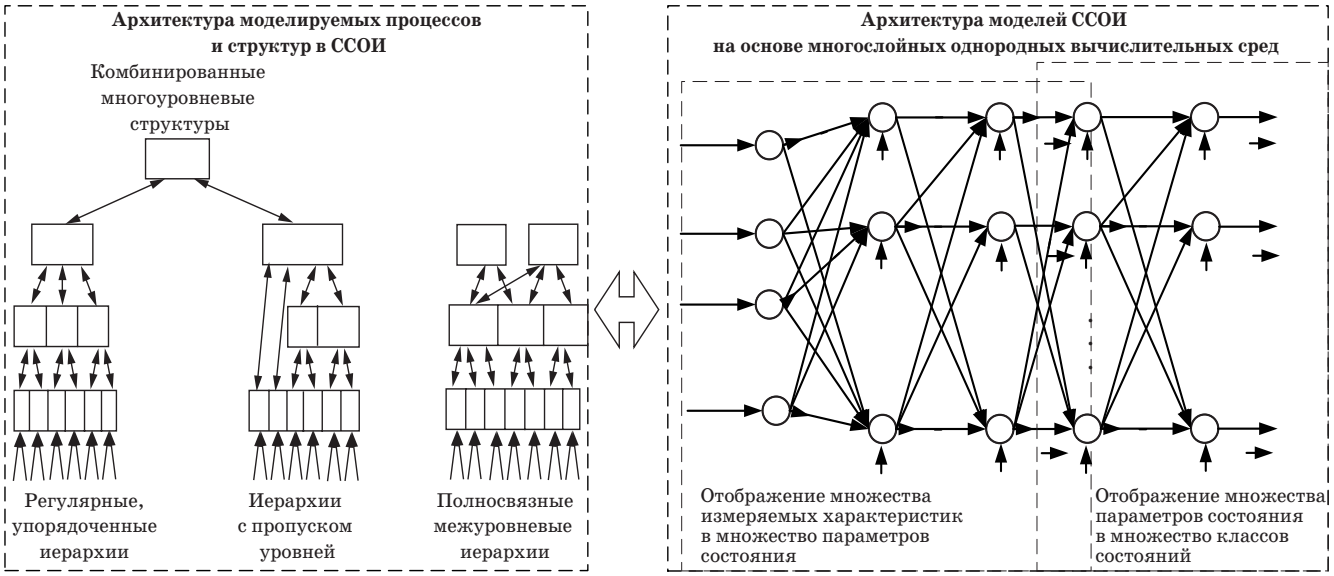
2. Управляемые элементы ССОИ из множества $\mathbf{U}^i = \left(u_1^i, u_2^i, \ldots, u_h^i, \ldots, u_H^i\right)$, $h = \overline{1, H}$, позволяющие обеспечить оптимальный функционал качества ССОИ на высшем уровне ее иерархии.

Под ограничениями на значения вероятностных функционалов качества функционирования $f\left(P\left(u_1^i\right)\right), \ldots, f\left(P\left(u_H^i\right)\right)$ функциональных звеньев на промежуточных уровнях иерархии ССОИ подразумеваются ограничения, обусловленные как выходом из строя звеньев ССОИ в результате невосстанавливаемых отказов программных и (или) технических средств, т. е. $f\left(P\left(u_j^i\right)\right) = 0$, так и ограничения, обусловленные техническими характеристиками звеньев ССОИ.

Модель структурно-параметрической адаптации

В основе решения поставленной задачи и разработанного метода структурно-параметрической адаптации лежит подобие структур распределенных ССОИ и однородных вычислительных сред. Структурно-параметрическая оптимизация (точнее, аппроксимация «вход-выход» ССОИ с помощью оптимизационных обучающих процедур), лежащая в основе адаптации ССОИ, базируется на широком арсенале методов параметрического синтеза моделей распознавания на основе однородных вычислительных сред [5, 6]. Такой подход открывает новые возможности для моделирования процессов в многоуровневых структурах с использованием различных архитектур однородных вычислительных сред, например таких, как MLP-классификаторов (Multilayer perceptron — многослойные нейросетевые архитектуры, обучаемые по модификациям метода обратного распространения ошибки). Подобие моделей ССОИ и однородных вычислительных сред иллюстрирует рис. 1.

Согласно теореме Хехт — Нильсена [5, 6], любую многоуровневую функциональную схему ССОИ можно представить в виде однородной вычислительной среды соответствующей архитектуры. Представим каждый j-й элемент ССОИ



■ ***Рис. 1.*** Подобие иерархий моделируемых структур и архитектур однородных вычислительных сред

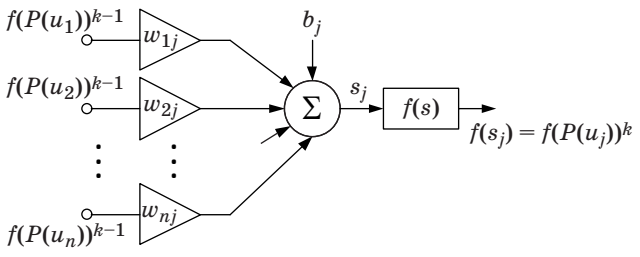
элементом на основе модели Маккалоха — Питтса [5] (рис. 2). Элемент реализует функцию нелинейного отображения многомерного пространства входов $\mathbf{R}^n$ в выход $\mathbf{R}^1$:

$$f(s_j) = f\left(P(u_j)\right)^k = f\left(\sum_{i=1}^{n} w_{ij} f\left(P(u_i)^{k-1}\right) - b_j\right), \quad (1)$$

где $f(s_j)$ — локальный стохастический функционал, значение которого есть вероятность правильного функционирования j-го звена ССОИ с областью значений [0, 1]; n — количество аргументов вероятностного функционала правильного функционирования j-го звена на k-м уровне иерархии ССОИ; w_{ij} — величина регулируемой функциональной связи между i-м и j-м функциональными элементами; $P(u_i)^{k-1}$ — вероятность правильного функционирования i-го звена на $(k-1)$-м уровне иерархии ССОИ.

В качестве стохастического функционала $f(*)$ определим функционал вида

$$f(x) = \frac{1}{1+e^{-ax}}, \quad (2)$$



■ ***Рис. 2.*** Элемент модели ССОИ, реализующий функцию нелинейного отображения

где x — индуцированное локальное поле нелинейного преобразователя, моделирующего функционирование элемента ССОИ, $-\infty < x < \infty$.

Синтезированную модель с настроенными по заданному критерию качества функционирования ССОИ коэффициентами межэлементных связей $\left\{w_{ij}^k, i, j = \overline{1, n^k}\right\}_{k=1}^{N}$, где N — количество уровней иерархии, можно рассматривать как «серый ящик», на вход которого поступает векторный сигнал $\mathbf{X}$. Элементы модели на промежуточных уровнях иерархии осуществляют последовательные преобразования от вероятностных характеристик физических величин λ, регистрируемых в определенные моменты времени, а на выходе формируется векторный сигнал $\mathbf{Y}$, характеризующий показатели качества ССОИ, обеспечиваемые в результате параметрического синтеза модели.

С помощью модели структурно-параметрической адаптации на основе отображения F: $\mathbf{R}^n \to \mathbf{R}^m$ n-мерного вектора $\mathbf{X} = (x_1, x_2, ..., x_n)^{\mathrm{T}}$ функционалов вероятностных характеристик измеряемых физических процессов в m-мерный вектор $\mathbf{Y} = (y_1, y_2, ..., y_m)^{\mathrm{T}}$ показателей качества ССОИ многократно вычисляются искомые приращения $\Delta y_i = \Delta w_{ij} f(P(u_i))$. Отображение должно быть оптимальным в смысле минимума среднеквадратической погрешности восстановления вектора $\mathbf{Y} = (y_1, y_2, ..., y_m)^{\mathrm{T}}$ показателей качества ССОИ при подаче на вход вектора $\mathbf{X} = (x_1, x_2, ..., x_n)^{\mathrm{T}}$ функционалов вероятностных характеристик измеряемых физических процессов. Модель адаптации типа «серого ящика» позволяет при изменении структуры и (или) параметров элементов ССОИ на низшем или промежуточных

уровнях иерархии переобучать модель F для обеспечения необходимого $\mathbf{Y}$ при заданном $\mathbf{X}$ на входе.

Зная вид и параметры функционалов структурных элементов ССОИ, реализовать параметрический синтез модели ССОИ известной структуры можно с использованием парадигмы «обучения с учителем», основанной на предъявлении смоделированных по методу Монте-Карло множеств обучающих образов, каждый из которых описывается своим входным вектором $\mathbf{X}$ и множеством целевых реакций $\mathbf{Y}$ [7]. Вводя для каждого k-го уровня иерархии ССОИ матрицу настраиваемых весов поэлементных межуровневых связей, модель F следует настроить так, чтобы минимизировать некоторую функцию невязки E отклонения фактического значения $\mathbf{Y}^i$ от желаемого $\mathbf{D}^i$, причем этот процесс синтеза продолжается до тех пор, пока выход модели F не станет для каждого i удовлетворять критерию $E^i < \Delta$. С математической точки зрения процесс синтеза модели ССОИ в этом случае сводится к минимизации показателя качества обучения (целевой функции в пространстве выходных характеристик ССОИ) по настраиваемым весам w_{ij} и может протекать как в непрерывном t, так и дискретном $k = 0, 1, 2, \ldots$ времени.

В дискретном представлении синтез модели ССОИ производится путем минимизации выходной невязки для каждого j-го структурного элемента ССОИ:

$$E_j(k) = \frac{1}{2}e_j^2(k) = \frac{1}{2}\left(d_j(k) - P\left(u_j(k)\right)\right)^2 = \\ = \frac{1}{2}\left(d_j(k) - f\left(\sum_{i=1}^{n} w_{ij}x_i(k)\right)\right)^2 \qquad (3)$$

с помощью рекуррентной процедуры

$$w_{ij}(k+1) = w_{ij}(k) + \eta(k)\delta_j(k)x_i(k), \qquad (4)$$

где $\delta_j(k) = e_j(k)f'\left(P\left(u_j(k)\right)\right) = \dfrac{\partial E_j(k)}{\partial P\left(u_j(k)\right)}$ — локальная ошибка на выходе структурного элемента ССОИ u_j; $f(*)$ — стохастический функционал вида (2).

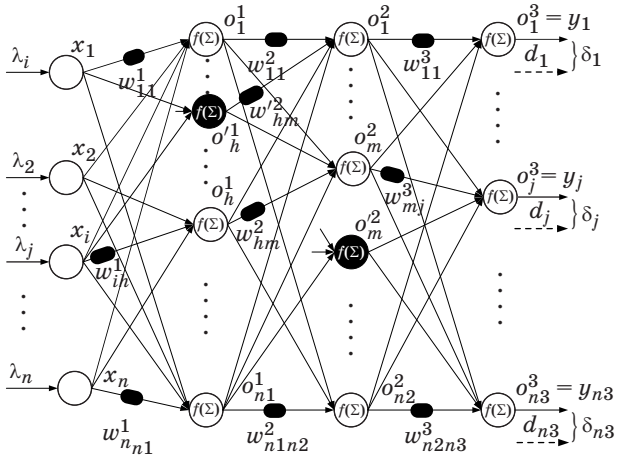
Параметрический синтез модели ССОИ, основанный на градиентных ньютоновских процедурах оптимизации, реализует так называемый регулярный подход [8], в рамках которого на каждом шаге вычисляются веса w_{ij}, с которыми значения некоторых функционалов $y_i = w_{ij}f(P(u_i))$ влияют на функционалы $y_j = w_{ij}f(P(u_j))$, находящиеся на последующих (более высоких) уровнях иерархии ССОИ. В случае если функционал элемента ССОИ не удается сформировать в виде монотонно возрастающей, ограниченной и имеющей отличные от нуля производные на всей области определения функции $f(*)$, или если глобальная целевая функция многоэкстремальна, недифференцируема, а также если $f(*)$ является не функционалом, а оператором, то следует применить эволюционные алгоритмы параметрического синтеза модели F [9].

Многоуровневая информационная структура ССОИ позволяет использовать для параметрического синтеза алгоритм обратного распространения ошибок или обобщенное дельта-правило [10, 11]. Именно благодаря процедуре обратного распространения ошибок имеется возможность решать задачу синтеза и применения модели адаптации ССОИ по предназначению, не прибегая к классическим процедурам параметрической оптимизации в пространствах большой (невычислимой) размерности.

Синтез алгоритма структурно-параметрической адаптации

Без потери общности для M уровней иерархии и неравном числе элементов на соседних уровнях рассмотрим использование концепции обратного распространения выходной невязки вида (3) применительно к трехслойной архитектуре информационной структуры ССОИ (рис. 3).

Исходная информация с помощью процедуры Монте-Карло задана в виде последовательности пар обучающих векторов «вход → выход», образующих обучающую выборку вида «Вектор преобразований f от вероятностных характеристик $P(\lambda)$ регистрируемых физических величин → Вектор преобразований f от множества значений показателей качества ССОИ». На рис. 3 o_{ns}^s — значения вероятностных функционалов, отмеченных для различных слоев и элементов одного слоя. Начальные значения вероятност-



■ ***Рис. 3.*** Модель трехуровневой архитектуры информационной структуры ССОИ, составленной из связанных по иерархии функциональных элементов MLP-классификатора

ных функционалов на промежуточных уровнях иерархии $y_i = w_{ij}f(P(u_i))$ установим либо на середину функционального диапазона звена u_i, либо равными математическому ожиданию $f(P(u_i))$. Ряд функциональных элементов ССОИ имеют ограничения на выходе $y_j = w_{ij}f(P(u_j))$ в виде равенств $w_{ij}f(P(u_j)) = y'_j$ и (или) неравенств $\Delta_j^1 < w_{ij}f(P(u_j)) < \Delta_j^2$, данные элементы на рис. 3 затемнены.

Исходные значения $w_{ij} = 0{,}5 \pm \xi_{wij}$, где ξ — некоторая случайная величина, как правило, распределенная по равномерному закону в диапазоне [0, ..., 0,1]. Начальные значения компонент вектора преобразований f от множества значений показателей качества ССОИ установим на номинальные значения, заданные при проектировании элементов высшего уровня информационной структуры ССОИ. Как правило, это вершины графа, соответствующие операциям принятия решения о состоянии контролируемого объекта.

Для рассмотренной структуры необходимо использовать алгоритм параметрического синтеза модели F, заключающийся в адаптации коэффициентов w_{ij} всех уровней (слоев) таким образом, чтобы расхождение между выходным и входным сигналами сети минимизировалось в смысле показателя $E_j(k)$. Из этого следует, что алгоритм синтеза представляет собой процедуру поиска экстремума специально сконструированной целевой функции ошибок на множестве значений $\{y_j = w_{ij}f(P(u_j))\}$. Модель имеет n_0 входов, n_1 элементов в первом скрытом слое, n_2 элементов — во втором и n_1 элементов — в выходном слое, в общем случае $n_1 \neq n_2 \neq n_3$. Каждый входной вектор синтезированной по методу Монте-Карло обучающей выборки представляет собой вектор $\mathbf{x} = [x_1, ..., x_i, ..., x_{n0}]^{\mathrm{T}}$, выходной вектор $\mathbf{y} = [y_1, ..., y_j, ..., y_{n3}]^{\mathrm{T}}$ и целевой вектор $\mathbf{d} = [d_1, ..., d_j, ..., d_{n3}]^{\mathrm{T}}$.

В процессе параметрического синтеза модели F необходимо обеспечить минимальное рассогласование между текущими значениями выходных $y_j(k)$ и целевых $d_j(k)$ сигналов для всех $j = 1, 2, ..., n_3$ и k. Для этого используем глобальную целевую функцию вида

$$E^k = \sum_k E(k) = \frac{1}{2}\sum_k \sum_j \left(d_j(k) - y_j(k)\right)^2 = \frac{1}{2}\sum_k \sum_j e_j^2(k). \quad (5)$$

Данная целевая функция соответствует процедуре «пакетного обучения», когда E^k минимизируется сразу по всей обучающей выборке. При малых значениях шага коррекции $\Delta w_{ji}^{[s]}(k)$, где s — номер уровня, удовлетворяющих условию Дворецкого [12], процедура обратного распространения ошибки минимизирует и целевую функцию

$$E(k) = \frac{1}{2}\sum_{j=1}^{n_3}\left(d_j(k) - y_j(k)\right)^2 = \frac{1}{2}\sum_{j=1}^{n_3} e_j^2(k) = \sum_{j=1}^{n_3} E_j(k). \quad (6)$$

В случае отсутствия выраженной иерархии в информационных связях в рамках метода адаптации ССОИ для синтеза оптимального отображения F: $\mathbf{R}^n \to \mathbf{R}^m$ n-мерного вектора $\mathbf{X} = (x_1, x_2, ..., x_n)^{\mathrm{T}}$ функционалов вероятностных характеристик измеряемых физических процессов в m-мерный вектор $\mathbf{Y} = (y_1, y_2, ..., y_m)^{\mathrm{T}}$ показателей качества можно использовать алгоритм Левенберга — Марквардта. Данный алгоритм обеспечивает более быстрое обучение сети (с увеличением скорости на порядок и более), чем описанный алгоритм обратного распространения ошибки, использующий градиентную оптимизацию. Для сокращения вычислительных затрат в алгоритме Левенберга — Марквардта матрица Гессе аппроксимируется в виде $\mathbf{H} = \mathbf{J}^{\mathrm{T}}\mathbf{J}$. В результате градиент величины коррекции весовых коэффициентов и величин смещения функциональных элементов вычисляется через определитель $\mathbf{J}$ Якоби, содержащий частные производные первого порядка ошибок весовых коэффициентов и пороговых величин [13]. Алгоритм синтеза модели F содержит 6 шагов.

1. Выбираются начальные значения подбираемых и вспомогательных переменных m, w_0, $r > 1$, v_0.

2. Рассчитывается антиградиент в k-й итерации по формуле $g(w_k) = [\mathbf{J}(w_k)]^{\mathrm{T}}e(w_k)$.

3. Вычисляется матрица $\mathbf{G}(w_k)$, аппроксимирующая гессиан: $\mathbf{G}(w_k) = [\mathbf{J}(w_k)]^{\mathrm{T}}e(w_k) + \mathbf{R}(w_k)$. Осуществляется регуляризация $\mathbf{R}(w_k) = v_k\mathbf{I}$, где v_k — параметр Левенберга — Марквардта: $\mathbf{G}(w_k) = \mathbf{J}(w_k)\mathbf{J}^{\mathrm{T}}(w_k) + v_k\mathbf{I}$.

4. Вычисляется направление движения в k-й итерации: $h = -\mathbf{G}^{-1}(w_k)g_k$.

5. Вычисляется значение v_k согласно правилу

$$v_k = \frac{v_k - 1}{r} \text{ при } E\left(\frac{v_{k-1}}{r}\right) \le E_k;$$

$$v_k = v_{k-1} \text{ при } E\left(\frac{v_{k-1}}{r}\right) > E_k \text{ и } E(v_{k-1}) > E_k;$$

$$v_k = v_{k-1}r^m \text{ при } E\left(\frac{v_{k-1}}{r}\right) > E_k \text{ и } E(v_{k-1}) > E_k.$$

6. Вычисляется ошибка E на обучающей выборке, и если ошибка существенна, повторяются шаги 2–6.

Рассмотренный алгоритм обучения Левенберга — Марквардта использует для поиска минимума функционала E комбинированную стратегию линейной аппроксимации и градиентного спуска с возможностью переключения с одной стратегии на другую [5, 14].

Применение метода структурно-параметрической адаптации для управления многоуровневой ССОИ

Рассмотрим механизм применения модели информационной структуры ССОИ в рамках метода структурно-параметрической адаптации при изменениях как в структуре самой ССОИ, так и в состоянии наблюдаемого объекта или процесса.

Пусть в результате изменений в состоянии наблюдаемого объекта (или процесса) или ССОИ обнаружено ограничение на выходной вероятностный функционал одного или нескольких функциональных звеньев ССОИ. При этом изменены параметры вектора Θ связности и (или) изменена структура графа ССОИ и, соответственно, изменены значения межэлементных связей в синтезированной стандартной модели ССОИ. При этом действуют ограничения:

— ограничение элемента ССОИ типа равенства

$$w_{ij}^{[s]} \cdot f\left(P\left(u_j\right)\right) = y'; \qquad (7а)$$

— ограничение элемента ССОИ типа неравенств

$$\Delta_j^1 < w_{ij} \cdot f\left(P\left(u_j^{[s]}\right)\right) < \Delta_j^2; \qquad (7б)$$

— элемент ССОИ неработоспособен

$$w_{ij}^{[s]} \cdot f\left(P\left(u_j\right)\right) = 0. \qquad (7в)$$

Стандартная модель F соответствует нормальному режиму функционирующей ССОИ. Предположим, что при номинальных значениях измеряемых параметров объекта или процесса воздействию подверглись элементы промежуточных уровней ССОИ. Тогда алгоритм выявления изменений на выходе элементов ССОИ во взвешенном пространстве $w_{ij} \cdot f\left(P\left(u_j^{[s]}\right)\right)$ модели F и локализации управляемых элементов ССОИ из множества $\mathbf{U}^i = \left(u_1^i, u_2^i, \ldots, u_h^i, \ldots, u_H^i\right)$, $h = \overline{1, H}$, позволяющих обеспечить оптимальный функционал качества ССОИ на высшем уровне ее иерархии, содержит 7 шагов.

1. Подача на входной слой модели F, соответствующий низшему уровню иерархии ССОИ вектора $\mathbf{X}_k$, где k — номер примера обучающей выборки, номинальных значений нелинейных функционалов от вероятностных характеристик измеряемых физических процессов $f(P(\lambda))$, т. е. значений номинальных параметров объекта или процесса.

2. Вычисление взвешенных выходных значений $\left\{w_{ij} \cdot f\left(P\left(u_j^{[s]}\right)\right)\right\}$ функционалов вероятностных характеристик всех последующих уровней ССОИ с учетом ограничений вида (7а)–(7в) с использованием функционала $f^{[s]}(x) = \dfrac{1}{1 + e^{-\alpha^{[s]} x}}$, $j = \overline{1, n_3}$.

3. По заданному целевому вектору $\mathbf{D}_k$, где k — номер примера обучающей выборки, и вычисленным промежуточным выходам $o_i^{[s]}(k)$, где k — номер примера обучающей выборки, соответствующей нормальному режиму функционирования ССОИ, расчет локальных ошибок $\delta_i^{[s]}(k)$ для всех слоев модели.

4. Расчет поправок всех весов $w_{ij}^{[s]}$ межэлементных связей в виде $\Delta w_{jl}^{[s]}(k) = \eta \delta_j^{[s]} x_i^{[s]}$, $s = 1, 2, 3, \ldots$, где s — количество слоев модели F или уровней иерархии ССОИ.

5. Подача на вход и установка на выходе модели следующего образа ($\mathbf{X}_k$, $\mathbf{D}_k$) из обучающей выборки, соответствующей нормально функционирующей ССОИ, и повторение шагов 1–4. Процесс обучения продолжается до тех пор, пока ошибка в выходном слое модели не станет удовлетворять критерию минимума E^k (5), а пересчитанные для «неисправной» структуры ССОИ веса $w_{ij}^{[s]}$ модели F стабилизируются на некоторых уровнях.

6. Поэлементный анализ значений взвешенных выходных функционалов $w_{ij}^* \cdot f\left(P\left(u_j^{[s]}\right)\right)$, где w_{ij}^* соответствует весу выхода элемента в «неисправной» ССОИ, в целях обнаружения направления и степени их изменения относительно w_{ij} (нормально функционирующей ССОИ) в нормированном диапазоне сжимающей функции (2).

7. Интерпретация изменений и принятие решений на управляющие воздействия в целях коррекции управляемых характеристик элементов реальной ССОИ, отображаемых в $w_{ij}^* \cdot f\left(P\left(u_j^{[s]}\right)\right)$ модели F.

Таким образом, определяется множество w_{ij} многослойной модели ССОИ, аппроксимирующей зависимость «вход/выход» для множества режимов функционирования ССОИ, и множество w_{ij}^* структурно и (или) параметрически видоизмененной модели «неисправной» ССОИ для множества тех же режимов функционирования. Это позволяет, проанализировав изменения в пространстве $w_{ij}^* \cdot f\left(P\left(u_j^{[s]}\right)\right)$, локализовать управляемые элементы ССОИ из множества $\mathbf{U}^i = \left(u_1^i, u_2^i, \ldots, u_h^i, \ldots, u_H^i\right)$, $h = \overline{1, H}$. При этом решение задачи управления при отклонении условий функционирования ССОИ от нормальных снимается не с выхода Y, а путем интерпретации динамики параметров модели F. Любой слой в разработанной модели является не только обрабатывающим, но и выходным, т. е., с одной стороны, выдает промежуточные результаты обработки информации, имеющие самосто-

ятельное значение, а с другой — доставляет информацию для последующих слоев более высоких уровней иерархии информационной структуры ССОИ.

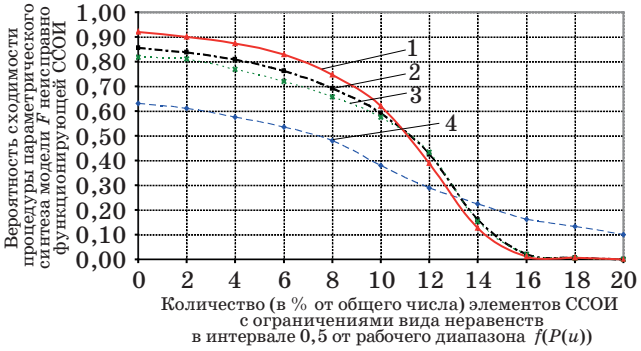
Было проведено моделирование фрагмента информационной структуры ССОИ, состоящей из 6 уровней иерархии (рис. 4, 5), при котором использовалась коррекция вида [15]

$$\Delta\bar{w}_{ij}^{[s]}(\nu)=\frac{\eta}{n_{s-1}(1-\chi)}\sum_{k}\delta_j^{[s]}(k)o_i^{[s-1]}(k)+$$
$$+\chi\Delta w_{ji}^{[s]}(\nu-1)-\alpha\Delta w_{ji}^{[s]}(\nu)+e(\nu), \qquad (8)$$

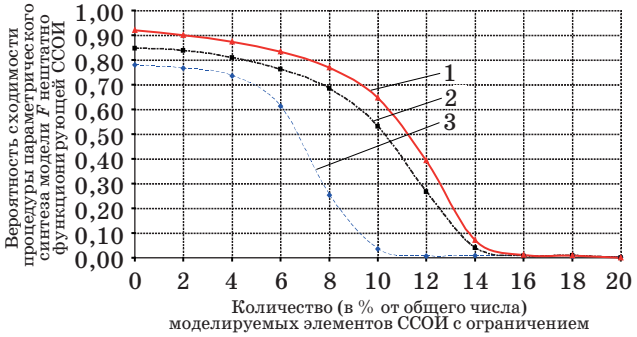
где $\nu = 1, 2, \ldots$ — номер итерации коррекции весов; $0 < \eta < 1$ — скорость обучения; n_s — количество элементов ССОИ на s-м уровне иерархии; χ — параметр регуляризации; $\alpha = 10^{-3} \div 10^{-5}$ — параметр, предохраняющий процесс обучения от возникновения недопустимо больших весов $w_{ij}^{[s]}$; $e(\nu)$ — шумовая составляющая.

С учетом ограничений на выходные вероятностные функционалы $o_i^{[s]}(k)$ элементов ССОИ каждый вес соответствует определенным значениям $w_{ij}^{[s]} = w_{ij}^{[s]\prime}$, усредненным по множеству k векторов «номинальной» обучающей выборки. На выходе модели в качестве целевого (оптимального с точки зрения разработчика ССОИ) $(n_3\times 1)$-мерного вектора используется совокупность значений вероятностного функционала показателей качества всей системы **D** с элементами $d_1 = f(D_1) = 0{,}99$; ... $d_z = f(D_z) = 0{,}99$; ... $d_{n_3-1} = f(C) = 0{,}01$; $d_{n_3} = f(T) = 0{,}01$.

Анализ представленных графиков позволяет выбрать алгоритм параметрического синтеза



■ ***Рис. 4.*** Зависимости вероятности сходимости четырех различных процедур параметрического синтеза модели ССОИ от количества элементов с ограничениями вида неравенств: *1* — алгоритм Левенберга — Марквардта; *2* — алгоритм оптимизации 1-го порядка для глобальной целевой функции (5); *3* — алгоритм оптимизации 1-го порядка для локальной целевой функции (6); *4* — алгоритм случайного поиска



■ ***Рис. 5.*** Зависимости вероятности сходимости процедуры Левенберга — Марквардта от количества ограничений на стохастические функционалы элементов ССОИ на внутренних иерархических уровнях: *1* — ограничения типа неравенства (7б); *2* — ограничения типа равенства (7а); *3* — элементы неработоспособны (7в)

модели в зависимости от информационной структуры, вида ограничений и количества отказавших элементов ССОИ. Зависимости на рис. 4 и 5 получены частотным способом соответственно по 100 и 60 экспериментам в каждой точке; сходимость к погрешности $\varepsilon = 0{,}01$. Количество функциональных элементов по шести слоям MLP-сети 50/40/30/20/10/5 и 20/18/16/14/10/5.

Синтезированная модель нормально функционирующих ССОИ и контролируемого объекта или процесса полностью описывается s-матрицами весов межэлементных связей $w_{ij}^{[s]}$, осуществляющих нелинейное отображение пространства входов в пространство выходов на основе аппроксимации сложных многомерных нелинейных функций, реализуемых в реальной ССОИ.

Заключение

Применение математического аппарата нелинейной оптимизации в сочетании с алгоритмом обратного распространения ошибки в многослойных сетях, моделирующих многоуровневые информационные процессы, позволило разработать модель адаптации показателей качества ССОИ к структурным и (или) параметрическим изменениям как в состоянии контролируемых объектов или процессов, так и в самой ССОИ. С помощью модели возможно определить, в каком функциональном элементе и на сколько (в смысле вероятностного функционала выполнения элементом своей целевой задачи) необходимо изменить выходные характеристики звена, для того чтобы при воздействии на ССОИ или объект/процесс обеспечить заданный функционал качества всей системы на высшем уровне ее иерархии.

Литература

1. **Турчин В. Ф.** Феномен науки. Кибернетический подход к эволюции. — М.: ЭТС, 2000. — 368 с.
2. **Цыпкин Я. З.** Вопросы кибернетики. Адаптивные системы / АН СССР. — М., 1974. — С. 5–20.
3. **Мальцев Г. Н., Стогов Г. В., Терехов А. В.** Перспективы создания комплексов управления космическими аппаратами на базе ключевых технологий // Информационно-управляющие системы. 2006. № 5. С. 2–5.
4. **Nazarov A. V., Kozyrev G. I., Shklyar S. V.** Prognostication of Technical for Low-Orbit Spacecraft with the Use of Neural Networks//Cosmic Research. 2002. Vol. 40. N 6. P. 594–604.
5. **Haykin S.** Neural Networks: A Comprehensive Foundation. — N. Y.: MacMillan College Publishing Co, 1994.— 1104 p.
6. **Галушкин А. И.** Нейрокомпьютеры в разработках военной техники США // Зарубежная радиоэлектроника. 1995. № 5. С. 3–48.
7. **Назаров А. В.** Алгоритм прогнозирования в пространстве параметров ситуации // Нейрокомпьютеры: разработка и применение. 2007. № 2–3. С. 24–28.
8. **Вахитов А. Т., Граничин О. Н., Гуревич Л. С.** Алгоритм стохастической аппроксимации с пробным возмущением на входе в нестационарной задаче оптимизации // Автоматика и телемеханика. 2009. № 11. С. 70–79.
9. **Бодянский Е. В., Руденко О. Г.** Искусственные нейронные сети: архитектуры, обучение, применения. — Харьков: Телетех, 2004. — 369 с.
10. **Назаров А. В., Лоскутов А. И.** Нейросетевые алгоритмы прогнозирования и оптимизации систем. — СПб.: Наука и Техника, 2003. — 384 с.
11. **Werbos P.** Backpropagation Through time. What it Does and How to do it // Proc. IEEE. 1990. Vol. 78. P. 1550–1560.
12. **Татузов А. Л.** Нейронные сети в задачах радиолокации. — М.: Радиотехника, 2009. — 432 с.
13. **Осовский С.** Нейронные сети для обработки информации. — М.: Финансы и статистика, 2004. — 344 с.
14. **Amari S.** Dreaming of Mathematical Neuroscience for Half a Century // Neural Networks. 2013. N 37. P. 48–51.
15. **Cichocki A., Unbehauen R.** Neural Networks for Optimization and Signal Processing. — Stuttgart: Teubner, 1993. — 526 p.

UDC [519.85+519.71]:681.5

Method of Structurally-Parametric Adaptation Multilayer Systems of Information Processing with usage of Quality Local Functionals

Nazarov A. V.[a], PhD, Tech., Associate Professor, naz_av@mail.ru
[a]A. F. Mozhayskii Military Space Academy, 13, Zhdanovskaia St., 197082, Saint-Petersburg, Russian Federation

Purpose: A wide class of application-oriented tasks deal with reallocation of restricted resources in hierarchical systems to provide extremes for the output quality coefficients, when the functionals of the internal level elements quality are restricted. If these tasks have big dimensionality, there are methodological problems of developing optimal models of distributed information-processing systems which function under the conditions of nonstationary changes of the local quality functionals. The aim of this work is developing a model and a method of structurally-parametrical adaptation of hierarchical big-dimensionality systems, localizing the changes of structural elements quality functionals. **Results:** Application of advanced mathematical apparatus of optimization methods combined with the error backpropagation algorithm in multilayer MLP-networks gave rise to the model in which the quality parameters of the measurement information collection/processing system are adapted to the structural and/or parametric changes of the information. The problem was formulated of synthesizing an input/ouput multidimentional adaptation model for a distributed system of measurement information collection/processing. Taking into account the similarity of hierarchies of the modelled processes and the architectures of the homogeneous computing environments, the modelling used the multilayer MLP-qualifier architecture. The method of structural-parametric adaptation of hierarchical systems was developed, with the usage of structural elements quality functionals. **Practical relevance:** The model is useful in defining the adjustments of functional elements at various hierarchical levels, proceeding from the given quality functional for the whole system at the top level of its hierarchy. The dependences were obtained which help to select an algorithm for the parametric synthesis of a hierarchical system information structure model, depending on the state of a set of its elements.

Keywords — Adaptation, System of Measurement Information Collection/Processing, Multiparameter Optimization, Neural Nets, Multilayered MLP-Qualifier.

References

1. Turchin V. F. *Fenomen nauki. Kiberneticheskii podkhod k evoliutsii* [Science Phenomenon. The Cybernetic Approach to Change of Aircraft Attitude]. Moscow, ETS Publ., 2000. 368 p. (In Russian).
2. Tsypkin Ia. Z. *Voprosy kibernetiki. Adaptivnye sistemy* [Cybernetics Questions. The Adaptive Systems]. Moscow, Nauka Publ., 1974. Pp. 5–20 (In Russian).
3. Maltsev G. N., Stogov G. V., Terekhov A. V. The Prospects of Spacecraft Control System Creation on the Basis of Key Technologies. *Informatsionno-upravliaiushchie sistemy*, 2006, no. 5, pp. 2–5 (In Russian).
4. Nazarov A. V., Kozyrev G. I., Shklyar S. V. Prognostication of Technical for Low-Orbit Spacecraft with the Use of Neural Networks. *Cosmic Research*, 2002, vol. 40, no. 6, pp. 594–604.
5. Haykin S. *Neural Networks: A Comprehensive Foundation*. New York, MacMillan College Publishing Co, 1994. 1104 p.
6. Galushkin A. I. Neurocomputer in Development of Military Technology of the USA. *Zarubezhnaja radioelektronika*, 1995, no. 5, pp. 3–48 (In Russian).
7. Nazarov A. V. Algorithm of Forecasting in Space of Situation Parameters. *Nejrokomp'jutery: razrabotka i primenenie*, 2007, no. 2–3, pp. 24–28 (In Russian).

8. Vahitov A. T., Granichin O. N., Gurevich L. S. Algorithm of Stochastic Approximation with Trial Perturbation on an Input in the Non-Stationary Task of Optimization. *Avtomatika i Telemehanika*, 2009, no. 11, pp. 70–79 (In Russian).
9. Bodianskii E. V., Rudenko O. G. *Iskusstvennye neironnye seti: arkhitektury, obuchenie, primeneniia* [Artificial Neural Networks: Architectures, Tutoring, Applications]. Khar'kov, Teletekh Publ., 2004. 369 p. (In Russian).
10. Nazarov A. V., Loskutov A. I. *Neirosetevye algoritmy prognozirovaniia i optimizatsii system* [Neural Nets Prediction Algorithms and Optimization of Systems]. Saint-Petersburg, Nauka i Tekhnika Publ., 2003. 384 p. (In Russian).
11. Werbos P. Backpropagation Through Time. What it Does and how to Do it. *Proc. IEEE*, 1990, vol. 78, pp. 1550–1560.
12. Tatuzov A. L. *Neironnye seti v zadachakh radiolokatsii* [Neural Networks in Radiolocation Problems]. Moscow, Radiotekhnika Publ., 2009. 432 p. (In Russian).
13. Osovskii S. *Neironnye seti dlia obrabotki informatsii* [Neural Networks for Information Processing]. Moscow, Finansy i statistika Publ., 2004. 344 p. (In Russian).
14. Amari S. Dreaming of Mathematical Neuroscience for Half a Century. *Neural Networks*, 2013, no. 37, pp. 48–51.
15. Cichocki A., Unbehauen R. *Neural Networks for Optimization and Signal Processing*. Stuttgart, Teubner, 1993. 526 p.

Уважаемые авторы!

При подготовке рукописей статей необходимо руководствоваться следующими рекомендациями.

Статьи должны содержать изложение новых научных результатов. Название статьи должно быть кратким, но информативным. В названии недопустимо использование сокращений, кроме самых общепринятых (РАН, РФ, САПР и т. п.).

Объем статьи (текст, таблицы, иллюстрации и библиография) не должен превышать эквивалента в 20 страниц, напечатанных на бумаге формата А4 на одной стороне через 1,5 интервала Word шрифтом Times New Roman размером 13, поля не менее двух сантиметров.

Обязательными элементами оформления статьи являются: индекс УДК, заглавие, инициалы и фамилия автора (авторов), ученая степень, звание (при отсутствии — должность), полное название организации, аннотация и ключевые слова на русском и английском языках, электронные адреса авторов, которые по требованию ВАК должны быть опубликованы на страницах журнала. При написании аннотации не используйте аббревиатур и не делайте ссылок на источники в списке литературы.

Статьи авторов, не имеющих ученой степени, рекомендуется публиковать в соавторстве с научным руководителем, наличие подписи научного руководителя на рукописи обязательно; в случае самостоятельной публикации обязательно предоставляйте заверенную по месту работы рекомендацию научного руководителя с указанием его фамилии, имени, отчества, места работы, должности, ученого звания, ученой степени — эта информация будет опубликована в ссылке на первой странице.

Формулы набирайте в Word, не используя формульный редактор (Mathtype или Equation), при необходимости можно использовать формульный редактор; для набора одной формулы не используйте два редактора; при наборе формул в формульном редакторе знаки препинания, ограничивающие формулу, набирайте вместе с формулой; для установки размера шрифта никогда не пользуйтесь вкладкой Other…, используйте заводские установки редактора, не подгоняйте размер символов в формулах под размер шрифта в тексте статьи, не растягивайте и не сжимайте мышью формулы, вставленные в текст; в формулах не отделяйте пробелами знаки: + = –.

Для набора формул в Word никогда не используйте Конструктор (на верхней панели: «Работа с формулами» — «Конструктор»), т. к. этот ресурс предназначен только для внутреннего использования в Word и не поддерживается программами, предназначенными для изготовления оригинал-макета журнала.

При наборе символов в тексте помните, что символы, обозначаемые латинскими буквами, набираются светлым курсивом, русскими и греческими — светлым прямым, векторы и матрицы — прямым полужирным шрифтом.

Иллюстрации в текст не заверстываются и предоставляются отдельными исходными файлами, поддающимися редактированию:

— рисунки, графики, диаграммы, блок-схемы предоставляйте в виде отдельных исходных файлов, поддающихся редактированию, используя векторные программы: Visio 4, 5, 2002-2003 (*.vsd); Coreldraw (*.cdr); Excel (*.xls); Word (*.doc); AdobeIllustrator (*.ai); AutoCad (*.dxf); Matlab (*.ps, *.pdf или экспорт в формат *.ai);

— если редактор, в котором Вы изготавливаете рисунок, не позволяет сохранить в векторном формате, используйте функцию экспорта (только по отношению к исходному рисунку), например, в формат *.ai, *.esp, *.wmf, *.emf, *.svg;

— фото и растровые — в формате *.tif, *.png с максимальным разрешением (не менее 300 pixels/inch).

Наличие подрисуночных подписей обязательно (желательно не повторяющих дословно комментарии к рисункам в тексте статьи).

В редакцию предоставляются:

— сведения об авторе (фамилия, имя, отчество, место работы, должность, ученое звание, учебное заведение и год его окончания, ученая степень и год защиты диссертации, область научных интересов, количество научных публикаций, домашний и служебный адреса и телефоны, e-mail), фото авторов: анфас, в темной одежде на белом фоне, должны быть видны плечи и грудь, высокая степень четкости изображения без теней и отблесков на лице, фото можно представить в электронном виде в формате *.tif, *.png с максимальным разрешением — не менее 300 pixels/inch при минимальном размере фото 40×55 мм;

— экспертное заключение.

Список литературы составляется по порядку ссылок в тексте и оформляется следующим образом:

— для книг и сборников — фамилия и инициалы авторов, полное название книги (сборника), город, издательство, год, общее количество страниц;

— для журнальных статей — фамилия и инициалы авторов, полное название статьи, название журнала, год издания, номер журнала, номера страниц;

— ссылки на иностранную литературу следует давать на языке оригинала без сокращений;

— при использовании web-материалов указывайте адрес сайта и дату обращения.

Список литературы оформляйте двумя отдельными блоками по образцам lit.dot на сайте журнала (http://i-us.ru/paperrules) по разным стандартам: Литература – СИБИД РФ, References – один из мировых стандартов.

Более подробно правила подготовки текста с образцами изложены на нашем сайте в разделе «Оформление статей».

Контакты

Куда: 190000, Санкт-Петербург,
Б. Морская ул., д. 67, ГУАП, РИЦ
Кому: Редакция журнала «Информационно-управляющие системы»
Тел.: (812) 494-70-02
Эл. почта: ius.spb@gmail.com
Сайт: www.i-us.ru

УДК 510.22.62-50

ПРИНЯТИЕ ПРОЕКТНЫХ РЕШЕНИЙ НА ОСНОВЕ НЕЧЕТКОГО ОТНОШЕНИЯ ПРЕДПОЧТЕНИЯ

С. Г. Толмачев[a]*, канд. техн. наук, начальник научно-исследовательской лаборатории*
[a]*ОАО «Концерн «Гранит-Электрон», Санкт-Петербург, РФ*

Постановка проблемы: *ответственным этапом процесса проектирования сложных технических объектов является анализ альтернативных проектных решений в целях выбора наиболее рационального варианта. На ранних стадиях проектирования задача анализа и выбора альтернатив решается в условиях большой неопределенности исходных данных, как правило, за счет использования знаний опытных разработчиков. Целью работы является разработка интеллектуальных алгоритмов анализа альтернатив для систем поддержки принятия проектных решений.* ***Результаты:*** *выбран метод анализа альтернативных решений, использующий нечеткое отношение порядка на множестве векторных лингвистических оценок экспертов и предполагающий выполнение следующих операций: вычисление значений функции принадлежности вида $\mu_<$ для каждого парного сравнения альтернатив по каждому r-му критерию $\mu_<(K_r(x_i), K_r(x_j))$; вычисление соответствующих значений функций принадлежности $\mu_\geq$; вычисление степени предпочтения для каждой альтернативы путем свертки значений функций принадлежности по критериям на основе заданной структуры предпочтений; сравнение альтернатив путем их ранжирования. Приводится пример расчета значений степеней предпочтения для случая двух альтернатив, оцениваемых по четырем показателям.* ***Заключение:*** *предложенный подход позволяет аргументировать выбор проектного решения, осуществляемый в условиях неопределенности исходных данных.*

Ключевые слова *— принятие решения, анализ альтернатив, нечеткое отношение предпочтения, лингвистические оценки.*

Введение

Процесс проектирования сложных технических объектов можно представить в виде отдельных независимых этапов. Каждый этап включает процесс принятия определенного проектного решения, являющегося основным элементом в творческой деятельности разработчика. В ходе проектирования проектировщики регулярно сталкиваются с задачами анализа и выбора решений в условиях неопределенности, вызванной неполными или неточными исходными данными. В связи с этим возникает необходимость в разработке соответствующей системы поддержки проектных решений, которая должна оказывать определенную помощь специалистам при анализе и обосновании выбора технических решений, предусмотренных этапами проектирования.

Методы, используемые в задачах поддержки принятия решений, должны учитывать особенности человеческого мышления. Основные трудности здесь связаны с тем, что некоторые категории, которыми оперируют специалисты, не всегда могут быть точно определены. Это связано с тем, что знания о проектируемом техническом объекте могут иметь неопределенную, неточную, нечеткую природу, что находит отражение в качественных оценках, выражаемых на естественном языке. Неточность исходных данных является следствием ошибок наблюдений, незнания точных значений параметров среды. Неопределенность обусловлена недостаточностью исходных данных для принятия решения. Нечеткость вызвана расплывчатой формой выражения качества объекта, которая может быть обозначена, прежде всего, средствами естественного языка.

Для решения подобных аналитических задач поддержки принятия решений необходимым условием, позволяющим получить приемлемые результаты, является всесторонний учет неопределенностей при формализации и обработке исходных данных. Эффективность учета таких данных напрямую зависит от выбора соответствующего математического аппарата. На сегодняшний день известен ряд математических методов [1–5], используемых для формализации неопределенных данных. Одним из наиболее эффективных средств решения рассматриваемых задач является интеллектуальная информационная технология Soft Computing. Эта технология, включающая теорию нечетких множеств и мер, позволяет с единых позиций рассмотреть различные виды неопределенности. В таких задачах анализ альтернативных решений проводится на основании мягких оценок показателей эффективности результатов принимаемых решений. При разработке процедур выбора альтернатив целесообразно использовать особенности, присущие выбору в расплывчатом пространстве состояний.

Основой исходной информации для принятия решения являются распределенные базы внутренних данных и данных, поступающих от разнородных внешних источников. Это могут быть данные математического моделирования, результаты натурных испытаний макетных образцов, экспертные оценки специалистов и т. п. Полученные такими способами знания о проектируемом объекте, как правило, выражаются с помощью нечетких лингвистических оценок, характерных для естественного языка [6, 7], таких как «лучше», «хуже», «большой», «малый» и т. п. При этом требуется предложить формальный метод

принятия решений, позволяющий сравнивать альтернативы путем расчета количественных значений их предпочтительности и установления отношения порядка.

Рассматриваемый в работе практический пример иллюстрирует процесс анализа альтернатив при принятии решений в нечеткой среде, когда на начальных стадиях проектирования, при отсутствии достаточных исходных данных, затруднено применение стандартных формальных процедур принятия решений.

Постановка задачи принятия решений в нечеткой среде

Задача принятия решений в нечеткой среде предполагает наличие множества альтернатив — вариантов решений. Реализация каждой альтернативы приводит к определенным последствиям — исходам. Альтернативы характеризуются по показателям эффективности (степени достижения поставленной цели) исходов. Анализ ведется на основе изучения предпочтений условного лица, принимающего решения. При этом необходимо учитывать наличие неопределенности исходной информации, которая может быть вызвана как субъективными, так и объективными факторами. Неопределенность как характеристика проектируемых технических систем определяется многообразием признаков, характеризующих объекты системы, изменениями их структуры, воздействием неучтенных, случайных факторов и т. д. Нечеткая составляющая неопределенности обусловлена необходимостью использования не только количественной, но и качественной (вербальной) оценочной информации [8].

В упрощенном виде модель задачи принятия проектных решений можно представить в следующей форме [9]:

$$< \mathbf{A}, E, \mathbf{X}, \mathbf{K}, P >,$$

где $\mathbf{A}$ — множество допустимых альтернатив (альтернатива — вариант проектного решения, удовлетворяющий ограничениям задачи и являющийся способом достижения поставленной цели); E — среда задачи, определяющая условия, в которых она решается; $\mathbf{X}$ — множество исходов; $\mathbf{K}$ — векторный критерий оценки исходов; P — структура предпочтений (определяет процедуру сравнения оценок $K(X)$).

Каждой альтернативе $a_i \in \mathbf{A}$ соответствует единственный (детерминированный или случайный) исход $x_i \in \mathbf{X}$, который характеризуется векторной оценкой $\mathbf{K}(x_i)$. Структура предпочтений P определяет процедуру сравнения оценок $\mathbf{K}(x_i)$, а решающее правило — принцип выбора элементов из множества $\mathbf{A}$ на основе результатов сравнения.

В реальных условиях альтернативы и их исходы оцениваются несколькими показателями (критериями) эффективности f_i: $\mathbf{X} \to \mathbf{K}$, $i = 1, ..., n$. Частные критерии f_i могут быть противоречивыми, например, по стоимости, по энергопотреблению, по массогабаритным характеристикам и т. д. При таких исходных условиях требуется выбрать из множества допустимых альтернатив наилучший вариант $a_{\text{opt}} \in \mathbf{A}$, обеспечивающий наиболее приемлемое, в некотором смысле, значение показателя эффективности $\mathbf{K}$ соответствующего исхода $x_{\text{opt}} \in \mathbf{X}$, т. е. $a_{\text{opt}} = \arg(\max(\mathbf{K}))$, где операция max интерпретируется как выбор наилучшего значения. Выбор наилучшей альтернативы в условиях неопределенности исходных данных является задачей принятия неструктурированных или слабоструктурированных решений.

В нечеткой среде в виде нечетких понятий и отношений могут быть выражены все элементы задачи: альтернативы, исходы, оценки исходов по различным критериям, отношения предпочтения и т. д. В данном случае неопределенность исходных данных выражается в виде нечетких векторных лингвистических оценок исходов по ряду критериев. В процессе анализа альтернатив путем совершения последовательности операций в нечеткой среде необходимо найти наиболее предпочтительную альтернативу, т. е. вариант решения, удовлетворяющий ограничениям задачи и имеющий наилучший показатель эффективности.

Выбор альтернативы в нечеткой среде

Рассмотрим метод выбора альтернативных решений, основанный на установлении отношения порядка на нечетких оценках исходов [10–12]. Альтернативы характеризуются лингвистическими оценками по ряду критериев. Эти оценки носят качественный характер и выражаются в виде нечетких чисел. Пусть $\mathbf{A} = \{a_1, ..., a_i, ..., a_n\}$ — множество альтернатив; $\mathbf{X} = \{x_1, ..., x_i, ..., x_n\}$ — множество исходов, причем исход x_i обусловлен альтернативой a_i, где $i = 1, ..., n$; $\mathbf{K}(x_i) = (K_1(x_i), ..., K_r(x_i), ..., K_m(x_i))$ — лингвистическая векторная оценка исхода x_i, $K_r(x_i)$ — лингвистическая векторная оценка (нечеткое число) исхода по r-му критерию, где $r = 1...m$. Нечеткое отношение порядка определим через вероятностные оценки для нечетких чисел. Введем нечеткое отношение порядка вида «больше-равно» ($\geq$) на множестве лингвистических векторных оценок исходов $\mathbf{K} = (K(x_1), ..., K(x_i), ..., K(x_n))$. Для этого определим функцию принадлежности нечеткого отношения следующим образом: $\mu_{\geq} : \mathbf{K} \times \mathbf{X} \to [0, 1]$. Введем обозначение $\mu_{\geq}(K_r(x_i), K_r(x_j))$ как $\mu^r_{\geq}(x_i, x_j)$. Значение этой функции для нечетких чисел $K_r(x_i)$ и $K_r(x_j)$ может быть вычислено по формуле

$\mu_{\geq}(A, B) = 1 - \mu_{<}(A, B)$, где A и B — нечеткие числа; $\mu_{<}$ — нечеткое отношение порядка вида «меньше» на множестве нечетких чисел. Степень истинности $\mu_{<}(A, B)$ нечеткого высказывания $A < B$ определяется как вероятность того, что точное значение нечеткого числа A будет меньше точного значения нечеткого числа B [1]: $\mu_{<}(A, B) = P(nf(A) < nf(B))$, где $nf(A)$ — четкое значение нечеткого числа A (рис. 1). Таким образом:

$$\mu_{<}(A,B) = \sum_{i=1}^{n-1} P(nf(A) = y_i \,\&\, nf(B) > y_i).$$

Предположив, что случайные величины, построенные на нечетких числах A и B, независимы, получим

$$P(nf(A) - y_i \& nf(B) > y_i = P(nf(A) = y_i)(P(nf(B) > y_i)) =$$
$$= p_A(y_i)(1 - P(nf(B) \leq y_i)) =$$
$$= p_A(y_i)(1 - P(nf(B) < y_{i+1})),\ i \in 1...n-1.$$

Тогда $\mu_{<}(A,B) = \sum_{i=1}^{n-1}(p_A(y_i)(1 - pm_B(y_{i+1}))$, где $p_A(y)$ — вероятность того, что в качестве точного значения нечеткого числа A используется величина y; $pm_B(y)$ — вероятность того, что в качестве точного значения числа B используется величина $z < y$:

$$pm_B(y) = \sum_{z \in S_B, z<y} p_B(y);$$

$$p_B(y) = \mu_B(y)\left(\sum_{y \in S_B} \mu_B(y)\right)^{-1};$$

$$p_A(y) = \mu_A(y)\left(\sum_{y \in S_A} \mu_A(y)\right)^{-1},$$

где $\mu_A(y)$, $\mu_B(y)$ — функции принадлежности нечетких чисел A и B соответственно.

Функцию $\mu_{\geq}$ определим как $\mu_{\geq}(K(x_i), K(x_j)) = \bigcup_{r \in (1..m)} \mu_{\geq}^{r}(x_i, x_j)$, где $\cup$ — знак обобщающей операции по всем r критериям. Поскольку между множеством альтернатив и исходов имеет место взаимно однозначное соответствие, нечеткое отношение предпочтения на множестве альтернатив определяется функцией принадлежности $\mu_{\geq}^{\Phi} : A \times A \to [0,1]$, которая может быть вычислена по формуле $\mu_{\geq}^{\Phi}(a_i, a_j) = \mu_{\geq}(K(x_i), K(x_j))$.

Для случая четкого векторного критерия $K(a_i) \geq K(a_j) \Leftrightarrow (\forall r \in (1, ..., m))(K_r(x_i) \geq K(x_j))$ и $a_i \geq a_j \Leftrightarrow K(a_i) \geq K(a_j)$. Выражения для $\mu_{\geq}^{\Phi}$ позволяют получить матрицу парных сравнений альтернатив по предпочтению $\Phi = \|\mu_{ij}\|_{nxn}$, где $\mu_{ij} = \mu_{\geq}^{\Phi}(a_i, a_j)$. На основе матрицы парных сравнений можно произвести ранжирование альтернатив.

Реализация описанного метода заключается в выполнении следующих операций.

1. Вычисление значений функции принадлежности вида $\mu_{<}$ для каждого парного сравнения альтернатив по каждому r-му критерию $\mu_{<}(K_r(x_i), K_r(x_j))$.

2. Вычисление соответствующих значений функций принадлежности $\mu_{\geq}$.

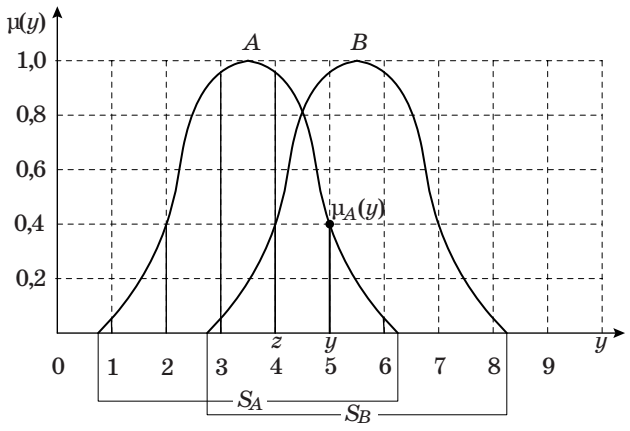
3. Вычисление степени предпочтения для каждой альтернативы путем свертки значений функций принадлежности по критериям на основе заданной структуры предпочтений.

4. Сравнение альтернатив путем их ранжирования.

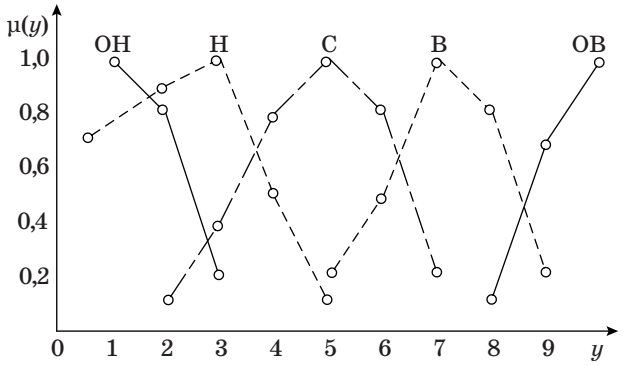
Рассмотрим пример. Пусть $\mathbf{A} = \{a_1, a_2\}$ — множество, состоящее из двух альтернативных проектных решений для технического объекта. Векторный критерий оценок исходов $\mathbf{K} = \{K_1, K_2, K_3, K_4\}$, где K_r — оценки исходов по критериям энергопотребления, стоимости, эффективности и конструктивной сложности. Предпочтения задаются вектором весовых коэффициентов $\mathbf{W} = \{w_1, w_2, w_3, w_4\}$, характеризующих важность соответствующего критерия с точки зрения проектировщика, принимающего решение. Задача состоит в нахождении альтернативы с наибольшим значением отношения предпочтительности $K(a_i) = \max_i \sum_r w_r \mu_{\geq}^{r}(x_i, x_j)$. Векторный лингвистический критерий $\mathbf{K}$ для альтернатив a_i определим в виде матрицы. Элементы матрицы представлены нечеткими оценками, заданными в форме нечетких чисел:

$\mathbf{K} =$		K_1	K_2	K_3	K_4
	a_1	ОН	В	Н	ОВ
	a_2	Н	С	С	В

где «очень низкий» ОН = {1,0/1; 0,8/2; 0,2/3}; «низкий» Н = {0,7/1; 0,9/2; 1,0/3; 0,5/4; 0,1/5}; «средний» С = {0,1/2; 0,4/3; 0,8/4; 1,0/5; 0,8/6; 0,2/7}; «высокий» В = {0,2/5; 0,5/6; 1,0/7; 0,8/8; 0,2/9}; «очень высокий» ОВ = {0,1/8; 0,7/9; 1,0/10}.



■ ***Рис. 1.*** Сравнение нечетких чисел



■ ***Рис. 2.*** Функции принадлежности нечетких оценок

Универсальное множество, на котором определены нечеткие числа, представлено в виде десятибалльной шкалы $Y = \{1, 2, ... 10\}$ на рис. 2. Определим предпочтения проектировщика в форме вектора весовых коэффициентов: $\mathbf{W} = \{0{,}3\ 0{,}2\ 0{,}4\ 0{,}1\}$.

Вычисление значений функции принадлежности $\mu_<(K_r(a_1), K_r(a_2))$:

$$\mu_<\left(K_r(a_1), K_r(a_2)\right) = \sum_{s=1}^{n} p_{K_r(a_1)}(y_s)\left(1 - \sum_{j=1}^{s} p_{K_r(a_2)}(y_j)\right).$$

В соответствии с формулой расчета вероятности $p_A(y)$ для различных альтернатив получим

$$p_{K_r(a_i)}(y_s) = \frac{\mu_{K_r(a_i)}(y_s)}{\sum\limits_{y \in S_{K_r(a_i)}} \mu_{K_r(a_i)}(y)},$$

где $r = 1, ..., 4$; $i = 1, 2$.

Каждому лингвистическому критерию K_r для альтернативы a_i соответствует оценка, принадлежащая множеству {ОН, Н, С, В, ОВ}; так, $K_1(a_1)$ = ОН, $K_1(a_2)$ = Н и т. д. Каждой оценке соответствует своя функция принадлежности нечеткого числа (см. рис. 2); так, $\mu_{K_1(a_1)}(y_1) = 1{,}0$; $\mu_{K_1(a_1)}(y_2) = 0{,}8$ и т. д. Следовательно:

$$\sum_{y \in S_{K_1(a_1)}} \mu_{K_1(a_1)}(y) = 1{,}0 + 0{,}8 + 0{,}2 = 2{,}0;$$

$$\sum_{y \in S_{K_1(a_2)}} \mu_{K_1(a_2)}(y) = 0{,}7 + 0{,}9 + 1 + 0{,}5 + 0{,}1 = 3{,}2;$$

$$\sum_{y \in S_{K_2(a_1)}} \mu_{K_2(a_1)}(y) = 0{,}2 + 0{,}5 + 1{,}0 + 0{,}8 + 0{,}2 = 2{,}7;$$

$$\sum_{y \in S_{K_2(a_2)}} \mu_{K_2(a_2)}(y) = 0{,}1 + 0{,}4 + 0{,}8 + 1{,}0 + 0{,}8 + 0{,}2 = 3{,}3;$$

$$\sum_{y \in S_{K_3(a_1)}} \mu_{K_3(a_1)}(y) = 3{,}2; \quad \sum_{y \in S_{K_3(a_2)}} \mu_{K_3(a_2)}(y) = 3{,}3;$$

$$\sum_{y \in S_{K_4(a_1)}} \mu_{K_4(a_1)}(y) = 0{,}1 + 0{,}7 + 1{,}0 = 1{,}8;$$

$$\sum_{y \in S_{K_4(a_2)}} \mu_{K_4(a_2)}(y) = 2{,}7.$$

Тогда

$$\mu_<\left(K_1(a_1), K_1(a_2)\right) = \mu_<(\text{ОН}, \text{Н}) = \frac{1{,}0}{2{,}0}(1-0) + \frac{0{,}8}{2{,}0}\left(1 - \frac{0{,}7}{3{,}2}\right) + \frac{0{,}2}{2{,}0}\left(1 - \frac{0{,}7+0{,}9}{3{,}2}\right) = 0{,}863;$$

$$\mu_<\left(K_2(a_1), K_2(a_2)\right) = \mu_<(\text{В}, \text{С}) = \frac{0{,}2}{2{,}7}\left(1 - \frac{0{,}1+0{,}4+0{,}8}{3{,}3}\right) + \frac{0{,}5}{2{,}7}\left(1 - \frac{0{,}1+0{,}4+0{,}8+1}{3{,}3}\right) + \frac{1}{2{,}7}\left(1 - \frac{0{,}1+0{,}4+0{,}8+1+0{,}8}{3{,}3}\right) = 0{,}124;$$

$$\mu_<\left(K_3(a_1), K_3(a_2)\right) = \mu_<(\text{Н}, \text{С}) = \frac{0{,}7}{3{,}2}(1-0) + \frac{0{,}9}{3{,}2}(1-0) + \frac{1}{3{,}2}\left(1 - \frac{0{,}1}{3{,}3}\right) + \frac{0{,}5}{3{,}2}\left(1 - \frac{0{,}1+0{,}4}{3{,}3}\right) + \frac{0{,}1}{3{,}2}\left(1 - \frac{0{,}1+0{,}4+0{,}8}{3{,}3}\right) = 0{,}956;$$

$$\mu_<\left(K_4(a_1), K_4(a_2)\right) = \mu_<(\text{ОВ}, \text{В}) = \frac{0{,}1}{1{,}8}\left(1 - \frac{0{,}2+0{,}5+1}{2{,}7}\right) + \frac{0{,}7}{1{,}8}\left(1 - \frac{0{,}2+0{,}5+1+0{,}8}{2{,}7}\right) = 0{,}049.$$

Вычисление нечеткого отношения $\mu_\geq(K_r(a_1), K_r(a_2))$:

$$\mu_\geq(K_r(a_1), K_r(a_2)) = 1 - \mu_<(K_r(a_1), K_r(a_2));$$

$$\mu_\geq(K_1(a_1), K_1(a_2)) = 0{,}137;$$

$$\mu_\geq(K_2(a_1), K_2(a_2)) = 0{,}876;$$

$$\mu_\geq(K_3(a_1), K_3(a_2)) = 0{,}044;$$

$$\mu_\geq(K_4(a_1), K_4(a_2)) = 0{,}951.$$

Вычисление степени предпочтения альтернативы a_1:

$$\mu_\geq(K(a_1), K(a_2)) = \sum_r w_r \mu_\geq^r(a_1, a_2) = 0{,}3 \times 0{,}137 + 0{,}2 \times 0{,}876 + 0{,}4 \times 0{,}044 + 0{,}1 \times 0{,}951 = 0{,}329,$$

т. е. степень предпочтения первой альтернативы $\mu_\geq(a_1) = 0{,}329$.

По такой же процедуре вычисляется степень предпочтения второй альтернативы a_2.

Вычисление значений функции принадлежности $\mu_<(K_r(a_2), K(a_1))$:

$$\mu_<\left(K_1(a_2), K_1(a_1)\right) = \mu_<(\text{Н}, \text{ОН}) = \frac{0{,}7}{3{,}2}(1-0) + \frac{0{,}9}{3{,}2}\left(1 - \frac{1{,}0}{2}\right) + \frac{1}{3{,}2}\left(1 - \frac{1{,}0+0{,}8}{2}\right) = 0{,}390;$$

$$\mu_<\left(K_2(a_2),K_2(a_1)\right)=\mu_<(\text{C},\text{B})=$$
$$=\frac{0,1}{3,3}(1-0)+\frac{0,4}{3,3}(1-0)+\frac{0,8}{3,3}(1-0)+\frac{1}{3,3}(1-0)+$$
$$+\frac{0,8}{3,3}\left(1-\frac{0,2}{2,7}\right)+\frac{0,2}{3,3}\left(1-\frac{0,2+0,5}{2,7}\right)=0,966;$$

$$\mu_<\left(K_3(a_2),K_3(a_1)\right)=\mu_<(\text{C},\text{H})=$$
$$=\frac{0,1}{3,3}\left(1-\frac{0,7}{3,2}\right)+\frac{0,4}{3,3}\left(1-\frac{0,7+0,9}{3,2}\right)+$$
$$+\frac{0,8}{3,3}\left(1-\frac{0,7+0,9+1,0}{3,2}\right)+$$
$$+\frac{1,0}{3,3}\left(1-\frac{0,7+0,9+1,0+0,5}{3,2}\right)=0,139;$$

$$\mu_<(K_4(a_2),K_4(a_1))=\mu_<(\text{B},\text{OB})=$$
$$=\frac{0,2}{2,7}(1-0)+\frac{0,5}{2,7}(1-0)+\frac{1}{2,7}(1-0)+$$
$$+\frac{0,8}{2,7}(1-0)+\frac{0,2}{2,7}\left(1-\frac{0,1}{1,8}\right)=0,995.$$

Вычисление нечеткого отношения $\mu_\geq(K_r(a_2), K_r(a_1))$:

$$\mu_\geq(K_1(a_2), K_1(a_1)) = 0,610;$$
$$\mu_\geq(K_2(a_2), K_2(a_1)) = 0,034;$$
$$\mu_\geq(K_3(a_2), K_3(a_1)) = 0,861;$$
$$\mu_\geq(K_4(a_2), K_4(a_1)) = 0,005.$$

Вычисление степени предпочтения альтернативы a_2:

$$\mu_\geq(K(a_2), K(a_1)) = 0,3 \times 0,610 + 0,2 \times 0,034 +$$
$$+ 0,4 \times 0,861 + 0,1 \times 0,005 = 0,535,$$

т. е. степень предпочтения второй альтернативы $\mu_\geq(a_2) = 0,535$.

Сравнивая альтернативы, видим, что альтернатива a_2 предпочтительнее, так как $\mu_\geq(a_2) > \mu_\geq(a_1)$.

Таким образом, в рассматриваемом примере рекомендуется выбор второго варианта проектного решения, имеющего наибольшее предпочтение. Реализация этого решения обеспечивает достижение нечетко поставленной цели.

Заключение

Применение предлагаемого алгоритма анализа альтернатив в нечеткой среде позволяет решить практические задачи, возникающие при проектировании сложных технических объектов. Необходимо отметить, что на выбор альтернативы существенное влияние оказывает принимаемая структура предпочтений P лица, принимающего решение. Наряду со средневзвешенной оценкой эффективности принимаемого решения может использоваться и оценка, полученная на основе минимизации отношения предпочтения. В этом случае альтернатива выбирается по методу максимина.

Литература

1. **Борисов А. Н., Крумберг О. А., Федоров И. П.** Принятие решений на основе нечетких моделей: примеры использования. — Рига: Зинатне, 1990. — 184 с.
2. **Островский Г. М., Волин Ю. М.** Технические системы в условиях неопределенности. — М.: Бином, 2008. — 319 с.
3. **Алтунин А. Е., Семухин М. В.** Модели и алгоритмы принятия решений в нечетких условиях: монография/ Тюменский гос. ун-т. — Тюмень, 2000. — 352 с.
4. **Саати Т.** Принятие решений. Метод анализа иерархий. — М.: Радио и связь, 1993. — 278 с.
5. **Райфа Г.** Анализ решений. Введение в проблему выбора в условиях неопределенности. — М.: Наука, 1977. — 408 с.
6. **Павлов А. Н., Соколов Б. В.** Принятие решений в условиях нечеткой информации: учеб. пособие для вузов. — СПб.: ГУАП, 2006. — 72 с.
7. **Piegat A.** Fuzzy Modeling and Control. — Physica-Verlag, Heidelberg, 2001. — 798 p.
8. **Заде Л. А.** Понятие лингвистической переменной и его применение к принятию приближенных решений. — М.: Мир, 1976. — 168 с.
9. **Толмачев С. Г.** Задача организации единого информационного пространства для поддержки принятия проектных решений в условиях нечеткой исходной информации // Изв. ГУАП. Аэрокосмическое приборостроение. 2013. Вып. 4. С. 29–33.
10. **Wang Y. J., Kao C. S., Liu L. J.** The Selection of Sales Managers in Enterprise by Fuzzy Multi-criteria Decision-making // Proc. of the Intern. Conf. on Artificial Intelligence and Computational Intelligence (AICI 2010), Sanya, China, Oct. 23–24, 2010. Part II. P. 142–151.
11. **Чернов В. Г.** Решение задач многокритериального альтернативного выбора на основе геометрической проекции нечетких множеств // Информационно-управляющие системы. 2007. № 1(26). С. 46–51.
12. **Ведерников Ю. В.** Метод многокритериального предпочтения сложных систем // Информационно-управляющие системы. 2009. № 1(38). С. 52–59.

UDC 510.22.62-50

Design Decision Making Based on Fuzzy Preference Relations

Tolmachev S. G.[a], PhD, Tech., Chief of Scientific Research Laboratory, cri-granit@peterlink.ru
[a]FSPC JSC «Concern «Granit-Electron», 3, Gospitalnaia St., 191014, Saint-Petersburg, Russian Federation

Purpose: One of the most crucial stages in designing sophisticated technical objects is analyzing alternative design decisions and choosing the best one. At early stages of the design, this problem has to be solved when the initial data are uncertain, relying on developers' knowledge and experience. The goal of this study is finding intellectual algorithms for analysis of design alternatives. **Results:** A method is chosen for the analysis of alternative decisions, using a fuzzy order relation on a set of linguistic vector evaluations from experts. It assumes the following operations: calculating the values of a $\mu_<$ membership function for every paired comparison of the alternatives by every r-th criterion $\mu_<(K_r(x_i), K_r(x_j))$; calculating the respective values of $\mu_\geq$ membership functions; calculating the preference degree for every alternative by convolution of the membership functions values according to the criteria based on the given structure of preferences; comparison of the alternatives by their ranking. An example is given for calculating the values of preference degrees for the case of two alternatives estimated by four parameters. **Conclusion:** The proposed approach can be used for a well-reasoned design decision making when the initial data are uncertain.

Keywords — Decision Making, Analysis of Alternatives, Fuzzy Preference Relation, Linguistic Evaluation.

References

1. Borisov A. N., Krumberg O. A., Fedorov I. P. *Priniatie reshenii na osnove nechetkikh modelei: primery ispol'zovaniia* [Decision-making Based on Fuzzy Models: Examples]. Riga, Zinatne Publ., 1990. 184 p. (In Russian).
2. Ostrovskii G. M., Volin Y. M. *Tekhnicheskie sistemy v usloviiakh neopredelennosti* [Technical Systems under Uncertainty]. Moscow, Binom Publ., 2008. 319 p. (In Russian).
3. Altunin A. E., Semuhin M. V. *Modeli i algoritmy priniatiia rechenii v nechetkih usloviah* [Models and Algorithms of Decision-making in Fuzzy Conditions: Monography]. Tumen, TGU Publ., 2000. 352 p. (In Russian).
4. Saaty T. L. *Priniatiia rechenii. Metod analiza ierarhii* [Decision-making. Method of the Analysis of Hierarchies]. Moscow, Radio i sviaz Publ., 1993. 278 p. (In Russian).
5. Raifa H. *Analiz reshenii. Vvedenie v problemu vybora v usloviiakh neopredelennosti* [Decision Analysis. Introductory Lectures on Choices under Uncertainty]. Moscow, Nauka Publ., 1977. 408 p. (In Russian)
6. Pavlov A. N., Sokolov B. V. *Priniatiia rechenii v usloviah nechetkoii informacii* [Decision-making in the Conditions of the Fuzzy Information]. Saint-Petersburg, GUAP Publ., 2006. 72 p. (In Russian).
7. Piegat A. *Fuzzy Modeling and Control*. Physica-Verlag, Heidelberg, 2001. 798 p.
8. Zadeh L. A. *Poniatie lingvisticheskoi peremennoi i ego primenenie k priniatiu priblijennih rechenii* [Concept of a Linguistic Variable and its Application to Adoption of Approximate Solutions]. Moscow, Mir Publ., 1976. 168 p. (In Russian).
9. Tolmachev S. G. The Task of Organizing a Common Information Space to Support Decision-making in Terms of Design Fuzzy Initial Information. *Izvestiia GUAP. Aerokosmicheskoe priborostroenie*, 2013, no. 4, pp. 29–33 (In Russian).
10. Wang Y. J., Kao C. S., Liu L. J. The Selection of Sales Managers in Enterprise by Fuzzy Multi-criteria Decision-making. *Proc. of the Intern. Conf. on Artificial Intelligence and Computational Intelligence (AICI 2010)*, Sanya, China, October 23–24, 2010, part II, pp. 142–151.
11. Chernov V. G. Solving Problems of Multicriterial Choice on the Basis of Geometrical Projection of Fuzzy Sets. *Informatsionno-upravliaiushchie sistemy*, 2007, no. 1, pp. 46–51 (In Russian).
12. Vedernikov Y. V. A Method of Multi-criterion Prioritization of Complex Systems. *Informatsionno-upravliaiushchie sistemy*, 2009, no. 1, pp. 52–59 (In Russian).

УДК 616-71

МИНИМИЗАЦИЯ НАГРЕВА ИМПЛАНТИРУЕМЫХ УСТРОЙСТВ С БЕСПРОВОДНОЙ ИНДУКТИВНОЙ СИСТЕМОЙ ПИТАНИЯ

О. В. Горский [a, 1], *аспирант, младший научный сотрудник*
[a]*Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, РФ*

Постановка проблемы: *потенциальными причинами нагрева тканей при использовании беспроводной индуктивной системы питания являются индуцируемые в них токи проводимости и смещения, а также выделение тепла на линейных стабилизирующих и прочих резистивных компонентах приемного модуля, предназначенного для подзарядки встроенного источника питания. При этом оптимальный уровень мощности электромагнитного поля находится в зависимости от расстояния между имплантируемым устройством и передающим индуктивным контуром. В связи с чем основной задачей исследования являлся синтез адекватного алгоритма автоматической подстройки мощности генератора, учитывающего вариабельность расстояния между индукторами, определяемого конкретными клинико-экспериментальными задачами.* ***Методы:*** *использовались расчетные методы комплексных амплитуд и отраженного импеданса трансформатора, численный расчет параметров индукторов методом конечных разностей во временной области, автоматизированный стендовый эксперимент. Исследования проводились на макете имплантируемого устройства объемом 9 см^3 в полимерном корпусе, находящемся на расстоянии 25–45 мм от передающего контура и обеспечивающем выходную мощность до 0,5 Вт для заряда аккумулятора при частоте поля до 1 МГц. В качестве имитационной среды организма использовался физиологический раствор.* ***Результаты:*** *на основании анализа расчета электрической цепи приемного модуля был синтезирован алгоритм автоматической подстройки мощности, основанный на нескольких линейных зависимостях тока в передающем контуре от сигналов обратной связи и не требующий расчета текущего значения коэффициента связи индукторов. В результате определялись три оптимальных коэффициента регулирования, соответствующие фазам недостаточной для начала заряда мощности, нарастания зарядного тока до номинального значения, чрезмерной мощности. Сравнительный анализ работы пропорционального и релейного регуляторов показал преимущество первого в условиях частого изменения расстояния между контурами, а также необходимость их реализации в целом, исходя из нагрева имплантата при постоянном уровне мощности. Предложенная конфигурация экспериментального стенда позволила оценить минимальное время безопасной работы системы и скорректировать величину зарядного тока, исходя из условия ограничения нагрева поверхности имплантата значением 2 °C.* ***Практическая значимость:*** *внедрение описанного подхода повышает безопасность применения имплантируемых устройств с перезаряжаемым беспроводным способом источником питания как в экспериментальной, так и в клинической практиках.*

Ключевые слова *— беспроводная передача энергии, индуктивное зарядное устройство, имплантируемое устройство, телеметрия, нагрев имплантата, коэффициент связи, автоматическая подстройка мощности.*

Введение

Одна из проблем создания имплантируемого устройства (ИУ) с беспроводным индуктивным модулем питания (БИМП) заключается в необходимости обеспечения безопасности жизнедеятельности организма наряду с поддержанием требуемого уровня выходной мощности для заряда аккумулятора.

Так, если массогабаритные характеристики ИУ не должны превышать 5 % от массы биологического объекта [1], что обеспечивает предупреждение механического повреждающего действия ИУ на ткани организма, то допустимый нагрев тканей, контактирующих с элементами системы, а также тканей, находящихся в зоне действия электромагнитного поля (ЭМП), не должен превышать 2 °C [2].

Вместе с тем в отличие от применения беспроводных зарядных устройств, используемых при подзарядке источников питания радиотелефонов, смартфонов и иных устройств, когда источник ЭМП и принимающий контур зарядного модуля радиоэлектронного устройства находятся на фиксированном расстоянии, расстояние между передающим (ПдК) и принимающим (ПрК) контурами БИМП ИУ может существенно изменяться.

В связи с чем возникает задача стабилизации мощности на выходе БИМП при вариабельности расстояния между ПдК и ПрК, система которых может быть описана как трансформатор с комбинированным воздушным и диамагнитным зазором с изменяемым коэффициентом связи, для которого требуется введение алгоритма автоматической подстройки мощности (АПМ) генератора. В противном случае избыток энергии будет преобразовываться в тепло на линейных регуляторах и стабилизирующих компонентах ИУ. Неоднозначность взаимного расположения ПдК и ПрК может возникнуть при таких функциональных задачах, как передача энергии на ИУ, находящееся в мелком лабораторном животном, которое свободно перемещается по клетке в зоне действия ЭМП, или при расположении ИУ

[1] Научный руководитель — кандидат технических наук, начальник научно-исследовательского отдела биотехнических проблем Санкт-Петербургского государственного университета аэрокосмического приборостроения *В. А. Килимник*.

в мышечной ткани более крупного объекта, когда ПдК и ПрК также не могут быть зафиксированы друг относительно друга.

На наш взгляд, алгоритм АПМ может быть основан на трех принципах: релейное регулирование с использованием минимального шага управляющего воздействия, пропорциональное регулирование, точный расчет необходимого значения выходной мощности. Первые два подхода, потенциально не требующие определения текущего значения коэффициента связи индукторов в процессе регулирования, и рассматриваются в данной статье. Реализация релейного регулятора широко освещена в литературных источниках, в то время как метод построения пропорционального регулятора, оптимального для любого коэффициента связи индукторов в заданном диапазоне, остается неизвестным. Влияние выбора алгоритма АПМ и его наличия в целом на температуру ИУ также является неоднозначным и требует экспериментальной оценки.

Устранение избыточной мощности на приемной стороне не гарантирует отсутствия чрезмерного нагрева ИУ ввиду наличия потерь на омическом сопротивлении цепей преобразования энергии, диэлектрического нагрева компонентов под действием импульсных сигналов в цепях, возникновения вихревых токов в проводящих материалах, нагрева элемента питания в процессе его разряда и заряда. Для оценки суммарного влияния описанных факторов на температуру ИУ и выбор параметров, подлежащих последующей оптимизации, требуется разработка макета системы с БИМП, а также экспериментального стенда, имитирующего нахождение ИУ в организме.

Введение в алгоритм АПМ обратной связи по температуре ИУ позволило бы снизить риск нанесения термической травмы при недостаточном отведении тепла от источника. На начальном этапе требуется рассмотреть линейную зависимость стабилизируемой величины от температуры ИУ для оценки целесообразности ее введения и характера изменения параметров системы.

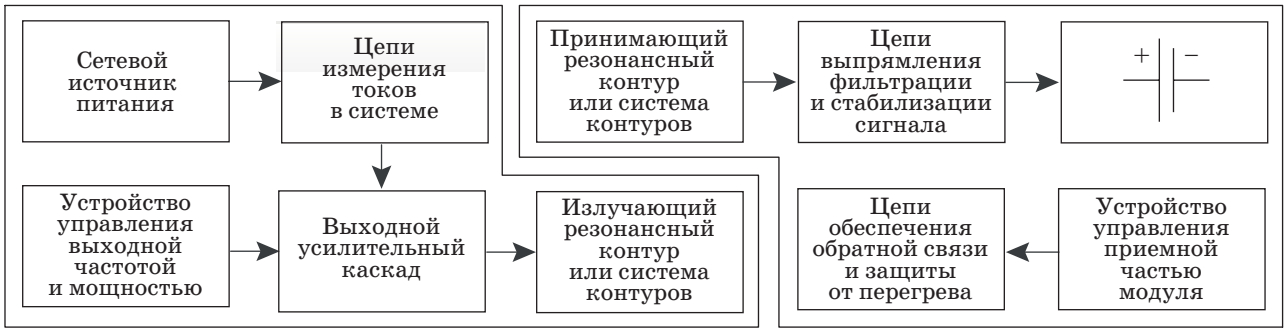
Структура макета и схемотехническая реализация приемной части БИМП

На первом этапе исследования были определены основные характеристики макета: выходная мощность до 0,5 Вт, частота ЭМП до 1 МГц, объем ИУ до 10 см^3, максимальное расстояние между ПдК и ПрК — 50 мм. Индукторы ПдК и ПрК представляют собой спиральные катушки с воздушным сердечником размерами соответственно 100×100×0,1 и 30×20×0,9 мм.

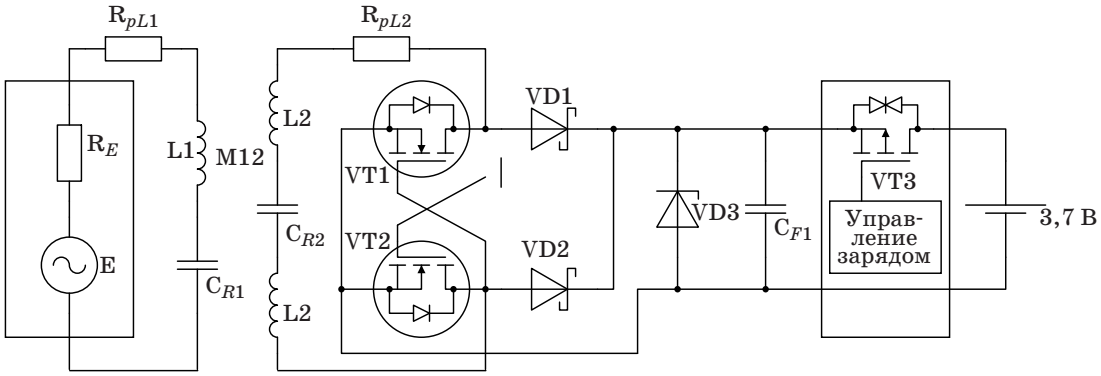
Далее на основании анализа литературных источников [3–7] была синтезирована структурная схема (рис. 1).

В качестве выходного усилительного каскада обычно применяются схемы класса *C*, полу- или полномостового *D*, *E*. В исследованиях [3, 4] показано, что наибольшей эффективностью передачи обладает система, состоящая из четырех резонансных индуктивных контуров. Однако для решения задач описываемого исследования достаточно было реализовать двухконтурную систему. Метод выбора между последовательным или параллельным резонансом определяется величиной нагрузки ПрК и описан в работе [5].

Схемотехническое решение приемной стороны (рис. 2) было реализовано на плате площадью 93 мм^2 при одностороннем монтаже компонентов. Было введено несколько изменений в стандартную схему [5]: реализованный на дискретных компонентах VT_1, VT_2, VD_1 и VD_2 полусинхронный выпрямитель, позволяющий снизить суммарное активное сопротивление цепи; включение резонансного конденсатора C_{R2} в середину индуктора ПрК (между L_2 и L_2') для снижения его диэлектрического нагрева, вызванного коммутацией ключей выпрямителя; диод Зенера VD_3, предназначенный для устранения кратковременных скачков напряжения, например, в момент изменения расстояния между контурами. В качестве нагрузки использовалась интегральная схема управления зарядом с линейной стабилизацией выходного сигнала и аккумулятор LP502030 (250 мА·ч).



■ ***Рис. 1.*** Структурная схема приемопередающих частей БИМП



■ ***Рис. 2.*** Принципиальная электрическая схема, рассматриваемая для аналитического описания нагрузки

Для реализации информационного канала данных обратной связи применялась модуляция нагрузки ПрК, детектируемая в сигнале потребляемого генератором тока. Модулирование нагрузки обеспечивалось двумя конденсаторами, подключенными параллельно ПрК и нагрузке перед выпрямителем и замыкаемыми полевыми транзисторами через землю. Протокол аналогичен описанному в стандарте *Qi* WPC (Version 1.0.1, 2010). Данные кодировались дифференциальным бифазным методом на частоте 4 кГц (длительность пакета 25 мс).

Аналитическое описание нагрузки ПрК

Для синтеза оптимального алгоритма регулирования необходимо было выразить зависимость напряжения и тока на выходе выпрямителя от тока в ПдК и проанализировать результаты аналитического описания взаимодействия цепей. Расчеты проводились для схемы, изображенной на рис. 2. Амплитуда тока в индукторе ПрК I_{2a} и наводимая на нем ЭДС индукции E_{2a} связаны выражением

$$E_{2a} = I_{2a}(Z_\Sigma + j(\omega L_2 - 1/\omega C_{R2}), \quad (1)$$

где Z_Σ — общее сопротивление нагрузки ПрК; C_{R2} — емкость резонансного конденсатора; ω — частота работы генератора.

В свою очередь амплитудные значения E_{2a} и тока ПдК I_{1a} могут быть связаны через значение коэффициента связи k катушек L_1 и L_2:

$$E_{2a} = \omega k\sqrt{L_1 L_2} I_{1a}. \quad (2)$$

Из (1) и (2), учитывая выполнение условия резонанса $\omega L_2 = 1/\omega C_{R2}$, получаем

$$I_{2a} = I_{1a}\omega k\sqrt{L_1 L_2}/Z_\Sigma. \quad (3)$$

Общее сопротивление нагрузки ПрК Z_Σ образовано параллельно включенным сопротивлением ИС управления зарядом R_{Chg} и стабилитрона R_Z (обозначим его как $R_\parallel$), а также сопротивлением индуктора ПрК R_{pL2}, поочередно работающих в каждый из полупериодов диода R_{VD} и транзистора R_{DS} выпрямителя:

$$Z_\Sigma \approx R_{pL2} + R_{VD}(V_d) + R_{DS} + R_\parallel(V_{In}, V_{Bat}), \quad (4)$$

где V_d — падение напряжения на диоде; V_{In} — напряжение на выходе выпрямителя; V_{Bat} — напряжение на аккумуляторе.

Сопротивление диода R_{VD} описывалось посредством уравнения Шокли, а сопротивление R_{DS} было принято постоянным.

Для описания вольт-амперной характеристики диода Зенера использовалась кусочно-линейная аппроксимация по характеристическим точкам, заявленным производителем:

$$I_Z(V_d) = \begin{cases} V_d \dfrac{I_r}{V_r}, \; V_d \le \dfrac{R_d I_z - V_z}{R_d I_r / V_r - 1} \\ \dfrac{V_d - V_z}{R_d} + I_z, \; V_d > \dfrac{R_d I_z - V_z}{R_d I_r / V_r - 1} \end{cases}, \quad (5)$$

где V_r — характеристическое напряжение до пробоя при токе I_r; V_z — характеристическое рабочее напряжение при токе I_z; R_d — дифференциальное сопротивление в точке $[V_z; I_z]$.

Эквивалентное сопротивление модуля заряда аккумулятора также описывалось кусочно-линейной аппроксимацией для трех диапазонов доступной от источника мощности: ниже требуемого уровня для обеспечения минимального зарядного тока I_{ChgMIN}, от предыдущего до уровня обеспечения установленного зарядного тока I_{ChgSET}, выше требуемого (далее, соответственно, режим 1, 2 и 3). С учетом тока собственного потребления I_{Sup} и сопротивления сток-исток ограничительного транзи-

стора R_{ChgDS} сопротивление R_{Chg} выражается как

$$R_{Chg}(V_{In},V_{Bat}) = \begin{cases} V_{In}/I_{Sup}, V_{In} < R_{ChgDS}I_{ChgMIN} + V_{Bat} \\ \dfrac{V_{In}}{(V_{In}-V_{Bat})/R_{ChgDS} + I_{Sup}} \\ R_{ChgDS}I_{ChgMIN} + V_{Bat} \le V_{In} \le \\ \le R_{ChgDS}I_{ChgSET} + V_{Bat} \\ V_{In}/\left(I_{ChgSET} + I_{Sup}\right) \\ R_{ChgDS}I_{ChgSET} + V_{Bat} < V_{In} \end{cases} . \quad (6)$$

Выпрямленное значение тока I_{VD} определяется как действующее значение тока в ПрК, т. е. $I_{2a}/\sqrt{2}$. С учетом выражений (3)–(6) можно вычислить V_{In} и I_{VD} путем решения системы уравнений

$$\begin{cases} V_{In} = I_{VD}(V_d)R_{\parallel}(V_{In},V_{Bat}) \\ \omega M_{12} I_{1a}/\sqrt{2} = \\ = I_{VD}(V_d)(R_{pL2} + R_{DS}) + V_{In} + V_d \end{cases}, \quad (7)$$

где $M_{12} = k\sqrt{(L_1L_2)}$ — взаимная индуктивность между L_1 и L_2.

При необходимости учесть внутреннее сопротивление генератора (R_ε — эквивалентное сопротивление источника синусоидального напряжения и R_{pL1} — активное сопротивление индуктора L_1) ток в ПдК I_{1a} может быть выражен через ток холостого хода ПдК I_{1_0a} (отсутствие ИУ в области генерации ЭМП) посредством теории отраженного импеданса:

$$I_{1a} = I_{1_0a}\frac{R_\varepsilon + R_{pL1}}{\dfrac{R_\varepsilon + R_{pL1} + \omega^2 M_{12}^2}{\left(R_{pL2} + R_{DS} + R_{\parallel}(V_{In},V_{Bat}) + R_{VD}(V_d)\right)}}. \quad (8)$$

Следующим шагом было определение диапазона изменения значения коэффициента связи.

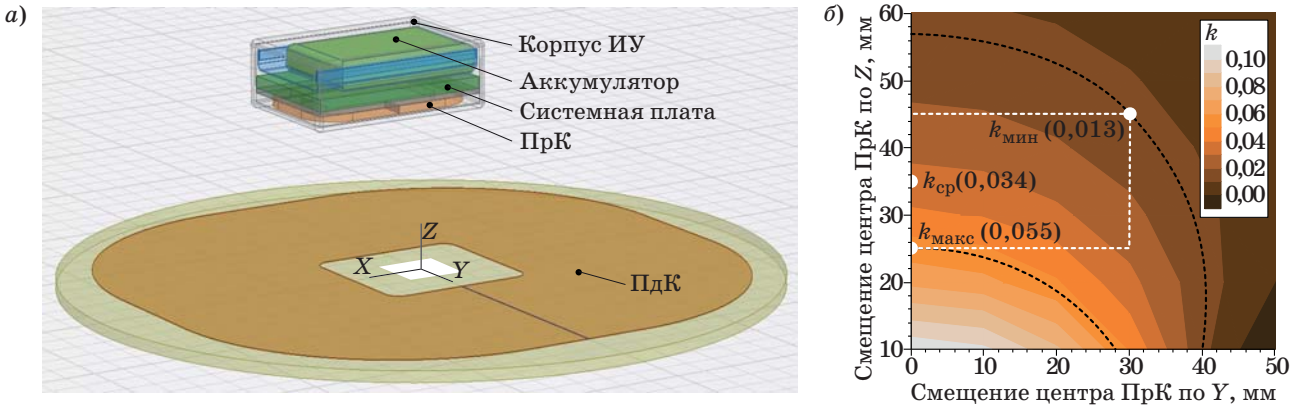
Учет вариабельности расстояния между контурами

В случае если бы мы рассматривали изолированные от окружающих объектов контуры, то целесообразно было бы воспользоваться аналитическими выражениями для расчета k, приведенными в работе [8]. Однако в реальной системе индуктор ПрК размещается в непосредственной близости от системной платы, аккумулятора, имеющего металлический корпус, а также может крепиться к ферритосодержащей подложке или сердечнику. Эти элементы влияют как на индуктивность L_2, так и на коэффициент связи k ввиду искажения магнитных линий поля и возникновения вихревых токов в электропроводящих деталях макета, поэтому распределение его значения в зависимости от координаты ПрК определялось в программе численного расчета ЭМП Ansoft Maxwell для трехмерной модели экспериментального макета (рис. 3, *а*, *б*). Ее адекватность была проверена в ходе исследований [9].

На этом этапе были выбраны условные пространственные границы неопределенности нахождения ИУ: от 25 до 45 мм по вертикали и до 30 мм смещение от оси индуктора ПдК. Были определены три точки, соответствующие минимальному, среднему и максимальному значениям k, в которых затем и производились измерения. Условность границ связана с тем, что они занимают лишь часть объема, описываемого эквипотенциальными плоскостями $k_{мин}$ и $k_{макс}$ (черные штрихпунктирные линии на рис. 3, *б*).

Расчет выходных характеристик в зависимости от тока в ПдК

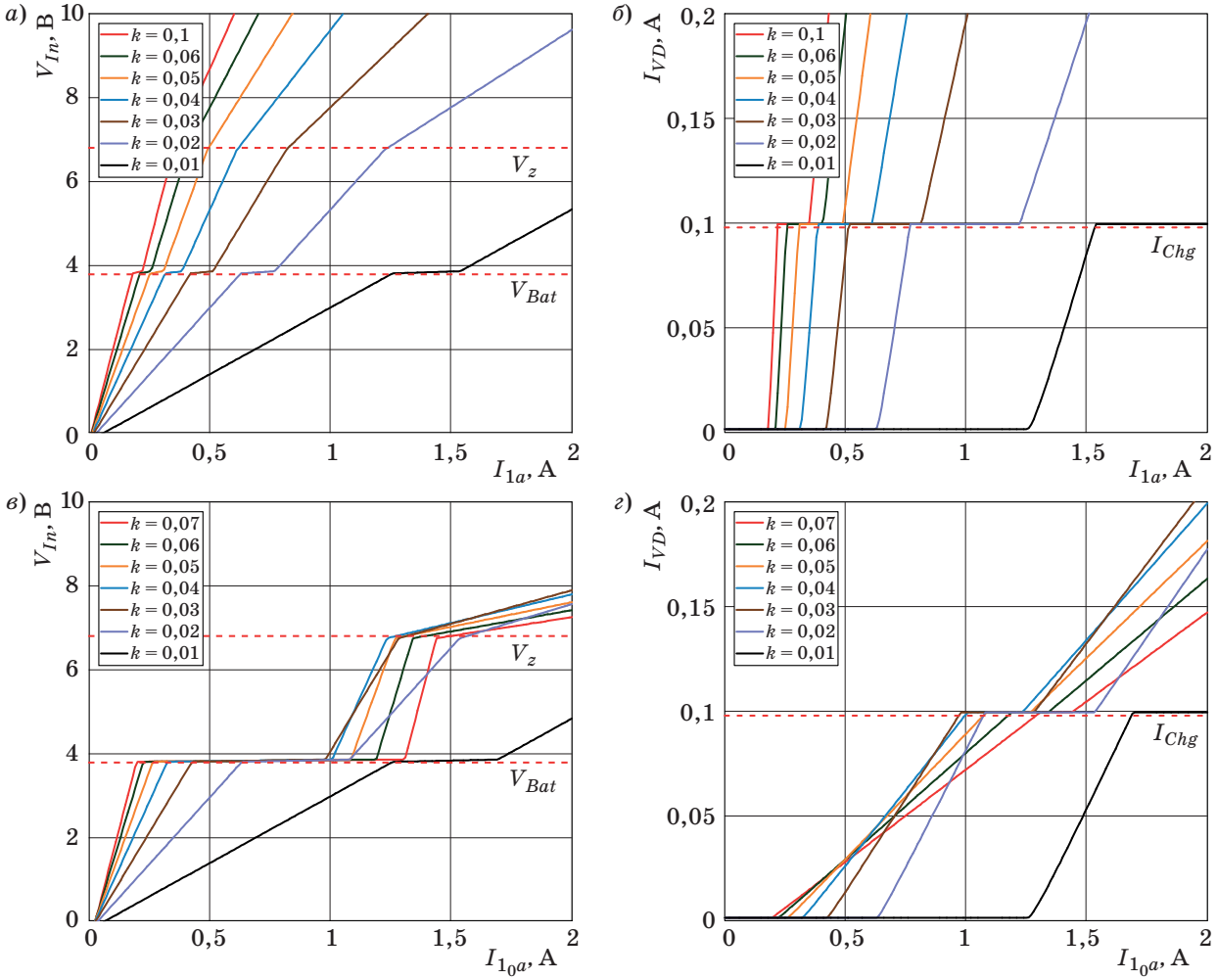
При решении системы (7) использовались данные из табл. 1. На рис. 4, *а*, *б* изображены рассчитанные характеристики V_{In} и I_{VD} в зависимо-



■ ***Рис. 3.*** Модель экспериментальной системы ИУ и ПдК (*а*) для расчета распределения величины k в зависимости от смещения ПрК по осям Y и Z (*б*)

■ ***Таблица 1.*** Характеристики экспериментального макета для расчета V_{In} и I_{VD}

Параметр	Значение	Параметр	Значение	Параметр	Значение
L_1, мкГн	83,1	R_ε, Ом	1,3	R_{DS}, Ом	0,03
L_2, мкГн	79,9	V_r, В	4	I_S, нА	830
k	0÷0,1	I_r, мкА	2	I_{ChgSET}, мА	100
R_{pL1}, Ом	1,9	V_z, В	6,8	I_{ChgMIN}, мА	20
R_{pL2}, Ом	7,5	I_z, мА	5	I_{Sup}, мА	1,4
ω, рад/мкс	5,5292	R_d, Ом	6	R_{ChgDS}, Ом	0,5



■ ***Рис. 4.*** Характеристики зависимостей V_{In} и I_{VD} от значения тока в L_1 при работе системы с нагрузкой (*а*, *б*) и в режиме холостого хода (*в*, *г*)

сти от I_{1a} при различных k. Режим 1 описывался нарастанием V_{In} до превышения уровня V_{Bat}. Затем, в режиме 2, зарядный ток аккумулятора возрастал до значения I_{ChgSET}, что означало достижение оптимального значения I_{1a}. В режиме 3 напряжение на входе микросхемы управления зарядом превышало необходимое значение, что приводило бы к дополнительному нагреву VT_3, а по достижении уровня V_z — и к выделению тепла на VD_3.

После подстановки (8) в систему уравнений (7) были получены характеристики V_{In} и I_{VD} (рис. 4, *в*, *г*). Режим 1 остался практически неизменным, так как ток I_{VD} незначителен. В режиме 2 отметим проявление эффекта согласованной нагрузки, так как при $k \approx 0{,}3$ требовалось мини-

мальное значение тока холостого хода, а следовательно, и управляющего воздействия для достижения установленного зарядного тока. Наклон характеристик в режиме 3 оставался неизменным до достижения V_{In} уровня V_z, когда также начинало сказываться наличие внутреннего сопротивления генератора.

Алгоритм автоматической подстройки мощности

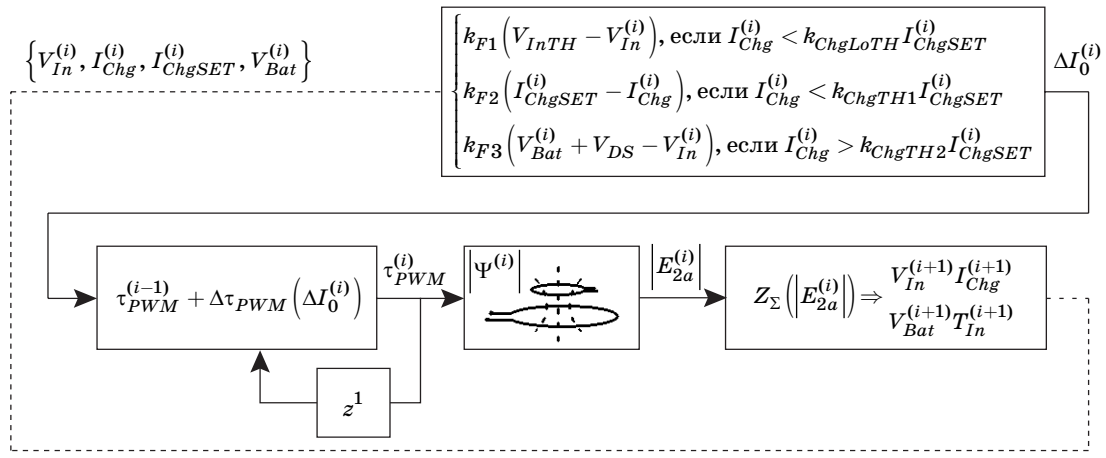
В ходе анализа кривых, представленных на рис. 4, *а*, *б*, был сделан вывод, что для реализации АПМ с использованием I_{1a} потребуется детектирование текущего режима и наклона соответствующей ему характеристики для расчета требуемого значения тока посредством экстраполяции. После определения I_{1a} необходима стабилизация параметра на новом уровне путем подстройки управляющего воздействия. Достоинства данного подхода: отсутствие необходимости вводить какие-либо калибровочные характеристики и, как следствие, отсутствие строгих требований к величине нагрузки ИУ. К недостаткам следует отнести необходимость реализовывать измеритель амплитуды тока в ПдК и проводить тестовые перестройки I_{1a} для определения коэффициента наклона в каждом из режимов.

При фиксированной нагрузке ИУ возможно применение другого подхода, лишенного описанных выше недостатков. Отказаться от реализации измерителя I_{1a} можно, введя в контроллер генератора заранее определенную зависимость тока холостого хода ПдК I_0 от управляющего воздействия. Тогда, принимая во внимание преимущественно групповой характер распределения кривых на рис. 4, *в*, *г*, возможно реализовать пропорциональный регулятор путем вычисления относительного значения тока холостого хода ПдК ΔI_0 по некоторой оптимальной для каждого из режимов и любого взаимного расположения ПдК и ПрК характеристике. Следовательно, требовалось определить масштабные коэффициенты линейных аппроксимирующих функций k_{F1}, k_{F2} и k_{F3} для выбранной конфигурации системы.

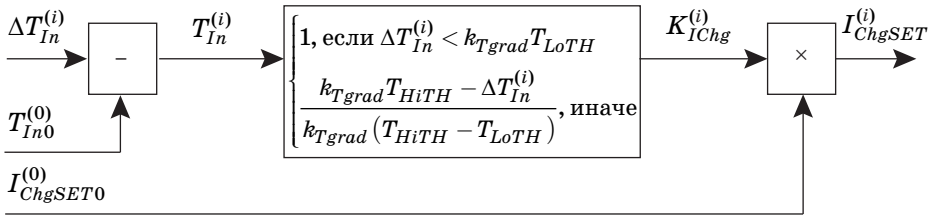
Были сформулированы критерии их выбора из соображений минимизации выделения тепла и суммарного времени воздействия ЭМП на объект. В режиме 1 допустима реализация быстрого перехода в режим 2, поэтому для расчета k_{F1} выбиралась самая пологая характеристика, но которая не допускала бы превышения оптимальной мощности при любом k. В режиме 2 оптимальная точка находилась на самой границе перед режимом 3, и при приближении к ней важно было обеспечить отсутствие перерегулирования, поэтому использовалась наиболее крутая зависимость. В случае, если все же произошел переход в режим 3, следовало максимально быстро перейти в режим 2 или 1, поэтому k_{F3} выбирался по наиболее «медленной», пологой характеристике, несмотря на возможное перерегулирование.

Согласно сформулированным критериям, были определены $k_{F1,2,3}$. При заданных параметрах системы (см. табл. 1) необходимо было выбрать k_{F1} меньше, чем при $k = 0{,}01$, так как переход между режимами 1 и 2 на максимальном удалении достигался при большем I_0, чем точка требуемой мощности при k, обеспечивающем наилучшее согласование нагрузки. Для режимов 2 и 3 выбраны кривые, рассчитанные при минимальном $k = 0{,}01$.

Предлагаемая функциональная схема алгоритма АПМ представлена на рис. 5. Индекс i обозначает значение величины в текущем цикле регулирования, при этом $i = 0$ определяет начальные значения. Расчет ΔI_0 производился по трем линейным функциям, соответственно для каждого из режимов, аргументами которых являлись параметры, передаваемые по каналу



■ ***Рис. 5.*** Функциональная схема модуля АПМ



■ ***Рис. 6.*** Функциональная схема блока ограничения I_{ChgSET}

■ ***Таблица 2.*** Значения коэффициентов регулятора мощности и температуры

Параметр	Значение	Параметр	Значение	Параметр	Значение
k_{F1}, А/В	0,244	$k_{ChgLoTH}$	0,05	k_{Tgrad}	{3, 4, 5}
k_{F2}, А/А	4,76	k_{ChgTH1}	0,85	T_{LoTh}, °С	0,5
k_{F3}, А/В	0,314	k_{ChgTH2}	0,95	T_{HiTh}, °С	2,0

обратной связи: входное напряжение V_{In}, зарядный ток I_{Chg}, номинальное значение зарядного тока I_{ChgSET}, напряжение на аккумуляторе V_{Bat}. Ввиду дискретности управляющего воздействия был введен гистерезис для I_{ChgSET}, определяемый коэффициентами k_{ChgTH1} и k_{ChgTH2}. Затем определялась величина управляющего воздействия, а именно τ_{PWM} — скважность широтно-импульсной модуляции (ШИМ) для полумостового усилителя D-класса, реализованного в макете.

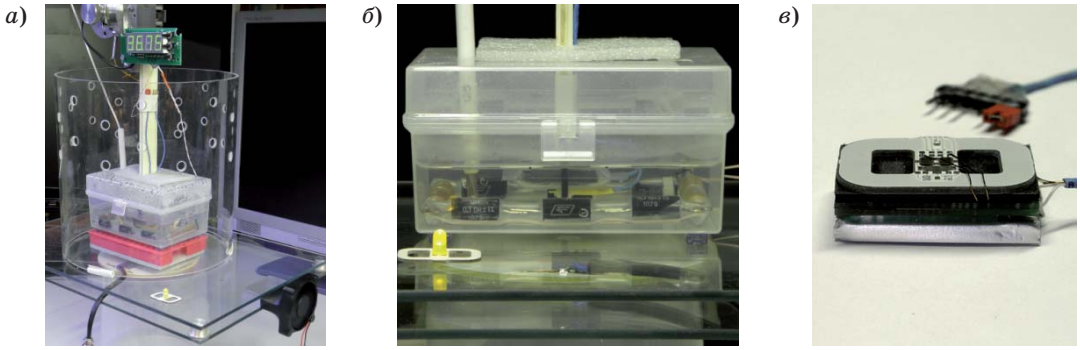
Ограничение внутренней температуры ИУ

Экспериментально было установлено, что при заданных характеристиках системы окружающая имитационная среда нагревается преимущественно от ИУ. При оптимальной установившейся величине принимаемой мощности основным источником тепла являлся индуктор ПрК, обладающий наибольшим активным сопротивлением среди всех компонентов. Для максимизации эффективности передачи энергии ПрК был расположен непосредственно у стенки полимерного корпуса ИУ. Наиболее удаленно от ПрК помещался аккумулятор, так как его металлический корпус негативно влиял на добротность индуктора. Между ними находилась системная плата. Задача нормализации температуры внешней поверхности корпуса требовала регулировки мощности распределенных источников тепла внутри него, а именно параметра I_{ChgSET} для алгоритма АПМ. Установив выводной датчик температуры на поверхности ИУ T_{Out}, можно было бы реализовать типовой регулятор, но в этом случае потребовалось бы вводить существенное конструкционное усложнение. Поэтому было решено использовать измеритель внутренней температуры T_{In}. В установившемся состоянии тепловой системы будет существовать некоторый постоянный градиент температуры $T_{In} - T_{Out}$, однако его введение привело бы к существенному снижению I_{ChgSET} уже на первых минутах заряда. Использование же линейной зависимости, определяемой коэффициентом k_{Tgrad}, позволило постепенно снизить динамику нагрева корпуса ИУ. Для этого был реализован регулятор, изображенный на рис. 6. Значения T_{LoTH} и T_{HiTH} определяли нижнюю и верхнюю границы регулирования T_{Out}.

Значения коэффициентов алгоритма автоматической подстройки мощности и температуры, использованные в экспериментах, приведены в табл. 2.

Экспериментальный стенд

Испытания макета ИУ производились на экспериментальном стенде (рис. 7, *а*). Выделение тепла, сопровождающее работу БИМП *in vivo*, происходит на фоне индивидуальных терморегуляторных процессов, обусловливаемых метаболизмом, кровотоком, теплопроводностью тканей, конвекцией тепла с поверхности кожи, что существенно усложняет синтез адекватной тепловой модели системы. Поэтому в емкости, содержащей имитационную среду (рис. 7, *б*), воспроизводились наиболее неблагоприятные условия — отсутствие температурных гомеостатических функций в условиях минимального объема. Этот подход обеспечивал термическую безопасность реального объекта. В качестве имитационной среды использовался 0,9 %-й раствор хлорида натрия, находящийся в герметичной емкости. Размер инкапсулированного макета ИУ (рис. 7, *в*) составил 34×22×12 мм. Учитывая ограничение на отношение размеров ИУ и объекта (5 %), минимальный допустимый объем имитационной среды составлял 180 см^3. Эксперименты проводились при комнатной температуре, при этом пе-



■ ***Рис. 7.*** Экспериментальный стенд: *а* — общий вид; *б* — емкость с имитационной средой; *в* — макет ИУ

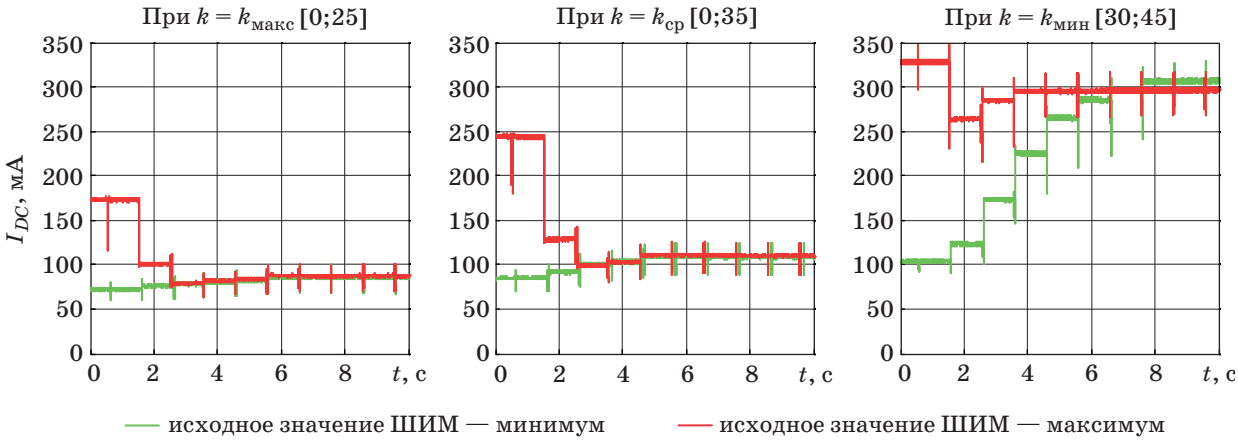
ред началом процесса заряда температура среды доводилась до установившегося значения в диапазоне 36÷38 °С нестабилизированным резистивным нагревателем мощностью 3,4 Вт. Влияние нагрева излучающего индуктора минимизировалось путем его размещения в вентилируемом зазоре между двумя пластинами.

Результаты

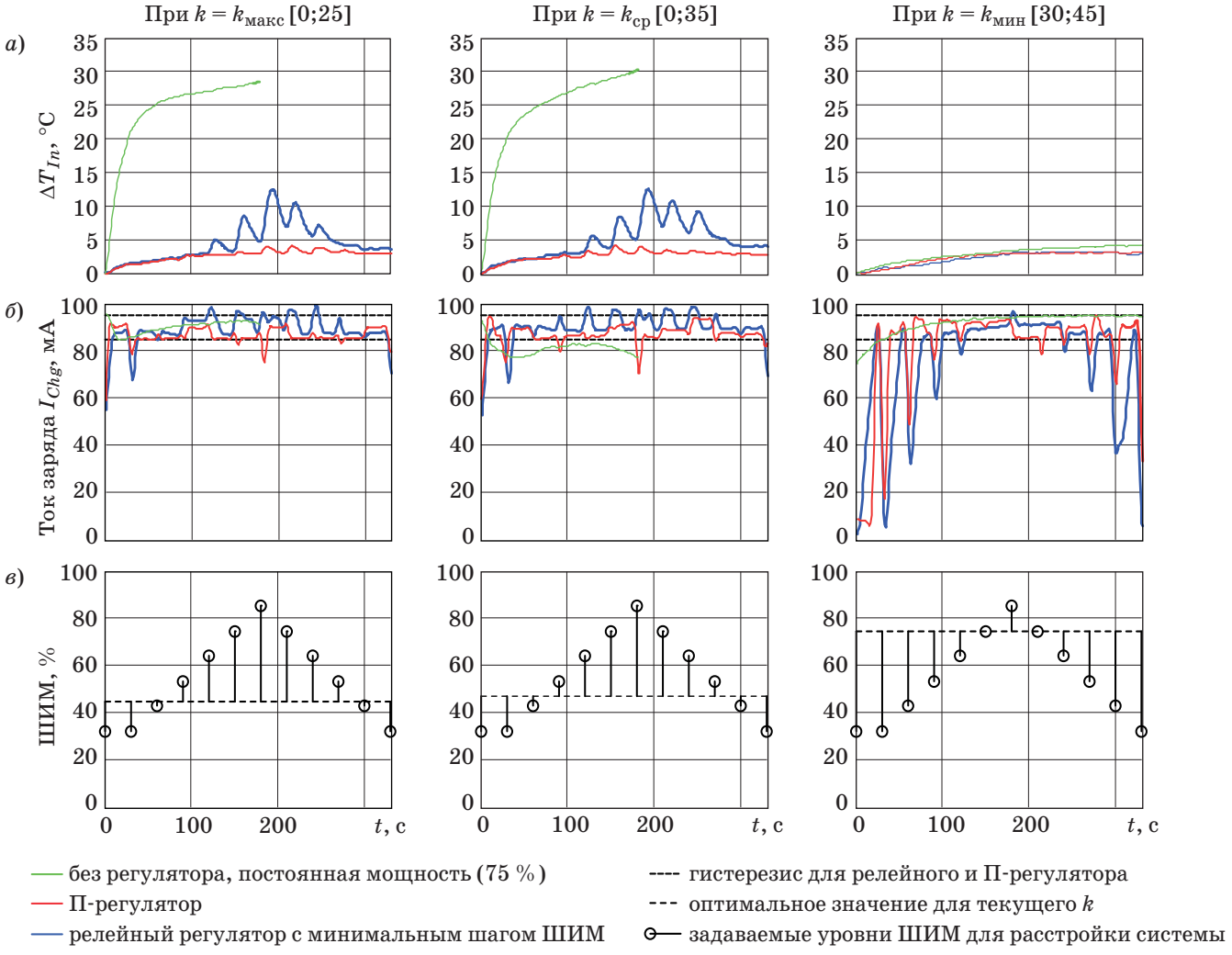
Характеристики регулирования выходной мощности генератора, управляемого описанным алгоритмом АПМ, зависимости от постоянного тока потребления генератора I_{DC} приведены на рис. 8. Отметим, что при любом k при перестройке с минимального уровня мощности нежелательное перерегулирование отсутствовало, а при перестройке с максимального уровня осуществлялся скорейший уход в безопасный режим. Различие в конечном значении I_{DC} может объясняться наличием гистерезиса для величины I_{ChgSET}.

В следующем эксперименте (рис. 9) оценивалось изменение ΔT_{In} и T_{Chg} при работе П-регулятора и релейного регулятора, использующего минимальный шаг управляющего воздействия (скважность ШИМ 2 %) для достижения требуемой мощности. Каждые 30 с производилась расстройка системы, условно имитирующая изменение коэффициента связи. П-регулятор имел преимущество по скорости работы в условиях постоянной частоты отправления данных обратной связи, что выражалось в меньшем нагреве системы по окончании теста. Для сравнения также приводятся кривые нагрева при отсутствии АПМ, когда при всех k генератор работал на мощности, необходимой для обеспечения номинального зарядного тока при $k_{мин}$.

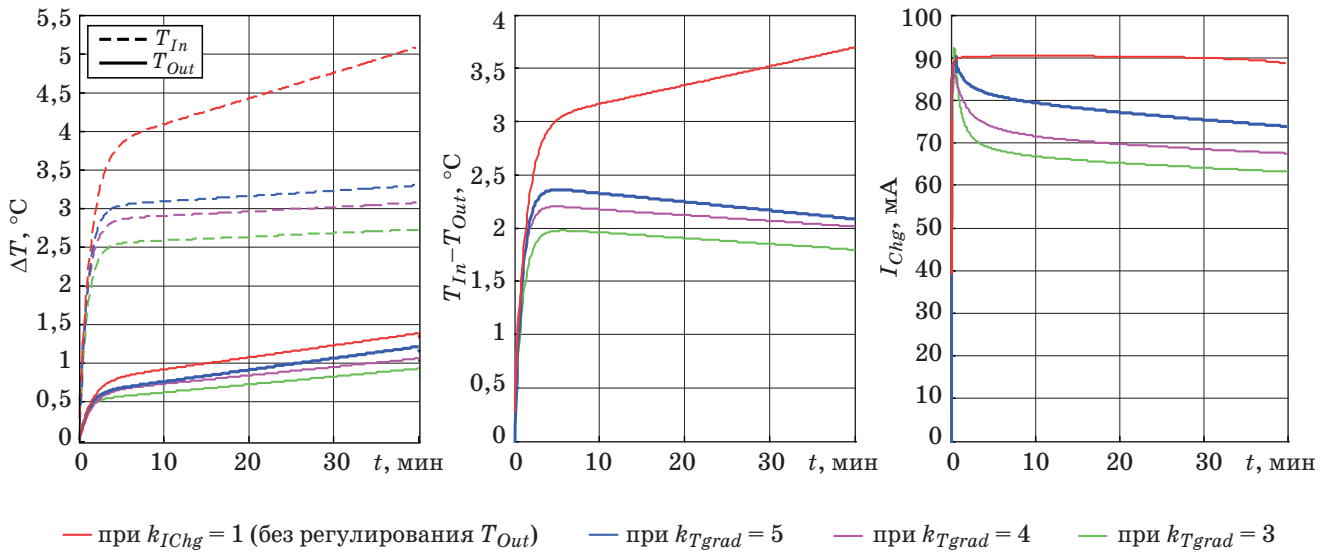
Заряд ИУ номинальным током при работе АПМ, а также регулирование температуры с использованием линейной зависимости T_{Out} от T_{In} позволило получить характеристики, представленные на рис. 10. Аппроксимация данных производилась экспоненциальной (два слагаемых) и рациональной ($n = 2$, $m = 3$) функциями соответственно для графиков температур и I_{Chg} с усреднением по трем сериям измерений. В первую очередь отметим, что ни одна из кривых T_{Out} на выбранном временном диапазоне не превысила порога безопасности +2 °С, однако динамика нерегулируемого нагрева позволяла предположить, что при заряде полностью разряженного



■ ***Рис. 8.*** Экспериментально полученные характеристики регулирования



■ ***Рис. 9.*** Изменение параметров ΔT_{In} (*а*) и I_{Chg} (*б*) в зависимости от наличия и типа регулятора при различных уровнях расстройки системы (*в*)



■ ***Рис. 10.*** Результат работы регулятора температуры при различных k_{Tgrad}

аккумулятора в течение 120 мин ΔT_{Out} превысит установленный порог (из расчета оптимального уровня I_{Chg} = 0,5 °С). Предложенный регулятор позволил замедлить рост и снизить относительную величину как ΔT_{In}, так и ΔT_{Out}. При k_{Tgrad} = 3 рост ΔT_{Out} на пологом участке составил 0,0102 °С/мин. Экстраполируя полученную характеристику, видим, что при сохранении динамики роста ΔT_{Out} порог достигался бы к 145-й минуте, при k_{Tgrad} = 4 — к 125-й минуте и при k_{Tgrad} = 5 — к 92-й минуте. Характерным являлось начало уменьшения градиента T_{In}–T_{Out} после 5-й минуты процесса заряда, что потенциально позволит ускорить достижение уравновешенного состояния описанной тепловой системы.

В заключение отметим, что нагрев имитационной среды организма под воздействием ЭМП максимальной требуемой мощности являлся пренебрежимо малым (ниже разрешения измерительного прибора, а именно 0,06 °С).

Заключение

Анализ электрических цепей БИМП показал, что пропорциональный алгоритм АПМ может быть синтезирован на основании нескольких линейных зависимостей управляющего воздействия от сигналов обратной связи. Независимо от диапазона изменения коэффициента связи индукторов требуется рассчитать функции выходных тока и напряжения от тока в ПдК при двух значениях k: минимальном и обеспечивающем наилучшее согласование нагрузки генератора. В результате определяются три оптимальных коэффициента регулирования, соответствующие режимам недостаточной для начала заряда мощности, нарастания зарядного тока до номинального значения, чрезмерной мощности.

Экспериментальная оценка работы пропорционального и релейного регуляторов показала преимущество первого в условиях частого изменения расстояния между контурами, а также необходимость их реализации в целом, исходя из нагрева ИУ при постоянном уровне мощности.

Помимо выбора алгоритма АПМ, основными параметрами для минимизации или ограничения нагрева ИУ значением +2 °С остаются активное сопротивление индуктора ПрК и зарядный ток. По результатам стендовых экспериментов могут определяться допустимые уровни I_{Chg} и выделяемой мощности на сопротивлении R_{pL2}, которое является одним из граничных условий задачи оптимизации добротности ПрК.

Линейная зависимость зарядного тока от температуры внутри ИУ позволяет ограничивать рост температуры корпуса ИУ до критического значения при определенном времени заряда и корректном выборе коэффициента в условиях минимальной термостабилизации имитационной среды.

Благодарности

Автор статьи выражает благодарность за помощь в подготовке исследований и публикационных материалов коллективу научно-исследовательского отдела биотехнических проблем ГУАП, на базе которого и была проведена настоящая работа.

Исследование выполнено при финансовой поддержке Российского научного фонда по гранту № 14-15-00788.

Литература

1. **Руководство** по экспериментальному (доклиническому) изучению новых фармакологических средств / под общ. ред. Р. У. Хабриева. 2-е изд., перераб. и доп. — М.: Медицина, 2005. – 832 с.
2. **Seese T. M., Harasaki H., Saidel G. M., Davies C. R.** Characterization of Tissue Morphology, Angiogenesis, and Temperature in the Adaptive Response of Muscle Tissue to Chronic Heating//Laboratory Investigation. 1998. Vol. 78. Iss. 12. P. 1553–1562.
3. **Kurs A.** et al. Wireless Power Transfer via Strongly Coupled Magnetic Resonances//Science. 2007. Vol. 317. P. 83–86.
4. **Xiuhan Li** et al. A Wireless Magnetic Resonance Energy Transfer System for Micro Implantable Medical Sensors//Sensors. 2012. Vol. 12. P. 10292–10308.
5. **Vandevoorde G., Puers R.** Wireless Energy Transfer for Stand-alone Systems: a Comparison Between Low and High Power Applicability//Sensor and Actuators a Physical. 2001. Vol. 92. N 1–3. P. 305–311.
6. **Artan N. S.** et al. A High-Performance Transcutaneous Battery Charger for Medical Implants//32nd Annual Intern. Conf. of the IEEE Engineering in Medicine and Biology Society (EMBC 2010), Buenos Aires, Argentina, Aug.-Sept. 2010. P. 1581–1584.
7. **Jow U., Ghovanloo M.** Design and Optimization of Printed Spiral Coils for Efficient Transcutaneous Inductive Power Transmission//IEEE Transactions on Biomedical Circuits and Systems. 2007. Vol. 1. N 3. P. 193–202.
8. **Zierhofer C. M., Hochmair E. S.** Geometric Approach for Coupling Enhancement of Magnetically Coupled Coils//IEEE Transactions on Biomedical Engineering. 1996. N 43. P. 708–714.
9. **Горский О. В.** Исследование базовой модели индуктивно связанных контуров бесконтактного зарядного устройства имплантируемых систем // Информационно-управляющие системы. 2013. № 6. С. 48–57.

UDC 616-71

Self-Heating Minimization of Implantable Devices with a Wireless Inductive Power Supply System

Gorskiy O. V.[a], Post-Graduate Student, Junior Researcher, gorskijoleg@gmail.com
[a]Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St., 190000, Saint-Petersburg, Russian Federation

Purpose: When using a wireless inductive power system, tissue heating can be caused by the conduction and displacement currents induced within the body, or by the heat discharged from the LDOs and other resistive components of the receiver module which is designed to recharge the internal battery. The optimum EMF power level depends on the distance between the implanted device and the transmitting coil. Therefore, the main objective of this study was synthesizing an adequate algorithm for the automatic adjustment of the generator power, taking into account the variability of the distance between the inductors defined by particular clinical and experimental tasks. **Methods:** The study used the calculation methods of complex amplitude and reflected transformer impedance, the calculation of inductor coupling coefficient by the finite difference time-domain method, and an automated simulation experiment. The study was performed on a 9 cm^3 model of implant in a polymer casing. At a distance of 25–45 mm from the transmitting coil, this model can provide an output power of 0.5 watts to charge the battery at EMF frequency of 1 MHz. Normal saline was used as the body simulation environment. **Results:** Analyzing the electrical circuit in the receiver module, an automatic power adjustment algorithm was designed, which is based on several linear dependencies between the current in the transmission coil and the feedback signals, without the need to calculate the current coupling coefficient of the inductors. As a result, three optimal adjustment coefficients were determined, corresponding to the following phases: insufficient power to start charging, increase of the charging current to the nominal value, and excessive power. Comparative analysis of the proportional and relay adjustors showed the advantage of the first under the conditions of frequent changes in the distance between coils, as well as the need for their implementation as a whole, based on the implant heating at a constant EMF power level. The proposed configuration of the experimental stand allowed us to estimate the minimum safe operation time for the system and adjust the value of the charging current, assuming that the implant case temperature increase is limited by 2 °C. **Practical relevance:** The described approach increases the safety of using implants with a wireless rechargeable power source in both experimental and clinical practices.

Keywords — Wireless Power Transmission, Inductive Charger, Implantable Device, Telemetry, Heating of Implant, Coupling Coefficient, Automatic Power Adjustment.

References

1. *Rukovodstvo po eksperimental'nomu (doklinicheskomu) izucheniiu novykh farmakologicheskikh sredstv* [Guide to the Experimental (Preclinical) Study of New Pharmacological Agents]. Ed. by Prof. Khabriev R. U. Moscow, Meditsina Publ., 2005. 832 p. (In Russian).
2. Seese T. M., Harasaki H., Saidel G. M., Davies C. R. Characterization of Tissue Morphology, Angiogenesis, and Temperature in the Adaptive Response of Muscle Tissue to Chronic Heating. *Laboratory Investigation*, 1998, vol. 78, iss. 12, pp. 1553–1562.
3. Kurs A., Karalis A., Moffatt R., Joannopoulos J. D., Fisher P., Soljacic M. Wireless Power Transfer via Strongly Coupled Magnetic Resonances. *Science*, 2007, vol. 317, pp. 83–86.
4. Xiuhan Li, Hanru Zhang, Fei Peng, Yang Li, Tianyang Yang, Bo Wang, Dongming Fang. A Wireless Magnetic Resonance Energy Transfer System for Micro Implantable Medical Sensors. *Sensors*, 2012, vol. 12, pp. 10292–10308.
5. Vandevoorde G., Puers R. Wireless Energy Transfer for Stand-alone Systems: a Comparison Between Low and High Power Applicability. *Sensor and Actuators a Physical*, 2001, vol. 92, no. 1–3, pp. 305–311.
6. Artan N. S., Vanjani H., Vashist G., Fu Z., Bhakthavatsala S., Ludvig N., Medveczky G., Chao H. J. A High-Performance Transcutaneous Battery Charger for Medical Implants. *32nd Annual Intern. Conf. of the IEEE Engineering in Medicine and Biology Society (EMBC 2010)*, Buenos Aires, Argentina, August-September 2010, pp. 1581–1584.
7. Jow U., Ghovanloo M. Design and Optimization of Printed Spiral Coils for Efficient Transcutaneous Inductive Power Transmission. *IEEE Transactions on Biomedical Circuits and Systems*, 2007, vol. 1, no. 3, pp. 193–202.
8. Zierhofer C. M., Hochmair E. S. Geometric Approach for Coupling Enhancement of Magnetically Coupled Coils. *IEEE Transactions on Biomedical Engineering*, 1996, no. 43, pp. 708–714.
9. Gorskiy O. V. Research on a Basic Model of Inductively Coupled Coils in a Charging System for Implanted Systems. *Informatsionno-upravliaiushchie sistemy*, 2013, no. 6, pp. 48–57 (In Russian).

УДК 656.22

МЕТОДЫ ОЦЕНКИ ПРОПУСКНОЙ СПОСОБНОСТИ ЖЕЛЕЗНЫХ ДОРОГ
Часть 1: Аналитические методы оценки и анализа использования

С. А. Браништов[a]***,*** *канд. техн. наук, исполняющий обязанности заведующего лабораторией*
А. М. Ширванян[a]***,*** *младший научный сотрудник, аспирант*
Д. А. Тумченок[a]***,*** *младший научный сотрудник, аспирант*
[a]*Институт проблем управления им. В. А. Трапезникова РАН, Москва, РФ*

Введение: *пропускная способность — важная характеристика участка железной дороги, показывающая его перевозочные возможности. Без ее учета невозможно безошибочно планировать грузовые перевозки по сети. Для получения этой характеристики в разных странах используют аналитические методы, основанные на моделях, которые включают в себя набор различных параметров, таких как интервал движения поездов; средний межпакетный интервал; коэффициент, учитывающий надежность работы технических средств, и др. В работе рассматриваются наиболее распространенные методы оценки пропускной способности.* ***Результаты:*** *приведены определения различных видов пропускной способности, используемых в данной отрасли: наличной, проектируемой, потребной и результативной; проведено сравнение аналитических методов анализа использования пропускной способности. Показано, что аналитические методы дают представление о пропускной способности сети, но не учитывают в совокупности все факторы, влияющие на пропускную способность.* ***Практическая значимость:*** *материалы статьи будут интересны работникам железнодорожных служб: диспетчерам, графистам, технологам и др., — так как применение аналитических методов при расчете самой пропускной способности и доли ее фактического использования поможет планировать грузовые и пассажирские перевозки более эффективно.*

Ключевые слова *— пропускная способность, железная дорога, сжатие расписания.*

Введение

Задача определения пропускной способности (ПС) транспортных магистралей всегда актуальна, его результаты используются при планировании строительства новых дорог, развития инфраструктуры, заказов на перевозку грузов и пассажиров, при управлении перевозочным процессом. Понятие пропускной способности относят к той части железной дороги, возможности которой по обеспечению трафика хотят обозначить. Это может быть целый железнодорожный участок, отдельный перегон или станция. Более того, есть предложения рассчитывать ПС разветвленных полигонов и направлений [1]. В данной статье в основном рассматривается ПС участка железной дороги.

В литературе встречается большое разнообразие формулировок, касающихся ПС. Но не существует единого устоявшегося общепринятого определения понятия ПС, и нет даже однозначного понимания этого термина. Неоднозначность в определении ПС характерна не только для железнодорожного транспорта, но и для других видов транспорта [2].

Основное определение, которым руководствуются железнодорожники России, приведено в Инструкции по расчету наличной пропускной способности [3]: «Наличной пропускной способностью железнодорожного участка называется максимальное число грузовых поездов (пар поездов) установленных веса и длины, которое может быть пропущено по этому участку за сутки в зависимости от его технической оснащенности и принятого способа организации движения поездов».

За рубежом наиболее часто ссылаются на определение, которое дал Крюгер (Krueger): «Пропускная способность — это возможность пропустить определенное количество поездов по заданной линии за единицу времени, при заданных ресурсах и графике движения» [4]. Есть и другие определения, например: «Способность объекта инфраструктуры обработать (пропустить) определенное количество поездов при соблюдении пунктуальности следования» [5].

Международный союз железных дорог (МСЖД (UIC)) в 2004 г. пришел к выводу, что однозначное определение пропускной способности давать не имеет смысла, поскольку ПС железнодорожного участка зависит от того, как используют железнодорожную инфраструктуру. Если железнодорожная инфраструктура задана, то значение ПС характеризуется четырьмя параметрами [6]. Число поездов — это общее количество поездов за заданный интервал времени (например, число поездов в сутки). Стабильность рассматривается как воздействие одной минуты задержки какого-либо поезда на движение последующих поездов. Гетерогенность движения определяется соотношением числа поездов различного типа. Средняя скорость характеризуется средней скоростью движения всех поездов.

Классификация пропускной способности

В соответствии с инструкцией [3] в России различаются следующие виды пропускной способности для участка дороги:

— наличная (максимальная) по ограничивающему перегону — характеризует текущие возможности инфраструктуры реализовать максимальные размеры движения в идеальных условиях;

— проектируемая при развитии технического оснащения инфраструктуры;

— потребная для обеспечения пропуска перспективных грузовых и пассажирских потоков при планировании инвестиций и проектировании новых линий;

— результативная — наименьшая среди ПС перегонов, станций, деповского хозяйства, устройств электроснабжения.

За рубежом используют следующую классификацию видов пропускной способности участка железных дорог [4, 7]:

— теоретическая — максимальное возможное расчетное значение ПС;

— практическая — предел ПС, реализуемый на практике, при заданной инфраструктуре;

— использованная — фактический объем трафика;

— доступная — разница между практической и использованной ПС, показывает резерв по трафику.

Очевидно, что теоретическое значение ПС никогда не может быть достигнуто на практике, поэтому удобней рассматривать практическую пропускную способность. Действительно, правильно определив практическую ПС и зная использованную ПС, можно получить величину доступной ПС.

Методы оценки и анализа использования пропускной способности

Все известные подходы к оценке и анализу использования пропускной способности делятся на:

— аналитические методы — используют математические зависимости ПС от параметров инфраструктуры и характера организации движения на участке [3, 6, 8];

— параметрические модели — предоставляют систему оценки эффекта изменения ПС при изменении параметров инфраструктуры и характера движения на участке [2, 9, 10];

— методы анализа использования ПС, основанные на оптимизации и регулировании параметров движения, ресурсов инфраструктуры, оптимизации операций с поездами. Применяются для задач планирования движения, например, формирования расписания, маршрутизации и распределения вагонопотоков грузовых поездов [10–13];

— методы, основанные на моделировании — позволяют оценить максимальные размеры движения при различных условиях в эксперименте для заданных моделей участка железной дороги, поездов, расписания [14–16].

Аналитические методы оценки пропускной способности

С 1953 г. было разработано более 50 методик расчета и оценки использования ПС и создано более 40 программных пакетов моделирования и оптимизации [17]. В этой работе коснемся лишь некоторых, получивших наибольшее распространение за рубежом.

Впервые аналитическое выражение для ПС в зависимости от характера движения поездов предложил Поле (Poole) [8]. Пропускная способность (число поездов в сутки) при однородном графике движения поездов оценивается по выражению

$$C = 1440 \times 2/(2 \times t + t/2 + m), \qquad (1)$$

где 1440 — число минут в сутках; t — интервал между поездами, мин; $t/2$ — средний межпакетный интервал между встречными поездами; m — задержка для каждой пары поездов из-за возможного ускорения и торможения; 2 — число поездов в паре.

В России аналитические выражения и правила расчета ПС зафиксированы в инструкции [3]. Исходными данными для расчета наличной ПС являются:

— количество главных путей на перегоне;

— средства сигнализации и связи по движению поездов;

— путевое развитие промежуточных раздельных пунктов;

— принятый тип графика движения;

— времена хода поездов по перегонам;

— станционные и межпоездные интервалы;

— особые условия организации движения поездов (подталкивание или двойная тяга поездов, обслуживание примыканий на перегоне, порядок следования по сплетениям путей, перегонам с однопутными мостами на двухпутных линиях и др.).

Пропускная способность вычисляется поразному в зависимости от принятого типа графика (непакетный, частично-пакетный, пакетный) и соотношения размеров движения в четном и нечетном направлениях.

Графики движения поездов классифицируются по следующим типам:

— по числу главных путей: однопутные, однопутно-двухпутные (однопутные участки с двухпутными вставками), двухпутные, многопутные;

— по используемым средствам сигнализации и связи: пакетные и частично-пакетные (когда на перегоне может находиться несколько поездов попутного направления; применяются на линиях с автоматической блокировкой), пачечные (применяются только на однопутных линиях, не оборудованных автоблокировкой, на перегоне может находиться только один поезд попутного направления);

— по соотношению скоростей движения поездов по участку и перегонам: параллельные (скорость всех поездов различных категорий одинаковая), непараллельные (поезда движутся с разными скоростями);

— по соотношению числа поездов по направлениям следования: парные и непарные.

Наличная ПС участка по перегонам определяется при параллельном графике движения поездов с округлением полученного результата до ближайшего целого значения в меньшую сторону. При этом на двухпутных линиях расчет ведется исходя из применения только пакетного графика движения поездов, а на однопутных линиях — при применении обоих типов графика в зависимости от средств сигнализации и связи по движению поездов [3].

Например, для двухпутного графика движения расчет ПС выполняется по формуле

$$N_{\text{нал}} = (1440 - t_{\text{тех}}) \times \alpha_{\text{н}}/J_{\text{р}}, \qquad (2)$$

где $N_{\text{нал}}$ — рассчитываемая наличная ПС; $t_{\text{тех}}$ — продолжительность суточного бюджета времени, выделяемого для производства плановых ремонтно-строительных работ (для двухпутных = = 150 мин); $\alpha_{\text{н}}$ — коэффициент, учитывающий надежность работы технических средств (для двухпутных $\alpha_{\text{н}}$ принят 0,96 при электрической и 0,95 при тепловозной тяге); $J_{\text{р}}$ — расчетный межпоездной интервал между поездами попутного направления, определяемый в соответствии с положениями [3] по определению станционных и межпоездных интервалов.

Аналитические методы используют простые математические выражения и сжатие расписания для количественной оценки пропускной способности участка железной дороги. Между тем эти методы обладают рядом недостатков.

В формуле (2) отсутствует ограничение на величину межпоездного интервала. По сути это означает, что теоретически ПС может быть бесконечно большой.

Зависимость между ПС и межпоездным интервалом носит линейный характер. При этом результаты моделирования движения поездов показывают, что эта зависимость имеет линейный характер только в области небольшой загрузки участка (до точки насыщения на рис. 1). В точке насыщения эта зависимость становится нелинейной и начинается разрыв между интенсивностью потока поездов на входе и выходе с участка (между теоретической и фактической ПС).

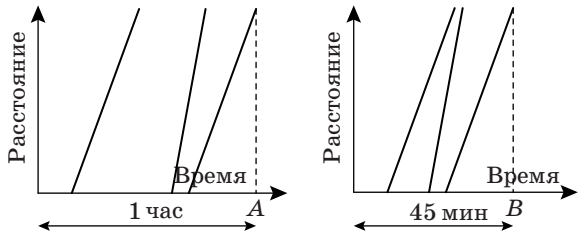
Одним из явных недостатков аналитических методов расчета ПС является допущение о равномерной скорости движения на перегоне, что не может быть совсем правильным [1].

Пропускную способность необходимо определять не в конкретной точке, а на всем протяжении участка ввиду реакции участка на различные размеры движения поездов. При этом важно учесть ограничения на ПС границ участка и станций. Реакция показывает взаимосвязь между интенсивностью входного и выходного транспортных потоков (рис. 2). На рисунке видно, что при некотором входном потоке создается насыщение участка и далее при возрастании этого потока возможно даже сокращение интенсивности движения через участок. Это связано с тем, что принимающая станция не успевает пропускать поезда и на участке падает скорость движения.

В аналитических моделях пытаются учесть все условия движения, но это приводит к тому, что методика расчета усложняется настолько, что ею перестают пользоваться [1]. В аналитических методах используют средние величины, которые не учитывают многообразие особенностей движения поездов.

Существенным недостатком является то, что аналитическими методами не определяются мак-

■ ***Рис. 1.*** Влияние интенсивности движения поездов на входе участка на пропускную способность



■ ***Рис. 2.*** Сжатие расписания методом CUI (слева — до сжатия, справа — после сжатия)

симальные размеры движения поездов. Это приводит к тому, что пропускная способность, вычисленная аналитическими методами, отличается от практической ПС.

На Западе более распространена оценка использования пропускной способности железнодорожного участка. Этот параметр непосредственно показывает свободные ресурсы железной дороги при принятой организации движения на этом участке в данный период времени. Под использованием ПС понимают ту часть пропускной способности, которая была использована при заданном графике движения и заданной инфраструктуре.

Метод CUI

Этот метод является основным для анализа использования ПС, принятым в Великобритании.

Чтобы рассчитать индекс использования ПС, расписание подвергают «сжатию», сокращая все незанятые поездами промежутки времени из расписания. По сути, нитки графика располагают наиболее компактно друг к другу. При этом график после «сжатия» остается реализуемым и учитывает все необходимые ограничения на межпоездной интервал и пр. Индекс определяется отношением времени «сжатого» графика ко времени текущего графика:

$$I = B/A, \tag{3}$$

где A и B — периоды времени графика до и после «сжатия» при сохранении размеров движения.

В примере на рис. 2 индекс составляет 45 мин/60 мин = 75%.

Сжатие выполняют по каждому перегону отдельно, при этом сокращая (если это допустимо) или удлиняя время обработки (стоянки) поездов на станции. Следовательно, сдвиги ниток на перегоне при согласовании всего хода по участку могут быть выполнены различными вариантами. Метод обладает недостатками: в зависимости от способа сжатия получается разная ПС, к тому же результат довольно неточен — метод оценивает ПС участка железной дороги, опираясь только на свойства перегонов, и не учитывает ограничения станций.

Метод UIC 406

Наиболее распространенным методом анализа ПС в Европе является метод UIC 406. Он был разработан МСЖД [6] и принят в 19 европейских странах. В основе метода также лежит сжатие расписания, но имеется различие в способе разделения участка на сегменты, по которым сжатие выполняется отдельно. Согласно рекомендации в работе [6], нитки в графике должны наиболее плотно находиться друг к другу, не нарушая интервалы безопасности. Иными словами, расписание должно быть «сжато» так, чтобы в нем оставалось как можно меньше времени между нитками графика. Как правило, запасное время вводят специально для уменьшения распространения задержек между поездами при нештатной ситуации. Это повышает надежность расписания, но существенно снижает ПС.

Пример сжатия расписания для однопутного и двухпутного перегонов методом UIC 406 показан на рис. 3.

Использованную пропускную способность определяют по формуле [5]

$$K = k \times 100/U\ [\%], \tag{4}$$

где U — рассматриваемый временной интервал, мин; k — суммарное время, мин:

$$k = A + B + C + D. \tag{5}$$

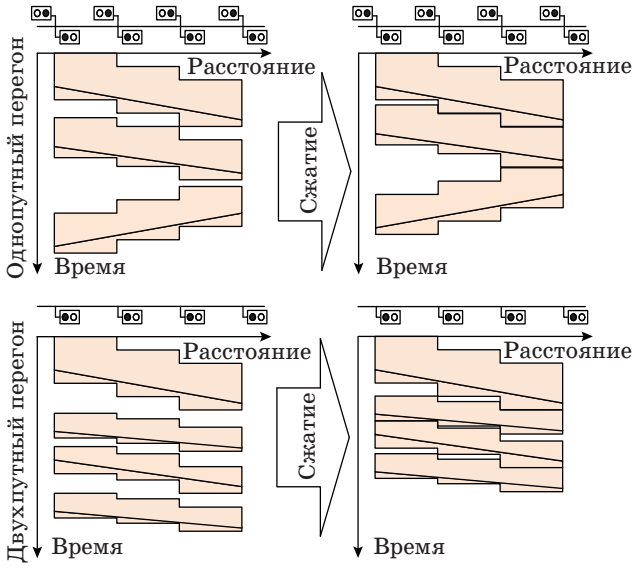
Здесь A — время занятости инфраструктуры поездами, мин; B — дополнительное время к межпоездному интервалу для снижения рисков распространения задержек, мин; C — межпакетный интервал (для однопутных перегонов), мин; D — продолжительность суточного бюджета времени, выделяемого для производства плановых ремонтно-строительных работ, мин.

Каас (Kaas) предложил [5] следующую формулу для расчета времени B из формулы (5) с учетом коэффициента использования ПС и межпоездного интервала:

$$K_{\max} = \Delta T/t_{h\,\min};$$

$$K_f = u \times K_{\max};$$

$$K_f = u \times \Delta T/t_h, \tag{6}$$



■ ***Рис. 3.*** Сжатие расписания методом UIC 406

где $K_{\max}$ — теоретическая ПС, число поездов; ΔT — рассматриваемый временной интервал, мин; $t_{h\,\min}$ — минимальный межпоездной интервал, мин/поезд; u — процент использования теоретической пропускной способности; K_f — практическая ПС, число поездов:

$$K_f = \Delta T/(t_{h\,\min} + t_b). \qquad (7)$$

Тогда из формул (6) и (7) можно выразить дополнительное время к межпоездному интервалу для снижения рисков распространения задержек t_b, мин/поезд:

$$K_f = u \times \Delta T/t_h = \Delta T/(t_{h\,\min} + t_b) \Rightarrow$$

$$\Rightarrow t_b = \Delta T/K_f - t_{h\,\min}.$$

Метод UIC 406 позволяет оценивать использование ПС для задач управления маршрутами поездов, но не для планирования развития инфраструктуры. Его возможности ограничены по следующим причинам:

— факторы стабильности и надежности движения, закладываемые в расписание, не принимаются во внимание, в то время как они в значительной степени влияют на используемую ПС. На станции тоже могут быть незапланированные операции, например перестыковка состава;

— все поезда считаются одинаковыми, хотя в действительности они имеют различные приоритеты;

— ПС больших станций не может быть найдена из-за отсутствия знаний о точных маршрутах поездов и операций на платформах [18];

— графики движения с различной комбинацией поездов, но приблизительно одинаковым использованием ПС не могут сравниваться друг с другом, так как ПС рассчитывается как невзвешенная сумма всех поездов;

— поскольку только короткие участки сети включены в анализ, то сетевые эффекты не учитываются.

Сравнение методов CUI и UIC 406

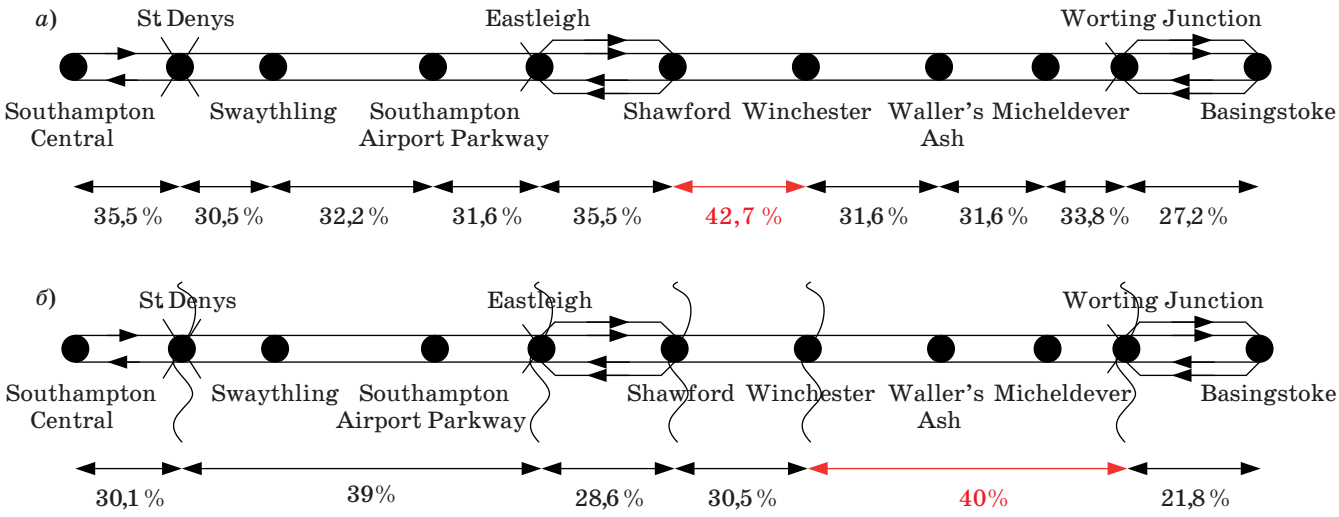
Эти два метода аналогичны в подходе, оба используют технику «сжатия расписания», но различаются по уровню детализации, на котором они применяются. Метод UIC 406 применяется на уровне блок-участков, а метод CUI — на более длинных участках сети и не рассматривает сжатие на отдельных блок-участках.

Сравнение методов CUI и UIC 406 было проведено в работе [19]. Эксперименты проводились на небольшом участке железной дороги на юге Великобритании между станциями Саутгемптон и Бейзингстоук. Сжатию подверглось расписание в утренний час-пик с 7:00 до 10:00. Результаты сжатия расписания представлены на рис. 4, *а* и *б*.

После сравнения результатов можно заметить, что средний индекс использования ПС методом CUI на 1,6 % больше, чем у метода UIC 406 (таблица). Это объясняется различным определением межпоездного интервала. Также при переходе с 4-колейной дороги на 2-колейную на станции Шоуфорд индекс использования ПС выше у метода CUI.

■ Сравнение результатов CUI и UIC 406

Метод	Значение индекса использования ПС, %	
	среднее	максимальное
CUI	33,2	42,7
UIC 406	31,6	40



■ ***Рис. 4.*** Сжатие расписания методом CUI (*а*) и UIC 406 (*б*)

Методы CUI и UIC 406 позволяют оценить использование ПС для управления поездами, но не для планирования развития инфраструктуры. Есть ряд существенных недостатков в методах:

— не учитываются стабильность и надежность расписания, в то время как они оказывают большое влияние на ПС;

— все поезда считаются одинаковыми, хотя они имеют различные скорость движения, приоритеты и другие характеристики;

— пропускная способность сложных станций не может быть оценена из-за отсутствия знаний о точных маршрутах поездов;

— используемая ПС вычисляется с помощью «невзвешенного» суммирования всех поездов. Это происходит из-за того, что не учитывается тип поездов;

— сетевые эффекты не рассматриваются, потому что в анализ включены только короткие участки сети.

Аналитические методы могут легко и быстро дать представление о ПС линий или сети, но не охватывают в совокупности все факторы, влияющие на ПС. Большее число факторов усложняет моделируемый процесс. Чем сложнее процесс, тем менее точной получается описывающая его теоретическая функция. Результат, получаемый аналитическими методами, приближенный и не показывает ПС, которую можно реализовать на практике.

В последние годы наметились следующие тенденции исследований и развития аналитических методов:

1) расширение области применения аналитических методов оценки ПС:

— для станций [18, 20];

— для железнодорожных полигонов [21];

— отдельно для грузового транспорта [22];

2) автоматизация аналитических методов:

— метод UIC 406 в новой версии RailSys [14];

— метод UIC 406 для огромных сетей [23];

— метод CUI [21];

3) развитие методологии UIC 406 — исследование характера изменения CUI при добавлении (удалении) поездов в расписание [19].

Заключение

В этой части работы рассмотрены распространенные аналитические методы анализа использования пропускной способности, применяемые в Европе, а именно методы CUI и UIC 406. Дана характеристика каждого из методов и общая оценка аналитических методов. Показано, что аналитические методы, описывающие железнодорожную инфраструктуру с помощью математических выражений, позволяют оценить пропускную способность участка лишь приблизительно. Приведены тенденции исследований и развития аналитических методов. Во второй части статьи будут обсуждаться методы, основанные на моделировании и оптимизации.

Литература

1. **Левин Д. Ю., Павлов В. Л.** Расчет и использование пропускной способности железных дорог: монография. — М.: ФГОУ «Учебно-методический центр по образованию на железнодорожном транспорте», 2011. — 364 с.
2. **Козлов И. Т.** Пропускная способность транспортных систем. — М.: Транспорт, 1985. — 214 с.
3. **Инструкция** по расчету наличной пропускной способности железных дорог /ОАО «РЖД». — М., 2010. — 305 с.
4. **Krueger H.** Parametric Modeling in Rail Capacity Planning //Proc. of 1999 Winter Simulation Conf., Piscataway, 1999. P. 1194—2000.
5. **Kaas A. H.** Methods to Calculate Capacity of Railways (Metoder Til Beregning af Jernbanekapacitet): PhD-thesis / Technical University of Denmark, 1998. — 182 p.
6. **UIC 2004**. Capacity (UIC Code 406)/ International Union of Railways (UIC). — Paris, 2004. — 56 p.
7. **Hansen I. A., Pachl J.** Railway Timetable and Traffic. — Hamburg: Eurailpress, 2008. — 332 p.
8. **Poole E. C.** Costs — A Tool for Railroad Management. — N. Y.: Simmons Boardman, 1962. — 175 p.
9. **Lai Y. C.** Increasing Railway Efficiency and Capacity Through Improved Operations, Control and Planning: PhD-thesis / University of Illinois at Urbana-Champaign, 2008. — 184 p.
10. **Lusby R., Larsen J., Ehrgott M., Ryan D.** Railway Track Allocation: Models and Methods //OR Spectrum. 2009. N 3. P. 843–883.
11. **Assad A. A.** Models for Rail Transportation// Transportation Research. Part A: General. 1980. Vol. 14. N 4. P. 205–220.
12. **Cordeau J. F., Toth P., Vigo D.** A Survey of Optimization Models for Train Routing and Scheduling// Transportation Science. 1998. Vol. 32. N 4. P. 380–420.
13. **Yuan J., Hansen I. A.** Optimizing Capacity Utilization of Stations by Estimating Knock-on Train Delays// Transportation Research. Part B: Methodological. 2007. Vol. 41. N 2. P. 202–217.
14. RMCON, 2009. RailSys Information Brochure [Online]. http://www.rmcon.de (дата обращения: 03.06.2014).
15. **Pachl J.** Railway Operation and Control, Mountlake Terrace (USA). — VTD Rail Publishing, 2009. — 275 p.
16. **Confessore G.** et al. A Simulation-Based Approach for Estimating the Commercial Capacity of Railways // Proc. of 2009 Winter Simulation Conf., Austin, Texas, USA, 2009. P. 2542–2552.

17. **Kontaxi E., Ricci S.** Techniques and Methodologies for Railway Capacity Analysis: Comparative Studies and Integration Perspectives// 3rd Intern. Seminar on Railway Operations Modelling and Analysis, RailZurich, 2009. P. 1051–1080.
18. **Landex A.** Station Capacity// 4th Intern. Seminar on Railway Operations Modelling and Analysis, Rome, Italy, 2011. P. 379–386.
19. **KhademSameni M., Landex A., Preston J.** Developing the UIC 406 Method for Capacity Analysis// 4th Intern. Seminar on Railway Operations Modelling and Analysis, Rome, Italy, 2011. P. 371–378.
20. **Lindner T.** Applicability of the Analytical Compression Method for Evaluating Node Capacity// 4th Intern. Seminar on Railway Operations Modelling and Analysis, Rome, Italy, 2011. P. 457–461.
21. **Armstrong J., Blainey S., Preston J.** Developing a CUI-Based Approach to Network Capacity Assessment// 4th Intern. Seminar on Railway Operations Modelling and Analysis, Rome, Italy, 2011. P. 57–63.
22. **Lindner T., Pachl J.** Recommendations for Enhancing UIC Code 406 Method to Evaluate Railroad Infrastructure Capacity// 89th Transportation Research Board Annual Meeting, Washington, USA, 2010. P. 120–127.
23. **Kuckelberg A., Wendler E., Groger T.** A UIC 406 Compliant, Practically Relevant Capacity-Consumption Evaluation Algorithm// 4th Intern. Seminar on Railway Operations Modelling and Analysis, Rome, Italy, 2011. P. 520–525.

UDC 656.22

Railway Capacity Estimation Methods. Part I. Analytical Methodsof Estimation and Capacity Utilization

Branishtov S. A.[a], PhD., Tech., Acting Head of Labs, pochta-na@mail.ru
Shirvanyan A. M.[a], Junior Researcher, Post-Graduate Student, artshirvanyan@mail.ru
Tumchenok D. A.[a], Junior Researcher, Post-Graduate Student, dmitriy_tumchenok@mail.ru
[a]V. A. Trapeznikov Institute of Control Sciences of RAS, 65, Profsoiuznaia St., 117342, Moscow, Russian Federation

Purpose: Capacity is an important characteristic of a railway track which determines its conveyance opportunities. Without taking it into account, you cannot plan freight transportation via a rail network. To get this characteristic, different countries use various analytical methods based on models including a set of parameters like the railway traffic interval, the average inter-packet gap, the coefficient of equipment reliability, etc. In this paper, we discuss the most popular methods of capacity evaluation. **Results:** In the first part of the work, we discuss various concepts of capacity term used in railway industry, describe and compare the methods of capacity usage analysis. In the second part, we discuss parametric methods, simulation methods and schedule optimization. **Practical relevance:** This work will interest rail service specialists: dispatchers, managers, engineers and others, as analytical methods applied to the calculation of the capacity itself or the portion of its actual usage can help them plan the rail traffic more efficiently.
Keywords Railway Capacity, Railroad, Schedule Compression.

References

1. Levin D. Ju., Pavlov V. L. *Raschet i ispol'zovanie propusknoi sposobnosti zheleznykh dorog* [Calculation and Using of Railway Capacity]. Moscow, FGOU «Uchebno-metodicheskii tsentr po obrazovaniiu na zheleznodorozhnom transporte» Publ., 2011. 364 p. (In Russian).
2. Kozlov I. T. *Propusknaia sposobnost' transportnyh sistem* [The Capacity of the Transport Systems]. Moscow, Transport Publ., 1985. 214 p. (In Russian).
3. *Instruktsiia po raschetu nalichnoi propusknoi sposobnosti zheleznykh dorog* [Instruction for Calculating the Capacity]. Moscow, OAO "RZhD" Publ., 2010. 305 p. (In Russian).
4. Krueger H. Parametric Modelling in Rail Capacity Planning. *Proc. of 1999 Winter Simulation Conf.*, Piscataway, 1999, pp. 1194–2000.
5. Kaas A. H. *Methods to Calculate Capacity of Railways* (*Metoder Til Beregning af Jernbanekapacitet*). PhD-thesis. Technical University of Denmark, 1998. 143 p.
6. *UIC 2004. Capacity* (*UIC Code 406*). Paris, France, International Union of Railways (UIC), 2004. 56 p.
7. Hansen I. A., Pachl J. *Railway Timetable and Traffic*. Hamburg, Eurailpress, 2008. 332 p.
8. Poole E. C. *Costs — A Tool for Railroad Management*. New York, Simmons Boardman, 1962. 175 p.
9. Lai Y. C. *Increasing Railway Efficiency and Capacity Through Improved Operations, Control and Planning*. PhD-thesis. University of Illinois at Urbana-Champaign, 2008. 184 p.
10. Lusby R., Larsen J., Ehrgott M., Ryan D. Railway Track Allocation: Models and Methods. *OR Spectrum*, 2009, no. 5, pp. 843–883.
11. Assad A. A. Models for Rail Transportation. *Transportation Research. Part A. General*, 1980, vol. 14, iss. 4, pp. 205–220.
12. Cordeau J. F., Toth P., Vigo D. A Survey of Optimization Models for Train Routing and Scheduling. *Transportation Science*, 1998, vol. 32, no. 4, pp. 380–420.
13. Yuan J., Hansen I. A. Optimizing Capacity Utilization of Stations by Estimating Knock-on Train Delays. *Transportation Research. Part B. Methodological*, 2007, vol. 41, no. 2, pp. 202–217.
14. *RMCON, 2009. RailSys Information Brochure* [*Online*]. Available at: http://www.rmcon.de (accessed 3 June 2014).
15. Pachl J. *Railway Operation and Control, Mountlake Terrace* (*USA*). VTD Rail Publishing, 2009. 275 p.
16. Confessore G., Cicini P., De Luca P., Liotta G., Rondinone F. A Simulation-Based Approach for Estimating the Commercial Capacity of Railways. *Proc. of 2009 Winter Simulation Conf.*, Austin, TX, USA, 2009, pp. 2542–2552.
17. Kontaxi E., Ricci S. Techniques and Methodologies for Railway Capacity Analysis: Comparative Studies and Integration Perspectives. *3rd Intern. Seminar on Railway Operations Modelling and Analysis*. RailZurich, 2009, pp. 1051–1080.
18. Landex A. Station capacity. *4th Intern. Seminar on Railway Operations Modelling and Analysis*. Rome, Italy, 2011, pp. 379–386.
19. KhademSameni M., Landex A., Preston J. Developing the UIC 406 Method for Capacity Analysis. *4th Intern. Seminar on Railway Operations Modelling and Analysis*. Rome, Italy, 2011, pp. 371–378.
20. Lindner T. Applicability of the Analytical Compression Method for Evaluating Node Capacity. *4th Intern. Seminar on Railway Operations Modelling and Analysis*. Rome, Italy, 2011, pp. 457–461.
21. Armstrong J., Blainey S., Preston J. Developing a CUI-based Approach to Network Capacity Assessment. *4th Intern. Seminar on Railway Operations Modelling and Analysis*. Rome, Italy, 2011, pp. 57–63.
22. Lindner T., Pachl J. Recommendations for Enhancing UIC Code 406 Method to Evaluate Railroad Infrastructure Capacity. *89th Transportation Research Board Annual Meeting*. Washington, USA, 2010, pp. 120–127.
23. Kuckelberg A., Wendler E., Groger T. A UIC 406 Compliant, Practically Relevant Capacity-Consumption Evaluation Algorithm. *4th Intern. Seminar on Railway Operations Modelling and Analysis*. Rome, Italy, 2011, pp. 520–525.

УДК 004.896

МОДЕЛЬ НАВИГАЦИИ РОБОТОТЕХНИЧЕСКОГО КОМПЛЕКСА В МНОГОКОМПОНЕНТНОЙ ИНФОРМАЦИОННОЙ СРЕДЕ

А. А. Кобяков[а], *заместитель генерального директора*
К. В. Лапшин[а], *начальник научно-исследовательской лаборатории*
Е. Л. Новикова[б], *ассистент*
Ю. А. Ямщиков[а], *инженер-программист*
[а]*ОАО «Концерн «Гранит-Электрон», Санкт-Петербург, РФ*
[б]*Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, РФ*

Постановка проблемы: *при проектировании современных морских робототехнических комплексов возникают различные проблемы: анализа информационных потребностей автономных агентов; исследования и моделирования информационных структур и процессов, связанных с поиском, получением, накоплением и обработкой информации искусственными когнитивными агентами; изучения методов формирования оценок, мнений и знаний искусственными когнитивными агентами на основе перерабатываемой ими информации. Для решения этих проблем авторами предлагается общая модель навигации робототехнического комплекса, основанная на агентно-ориентированной методологии, в которой рассматриваемые системы и их компоненты интерпретируются как когнитивные агенты.* ***Результаты:*** *исследованы основные особенности проектирования робототехнических комплексов с использованием агентно-ориентированного подхода, в том числе раскрыты особенности архитектуры и функционирования интелектуальных агентов. Описана особенность искусственных когнитивных агентов, которая отличает их от других интеллектуальных систем, — получение информации непосредственно от человека, от сенсорной сети и из своей базы знаний и данных. Разработана общая структура комбинированной навигации когнитивного агента, обеспечивающая его функционирование в двух разных режимах: «первичной» навигации, связанной с перемещением агента к цели на основе гранулярной информации; «уточненной» навигации, опирающейся на текущие числовые данные о среде, получаемые от сенсорной системы. Сформирована иерархическая двухконтурная система управления, где обычная схема классического управления дополняется подсистемой нечеткого управления.* ***Практическая значимость:*** *предложенная авторами навигационная модель, основанная на агентно-ориентированном подходе, может быть использована при проектировании морских робототехнических комплексов как гражданского, так и военного назначения, что позволит значительно уменьшить трудоемкость проектирования в целом.*

Ключевые слова *— робототехнические комплексы, когнитивные агенты, архитектура, информационное взаимодействие, диалоговое и рефлексивное управление, многокомпонентная внешняя среда, восприятие, поведение, навигация.*

Введение

Современные робототехнические комплексы нуждаются в разработке общих навигационных моделей для многокомпонентных информационных пространств, где системы и их компоненты рассматриваются как когнитивные агенты. Основная особенность таких агентов — информационное взаимодействие высокого уровня. В рассматриваемой многокомпонентной среде присутствуют как естественные, так и искусственные информационные агенты. Исходя из этого, мы отмечаем необходимость анализа потребностей когнитивных агентов при моделировании ситуаций взаимодействий (поиск, получение и обработка информации когнитивными агентами). Очень важным моментом при этом является возможность обрабатывать разноуровневые и слабоформализованные информационные потоки, а также формализовать взаимодействия когнитивных агентов. Последнее потребует применения специфических методов и алгоритмов. Отдельно стоит рассмотреть методы управления когнитивными агентами, исходя из специфики решаемых задач.

Основы проектирования когнитивных агентов

Уровень интеллектуальности робота оценивают по следующим параметрам [1]:

— сложность и динамичность внешней среды;

— восприятие роботом информации о внешней среде;

— гибкость планирующей и управляющей систем робота;

— степень автономности робота.

Главным признаком интеллектуальности служит наличие развитой модели внешней среды (динамической базы знаний), что позволяет роботу действовать в условиях неопределенности. Роботы должны быть способны:

— работать в открытых динамических мирах;

— строить сложные многоцелевые планы поведения, определяемые как оценкой внешней ситуации, так и внутренней мотивацией;

— вести диалог с другими агентами.

Физический интеллектуальный агент (робот) — это техническое устройство, способное самостоятельно и целенаправленно функционировать в реальной физической среде и адекватно

реагировать на происходящие в ней изменения [2]. В его состав входит интеллектуальная система управления. Помимо этого, интеллектуальный робот должен иметь внутреннюю модель внешней среды, развитую сенсорную систему, способность к распознаванию различных ситуаций [3].

Отличительной особенностью интеллектуального агента является способность эффективно работать в условиях неполной, противоречивой, неточной, нечеткой входной (рецепторной) информации. Подобные агенты требуются, в первую очередь, для функционирования в агрессивных и экстремальных средах.

Интеллектуальный робот может рассматриваться как когнитивная система, обладающая возможностью действовать после принятия решения. Общая структура интеллектуального робота соответствует следующей схеме: интеллектуальный робот = подсистема восприятия + интеллектуальная система + подсистема действия. В развитие этой позиции можно утверждать, что роботы нового поколения должны иметь статус когнитивного агента [4].

Характер среды накладывает существенные требования на модель (архитектуру) агента, обращение к теории деятельности представляется необходимым условием проектирования индивидуальных и совместных действий агентов, а выявление особенностей взаимодействия (влияния, кооперации, коммуникации) агентов позволяет разработать исходную структуру многоагентной системы [5].

Представление об агенте как искусственном организме, развивающемся в некоторой среде, предполагает формирование и использование в качестве одной из базовых моделей агента структуры «организм — среда». Модель простейшего агента представлена на рис. 1.

Рецепторы (сенсоры) образуют систему восприятия агента, обеспечивая при этом первичную обработку информации. В памяти агента должны храниться сведения о типовых реакциях на информационные сигналы от рецепторов (датчиков, устройств контроля), а также информация о состоянии эффекторов (исполнительных устройств) и о располагаемых ресурсах (других агентах, располагаемом времени и пр.). В памяти должны содержаться программы переработки входной информации в управляющие сигналы. Блок памяти должен включать внутреннюю модель внешнего мира, модель самого агента и систему фильтров, позволяющую выделять значимую для агента информацию.

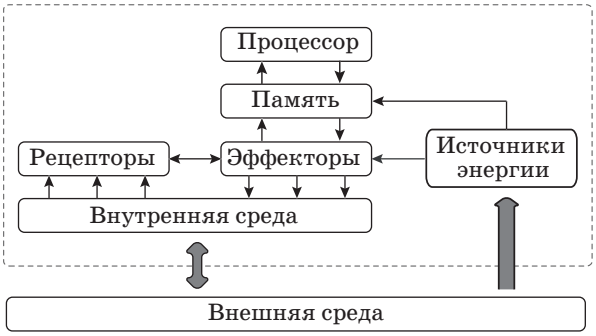
Процессор (система процессоров) обеспечивает объединение и переработку разнородных данных, выработку соответствующих решений о выполнении тех или иных действий. Выбор необходимых действий при заданных ограничениях — это ключевая способность любых агентов.

Функция эффекторов состоит в воздействии на среду, например, в захвате или перемещении объектов внешней среды.

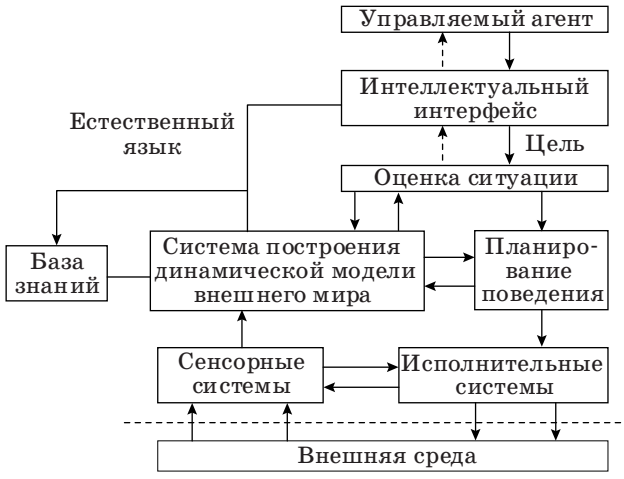
Общая структура искусственного интеллектуального агента, получающего целеуказания от управляющего агента, приведена на рис. 2. Архитектура физического агента, управляемого путем постановки целей, включает интеллектуальный интерфейс; систему оценки ситуации; модель внешнего мира; систему планирования поведения; информационно-сенсорную и исполнительную системы, обрабатывающие информацию в реальном масштабе времени. Модель внешнего мира строится на основе базы знаний и данных, получаемых от сенсорной системы.

Главная особенность искусственного когнитивного агента (ИКА), отличающая его от других интеллектуальных систем, заключается в том, что он получает и интегрирует информацию I из трех источников:

1) от человека-пользователя на ограниченном естественном языке в виде целеуказаний и инструкций I_U;



■ *Рис. 1.* Модель простейшего агента



■ *Рис. 2.* Архитектура искусственного интеллектуального агента

2) от датчиков сенсорной системы I_S;

3) из собственной базы знаний I_{kb}.

Неоднозначным (полиморфным) оказывается соответствие между множеством входных воздействий внешней среды и сенсорно-информационным множеством, а также между восприятием и представлением агента. Таким образом, основные функции агента можно описать с помощью отображений вида «один-ко-многим»:

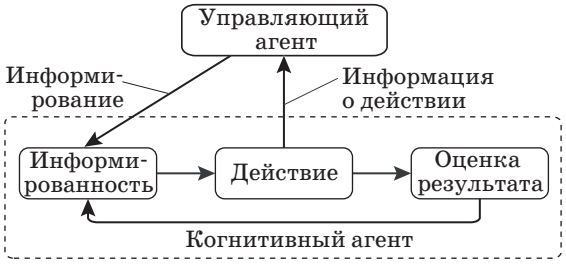
— функция восприятия имеет вид Per: $E \rightarrow A_i$, где E — внешняя среда, а A_i — множество значений атрибутов, соответствующих ее воспринимаемым компонентам (например, пространственным — «далеко», временным — «немного позже», динамическим — «движение с большой скоростью» и пр.);

— функция построения обобщенной оценки (решения) Dec: $A_i \rightarrow B_0$, где B_0 — оценка общего состояния агента («нормальное», «хорошее» и др.).

Следовательно, все большую важность приобретает проблема преобразования многоуровневой системы абстрактных пространств, используемых при описании поведения агента, с помощью семейств полиморфных отображений (т. е. отображений «один-ко-многим»).

Отличительными особенностями ИКА являются возможность общения с человеком на ограниченном естественном языке, интерпретация понятий и формирование модели внешней среды, распознавание и анализ ситуаций. Выделяются две функции общения — коммуникативно-регулятивная и коммуникативно-информационная [6]. Эти функции могут использоваться в контексте управления ИКА, когда его взаимодействие с человеком носит интерактивный характер, что приводит к сочетанию процессов самоуправления и внешнего управления. Так, достижение автономным мобильным роботом статуса когнитивного агента требует развития новых стратегий внешнего управления (со стороны человека). К их числу относятся понятия информационного, рефлексивного, адаптивного, диалогового управления.

Под информационным управлением (рис. 3) здесь понимается любое целенаправленное воздействие естественного агента (человека), связанное с информированием искусственного агента, которое побуждает последнего к совершению требуемых действий. Информирование может носить характер целеуказания, ограничения, создания общей информационной картины, уточнения ситуации или оценки действия. Управляющий агент передает сообщение, связанное с его потребностью, мобильному когнитивному агенту, который выбирает действие на основе своей информированности о существенных параметрах задачи. Совершив действие, ИКА наблюдает его результат и оценивает его, что, соответственно, меняет уровень информированности ИКА.



■ ***Рис. 3.*** Общая модель информационного управления

Таким образом, управляющее воздействие носит косвенный характер — оно запускает определенный алгоритм поведения физического когнитивного агента в плохо определенной среде [7].

Близкое понятие рефлексивного управления заключается в том, что управляющий агент вначале прогнозирует возможные действия управляемого агента в конкретной ситуации, сообщая ему затем определенную информацию, которая стимулирует желательный для управляющей системы выбор. Рефлексивное управление обладает рядом особенностей:

1) оно носит отражательный характер (у управляющего агента создается представление о возможной реакции управляемого агента);

2) в рефлексивном управлении велика роль формирования мотивации, определяющей цели управления;

3) рефлексивное управление пронизано неопределенностями.

Условия функционирования искусственного агента могут быть заранее неизвестными или меняться непредвиденным образом в процессе его работы. Для мобильного робота неизвестными могут быть объекты внешней среды и их отдельные параметры, характеристики грунта или характеристики информационно-измерительных датчиков, исполнительных приводов и механизмов.

Таким образом, возникает необходимость в построении адаптивных управляющих систем с элементами искусственного интеллекта, т. е. таких систем, которые способны обеспечивать целесообразное поведение агента в условиях неопределенности. Характерной чертой функционирования таких систем является то, что недостаток априорной информации компенсируется оперативной обработкой текущей информации, получаемой от сенсоров.

Диалоговое управление искусственным агентом представляет собой высшую форму интерактивного управления. Под диалогом понимается последовательность коммуникативных актов между человеком и ИКА, которые считаются способными меняться ролями («активный-пассив-

ный» участник или «говорящий-слушающий» в процессе общения). Любой диалог предполагает обмен сообщениями между агентами, связанный с изменением их задач и состояний (мнений, целей, обязательств и пр.). Диалог человека с искусственным агентом предполагает двустороннюю связь: с одной стороны, целеуказания и инструкции, передаваемые человеком агенту, с другой стороны — просьба от агента человеку уточнить исходные инструкции, сообщение сведений о текущей ситуации или информации о достижении поставленной цели.

Он может осуществляться разными способами, например, с использованием естественно-языковых средств (текстовых или голосовых). Общая модель диалогового управления представлена на рис. 4 [8].

Структура диалога может рассматриваться на трех уровнях: глобальном, тематическом и локальном. Глобальная структура определяется общими свойствами решаемых системой «человек — искусственный агент» задач. Тематическая структура диалога зависит от конкретных особенностей решаемой задачи, т. е. от алгоритма ее решения (распределения задач на подзадачи) и распределения ролей между человеком и ИКА [9–11].

На локальном уровне рассматриваются отдельные шаги диалога, образуемые взаимосвязанными высказываниями его участников. Здесь шаг диалога понимается как пара «действие-реакция», где высказывание активного участника соответствует действию, а пассивного — реакции.

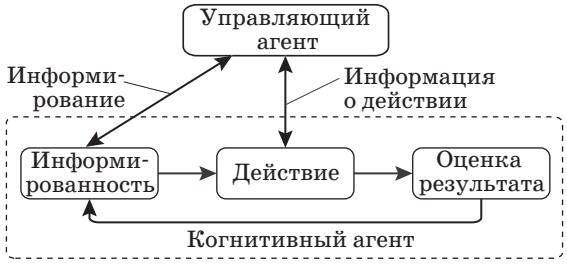
Основными параметрами структуры диалога на этом уровне являются инициатор шага и вид инициирования (вид действия), способ влияния действия на реакцию, способ спецификации задачи, решаемой на данном шаге. В то же время структура диалога может быть жесткой, альтернативной, гибкой (с перехватом инициативы), свободной.

Принцип диалогового управления лежит в основе построения гибкой системы навигации, способной функционировать в разных режимах (рис. 5):

1) «первичная» навигация связана с обеспечением перемещения физического когнитивного агента (ФКА) к цели на базе указаний и инструкций, задаваемых человеком на ограниченном естественном языке;

2) «уточненная» навигация опирается на текущие данные о среде, получаемые от сенсорной системы.

В результате формируется иерархическая двухконтурная система управления, где обычная схема классического управления дополняется подсистемой нечеткого управления. Этот подход предполагает переходы от точной информации к гранулярной и наоборот.



■ ***Рис. 4.*** Общая модель диалогового управления

■ ***Рис. 5.*** Иерархическая схема информационного взаимодействия когнитивного агента со средой

Заключение

В статье предложены основы единого агентно-ориентированного подхода к построению модели навигации робототехнических комплексов, согласно которому системы и все их компоненты рассматриваются как естественные и искусственные агенты, взаимодействующие между собой. Сделан обзор основных свойств, интерпретаций и типов искусственных агентов, раскрыты особенности архитектуры и функционирования интеллектуальных агентов.

Рассмотрена концепция когнитивных агентов, получающих информацию из трех источников: в процессе диалога от человека, из собственной базы знаний (данных) и от сенсорной системы.

Предложенная навигационная модель когнитивного агента обеспечивает его работу в двух разных режимах: «первичной» навигации, связанной с движением агента к цели, и «уточненной» навигации, основанной на текущих данных о среде (от сенсорной системы). В основе режима «первичной» навигации лежит организация информационного (диалогового) взаимодействия между человеком и искусственным агентом.

Литература

1. **Павловский В. Е.** Задачи динамики и управления мобильными роботами // Искусственный интеллект — проблемы и перспективы. Политехнические чтения. М.: Политехнический музей; РАИИ. 2006. Вып. 7. С. 155–174.
2. **Скобелев П. О.** Виртуальные миры и интеллектуальные агенты для моделирования деятельности компаний // Сб. науч. тр. 6-й Национальной конф. по искусственному интеллекту, Пущино, 5–11 октября 1998 г. / РАИИ. Пущино, 1998. Т. 2. С. 714–719.
3. **Платонов А. К.** Проблемы и перспективы робототехники // Робототехника, прогноз, программирование. — М.: ЛКИ, 2008. С. 9–36.
4. **Кузнецов О. П.** Когнитивное моделирование слабоструктурированных ситуаций // Искусственный интеллект — проблемы и перспективы. Политехнические чтения. М.: Политехнический музей; РАИИ. 2006. Вып. 7. С. 86–100.
5. **Каляев И. А., Гайдук А. Р., Капустян С. Г.** Модели и алгоритмы коллективного управления в группах роботов. — М.: Физматлит, 2009. — 280 с.
6. **Попов Э. В.** Общение с ЭВМ на естественном языке. 2-е изд. — М.: Едиториал УРСС, 2004. — 360 с.
7. **Мартыненко Ю. Г.** Проблемы управления и динамики мобильных роботов // Новости искусственного интеллекта. 2002. № 4. С. 18–23.
8. **Васильевский А. С., Коржавин Г. А., Лапшин К. В., Никольцев В. А.** Технология многоагентных систем в задаче проектирования комплекса имитационного моделирования //Менеджмент качества. Информационные технологии. 2007. № 5. С. 12–17.
9. **Рыбина Г. В., Паронджанов С. С.** Моделирование процессов взаимодействия интеллектуальных агентов в многоагентных системах // Искусственный интеллект и принятие решений. 2008. № 3. С. 3–15.
10. **Тимофеев А. В.** Многоагентное и интеллектуальное управление сложными робототехническими системами // Теоретические основы и прикладные задачи интеллектуальных информационных технологий: сб. статей/ СПИИРАН, 1998. С. 71–81.
11. **Ющенко А. С.** Диалоговое управление роботами с использованием нечетких моделей // Интегрированные модели и мягкие вычисления в искусственном интеллекте: сб. тр. 5-й Междунар. науч.-практ. конф., Коломна, 28–30 мая 2009 г. М.: Физматлит, 2009. Т. 1. С. 97–108.

UDC 004.896

Robotic Complex Navigation Model in Multicomponent Information Environment

Kobyakov A. A.[a], Deputy General Director, cri-granit@peterlink.ru
Lapshin K. V.[a], Chief of Scientific Research Laboratory, kir_i_k@mail.ru
Novikova E. L.[b], Assistant Professor, kir_i_k@mail.ru
Yamshchikov Y. A.[a], Programmer Engineer, gcabman@yandex.ru
[a]FSPC JSC «Concern «Granit-Electron», 3, Gospitalnaia St., 191014, Saint-Petersburg, Russian Federation
[b]Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St., 190000, Saint-Petersburg, Russian Federation

Purpose: In the design of modern marine robotic complexes, various problems arise: analyzing the informational needs of autonomous agents; studying and modeling the information structures and processes associated with the search, acquisition, accumulation and processing of the information by artificial cognitive agents; the development of estimates, opinions and knowledge by artificial cognitive agents on the basis of the information they process. To solve these problems, the authors propose a general model of a navigational robotic complex based on agent-oriented methodology where the systems and their components are interpreted as cognitive agents. **Results:** The main features of developing robotic complexes using agent-oriented approach were studied, including the architectural features and intelligent agent functioning. A feature of artificial cognitive agents was described which distinguishes them from other intelligent systems – getting information from three sources: directly from a human, from a sensory system and from its own database/ knowledge base. A general scheme was developed of a combined navigation for a cognitive agent, which provides its functioning in two different modes: "rough" navigation associated with the movement of the agent to the target on the base of the granular information, and "accurate" navigation based on the current numerical data about the environment obtained from the sensor system. A hierarchical dual control system was formed where the classical control scheme is complemented by a fuzzy control subsystem. **Practical relevance:** The proposed navigation model based on the agent-oriented approach can be used in the design of marine robotic complexes for both civilian and military purposes, which will greatly reduce the complexity of the design as a whole.

Keywords — Robotic Complexes, Cognitive Agents, Architecture, Information Interaction, Dialog and Reflexive Control, Multicomponent External Environment, Perception, Behavior, Navigation.

References

1. Pavlovskii V. E. Problems of Dynamics and Control of Mobile Robots. *Iskusstvennyi intellekt — problemy i perspektivy. Politekhnicheskie chteniia*. Polytechnical Museum; RAAI Publ., 2006, vol. 7, pp. 155–174 (In Russian).
2. Skobelev P. O. Virtual Worlds and Intelligent Agents for the Simulation of the Companies. *Sbornik nauchnykh trudov 6 Natsional'noi konferentsii po iskusstvennomu intellektu* [Proc. 6th Nat. Conf.]. Pushino, RAAI Publ., 1998, vol. 2, pp. 714–719 (In Russian).
3. Platonov A. K. Problems and Prospects of Robotics. *Robototekhnika, prognoz, programmirovanie* [Robotics, forecast, programming]. Moscow, LKI Publ., 2008, pp. 9–36 (In Russian).

4. Kuznetsov O. P. Cognitive Modeling Semistructured Situations. *Iskusstvennyi intellekt — problemy i perspektivy. Politekhnicheskie chteniia*. Polytechnical Museum; RAAI Publ., 2006, vol. 7, pp. 86–100 (In Russian).
5. Kalyaev I. A., Gaiduk A. P., Kapustian S. G. *Modeli i algoritmy kollektivnogo upravleniia v gruppakh robotov* [Models and Algorithms of Collective Management in Groups of Robots]. Moscow, Fizmatlit Publ., 2009. 280 p. (In Russian).
6. Popov E. V. *Obshchenie s EVM na estestvennom iazyke* [Communication with the Computer in Natural Language]. Moscow, Editorial URSS Publ., 2004. 360 p. (In Russian).
7. Martynenko Y. G. Problems of Control and Dynamics of Mobile Robots. *Novosti iskusstvennogo intellekta*, 2002, vol. 4, pp. 18–23 (In Russian).
8. Vasilievskii A. S., Korzhavin G. A., Lapshin K. V., Nikoltsev V. A. Multiagent Systems Technology in the Problem of Designing Complex Simulation. *Menedzhment kachestva. Informatsionnye tekhnologii*, 2007, no. 5, pp. 12–17 (In Russian).
9. Rybina G. V., Parondzhanov S. S. Simulation of Interaction of Intelligent Agents in Multi-agent Systems. *Iskusstvennyi intellekt i priniatie reshenii*, 2008, vol. 3, pp. 3–15 (In Russian).
10. Timofeev A. V. Multi-agent and Intelligent Control of Difficult Robotic Complexes. *Teoreticheskie osnovy i prikladnye zadachi intellektual'nykh informatsionnykh tekhnologii* [Theoretical Bases and Applied Problems of Intelligent Information Technologies]. SPIIRAN Publ., 1998, pp. 71–81 (In Russian).
11. Iushchenko A. S. Dialog Control Robots Using Fuzzy Models. *Sbornik trudov 5-i Mezhdunarodnoi nauchno-prakticheskoi konferentsii "Integrirovannye modeli i miagkie vychisleniia v iskusstvennom intellekte"* [Proc. 5th Int. Conf. "Integrated Models and Soft Computing in Artificial Intelligence"]. Moscow, Fizmatlit Publ., 2009, vol. 1, pp. 97–108 (In Russian).

УДК 681.324

ПРИНЦИПЫ ПОСТРОЕНИЯ ВЫЧИСЛИТЕЛЬНЫХ КОМПОНЕНТОВ СИСТЕМ ИНТЕГРИРОВАННОЙ МОДУЛЬНОЙ АВИОНИКИ

А. В. Шукалов[а, б], *доцент, генеральный директор*
П. П. Парамонов[а, б], *доктор техн. наук, профессор, советник генерального директора*
Е. В. Книга[а, б], *аспирант, старший инженер*
И. О. Жаринов[а, б], *доктор техн. наук, заведующий кафедрой, руководитель учебно-научного центра*
[а]*Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, Санкт-Петербург, РФ*
[б]*ФГУП «Санкт-Петербургское ОКБ «Электроавтоматика» им. П. А. Ефимова», Санкт-Петербург, РФ*

Постановка проблемы: *развитие современного авиационного приборостроения связано с внедрением на борт летательных аппаратов вычислительных систем класса интегрированной модульной авионики. Для создания таких систем требуются специальные проектные решения, обладающие повышенными показателями унификации и стандартизации. Цель исследования заключается в разработке структур модулей вычислительных систем интегрированной модульной авионики.* ***Методы:*** *внутренние структуры вычислительных компонентов получены с использованием методов инженерного синтеза, методов и систем автоматизации проектирования, методов теории выбора и методов автоматизированной генерации проектных решений.* ***Результаты:*** *основными результатами работы являются внутренние структуры модулей: вычислительного, графического, коммутатора, ввода-вывода, массовой памяти. Структуры получены путем преобразования модификации унифицированного вычислительного компонента — базового модуля. Базовый модуль включает узлы поддержки модуля, межмодульного интерфейса, функций модуля, контроля и диагностики, внешних интерфейсов, связи с мезонинами, интеллектуальный узел электропитания. Структура вычислителя совпадает со структурой базового модуля. Структура модуля ввода-вывода основана на структуре базового модуля и дополнена платами-мезонинами, обеспечивающими аппаратно-программную поддержку функций ввода-вывода данных по специализированным бортовым интерфейсам. Структура модуля графического основана на структуре базового модуля с дополнением узла функций модуля узлом специализированного графического контроллера, поддерживающего функцию передачи видеоизображения по интерфейсу Fibre Channel. Структура модуля-коммутатора основана на структуре базового модуля с расширением узла функций модуля и включением в него специализированных элементов: приемников и передатчиков оптического сигнала Fibre Channel и контроллера интерфейса Fibre Channel. Структура модуля массовой памяти основана на структуре базового модуля и дополнена специализированными платами-мезонинами для расширения объема постоянной памяти модуля.* ***Практическая значимость:*** *результаты получены при выполнении научно-исследовательской и опытно-конструкторской работы по созданию перспективных образцов вычислительной техники в классе аппаратуры интегрированной модульной авионики. Результаты доведены до промышленных образцов, находящихся в настоящее время на этапе испытаний.*

Ключевые слова *— интегрированная модульная авионика, вычислительные системы, модули, внутренняя структура.*

Введение

Бортовые цифровые вычислительные системы (БЦВС) перспективного летательного аппарата (ЛА) представляют собой многопроцессорные многомодульные реконфигурируемые структуры, выполненные в классе аппаратуры интегрированной модульной авионики (ИМА) и построенные на базе унифицированных быстросменных конструктивно-функциональных модулей (КФМ) [1–5].

Номенклатура КФМ ИМА представлена пятью функциональными вычислительными компонентами, классифицируемыми в соответствии со своим назначением на модуль вычислительный (МВ), модуль графический (МГ), модуль ввода-вывода (МВВ), модуль-коммутатор (МК), модуль массовой памяти (ММП). Модуль напряжений (МН) не использует вычислительные ресурсы, но также присутствует в составе БЦВС.

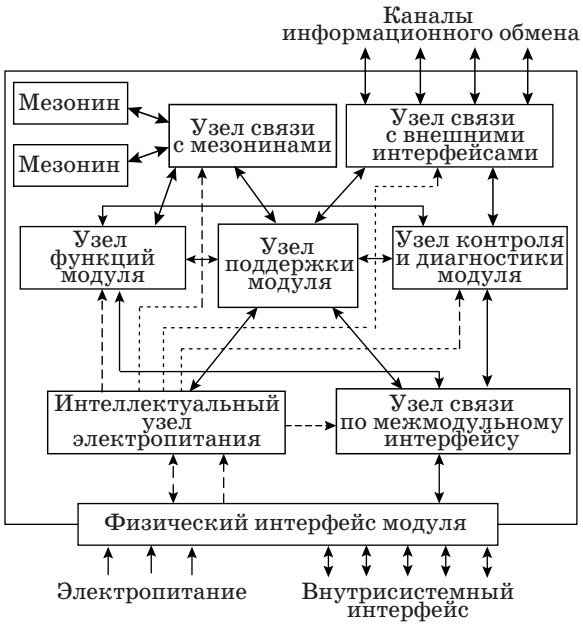
Как показано в работе [6], принцип построения всех КФМ основывается на базовой структуре одного вычислительного компонента, которая включает:

— узел поддержки модуля (УПМ);
— интеллектуальный узел электропитания (ИУЭП);
— узел межмодульного интерфейса (УМИ);
— узел функций модуля (УФМ);
— узел контроля и диагностики (УКД);
— узел внешних интерфейсов (УВИ);
— узел связи с мезонинами (УСМ).

В зависимости от назначения КФМ в его внутренней структуре присутствуют дополнительные функциональные элементы. Таким образом, внутренняя структура МВ, МГ, МВВ, МК или ММП может быть получена путем преобразования структуры одного базового модуля ИМА. Цель настоящей статьи заключается в изложении принципов построения вычислительных компонентов, применяемых в перспективных системах ИМА и обладающих высокими значениями показателей унификации и стандартизации проектных решений.

Внутренняя структура базового вычислительного компонента ИМА

Функциональная схема базового КФМ для БЦВС ИМА представлена на рис. 1.



■ ***Рис. 1.*** Функциональная схема базового КФМ ИМА

Узел поддержки модуля синхронизирует работу всех узлов КФМ, управляет инициализацией КФМ, управляет встроенным аппаратно-программным контролем модуля, а также осуществляет:

— управление электропитанием модуля (формирует сигналы управления электропитанием — «авария сети электропитания», «отключить электропитание модуля»);

— контроль качества электропитания модуля (сохраняет контекстные параметры внешнего электропитания);

— инициализацию и идентификацию модуля в составе БЦВС (сохраняет и формирует контекстную информацию о КФМ: индивидуальную информацию завода-изготовителя, тип модуля, номер производственной партии, основные технические характеристики модуля и т. д.);

— контроль и регистрацию исправности модуля (формирует результаты тестирования и другую сервисную информацию, определяющую текущее состояние модуля);

— управление загрузкой программного обеспечения модуля;

— ведение журнала состояния модуля (сохраняет параметры состояния модуля, характеризующие его долговременные свойства либо нарушение работоспособности (количество рабочих часов, выполненные работы по техническому обслуживанию, отказы модуля и др.) в специальной энергонезависимой памяти).

Интеллектуальный узел электропитания обеспечивает преобразование первичных напряжений электропитания модуля во вторичные напряжения, которые необходимы для работы узлов модуля; коммутацию напряжений питания на внутренние узлы модуля; защиту системы энергоснабжения БЦВС от короткого замыкания по первичным и вторичным сетям электропитания; выдачу в УПМ информации о параметрах внешнего электропитания.

Узел межмодульного интерфейса обеспечивает сопряжение УФМ с межмодульным интерфейсом БЦВС.

Узел функций модуля предназначен для реализации функционального назначения модуля, которое различается в зависимости от типа КФМ (обработка данных, обработка сигналов от датчиков пилотажно-навигационного комплекса, обработка и формирование изображений в графическом и совмещенном «графика и метеоданные», «графика и геоинформационные данные» режимах и т. д.).

Узел контроля и диагностики обеспечивает контроль и автоматическую диагностику всех внутренних узлов модуля.

Узел внешних интерфейсов обеспечивает обмен информацией КФМ по внешним интерфейсам (разовые команды и последовательные каналы связи, мультиплексные каналы информационного обмена, оптические каналы связи) с УФМ и в обратном направлении.

Узел связи с мезонинами обеспечивает обмен информацией УФМ с различными мезонинными компонентами (платами), устанавливаемыми на КФМ для расширения функциональных возможностей модуля и построения новых конфигураций (увеличение числа каналов обмена, введение сопроцессора поддержки вычислений и др.). Так, например, на основе МВ можно сконфигурировать ММП, добавив мезонинные платы с большим объемом памяти, или сконфигурировать МВВ, установив платы-мезонины, реализующие дополнительное число входных-выходных интерфейсов БЦВС.

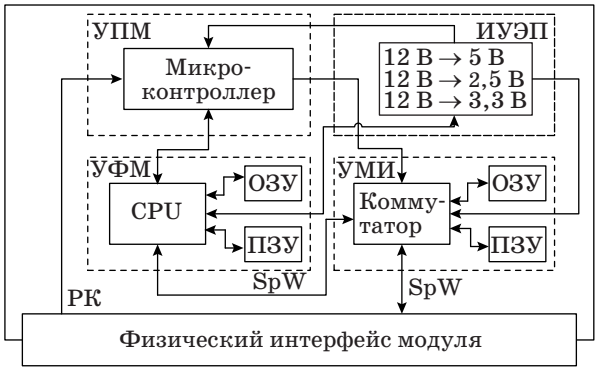
Физический интерфейс КФМ обеспечивает подключение оптических и электрических сигналов модуля в составе единой БЦВС.

Внутренняя структура вычислительных компонентов ИМА

Модуль вычислительный (рис. 2) предназначен для расчета общих и специальных алгоритмов управления движением ЛА, выполнения математических расчетов в реальном масштабе времени, диагностики бортового оборудования и т. д. средствами центрального процессора (*CPU* — Central Processor Unit).

Модуль вычислительный в составе БЦВС обеспечивает:

— прием от ММП по внутренней локальной сети SpaceWire *SpW* специализированного программного обеспечения, занесение полученных



■ ***Рис. 2.*** Функциональная схема МВ

данных в резидентное оперативное запоминающее устройство (ОЗУ) и их исполнение на встроенном вычислительном узле;

— информационный обмен данными по бортовой сети ЛА с другими абонентами комплекса авионики;

— предоставление функциональному программному обеспечению (ФПО) программных, аппаратных и временных ресурсов для возможности обработки полученной информации;

— выдачу подготовленной ФПО информации в бортовую информационную сеть ЛА.

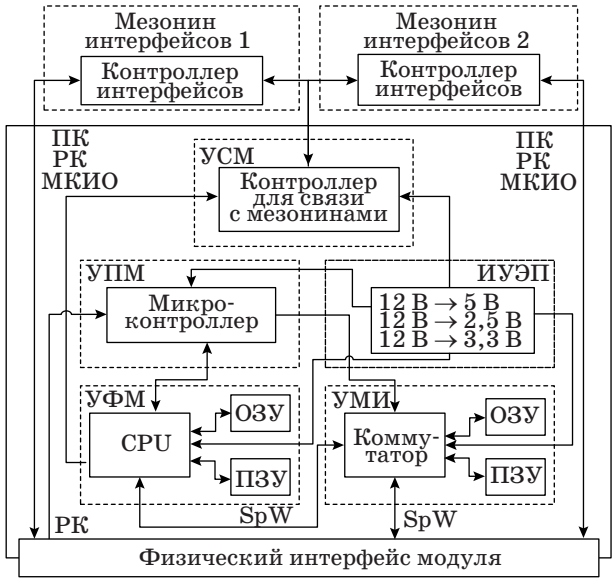
Принцип работы МВ заключается в следующем: при подаче электропитания модуль осуществляет инициализацию входящих в его состав компонентов (микросхем программируемой логики, микроконтроллера, микропроцессора и др.). После инициализации МВ принимает из постоянного запоминающего устройства (ПЗУ) ММП функциональное программное обеспечение БЦВС по внутренней локальной сети SpaceWire [7] и заносит его в свое внутреннее ОЗУ. Дальнейшая работа МВ в составе БЦВС определяется алгоритмом ФПО, заданным разработчиком БЦВС. Дополнительно в модуле реализована функция внешнего управления режимами работы модуля сигналом разовой команды *РК*.

Модуль ввода-вывода (рис. 3) предназначен для организации взаимодействия абонентов на борту ЛА друг с другом по мультиплексным каналам информационного обмена *МКИО* по ГОСТ Р 52070-2003 (аналог стандарта MIL-1553B), по последовательным каналам *ПК* связи и по *РК* по ГОСТ 18977-79 (аналог стандарта ARINC-429).

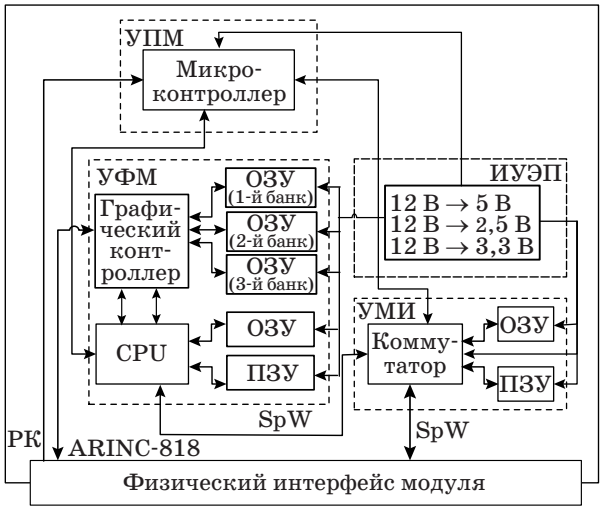
Внутренняя структура МВВ основана на структуре базового вычислительного КФМ и дополнена платами-мезонинами, обеспечивающими аппаратно-программную поддержку функций ввода-вывода данных по специализированным бортовым интерфейсам.

Принцип работы МВВ в составе БЦВС описывается следующим образом: при включении напряжения электропитания начинается процесс инициализации модуля, включающий предустановку и запуск микроконтроллера, микропроцессора, коммутатора. Затем из ММП загружается ФПО в ОЗУ МВВ по внутренней локальной сети SpaceWire. Дальнейшая работа модуля в составе БЦВС определяется алгоритмом ФПО, предусмотренным разработчиком. В процессе функционирования БЦВС МВВ получает результаты расчетов по локальной сети SpaceWire и передает их в УСМ для выдачи по требуемому бортовому интерфейсу абонентам через платы-мезонины, на которых реализованы программно управляемые контроллеры бортовых интерфейсов.

Модуль графический (рис. 4) предназначен для организации приема, обработки внешней видео-



■ ***Рис. 3.*** Функциональная схема МВВ



■ ***Рис. 4.*** Функциональная схема МГ

информации и формирования выходного видеосигнала на бортовые средства индикации информационно-управляющего поля кабины пилота ЛА.

Модуль графический в составе БЦВС обеспечивает:

— выполнение математических операций (преимущественно в полярной системе координат);

— выполнение специализированных преобразований данных для поддержки функций OpenGL (Open Graphic Library);

— прием и передачу видеоданных по цифровому оптическому интерфейсу на основе технологии Fibre Channel (стандарт ARINC-818);

— прием и передачу данных по внутреннему межмодульному интерфейсу БЦВС по сети SpaceWire.

Внутренняя структура МГ основана на структуре базового вычислительного модуля и на структуре базового модуля с дополнением УФМ узлом специализированного графического контроллера, поддерживающего функцию передачи видеоизображения по интерфейсу Fibre Channel.

Принцип работы МГ в составе БЦВС заключается в следующем. При подаче напряжения электропитания МГ проводит инициализацию внутренних узлов модуля. Затем по локальной сети SpaceWire модуль получает от ММП и заносит в свое ОЗУ ФПО, алгоритмом которого определяется дальнейшая работа модуля в составе БЦВС. В частности, для нашлемной системы целеуказания и индикации [8] МГ получает видеоизображение с камеры обзора закабинного пространства и пилотажно-навигационную информацию для построения графического изображения, два изображения совмещаются в МГ с учетом заданного угла поворота ЛА. Для бортовой цифровой картографической системы [9, 10] МГ формирует видеоизображение геоинформационных данных в совмещенном с пилотажно-навигационной или метеорологической информацией режиме.

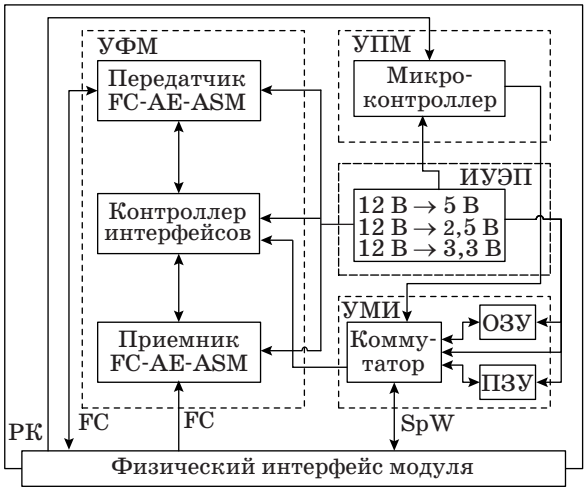
Синтезированное в МГ изображение передается по цифровому каналу обмена Fibre Channel на средства индикации бортовой системы отображения, входящей в состав информационно-управляющего поля кабины пилота ЛА.

Модуль-коммутатор (рис. 5) предназначен для согласования разнородных видов интерфейсов бортового оборудования авионики и интерфейсов БЦВС. МК в составе БЦВС обеспечивает:

— преобразование электрического сигнала в оптический сигнал и оптического сигнала в электрический сигнал интерфейса Fibre Channel *FC*;

— выполнение функции оптико-электронного согласования интерфейсов SpaceWire и Fibre Channel (спецификация *FC-AE-ASM*);

— выполнение функции электрического согласования интерфейса SpaceWire и МКИО по ГОСТ Р 52070-2003;



■ ***Рис. 5.*** Функциональная схема МК

— выполнение функции коммутации электрических сигналов бортовой сети ЛА на основе интерфейса SpaceWire с сигналами внутренней локальной сети БЦВС на основе SpaceWire.

Внутренняя структура МК основана на расширении УФМ базового вычислительного КФМ добавлением в него специализированных элементов: приемников и передатчиков оптического сигнала Fibre Channel и контроллера интерфейса Fibre Channel. Принцип работы МК в составе БЦВС состоит в следующем. При включении напряжения электропитания происходит инициализация всех узлов модуля. Затем по локальной сети SpaceWire МК получает ФПО от модуля ММП и заносит его в свое ОЗУ. Дальнейшая работа модуля в составе БЦВС определяется алгоритмом ФПО, предусмотренным разработчиком.

Модуль массовой памяти (рис. 6) выполняет роль арбитра в БЦВС. Модуль обеспечивает прием информации по сети информационного обмена ЛА; хранение в энергонезависимой памяти данных ФПО для каждого КФМ, входящего в состав БЦВС; выдачу данных по запросам по внутренней локальной сети БЦВС в любой КФМ.

Модуль массовой памяти в составе БЦВС обеспечивает:

— прием информации по информационной сети обмена данными ЛА;

— хранение в энергонезависимой памяти данных (ФПО, компонентов конфигурирования радиоэлементов программируемых логических интегральных схем КФМ и т. п.);

— загрузку в резидентное ОЗУ данных ФПО и инициализацию их исполнения;

— выдачу хранимых данных по локальной сети в соответствующие КФМ;

— выдачу сформированной средствами ФПО информации по сети информационного обмена абонентам бортового оборудования авионики.

■ ***Рис. 6***. Функциональная схема ММП

Внутренняя структура ММП основана на структуре базового вычислительного модуля и дополнена специализированными платами-мезонинами для расширения объема постоянной памяти модуля, предназначенной для хранения ФПО.

Работа ММП в составе БЦВС происходит по следующему принципу. При включении напряжения электропитания ММП инициализирует входящие в его состав компоненты. Затем ММП по внутренней локальной сети SpaceWire передает в ОЗУ всех КФМ компоненты ФПО. Далее ММП осуществляет проверку модулей, анализ данных встроенного тестового контроля и при выявлении отказа и наличии имеющихся в системе аппаратных и программных ресурсов производит реконфигурацию БЦВС, перераспределяя ФПО между исправными КФМ. Алгоритм теста проверки БЦВС подробно описан в работе [11].

Вычислительные структуры ИМА на основе номенклатуры КФМ

Предлагаемые структуры КФМ предназначены для создания реконфигурируемых БЦВС, выполненных в соответствии с рекомендациями группы стандартов ARINC-651–ARINC-655, распространяющихся на бортовую аппаратуру класса ИМА. Показано, что различные по функциональному назначению КФМ могут быть построены на основе внутренней структуры базового вычислительного модуля путем добавления новых специализированных узлов и расширения узла функций модуля. В табл. 1 приведено распределение узлов базового модуля по вычислительным компонентам КФМ, полученное путем автоматизированной генерации проектных решений по методикам [12–19] в отраслевой системе автоматизированного проектирования авиационного приборостроения.

Анализ данных табл. 1 показывает, что предлагаемая номенклатура КФМ является достаточной для создания семейства бортовых вычислителей, покрывающих потребности авиационной промышленности в создании первоочередных образцов бортового приборного оборудования.

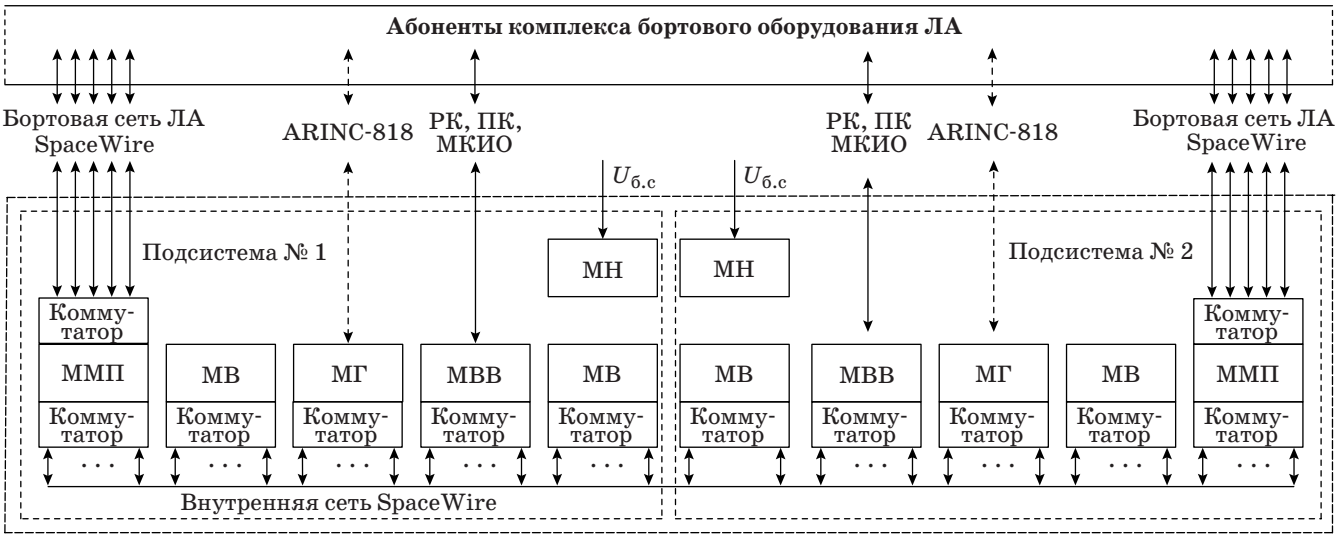
В табл. 2 представлен помодульный состав БЦВС, бортовой системы картографической информации (БСКИ), бортовой графической станции (БГС), бортовой интерфейсной станции (БИС), выполненных с применением технологии ИМА

■ ***Таблица 1***. Распределение унифицированных узлов по КФМ

КФМ	УФМ			УПМ	УМИ	УСМ	Мезонин	
	CPU	Графика	Интерфейсы				Память	Интерфейс
МВ	+	–	–	+	+	–	–	–
ММП	+	–	–	+	+	+	+	–
МГ	–	+	–	+	+	–	–	–
МВВ	–	–	+	+	+	–	–	+
МК	–	–	+	+	+	–	–	–

■ ***Таблица 2***. Помодульный состав бортовых вычислителей класса ИМА различного назначения

Наименование изделия авионики	МВ	ММП	МН	МВВ	МГ	МК
БЦВС	+	+	+	–	–	–
БСКИ	+	+	+	+	+	–
БГС	+	+	+	–	+	+
БИС	+	+	+	+	–	–



■ ***Рис. 7.*** Функциональная схема БСКИ ($U_{б.с}$ — напряжение бортовой электрической сети питания)

на базе МВ, МВВ, МГ, ММП, МК, МН. Пример внутренней структуры БСКИ приведен на рис. 7. Система БСКИ построена по двухконтурной схеме. Составы контуров идентичны. В составе ЛА каждый контур может использоваться как независимый вычислитель или как резервирующий вычислитель второго контура.

Заключение

В результате проектирования были получены внутренние структуры КФМ для реконфигурируемой БЦВС, выполненной в соответствии с рекомендациями группы стандартов ARINC-651–ARINC-655, распространяющихся на бортовую аппаратуру класса ИМА. Показано, что различные по функциональному назначению КФМ могут быть построены на основе внутренней структуры одного базового вычислительного модуля путем добавления новых специализированных узлов и расширения узла функций модуля.

Анализ данных табл. 1 и 2 показывает, что предлагаемые конструктивные и схемотехнические решения обладают показателями стандартизации и унификации проектных решений не ниже 70 %, что является достаточным для разработки базовой номенклатуры КФМ и перспективных вычислителей класса ИМА с поддержкой жизненного цикла «проектирование-производство-эксплуатация» авиационной аппаратуры [20].

Литература

1. **Гатчин Ю. А., Жаринов И. О.** Основы проектирования вычислительных систем интегрированной модульной авионики. — М.: Машиностроение, 2010. — 224 с.
2. **Парамонов П. П., Жаринов И. О.** Интегрированные бортовые вычислительные системы: обзор современного состояния и анализ перспектив развития в авиационном приборостроении // Научно-технический вестник информационных технологий, механики и оптики. 2013. № 2. С. 1–17.
3. **Жаринов О. О., Видин Б. В., Шек-Иовсепянц Р. А.** Принципы построения крейта бортовой многопроцессорной вычислительной системы для авионики пятого поколения // Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики. 2010. № 4. С. 21–27.
4. **Книга Е. В., Жаринов И. О., Богданов А. В., Виноградов П. С.** Принципы организации архитектуры перспективных бортовых цифровых вычислительных систем в авионике // Научно-технический вестник информационных технологий, механики и оптики. 2013. № 2. С. 163–165.
5. Пат. на полезную модель 108868 RU, МПК G06F 9/00. Платформа интегрированной модульной авионики / А. В. Богданов, Г. А. Васильев, П. С. Виноградов, К. А. Егоров, А. Н. Зайченко, И. В. Ковернинский, В. И. Петухов, А. Н. Романов, Е. В. Смирнов, Б. В. Уткин, Е. А. Федосов, А. В. Шукалов — № 2011121962/08; заявл. 01.06.2011; опубл. 27.09.2011, Бюл. № 27. — 2 с.
6. **Книга Е. В., Жаринов И. О.** Организация внутренней структуры модулей перспективных бортовых вычислительных систем авионики// Информационная безопасность, проектирование и технология элементов и узлов компьютерных систем: сб. тр. молодых ученых, аспирантов и студентов научно-педагогической школы кафедры ПБКС. СПб.: НИУ ИТМО, 2013. Вып. 1. С. 127–131.

7. **Книга Е. В., Жаринов И. О.** Принципы построения комбинированной топологии сети для перспективных бортовых вычислительных систем // Научно-технический вестник информационных технологий, механики и оптики. 2013. № 6. С. 92–98.
8. **Шепета А. П., Жаринов И. О.** Перспективы применения в авиации интегрированных нашлемных систем нейрофизиологического контроля // Информационно-управляющие системы. 2003. № 6. С. 58–62.
9. **Парамонов П. П., Костишин М. О., Жаринов И. О., Нечаев В. А., Сударчиков С. А.** Принцип формирования и отображения массива геоинформационных данных на экран средств бортовой индикации // Научно-технический вестник информационных технологий, механики и оптики. 2013. № 6. С. 136–142.
10. **Костишин М. О., Жаринов И. О., Жаринов О. О., Нечаев В. А., Суслов В. Д.** Оценка точности визуализации местоположения объекта в геоинформационных системах и системах индикации навигационных комплексов пилотируемых летательных аппаратов // Научно-технический вестник информационных технологий, механики и оптики. 2014. № 1. С. 87–93.
11. **Kniga E. V., Zharinov I. O.** Analysis and Algorithms of the Control in Advanced Digital Avionics Ssystems // Automation & Control: Proc. of the Intern. Conf. of Young Scientists, Saint-Petersburg, Nov. 21–22, 2013. National Research University Saint-Petersburg State Polytechnical University, 2013. P. 28–32.
12. **Шек-Иовсепянц Р. А., Жаринов И. О.** Генерация проектных решений бортового оборудования с использованием аппарата генетических алгоритмов // Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики. 2010. № 3. С. 67–70.
13. **Дейко М. С., Жаринов И. О.** Применение симплекс-метода и метода искусственного базиса при проектировании бортового приборного оборудования // Научно-технический вестник информационных технологий, механики и оптики. 2013. № 1. С. 124–129.
14. **Гатчин Ю. А., Видин Б. В., Жаринов И. О., Жаринов О. О.** Метод автоматизированного проектирования аппаратных средств бортового оборудования // Изв. вузов. Приборостроение. 2010. Т. 53. № 5. С. 5–10.
15. **Сабо Ю. И., Жаринов И. О.** Критерий подобия проектных решений требованиям технического задания в авионике // Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики. 2010. № 3. С. 57–63.
16. **Гатчин Ю. А., Видин Б. В., Жаринов И. О., Жаринов О. О.** Модели и методы проектирования интегрированной модульной авионики // Вестник компьютерных и информационных технологий. 2010. № 1. С. 12–20.
17. **Парамонов П. П., Гатчин Ю. А., Видин Б. В., Жаринов И. О., Жаринов О. О.** Модели композиционного проектирования авионики // Изв. вузов. Приборостроение. 2010. Т. 53. № 7. С. 5–13.
18. **Гатчин Ю. А., Жаринов И. О., Жаринов О. О.** Архитектура программного обеспечения автоматизированного рабочего места разработчика бортового авиационного оборудования // Научно-технический вестник информационных технологий, механики и оптики. 2012. № 2. С. 140–141.
19. **Парамонов П. П., Гатчин Ю. А., Жаринов И. О., Жаринов О. О., Дейко М. С.** Принципы построения отраслевой системы автоматизированного проектирования в авиационном приборостроении // Научно-технический вестник информационных технологий, механики и оптики. 2012. № 6. С. 111–117.
20. **Гатчин И. Ю., Жаринов И. О., Жаринов О. О., Косенков П. А.** Реализация жизненного цикла «проектирование-производство-эксплуатация» бортового оборудования на предприятиях авиационной промышленности // Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики. 2012. № 2. С. 141–143.

UDC 681.324

Design of Computing Components for Integrated Modular Avionics Systems

Shukalov A. V.[a, b], Associate Professor, Director, aviation78@mail.ru
Paramonov P. P.[a, b], Dr. Sc., Tech., Professor, Advisor to Director, postmaster@elavt.spb.ru
Kniga E. V.[a, b], Post-Graduate Student, Senior Engineer, ekovinskaya@gmail.com
Zharinov I. O.[a, b], Dr. Sc., Tech., Head of Department, Head of Learning-Scientist Center, igor_rabota@pisem.net
[a]Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics, 49, Kronverkskii St., 197101, Saint-Petersburg, Russian Federation
[b]P. A. Efimov Saint-Petersburg Scientific Design Bureau «Electroavtomatika», 40, Marshala Govorova St., 198095, Saint-Petersburg, Russian Federation

Purpose: The development of modern aviation instrumentation assumes the introduction of airborne computer systems of integrated modular avionics. To create such systems, special design solutions are required with a higher level of unification and standardization. The purpose of this research is developing structures of integrated modular avionics computing modules. **Methods:** The internal structure of the computational components was obtained using the methods of engineering synthesis, design automation systems, choice theory

techniques and automated generation of design solutions. **Results:** The main result is the internal structure of the following modules: the computing module, the graphic module, the switch module, the input-output module and the mass storage module. In each case, the structure was obtained by modifying the unified computing component called "basic module". The basic module includes units which support the module, the intermodule interface, the functions of the module, the control and diagnostic of the external interfaces and the communication with the mezzanine boards. It also includes an intelligent power unit. The structure of the calculator coincides with the structure of the basic module. The input-output module is based on the basic module structure supplemented with mezzanine boards providing hardware and software support for the data input-output functions via specialized aiborne interfaces. To obtain the graphic module, the basic module is supplemented with a specialized graphic controller supporting the function of transmitting video via Fibre Channel interface. The switch module contains specialized elements: transmitters and receivers of Fibre Channel optical signal and Fibre Channel interface controller. The mass storage module structure assumes specialized mezzanine boards to expand the scope of the module memory. **Practical relevance:** The results were obtained during the research and development work on the design of advanced models of computing equipment for integrated modular avionics. These results have been brought to the industrial samples which are currently being tested.

Keywords — Integrated Modular Avionics, Computer Systems, Modules, Internal Structure.

Reference

1. Gatchin Iu. A., Zharinov I. O. *Osnovy proektirovaniia vychislitel'nykh sistem integrirovannoi modul'noi avioniki* [Basics of Designing Computer Systems Integrated Modular Avionics]. Moscow, Mashinostroenie Publ., 2010. 224 p. (In Russian).
2. Paramonov P. P., Zharinov I. O. Integrated On-Board Computing Systems: Present Situation Review and Development Prospects Analysis in the Aviation Instrument-making Industry. *Nauchno-tekhnicheskii vestnik informatsionnykh tekhnologii, mekhaniki i optiki*, 2013, no. 2, pp. 1–17 (In Russian).
3. Zharinov O. O., Vidin B. V., Shek-Iovsepiants R. A. Crate Creation Strategy of the Onboard Multiprocessing Computing System for the Fifth Generation Avionics. *Nauchno-tekhnicheskii vestnik informatsionnykh tekhnologii, mekhaniki i optiki*, 2010, no. 4, pp. 21–27 (In Russian).
4. Kniga E. V., Zharinov I. O., Bogdanov A. V., Vinogradov P. S. Rules of Architecture Design for Advanced Onboard Digital Computer Systems in Avionics. *Nauchno-tekhnicheskii vestnik informatsionnykh tekhnologii, mekhaniki i optiki*, 2013, no. 2, pp. 163–165 (In Russian).
5. Bogdanov A. V., et al. *Platforma integrirovannoi modul'noi avioniki* [Platform Integrated Modular Avionics]. Patent Russian Federation, no. 108868, 2011.
6. Kniga E. V., Zharinov I. O. Organization of the Internal Structure of the Modules Promising Onboard Computing Avionics Systems. *Sbornik trudov molodykh uchenykh, aspirantov i studentov nauchno-pedagogicheskoi shkoly kafedry PBKS "Informatsionnaia bezopasnost', proektirovanie i tekhnologiia elementov i uzlov komp'iuternykh sistem"* [Collected Works of Young Scientists and Students of Scientific and Pedagogical School Department PBKS "Information Security, Design and Technology Elements and Units of Computer Systems"]. Saint-Petersburg, NIU ITMO Publ., 2013, vol. 1, pp. 127–131 (In Russian).
7. Kniga E. V., Zharinov I. O. Design Principles of a Combined Network Topology for Advanced On-board Computing System. *Nauchno-tekhnicheskii vestnik informatsionnykh tekhnologii, mekhaniki i optiki*, 2013, no. 6, pp. 92–98 (In Russian).
8. Shepeta A. P., Zharinov I. O. Application of Helmet-Mounted System of Neurophysiology Control in Aviation. *Informatsionno-upravliaiushchie sistemy,* 2003, no. 6, pp. 58–62 (In Russian).
9. Paramonov P. P., Kostishin M. O., Zharinov I. O., Nechaev V. A., Sudarchikov S. A. Formation and Display Principles for an Array of Geoinformation Data by Means of Onboard Display Screen. *Nauchno-tekhnicheskii vestnik informatsionnykh tekhnologii, mekhaniki i optiki,* 2013, no. 6, pp. 136–142 (In Russian).
10. Kostishin M. O., Zharinov I. O., Zharinov O. O., Nechaev V. A., Suslov V. D. Accuracy Evaluation of the Object Location Visualization for Geo-information and Display Systems of Manned Aircraft Navigation Complexes. *Nauchno-tekhnicheskii vestnik informatsionnykh tekhnologii, mekhaniki i optiki,* 2014, no. 1, pp. 87–93 (In Russian).
11. Kniga E. V., Zharinov I. O. Analysis and Algorithms of the Control in Advanced Digital Avionics Systems. *Proc. of the Intern. Conf. of Young Scientists "Automation & Control"*, Saint-Petersburg, November 21–22, 2013. National Research University Saint-Petersburg State Polytechnical University Publ., 2013, pp. 28–32.
12. Shek-Iovsepiants R. A., Zharinov I. O. Design Generation of the Avionic Equipment by Genetic Algorithms. *Nauchno-tekhnicheskii vestnik informatsionnykh tekhnologii, mekhaniki i optiki*, 2010, no. 3, pp. 67–70 (In Russian).
13. Deiko M. S., Zharinov I. O. Simplex-method and Artificial Basis Method Application for Onboard Equipment Designs. *Nauchno-tekhnicheskii vestnik informatsionnykh tekhnologii, mekhaniki i optiki*, 2013, no. 1, pp. 124–129 (In Russian).
14. Gatchin Iu. A., Vidin B. V., Zharinov I. O., Zharinov O. O. A Method of Computer-aided Design of Airborne Hardware. *Izvestiia vuzov. Priborostroenie*, 2010, vol. 53, no. 5, pp. 5–10 (In Russian).
15. Sabo Iu. I., Zharinov I. O. Similarity Criterion of Design Decisions to Requirements of the Technical Project in Avionics. *Nauchno-tekhnicheskii vestnik informatsionnykh tekhnologii, mekhaniki i optiki*, 2010, no. 3, pp. 57–63 (In Russian).
16. Gatchin Iu. A., Vidin B. V., Zharinov I. O., Zharinov O. O. Models and Methods of Integrated Modular Avionics Designing. *Vestnik komputernih i informatsionnykh tekhnologii*, 2010, no. 1, pp. 12–20 (In Russian).
17. Paramonov P. P., Gatchin Iu. A., Vidin B. V., Zharinov I. O., Zharinov O. O. Models for Composition Design of Avionic Systems. *Izvestiia vuzov. Priborostroenie*, 2010, vol. 53, no. 7, pp. 5–13 (In Russian).
18. Gatchin Iu. A., Zharinov I. O., Zharinov O. O. Software Architecture for the Automated Workplace of the Onboard Aviation Equipment Developer. *Nauchno-tekhnicheskii vestnik informatsionnykh tekhnologii, mekhaniki i optiki,* 2012, no. 2, pp. 140–141 (In Russian).
19. Paramonov P. P., Gatchin Iu. A., Zharinov I. O., Zharinov O. O., Deiko M. S. Principles of Branch System Creation for the Automated Design in Aviation Instrumentation. *Nauchno-tekhnicheskii vestnik informatsionnykh tekhnologii, mekhaniki i optiki*, 2012, no. 6, pp. 111–117 (In Russian).
20. Gatchin I. Iu., Zharinov I. O., Zharinov O. O., Kosenkov P. A. Life Cycle "Design-Manufacture-Operation" Realization for Onboard Equipment at the Aviation Industry Enterprises. *Nauchno-tekhnicheskii vestnik informatsionnykh tekhnologii, mekhaniki i optiki*, 2012, no. 2, pp. 141–143 (In Russian).

УДК 004.056

ИССЛЕДОВАНИЕ ОТКРЫТЫХ БАЗ УЯЗВИМОСТЕЙ И ОЦЕНКА ВОЗМОЖНОСТИ ИХ ПРИМЕНЕНИЯ В СИСТЕМАХ АНАЛИЗА ЗАЩИЩЕННОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ

А. В. Федорченко[a], *младший научный сотрудник*
А. А. Чечулин[a], *канд. техн. наук, старший научный сотрудник*
И. В. Котенко[a], *доктор техн. наук, профессор, заведующий лабораторией проблем компьютерной безопасности*
[a]*Санкт-Петербургский институт информатики и автоматизации РАН, Санкт-Петербург, РФ*

Постановка проблемы: *ежегодно количество обнаруживаемых уязвимостей в программных и аппаратных продуктах остается на высоком уровне. Вместе с этим несогласованная работа компаний и организаций, занимающихся поиском и классификацией уязвимостей, приводит к уменьшению эффективности использования их баз уязвимостей в системах анализа защищенности. Целью работы является анализ открытых баз уязвимостей и оценка возможности их применения в системах анализа защищенности компьютерных сетей, в том числе получение статистики и выявление общих тенденций обнаружения уязвимостей в программно-аппаратном обеспечении.* ***Результаты:*** *проведены разбор и сравнение форматов открытых баз уязвимостей, таких как CVE, NVD, X-Force и OSVDB, а также форматов словарей продуктов и показателей, таких как CPE и CVSS, характеризующих уязвимости. Собрана статистика обнаруженных уязвимостей в распространенных операционных системах и веб-браузерах, получено распределение уязвимых продуктов основных разработчиков программного обеспечения за последние 10 лет. Выявлены общие тенденции обнаружения, опубликования и устранения уязвимостей в наиболее используемых продуктах различных производителей программного обеспечения (Microsoft, Google, Oracle, Apple и др.).* ***Практическая значимость:*** *анализ форматов представления уязвимостей в открытых базах дает возможность выделить наиболее значимые атрибуты, что позволит в дальнейшем решить задачу интеграции (объединения) этих баз для повышения эффективности их применения в системах анализа защищенности компьютерных систем и сетей.*

Ключевые слова *— защита информации, уязвимости, базы уязвимостей, тенденции обнаружения уязвимостей, анализ защищенности, компьютерные атаки, программно-аппаратное обеспечение.*

Введение

За последние десятилетия зависимость современного общества от компьютерных систем существенно возросла. Банковские операции, управление торговлей рынков, автоматизированные военные и государственные системы все в большей степени зависят от компьютерных систем. В результате риск реализации различных классов атак, базирующихся на эксплуатации имеющихся уязвимостей в программно-аппаратном обеспечении, для критически важных объектов очень велик.

Как следствие, в наши дни проводятся крупномасштабные исследования проблем безопасности, вызванных уязвимостями программно-аппаратного обеспечения. Несмотря на существующие угрозы, общество не готово отказаться от использования сети Интернет и компьютерных сетей в целом, так как они предоставляют огромные возможности в финансовой, политической и военной сферах. Постоянное совершенствование технологий безопасности в информационном мире не может дать гарантий абсолютной защищенности компьютерных систем.

Уязвимости обнаруживались во всех основных операционных системах и приложениях. Так как новые уязвимости находят непрерывно, единственный путь уменьшить вероятность их использования злоумышленниками заключается в выполнении непрерывного мониторинга защищенности, заключающегося в постоянном отслеживании появления уязвимостей, оперативном установлении обновлений и использовании инструментов, которые помогают противодействовать возможным атакам, базирующимся на эксплуатации этих уязвимостей [1–6].

Классификации уязвимостей систематизируют различные виды искусственных и естественных, случайных и злонамеренных, внутренних и внешних угроз по множеству параметров. Как правило, имеющиеся системы классификации уязвимостей выделяют класс угроз, связанный с возможностью реализации нарушителем программных и аппаратных уязвимостей, однако классы уязвимостей описываются только в общем плане. При всем этом классификации уязвимостей являются основой для построения моделей угроз безопасности компьютерных сетей.

Уязвимости можно классифицировать по этапам жизненного цикла, на которых они появляются: 1) уязвимости этапа проектирования; 2) уязвимости этапа реализации; 3) уязвимости этапа эксплуатации. По объекту воздействия выделяются следующие типы уязвимостей: уровня сети; уровня операционной системы; уровня баз данных; уровня приложений [7]. Также можно классифицировать уязвимости по типу целевого средства, а именно: 1) аппаратных средств; 2) операционных систем; 3) приложений.

Первые инциденты нарушения безопасности, официально зарегистрированные в базах данных уязвимостей, появились в 1988 г. С тех пор ведется постоянный поиск и регистрация уязвимостей как в рамках различных открытых проектов, так и коммерческими компаниями, исследовательскими институтами и добровольцами. Среди лидеров детектирования уязвимостей можно выделить компанию MITRE и ее базу «Общие уязвимости и воздействия» (Common Vulnerabilities and Exposures — CVE) [8], Национальный институт стандартов и технологий (National Institute of Standardsand Technology — NIST) и его «Национальную базу данных уязвимостей» (National Vulnerabilities Database — NVD) [9], проект «Открытая база данных уязвимостей» (Open Source Vulnerabilities Data Base — OSVDB) [10], Группу чрезвычайного компьютерного реагирования Соединенных Штатов (United State Computer Emergency Readiness Team — US-CERT) с «Базой данных записей уязвимостей» (Vulnerability Notes Database — VND) [11], проект SecurityFocus и его ленту уязвимостей BugTraq [12], компанию IBM с базой уязвимостей X-Force [13], а также коммерческие («закрытые») базы компаний Secunia [14] и VUPEN Security [15].

Представляемые в статье результаты анализа открытых баз уязвимостей были получены в рамках разработки интегрированной базы уязвимостей. Практическая реализация данной базы в дальнейшем будет использоваться в качестве компонента системы оценки защищенности компьютерных сетей [4]. Все полученные статистические данные были собраны посредством автоматизированной обработки информации каждой используемой базы, ее дальнейшего разбора и анализа.

Проведенное исследование позволяет получить ясную картину в области обнаружения уязвимостей, что, в свою очередь, дает возможность проводить оценки качества производимых продуктов различных мировых компаний, а также сравнивать по степени безопасности как типы программно-аппаратного обеспечения, так и конкретные решения, вышедшие на рынок.

Открытые базы уязвимостей

Для получения представления о содержании открытых баз данных уязвимостей необходимо произвести их анализ. В качестве основных были выбраны следующие источники: CVE, NVD, OSVDB, база уязвимостей X-Force.

База уязвимостей CVE и переход к формату CVRF

База данных уязвимостей CVE ведется с 1999 г. и на 5 мая 2014 года включала 70 078 записей. Основное отличие данной базы заключается в том, что она является наиболее полной и систематизированной, поэтому ее используют как основу для указания соответствия записей уязвимостей в других базах.

К основным полям (элементам структуры) записей уязвимостей относятся:

1) статус — в этом поле может содержаться либо значение Entry (проверенная запись), либо значение Candidate (еще не проверенная уязвимость);

2) фаза — в этом поле содержится значение этапа развития уязвимости, а также дата присвоения указанного этапа. В качестве значений могут быть: Proposed — фаза предложения уязвимости; Interim — промежуточная фаза уязвимости; Modified — фаза модификации уязвимости; Assigned — фаза установления уязвимости;

3) описание — поле содержит текстовое описание уязвимости;

4) ссылки — в данном поле содержатся ссылки на другие источники с указанием конкретного адреса интернет-ресурса описания уязвимости и идентификатора источника;

5) голоса — поле содержит имена членов голосования, принявших решение о занесении уязвимости в базу;

6) комментарии — в поле имеется имя автора комментария и его текстовое содержание.

Также в атрибутах записей уязвимостей содержится тип уязвимости, имя и идентификатор. Имя уязвимости имеет формат «*CVE-YYYY-NNNN*», где *YYYY* — это год обнаружения уязвимости, а *NNNN* — ее порядковый номер. У идентификатора уязвимостей в записи присутствует только год и порядковый номер.

Процесс добавления уязвимости в базу содержит три этапа:

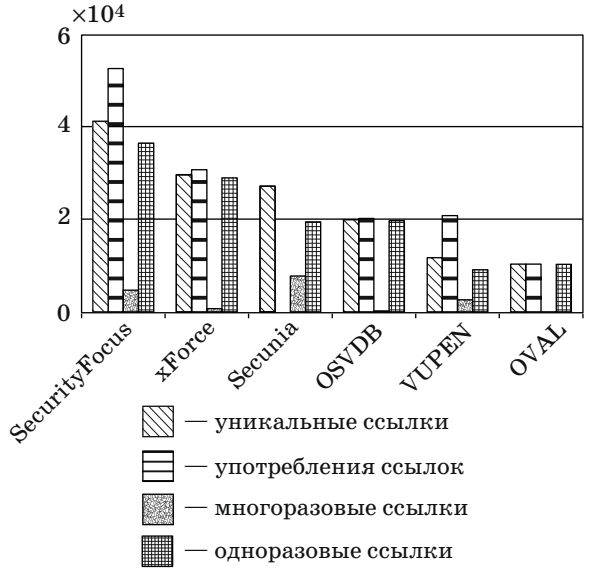
1) обработку — анализ, исследование и процесс приведения уязвимости к формату CVE;

2) присвоение — назначение конкретной записи уязвимости идентификатора CVE;

3) публикацию — добавление новой записи и публикация ее на интернет-ресурсе CVE [8], как только идентификатор CVE официально присвоен.

Статистика количества ссылок на сторонние источники в уязвимостях из базы CVE представлена на рис. 1. Стоит отметить, что наибольшее число ссылок ведет на ресурсы других баз данных уязвимостей, а остальные — на наиболее крупных производителей программно-аппаратного обеспечения.

Исходя из результатов анализа и полученной статистики связей с другими источниками, можно сделать вывод о том, что база данных уязвимостей CVE представляет собой достаточно полный список уязвимостей и имеет большое количество ссылок на базы уязвимостей и производителей программных и аппаратных средств. С другой



■ ***Рис. 1.*** Статистика использования ссылок на сторонние источники в базе CVE

стороны, в базе CVE отсутствует механизм описания принадлежности уязвимостей к конкретным продуктам, а также присвоение им метрик и расчета степени опасности.

В мае 2012 года был представлен формат «Общая структура сообщений об уязвимостях» (Common Vulnerability Reporting Framework — CVRF) [16], и сейчас происходит переход записей уязвимостей CVE на данный формат. Основными отличиями формата CVRF от формата CVE являются:

1) представление полей «Описание», «Этап добавления» и «Фаза» в едином элементе «Запись» (Note);

2) наличие у каждой записи уязвимости порядкового номера (атрибут Order), считая от начала составления базы CVE;

3) возможность привязки записей уязвимостей к списку продуктов, подвергающихся данной уязвимости.

Безусловно, все указанные изменения являются преимуществом формата CVRF, но вместе с тем наиболее явным достоинством обладает п. 3, описание которого будет приведено далее.

База уязвимостей NVD

Национальная база данных уязвимостей США (NVD) — хранилище данных уязвимостей, основанное на стандартах протокола автоматизации содержимого безопасности (Security Content Automation Protocol — SCAP). База NVD объединила в себе описание уязвимостей, названия программного обеспечения с этими уязвимостями и оценки опасности уязвимостей [17, 18]. На 5 мая 2014 года база данных уязвимостей NVD имела 62 124 записи уязвимостей.

Структура записи уязвимости в базе NVD является расширенной формой представления записи в базе CVE, за счет наличия следующих полей: 1) конфигурации уязвимых продуктов с учетом зависимостей; 2) списка уязвимых продуктов; 3) показателей, характеризующих уязвимость в формате «Общей системы оценки уязвимостей» (Common Vulnerability Scoring System — CVSS) версии 2.0 [19]; 4) типа доступа для реализации уязвимости.

В ходе исследования базы NVD было установлено, что 82,77 % уязвимостей принадлежат приложениям, и всего лишь 12,28 и 3,59 % — операционным системам и аппаратному обеспечению соответственно (рис. 2).

Также было выявлено, что зависимости конфигураций уязвимых продуктов (когда уязвимость характерна не для отдельного продукта, а для комбинации нескольких, например, операционной системы и приложения) встречаются лишь в 7,95 % всех записей уязвимостей (рис. 3).

■ ***Рис. 2.*** Статистика принадлежности записей по типу уязвимых продуктов

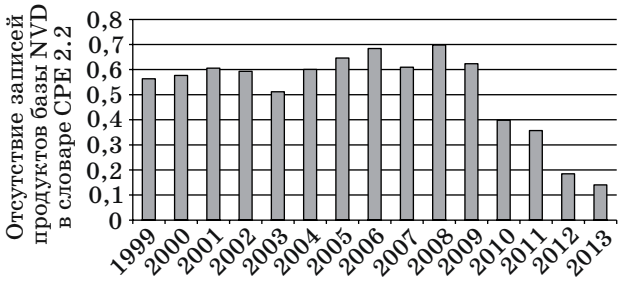
■ ***Рис. 3.*** Статистика распределения записей уязвимостей по наличию зависимостей продуктов, %

Основную часть зависимостей в конфигурациях составляют записи пар продуктов (например, приложения и операционной системы), а уязвимости, в которых больше чем один продукт влияет на ее успешную реализацию, встречаются около 30 раз, и, как правило, это некорректные записи.

Отличительной особенностью базы NVD от всех рассматриваемых баз уязвимостей является использование «Общего перечисления платформ» (Common Platform Enumeration — CPE) [20], являющегося одним из лучших словарей продуктов среди известных аналогов за счет большого числа записей и унифицированного формата имен программно-аппаратного обеспечения. Однако даже у данного формата представления записей продуктов есть недостатки, а именно: 1) неоднозначность значений разных полей формата; 2) недостаточное использование записей данного словаря базой NVD (рис. 4).

Первый недостаток был выявлен при выделении значений каждого из полей формата записи продуктов и дальнейшем сравнении со значениями смежных полей. Результаты анализа показали, что достаточно большое количество (около 70) значений разных полей пересекаются (равны), что приводит к неточному распознаванию неформатированных имен, а значит, точность определения наличия уязвимости по таким именам существенно падает. Второй недостаток заключается в неполноте (по количеству записей) словаря CPE, что было обнаружено в результате поиска в нем используемых в базе NVD записей продуктов.

Как было сказано ранее, формат CVRF имеет собственную структуру представления как словаря продуктов, так и механизма описания конфигураций уязвимого программно-аппаратного обеспечения. Главной особенностью данной структуры является ее иерархичность, которая обеспечивает более удобный доступ к данным, их представление и использование, чем в словаре CPE. Основа структуры (главный элемент) представлена полем «Ветка» (Branch), которое отвечает за соблюдение правил построения дерева



■ ***Рис. 4.*** Распределение отсутствующих записей продуктов из базы NVD в словаре CPE

продуктов. Таким образом, исключается дублирование данных, но, что более важно, это позволяет указывать в конфигурации уязвимых продуктов не только отдельные записи продуктов, но и группы продуктов, также имеющих свои идентификаторы. К сожалению, доступ к данному словарю в настоящий момент закрыт, в связи с чем провести качественный анализ и сравнение данного словаря со словарем CPE не удалось.

База уязвимостей OSVDB

Независимая и открытая база данных уязвимостей OSVDB создана для сообщества специалистов в области безопасности. Цель проекта состоит в том, чтобы обеспечить точную, детализированную, актуальную информацию об уязвимостях для систем обеспечения безопасности [21]. На 5 мая 2014 года данная база содержала 105 413 уязвимостей.

Структура данной базы не сильно отличается от ранее рассмотренной базы NVD, однако стоит отметить основные поля ее записи уязвимости: «Идентификатор OSVDB»; «Дата обнаружения»; «Имя производителя»; «Имя продукта»; «Версия продукта», которая содержит строковое значение версии продукта, имеющего данную уязвимость; «Ссылка», указывающая на прямой адрес к интернет-ресурсу другой базы или базы производителя, в котором описывается данная уязвимость; «Решение», имеющее строковое описание «исправления» уязвимости; «Метрики уязвимости», содержащие критерии оценки уязвимостей в формате CVSS версии 2.0; это поле не является обязательным (ввиду того, что поле присутствует при наличии ссылки на базу NVD).

База уязвимостей X-Force

База уязвимостей X-Force является проектом компании IBM и находится в открытом доступе в сети Интернет. Поля данных, описывающих записи уязвимостей этой базы, не сильно отличаются от полей баз уязвимостей, описанных ранее. Однако в их состав входят элементы, указывающие на преимущество базы X-Force: поле «Последствия», выражающее в формализованном виде возможный результат эксплуатации уязвимости; поле TemporalScore, являющееся элементом системы метрик CVSS, используемой для оценивания временных характеристик уязвимости. Также стоит отметить наличие в базе довольно подробных описаний и заключений об уязвимостях.

На 19 мая 2014 года база содержала 65 550 записей уязвимостей, 69,19 % из которых имеют базовую и временную оценки системы показателей CVSS, характеризующих данные уязвимости. Описания уязвимостей также содержат параметр, определяющий риск, которому подвергается система при реализации конкретной

уязвимости. Уязвимости низкого уровня опасности составляют всего 12 %, а на уязвимости среднего и высокого уровня опасности приходится 82 % (62 и 26 % соответственно), что определяет существующую проблему как в области разработки программно-аппаратного обеспечения, так и в области его безопасного использования.

В результате анализа уязвимостей по базовой и временной оценкам системы CVSS было получено распределение записей по шкале от 1 до 10 (рис. 5).

На рисунке x — это текущий диапазон значений для базовых и временных оценок. Стоит отметить, что наибольшее число уязвимостей имеет по базовым показателям оценку от 4 до 8, а по временным показателям — от 3 до 8, с максимами в диапазонах значений от 3 до 4 и от 4 до 5 соответственно.

При сравнительном анализе рассматриваемых баз данных уязвимостей по количеству ссылок на источники описания уязвимостей было установлено, что лидером является база OSVDB с результатом в среднем 11,5 ссылок на уязвимость, далее следует база X-Force — 6 ссылок на уязвимость и, наконец, базы CVE/NVD/CVRF со значением в среднем 5,6 ссылок на уязвимость.

■ ***Рис. 5.*** Распределение уязвимостей базы X-Force по базовой и временной оценкам системы CVSS

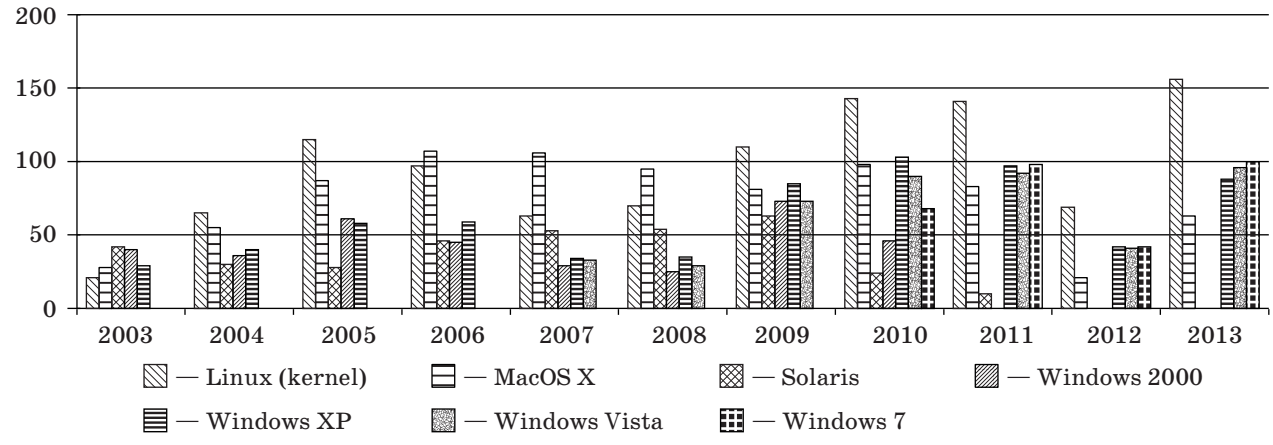
Тенденции в области обнаружения уязвимостей программно-аппаратного обеспечения

По общему числу зарегистрированных в базе NVD уязвимостей за последние 10 лет можно выделить следующих производителей программно-аппаратного обеспечения: 1) Microsoft (4,67 %); 2) Apple (3,93 %); 3) Oracle (3,65 %); 4) IBM (3,08 %); 5) Cisco (2,65 %); 6) Sun (2,33 %); 7) Mozilla (2,28 %); 8) Linux (1,99 %); 9) Google (1,88 %); 10) HP (1,59 %); 11) RedHat (1,11 %); 12) Apache (0,77 %).

В ходе сравнения числа уязвимостей операционных систем было выявлено, что на один продукт семейства Windows в среднем в год приходится 60 уязвимостей, Mac OS X — 75, Linux (kernel) — 95.

Распределение уязвимостей в клиентских операционных системах представлено на рис. 6. По данному рисунку видно, что в последние 5 лет наиболее уязвимым является ядро операционных систем Linux, более безопасными по количеству уязвимостей являются операционные системы корпорации Microsoft и наименьшее число уязвимостей в данный момент обнаруживается в операционной системе Mac OS компании Apple.

В ходе исследования открытых баз уязвимостей был проведен анализ уязвимостей по их принадлежности к конкретным типам продуктов: 1) операционные системы (клиентские); 2) серверные операционные системы и 3) веб-браузеры. Из полученных результатов можно выделить то, что на протяжении всего времени большее количество уязвимостей детектируется



■ ***Рис. 6.*** Распределение уязвимостей среди операционных систем

в программном обеспечении первого типа (исключением является 2011 г., в который по числу уязвимостей лидирует третий тип продуктов). Также за рассматриваемый временной интервал количество уязвимостей во всех трех типах продуктов сохраняется на довольно высоком уровне (рис. 7).

Стоит отметить, что в 2012 г. Microsoft значительно уступила по числу обнаруженных уязвимостей таким компаниям, как Mozilla, Cisco, IBM, Apple и Oracle, хотя до 2011 г. данная компания являлась абсолютным лидером по числу уязвимостей (рис. 8).

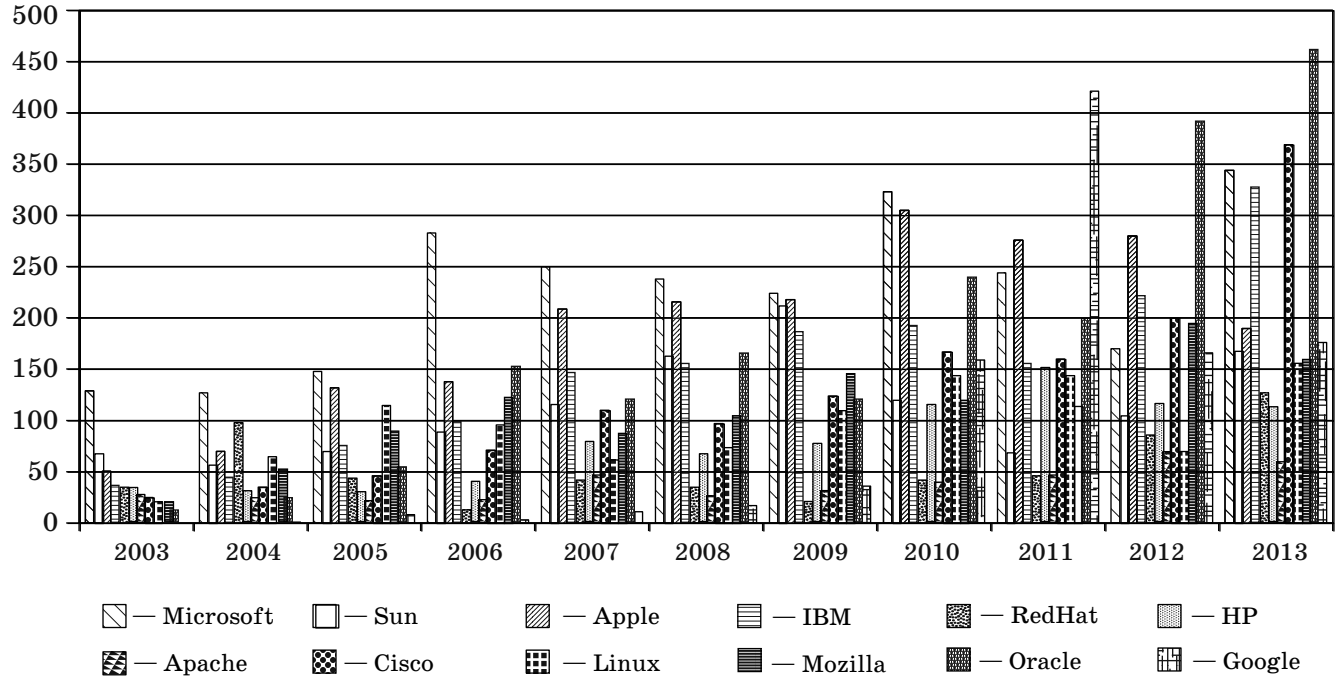
■ ***Рис. 7.*** Распределение уязвимостей однотипных продуктов

Это обусловлено тем, что в последние годы происходит активное перераспределение рынка программно-аппаратного обеспечения. В свою очередь, стремительный рост количества уязвимостей в продуктах компании Oracle можно объяснить покупкой Java в 2010 г. Резкий скачок в 2011 г. числа уязвимостей в продуктах компании Google объясняется выпуском браузера Chrome, который являлся самым уязвимым продуктом в 2010 и 2011 годах.

Проведенное исследование открытых баз уязвимостей дало ясную картину развития и текущего состояния в области уязвимостей программно-аппаратного обеспечения. Опираясь на полученные результаты, можно сделать вывод, что в данный момент происходят положительные изменения (более точное детектирование уязвимостей; работы над новыми форматами записей уязвимостей и продуктов; увеличение количества уязвимостей, подвергшихся оцениванию по различным показателям).

Вместе с тем отрицательно сказывается сохранение существующих недостатков баз уязвимостей — отсутствие форматов записей продуктов (базы OSVDB и X-Force), невозможность прямой загрузки баз уязвимостей. Исходя из данных фактов нельзя судить однозначно ни об общем улучшении баз уязвимостей, ни о качестве их использования в различных системах безопасности.

В свою очередь именно множественные несоответствия форматов описания уязвимостей и продуктов, а также несогласованное составление баз уязвимостей привело авторов настоящей ста-



■ ***Рис. 8.*** Распределение уязвимостей крупнейших производителей программно-аппаратного обеспечения

тьи к необходимости создания интегрированной базы уязвимостей, которая должна собрать в себе только полезную информацию, необходимую для более эффективного функционирования разрабатываемой системы оценки защищенности компьютерных сетей [4].

Заключение

В результате проделанного анализа можно сделать вывод о том, что, несмотря на большое количество баз данных уязвимостей, каждая база имеет выраженные преимущества и недостатки. В свою очередь накопление информации об уязвимостях и их возрастающее количество в настоящее время может привести к большим несогласованностям между имеющимися базами данных уязвимостей в будущем, что усложнит их использование отдельно друг от друга. Тенденции в области обнаружения уязвимостей в различных продуктах дают понять, что основная масса программно-аппаратного обеспечения, подвергающего систему высокому риску нарушения безопасности, принадлежит лидирующим компаниям. Вместе с этим их популярность среди пользователей только увеличивает шансы на успешную эксплуатацию той или иной уязвимости, что указывает на недостаточную защищенность данных продуктов и ставит под сомнение их репутацию в рамках обеспечения должного уровня безопасности.

Работа выполняется при финансовой поддержке РФФИ (13-01-00843, 13-07-13159, 14-07-00697, 14-07-00417), программы фундаментальных исследований ОНИТ РАН (контракт № 2.2), проекта ENGENSEC программы Европейского сообщества TEMPUS и государственных контрактов № 14.604.21.0033 и 14.604.21.0137.

Литература

1. **Kotenko I. V., Stepashkin M. V.** Network Security Evaluation Based on Simulation of Malefactor's Behavior // Proc. of the Intern. Conf. on Security and Cryptography, (SECRYPT 2006), Portugal, Aug. 7–10, 2006. P. 339–344.
2. **Котенко И. В., Степашкин М. В., Богданов В. С.** Архитектуры и модели компонентов активного анализа защищенности на основе имитации действий злоумышленников // Проблемы информационной безопасности. Компьютерные системы. 2006. № 2. С. 7–24.
3. **Ruiz J. F.**, at al. A Methodology for the Analysis and Modeling of Security Threats and Attacks for Systems of Embedded Components/ J. F. Ruiz, R. Harjani, A. Mana, V. Desnitsky, I. V. Kotenko, A. A. Chechulin // Proc. of the 20th Euromicro Intern. Conf. on Parallel, Distributed and Network-Based Processing (PDP 2012), Garching, Germany, 2012. P. 261–268.
4. **Kotenko I. V., Chechulin A. A.** Common Framework for Attack Modeling and Security Evaluation in SIEM Systems // Proc. of IEEE Intern. Conf. on Green Computing and Communications, Conf. on Internet of Things, and Conf. on Cyber, Physical and Social Computing, Besanson, France, Sept. 11–14, 2012. Los Alamitos, California, USA: IEEE Computer Society, 2012. P. 94–101.
5. **Чечулин А. А., Котенко И. В.** Комбинирование механизмов защиты от сканирования в компьютерных сетях // Информационно-управляющие системы. 2010. № 6. С. 21–27.
6. **Котенко И. В., Новикова Е. С.** Визуальный анализ для оценки защищенности компьютерных сетей // Информационно-управляющие системы. 2013. № 3. С. 55–61.
7. **Компьютерная** безопасность: вопросы и решения. http://comp-bez.ru/?p=782 (дата обращения: 06.06.2014).
8. **Common** Vulnerabilities and Exposures (CVE). http://cve.mitre.org (дата обращения: 06.06.2014).
9. **National** Vulnerabilities Database (NVD). http://nvd.nist.gov (дата обращения: 06.06.2014).
10. **Open** Source Vulnerabilities Data Base (OSVDB). http://osvdb.org (дата обращения: 06.06.2014).
11. **United** States Computer Emergency Readiness Team (US-CERT). http://www.us-cert.gov (дата обращения: 06.06.2014).
12. **BugTraq.** http://securityfocus.com (дата обращения: 06.06.2014).
13. **X-Force.** http://xforce.iss.net (дата обращения: 06.06.2014).
14. **Secunia.** http://secunia.com (дата обращения: 11.10.2013).
15. **Vupen** Security. http://www.vupen.com (дата обращения: 25.05.2014).
16. **Common** Vulnerability Reporting Framework (CVRF). http://www.icasi.org/cvrf-1.1 (дата обращения: 06.06.2014).
17. **Common** Vulnerability Scoring System. http://www.first.org/cvss (дата обращения: 06.06.2014).
18. **Котенко И. В., Дойникова Е. В.** Система оценки уязвимостей CVSS и ее использование для анализа защищенности компьютерных систем // Защита информации. Инсайд. 2011. № 5. С. 54–60.
19. **Котенко И. В., Дойникова Е. В.** Анализ протокола автоматизации управления данными безопасности SCAP// Защита информации. Инсайд. 2012. № 2. С. 56–63.
20. **Common** Platform Enumeration (CPE). http://cpe.mitre.org (дата обращения: 05.06.2014).
21. **Open** Source Vulnerabilities Data Base (OSVDB). http://osvdb.org/about (дата обращения: 05.06.2014).

UDC 004.056

Open Vulnerability Bases and their Application in Security Analysis Systems of Computer Networks

Fedorchenko A. V.[a], Junior Researcher, fedorchenko@comsec.spb.ru
Chechulin A. A.[a], PhD, Tech., Senior Researcher, chechulin@comsec.spb.ru
Kotenko I. V.[a], Dr. Sc., Tech., Head of Laboratory of Computer Security Problems, ivkote@comsec.spb.ru
[a]Saint-Petersburg Institute of Informatics and Automation of RAS, 39, 14 Line, V. O., 199178, Saint-Petersburg, Russian Federation

Purpose: The amount of disclosed vulnerabilities in popular software and hardware stays high from year to year. At the same time, the lack of coordination between companies and communities which detect and classify vulnerabilities reduces the efficiency of vulnerability databases applicability in security analysis systems. The goal of the study is analyzing the open vulnerability bases and the assessment of their possible application in computer network security analysis systems, including the acquisition of statistic data and elicitation of the main trends in vulnerability detection. **Results:** Several open vulnerability databases (namely, CVE, NVD, X-Force and OSVDB) were analized and compared, as well as software/hardware dictionaries (like CPE) and vulnerability metrics (like CVSS). Statistic data were collected on disclosed vulnerabilities in popular operation systems and web browsers, showing the distribution of vulnerable products of the major software makers for the last 10 year. For the most popular products (from Microsoft, Google, Oracle, Apple, etc.), the general tendencies in detecting, publishing and patching vulnerabilities were displayed and discussed. **Practical relevance:** The analysis of vulnerability representation formats in open databases enables us to pick out the most significant attributes. This can help develop an approach to the integration of these databases, increasing the efficiency of their usage in security analysis systems for computer systems and networks.

Keywords — Information Security, Vulnerabilities, Vulnerability Databases, Tendencies of Vulnerabilities Detection, Security Analysis, Computer Attacks, Hardware and Software.

References

1. Kotenko I. V., Stepashkin M. V. Network Security Evaluation Based on Simulation of Malefactor's Behavior. *Proc. Int. Conf. "Security and Cryptography"*, Portugal, 2006, pp. 339–344.
2. Kotenko I. V., Stepashkin M. V., Bogdanov V. S. Architectures and Models of Active Vulnerabilities Analysis Based on Simulation of Malefactors' Actions. *Problemy informatsionnoi bezopasnosti. Komp'iuternye sistemy*, 2006, no. 2, pp. 7–24 (In Russian).
3. Ruiz J. F., Harjani R., Mana A., Desnitsky V., Kotenko I. V., Chechulin A. A. A Methodology for the Analysis and Modeling of Security Threats and Attacks for Systems of Embedded Components. *Proc. 20th Euromicro Int. Conf. "Parallel, Distributed and Network-Based Processing (PDP-2012)"*. Garching, Germany, 2012, pp. 261–268.
4. Kotenko I. V., Chechulin A. A. Common Framework for Attack Modeling and Security Evaluation in SIEM Systems. *Proc. IEEE Int. Conf. "Green Computing and Communications, Internet of Things, and Cyber, Physical and Social Computing"*. Besanson, France, 2012, pp. 94–101.
5. Chechulin A. A., Kotenko I. V. Combining Scanning Protection Mechanisms in Computer Networks. *Informatsionno-upravliaiushchie sistemy*, 2010, no. 6, pp. 21–27 (In Russian).
6. Kotenko I. V., Novikova E. S. Visual Analysis of Computer Network Security Assessment. *Informatsionno-upravliaiushchie sistemy*, 2013, no. 3, pp. 55–61 (In Russian).
7. *Komp'iuternaia bezopasnost': voprosy i resheniia* [The Computer Security: Answers and Solutions]. Available at: http://comp-bez.ru/?p=782 (accessed 5 June 2014).
8. *Common Vulnerabilities and Exposures (CVE)*. Available at: http://cve.mitre.org (accessed 5 June 2014).
9. *National Vulnerabilities Database (NVD)*. Available at: http://nvd.nist.gov (accessed 5 June 2014).
10. *Open Source Vulnerabilities Data Base (OSVDB)*. Available at: http://osvdb.org (accessed 5 June 2014).
11. *United States Computer Emergency Readiness Team (US-CERT)*. Available at: http://www.us-cert.gov (accessed 5 June 2014).
12. *BugTraq*. Available at: http://securityfocus.com (accessed 5 June 2014).
13. *X-Force*. Available at: http://xforce.iss.net (accessed 5 June 2014).
14. *Secunia*. Available at: http://secunia.com (accessed 11 October 2013).
15. *Vupen Security*. Available at: http://www.vupen.com (accessed 25 May 2014).
16. *Common Vulnerability Reporting Framework (CVRF)*. Available at: http://www.icasi.org/cvrf-1.1 (accessed 5 June 2014).
17. *Common Vulnerability Scoring System*. Available at: http://www.first.org/cvss (accessed 5 June 2014).
18. Kotenko I. V., Doynikova E. V. Vulnerabilities Scoring System CVSS and its Application for the Computer Systems Security Analysis. *Zashchita informatsii. Insaid*, 2011, no. 5, pp. 54–60 (In Russian).
19. Kotenko I. V., Doynikova E. V. SCAP Protocol Overview. *Zashchita informatsii. Insaid*, 2012, no. 4, pp. 54–66 (In Russian).
20. *Common Platform Enumeration (CPE)*. Available at: http://cpe.mitre.org (accessed 5 June 2014).
21. *Open Source Vulnerabilities Data Base (OSVDB)*. Available at: http://osvdb.org/about (accessed 5 June 2014).

УДК 681.3

ОТРИЦАЕМОЕ ШИФРОВАНИЕ НА ОСНОВЕ БЛОЧНЫХ ШИФРОВ

Н. А. Молдовян[а], *доктор техн. наук, заведующий лабораторией*
А. Р. Биричевский[а], *аспирант*
Я. А. Мондикова[б], *аспирантка*
[а]*Санкт-Петербургский институт информатики и автоматизации РАН, Санкт-Петербург, РФ*
[б]*Санкт-Петербургский государственный электротехнический университет «ЛЭТИ», Санкт-Петербург, РФ*

Постановка проблемы: *известные способы отрицаемого шифрования с разделяемым ключом, удовлетворяющие условию неотличимости по криптограмме от вероятностного шифрования, обладают сравнительно малой производительностью. Цель работы — повышение быстродействия алгоритмов отрицаемого шифрования, основанных на использовании блочных шифров.* ***Методы:*** *обращение блочного шифрующего преобразования, статистические эксперименты, одновременное шифрование двух независимых сообщений на двух различных ключах.* ***Результаты:*** *разработан новый способ выполнения процедуры отрицаемого шифрования, отличающийся от известных аналогов тем, что при зашифровании двух сообщений блочный шифр используется для выполнения прямого блочного преобразования по первому ключу и обратного преобразования по второму ключу. Получены формулы для оценки параметров алгоритмов на основе предложенного способа.* ***Практическая значимость:*** *предложенный способ представляет интерес для использования в средствах защиты информации от несанкционированного доступа.*

Ключевые слова *— компьютерная безопасность, криптография, отрицаемое шифрование, вероятностное шифрование, блочные шифры, криптограмма.*

Введение

В целях защиты информации от атак с принуждением предложены процедуры отрицаемого шифрования (ОШ) [1]. В атаках указанного типа предполагается, что атакующий перехватывает криптограмму и принуждает отправителя и получателя раскрыть исходное сообщение и использованные при шифровании ключи и случайные значения (если последние применялись). Различают ОШ по открытому ключу получателя сообщения и по разделяемому секретному ключу, которым владеют отправитель и получатель. При этом второй тип ОШ главным образом связывается с шифрованием двух и более сообщений на различных ключах и соединением независимых криптограмм в единый шифртекст. При принуждающей атаке предполагается достаточным предоставление атакующему только одного из ключей (фиктивного ключа) для расшифрования соответствующего ему участка шифртекста и восстановления фиктивного сообщения [1]. При этом оставшаяся часть шифртекста интерпретируется как случайная последовательность, использованная для маскирования криптограммы. Несмотря на явную наивность такого понимания ОШ по разделяемым секретным ключам, оно лежит в основе ряда средств компьютерной безопасности, например, Best Crypt [www.jetico.com/products/personal-privacy/bestcrypt-container-encryption], FreeOTFE [www.softpedia.com/get/Security/Encrypting/FreeOTFE.shtml], True Crypt [www.truecrypt.org].

Однако для защиты отдельных сообщений, которыми обмениваются удаленные пользователи, и отдельных файлов, хранимых в постоянной памяти ЭВМ, а также для построения защитных механизмов типа криптографических обманных ловушек [2], ориентированных на навязывание атакующему ложной информации, наивный подход к построению процедуры ОШ по разделяемому ключу представляется недостаточным. Действительно, наличие участков шифртекста, которые не используются для раскрытия фиктивного сообщения, дает атакующему существенные основания утверждать о неполноте раскрытия шифртекста. Устранение этого недостатка обеспечивается требованием неотличимости шифртекста, полученного в результате ОШ, от шифртекста, полученного в результате вероятностного шифрования фиктивного сообщения по фиктивному ключу, впервые обоснованным в работе [2] как одно из важных условий для обеспечения стойкости к принуждающим атакам.

В работе [3] описан общий способ построения алгоритмов ОШ, неотличимых по шифртексту от алгоритмов вероятностного шифрования, с использованием хэш-функций, а также представлен вариант реализации аналогичных алгоритмов с использованием блочных шифров. Однако недостатком способа [3] является сравнительно низкая производительность процедур ОШ, реализуемых на его основе.

В настоящей работе решается задача повышения производительности процедур ОШ, построенных на основе использования блочных шифров. Предложенный способ обеспечивает построение алгоритмов ОШ, обладающих в 100 и более раз высокой скоростью шифрования по сравнению с алгоритмами ОШ, построенными

на основе способа [3]. Существенный выигрыш в производительности достигается за счет того, что в процедуре ОШ блочный шифр используется не только в режиме шифрования, но и в режиме расшифрования.

Способ-прототип

Способ, предложенный в работе [3], позволяет любое трудно обратимое (однонаправленное) преобразование использовать для построения процедуры ОШ. В качестве однонаправленного преобразования рассматривались хэш-функции и блочные шифры. Отрицаемое шифрование предлагалось в виде одновременного шифрования двух сообщений (секретного и фиктивного) по двум независимым ключам, один из которых (фиктивный ключ) предназначен для раскрытия в случае принуждающей атаки. Способ легко расширяется на случай одновременного шифрования трех и более сообщений, однако при этом существенно падает производительность процедуры ОШ. Такое расширение интересно с теоретической точки зрения, но для практического применения его обоснование неочевидно, поэтому в дальнейшем будет рассмотрен только случай одновременного шифрования двух сообщений.

Важным требованием к процедурам ОШ является неотличимость криптограммы, формируемой в результате выполнения ОШ, от криптограммы, формируемой при вероятностном шифровании фиктивного сообщения. Это требование обеспечивается тем, что с алгоритмом ОШ ассоциируется некоторый алгоритм вероятностного шифрования (шифрования, в котором используются случайные значения) [2, 3]. Наряду с этим для последнего доказывается, что при определенных случайных значениях фиктивное сообщение в результате его шифрования по фиктивному ключу преобразуется в криптограмму, полученную в результате выполнения процедуры ОШ. При этом сама процедура ОШ также может быть как детерминистической, так и вероятностной. В последнем случае при выполнении процедуры ОШ используются случайные значения, которые определяют выработку конкретной криптограммы из множества возможных. В работе [3] предложен способ вероятностного ОШ, основанный на использовании односторонних преобразований, например хэш-функций.

В соответствии со способом [3] при использовании хэш-функции F_H процедура ОШ реализуется следующим образом. Пусть даны сообщения T (фиктивное) и M (секретное), представленные в виде последовательностей u-битовых знаков $\{t_1, t_2, ..., t_i, ..., t_z\}$ и $\{m_1, m_2, ..., m_i, ..., m_z\}$ соответственно. Одновременное шифрование этих сообщений по ключам K_T и K_M состоит в подборе таких случайных k-битовых значений $r_1, r_2, ..., r_i, ..., r_z$ ($k > 2u$), для которых одновременно выполняются соотношения

$$F_H(K_T, i, r_i) \bmod 2^u = t_i \text{ и } F_H(K_M, i, r_i) \bmod 2^u = m_i,$$

где предполагается использование хэш-функций, выходное значение которых имеет разрядность не менее u бит. Значение счетчика i включено в аргумент хэш-функции для улучшения статистических свойств криптограммы при сравнительно малых значениях k и u. Если последние два значения достаточно велики, то можно обойтись без задания зависимости значения хэш-функции от номера преобразуемого знака исходного текста.

В случае построения процедуры вероятностного ОШ на основе n-битового блочного шифра E ($n > 2u$) одновременное шифрование пары сообщений T и M по ключам K_M и K_T выполняется как подбор случайных значений r_i, удовлетворяющих следующим двум условиям:

$$E_{K_T}(r_i) \bmod 2^u = t_i \text{ и } E_{K_M}(r_i) \bmod 2^u = m_i. \quad (1)$$

Формируемая криптограмма имеет вид $R = \{r_1, r_2, ..., r_i, ..., r_z\}$. Расшифрование выполняется по формуле $E_K(r_i) \bmod 2^u = q_i$, где q_i — знаки восстановленного текста (T или M при $K = K_T$ или $K = K_M$ соответственно). При использовании блочных шифров обеспечивается более высокая скорость ОШ по сравнению со случаем использования хэш-функций. Однако по сравнению с производительностью $\lambda_{б.ш}$ [бит/с] блочного алгоритма шифрования E достигаемая скорость ОШ $\lambda_{ОШ}$ существенно меньше:

$$\lambda_{ОШ} \approx (2^{-2u-1}u/n)\lambda_{б.ш}. \quad (2)$$

Наиболее существенный вклад в снижение скорости шифрования при выполнении процедуры ОШ вносит необходимость многократного вычисления значений $E_{K_T}(r_i)$ и $E_{K_M}(r_i)$ для подбора такого r_i, при котором одновременно выполняются соотношения (1). Действительно, для текущего случайного значения r_i вероятность выполнения каждого из двух условий (1) равна 2^{-u}, а вероятность их одновременного выполнения — 2^{-2u}.

Существенное повышение производительности процедуры ОШ, основанной на выполнении шифрующих блочных преобразований, может быть достигнуто использованием свойства обратимости функции блочного шифрования E, которое принципиально отличает блочные шифры от хэш-функций. Однако для эксплуатации этого свойства требуется использовать в качестве знаков криптограммы выходные значения функции E, а не входные, как это имеет место в способе [3]. Предлагаемый новый вариант построения процедур ОШ на основе блочных шифров описывается в следующем разделе.

Новый способ отрицаемого шифрования

Предлагаемый способ ОШ реализуется как выполнение процедуры одновременного шифрования сообщений T и M в соответствии с формулами

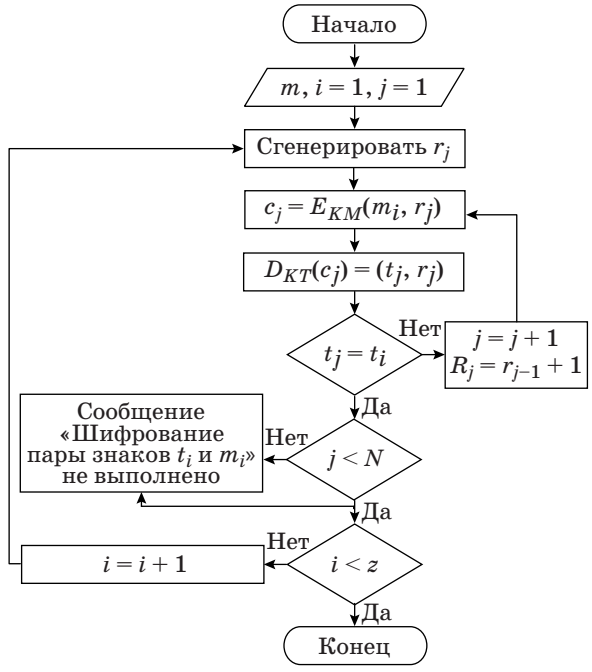
$$E_{K_T}(t_i, r_i') = c_i \text{ и } E_{K_M}(m_i, r_i) = c_i, \qquad (3)$$

где c_i — n-битовые блоки (знаки) криптограммы; r_i' и r_i — случайные значения. Восстановление знаков исходных сообщений из криптограммы $C = \{c_1, c_2, ..., c_i, ..., c_z\}$ предполагается осуществлять по формулам

$$D_{K_T}(c_i) = (t_i, r_i') \text{ и } D_{K_M}(c_i) = (m_i, r_i), \qquad (4)$$

где D — функция расшифрования, обратная к функции E, т. е. $D = E^{-1}$, а случайные k-битовые значения r_i' и r_i в выходном значении функции D отбрасываются ($k \geq 2u$; $n = u + k$), в результате чего получают знаки t_i и m_i. В соответствии с (3) процедура ОШ требует нахождения двух случайных значений r_i' и r_i, которые обеспечивают выполнимость условия $E_{K_T}(t_i, r_i') = E_{K_M}(m_i, r_i)$. Для случайно выбранных значений r_i' и r_i вероятность выполнения последнего равенства имеет достаточно малое значение $2^{-n} << 2^{-2u}$, что ограничивает скорость ОШ при использовании непосредственного подбора пар случайных значений r_i' и r_i.

Существенный выигрыш в производительности ОШ достигается применением следующего варианта нахождения блока криптограммы c_i по значениям t_i и m_i, обеспечивающего выполнение условий (3) и лежащего в основе алгоритма 1 (рис. 1). Предварительно выбирается произвольное значение r_j и вычисляется значение $c_j = E_{K_M}(m_i, r_j)$, затем — значение $D_{K_T}(c_j)$, которое рассматривается как конкатенация u-битового значения t_j и k-битового значения r_j', т. е. $D_{K_T}(c_j) = (t_j, r_j')$. При нахождении такого значения r_j, при котором $t_j = t_i$, полученное значение c_j может быть взято в качестве блока криптограммы c_i. При этом вероятность выполнения равенства $t_j = t_i$ (совпадение случайного u-битового значения t_j с заданным u-битовым значением t_i) равна $2^{-u} >> 2^{-2u}$, что определяет существенное повышение скорости ОШ по сравнению со способом [3].



■ ***Рис. 1.*** Блок-схема разработанного алгоритма ОШ

Алгоритм 1: совместное шифрование сообщений T и M.

1. Установить значение счетчика $i = 1$.
2. Установить значение счетчика $j = 1$.
3. Сгенерировать случайное k-битовое число r_j.
4. Вычислить значение $c_j = E_{K_M}(m_i, r_j)$.
5. Вычислить значение $D_{K_T}(c_j) = (t_j, r_j')$, где выходное n-битовое значение функции расшифрования интерпретируется как конкатенация u-битового значения t_j и k-битового значения r_j'.
6. Сравнить значения t_j и t_i. Если $t_j = t_i$, то взять в качестве значения c_i значение c_j и перейти к шагу 7, в противном случае перейти к шагу 3.
7. Если $j < N$, то прирастить значение счетчика $j \leftarrow j + 1$, вычислить $r_j \leftarrow r_{j-1} + 1$ и перейти к шагу 4, иначе вывести сообщение «Шифрование пары знаков t_i и m_i не выполнено». (Вопрос о выборе значения N рассмотрен в следующем разделе.)
8. Если $i < z$, то прирастить значение счетчика $i \leftarrow i + 1$ и перейти к шагу 2, иначе СТОП.

Алгоритм 1, описывающий процедуру ОШ, формирует выходную криптограмму C, которая вычислительно неотличима от криптограммы, полученной в процессе следующего алгоритма вероятностного шифрования фиктивного сообщения. Данный алгоритм относится к вероятностным процедурам ОШ, в которых в ходе шифрования используются случайные значения.

Алгоритм 2: ассоциируемый алгоритм вероятностного шифрования фиктивного сообщения M по фиктивному ключу K_M.

1. Установить значение счетчика $i = 1$.
2. Сгенерировать случайное k-битовое число r_i.
3. Вычислить значение $c_i = E_{K_M}(m_i, r_i)$.
4. Если $i < z$, то прирастить значение счетчика $i \leftarrow i + 1$ и перейти к шагу 2, иначе СТОП.

Наличие алгоритма 2 явно показывает, что алгоритм 1 удовлетворяет требованию неотличимости ОШ от вероятностного шифрования. Действительно, потенциально реализуем выбор случайных значений r_i, при котором выходная криптограмма алгоритма 2 совпадает с выходной криптограммой алгоритма 1 (при одних и тех же значениях M и K_M).

Алгоритм 3: расшифрование криптограммы C по ключу K.

1. Установить ключ шифрования $K = K_M$ (восстановление фиктивного сообщения M) или $K = K_T$ (восстановление секретного сообщения T) и значение счетчика $i = 1$.

2. Вычислить значение $\chi_i = D_K(c_i) \operatorname{div} 2^k$.

3. Если $i < z$, то прирастить значение счетчика $i \leftarrow i + 1$ и перейти к шагу 2, иначе СТОП.

Алгоритм 3 выдает выходное сообщение $\{\chi_1, \chi_2, ..., \chi_i, ..., \chi_z\}$, которое совпадает с фиктивным сообщением M, если было установлено значение ключа $K = K_M$, или с секретным сообщением T, если было установлено значение ключа $K = K_T$.

Описанные алгоритмы 1, 2 и 3 реализуют передачу секретного сообщения T между удаленными пользователями, которые предварительно согласовывают общий секретный ключ K_T и общий фиктивный ключ K_M по следующему сценарию, стойкому к принуждающей атаке.

1. Алиса (отправитель) генерирует фиктивное сообщение M, после чего, используя алгоритм 1 и ключи K_T и K_M, зашифровывает совместно сообщения T и M и полученную криптограмму C направляет по открытому каналу Бобу (получателю).

2. Боб расшифровывает криптограмму C, используя алгоритм 3 и ключ K_T, и получает секретное сообщение T.

3. Ева (атакующий), имеющая возможность наблюдать за трафиком открытого канала, перехватывает криптограмму C, после чего принуждает одновременно Алису и Боба раскрыть сообщение, содержащееся в криптограмме C, и ключ шифрования.

4. Алиса (и Боб) предоставляют Еве ключ K_M и алгоритм 2 как алгоритм, использованный для зашифрования переданного (полученного) сообщения, и алгоритм 3 как алгоритм для расшифрования сообщения.

5. Ева расшифровывает криптограмму C, используя алгоритм 3 и ключ K_M, в результате чего получает сообщение M. После этого Ева зашифровывает сообщение M по ключу K_M в соответствии с алгоритмом 2, используя случайные k-битовые значения r_i, восстановленные при расшифровании криптограммы C, и убеждается, что сообщение M действительно преобразуется в криптограмму C.

Для того чтобы уличить Алису и Боба в обмане, Ева должна взломать базовый алгоритм блочного шифрования, т. е. вычислить ключ K_T, что практически невыполнимо, если разрядность этого ключа составляет 128 бит и более, а в качестве базового алгоритма используется стойкий блочный шифр, например ГОСТ 28147 [4].

Выбор параметров и оценка производительности алгоритма отрицаемого шифрования

Производительность алгоритма, описанного в предыдущем разделе, существенно зависит от среднего числа η выбираемых значений r_j при шифровании одной пары знаков t_i и m_i. Значение η зависит от вероятности выполнения на шаге 6 условия $t_j = t_i$, которая равна $\Pr(t_j = t_i) = 2^{-u}$ и определяется разрядностью знаков t_i и m_i. Вероятность невыполнения условия $t_j = t_i$ для μ последовательных значений $j = 1, 2, ..., \mu$ равна

$$\Pr_\mu(t_j \neq t_i) = (1 - 2^{-u})^\mu, \qquad (5)$$

откуда получаем значение вероятности выполнения условия $t_j = t_i$ на μ-м шаге

$$\Pr_\mu(t_j = t_i) = 1 - (1 - 2^{-u})^\mu \qquad (6)$$

и значение η:

$$\eta = 2^{-u} + 2[1 - (1 - 2^{-u})^2] + ... + \\ + \mu[1 - (1 - 2^{-u})^\mu] + ... + N[1 - (1 - 2^{-u})^N].$$

Более удобной является приближенная формула

$$\eta \approx [\Pr(t_j = t_i)]^{-1} = 2^u, \qquad (7)$$

с помощью которой получаем следующую оценку производительности предложенного алгоритма ОШ:

$$\lambda'_{\text{ОШ}} \approx (2^{-u-1}u/n)\lambda_{\text{б.ш}}. \qquad (8)$$

Сравнение с формулой (2), относящейся к ОШ по способу [3], показывает, что предложенный вариант реализации процедуры ОШ на основе блочных шифрующих преобразований дает увеличение производительности ОШ примерно в 2^u раз.

Значение N в предложенном алгоритме выбирается с учетом получения достаточно малого значения $\Pr_N(t_j \neq t_i)$, т. е. вероятности того, что шифрование текущей пары знаков t_i и m_i не будет выполнено. Из формулы (5) получаем уравнение для вычисления N по заданному значению $\Pr_N(t_j \neq t_i)$:

$$\Pr_N(t_j \neq t_i) = (1 - 2^{-u})^N . \qquad (9)$$

Оценим порядок некоторого значения $N' > N > \eta$, для чего подставим в (5) значение $\mu = \eta/2 \approx 2^{u-1}$ и воспользуемся соотношением

$$\Pr_\mu(t_j \neq t_i) < 1 - \mu 2^{-u} = 1 - 2^{u-1}2^{-u} = 1/2. \qquad (10)$$

Обозначая целую часть отношения $N'/(\eta 2^{-1})$ как некоторое натуральное число ω, получаем

$$\Pr_{N'}(t_j \neq t_i) < (1/2)^\omega = (1/2)^{2N'/\eta}. \qquad (11)$$

Задавая пороговое значение вероятности $\Pr_{N'}(t_j \neq t_i)$ в виде отрицательной степени s числа 2, легко вычислить N':

$$2^{-s} > 2^{-N'/\eta} \Rightarrow N' \geq s\eta = s2^{u-1}. \qquad (12)$$

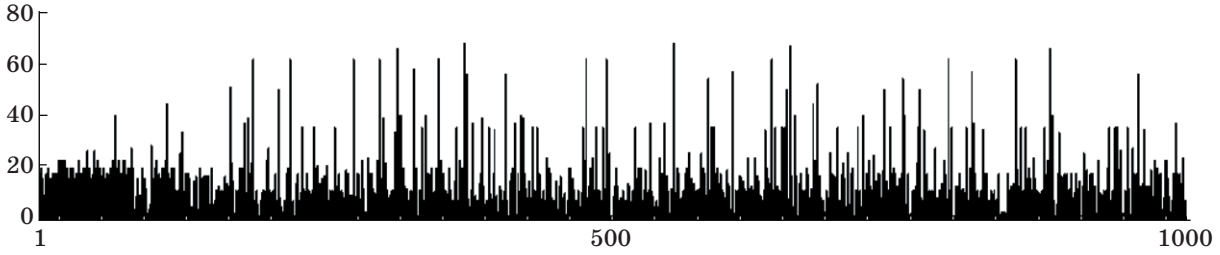
Последнее значение может быть использовано в качестве значения N в алгоритме 1, задающем процедуру ОШ. Выбор больших значений параметра N в алгоритме 1 практически не влияет на его производительность, поскольку случаи, когда требуется выполнить число попыток выбора значения r_j, существенно превосходящее значение η, встречаются сравнительно редко.

Типичная зависимость количества выборок значений r_j от номера шифруемого блока при значении параметра $u = 4$ показана на рис. 2. Из графика видно, что большинство значений лежит в пределах 20 выборок на блок. Среднее число η выборок значений r_j, определенное экспериментально для различных режимов ОШ, близко к теоретическим значениям, вычисляемым по формуле (7).

Значение параметров u и n следует выбирать таким образом, чтобы число N_r всех возможных случайных значений r превосходило N, для чего достаточно выполнения неравенства $N_r > N'$. Поскольку $N_r = 2^k$, последнее неравенство выполняется при $2^k > 2^u \log_2 \Pr_{N'}(t_j \neq t_i)$. Варианты выбора параметров алгоритма ОШ, представляющие практический интерес, приведены в табл. 1.

Экспериментальная проверка эффективности работы разработанного способа отрицаемого шифрования была выполнена на базе программной платформы Microsoft .NET Framework. Результаты измерений скорости шифрования приведены в табл. 2.

Производительность предложенного способа ОШ прямо пропорциональна производительности используемого алгоритма блочного шифрования. Современные аппаратные реализации алгоритма ГОСТ 28147 обеспечивают производительность 1000 Мбит/с и более. При таких реализациях



■ ***Рис. 2.*** Зависимость количества выборок значений r_j от значения i при использовании алгоритма ГОСТ 28147 в качестве базового блочного шифра и параметров $u = 4$, $k = 60$

■ ***Таблица 1.*** Варианты выбора параметров алгоритма ОШ и оценка достигаемой скорости шифрования ($\lambda'_{ОШ}$)

n	u	k	η	$\Pr_{N'}(t_j \neq t_i)$ (s)	N'	N_r	$\lambda'_{ОШ}$, отн. ед.
32	4	28	2^4	2^{-16} (2^4)	2^7	2^{28}	2^{24}
32	8	24	2^8	2^{-16} (2^4)	2^{11}	2^{24}	2^{21}
64	8	56	2^8	2^{-32} (2^5)	2^{12}	2^{56}	2^{20}
64	8	56	2^8	2^{-64} (2^6)	2^{13}	2^{56}	2^{20}
96	8	88	2^8	2^{-32} (2^5)	2^{12}	2^{88}	2^{20}
96	12	84	2^{12}	2^{-64} (2^6)	2^{17}	2^{84}	2^{16}
128	16	112	2^{16}	2^{-64} (2^6)	2^{21}	2^{112}	2^{12}

■ ***Таблица 2.*** Результаты измерений скорости шифрования алгоритма ОШ при использовании в качестве базового алгоритма блочного шифрования шифров RC5 [5] и ГОСТ 28147 [4]

Режим работы алгоритма ОШ	Производительность алгоритма 1: эксперимент/формула (8), бит/с	Значение η: эксперимент/формула (7)	Производительность базового шифра, бит/с
$n = 32$, $u = 8$, $k = 24$ (бит); базовый шифр — RC5	1150/1360	257/256	2 728 211
$n = 32$, $u = 4$, $k = 28$ (бит); базовый шифр — RC5	10260/10920	14/16	2 728 211
$n = 64$, $u = 8$, $k = 56$ (бит); базовый шифр — ГОСТ 28147	1176/1000	240/256	4 093 953
$n = 64$, $u = 4$, $k = 60$ (бит); базовый шифр — ГОСТ 28147	9627/8000	15/16	4 093 953

производительность ОШ на базе ГОСТ 28147-89 будет достигать значения 6,3 Мбит/с.

Также ощутимое влияние на скорость ОШ оказывает значение параметра u. Однако повышение быстродействия за счет уменьшения значения u ограничивается тем, что при этом возрастает отношение размера криптограммы к размеру шифруемых сообщений. По сравнению со способом ОШ [3], основанным на использовании блочных шифров, алгоритм 1 обладает производительностью в $\psi \approx 2^u$ раз более высокой при использовании одного и того же базового блочного шифра. Значение коэффициента ψ равно 16 при $u = 4$ и 256 при $u = 8$.

Заключение

Впервые алгоритмы ОШ, удовлетворяющие требованию неотличимости от вероятностного шифрования, предложены в работе [2] с использованием операций возведения в большую дискретную степень по простому модулю. При таком подходе к построению алгоритмов ОШ требуется выполнение самостоятельных исследований их стойкости. В работе [3] впервые предложено построение алгоритмов ОШ указанного типа с использованием известных хэш-функций и алгоритмов блочного шифрования, стойкость которых хорошо исследована. Основной результат настоящей работы состоит в разработанном новом способе ОШ, удовлетворяющего требованию неотличимости от вероятностного шифрования и основанного на использовании блочных шифров. Предложенный способ позволяет построить алгоритмы ОШ, производительность которых существенного выше (в 16 раз и более) по сравнению с алгоритмами, основанными на способе [3]. Применение стойких блочных шифров для реализации предложенного способа ОШ обеспечивает стойкость разрабатываемых на его основе алгоритмов ОШ. Действительно, гипотетическая успешная атака на такие алгоритмы ОШ, например атака на основе известных или специально подобранных исходных текстов, может быть применена и для взлома базового алгоритма шифрования.

Другим результатом выполненной работы является получение формул для оценки значений параметров алгоритма ОШ, основанного на предложенном способе. Из данных табл. 1 видно, что производительность не зависит от выбираемого значения N, что объясняется малой вероятностью случаев, когда процесс шифрования пары знаков исходных тестов t_i и m_i потребует выполнения N циклов, включающих шаги 3–6 алгоритма ОШ, если задано малое значение вероятности $\Pr_N(t_j \neq t_i)$. Экспериментом подтверждено, что среднее число (η) выбираемых значений r_j много меньше значения N.

В качестве базового алгоритма блочного шифрования E представляет интерес использование 64-битовых скоростных шифров с высокой эффективностью аппаратной реализации [6–8], что позволит достигнуть производительности ОШ, равной 10–100 Мбит/с. Более высокая производительность достигается при использовании блочных шифров с малым размером входного блока n, однако использование значений $n < 32$ требует решения задачи разработки режимов использования ОШ, обеспечивающих улучшение маскирования статистических свойств исходных текстов. Последнее представляет самостоятельную задачу отдельного исследования.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 14-07-00061-а.

Литература

1. **Canetti R., Dwork C., Naor M., Ostrovsky R.** Deniable Encryption // Advances in Cryptology — CRYPTO 1997: Proc.17th Annual Intern. Cryptology Conf., Santa Barbara, California, USA, Aug. 17–21, 1997. P. 90–104.
2. **Березин А. Н., Биричевский А. Р., Молдовян Н. А., Рыжков А. В.** Способ отрицаемого шифрования // Вопросы защиты информации. 2013. № 2. С. 18–21.
3. **Морозова Е. В., Мондикова Я. А., Молдовян Н. А.** Способы отрицаемого шифрования с разделяемым ключом // Информационно-управляющие системы. 2013. № 6. С. 73–78.
4. **ГОСТ** 28147–89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. — М.: Изд-во стандартов, 2007. — 28 с.
5. **Rivest R. L.** The RC5 Encryption Algorithm // Fast Software Encryption: Proc. 2nd Int. Workshop. 1995. Vol. 1008. P. 86–96.
6. **Moldovyan N. A., Moldovyan A. A.** Data-Driven Block Ciphers for Fast Telecommunication Systems. Auerbach Publications. — N. Y.; London: Talor & Francis Group, 2008. — 185 p.
7. **Moldovyan N. A., Moldovyan A. A., Eremeev M. A.** A Class of Data-Dependent Operations // International Journal of Network Security. 2006. Vol. 2. N 3. P. 187–204.
8. **Moldovyan N. A., Moldovyan A. A., Sklavos N.** Controlled Elements for Designing Ciphers Suitable to Efficient VLSI Implementation // Telecommunication Systems. 2006. Vol. 32. N 2/3. P. 149–163.

UDC 681.3

Deniable Encryption Based on Block Ciphers

Moldovyan N. A.[a], Dr. Sc., Tech., Head of a Research Laboratory, Professor, nmold@mail.ru
Birichevskiy A. R.[a], Post-Graduate Student, lehabirich@mail.ru
Mondikova Ya. A.[b], Post-Graduate Student, mondikovay@gmail.com
[a]Saint-Petersburg Institute for Informatics and Automation of RAS, 39, 14 Line, V. O., 199178, Saint-Petersburg, Russian Federation
[b]Saint-Petersburg State Electrotechnical University "LETI", 5, Professora Popova St., 197376, Saint-Petersburg, Russian Federation

Purpose: The available methods of shared-key deniable encryption satisfying the criterion of indistinguishability from probabilistic encryption have comparatively low performance. This paper is devoted to developing a method for faster deniable encryption based on using block ciphers. **Methods:** Reversing the block-ciphering transformation, statistic experiments, simultaneous encryption of two independent messages using two different keys. **Results:** A new method was developed to carry out deniable encryption by performing direct block transformation with the first key and inverse block transformation with the second key when encrypting two messages. The formulas were derived to estimate the parameters of the algorithms based on the proposed method. **Practical relevance:** The proposed method can be applied in computer security systems.

Keywords — Computer Security, Cryptography, Deniable Encryption, Probabilistic Encryption, Block Ciphers, Cryptogram

References

1. Canetti R., Dwork C., Naor M., Ostrovsky R. Deniable Encryption. *Advances in Cryptology — CRYPTO 1997*. Proc. 17th Annual Intern. Cryptology Conf., 1997, pp. 90–104.
2. Birichevskiy A. R., Moldovyan N. A., Berezin A. N., Ryzhkov A. V. A Method of the Deniable Encryption. *Voprosy zashchity informatsii*, 2009, no. 2, pp. 18–21 (In Russian).
3. Morozova E. V., Mondikova Y. A., Moldovyan N. A. Methods of Deniable Encryption with a Shared Key. *Informatsionno-upravliaiushchie sistemy*, 2013, no. 6, pp. 73–78 (In Russian).
4. Russian Standard GOST 28147–89. Systems for Processing Information. Cryptographic Protection. Algorithm for Cryptographic Transformation. Moscow, Standartov Publ., 2007. 28 p. (In Russian).
5. Rivest R. L. The RC5 Encryption Algorithm. *Proc. 2nd Int. Workshop "Fast Software Encryption"*, 1995, vol. 1008, pp. 86–96.
6. Moldovyan N. A., Moldovyan A. A. Data-driven Block Ciphers for Fast Telecommunication Systems. Auerbach Publications. New York, London, Talor & Francis Group, 2008. 185 p.
7. Moldovyan N. A., Moldovyan A. A., Eremeev M. A. A Class of Data-dependent Operations. *International Journal of Network Security*, 2006, vol. 2, no. 3, pp. 187–204.
8. Moldovyan N. A., Moldovyan A. A., Sklavos N. Controlled Elements for Designing Ciphers Suitable to Efficient VLSI Implementation. *Telecommunication Systems*, 2006, vol. 32, no. 2/3, pp. 149–163.

УДК 621.396:621.391.26

КОРРЕЛЯЦИОННЫЕ ХАРАКТЕРИСТИКИ НЕКОТОРЫХ БИНАРНЫХ R4-КОДОВ И АНСАМБЛЕЙ СИГНАЛОВ НА ИХ ОСНОВЕ

Ю. В. Чепруков[а], *канд. техн. наук*
М. А. Соколов[б], *доктор техн. наук, профессор*
[а]*Российский государственный университет туризма и сервиса, филиал в г. Сочи, РФ*
[б]*Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, РФ*

Введение: *постоянное повышение эффективности различных систем управления и связи возможно при использовании более совершенных бинарных кодов и систем сигналов на их основе. Известные N элементные бинарные коды, используемые в упомянутых системах, не позволяют получить достаточно низкий уровень боковых пиков автокорреляционной и взаимной корреляционной функций совокупности кодов при вариации N в широких пределах. Целью работы является исследование вопросов синтеза N элементных бинарных кодов с заданными уровнями R и W боковых пиков автокорреляционной и взаимной корреляционной функций.* ***Результаты:*** *приведена таблица результатов синтеза кодов с R = 4 при N ≤ 32. Изложена в общем виде методика и особенности синтеза ансамблей бинарных кодов с заданным уровнем W боковых пиков взаимной корреляционной функции. Выдвинуты гипотезы и составлены модели, позволившие получить аналитические оценки количественных характеристик таких наборов кодов, приведен пример.* ***Практическая значимость:*** *возможно использование в системах управления и связи. Выдвинута идея шифрования с помощью этих кодов. Указана потенциальная возможность создания «тихих» компьютеров и компьютерных сетей, что может позже привести к разработке «тихого» Интернета.*

Ключевые слова *— ансамбли, системы сигналов, бинарные коды, автокорреляционная функция, уровень боковых пиков.*

Введение

В современных системах управления, связи и радиолокации широко используются шумоподобные сигналы (ШПС). Разновидностью ШПС являются фазоманипулированные сигналы [1], которые характеризуются бинарными кодовыми последовательностями, или просто кодами. Примером систем, в которых используются указанные сигналы, являются системы связи с кодовым разделением абонентов. Главным вопросом является выбор сигналов. Под системой понимается множество сигналов, определяемых единым правилом их построения [1]. Обозначим базу ШПС B^*. Число сигналов в системе L называют объемом системы сигналов. Система считается малой, когда $L = \sqrt{B^*} << B^*$, нормальной при $L \approx B^*$ и большой при $L >> B^*$. Существует нерешенная проблема разработки алгоритмов построения систем фазоманипулированных сигналов [1]. Примером малой системы являются функции Уолша, используемые в CDMA (Code Division Multiple Access — системы с кодовым разделением каналов) [2]. Представлены требования к системам сигналов для CDMA, которые сформулированы в виде минимаксного критерия качества. Системы сигналов, удовлетворяющие таким условиям, названы оптимальными. К ним отнесены, например, ансамбли Голда, Касами, Камалетдинова. В работе [3] отмечен недостаток упомянутых систем, заключающийся в сильной разреженности значений длин кодов ($N = 2^n - 1 = 3, 7, 15, 31, 63, 127...$; $n = 2, 3, ...$), что ограничивает их применение. Указанные системы основаны на M-последовательностях, характеристики которых изложены в работах [1, 3]. Из них следует, что минимальное значение уровня боковых пиков (УБП) автокорреляционной функции (АКФ) $B_1 \approx (0{,}7...1{,}25)/\sqrt{N}$, а УБП взаимной корреляционной функции (ВКФ) $B_2 \approx (1{,}4...5)/\sqrt{N}$. Используемый для исследований математический аппарат — поля Галуа. В монографии [4] дана классификация ансамблей и методов синтеза, указаны проблемы применения известных методов. Например, при синтезе ансамблей кодов на основе полей Галуа сейчас применяются таблицы полиномов первой половины прошлого века.

Вопросы синтеза кодовых последовательностей при наличии требований к периодической АКФ и ВКФ изложены в работе [5]. Однако предложенные варианты решения не предназначены для синтеза одиночных бинарных кодов и ансамблей.

Таким образом, вопросы синтеза ансамблей сигналов актуальны для широкого класса коммуникационных систем, но недостаточно исследованы.

В работе [6] сформулирована задача, предложен метод решения, представлены результаты синтеза для $R = 2{,}3$; $N \le 25$. Показаны существенные преимущества синтезированных кодов по сравнению с M-последовательностями.

Коды с $R = 1$ (коды Баркера) и коды с $R = 2;3$ ($R2$- и $R3$-коды) составляют подмножества $R4$-кодов

(согласно данному ниже определению), для них $R = 4$.

Краткий обзор литературы, проведенный в работе [7], показал, что сейчас в различных системах используются в основном давно предложенные и подробно изученные сигналы. Там же представлены результаты синтеза $R2$-кодов. Они эффективнее лучших кодов Баркера по относительному УБП в 14/13 раза, позволяют получить разнообразные коэффициенты сжатия (22 варианта) и количество кодов 480 достаточно велико. Составлена таблица $R2$-кодов. Обосновано предположение, что $N = 28$ соответствует максимальному порядку $R2$-кодов.

В данной работе получены $R4$-коды для $N \le 32$. Выполнен анализ их корреляционных характеристик, показаны возможности синтеза множества ансамблей сигналов.

Назовем бинарные коды, АКФ которых в области боковых пиков может изменяться в пределах $\pm R$ ($0 \le R \le N - 1$, R — целое), R-кодами. Они составляют множество $G_{R,N}$. Пусть $B_3 = R/N$ — относительная величина УБП АКФ кодов, а T — длительность каждого из N импульсов. Тогда можно обозначить

$$\left\{G^i_{R,N}\right\} = \left\{P^i_j,\ j = \overline{1,N}\right\},\ P^i_j = \pm 1,\ i = \overline{1, g_{R,N}} \qquad (1)$$

множество бинарных последовательностей условных значений начальных фаз $P^i_j = \pm 1$ импульсов, которые соответствуют R-кодам [6, 7], количество которых равно $g_{R,N}$. Здесь P^i_j — коэффициенты последовательностей, причем индексы i, j определяют, соответственно, порядковый номер последовательностей и различные элементы каждой из них. Совокупности R-кодов будем называть W-ансамблями, если значения ВКФ всевозможных пар кодов изменяются в пределах $\pm W (1 \le W \le N - 1$, W — целое). Эти совокупности составляют системы сигналов, если обладают свойствами, упоминавшимися выше. Цель работы — получить $R4$-коды (найти $G_{4,N}$ и $g_{4,N}$) для $N \le 32$, построить W-ансамбли, провести анализ их характеристик, высказать предложения по применению.

Задача и методика синтеза, особенности решения

Введем для R-кодов функции $S^*(t)$ и $S(t)$, которые определяют, соответственно, АКФ и его модуль. В моменты $t_k = kT$, отсчитываемые от начала АКФ, эти функции принимают экстремальные или нулевые значения, причем $S(t_N) = N$. Аналогично введем $V_{x,y}(t)$ для модуля ВКФ $R4$-кодов с индексами «x» и «y» (пояснения даны ниже). Эти функции также будем рассматривать в моменты $t_k = kT$, отсчитываемые от начала ВКФ. Тогда задача синтеза заключается в определении коэффициентов кодов, для которых выполняются неравенства [6, 7]

$$S(t_k) = \left|\sum_{j=1}^{k} P^i_j \cdot P^i_{N+j-k}\right| \le R;$$

$$k = \overline{1, N-1},\ i = \overline{1, g_{4,N}}. \qquad (2)$$

После решения получим $R4$-коды, которые можно пронумеровать (1, ..., $g_{4,N}$) и составить множество $G_{4,N}$. Коды из этого множества включаются в W-ансамбль, если для совокупности пар кодов выполняются условия

$$V_{x,y}(t_k) = \left|\sum_{j=1}^{k} P^x_j \cdot P^y_{N+j-k}\right| \le W;\ k = \overline{1, 2 \cdot N - 1}, \qquad (3)$$

где x, y ($x \ne y$) — номера (индексы) $R4$-кодов из множества $G_{4,N}$. Обозначим $H(N, R, W)$ количество W-ансамблей, но объем кодов в них может быть различным, поэтому введем величину $H(N, R, W, J)$, где J — численность каждой из систем сигналов, $J = 2$, ..., $g_{R,N}$. Следовательно, общее количество W-ансамблей равно сумме количества ансамблей численностью ($J1$, $J2$ ...): $H(N, R, W) = (H(N, R, W, J1) + H(N, R, W, J2) + ...)$. Примеры использования этих параметров даны ниже. Итак, задача синтеза (2), (3) решается в два этапа.

Этап 1: рассматривается система неравенств (2) и в соответствии с работами [6, 7] определяются $R4$-коды в количестве $g_{4,N}$, составляющие множество $G_{4,N}$. Перейдем к полученным результатам этапа 1.

Результаты синтеза $R4$-кодов

Некоторые результаты синтеза $R4$-кодов для $6 \le N \le 32$ представлены в табл. 1. Использован метод упорядоченного перебора [7]. Указаны коды с первым коэффициентом (+1) (прямые коды). Имеются в том же количестве коды с противоположными знаками всех коэффициентов, но их АКФ одинаковы. Прочерки во второй колонке означают, что для $N = 25$, ..., 30 общее количество кодов $g_{4,N}$ не определялось, но даны примеры. В первой и второй колонках указаны значения N и количество $R4$-кодов, а в третьей колонке — кодовые последовательности и половины их АКФ (в круглых скобках), так как они симметричны относительно максимума. Вычисления выполнены на общедоступном персональном компьютере, программы составлены на языке QBasic.

■ *Таблица 1*

N	$g_{4,N}$	$\{P_{i,j}\}$; ($S^*(t_k)$, $k = 1, \ldots, N$)
6	30	1,1,–1,–1,1,1; (1,2,–1,–4,1,6). 1,–1,–1,1,1,–1; (–1,2,1,–4,–1,6)
7	65	1,1,–1,–1,–1,1,1; (1,2,–1,–4,–3,2,7). 1,1,1,–1,–1,–1,1; (1,0,–1,–4,–1,2,7)
8	104	1,1,–1,–1,–1,–1,1,1; (1,2,–1,–4,–3,–2,3,8). 1,1,1,1,1,1,–1,1; (1,0,1,2,3,4,3,8)
9	194	1,1,1,1,–1,1,1,1,1; (1,2,3,4,1,2,3,4,9)
10	334	1,1,1,1,–1,1,–1,1,1,1; (1,2,3,2,1,0,–1,4,1,10)
11	616	1,1,1,1,–1,1,1,–1,1,1,1; (1,2,3,2,1,2,1,4,1,2,11)
12	936	1,1,1,1,–1,1,–1,–1,1,1,1,1; (1,2,3,4,1,0,–1,–4,1,2,3,12)
13	1672	1,1,1,1,1,–1,–1,1,–1,1,1,1,1; (1,2,3,4,3,2,–1,–2,–3,2,3,4,13)
14	2582	1,–1,1,1,1,–1,–1,1,–1,1,1,1,1,1; (1,0,1,2,3,0,3,–2,–1,0,1,2,1,14)
15	4130	1,1,–1,1,1,1,–1,–1,1,–1,1,1,1,1,1; (1,2,1,2,3,2,1,2,–3,0,1,2,1,2,15)
16	6170	1,1,1,1,1,1,–1,1,–1,–1,1,1,1,–1,1,1; (1,2,1,2,3,4,1,0,3,–4,1,2,3,2,3,16)
17	10202	1,1,1,–1,1,1,1,–1,–1,1,–1,1,1,1,1,1,1; (1,2,3,2,3,4,3,2,–1,2,–3,2,3,2,3,4,17)
18	13458	1,1,1,–1,1,1,1,1,–1,1,–1,–1,1,1,–1,–1,1,1; (1,2,1,–2,–1,4,3,–2,–3,0,3,–2,3,4,1,–4,1,18)
19	20316	1,1,1,1,1,–1,1,–1,1,1,–1,–1,1,1,–1,1,1,1,1; (1,2,3,4,3,2,3,0,–1,4,–1,0,1,0,3,4,1,2,19)
20	27490	1,1,1,1,1,1,–1,–1,1,1,–1,–1,1,–1,1,–1,1,1,1,1; (1,2,3,4,3,4,1,0,–1,–2,1,0,–1,–4,1,4,1,2,3,20)
21	41320	1,1,1,1,1,1,–1,1,–1,–1,1,1,–1,–1,–1,1,–1,1,1,1,1; (1,2,3,4,3,4,1,0,–3,–4,1,–4,1,0,–3,–2,1,2,3,4,21)
22	48870	1,1,1,1,1,1,–1,1,–1,1,–1,–1,1,–1,1,1,–1,–1,1,1,1,1; (1,2,3,4,3,2,1,2,–1,0,1,–2,–1,–4,1,0,3,–2,3,4,1,22)
23	68172	1,1,1,1,–1,–1,–1,1,1,–1,1,–1,1,–1,–1,1,1,–1,–1,1,1,1,1; (1,2,3,4,1,–2,–3,–2,1,2,3,–4,–3,2,1,2,–3,2,–1,–4,–3,2,23)
24	86124	1,1,1,1,1,1,–1,–1,–1,1,1,–1,1,–1,1,–1,–1,1,1,–1,1,1,1,1; (1,2,3,4,3,4,3,0,–3,–2,1,0,–1,–2,3,4,–3,–4,1,0,1,2,3,24)
25	–	1,1,1,1,1,–1,1,1,–1,1,–1,–1,1,1,1,–1,1,–1,–1,–1,1,1,1,–1,1; (1,0,1,2,3,0,3,–2,–3,0,–1,2,3,–2,1,0,3,2,1,–2,–1,0,1,0,25)
26	–	1,1,1,1,1,1,–1,–1,1,1,–1,–1,1,–1,1,–1,1,1,–1,1,–1,–1,–1,1,1,1,1; (1,2,3,4,3,2,1,–2,–1,0,1,4,–1,–2,1,–2,–1,4,1,–4,3,–2,3,0,1,26)
27	–	1,1,1,1,1,1,1,–1,–1,1,1,–1,–1,1,–1,1,–1,1,1,–1,1,–1,–1,–1,1,1,1,1; (1,2,3,4,3,2,3,0,–1,0,–1,2,3,0,–3,0,–1,0,3,0,–3,4,–1,4,1,2,27)
28	–	1,1,1,1,1,1,–1,–1,–1,1,1,1,1,–1,1,–1,1,–1,1,1,1,–1,–1,1,1,–1,1,1,1,1,1; (1,2,3,4,3,4,3,0,–3,–2,3,2,1,0,3,2,1,–2,3,4,1,0,–3,4,–3,2,3,28)
29	–	1,1,1,1,1,1,–1,–1,–1,1,1,1,1,–1,1,–1,1,1,1,–1,1,1,1,–1,–1,1,1,–1,1,1,1,1,1; (1,2,3,4,3,4,3,0,–3,–2,3,2,1,2,3,4,3,–2,3,4,1,2,1,–2,1,2,–1,4,29)
30	–	1,1,–1,1,1,1,1,1,1,–1,1,1,1,–1,1,–1,–1,–1,1,1,1,1,–1,1,–1,–1,1,–1,1,–1,1,1; (1,2,–1,0,3,0,3,–2,1,0,1,2,1,–4,1,–2,1,0,1,2,–3,4,3,2,–1,2,–1,4,–3,30)
31	286977	1,1,1,1,1,–1,1,1,1,–1,–1,1,1,–1,1,–1,1,–1,1,1,–1,1,–1,–1,1,1,–1,1,1,1,1,1; (1,2,3,4,3,2,3,2,1,4,–3,–2,3,4,1,–2,–1,4,1,2,3,–2,1,0,1,4,3,4,1,–2,31)
32	358464	1,–1,–1,1,1,1,1,1,1,1,–1,1,1,1,–1,–1,1,1,–1,1,–1,1,–1,–1,–1,1,1,1,1,1,–1,1,1,–1; (–1,2,1,–4,1,2,–1,0,–1,4,3,4,3,2,–1,–4,1,2,–3,4,–3,0,1,4,–3,–2,3,4,–1,–2,1,32)

Синтез *W*-ансамблей *R*-кодов

Перейдем к следующему этапу.

Этап 2: исследуется система неравенств (3), определяются *W*-ансамбли, находятся $H(N, R, W)$, $H(N, R, W, J)$. На этом этапе используется способ, применимый для произвольных значений (R, N, W). Он состоит в том, что берется множество $G_{R,N}$ и среди всех пар находятся такие коды, для которых УБП ВКФ превышает допустимое заданное значение. Возможно существование нескольких таких пар, они последовательно «разрываются» путем перемещения в разные вновь создаваемые подмножества. Это позволяет собрать в этих подмножествах лишь коды, для которых УБП ВКФ не более допустимой величины. Употребим этот способ и рассмотрим синтез *W*-ансамблей, используя все имеющиеся

$g_{4,N}$-коды. Обозначим $\mathbf{V}_{i,j}$ матрицу наибольших значений УБП модулей ВКФ всех пар (i, j) кодов из $G_{R,N}$ (учитывается корреляция каждого кода с номером i с произвольным другим кодом j). Эти значения матрицы ВКФ $\mathbf{V}_{i,j}$ потенциально могут принимать значения (1, ..., (N − 1)), причем наибольшая величина соответствует случаю, когда в $G_{R,N}$ имеются коды, различающиеся лишь одним символом. Очевидно, что $\mathbf{V}_{i,j} = \mathbf{V}_{j,i}$ и размер матрицы равен $g_{4,N} \times g_{4,N}$. Пример матрицы имеется ниже. Обозначим V_m и V_n наибольшее и наименьшее значения всех элементов $\mathbf{V}_{i,j}$. Введем набор $G0$ натуральных чисел (1, ..., $g_{4,N}$), позволяющий пронумеровать все коды, и назовем его исходным множеством номеров кодов. Рассмотрим следующие операции.

Шаг 0. В первую по счету строку табл. 2 записываются номера элементов $G0$. Это множество соответствует единственному $W = V_m$-ансамблю (здесь $H(N, R, V_m) = H(N, R, V_m, J) = 1$, $J = g_{4,N}$). В последней колонке даны значения УБП ВКФ и количество ансамблей, равное числу колонок со списками кодов.

Шаг 1. Из матрицы $\mathbf{V}_{i,j}$ выбираются пары индексов (s, u) ($s \neq u$) (s, u — индексы, порядковые номера R-кодов из $G0$), для которых ее значения равны V_m. Например, это пары ((s_1, u_1), ..., (s_{p1}, u_{p1})). Их необходимо «развести» путем перемещения в разные множества. Возможно появление разных типов пар индексов, существенно влияющих на результат. Ниже рассмотрены некоторые из них. Роль таких множеств выполняют колонки табл. 2. Для упрощения чтения цифровая часть индексов в строках таблиц поднята в строку (s_1 записано $s1$). Перед рассмотрением методики синтеза в общем виде, переходом к анализу и заполнению таблиц разберем несколько возможных вариаций образования пар номеров кодов, обоснуем для приложения выбор типичных версий.

Отвлечемся от действий 1-го шага и сформулируем способ пересмотра всех пар (s, u) номеров кодов из $G0$. Это возможно при изменении индексов по следующему правилу: для каждого s = 1, ..., ($g_{4,N}$ − 1) проводится вариация значений $u = s + 1$, ..., $g_{4,N}$, при этом всегда будет справедливо $s < u$. Перейдем к рассмотрению некоторых вариантов образования пар индексов. Это позволит позже дать оценку количества ансамблей, получаемых в результате удалений. На нее существенное влияние оказывает соотношение между номерами кодов разделяемых пар.

Вариант 1: все p_1 пар состоят из различных индексов, т. е. (s_1, u_1), (s_2, u_2), ..., (s_{p1}, u_{p1}). Это означает, что имеются ансамбли из двух кодов, удаления не требуются и надо перейти к следующему шагу методики.

Вариант 2: имеется множество пар с одинаковым первым номером пары (s_1, u_1; s_1, u_2; s_1, u_3; ...). Учитывая, что пары требуется разделить, целесообразно их объединить в обобщенную пару номеров (s_1, (u_1, u_2, u_3, ...)), тогда при разрыве пар удаляется s_1 либо все индексы в скобке. Синтез ансамблей начинается с анализа пар, имеющих наибольшее значение ВКФ. Целесообразно обратиться к парам, относящимся к случаю варианта 2, например (s_1, (u_1, u_2, u_3)). Укажем на другие модификации пар.

Вариант 3: простые пары (s, u) с индексом s, близким к своему наибольшему значению ($g_{4,N}$ − 1). Так как $u > s$ и $u \leq g_{4,N}$, то количество вариантов значений для u будет мало, что и определяет образование небольшого количества таких простых пар, а не обобщенных.

Вариант 4: имеется набор номеров кодов, в котором часть индексов удалена при выполнении предыдущих действий. Далее в соответствии с методикой удаляются оставшиеся не удаленными индексы либо никакие действия не осуществляются, если один из индексов простой пары или они оба оказались в числе ранее удаленных. То же касается обобщенных пар. Количество колонок в таблице не увеличивается (примеры ниже).

Вернемся к 1-му шагу. В 1-й колонке табл. 2 используется двойной индекс: первое число — номер шага; второе число — номер операции разделения пар кодов. Поэтому п. 1.2 означает, что рассматривается 2-я операция 1-го шага для УБП ВКФ V_m. Во 2-й строке табл. 2 показано разделение кодов в разные колонки. Начиная со 2-й по счету строки, в колонках приводятся индексы удаляемых кодов. Поэтому во 2-й строке 2-й и 3-й колонок удалены коды с индексами s_1 и (u_1, u_2, u_3) соответственно, а коды со всеми другими индексами сохраняются (номера удаленных кодов отмечаются знаком (^)). В результате колонка разделяется надвое и образуется два новых списка номеров индексов. Будем называть такие совокупности текущими множествами номеров кодов.

■ ***Таблица 2***

№ п. п.	Группы индексов						V_{ij}
0	(1,2, ..., $g_{4,N}$)						$V_m/1$
1.1	($\hat{s}1$)			($\hat{u}1$, $\hat{u}2$, $\hat{u}3$)			$V_m/2$
1.2	($\hat{s}1$; $\hat{s}2$)		($\hat{s}1$; $\hat{u}4$, $\hat{u}5$, $\hat{u}6$)	($\hat{u}1$, $\hat{u}2$, $\hat{u}3$; $\hat{s}2$)		($\hat{u}1$, $\hat{u}2$, $\hat{u}3$; $\hat{u}4$, $\hat{u}5$, $\hat{u}6$)	$V_m/4$
1.3	($\hat{s}1$; $\hat{s}2$; $\hat{s}3$)	($\hat{s}1$; $\hat{s}2$; $\hat{u}5$)	($\hat{s}1$; $\hat{u}4$, $\hat{u}5$, $\hat{u}6$)	($\hat{u}1$, $\hat{u}2$, $\hat{u}3$; $\hat{s}2$; $\hat{s}3$)	($\hat{u}1$, $\hat{u}2$, $\hat{u}3$; $\hat{s}2$; $\hat{u}5$)	($\hat{u}1$, $\hat{u}2$, $\hat{u}3$; $\hat{u}4$, $\hat{u}5$, $\hat{u}6$)	$V_{m-1}/6$

Их количество фиксируется в последней колонке, и после рассмотренного разделения обобщенной пары оно равно двум. Процедура аналогично проводится и для других пар. Например, для (s_2, (u_4, u_5, u_6)) проведено разделение, результаты занесены в 3-ю строку табл. 2, количество колонок (текущих множеств номеров кодов) равно четырем.

Ниже понадобится следующее по порядку убывания значение УБП ВКФ, обозначим его V_{m-1}. Оно может отличаться от V_m более чем на единицу. Допустим, $V_m = N - 1$, тогда последующее в таком ряду значение $\mathbf{V}_{i,j}$ может быть, к примеру, $V_{m-1} = N - 3$. Также заметим, что символ «V» относится к матрице, а родственная величина «W» — к ансамблям. Полученные в результате проведения операций на выбранном шаге текущие множества номеров соответствуют W-ансамблям.

При рассмотрении методики количество операций разделения обобщенных пар может быть велико. Индекс s непременно будет приближаться к своему наибольшему значению ($g_{4,N} - 1$), поэтому в соответствии с данными ранее объяснениями вероятно появление простых пар (вариант 3), например (s_3, u_5).

Для наборов в 3-й строке 2-й колонки разделение есть (получим 4-ю строку, 2-ю и 3-ю колонки), а 3-я строка, 3-я колонка не делится, дадим пояснения. Показан один из вариантов последствий, связанных с повторным появлением одного из номеров индексов в паре (здесь это u_5). Такой номер появлялся ранее в другой паре (возможность указана в варианте 4). Следовательно, в текущем множестве (3-я строка, 3-я колонка) ничего удалять не требуется, так как пара (s_3, u_5) разорвана путем удаления u_5 в предыдущей строке и указанная колонка не разделяется. То же относится и к набору номеров из 3-й строки 5-й колонки. В результате количество кодов не удваивается, а становится равным шести (последняя колонка 4-й строки). Иначе говоря, часть ансамблей может состоять из кодов, для которых все пары имеют УБП ВКФ меньше V_m, поэтому для них на этом шаге удаления не производятся, они не делятся (содержат коды с достаточно хорошими корреляционными свойствами).

По итогам операций 1-го шага получены текущие множества, представленные в 4-й строке, у которых УБП ВКФ меньше, чем был ранее. Обозначим их $G1(i)$, $i = (1, ..., 6)$. Они составляют $W = V_{m-1}$ -ансамбли в количестве $H(N,R,V_{m-1}) = 6$. С учетом проведенных удалений два ансамбля имеют численность $J1 = g_{4,N} - 3$ (это следует из 2-й, 3-й колонок), один — $J2 = g_{4,N} - 4$ (4-я колонка), два — $J3 = g_{4,N} - 5$ (5-я, 6-я колонки), один — $J4 = g_{4,N} - 6$ (7-я колонка). Следовательно, $H(N, R, V_{m-1}, J1) = 2$, $H(N, R, V_{m-1}, J2) = 1$, $H(N, R, V_{m-1}, J3) = 2$, $H(N, R, V_{m-1}, J4) = 1$, а всего 6.

Шаг 2. Выполняются операции, изложенные для шага 1, с учетом значений матрицы ВКФ, равных $\mathbf{V}_{i,j} = V_{m-1}$, формируются новые пары. Например, рассмотрим набор (s_1, (u_k, u_m, u_n)), где индексы во внутренних скобках примем (s_2, s_3, u_6). Количество колонок стремительно увеличивается. Перенесем первые четыре колонки табл. 2 в новую табл. 3, добавив еще одну для значения УБП ВКФ и количества текущих множеств (ансамблей кодов здесь три). Остальные колонки транспортируем в табл. 4. В созданных таблицах повторена последняя строка, так как конец одного шага удобно считать началом другого.

В табл. 3 индекс s_1 удален ранее, поэтому пары для разрыва отсутствуют, колонки не меняются. В табл. 4 пары «разъединяются» путем удаления s_1 либо (s_2, s_3, u_6), причем какие-то из этих индексов оказываются удаленными ранее. Для удобства последующей проверки удаляемые номера отделяются в строках таблиц знаком (;) и записываются в порядке их удаления, а не по порядку

■ ***Таблица 3***

№ п. п.	Группы индексов				V_{ij}
2.1	($\hat{s}1$; $\hat{s}2$; $\hat{s}3$)		($\hat{s}1$; $\hat{s}2$; $\hat{u}5$)	($\hat{s}1$; $\hat{u}4$, $\hat{u}5$, $\hat{u}6$)	$V_{m-1}/3$
2.2	($\hat{s}1$; $\hat{s}2$; $\hat{s}3$)		($\hat{s}1$; $\hat{s}2$; $\hat{u}5$)	($\hat{s}1$; $\hat{u}4$, $\hat{u}5$, $\hat{u}6$)	$V_{m-1}/3$
2.3	($\hat{s}1$; $\hat{s}2$; $\hat{s}3$; $\hat{u}5$)	($\hat{s}1$; $\hat{s}2$; $\hat{s}3$; $\hat{u}6$)	($\hat{s}1$; $\hat{s}2$; $\hat{u}5$)	($\hat{s}1$; $\hat{u}4$, $\hat{u}5$, $\hat{u}6$)	$V_{m-2}/4$

■ ***Таблица 4***

№ п. п.	Группы индексов							V_{ij}
2.1	($\hat{u}1$, $\hat{u}2$, $\hat{u}3$;$\hat{s}2$; $\hat{s}3$)			($\hat{u}1$, $\hat{u}2$, $\hat{u}3$; $\hat{s}2$; $\hat{u}5$)		($\hat{u}1$, $\hat{u}2$, $\hat{u}3$; $\hat{u}4$, $\hat{u}5$, $\hat{u}6$)		$V_{m-1}/3$
2.2	($\hat{u}1$, $\hat{u}2$, $\hat{u}3$; $\hat{s}2$; $\hat{s}3$; $\hat{s}1$)		($\hat{u}1$, $\hat{u}2$, $\hat{u}3$; $\hat{s}2$, $\hat{s}3$, $\hat{u}6$)	($\hat{u}1$, $\hat{u}2$, $\hat{u}3$; $\hat{s}2$; $\hat{u}5$; $\hat{s}1$)	($\hat{u}1$, $\hat{u}2$, $\hat{u}3$; $\hat{s}2$; $\hat{u}5$; $\hat{s}3$, $\hat{u}6$)	($\hat{u}1$, $\hat{u}2$, $\hat{u}3$; $\hat{u}4$, $\hat{u}5$, $\hat{u}6$; $\hat{s}1$)	($\hat{u}1$, $\hat{u}2$, $\hat{u}3$; $\hat{u}4$, $\hat{u}5$, $\hat{u}6$; $\hat{s}2$, $\hat{s}3$)	$V_{m-1}/6$
2.3	($\hat{u}1$, $\hat{u}2$, $\hat{u}3$; $\hat{s}2$; $\hat{s}3$; $\hat{s}1$; $\hat{u}5$)	($\hat{u}1$, $\hat{u}2$, $\hat{u}3$; $\hat{s}2$; $\hat{s}3$; $\hat{s}1$; $\hat{u}6$)	($\hat{u}1$, $\hat{u}2$, $\hat{u}3$; $\hat{s}2$, $\hat{s}3$, $\hat{u}6$)	($\hat{u}1$, $\hat{u}2$, $\hat{u}3$; $\hat{s}2$; $\hat{u}5$; $\hat{s}1$)	($\hat{u}1$, $\hat{u}2$, $\hat{u}3$; $\hat{s}2$; $\hat{u}5$; $\hat{s}3$, $\hat{u}6$)	($\hat{u}1$, $\hat{u}2$, $\hat{u}3$; $\hat{u}4$, $\hat{u}5$, $\hat{u}6$; $\hat{s}1$)	($\hat{u}1$, $\hat{u}2$, $\hat{u}3$; $\hat{u}4$, $\hat{u}5$, $\hat{u}6$; $\hat{s}2$, $\hat{s}3$)	$V_{m-2}/7$

из первоначального следования в 1-й строке табл. 2 (если удаляется, например, s_1, то записываем его в конце строки удаления, а не в начале). В конце этого шага, как и предыдущего, в соответствии с изложенными ранее причинами, рассмотрим простую пару (по варианту 3). Допустим, это (s, u), где $s = u_5$, $u = u_6$. В табл. 3 набор номеров (2-я колонка, 2-я строка) делится, а 3-я и 4-я колонки — нет, так как там u_5, а (u_5, u_6) уже удалены. В табл. 4 по тем же причинам разделяется лишь совокупность номеров (2-я колонка, 2-я строка), а все другие — нет. В конце 2-го шага получим текущие множества $G2(i)$, $i = (1, ..., 11)$, составляющие $W = V_{m-2}$-ансамбли (3-я строка табл. 3, 4). Здесь $H(N, R, V_{m-2}) = 11$ (общее количество последних колонок указанных таблиц) и $J1 = g_{4,N} - 3$, $J2 = g_{4,N} - 4$, $J3 = g_{4,N} - 6$, $J4 = g_{4,N} - 7$, $J5 = g_{4,N} - 8$, т. е. $H(N, R, V_{m-1}, J1) = 1$, $H(N, R, V_{m-1}, J2) = 3$, $H(N, R, V_{m-1}, J3) = 4$, $H(N, R, V_{m-1}, J4) = 2$, $H(N, R, V_{m-1}, J5) = 1$ (всего 11). Эти наборы параметров интересны для исследования дифференциации по численности.

Шаг 3. Процедура повторяется до получения W-ансамблей с требуемым объемом кодов, необходимым значением УБП ВКФ либо при достижении V_n. Если в ансамблях остается лишь два кода либо значения УБП ВКФ для всех пар кодов равны, то операции с ними далее не производятся. Введем $\hat{G}_{R,N,W}$ — множество номеров кодов, удаленных при реализации методики. Тогда, если интерпретировать W как искомое множество номеров кодов, эти индексы ансамблей можно представить в виде разности множеств $W = G_{R,N} / \hat{G}_{R,N,W}$ (исходное множество без удаленных индексов). Окончательные результаты получаются, если в исходной последовательности (1-я строка табл. 2) удалить индексы, записанные в последних строках табл. 3, 4. После нахождения $H(N,R,V_n)$, $H(N,R,V_n,J)$ и нужных кодов рассмотрение задачи завершается.

Заметим, что параметр J (численность наборов кодов) по существу соответствует использованной ранее величине L — количеству сигналов, а $B^* = N$ (для бинарных кодов). Сравнивая все J с N, можно делать выводы о соответствии полученных W-ансамблей введенным понятиям о системе сигналов и ее объеме. Так как количество ансамблей равно $H(N, R, W, J)$, то допустимо говорить о синтезе комплекта или совокупности систем бинарных сигналов.

В первой строке табл. 2 даны номера исходного множества кодов, а в последней колонке — УБП ВКФ и количество наборов (колонок с номерами).

Уделим внимание матрице $\mathbf{V}_{i,j}$, конкретизация которой в начале методики синтеза при рассмотрении задачи в общем виде, возможно, отвлекла бы внимание от сути задачи. Теперь целесообразно представить ее с учетом проведенных операций. Матрица изображена в виде табл. 5, где даны две системы обозначений индексов i, j: по порядку номеров (условно до $g_{4,N} = 9$) и в соответствии с обозначениями индексов в рассмотренной выше методике (в скобках). Значения в ячейках заданы согласно проведенным операциям (V_m и V_{m-1}), а все прочие заданы символически величинами V_{m-2}. Элементы главной диагонали не относятся по смыслу к $\mathbf{V}_{i,j}$ и вычеркнуты.

Данная матрица позволяет полнее изложить сущность методики синтеза.

Количество ансамблей $H(N,R,W)$ можно получить, проведя все указанные операции методики, но их трудоемкость велика, и желательно иметь аналитическое выражение для приближенной оценки. Получим такое соотношение.

Общее количество всевозможных пар (s, u) равно $Po = g_{R,N}(g_{R,N} - 1)/2$. Предположим, что для любого значения матрицы ВКФ в образовании пар участвуют почти все коды. То есть коды в $G0$ не разделяются на совокупности, в которых для некоторых значений $\mathbf{V}_{i,j}$ пары образуются

■ ***Таблица 5***

i / *j*	1 (*s*1)	2 (*s*2)	3 (*s*3)	4 (*u*1)	5 (*u*2)	6 (*u*3)	7 (*u*4)	8 (*u*5)	9 (*u*6)
1 (*s*1)		V_{m-1}	V_{m-1}	V_m	V_m	V_m	V_{m-2}	V_{m-2}	V_{m-1}
2 (*s*2)	V_{m-1}		V_{m-2}	V_{m-2}	V_{m-2}	V_{m-2}	V_m	V_m	V_m
3 (*s*3)	V_{m-1}	V_{m-2}		V_{m-2}	V_{m-2}	V_{m-2}	V_{m-2}	V_m	V_{m-2}
4 (*u*1)	V_m	V_{m-2}	V_{m-2}		V_{m-2}	V_{m-2}	V_{m-2}	V_{m-2}	V_{m-2}
5 (*u*2)	V_m	V_{m-2}	V_{m-2}	V_{m-2}		V_{m-2}	V_{m-2}	V_{m-2}	V_{m-2}
6 (*u*3)	V_m	V_{m-2}	V_{m-2}	V_{m-2}	V_{m-2}		V_{m-2}	V_{m-2}	V_{m-2}
7 (*u*4)	V_{m-2}	V_m	V_{m-2}	V_{m-2}	V_{m-2}	V_{m-2}		V_{m-2}	V_{m-2}
8 (*u*5)	V_{m-2}	V_m	V_m	V_{m-2}	V_{m-2}	V_{m-2}	V_{m-2}		V_{m-1}
9 (*u*6)	V_{m-1}	V_m	V_{m-2}	V_{m-2}	V_{m-2}	V_{m-2}	V_{m-2}	V_{m-1}	

из кодов одного списка номеров, а для других $\mathbf{V}_{i,j}$ — иного комплекта кодов. Иначе говоря, отсутствует группировка кодов, и в парах участвуют примерно одинаково часто все коды. Это приводит к тому, что когда для пар (s, u) индексы s и u изменяются пропорционально соответственно от 1 до ($g_{R,N} - 1$) и от $s + 1$ до $g_{R,N}$, то и количество пар в целом, можно ожидать, будет изменяться с такой же закономерностью. Поэтому, пока s мало, то количество версий составления обобщенных пар со всеми другими кодам велико.

При разделении таких пар происходит раздвоение текущих множеств и колонок таблиц, в которые они входили. Общее количество множеств, а потом и ансамблей увеличивается. Поэтому можно сделать два предположения:

1) если имеется Pr обобщенных пар, то из исходного набора кодов при последовательном делении этих пар можно получить новые множества, количество которых будет равно $N_W \sim 2^{Pr}$, и это справедливо для любой первоначальной совокупности кодов любого текущего множества. Иначе говоря, для любой операции и на всех шагах каждое множество номеров кодов непременно должно содержать также номера кодов, входящих в рассматриваемую обобщенную пару, и поэтому обязательно осуществляется деление надвое;

2) весь комплект простых пар всегда разделяется на предыдущих операциях с обобщенными парами. Когда доходит очередь до операций с простыми парами (вариант 4), то деления не происходит.

Практически эти условия могут не всегда выполняться, что приведет к погрешностям оценок. Однако условия 1 и 2 являются разнохарактерными (невыполнение 1-го приводит к уменьшению, а 2-го — к росту количества множеств), поэтому их одновременное невыполнение может привести к компенсации и результату, близкому к истинному. Учтя указанную неопределенность путем расширения значений ξ, введем искомую оценку в виде

$$N_W = 2^{\xi},\ \xi = Pr \pm 1. \qquad (4)$$

Положения 1, 2 возьмем за основу создания *модели 1* вычисления количества ансамблей. В дальнейших работах она может быть уточнена на основании более подробного анализа матрицы $\mathbf{V}_{i,j}$.

Заметим, что количество обобщенных пар зависит от параметров сигналов, что можно в общем виде представить функцией $Pr = f(N, R, W)$. Для ее нахождения используется матрица ВКФ (см. табл. 5). Например, для $W = V_{m-1}$ нужно принять во внимание и все индексы, соответствующие большим значениям ВКФ (не только для V_{m-1}, но и для V_m). Начнем с уровня V_m и выберем s_1 во 2-й колонке. Движемся вниз по строчкам, находящимся ниже главной диагонали матрицы (т. е., начиная со 2-й строчки). Определяем для выбранного значения ВКФ величины 2-го индекса обобщенной пары. Это позволяет найти такую пару, состоящую из индексов (s_1, (u_1, u_2, u_3)). Потом отметим s_2 в 3-й колонке, спускаемся ниже диагонали до 3-й строчки и для V_m определяем вторые индексы и всю пару (s_2, (u_4, u_5, u_6)). Действуя сходно для s_3, получим набор (s_3, u_5) (это не обобщенная пара). Видно, что других вариантов нет, для этого шага $Pr = 2$. Того же достигнем, если двигаться по колонкам. Далее задаем V_{m-1}, действуем аналогично, находим обобщенную пару (s_1, (s_2, s_3, u_6)), а (u_5, u_6) таковой не является. Всего получим $Pr = 3$ и для $\xi = Pr$ справедливо $N_W = 8$, что меньше $H(N, R, V_{m-2}) = 11$. Различия связаны с условностью выбора обобщенных пар для наглядной иллюстрации разнообразных случаев. Имеются ограничения на применение модели 1 для W, близких к V_n, когда по указанным ранее причинам множества не разделяются и операции с ними не осуществляются. Итак, в результате анализа количество ансамблей можно оценить величиной $H(N,R,W) \approx N_W = 2^{\xi}$ ($\xi = Pr \pm 1$).

Далее исследуем изменение числа кодов J в ансамблях в зависимости от W при фиксированных N, R. Ранее отмечалось, что после разрыва пар количество кодов быстро растет, поэтому рассмотрим указанную зависимость для случая, когда после разделения пар сохраняются не два, а один набор кодов. Удобно оставлять для дальнейшего анализа исключительно наборы с удаленным первым индексом пары. Это означает, что в табл. 2–4 сохраняется лишь крайняя левая колонка с номерами кодов. Так, при «разделе» простой пары (s, u) из двух текущих множеств ($G_1(\hat{s})$ и $G_1(\hat{u})$) оставляется единственно первый, а при операции с двумя парами (s_1, u_1), (s_2, u_2) из четырех возможных оставляется только $G_2(\hat{s}1, \hat{s}2)$. В итоге можно быстрее получить хотя бы не полный, а частичный результат для предварительного анализа (ценой потери общности решения). Это важно при больших N. Теперь требуется наблюдать за изменениями одного множества кодов после каждого «обрыва» пар и можно получать для разных W хотя бы по одному ансамблю из всех. Применим такой подход («быстрый синтез») для поиска зависимости количества кодов в ансамбле от уровня W.

Приведем соображения для обоснования требуемого аналитического соотношения. Выберем один из R-кодов с $W = V_n$. В бинарных кодах коэффициенты принимают значения (±1). Будем рассматривать, для конкретности, коды с $P_1 = 1$, а все другие P_j пусть могут соответствовать любому из этих двух вариантов. Поэтому будем последовательно, начиная с P_2, варьировать знаки коэффициентов, получая наборы разнообразных

кодов. Если осуществить это с P_2, то вместе с исходным кодом получим всего $n = 2$ кода; если изменить P_2 и P_3, то всего будет $n = 4$ кода, т. е. при последовательном изменении знаков t коэффициентов получим $n = 2^t$ вариантов кодов. Обоснуем связь t и W. Пусть t мало, тогда лишь небольшое количество кодов может удовлетворять жестким корреляционным требованиям и составлять ансамбли с W, близким к V_n (это могут быть наборы из двух, трех кодов). При увеличении t количество вариантов комбинаций будет расти, и для получения больших по численности ансамблей непременно необходимо увеличивать W. Однако при этом не все коды могут удовлетворять требованиям (2), и функциональная связь t и W существенно изменится (пример ниже). Вместе с ростом W и приближением его к V_m количество R-кодов, различающихся лишь одним символом, невелико. С другой стороны, известно, что ВКФ есть сумма произведений коэффициентов двух сдвигаемых друг относительно друга последовательностей. Следовательно, ориентируясь на наихудший случай, вместе с изменениями знаков кодов и повышением их количества найдутся такие пары, что для них пропорционально увеличится максимальное значение УБП ВКФ, поэтому создание больших по объему ансамблей возможно лишь при росте W. С учетом всех приведенных обстоятельств логично предположить, что $W \sim t$, и тогда $n \approx 2^W$. Дополнительно подчеркивая зависимость n от W, запишем $n_W \approx 2^W$. Ранее численность ансамблей обозначалась символом J. Поэтому $J_W \approx 2^W$ — оценка объема W-ансамблей R-кодов при вариации W.

Из проведенных рассуждений сформулируем два положения:

1) численность W-ансамблей пропорциональна показательной функции от W ($J_W \approx 2^W$);

2) указанная закономерность справедлива для всех W-ансамблей.

Эти высказывания примем как гипотезы и возьмем за основу *модели 2* вычисления количества кодов в W-ансамблях. Она применима, как было обосновано, лишь для W, которые заметно меньше V_m. Степень корректности моделей 1, 2 можно будет оценить впоследствии на основании разбора результатов синтеза. Совместное применение обеих моделей позволяет найти объем и численность ансамблей R-кодов, при этом считается, что число J_W кодов во всех наборах одинаковое.

Назовем зависимость характерной численности от уровня W ансамблей ($J_W \approx 2^W$) калибровочной характеристикой. Пусть $J_W = \alpha 2^{W(1-Vn/N)}$, где α — неопределенный коэффициент, подлежащий выбору. Для построения графика удобно провести переобозначение

$$Q(W) = \alpha 2^{W(1-Vn/N)}. \qquad (5)$$

Уровень α выбирается из условия нормировки: при $W = V_n$ имеем минимально возможную численность $J_{W\ \min} = 2$. Подставив $J_W = Q = 2$ в левую часть (5), получим α, которую обозначим $\alpha 1$ (1-й вариант):

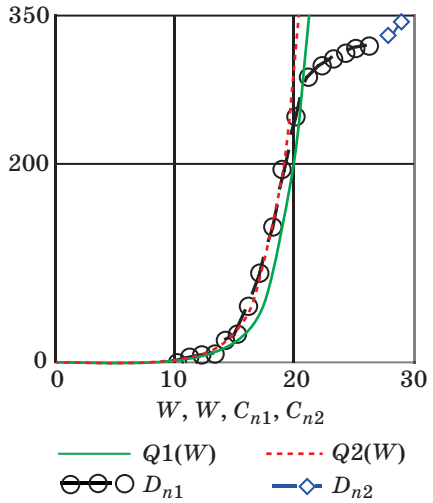
$$\alpha = \alpha 1 = 2^{1-\delta}, \text{ где } \delta = (1 - V_n/N)V_n. \qquad (6)$$

Для $N = 30$, $V_n = 10$ вычислим по (6) $\alpha 1 \approx 0{,}02$ и получим калибровочную характеристику $Q1(W) = 0{,}02 \cdot 2^{W \cdot 2/3}$.

Это соотношение, установленное на основании модели 2, сопоставим с имеющимися результатами синтеза $R3$-кодов (они входят в множество $R4$-кодов) с $N = 30$, для которых $g_{3,30} = 344$. Использован «быстрый синтез», найдена функция $J = D_n(W)$ — зависимость численности ансамблей J от уровня W (это дискретная функция с дискретным аргументом), а также $V_n = 10$, $V_m = 29$ (при $W = 27$ ансамбли отсутствуют). Результаты синтеза представлены ниже графически.

Согласно модели 2, объем всех ансамблей одинаков и равен характерной численности $J_W = Q(W)$ (расчетная характеристика). Вместе с тем для одного из ансамблей по результатам синтеза получена $J = D_n(W)$ (фактическая зависимость), следовательно, имеются основания для сравнения $Q(W)$ и $D_n(W)$. Введем для дальнейшего применения нормированную величину $C = W/N$, которая определяет «долю» W относительно N.

Графики дискретной функции $D_n(W)$, данной в форме отсчетов, и калибровочной характеристики $Q1(W)$, представленной в виде непрерывной линии, приведены на рисунке. По оси абсцисс отложены уровни W, которые могут изменяться в пределах [1, ..., 29], а по оси ординат — значения указанных функций, способные варьироваться в интервале [2, 344]. Знаком ○ отмечены дискретные величины для W из интервала [10, ..., 26], а ◇ — на промежутке [28, 29].



■ Калибровочные характеристики

Такая калибровочная характеристика является универсальной и может быть применена в интервале $[W_н, W_в]$, где $W_н = V_n$, а $W_в = N/\sqrt{2}$, однако при этом максимальная погрешность составляет около 42 % (для центральных значений аргумента). Вместе с тем возможно увеличение точности. Если W принадлежит интервалам [10; 14] или [20; 21] (для C это [0,33; 0,47] и [0,67; 0,7]), то погрешность менее 10 %. Когда W принимает значения между (14; 20) (C в пределах (0,47; 0,67)), то необходимо определять коэффициент α по формуле (2-й вариант)

$$\alpha = \alpha 2 = (1 + V_n/N)2^{1-\delta},$$
$$\delta = (1 - V_n/N)V_n. \qquad (7)$$

Тогда округленно $\alpha = \alpha 2 = 0{,}03$, а график $Q2(W)$ пунктирно дан на рисунке, причем точность значительно увеличилась. Итак, модель 2 качественно совпадает с результатами синтеза в широком диапазоне вариаций аргумента.

Если задать параметры N, R, W, определить $g_{R,N}$, найти уровень V_n, то, используя (5)–(7) и варьируя W от 1 до N–1, возможно получить искомую оценку $J_W = Q(W)$ численности W-ансамблей. Она может изменяться от двух до $g_{R,N}$. Для $R4$-кодов $g_{R,N}$ велико, поэтому могут быть получены W-ансамбли большой численности, а также составлены комплекты ансамблей (системы сигналов).

Анализ позволил оценить характерную численность ансамблей, но актуальной задачей является и определение диапазона отклонений σ_W от уровня J_W. Если J_W — характерная численность большинства ансамблей из общего их количества, то интересно оценить, какие значения объемов ансамблей еще возможны.

В рамках методики синтеза во всех множествах проводятся удаления. При наименьшем количестве удаленных индексов численность ансамблей будет наибольшей (левые колонки табл. 2–4). Если удаляется много номеров, то объем ансамблей мал (крайние правые столбцы таблиц). Максимальную численность $J_{W\max}$ будут иметь ансамбли, в которых каждый из Pr раз будет удаляться по одному индексу кодов, поэтому $J_{W\max} = g_{R,N} - Pr$. Введем уровни, по которым будут определяться отклонения σ_W. Обозначим $J_{W в} = (J_{W\max} + J_W)/2$ и $J_{W н} = (J_{W\min} + J_W)/2$ верхнюю и нижнюю граничные численности W-ансамблей. Теперь определим отклонение соотношением $\sigma_W = J_{W в} - J_{W н}$, тогда получим

$$\sigma_W = (g_{R,N} - Pr)/2 - 1. \qquad (8)$$

Численность основного объема ансамблей изменяется в интервале $[J_W - 0{,}5\sigma_W; J_W + 0{,}5\sigma_W]$, в котором средним значением является J_W — численность большинства ансамблей основного объема.

Для удобства и компактного анализа рассмотрим простейший **пример**.

Дано: $N = 5$, $R = 3$, $g_{3,N} = 14$, $Pr = 7$, $V_n = 2$. *Найти*: все расчетные характеристики W-ансамблей (N_W, J_W, σ_W).

Решение:

1) исходные коды составляют один ансамбль с $W = 4$, и можно синтезировать ансамбли с $W = 2{,}3$. Как отмечалось, модель 1 не применима для малых W, поэтому Pr задано лишь для $W = 3$. Используем (4) для $\xi = Pr$ и получим $N_3 = 128$;

2) так как $C = 0{,}6$ для $W = 3$, то, применив (7), найдем $\alpha 2 = 1{,}22$ и с помощью (5) вычислим $J_3 = Q(3) = 4{,}0$. При $W = 2$ всегда имеется наименьшая численность $J_2 = 2$;

3) из (8) найдем $\sigma_3 = 2{,}5$, а σ_2 не может быть найдена из-за несуществования, как было сказано, Pr для $W = 2$. Поэтому большинство ансамблей с $W = 3$ имеют численность $J_3 = 4$, но имеются также ансамбли с численностью $J_3 \pm \sigma_3/2$, т. е. $J = 3$ и $J = 5$.

Ответ: количество ансамблей предположительно равно 128; среди них большинство для $W = 3$ имеет численность по четыре кода, а при $W = 2$ — по два кода; в общем количестве ансамблей с $W = 3$ присутствуют ансамбли с тремя и пятью кодами. (Использованы оценочные параметры, поэтому ответ сформулирован в предположительной форме).

Полученные величины сравним с итогами полного синтеза. Всего для данных, приведенных в примере, в случае $W = 3$ существует $H(5,3,3) = 99$ кодов, т. е. погрешность сделанной оценки 29 %. Распределение по численностям набора кодов: пар — $H(5,3,3,2) = 4$; троек — $H(5,3,3,3) = 23$; четверок — $H(5,3,3,4) = 46$; пятерок — $H(5,3,3,5) = 24$; шестерок — $H(5,3,3,6) = 2$. Распределение практически симметрично относительно наибольшего количества четверок. Основной объем ансамблей, состоящих из троек, четверок и пятерок, составляет почти 94 % от общего числа. Если $W = 2$, то $H(5,3,2) = 18$. Сравнивая с ответом примера, видим, что оценки численности вполне удовлетворительны. Вот вариант ансамбля кодов с характерной численностью: 1, –1, 1, –1, –1; 1, 1, –1, 1, 1; 1, –1, –1, 1, 1; 1, –1, –1, –1, 1. Согласно классификации, приведенной выше, этот ансамбль можно отнести, вероятно, к нормальной системе сигналов.

Заключение

Известна система кодирования ASCII (American Standard Code for Information Interchange — стандартный код информационного обмена). Каждый из 256 символов характеризуется комбинацией из восьми двоичных символов или

импульсов (байт). Каждому байту можно сопоставить один из $R4$-кодов в соответствии с алфавитом. Количество кодов $g_{4,N}$ велико, и можно получить большой объем вариантов алфавитов системы ASCII. Это позволяет пользователям средств вычислительной техники выбирать алфавит представления своих рабочих данных, что совместно с известными достоинствами ШПС [1] затруднит несанкционированный доступ к ним, повысит информационную безопасность. Эти возможности могут использоваться в системах управления, передачи данных и вычислительных системах, в том числе в компьютерах. По аналогии с радиолокационными системами на ШПС [4] их разумно назвать «тихими» компьютерами, они будут обладать всеми достоинствами ШПС. Эти возможности могут быть распространены на локальные и глобальные компьютерные сети с перспективой создания «тихого» Интернета, в котором повышена защищенность от несанкционированного доступа к электронной персональной информации.

Обширный набор алфавитов позволяет решать задачи шифрования путем выбора кодов, привлекаемых для их создания, независимо от известных методов шифрования. Появляется новая, дополнительная ступень защиты.

Литература

1. **Варакин Л. Е.** Системы связи с шумоподобными сигналами. — М.: Радио и связь, 1985. — 384 с.
2. **Ипатов В. П., Орлов В. К., Самойлов И. М., Смирнов В. Н.** Системы мобильной связи: учеб. пособие для вузов/ под ред. В. П. Ипатова. — М.: Горячая линия – Телеком, 2003. — 272 с.
3. **Ipatov V. P.** Spread Spectrum and CDMA. Principles and Applications. — N. Y.: John Wiley and Sons Ltd., 2004. — 373 p.
4. **Гантмахер В. Е., Быстров Н. Е., Чеботарев Д. В.** Шумоподобные сигналы. Анализ, синтез, обработка. — СПб.: Наука и техника, 2005. — 400 с.
5. **Tang X., Ding C.** New Classes of Balanced Quaternary and Almost Balanced Binary Sequences With Optimal Autocorrelation Value// IEEE Transactions on Information Theory. 2010. Vol. 56. N 12. P. 6398–6405.
6. **Чепруков Ю. В., Соколов М. А.** Синтез фазоманипулированных сигналов с требуемым уровнем боковых пиков АКФ // Радиотехника. 1991. № 5. С. 68–70.
7. **Чепруков Ю. В., Соколов М. А.** Бинарные R2-коды, их характеристики и применение // Информационно-управляющие системы. 2014. № 1. С. 76–83.

UDC 621.396:621.391.26

Correlation Characteristics of Some Binary R-4 Codes and Ensembles of Signals on Their Basis

Cheprukov Yu. V.[a], PhD., Tech., chuv52@mail.ru
Socolov M. A.[b], Dr. Sc., Tech., Professor, guap22@mail.ru
[a]Russian State University of Tourism and Service in Sochi, 24/a, Kirpichnaia St.,354340, Sochi, Russian Federation
[b]Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St., 190000, Saint-Petersburg, Russian Federation

Purpose: Continuous increase in the efficiency of various control & communication systems is possible when using more advanced binary codes and signaling systems on their basis. Known N-element binary codes used in these systems do not allow us to obtain a sufficiently low level of the lateral peaks of the autocorrelation and mutual correlation functions of a set of codes when N varies over a wide range. The purpose of this work is studying the synthesis of N-element binary codes with given R and W levels of lateral peaks of the autocorrelation and mutual correlation functions. **Results:** A table of code synthesis results is given for $R = 4$ and $N \le 32$. A general account is given of the technique and features of binary code ensemble synthesis with a given level W of lateral peaks of mutual correlation function. To obtain analytical estimates of quantitative characteristics of such code sets, certain hypotheses are proposed, models built and an example given. **Practical relevance:** The results can be used in control & communication systems. The idea of encipherement with these codes has been formulated. There is a potential way to create «quiet» computers and computer networks, leading to the development of «quiet» Internet.

Keywords — Group, Binary Code, Autocorrelation Function, Side Level.

References

1. Varakin L. E. *Sistemy sviazi s shumopodobnymi signalami* [Communication Systems with Noise Signals]. Moscow, Radio i sviaz' Publ., 1985. 384 p. (In Russian).
2. Ipatov V. P., Orlov V. K., Samoilov I. M., Smirnov V. N. *Sistemy mobil'noi sviazi* [Mobile Communication Systems]. Ed. V. P. Ipatov. Moscow, Goriachaia liniia – Telekom Publ., 2003, 272 p. (In Russian).
3. Ipatov V. P. *Spread Spectrum and CDMA. Principles and Applications*. New York, John Wiley and Sons Ltd., 2004. 373 p.
4. Gantmaher V. E., Bystrov N. E., Chebotarev D. V. *Shumopodobnye signaly. Analiz, sintez, obrabotka* [Pseudo-noise Signals. Analysis, Synthesis, and Processing]. Saint-Petersburg, Nauka i tehnika Publ., 2005. 400 p. (In Russian).
5. Tang X., Ding C. New Classes of Balanced Quaternary and Almost Balanced Binary Sequences with Optimal Autocorrelation Value. *IEEE Transactions on Information Theory*, 2010, vol. 56, no. 12, pp. 6398–6405.
6. Cheprukov Ju. V., Socolov M. A. Synthesis of Phasemanipulated Signals with Required Level of Side Peaks ACF. *Radiotehnika*, 1991, no. 5, pp. 68–70 (In Russian).
7. Cheprukov Yu. V., Socolov M. A. Binary R2-Codes, Their Features and Application. *Informatsionno-upravliaiushchie sistemy*, 2014, no. 1, pp. 76–83 (In Russian).

УДК 519.876.2, 519.876.5

ОПТИМАЛЬНОЕ УПРАВЛЕНИЕ ОЧЕРЕДЬЮ В СИСТЕМЕ МАССОВОГО ОБСЛУЖИВАНИЯ С ОГРАНИЧЕННОЙ ПРОИЗВОДИТЕЛЬНОСТЬЮ

Д. А. Зубок[a]*, канд. физ.-мат. наук, заместитель заведующего кафедрой*
А. В. Маятин[a]*, канд. пед. наук, доцент*
[a]*Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, Санкт-Петербург, РФ*

Постановка проблемы: *для систем массового обслуживания с бесконечным числом приборов отсутствует детальное исследование аналогов пороговому характеру оптимальных дисциплин обслуживания, установленных для систем массового обслуживания с конечным числом неоднородных приборов. В то же время модели систем с бесконечным числом приборов дают удовлетворительное описание вычислительных узлов с многопоточностью. Целью работы является выявление порогового характера оптимальной дисциплины управления системами с бесконечным числом приборов переменной производительности, зависящей от числа требований в системе.* ***Методы:*** *для описания процесса обслуживания применяются методы процессов с дискретным временем и счетным числом состояний. При описании выходящего потока используется авторегрессионная схема.* ***Результаты:*** *в приближении процессов с дискретным временем выведены уравнения авторегрессии и скользящего среднего для описания входящего и выходящего потоков процесса обслуживания. При этом предполагается, что порядок окончания выполнения требований совпадает с порядком их поступления на выполнение. Для проверки гипотезы о существовании оптимальной дисциплины управления очередью проводятся имитационные эксперименты. При проведении экспериментов интенсивность входящего потока принимала значения как меньше, так и больше производительности системы при выполнении только одного требования. Имитационные эксперименты показали зависимость среднего времени пребывания требования в системе от разрешенной величины очереди и интенсивности входящего потока. Таким образом, принцип повышения производительности заключается в том, что при заданной интенсивности потока требований однозначно определяется нижняя граница для величины очереди, начиная с которой производительность системы не растет.* ***Практическая значимость:*** *предложенные математическая и имитационная модели можно применять для изучения одно- и многофазных систем с различным распределением времени выполнения требований и различными законами падения производительности.*

Ключевые слова *— система массового обслуживания, бесконечное число приборов, управляемый марковский процесс, качество обслуживания, имитационная модель.*

Введение

Модели однопроцессорных систем с распределением процессорного времени по задачам изучаются с 70-х годов прошлого столетия [1, 2]. Задачи исследования времени отклика, времени выполнения операций решаются в рамках систем массового обслуживания (СМО) $M \mid M \mid 1\ PS$, которые обобщают системы $M \mid M \mid 1$ на уровне дисциплины обслуживания заявок тем, что предусмотрены циклы, охватывающие буфер с очередью задач и центральный процессор. Таким образом, для обработки заявки выделяется системное время, по окончании которого заявка переходит в режим ожидания, пока обрабатываются другие заявки. В работах [3, 4] изучены такие характеристики качества СМО $M \mid M \mid 1\ PS$, как среднее время ожидания и среднее время выполнения. Кроме того, математические модели таких задач близки к моделям задач управления транспортными потоками [5]. Модели управляемых случайных процессов и цепей находят применение при решении ряда других вопросов, связанных с организацией работы вычислительных средств, например, обработки информации, оптимального обмена данными.

Модели типа $M \mid G \mid 1$ и $M \mid G \mid c$, в том числе с учетом простоев приборов, изучены в работах [6–11], где рассматривается как детерминированный, так и стохастический процесс прерываний. Другой цикл работ [12, 13] посвящен исследованию систем типа $M \mid G \mid \infty$, в том числе с внешним марковским управлением, которые моделируют широкий класс систем от телекоммуникационных до биологических.

Однако довольно мало исследований в рамках моделей управляемых марковских систем или управляемых СМО для систем $M \mid M \mid 1\ PS$, $M \mid G \mid c$, $M \mid G \mid \infty$, т. е. проблема оптимального управления для систем класса $M \mid G \mid \infty$ является актуальной.

Задача оптимального управления СМО с $K > 2$ неоднородными приборами при различных предположениях относительно входного потока требований (пуассоновского, рекуррентного, марковского) и распределений длительностей их обслуживания (показательных, эрланговских или фазового типа) подробно изучена в работах [14–16]. Показано [14], что оптимальная дисциплина обслуживания требований в системе с K приборами фиксированной суммарной производительностью $M = \mu_1 + ... + \mu_K$ ($\mu_1 > \mu_2 > ... > \mu_K$) с ожиданием и конечной очередью по критерию минимизации среднего числа требований в системе имеет пороговый характер. Суть дисциплины обслуживания порогового типа заключается в том, что относительно критерия «среднее время

пребывания требования в системе» оптимальная дисциплина определяет для каждого состояния системы $x = (q, d_1, ..., d_K)$, где q — длина очереди; $d_i = 1$, если i-й прибор включен, и $d_i = 0$, если i-й прибор выключен, значение $q_j^*(x) = q^*(x)$ порога длины очереди q, начиная с которого ($q_j^*(x) \geq q^*(x)$, $q(x)$ — длина очереди в состоянии x) включается прибор j с наибольшей производительностью из оставшихся выключенных приборов. Значение порога $q_j^*(x)$ включения j-го прибора определяется соотношением

$$q_j^*(x) = \left[\frac{1}{\mu_j}\sum_{k=1}^{j-1}\mu_k\right] - (j-1),\ j = 2, 3, \ldots, K.$$

При этом система описывается управляемыми случайными процессами; для функции потерь в задаче оптимизации используется уравнение Беллмана. В работе [17] вычислены различные характеристики производительности СМО с неоднородными приборами при различных дисциплинах занятия приборов.

В то время как описанные выше многолинейные СМО являются адекватной моделью работы узла сети передачи данных, модель вычислительного узла слабо проработана в рамках теории управляемых СМО.

В настоящей работе проводится исследование типа оптимального управления системой $M \mid M \mid \infty$ в предположении, что производительность системы по выполняемому требованию зависит от числа уже выполняемых требований в системе. Для системы строится стохастическая модель процесса в дискретном времени как приближение к однородным управляемым марковским процессам с непрерывным временем, конечными пространствами состояний и управлений и аддитивным функционалом потерь. При этом используется модель авторегрессии и скользящего среднего [18]. Приближение дискретного времени позволяет сформулировать основные уравнения системы и проанализировать пространства решений, а также использовать имитационное моделирование для исследования поведения системы. Возможность построения моделей СМО в приближении непрерывного или дискретного времени подробно обсуждается в работе [19].

Математическая и имитационная модели системы $M \mid M \mid \infty$ с очередью переменной длины

Будем считать, что поведение системы описывается случайным процессом. На вход в систему подается однородный поток требований с интенсивностью $\lambda(t)$. В системе предусмотрена очередь ограниченной длины r. Дисциплина обслуживания: требования из очереди принимаются на выполнение в том случае, если система свободна или очередь полностью заполнена в момент поступления нового требования в систему. Величины $r, d_1, d_2, ..., d_n...$ — параметры управления; $L(r)$ — накладные расходы на содержание очереди длины r в системе; производительность системы $\mu(n)$ — количество требований, обрабатываемых в единицу времени при условии, что в системе обрабатывается n требований, требования начали обрабатываться в один и тот же момент времени и время выполнения требования распределено по показательному закону. Пусть $\mu(n)$ имеет вид $\mu(n) = \beta + (\alpha n)^{-1}$ при $n \geq 1$, не зависит от числа требований в очереди и не является случайной величиной при фиксированном значении n. Введем для дальнейшего изложения обозначение $\mu(1) = \mu_0$. Входящий поток опишем процессом восстановления, а именно введем случайную величину $S_k = T_1 + ... + T_k$, где S_k есть время поступления k-го требования в систему; величина k — случайная, зависящая от времени; T_i — независимые одинаково распределенные экспоненциально величины. Введем случайную величину Q_k — время окончания выполнения k-го требования.

Введем предположения:

1) порядок окончания выполнения требований совпадает с порядком их поступления в систему;

2) величина $\mu(n)$ не является случайной величиной при фиксированном значении n.

Пусть t_k — момент поступления k-го требования из очереди на выполнение. Выражение

$$\int_{t_k}^{\tau_k} \mu(t)\mathrm{d}t = 1$$

определяет для k-го требования, поступившего в момент времени t_k, момент времени его выполнения $\tau_k (Q_k = \tau_k)$. Производительность системы $\mu(t)$ — случайный скачкообразный процесс с разрывами в точках t_i и τ_j такой, что $\mu(t) = \mu(n_t)$, где n_t — случайная величина — число обрабатываемых требований в системе. Таким образом, время выполнения i-го требования зависит от случайных моментов времени поступления входящих требований в процессе его выполнения и моментов времени окончания выполнения требований в интервале времени выполнения i-го требования. При этом наличие очереди не предполагается.

В случае если верно предположение 1, момент времени окончания выполнения k-го требования будем определять из уравнения

$$\int_{t_1}^{\tau_k} \mu(t)\mathrm{d}t = k. \qquad (1)$$

Уравнение (1) можно переписать в терминах случайных величин S_k и Q_k следующим образом:

$$\alpha_n Q_n = -n + \mu S_1 - \beta \sum_{k:\, S_k \le t} S_k + \sigma \sum_{k<n} Q_k, \qquad (2)$$

где $\alpha_n = \mu - \beta N_t + \sigma(n-1)$; β — падение производительности при поступлении требования в систему; σ — возрастание производительности при окончании выполнения требования.

В том случае если допускается $\tau_k > \tau_j$ при $k<j$, то уравнение (1) перепишется в виде

$$\int_{t_1}^{\tau_k} \mu(t)\mathrm{d}t = G_t, \qquad (3)$$

где G_t — число выполненных требований к моменту времени t.

При этом выражение (2) заменится на выражение

$$\alpha_n Q_n = -G_t + \mu S_1 - \beta \sum_{k:S_k<t} S_k + \sigma \sum_{k:Q_k<t} Q_k, \qquad (4)$$

где $\alpha_n = \mu - \beta N_t + \sigma G_t$; $Q_n \ge t$.

Если предположить случайный характер времени обслуживания в расчете на одно требование, то выражения (2), (4) преобразуются к виду

$$\alpha_n Q_n = -G_t + \mu S_1 - \sum_{k:S_k<t} \beta_k S_k + \sum_{k:Q_k<t} \sigma_k Q_k. \qquad (5)$$

Для оценки статистических характеристик случайной последовательности Q_k, определяемой выражением (2), требуется это выражение преобразовать к модели авторегрессии и скользящего среднего с «белым шумом» и дать статистическую оценку математического ожидания, среднеквадратичного отклонения и функции ковариации. При этом аналитическая постановка задачи фильтрации, описывающей преобразование входящего потока в выходящий поток, затруднена.

В настоящей работе задача расчета величины очереди рассматривается в среде имитационного моделирования AnyLogic Professional 6.4.1, т. е. воспроизводится процесс преобразования входящего потока в выходящий поток и подбирается оптимальное значение очереди, минимизирующее среднее время пребывания требования в системе.

Для проведения экспериментов, подтверждения адекватности построенной модели и полученных результатов были приняты следующие параметры модели и их значения:

1) интенсивность потока требований (задач) требования (lambda) от 0,04 до 0,06 с шагом 0,01;

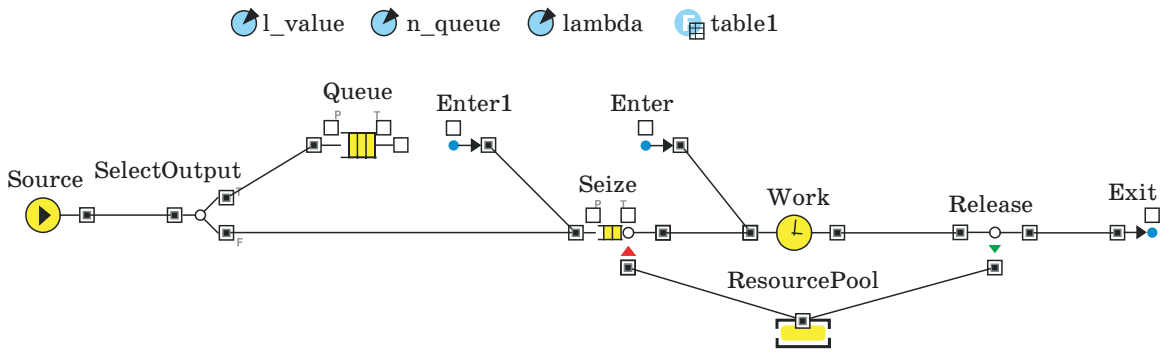
2) кортеж требований (l_value) от 1500 до 2500 с шагом 500 (ограничивает количество поступаемых требований в систему);

3) вместимость очереди (n_queue) от 1 до 50 с шагом 1 (ограничивает максимальное количество требований, находящихся в очереди);

4) закон падения производительности (table1). Значения зависимости количества одновременно обслуживаемых требований от времени их выполнения задаются в табличной форме, после чего производится экстраполяция. Исходные значения нами были получены с помощью эксперимента: производился запуск архивации файла и замер времени выполнения этой операции. Затем эксперимент проводился для двух файлов одинакового объема одновременно. Далее количество файлов на параллельную архивацию увеличивали.

Реализованы параметрические статистические оптимизационные эксперименты. Проводилось усреднение по серии более 100 экспериментов для каждого набора параметров. Вычислялось минимальное значение очереди по критерию минимального среднего времени обслуживания требований в системе с учетом пребывания требований в очереди.

Данная система (рис. 1) построена на стандартных элементах и классах библиотеки Enterprise Library пакета имитационного моделирования AnyLogic Professional 6.4.1.



■ ***Рис. 1.*** Схема модели системы в пакете AnyLogic Professional 6.4.1

Для моделирования объекта *Source* взят стандартный класс Entity, который модифицирован добавлением уникального идентификатора заявки и начального времени обслуживания заявки. Поток заявок является пуассоновским, table1.get(0) задает время обслуживания заявки для одной выполняемой заявки в системе.

Объект *SelectOutput* направляет входящие требования в один из двух выходных портов в зависимости от выполнения заданного условия. Поступившее требование покидает объект SelectOutput в тот же момент времени и поступает в очередь (queue) при условии, что в данный момент времени существует нагрузка на систему (resourcePool.busy()) и очередь не заполнена (queue.canEnter()). Если же очередь заполнена, то первое стоящее в очереди требование поступает на обработку (Enter1.take()), а текущее требование становится в очередь. В противном случае, если система не нагружена, требование отправляется на обслуживание (seize). Объект *Queue* моделирует очередь требований. Вместимость данного объекта задается параметром n_queue.

Требования покидают объект только путем вызова функции removeFirst(). *Enter1* — технический элемент модели, служащий для маршрутизации требований из очереди (queue) на обслуживание с помощью функции take(). *ResourcePool* задает набор ресурсов, которые могут захватываться и освобождаться требованиями с помощью объектов *Seize*, *Release*. В данной модели используется моделирование ресурса как числа (а не отдельного объекта), что позволяет получать с помощью метода resourcePool.busy() текущее количество одновременно обслуживаемых требований в каждый дискретный момент времени.

Попадая на обслуживание в объект *Seize*, очередное требование захватывает с собой ресурс и освобождает его только после обслуживания. Реализация данного элемента позволяет моделировать многопоточность обслуживания требования и перерасчет времени обслуживания для каждого требования.

Seize захватывает для требования заданное количество ресурсов определенного типа. При захвате ресурса требование мгновенно покидает этот объект. Для моделирования процесса (эффекта) падения производительности при увеличении количества одновременно выполняемых требований был реализован следующий алгоритм при выходе требования из объекта:

1. Изымаются все требования, находящиеся на обслуживании в данный момент, со значением времени, необходимым до конца обслуживания (work.getRemainingTime()).

2. Время обслуживания каждого требования (delay) пересчитывается с учетом коэффициента падения производительности.

3. Рассчитывается время обслуживания текущего требования из расчета текущей производительности системы.

4. Все требования отправляются на обработку одновременно (enter) с заново рассчитанными параметрами.

Enter — технический объект модели, служит либо для поступления требований с пересчитанными параметрами времени обслуживания, изъятых в момент поступления, либо для выхода требования из обслуживания.

Элемент *Work* построен на основе стандартного элемента Delay. Задерживает требование на заданный период времени, тем самым моделируя время обслуживания требования. Данное время задается параметром требования delay. При этом данный объект позволяет задерживать множество требований одновременно. Ограничения по вместимости нет.

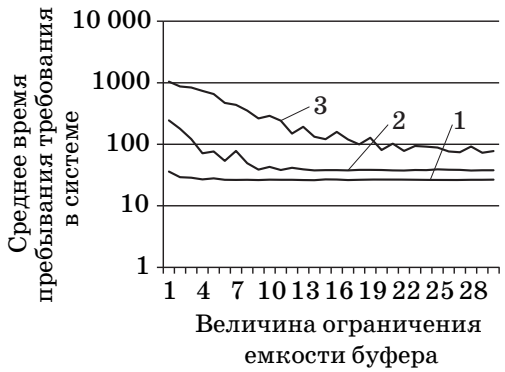
Объект *Release* освобождает после обслуживания требования захваченное им количество ресурсов, тем самым изменяется производительность системы. Соответственно, необходим пересчет времени обслуживания требований, находящихся в текущий момент на обслуживании. Рассматриваемый процесс был реализован с помощью следующего алгоритма:

1. Изымаются все требования, находящиеся на обслуживании в данный момент, со значением времени, необходимым до конца обслуживания (work.getRemainingTime()).

2. Время обслуживания каждого требования (delay) пересчитывается с учетом коэффициента падения производительности.

3. Все требования отправляются на обработку одновременно (enter) с заново рассчитанными параметрами.

4. Если система является не нагруженной (resourcePool.busy()=0) и существуют требования в очереди на обслуживание (queue.size()!=0), то



■ ***Рис. 2***. Зависимость среднего времени пребывания требования в системе от разрешенной величины буфера для значений интенсивности входящего потока: *1* — $\lambda = 0{,}04$; *2* — $\lambda = 0{,}05$; *3* — $\lambda = 0{,}06$; $\mu_0 = 0{,}066$

очередное требование из очереди отправляется на обслуживание.

Объект *Exit* служит для учета времени окончания обслуживания требования.

Результаты проведенных экспериментов, представленных на рис. 2, позволяют высказать гипотезу о существовании для значений $\lambda/\mu_0 \sim 1$ величины очереди (емкости буфера) $r_b(\lambda, \mu)$, минимизирующей функцию критерия «среднее время пребывания требования в системе». Дисперсия случайной величины также минимизируется, начиная с порогового значения очереди r_b.

Заключение

Предложенная модель позволяет использовать в качестве управляющего параметра длину очереди требований, ожидающих обработку, в зависимости от интенсивности потока заявок и закона падения производительности.

Дальнейшее исследование $r_b(\lambda, \mu)$ для системы необходимо проводить для значений $\lambda / \mu_0 > 1 + \varepsilon$, проводить расчет среднего времени пребывания требования в очереди, вводить функцию потерь, учитывающую затраты на содержание очереди.

Литература

1. **Kleinrock L.** Time-Shared Systems: a Theoretical Treatment // Journal of the ACM. 1967. Vol. 14. N 2. P. 242–261.
2. **Cohen J. W.** The Multiple Phase Service Network with Generalized Processor Sharing // Acta Information. 1979. Vol. 12. N. 3. P. 245–284.
3. **Guillemin F., Boyer J.** Analysis of the M/M/1 Queue with Processor Sharing via Spectral Theory // Queueing Systems. 2001. Vol. 39. P. 377–397.
4. **Kim J., Kim B.** Sojourn Time Distribution in the M/M/1 Queue with Discriminatory Processor-Sharing // Performance Evaluation. 2004. Vol. 58. N 4. P. 341–365.
5. **Рыков В. В.** Управляемые системы массового обслуживания // Итоги науки и техники. Сер. Теория вероятностей и математическая статистика. Теория кибернетики. 1975. Т. 12. С. 43–153.
6. **Bansal N.** Analysis of the M/G/1 Processor-Sharing Queue with Bulk Arrivals // Operations Research Letters. 2003. Vol. 31. N 5. P. 401–405.
7. **Avrachenkov K. E., Ayesta U., Brown P.** Batch Arrival Processor-Sharing with Application to Multi-Level Processor-Sharing Scheduling // Queueing Systems. 2005. Vol. 50. P. 459–480.
8. **Brandt A., Brandt M.** Workload and Busy Period for M/GI/1 with a General Impatience Mechanism // Queueing Systems. 2013. Vol. 75. P. 189–209.
9. **Yamamuro K.** The Queue Length in an M/G/1 Batch Arrival Retrial Queue // Queueing Systems. 2012. Vol. 70. P. 187–205.
10. **Sigman K.** Exact Simulation of the Stationary Distribution of the FIFO M/G/c Queue: the General Case for $\rho < c$ // Queueing Systems. 2012. Vol. 70. P. 37–43.
11. **Zhang Z. G., Tian N.** Analysis on Queueing Systems with Synchronous Vacations of Partial Servers // Performance Evaluation. 2003. Vol. 52. P. 269–282.
12. **Blom J., Kella O., Mandjes M., Thorsdottir H.** Markov-Modulated Infinite-server Queues with General Service Times // Queueing Systems. 2014. Vol. 76. P. 403–424.
13. **Baykal-Gursov M., Xiao W.** Stochastic Decomposition in M/M/∞ Queues with Markov Modulated Service Rates // Queueing Systems. 2004. Vol. 48. P. 75–88.
14. **Rykov V. V.** Monotone Control of Queueing Systems with Heterogeneous Servers // Queueing Systems. 2001. Vol. 37. P. 391–403.
15. **de Vericourt F., Zhou Y.-P.** On the Incomplete Results for the Heterogeneous Servers Problem // Queueing Systems. 2006. Vol. 52. P. 189–191.
16. **Rykov V. V., Efrosinin D. V.** Optimal Control of Queueing Systems with Heterogeneous Servers // Queueing Systems. 2004. Vol. 46. P. 389–407.
17. **Евфросинин Д. В., Рыков В. В.** К анализу характеристик производительности СМО с неоднородными приборами // Автоматика и телемеханика. 2008. № 1. С. 64–82.
18. **Shiryaev A. N.** Problems in Probability. Problem Books in Mathematics. — N. Y.: Springer, 2012. — 427 p.
19. **Бочаров П. П., Печенкин А. В.** Теория массового обслуживания / РУДН. — М., 1995. — 529 с.

UDC 519.876.2, 519.876.5

Optimal Control of Queues in Queueing Systems with Limited Performance

Zubok D. A.[a], PhD, Phys.-Math., Deputy Head of Chair, zubok@mail.ifmo.ru
Maiatin A. V.[a], PhD, Pedagogic, Associate Professor, mayatin@mail.ifmo.ru
[a]Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics, 49, Kronverkskii St., 197101, Saint-Petersburg, Russian Federation

Purpose: For queuing systems with infinite servers, there is no detailed study of the analogues of the threshold nature of the optimal policy queueing systems established for queuing systems with non-homogeneous infinite servers. At the same time, the model systems with infinite servers provide a satisfactory description of the computing nodes with multi-threading. The aim of this study is to discover

the threshold nature of optimal policy control queueing systems for infinite servers with the performance of a server depending on the amount of the requests in the system. **Methods**: To describe queuing, we use processes with discrete time and a finite number of states. In describing the outgoing flow, an autoregressive scheme is used. **Results:** An approach was proposed to the solution of the basic equations of the model. A simulation experiment was carried out to test the hypothesis of the threshold nature of queue management. In the approximation of the processes with discrete time, equations of autoregression and moving average were derived to describe the incoming and outgoing flows of the queueing process. It is assumed that the order of closure compliance coincides with the order in which they are received to be performed. To test the hypothesis of the existence of an optimal queueing discipine, simulation experiments were conducted. In the experiments, the intensity of the incoming flow took values both less and greater than the performance of the system, meeting only one requirement. The simulation experiments showed that the mean time a requirement spends in the system depends on the allowed queue size and the intensity of the incoming stream. Thus, to improve the performance for a given flow rate, we need to uniquely determine the lower bound for the queue value, starting from which the performance of the system does not grow. **Practical relevance:** The proposed mathematical and simulation models can be used for studying single and multi-phase systems with various distributions of run-time requirements and various patterns of productivity drop.

Keywords — Queueing Systems, Infinite Servers, Markov Decision Processes, Servering Quality, Simulation Model.

References

1. Kleinrock L. Time-Shared Systems: a Theoretical Treatment. *Journal of the ACM*, 1967, vol. 14, no. 2, pp. 242–261.
2. Cohen J. W. The Multiple Phase Service Network with Generalized Processor Sharing. *Acta Information*, 1979, vol. 12, no. 3, pp. 245–284.
3. Guillemin F., Boyer J. Analysis of the M/M/1 Queue with Processor Sharing via Spectral Theory. *Queueing Systems*, 2001, vol. 39, pp. 377–397.
4. Kim J., Kim B. Sojourn Time Distribution in the M/M/1 Queue with Discriminatory Processor-Sharing. *Performance Evaluation*, 2004, vol. 58, no. 4, pp. 341–365.
5. Rykov V. V. Controllable Queuing Systems. *Itogi nauki i tekhniki. Seriia "Teoriia veroiatnostei i matematicheskaia statistika. Teoriia kibernetiki"*, 1975, vol. 12, pp. 45–152 (In Russian).
6. Bansal N. Analysis of the M/G/1 Processor-Sharing Queue with Bulk Arrivals. *Operations Research Letters*, 2003, vol. 31, no. 5, pp. 401–405.
7. Avrachenkov K. E., Ayesta U., Brown P. Batch Arrival Processor-Sharing with Application to Multi-Level Processor-Sharing Scheduling. *Queueing Systems*, 2005, vol. 50, pp. 459–480.
8. Brandt A., Brandt M. Workload and Busy Period for M/GI/1 with a General Impatience Mechanism. *Queueing Systems*, 2013, vol. 75, pp. 189–209.
9. Yamamuro K. The Queue Length in an M/G/1 Batch Arrival Retrial Queue. *Queueing Systems*, 2012, vol. 70, pp. 187–205.
10. Sigman K. Exact Simulation of the Stationary Distribution of the FIFO M/G/c Queue: the General Case for $\rho<c$. *Queueing Systems*, 2012, vol. 70, pp. 37–43.
11. Zhang Z. G., Tian N. Analysis on Queueing Systems with Synchronous Vacations of Partial Servers. *Performance Evaluation*, 2003, vol. 52, pp. 269–282.
12. Blom J., Kella O., Mandjes M., Thorsdottir H. Markov-Modulated Infinite-Server Queues With General Service Times. *Queueing Systems*, 2014, vol. 76, pp. 403–424.
13. Baykal-Gursov M., Xiao W. Stochastic Decomposition in M/M/∞ Queues with Markov Modulated Service Rates. *Queueing Systems*, 2004, vol. 48, pp. 75–88.
14. Rykov V. Monotone Control of Queueing Systems with Heterogeneous Servers. *Queueing Systems*, 2001, vol. 37, pp. 391–403.
15. de Veri court F., Zhou Y.-P. On the Incomplete Results for the Heterogeneous Servers Problem. *Queueing Systems*, 2006, vol. 52, pp. 189–191.
16. Rykov V. V., Efrosinin D. V. Optimal Control of Queueing Systems with Heterogeneous Servers. *Queueing Systems*, 2004, vol. 46, pp. 389–407.
17. Efrosinin D. V., Rykov V. V. On Performance Characteristics for Queueing Systems with Heterogeneous Servers. *Automation and Remote Control*, 2008, no. 1, pp. 64–82 (In Russian).
18. Shiryaev A. N. *Problems in Probability. Problem Books in Mathematics.* New York, Springer Publ., 2012. 427 p.
19. Bocharov P. P., Pechinkin A. V. *Teoriia massovogo obsluzhivaniia* [Theory of Queueing Systems]. Moscow, RUDN Publ., 1995. 529 p. (In Russian).

УДК 512.62

ПЕРЕСТАНОВОЧНЫЕ МНОГОЧЛЕНЫ МАЛОЙ ДЛИНЫ НАД ПРОСТЫМИ КОНЕЧНЫМИ ПОЛЯМИ

М. А. Рыбалкин[a, 1], *аспирант*
[a]*Санкт-Петербургское отделение Математического института им. В. А. Стеклова РАН, Санкт-Петербург, РФ*

Постановка проблемы: *перестановочным многочленом над конечным полем называется многочлен, реализующий перестановку элементов конечного поля. В настоящее время не известно эффективных критериев для определения перестановочных многочленов над конечными полями даже для многочленов малой длины, состоящих из нескольких мономов. Для построения таких критериев нами была поставлена задача о построении таблиц перестановочных многочленов, зависимости в которых можно использовать для нахождения новых серий перестановочных многочленов, а также для построения эффективных критериев таких многочленов.* ***Методы:*** *реализация алгоритма перебора на C++, численные эксперименты в системе компьютерной алгебры Sage, вычисление порядков групп перестановок в системе компьютерной алгебры GAP.* ***Результаты:*** *разработан метод перечисления перестановочных многочленов, работающий для многочленов малой длины, на основе которого были вычислены таблицы перестановочных пятичленов для простых конечных полей характеристики до 100. Полученные таблицы пятичленов были сравнены с таблицами перестановочных четырехчленов, трехчленов и двучленов над конечными полями из предыдущих работ. Исследование общих зависимостей и сравнение с предыдущей гипотезой о классификации многочленов меньшей длины позволили сформулировать гипотезу об общей классификации перестановочных многочленов с не более чем пятью членами. Также было проведено исследование статистических свойств случайных перестановок, соответствующих случайному выбору равнораспределенных случайных перестановочных многочленов с фиксированным количеством мономов. Было показано, что получающееся распределение на перестановках уже не является равномерно распределенным.* ***Практическая значимость:*** *сформулированные гипотезы о классификации перестановочных многочленов малой длины являются шагом к построению полной доказанной классификации перестановочных многочленов, а также могут быть использованы при построении криптографических протоколов с открытым ключом на основе перестановочных многочленов.*

Ключевые слова *— перестановочные многочлены, конечные поля, криптография с открытым ключом.*

Введение

Пусть p — просто число и $q = p^n$. Многочлен $f(x)$ называется перестановочным многочленом над конечным полем $GF(q)$, если соответствующее ему отображение задает перестановку элементов множества $GF(q)$. Перестановочный многочлен можно использовать как полиномиальную форму перестановки. Исследование перестановочных многочленов началось с работ Эрмита и Диксона [1, 2]. Перестановочные многочлены могут представлять собой краткую форму нетривиальных перестановок над конечными полями, и в связи с этим в настоящее время наблюдается повышение интереса к перестановочным многочленам из-за их потенциальных приложений в криптографии, теории кодирования и комбинаторике. Над конечным полем $GF(q)$ существует $q!$ перестановок, и каждую такую перестановку задает единственный перестановочный многочлен степени, меньшей q, который может быть получен как интерполяционный многочлен. Интерес представляют задачи о характеризации перестановок, которые бы соответствовали многочленам с небольшим количеством членов: двучленам, трехчленам, четырехчленам и пятичленам. Иногда такие многочлены называются малочленами. Их важным обобщением являются многочлены с низкой алгоритмической сложностью вычисления. Также очень интересной является задача об исследовании полиномиальной формы перестановок определенного вида, например транспозиций и инволюций.

Теория перестановочных многочленов содержит большое число открытых вопросов и гипотез [3, 4]: вопрос об эффективном критерии различных классов перестановочных многочленов, сложность нахождения обратной перестановки, нахождение новых серий перестановочных многочленов, нахождение критериев перестановочных двучленов и трехчленов, вопрос о возможности и эффективности использования перестановочных многочленов в криптографии.

В данной работе исследуются перестановочные многочлены малой длины, а именно двучлены, трехчлены, четырехчлены и пятичлены. Такие многочлены могут быть использованы в качестве компактного представления нетривиальных перестановок и при этом имеют эффективную процедуру вычисления значений ввиду малой длины. Нами был разработан метод по перечислению перестановочных многочленов малой длины, а также проведен анализ его результатов. На основе данного анализа мы выдвинули гипотезу о классификации перестановочных пятичленов над простыми конечными полями.

[1] Научный руководитель — кандидат физико-математических наук, старший научный сотрудник лаборатории теории представлений и динамических систем Санкт-Петербургского отделения Математического института им. В. А. Стеклова Российской академии наук *Н. Н. Васильев*.

Связь между перестановочными многочленами и перестановками

Группы, порождаемые перестановочными двучленами

Каждой перестановке элементов конечного поля можно сопоставить перестановочный многочлен, задающий данную перестановку. Тогда композиции многочленов будет соответствовать умножение перестановок, а значит можно рассматривать группы, образованные перестановочными многочленами разных классов. В 1953 г. было доказано [5] в общем случае, что вся группа перестановок S_q конечного поля $GF(q)$ порождается линейными многочленами и многочленом x^{q-2}. Нами были исследованы перестановочные двучлены над конечными полями [6], и для некоторых конечных полей мы обнаружили, что перестановочные двучлены порождают всю группу S_{q-1} перестановок, оставляющих элемент 0 неподвижным. Обозначим через $G(q)$ группу, порожденную перестановочными двучленами. Факт об изоморфизме S_{q-1} и $G(q)$ может быть обобщен и сформулирован в виде гипотезы 1.

Гипотеза 1. Существует бесконечное количество конечных полей $GF(q)$, для которых симметрическая группа S_{q-1} перестановок, оставляющих элемент 0 неподвижным, порождается перестановками, задаваемыми перестановочными двучленами $ax^n + bx^m$.

Экспериментально данная гипотеза бала нами проверена для следующих порядков конечных полей: 31, 61, 64, 211, 256, 421, 841, 1024, 1331, 1849, 2521, 2809, 3125, 3481, 3721, 4096, 4489, 4621. Можно отметить, что среди данной последовательности есть все элементы вида 4^n, $n > 2$. В недавней работе [7] был доказан частный случай гипотезы 1 для случая конечных полей $GF(p^2)$ в следующем виде.

Теорема 2 ([7], *частный случай гипотезы*). Существует бесконечно много простых чисел p, для которых группа $G(p^2)$ изоморфна S_{p^2-1}. В частности:

$$\liminf_{N\to\infty} \frac{\text{количество } p : G(p^2) \cong S_{p^2-1}}{\text{количество простых } p < N} \geq \frac{1}{96}.$$

Вопрос о справедливости гипотезы 1 для случая простых конечных полей остается открытым.

Инволюции

Интересным вопросом является характеризация перестановочных многочленов, задающих инволюции, т. е. перестановок, обратными к которым являются они сами. Нами были рассмотрены два вида перестановочных двучленов, задающих инволюции. Критерии таких многочленов представлены в виде теорем 3 и 4, доказательство которых может быть получено проверкой условия $f(x) = x \bmod x^p - x$.

Теорема 3 (*класс 1*). Перестановочный многочлен $ax\left(b + x^{\frac{p-1}{2}}\right)$ над простым конечным полем $GF(p)$ задает инволюцию тогда и только тогда, когда $a^2(b^2 - 1) = 1$ и $\chi(b + 1) = \chi(b - 1) = \chi(a)$, где χ — квадратичный характер.

Теорема 4 (*класс 2*). Перестановочный многочлен $ax^{\frac{p-3}{2}}\left(b + x^{\frac{p-1}{2}}\right)$ над простым конечным полем $GF(p)$ задает инволюцию тогда и только тогда, когда $\chi(b^2 - 1) = -1$ и $\chi(b + 1) = \chi(a)$.

Количество перестановочных двучленов указанных классов над простым конечным полем $GF(p)$ равно $\frac{p-3}{2}$ и $\frac{p-1}{2}\frac{p-3}{2}$ соответственно. Можно показать, что если $\frac{p-1}{2}$ является простым числом, то не существует других классов перестановочных двучленов, задающих инволюции. Вопрос о полной классификации перестановочных многочленов, задающих инволюции, представляет большой интерес и будет рассмотрен в следующих работах.

Перечисление перестановочных многочленов малой длины

Нормированный многочлен с фиксированным количеством членов описывается его степенями и всеми коэффициентами за исключением старшего.

Например, в общем случае для перечисления всех перестановочных четырехчленов требуется найти множество наборов $(n_1, n_2, n_3, n_4, c_2, c_3, c_4)$ таких, что многочлен $x^{n1} + c_2x^{n2} + c_3x^{n3} + c_4x^{n4}$ является перестановочным. Множество перестановочных многочленов над любым конечным полем $GF(q)$ бесконечно, так как к любому перестановочному многочлену можно добавить $x^q - x$. Поэтому достаточно перечислять многочлены степени, меньшей q. Они представляют все полиномиальные перестановки над $GF(q)$. Для сокращения пространства поиска нами используется тот факт, что композиция перестановочных многочленов также является перестановочным многочленом. Если рассмотреть всевозможные подстановки перестановочных одночленов x^k, можно ввести ограничения на перебираемые значения $(n_1, n_2, n_3, n_4, c_2, c_3, c_4)$ и существенно сократить пространство поиска. Так, например, если мы нашли перестановочный многочлен, то из процесса перечисления можно исключить все многочлены, получаемые из данного подстановками перестановочных одночленов x^k с последующим

приведением по модулю $x^q - x$. Представителей из класса эквивалентных многочленов будем называть представительными многочленами.

По аналогии с алгоритмом перечисления перестановочных двучленов [6] можно показать, что достаточно проверять показатели степеней (n_1, n_2, n_3, n_4), удовлетворяющие следующим свойствам:

1) $n_1 < n_2 < n_3 < n_4$;
2) $\gcd(n_1, n_2, n_3, n_4) = 1$;
3) $n_1 \mid q - 1$;
4) $n_1 \geq \gcd(n_i, q - 1)$ для $i = 2, 3, 4$.

Для дальнейшего использования обозначим через $NoneqDeg(q)$ множество показателей степеней (n_1, n_2, n_3, n_4), удовлетворяющих приведенными выше условиями.

Одним из основных инструментов для проверки критерия перестановочного многочлена общего вида является критерий Эрмита.

Теорема 5 (*критерий Эрмита*). Пусть p — характеристика поля $GF(q)$. Тогда многочлен $f \in GF(q)[x]$ является перестановочным многочленом тогда и только тогда, когда:

1) для любого i от 1 до $q - 2$ и $i \neq 0 \bmod p$ результат приведения f^i по модулю $x^q - x$ имеет степень меньше $q - 1$;

2) многочлен f имеет ровно один корень в $GF(q)$.

Критерий Эрмита позволяет доказывать, что какой-то многочлен не является перестановочным, так как для этого достаточно привести значение i такое, что $\deg(f^i \bmod x^q - x) = q - 1$. Вместе с тем если показатели степеней мономов фиксированы, а неизвестны только коэффициенты при этих мономах, критерий Эрмита позволяет получить систему полиномиальных уравнений, соответствующих коэффициенту при мономе x^{q-1} в многочлене $f^i \bmod x^q - x$ для всех i от 1 до $q - 2$. На практике же такие коэффициенты, как многочлены от коэффициентов c_2, c_3, c_4, могут быть очень большими, и для многих многочленов длина коэффициента начинает экспоненциально расти вместе с ростом i, что не позволяет использовать критерий Эрмита напрямую. Поэтому с вычислительной точки зрения имеет смысл проверять коэффициент при x^{p-1} только в том случае, если длина этого коэффициента мала. Для нахождения коэффициентов малой длины в данной работе предлагается вычислять усеченные степени $f^i \bmod x^q - x$, где все длины коэффициентов меньше наперед заданного ограничения N. Если длина какого-то коэффициента становится больше N, то он заменяется на неизвестное значение ε. При этом вводится тождество, что умножение любого многочлена f на неизвестное значение ε также дает неизвестное значение ε, что можно записать как $f\varepsilon = \varepsilon$.

Через $Truncate_N(f)$ обозначим функцию, которая заменяет коэффициенты многочлена f на ε, если длина такого коэффициента больше N. Тогда получение условий из критерия Эрмита можно записать в виде следующего алгоритма:

Вход: f — многочлен с неизвестными коэффициентами

Выход: условия в критерии Эрмита длины меньше N

function $TruncatedHermite_N(f)$
$f' := f$
$Conditions := \varnothing$
for all $i = 2..q - 2$ **do**
$f' := Truncate_N(f' f \bmod x^q - x)$
$c := Coef(f', x^{q-1})$
if $i \neq 0 \bmod p$, $c \neq 0$, $c \neq \varepsilon$ **then**
$Conditions := Conditions \cup \{c\}$
end for
return $Conditions$
end function

Для конкретных показателей степеней (n_1, n_2, n_3, n_4) алгоритм для вычисления $TruncatedHermite_N(f)$ позволяет получить из критерия Эрмита условия, длина которых не превосходит N. Если множество таких условий оказалось пустым или состоящим только из одного-двух элементов, это значит, что выражения в критерии Эрмита имеют большую длину, и для их получения можно просто увеличить N. На практике нами использовалось начальное значение $N = 5$ с последующим увеличением до 60. Существуют многочлены, для которых все условия Эрмита имеют большую длину, но которые не являются перестановочными многочленами ни для каких значений параметров. Примером такого многочлена является $x + c_2x^2 + c_3x^{166} + c_4x^{167}$ над $GF(331)$.

Итоговый алгоритм перечисления перестановочных четырехчленов можно записать в следующем виде:

Вход: q — порядок конечного поля

Выход: перестановочные четырехчлены вида $x^{n_1} + c_2x^{n_2} + c_3x^{n_3} + c_4x^{n_4}$

for all (n_1, n_2, n_3, n_4) **in** $NoneqDeg(q)$ **do**
$HermiteConditions :=$
$:= TruncatedHermite_N(x^{n_1} + c_2x^{n_2} + c_3x^{n_3} + c_4x^{n_4})$
for all (c_2, c_3, c_4) **in** Solve($HermiteConditions$)
$f := x^{n_1} + c_2x^{n_2} + c_3x^{n_3} + c_4x^{n_4}$
if f — перестановочный многочлен
yield f
end for
end for

Алгоритм для перечисления трехчленов и пятичленов аналогичен данному алгоритму. На практике данный алгоритм применим для перечисления перестановочных многочленов, содержащих до пяти членов, т. е. двучленов, трехчленов, четырехчленов и пятичленов. Этот алгоритм позволил перечислить все перестановочные пятичлены для простых конечных полей $GF(p)$, $p < 100$,

■ ***Таблица 1.*** Примеры перестановочных малочленов

Перестановочный многочлен	Конечное поле
$x + 61x^{45}$	$GF(67)$
$x + 122x^{114}$	$GF(227)$
$x^3 + 154x^{263}$	$GF(313)$
$x^4 + 194x^{241}$	$GF(317)$
$x + 143x^{174}$	$GF(347)$
$x + x^2 + 44x^3$	$GF(131)$
$x + 6x^{39} + 49x^{77}$	$GF(229)$
$x^3 + 20x^{210} + 200x^{256}$	$GF(277)$
$x + 194x^{142} + 257x^{189}$	$GF(283)$
$x + x^2 + 24x^4 + 33x^5$	$GF(53)$
$x + x^4 + 66x^{34} + x^{37}$	$GF(67)$
$x^2 + 8x^{15} + 53x^{28} + 11x^{54}$	$GF(79)$
$x + x^{40} + 82x^{42} + x^{81}$	$GF(83)$
$x + 2x^3 + 46x^5 + 40x^7 + 9x^9$	$GF(59)$
$x^4 + 4x^{16} + 12x^{25} + 47x^{28} + 9x^{52}$	$GF(61)$

все четырехчлены при $p < 500$ и все трехчлены для простых конечных полей $GF(p)$, $p < 5000$. Примеры некоторых перечисленных многочленов приведены в табл. 1. Результаты перечислений и гипотезы о свойствах перестановочных малочленов приводятся в следующих разделах.

Анализ серий и классификация перестановочных многочленов

Любой многочлен над конечным полем $GF(q)$ может быть представлен в виде $x^r f\left(x^{\frac{q-1}{d}}\right)$, где значение параметра d является важной характеристикой. Такое представление является интересным при $d > 1$. Так, проверка перестановочного многочлена может быть осуществлена за $O(d^2)$ операций [8, 9], а многочлен, соответствующий обратному отображению, также может быть найден за $O(d^2)$ операций [10]. При фиксированном d класс таких многочленов замкнут относительно операции композиции, и в работе [8] исследуется размер порождаемой группы. В работе [11] доказывается, что для перестановочных двучленов над простыми конечными полями $GF(p)$ значение d ограничено снизу значением $\sqrt{p}$, а также выдвигается гипотеза о том, что $d < 2\log p$. При выполнении этой гипотезы за полиномиальное время могут быть эффективно реализованы следующие операции с перестановочными двучленами над конечными полями:

1) проверка того, что двучлен является перестановочным;

2) построение случайных перестановочных двучленов;

3) нахождение многочлена, соответствующего обратному отображению.

Из работы [11] следует, что все множество перестановочных двучленов принадлежит одному классу вида $x^r f\left(x^{\frac{p-1}{d}}\right)$, где $d < 2\log p$ в предположении справедливости гипотезы о классификации. В нашей предыдущей работе [12] была предложена гипотеза о классификации, которая показывает, что для трехчленов и четырехчленов большинство многочленов принадлежит аналогичному классу, но в дополнение для трехчленов появляется еще один класс, а для четырехчленов появляются два класса. Экспериментальные результаты данной работы показывают, что классификация для пятичленов также аналогична классификации для четырехчленов.

Сравнение классификаций для перестановочных двучленов, трехчленов и четырехчленов и пятичленов приведено в табл. 2. Класс 1 содержит все многочлены вида $x^r f\left(x^{\frac{p-1}{d}}\right)$, свойства которых были описаны выше.

Неравенство в ограничении на d не является строгим, но позволяет сравнить соответствующее значение для многочленов разной длины. Из таблицы видно, что с увеличением длины многочлена значение d также увеличивается. Класс 2 представляет собой композицию монома и многочлена малой степени. При этом прослеживается зависимость между степенью такого многочлена: она ограничена значением $2n - 1$, где n — длина многочлена.

■ ***Таблица 2.*** Классификация перестановочных многочленов

Тип	Класс 1 $x^r f\left(x^{\frac{p-1}{d}}\right)$	Класс 2 $f\left(x^r\right)$	Специальный класс
Двучлены	$d < 2\log p$	—	—
Трехчлены	$d < 4\log p$	$\deg f \le 5$	—
Четырехчлены	$d < 6\log p$	$\deg f \le 7$	Серия Эрмита [12]
Пятичлены	$d < 8\log p$	$\deg f \le 9$	Новый класс

■ ***Таблица 3.*** Примеры перестановочных пятичленов, попадающих в классы 1 и 2

Перестановочный пятичлен	Конечное поле
$x + 6x^3 - 9x^{21} + 6x^{22} + 13x^{23}$	$GF(41)$
$x + 2x^3 - x^5 + 6x^{28} - 21x^{30}$	$GF(53)$
$x + x^7 + x^{29} - x^{45} + x^{51}$	$GF(67)$
$x + x^7 + x^{23} + x^{45} - x^{51}$	$GF(67)$
$x + x^{21} + x^{23} - x^{43} + x^{45}$	$GF(67)$

■ ***Таблица 4.*** Среднее значение нормированной длины наибольшего цикла

p	Двучлены	Трехчлены	Четырехчлены	Пятичлены
29	0,366	0,394	0,434	0,479
31	0,350	0,365	0,440	0,478
43	0,259	0,356	0,435	0,491
53	0,240	0,306	0,307	0,432

Классификация перестановочных четырехчленов [14] содержит класс, названный серией Эрмита ввиду того, что он был приведен в работе Эрмита [1] в качестве примера нетривиального перестановочного многочлена:

$$ax^r\left(x^{\frac{p-1}{2}}+1\right)+bx^m\left(x^{\frac{p-1}{2}}-1\right).$$

Экспериментальные результаты по перестановочным пятичленам также содержат небольшое число многочленов, не принадлежащих классу 1 и 2 и похожих на многочлены из серии Эрмита, но вычислительная сложность перечисления не позволила нам получить достаточное количество таких многочленов, чтобы можно было обобщить их форму. Несколько таких многочленов приведены в табл. 3. Обобщение данного класса будет сделано в следующих работах.

Анализ результатов перечисления показывает, что большинство перестановочных многочленов малой длины принадлежит первому классу, т. е. представимо в виде $x^r f\left(x^{\frac{p-1}{d}}\right)$ с малым значением параметра d.

Исследование статистических свойств перестановочных многочленов

Одним из основных приложений теории перестановочных многочленов может стать криптография с открытым ключом, в которой перестановочный многочлен будет использоваться в качестве функции шифрования. Данный вопрос поднимался в нескольких работах [13–15]. В работе [6] показано, что перестановочные двучлены не подходят на роль обобщения криптографического протокола RSA ввиду свойств степеней мономов. При этом вопрос об использовании более сложных многочленов остается открытым.

Разбиение перестановочных многочленов по количеству мономов естественным образом соответствует мере случайности задаваемых перестановок: перестановочные многочлены длины q задают все перестановки над конечным полем $GF(q)$, в то время как перестановочные одночлены x^k задают перестановки с простой структурой циклов, которые не могут считаться случайными. Но многочлены меньшей длины могут быть вычислены за меньшее время. Использование перестановок, заданных перестановочными многочленами малой длины, позволяет эффективно вычислять данные перестановки, а также исследовать получаемые алгоритмы алгебраическими методами. При этом возникает вопрос, насколько такие перестановки могут быть отличимы от случайных перестановок, и для этого можно исследовать различные статистики. Нами была исследована максимальная длина цикла, соответствующая двучленам, трехчленам, четырехчленам и пятичленам, нормированная на длину перестановки. Для случайной перестановки данная статистика равна постоянной Голомба — Дикмана $\lambda \approx 0{,}6243$ [16]. Соответствующие значения для перестановочных многочленов над некоторыми конечными полями приведены в табл. 4.

Экспериментальные результаты, приведенные в табл. 4, показывают, что перестановочные многочлены малой длины задают перестановки, статистические свойства которых значительно отличаются от случайных перестановок с равномерным распределением. Вопрос об асимптотическом поведении данных характеристик для перестановочных многочленов остается открытым.

Заключение

В представляемой работе описывается алгоритм перечисления и исследуются свойства перестановочных многочленов малой длины над простыми конечными полями. Об общих свойствах таких перестановочных многочленов малой длины известно очень мало, поэтому для нахождения таких свойств нами были применены компьютерные эксперименты по полному перечислению таких многочленов. Задача перечисления является алгоритмически сложной ввиду огромного пространства поиска параметров многочлена, и для перечисления нами были разработаны различные методы по сокращению этого пространства поиска.

Анализ результатов компьютерного перечисления позволил сформулировать гипотезы

о классификации перестановочных многочленов, состоящих не более чем из пяти членов. Эта классификация является расширением аналогичной классификации перестановочных двучленов, в которую были добавлены два новых класса. Также на основе проведенных компьютерных вычислений можно сделать наблюдение о том, что все множество перестановочных пятичленов может быть разбито на три класса. Вопрос о доказательстве полноты и корректности этой классификации будет предметом обсуждения в последующих работах.

Литература

1. **Hermite C.** Sur Les Fonctions de Sept Lettres // C. R. Acad. Sci. Paris. 1905. P. 750–757.
2. **Dickson L. E.** The Analytic Representation of Substitutions on a Power of a Prime Number of Letters with a Discussion of the Linear Group // Annals of Mathematics. 1896. Vol. 11. N 1/6. P. 161–183.
3. **Lidl R., Mullen G. L.** When Does a Polynomial over a Finite Field Permute the Elements of the Field? // The American Mathematical Monthly. 1988. Vol. 95. P. 243–246.
4. **Lidl R., Mullen G. L.** When Does a Polynomial over a Finite Field Permute the Elements of the Field? II // The American Mathematical Monthly. 1993. Vol. 100. P. 71–74.
5. **Carlitz L.** Permutations in a Finite Field // Proc. of the American Mathematical Society. 1953. Vol. 4. P. 538.
6. **Vasilev N., Rybalkin M.** Permutation Binomials and their Groups // J. of Mathematical Sciences. 2011. Vol. 179. P. 679–689.
7. **Zieve M. E.** Permutation Groups Generated by Binomials // ArXiv e-prints. Dec. 2013. http://arxiv.org/pdf/1312.2649.pdf (дата обращения: 13.01.2014).
8. **Wan D., Lidl R.** Permutation Polynomials of the Form $x^r f(x^{(q-1)/d})$ and their Group Structure // Monatshefte fur Mathematik. 1991. Vol. 112. N 2. P. 149–163.
9. **Zieve M. E.** On Some Permutation Polynomials over Fq of the Form $x^r h(x^{(q-1)/d})$ // Proc. of the American Mathematical Society. 2009. Vol. 137. N 7. P. 2209–2216.
10. **Wang Q.** On Inverse Permutation Polynomials // Finite Fields and Their Applications. 2009. Vol. 15. N 2. P. 207–213.
11. **Masuda A. M., Zieve M. E.** Permutation Binomials over Finite Fields // Transactions of the American Mathematical Society. 2009. Vol. 361. N 8. P. 4169–4180.
12. **Рыбалкин М.** Классификация перестановочных многочленов малой длины над простыми конечными полями // Записки научных семинаров ПОМИ. 2014. № 421. С. 152–165.
13. **Singh R. P., Sarma B. K., Saikia A.** Public Key Cryptography Using Permutation p-polynomials over Finite Fields // IACR Cryptology ePrint Archive. 2009. http://eprint.iacr.org/2009/208 (дата обращения: 23.04.2014).
14. **Castagnos G., Vergnaud D.** Trapdoor Permutation Polynomials of Z/nZ and Public Key Cryptosystems // Lecture Notes in Computer Science. 2007. Vol. 4779. P. 333–350.
15. **Lidl R., Muller W. B.** Permutation Polynomials in RSA-cryptosystems //Proc. of Conf. «Advances in Cryptology» (CRYPTO 83), Santa Barbara, California, 1983. P. 293–301.
16. **Finch S. R.** Mathematical Constants//Encyclopedia of Mathematics and its Applications. 2003. Vol. 94. P. 284–286.

UDC 512.62

Permutation Polynomials of Small Length over Prime Finite Fields

Rybalkin M. A.[a], Post-Graduate Student, rybalkin@pdmi.ras.ru
[a]Saint-Petersburg Department of the Steklov Mathematical Institute of RAS, Saint-Petersburg, Russian Federation

Purpose: A permutation polynomial over a finite field is a polynomial inducing a permutation of finite field elements. At present, there are no known efficient criteria for permutation polynomials even with a small number of monomials. The purpose of this work was to generate tables of permutation polynomials, to study these tables in order to find new series of permutation polynomials, and to propose and prove some hypotheses about permutation polynomials. **Methods:** C++ algorithm implementation, numeric experiments in the Sage computer algebra system, computation of permutation group orders in the GAP computer algebra system. **Results:** A permutation polynomials enumeration algorithm was developed which works for polynomials of small length. Using it, tables of permutation quintics were built for prime finite fields up to order 100. These tables were compared with the tables for permutation quadrinomials, trinomials and binomials obtained in our previous works. To formulate a hypothesis on permutation polynomials classification, we studied dependencies between polynomials in the obtained tables. We also studied the statistical properties of random permutations generated by random permutation polynomials with a fixed number of monomials using uniform distribution. It was shown that the obtained distribution is not uniform. **Practical relevance:** The stated hypotheses on the classification of small-length permutation polynomials lead towards their complete proved classification. These hypotheses can also be used for constructing public-key cryptographic protocols based on permutation polynomials.

Keywords — Permutation Polynomials, Finite Fields, Public Key Cryptography.

References

1. Hermite C. Sur Les Fonctions de Sept Lettres. *C. R. Acad. Sci.*, Paris, 1905, pp. 750–757.
2. Dickson L. E. The Analytic Representation of Substitutions on a Power of a Prime Number of Letters with a Discussion of the Linear Group. *Annals of Mathematics*, 1896, vol. 11, no. 1/6, pp. 161–183.
3. Lidl R., Mullen G. L. When Does a Polynomial over a Finite Field Permute the Elements of the Field? *The American Mathematical Monthly*, 1988, vol. 95, pp. 243–246.
4. Lidl R., Mullen G. L. When Does a Polynomial over a Finite Field Permute the Elements of the Field? II. *The American Mathematical Monthly*, 1993, vol. 100, pp. 71–74.
5. Carlitz L. Permutations in a Finite Field. *Proc. of the American Mathematical Society*, 1953, vol. 4, p. 538.
6. Vasilev N., Rybalkin M. Permutation Binomials and their Groups. *Journal of Mathematical Sciences*, 2011, vol. 179, pp. 679–689.
7. Zieve M. E. Permutation Groups Generated by Binomials. *ArXiv e-prints*, 2013. Available at: http://arxiv.org/pdf/1312.2649.pdf (accessed 13 January 2014).
8. Wan D., Lidl R. Permutation Polynomials of the Form $x^r f(x^{(q-1)/d})$ and their Group Structure. *Monatshefte fur Mathematik*, 1991, vol. 112, no. 2, pp. 149–163.
9. Zieve M. E. On Some Permutation Polynomials over Fq of the Form $x^r h(x^{(q-1)/d})$. *Proc. of the American Mathematical Society*, 2009, vol. 137, no. 7, pp. 2209–2216.
10. Wang Q. On Inverse Permutation Polynomials. *Finite Fields and Their Applications*, 2009, vol. 15, no. 2, pp. 207–213.
11. Masuda A. M., Zieve M. E. Permutation Binomials over Finite Fields. *Transactions of the American Mathematical Society*, 2009, vol. 361, no. 8, pp. 4169–4180.
12. Rybalkin M. Classification of Permutation Trinomials and Quadrinomials over Prime Fields. *Zapiski nauchnykh seminarov POMI*, 2014, vol. 200, no. 6, pp. 734–741 (In Russian).
13. Singh R. P., Sarma B. K., Saikia A. Public Key Cryptography Using Permutation p-polynomials over Finite Fields. *IACR Cryptology ePrint Archive*, 2009. Available at: http://eprint.iacr.org/2009/208 (accessed 24 April 2014).
14. Castagnos G., Vergnaud D. Trapdoor Permutation Polynomials of Z/nZ and Public Key Cryptosystems. *Lecture Notes in Computer Science*, 2007, vol. 4779, pp. 333–350.
15. Lidl R., Muller W. B. Permutation Polynomials in RSA-cryptosystems. *Proc. of Conf. "Advances in Cryptology" (CRYPTO 83)*, Santa Barbara, California, 1983, pp. 293–301.
16. Finch S. R. Mathematical Constants. *Encyclopedia of Mathematics and its Applications*, 2003, vol. 94, pp. 284–286.

ПАМЯТКА ДЛЯ АВТОРОВ

Поступающие в редакцию статьи проходят обязательное рецензирование.

При наличии положительной рецензии статья рассматривается редакционной коллегией. Принятая в печать статья направляется автору для согласования редакторских правок. После согласования автор представляет в редакцию окончательный вариант текста статьи.

Процедуры согласования текста статьи могут осуществляться как непосредственно в редакции, так и по e-mail (ius.spb@gmail.com).

При отклонении статьи редакция представляет автору мотивированное заключение и рецензию, при необходимости доработать статью — рецензию. Рукописи не возвращаются.

Редакция журнала напоминает, что ответственность за достоверность и точность рекламных материалов несут рекламодатели.

УДК 551.510

МЕТОД АДАПТИВНОГО УПРАВЛЕНИЯ КАЛИБРОВКОЙ МУЛЬТИСПЕКТРАЛЬНЫХ ФОТОМЕТРИЧЕСКИХ СИСТЕМ АТМОСФЕРНЫХ ИЗМЕРЕНИЙ

Р. О. Гусейнова[a, 1], *старший преподаватель, диссертант*
[a]*Азербайджанский государственный архитектурно-строительный университет, Баку, Азербайджанская Республика*

Постановка проблемы: *солнечные фотометры являются наиболее универсальными измерительными устройствами, позволяющими исследовать как аэрозоль, некоторые малые газы и водяные пары, имеющиеся в атмосфере, так и показатели солнечной радиации. При этом правильная калибровка солнечных фотометров является важным условием достижения высокой достоверности полученных результатов измерения. Известный метод калибровки солнечных фотометров при двух различных значениях оптической воздушной массы имеет характерную аэрозольную погрешность, которая вызвана временной изменчивостью атмосферного аэрозоля во временном интервале, формирующемся вышеуказанными двумя оптическими воздушными массами. Целью исследования является усовершенствование данного метода для повышения точности калибровки солнечных фотометров.* ***Результаты:*** *разработан алгоритм реализации метода: коэффициент калибровки должен быть вычислен с учетом выходных сигналов фотометра, взятых в такие определенные моменты времени, при которых выполнялось бы сформулированное особое условие равенства функциональных величин временных отношений оптической воздушной массы и оптической толщины аэрозоля, вычисленных раздельно. Модельные исследования, проведенные с учетом зависимости оптической воздушной массы от угла высоты Солнца, показали, что сформулированное условие проведения калибровки может быть удовлетворено в течение временного промежутка с 9^{00} до 11^{00}, когда уровень аэрозольного загрязнения воздуха возрастает.* ***Практическая значимость:*** *повышение точности калибровки солнечных фотометров позволяет более точно оценить степень аэрозольной загрязненности атмосферы. Это важно для предсказания состояния климата, а также для решения ряда экологических задач, связанных со здоровьем населения региона.*

Ключевые слова *— адаптивность, фотометр, калибровка, атмосфера, измерение.*

Введение

Хорошо известно, что спектральные системы атмосферных измерений, в том числе мультиспектральные солнечные фотометры, должны пройти точную калибровку при стабильных внешних условиях. Например, многоканальные солнечные фотометры марки CIMEL, используемые во Всемирной сети аэрозольных измерений AERONET, проходят периодическую калибровку в научно-исследовательской лаборатории NASA, расположенной на Гавайских островах на высоте 2000 м над уровнем моря, в местечке Маона-Лоа. Удаленность этой станции от материков и высота расположения позволяют обеспечить высокоточную калибровку солнечных фотометров путем сведения к минимуму влияния атмосферного аэрозоля [1–4].

Вместе с тем существуют многочисленные локальные станции и сети атмосферных измерений, где используются солнечные фотометры различных типов, также подлежащие калибровке. Для калибровки этих приборов применяют метод эталонных источников излучателей, а также метод сравнения с использованием эталонного прибора.

Появившийся в последнее время метод калибровки солнечных фотометров при разных оптических воздушных массах позволяет осуществить калибровку с определенной степенью точности. В настоящей статье анализируется погрешность этого метода и предлагается качественно новый метод, содержащий элементы адаптивного управления режимом калибровки.

Постановка задачи организации адаптивной калибровки солнечных фотометров

В работах [5–7] авторами был предложен и развит метод проведения калибровки солнечных фотометров путем фотометрических измерений при разных оптических массах. Согласно этому методу, фотометрические измерения должны осуществляться при оптических воздушных массах $m(t_1)$ и $m(t_2)$, где $t_2 = t_1 + \Delta t$. Результаты проведенных измерений с учетом закона Бугера — Бера могут быть определены как

$$I(\lambda, t_1) = CI_0(\lambda_1)e^{-m(t_1)\cdot\tau(\lambda_1, t_1)}; \quad (1)$$

$$I(\lambda, t_2) = CI_0(\lambda_1)e^{-m(t_2)\cdot\tau(\lambda_1, t_2)}; \quad (2)$$

где $I(\lambda_1, t_i)$ — выходной сигнал фотометра при проведении измерений в момент t_i на длине волны λ_1; $i = \overline{1,2}$; C — коэффициент калибровки; $I_0(\lambda_1)$ — интенсивность внеатмосферного солнечного измерения на длине волны λ_1; $\tau(\lambda_1, t_i)$ — оптическая толщина атмосферы.

[1] Научный руководитель — доктор технических наук, профессор *Агаев Фахраддин Гюлали оглы*.

Отметим, что в выражениях (1) и (2) аппаратная функция прибора условно принята равной единице.

Хорошо известно, что оптическая толщина атмосферы в видимом диапазоне определяется как [8–11]

$$\tau(\lambda_1, t_i) = \tau_{aer}(\lambda_1, t_i) + \tau_r(\lambda_1, t_i) + \tau_g(\lambda_1, t_i), \quad (3)$$

где $\tau_{aer}(\lambda_1, t_i)$ — оптическая толщина атмосферного аэрозоля; $\tau_r(\lambda_1, t_i)$ — оптическая толщина релеевского рассеяния; $\tau_g(\lambda_1, t_i)$ — оптическая толщина атмосферных газов.

Длина волны λ_1 при калибровке многоканального фотометра выбирается таким образом, чтобы она не совпадала с линиями поглощения различных атмосферных газов. При этом ввиду того, что калибровка осуществляется в обычных условиях, релеевское рассеяние из-за малости по сравнению с аэрозольным рассеянием не учитывается.

Таким образом, имеем

$$\tau_r(\lambda_1, t_i) = \tau_{aer}(\lambda_1, t_i). \quad (4)$$

С учетом условия (4) выражения (1) и (2) имеют следующий вид:

$$I(\lambda_1, t_1) = CI_0(\lambda_1) e^{-m(t_1)\cdot\tau_{aer}(\lambda_1, t_1)}; \quad (5)$$

$$I(\lambda_1, t_2) = CI_0(\lambda_1) e^{-m(t_2)\cdot\tau_{aer}(\lambda_1, t_2)}. \quad (6)$$

Далее, в известных работах [5–7] предлагается проведение следующих операций. Правая и левая стороны выражения (5) возводятся в степень k_0, где

$$k_0 = \frac{m(t_2)}{m(t_1)}. \quad (7)$$

Имеем

$$I(\lambda_1, t_1)^{k_0} = C^{k_0} I_0^{k_0}(\lambda_1) e^{-m(t_1)k_0\cdot\tau_{aer}(\lambda_1, t_1)}. \quad (8)$$

Уравнение (6) с учетом (7) может быть выражено следующим образом:

$$I(\lambda_1, t_2) = CI_0(\lambda_1) e^{-k_0 m(t_1)\cdot\tau_{aer}(\lambda_1, t_2)}. \quad (9)$$

Деление (8) на выражение (9) дает

$$\frac{I(\lambda_1, t_1)^{k_0}}{I(\lambda_1, t_2)} = C^{k_0-1} I_0^{k_0-1}(\lambda_1) e^{-m(t_1)\cdot k_0\left[\tau_{aer}(\lambda_1, t_1) - \tau_{aer}(\lambda_1, t_2)\right]}. \quad (10)$$

Из выражения (10) находим

$$\left[CI_0(\lambda_1)\right] = \sqrt[k_0-1]{\frac{I(\lambda_1, t_1)}{I(\lambda_1, t_2)} e^{m(t_1)\cdot k_0\left[\tau_{aer}(\lambda_1, t_1) - \tau_{aer}(\lambda_1, t_2)\right]}}. \quad (11)$$

Таким образом, при $C = 1$ и при

$$\tau_{aer}(\lambda_1, t_1) = \tau_{aer}(\lambda_1, t_2) \quad (12)$$

формула (11) совпадает с формулой, приведенной в работах [5–7]. Однако с учетом дневного изменения оптической толщины атмосферного аэрозоля по часам можно ожидать, что точность калибровки на базе выражения (11) будет невысокой. Следовательно, имеет смысл усовершенствовать известный метод калибровки, вводя в метод элементы адаптивного контроля.

Решение задачи

В предлагаемом новом варианте правая и левая стороны выражения (5) возводятся в степень k, который определяется как

$$k = \sqrt{\frac{m(t_2)}{m(t_1)}}. \quad (13)$$

В этом случае выражение (6) с учетом (13) принимает следующий вид:

$$I(\lambda_1, t_2) = CI_0(\lambda_1) e^{-k^2 m(t_1)\cdot\tau_{aer}(\lambda_1, t_2)}. \quad (14)$$

Деление (8) на выражение (14) дает

$$\frac{I(\lambda_1, t_1)^k}{I(\lambda_1, t_2)} = C^{k-1} I_0^{k-1}(\lambda_1) e^{-km(t_1)\left[\tau_{aer}(\lambda_1, t_1) - k\tau_{aer}(\lambda_1, t_2)\right]}. \quad (15)$$

Из выражения (15) находим

$$CI_0(\lambda_1) = \sqrt[k-1]{\frac{I(\lambda_1, t_1)^k}{I(\lambda_1, t_2)} e^{-km(t_1)\left[\tau_{aer}(\lambda_1, t_1) - k\tau_{aer}(\lambda_1, t_2)\right]}}. \quad (16)$$

Таким образом, полученное выражение (16) предъявляет новое требование к выбору величины коэффициента k, которое формируется следующим образом:

$$k = \frac{\tau_{aer}(\lambda_1, t_1)}{\tau_{aer}(\lambda_1, t_2)}. \quad (17)$$

Следовательно, с учетом выражений (13) и (17) можно получить следующее общее условие проведения калибровки по предлагаемому методу:

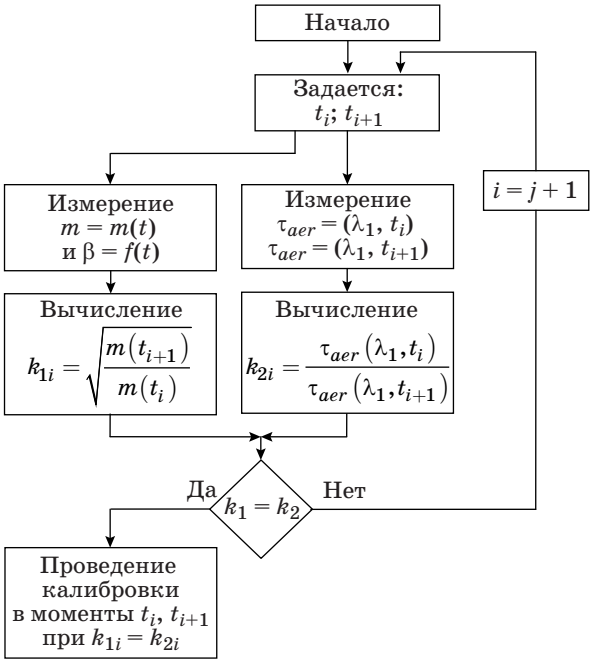
$$k = \sqrt{\frac{m(t_2)}{m(t_1)}} = \frac{\tau_{aer}(\lambda_1, t_1)}{\tau_{aer}(\lambda_1, t_2)}. \quad (18)$$

При выполнении условий (17) и (18) выражение (16) принимает следующий вид:

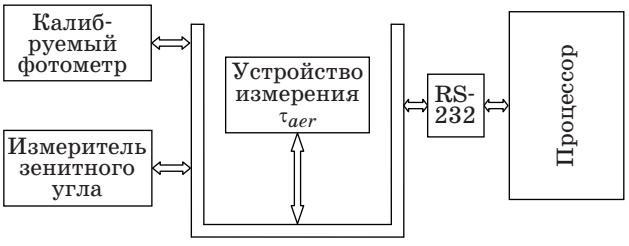
$$CI_0(\lambda_1) = \sqrt[k-1]{\frac{I(\lambda_1, t_1)^k}{I(\lambda_1, t_2)}}. \qquad (19)$$

Как видно из представленной схемы (рис. 1), предлагаемый метод калибровки обладает свойством адаптивности, так как параметры рабочего режима калибровки t_1, t_2 и k определяются в зависимости от показателей аэрозольной загрязненности атмосферы $\tau_{aer}(t_1)$ и $\tau_{aer}(t_2)$.

Устройство, обеспечивающее адаптивную калибровку фотометра по предлагаемому методу (рис. 2), содержит блок измерения зенитного угла. Проведение таких измерений объясняется большим разбросом функции зависимости зенитного угла от дневного времени и требуется для осуществления необходимых корректировок этой зависимости исходя из географических координат пункта проведения калибровки.



■ ***Рис. 1.*** Алгоритм реализации предлагаемого метода калибровки фотометра



■ ***Рис. 2.*** Блок-схема устройства калибровки

Модельные исследования

Из вышеизложенного становится ясным, что для реализации вновь предлагаемого метода калибровки следует проводить синхронные аэрозольные измерения для определения значения коэффициента k по выражению (17). Полученная величина также должна удовлетворять условию (18). Хорошо известно, что оптическая воздушная масса может быть интерпретирована в качестве отношения оптической толщины атмосферы, вычисленной для угла высоты Солнца α к оптической толщине воздуха в зенитном направлении (рис. 3) [12–15], т. е. при зенитном угле $\beta = 0$. По значениям оптической воздушной массы для различных зенитных углов (таблица) видно, что при наиболее вероятном диапазоне зенитного угла $\beta = 0 \div 60°$ оптическая воздушная масса растет от 1 до 2. Согласно работе [12], зависимость $m = m(\beta)$ в этом диапазоне практически линейна (рис. 4). На рисунке параллельно оси абсцисс также условно показаны дневные часы, соответствующие указанным значениям оптической воздушной массы. Как видно из рис. 4, если принять $t_2 = 11.00$; $t_1 = 9.00$, из выражения (18) получим

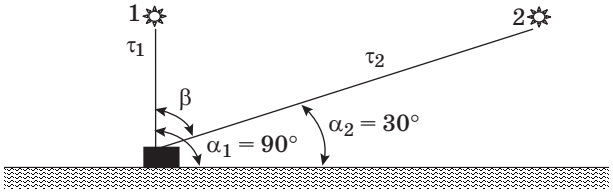
$$k = \sqrt{\frac{2}{1{,}5}} \approx 1{,}15. \qquad (20)$$

При этом, согласно условию (18), должно быть удовлетворено условие

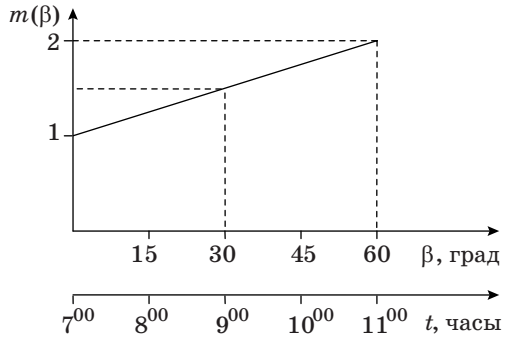
$$\frac{\tau_{aer}(\lambda_1, 9.00)}{\tau_{aer}(\lambda_1, 11.00)} \approx 1{,}15. \qquad (21)$$

■ Значения оптической воздушной массы для различных зенитных углов

β, град	m	β, град	m
0	1,0	80	5,6
60	2,0	85	10,3
70	2,9	88	19,4
75	3,8	90	37,9



■ ***Рис. 3.*** Определение понятия «оптическая воздушная масса»: α_i — угол высоты Солнца, $i = 1, 2$; β — зенитный угол; τ_i — оптическая толщина атмосферы при углах высоты Солнца α_i; *1*, *2* — позиции Солнца



■ ***Рис. 4.*** Зависимость оптической массы воздуха от зенитного угла β и текущего дневного времени *t*

Если учесть, что пик производственной деятельности, скорее, близок к 9.00, чем к 11.00, то можно ожидать, что в городской местности условие (21) может быть удовлетворено. Таким образом, оптимальными в рассматриваемом модельном случае параметрами, определяющими условия проведения калибровки, являются: $t_2 = 11.00$; $t_1 = 9.00$; $k = 1{,}15$.

Заключение

На основе исследований существующей практики калибровки солнечных фотометров критически проанализирован известный метод проведения калибровки солнечных фотометров, реализованный на базе измерений при двух значениях оптической воздушной массы. Предложен новый метод калибровки, реализующий измерения солнечных фотометров при двух значениях оптической воздушной массы, корень отношения величин которых равен отношению оптических толщин атмосферного аэрозоля, измеренных в обратной временной последовательности. Такой порядок проведения калибровки позволяет уменьшить аэрозольную погрешность известного метода калибровки солнечного фотометра.

Разработаны алгоритм выполнения и блок-схема устройства для практической реализации метода.

Литература

1. **Shaw G. E.** Aerosols at Mauna Loa: Optical Properties // J. of the Atmospheric Sciences. 1979. Vol. 36. P. 862–869.
2. **Kim S.-W.** et al. Global Surface-Based Sun Photometer Network for Long-Term Observations of Column Aerosol Optical Properties: Intercomparison of Aerosol Optical Depth // Aerosol Science and Technology. 2008. Vol. 42. P. 1–9.
3. **Livingston J. M.** et al. Retrieval of Ozone Column Content from Airborne Sun Photometer Measurements During SOLVE II: Comparison with Coincident Satellite and Aircraft Measurements // Atmospheric Chemistry and Physics. 2005. Vol. 5. P. 2035–2054.
4. **Beegum S. N.** et al. Characteristics of Spectral Aerosol Optical Depths over India During ICARB // J. of Earth System Sciences. July 2008. Vol. 117. Iss. 1 Supplement. P. 303–313.
5. **Asadov H. H., Chobanzadeh I. G.** New method for calibration of Sun Photometers//Chine Optics Letters. Sept. 2009. Vol. 7. N 9. P. 760–763.
6. **Асадов Х. Г., Чобанзаде И. Г., Алиев Д. З.** Дистанционное зондирование с переменным углом обзора. Состояние и перспективы для исследования поверхности Земли и атмосферы // Авиакосмическое приборостроение. 2009. № 1. С. 31–34.
7. **Асадов Х. Г., Чобанзаде И. Г., Агаев Ф. Г.** Метод калибровки трехволновых солнечных фотометров // Инженерная физика. 2009. № 6. С. 26–28.
8. **Гущин Г. П., Виноградова Н. Н.** Суммарный озон в атмосфере. — Л.: Гидрометеоиздат, 1983. — 342 с.
9. **Liang Sh., Zhong B., Fang H.** Improved Estimation of Aerosol Optical Depth from MODIS Imagery over Land Surfaces // Remote Sensing of Environment. 2006. Vol. 104. P. 416–425.
10. **Li G., Li Ch., Mao J.** Evaluation of Atmospheric Aerosol Optical Depth Products at Ultraviolet Banda Derived from MODIS Products // Aerosol Science and Technology. 2012. Vol. 46. Iss. 9. P. 1025–1034.
11. **Retails A.** et al. Comparison of Aerosol Optical Thickness with in Situ Visibility Data over Cyprus // Natural Hazards and Earth System Sciences. 2010. Vol. 10. P. 421–428.
12. **Kasten F., Young A. T.** Revised Optical Air Mass Tables and Approximation Formula // Applied Optics. 1989. Vol. 28. Iss. 22. P. 4735–4738.
13. **Rapp-Arraras I., Domingo-Santos J. M.** Functional Forms for Approximating the Relative Optical Air Mass // Journal of Geophysical Researches. 2011. Vol. 116. D24308. doi:10.1029/2011JD016706
14. **Bayat A., Masoumi A., Khalesifard H. R.** Retrieval of Atmospheric Optical Parameters from Ground-Based Sun-Photometer Measurements for Zanjan, Iran // Atmospheric Measurement Techniques. 2011. Vol. 4. P. 857–863. doi:10.519/amt-4-857-2011
15. **Vollmer M., Gedzelman S. D.** Colours of the Sun and Moon: the Role of the Optical Air Mass // European Journal of Physics. 2006. N 27. P. 299–309. doi:10.1088/0143-0807/27/2/013

UDC 551.510

Method of Adaptive Control of Calibration of Multispecral Photometric Systems of Atmospheric Measurements

Huseynova R. O.[a], Senior Lecturer, Dissertant, renahuseynova55@gmail.com
[a]Azerbaijan Architecture and Construction University, 5, A. Sultanova St., AZ1073, Baku, Azerbaijan Republic

Purpose: Sun photometers are versatile measuring instruments, allowing to study aerosol, certain atmospheric trace gases and water vapors, as well as some parameters of solar radiation. Correct calibration of sun photometers is an important condition of reaching high authenticity of measurement results. The well-known method of calibrating a sun photometer upon two different optical air masses has a specific aerosol error. This error is caused by temporal variability of the atmospheric aerosol within the time interval formed by the two above-mentioned optical air masses. A modification of this method could allow us to increase the accuracy of sun photometer calibration. **Results:** As an implementation of the new method, a special algorithm was developed. According to it, the calibration coefficient should be calculated taking into account the photometer output signals taken in such diurnal time moments when a special condition is met about the equality of functional values of temporal ratios for the optical air mass and the aerosol optical depth calculated separately. A model research performed with due regards for the dependence of the optical air mass on the sun elevation angle showed that the formulated calibration condition can be met during the time interval from 9:00 to 11:00 when the air aerosol pollution level increases. **Practical relevance:** The algorithm for the proposed method is developed and a block scheme of the instrument is composed. The results of the performed model research are given, confirming the feasibility of the calibration accuracy increase. **Social implications:** The increase in sun photometer calibration accuracy enables more precise estimation of atmospheric aerosol pollution level. This is important for climate prediction and for solving certain ecological problems linked to people's health.

Keywords — Adaptiveness, Photometer, Calibration, Atmosphere, Measurement.

References

1. Shaw G. E. Aerosols at Mauna Loa: Optical Properties. *Journal of the Atmospheric Sciences*, 1979, vol. 36, pp. 862–869.
2. Kim S.-W., et al. Global Surface-Based Sun Photometer Network for Long-Term Observations of Column Aerosol Optical Properties: Intercomparison of Aerosol Optical Depth. *Aerosol Science and Technology*, 2008, vol. 42, pp. 1–9.
3. Livingston J. M., et al. Retrieval of Ozone Column Content from Airborne Sun Photometer Measurements During SOLVE II: Comparison with Coincident Satellite and Aircraft Measurements. *Atmospheric Chemistry and Physics*, 2005. vol. 5, pp. 2035–2054.
4. Beegum S. N., et al. Characteristics of Spectral Aerosol Optical Depths over India During ICARB. *Journal of Earth System Sciences*, July 2008, vol. 117, iss. 1 Supplement, pp. 303–313.
5. Asadov H. H., Chobanzadeh I. G. New Method for Calibration of Sun Photometers. *Chine Optics Letters*, September 2009, vol. 7, no. 9, pp. 760–763.
6. Asadov H. H., Chobanzadeh I. G., Aliyev D. Z. Remote Sensing with Changing Angle of View. Condition and Perspectives for Research of the Earth Surface and Atmosphere. *Aviakosmicheskoe priborostroenie*, 2009, no. 1, pp. 31–34 (In Russian).
7. Asadov H. H., Chobanzadeh I. G., Agayev F. G. Method for Calibration of Three-Wavelengths Sun Photometers. *Inzhenernaia fizika*, 2009, no. 6, pp. 26–28 (In Russian).
8. Guchin G. P., Vinogradova N. N. *Summarnyi ozon v atmosfere* [Total Ozone in Atmosphere]. Leningrad, Gidrometeoizdat Publ., 1982. 342 p. (In Russian).
9. Liang Sh., Zhong B., Fang H. Improved Estimation of Aerosol Optical Depth from MODIS Imagery over Land Surfaces. *Remote Sensing of Environment*, 2006, vol. 104, pp. 416–425.
10. Li G., Li Ch., Mao J. Evaluation of Atmospheric Aerosol Optical Depth Products at Ultraviolet Banda Derived from MODIS Products. *Aerosol Science and Technology*, 2012, vol. 46, iss. 9, pp. 1025–1034.
11. Retails A., et al. Comparison of Aerosol Optical Thickness with in Situ Visibility Data over Cyprus. *Natural Hazards and Earth System Sciences*, 2010, vol. 10, pp. 421–428.
12. Kasten F., Young A. T. Revised Optical Air Mass Tables and Approximation Formula. *Applied Optics*, 1989, vol. 28, iss. 22, pp. 4735–4738.
13. Rapp-Arraras I., Domingo-Santos J. M. Functional Forms for Approximating the Relative Optical Air Mass. *Journal of Geophysical Researches*, 2011, vol. 116, D24308. doi:10.1029/2011JD016706
14. Bayat A., Masoumi A., Khalesifard H. R. Retrieval of Atmospheric Optical Parameters from Ground-Based Sun-Photometer Measurements for Zanjan, Iran. *Atmospheric Measurement Techniques*, 2011, vol. 4, pp. 857–863. doi:10.519/amt-4-857-2011
15. Vollmer M., Gedzelman S. D. Colours of the Sun and Moon: the Role of the Optical Air Mass. *European Journal of Physics*, 2006, no. 27, pp. 299–309. doi:10.1088/0143-0807/27/2/013

УДК 004.891.3

КОМПОЗИЦИЯ ДЕРЕВЬЕВ РЕШЕНИЙ ДЛЯ РАСПОЗНАВАНИЯ СТЕПЕНИ ТЯЖЕСТИ ХРОНИЧЕСКОЙ ОБСТРУКТИВНОЙ БОЛЕЗНИ ЛЕГКИХ

Н. И. Омирова[а], *преподаватель*
М. Н. Палей[б], *заочный аспирант*
Е. В. Евсюкова[б], *доктор мед. наук, профессор*
А. В. Тишков[в], *канд. физ.-мат. наук, доцент*
[а]*Первый Санкт-Петербургский государственный медицинский университет им. акад. И. П. Павлова, Санкт-Петербург, РФ*
[б]*Санкт-Петербургский государственный университет, Санкт-Петербург, РФ*
[в]*Санкт-Петербургский институт информатики и автоматизации РАН, Санкт-Петербург, РФ*

Цель: *наиболее важным вариантом диагностики степени тяжести одного из самых распространенных бронхолегочных заболеваний — хронической обструктивной болезни легких — является спирометрия. Однако она доступна не во всех лечебно-профилактических учреждениях Российской Федерации. Целью работы является построение алгоритма диагностики хронической обструктивной болезни легких без учета спирометрии.* ***Методы:*** *в качестве математического аппарата диагностики были выбраны деревья решений, на основе которых создан коллективный классификатор; в нем реализована двухуровневая схема: предварительный диагноз по первичному дереву решений уточняется на втором этапе другим деревом решений с более узкой компетенцией.* ***Результаты:*** *низкая точность классификатора может быть повышена, если матрица результатов кросс-валидации имеет блочно-диагональную структуру и классификаторы, построенные для каждого блока, имеют более высокую точность, чем исходный классификатор. Для повышения точности классификатора с результатами кросс-валидации менее 55 % предложена и опробована схема двухуровнего классификатора. На первом этапе строится первичный классификатор, предсказания которого уточняются классификаторами, построенными для диагональных блоков исходной матрицы. Предлагаемое решение позволяет улучшить точность диагностики степени тяжести хронической обструктивной болезни легких с 52,5 до 65 %.* ***Практическая значимость:*** *дифференциальная диагностика степени тяжести хронической обструктивной болезни легких может быть проведена с удовлетворительной точностью в лечебно-профилактических учреждениях, не обладающих спирометрическим оборудованием. Предлагаемый способ улучшения точности классификатора может быть применен и в других классификаторах диагностики, если удается построить набор решателей, более компетентных в узких областях, чем первичные.*

Ключевые слова *— деревья решений, коллективные классификаторы, медицинская диагностика, хроническая обструктивная болезнь легких.*

Введение

Задача диагностики с математической точки зрения представляется задачей классификации [1]. Классифицируемыми объектами являются пациенты, атрибутами объектов — антропометрические, социально-паспортные, клинико-лабораторные и другие показатели, а классами — диагнозы. Задача диагностики может заключаться в определении отсутствия или наличия заболевания, а также в определении вида заболевания или степени тяжести. В настоящей работе определяется степень тяжести хронической обструктивной болезни легких (ХОБЛ).

Рассматриваемая выборка пациентов, страдающих ХОБЛ, содержит как числовые, так и номинальные данные. Из наиболее широко известных алгоритмов классификации деревья решений [2] являются основным классификатором, работающим с номинальными данными. Когда точность классификатора оказывается ниже приемлемого уровня согласно кросс-валидации [3], ее можно повысить с помощью построения коллективов классификаторов [4]. Обычно в этом случае исходный классификатор заменяют на смесь других и вводят решающее правило получения окончательного результата на основе результатов каждого из членов коллектива. В данной работе предлагается ответ первичного классификатора в качестве исходного результата, который подлежит уточнению коллективом классификаторов.

Описание выборки и диагностическая задача

Хроническая обструктивная болезнь легких представляет серьезную проблему в современной медицине, поскольку распространенность и летальность от этого заболевания постоянно увеличиваются [5, 6]. Диагностика степени тяжести ХОБЛ в настоящее время проводится на основании результатов исследования функции внешнего дыхания (ФВД). Однако в лечебно-профилактических учреждениях не всегда имеется необходимое оборудование для ФВД. Данные о пациентах в настоящей работе не включали ФВД.

Выборка пациентов с ХОБЛ состояла из 80 пациентов четырех степеней тяжести: первой — 19 пациентов, второй — 23, третьей — 19 и четвертой — 19 пациентов. Здоровых пациентов в выборке не было, поэтому стояла задача дифференциальной диагностики степени ХОБЛ. Выборка содержала следующие клинические и лабораторные показатели: индекс курения; признаки гиперреактивности бронхов; кашель сухой; кашель продуктивный; частота сердечных сокращений; частота дыхания; подвижность легочного края при объективном осмотре пациента; степень одышки по шкале MRC; насыщение крови кислородом; индекс массы тела; количество систем органов, со стороны которых имеется патология; показатель коморбидности (общее количество заболеваний у пациента); кумулятивный рейтинговый показатель заболеваний у гериатрических пациентов (шкала Миллера); тест с 6-минутной ходьбой; показатели качества жизни по опроснику SF-36: физический компонент здоровья PH (включающий шкалы: физическое функционирование — PF, ролевое физическое функционирование — RP, интенсивность боли — BP, общее состояние здоровья — GH) и психологический компонент здоровья MH (включающий шкалы: жизненная активность — VT, социальное функционирование — SF, ролевое эмоциональное функционирование — RE, психическое здоровье — MH); лабораторные показатели: содержание в крови гемоглобина и эритроцитов, кальций, общий белок.

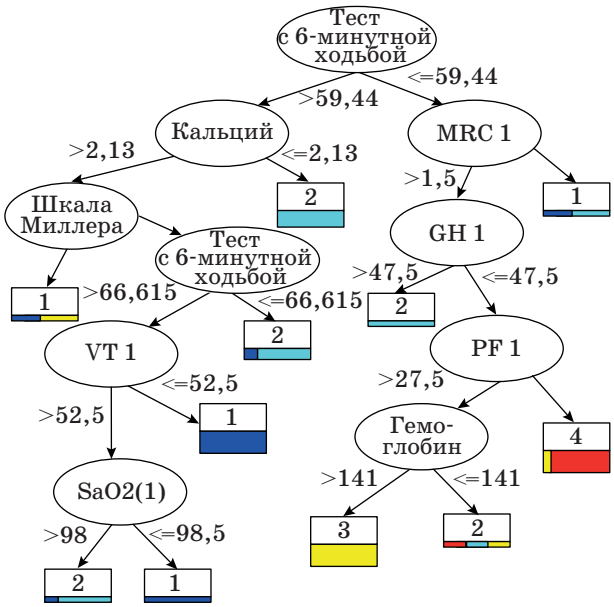
Все перечисленные показатели не относятся напрямую к симптомам бронхо-легочных заболеваний. По таким исходным данным установить тяжесть степени ХОБЛ достаточно непросто. Для достижения приемлемой точности далее предлагается схема взаимодействия классификаторов, при которой предполагаемый диагноз по первичному классификатору уточняется на втором этапе.

Двухуровневый классификатор

На первом этапе было построено дерево решений (рис. 1) для классификации пациентов по всем четырем степеням тяжести ХОБЛ.

Дерево условно делит все обучающие примеры на две группы. Правое, относительно корня, поддерево включает в основном пациентов с высокой степенью тяжести ХОБЛ: больше всего пациентов с четвертой и третьей степенью и лишь несколько пациентов со второй и первой. Левое поддерево включает обучающие примеры только первой и второй степени тяжести ХОБЛ.

В результате кросс-валидации была достигнута точность классификации (52,5±16,5) % (табл. 1). Такой уровень точности следует признать посредственным.



■ ***Рис. 1.*** Дерево решений по четырем классам

■ ***Таблица 1.*** Результат кросс-валидации по четырем классам

Предполагаемый класс и точность предсказания	Фактический класс				Точность распознавания, %
	1	2	3	4	
Класс 1	10	9	0	0	52,63
Класс 2	9	9	4	1	39,13
Класс 3	0	3	8	3	57,14
Класс 4	0	2	7	15	62,50
Точность предсказания, %	52,63	39,13	42,11	78,95	–

Ошибки классификации возникают в большей степени между классами 1 и 2, 2 и 3, 3 и 4, в меньшей степени — между 2 и 4 и не возникают между 1 и 3, 1 и 4.

Блочно-диагональный вид матрицы предсказаний порождает гипотезу о возможности построения классифиторов, анализирующих пары соседних классов: первого со вторым, второго с третьим и третьего с четвертым. Эти классификаторы будут использоваться для уточнения первичной классификации по четырем классам.

Для каждого класса строится цепочка классов, «достижимых» из данного. Достижимость означает наличие соответствующих ошибок между рассматриваемыми классами при кросс-валидации.

Например, из класса 1 достижим только класс 2, для которого имеется девять ложноположительных результатов. Ложноположительные результаты для класса 1 относительно классов 3 и 4

отсутствуют. Таким образом, для класса 1 имеем короткую цепочку 1–2. Поэтому если первичный классификатор покажет класс 1, то будет использован только один уточняющий классификатор 1–2.

Из класса 2 достижимы классы 1, 3 и 4. Поэтому цепочка для класса 2 будет выглядеть следующим образом: 1–2–3–4. Соответственно, при классификации будут использованы уточняющие классификаторы 1–2, 2–3 и 3–4. Движение по цепочке возможно от класса 2 в меньшую сторону к классу 1 по результату классификатора 1–2 или в большую сторону к классу 3 по результату классификатора 2–3 и, возможно, к классу 4 по результату классификатора 3–4. Если на первом шаге классификаторы 1–2 и 2–3 показали разнонаправленное движение, необходимо остановиться на классе 2. Движение по цепочке останавливается, если очередной уточняющий классификатор подтверждает результат предыдущего. Аналогично для класса 3 строится цепочка 2–3–4, а для класса 4 — цепочка 2–3–4.

Далее необходимо убедиться в достаточной точности уточняющих классификаторов.

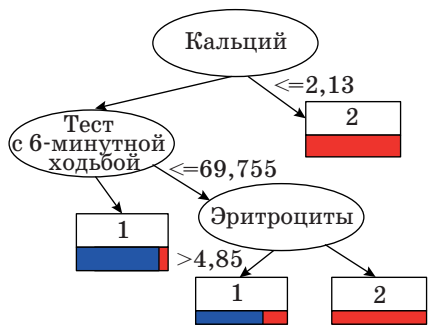
Классификатор 1–2 (рис. 2) строится на обучающей выборке, включающей два класса (первый — 1-я степень ХОБЛ и второй — 2-я степень ХОБЛ).

В качестве корневого атрибута дерева решений выступает показатель — содержание кальция в крови пациента. В результате кросс-валидации достигнута точность классификации (75±19,4) % (табл. 2).

Заметим, что суммарное количество ошибок распознавания классов 1 и 2 уменьшилось с 23 до 10 по сравнению с первичным классификатором, что составляет 31 % от общего количества пациентов класса 1 и 2.

Точность представлена в табл. 3 согласно кросс-валидации всех уточняющих классификаторов.

Поскольку распознавательная способность уточняющих классификаторов выше исходного, можно предположить, что двухуровневая система — первичный классификатор плюс уточняющий — повысит точность классификации.



■ ***Рис. 2.*** Классификатор для классов 1 и 2

■ ***Таблица 2.*** Таблица точности классификатора по кросс-валидации

Предполагаемый класс и точность предсказания	Фактический класс		Точность распознавания, %
	1	2	
Класс 1	13	4	76,47
Класс 2	6	19	76,00
Точность предсказания, %	68,42	82,61	–

■ ***Таблица 3.*** Точность уточняющих классификаторов

Уточняющий классификатор	Точность уточняющего классификатора, %	Повышение точности относительно первичного классификатора (по соответствующим классам), %
1–2	75,00±19,40	31
2–3	64,50±26,50	25
3–4	84,17±17,26	23

■ ***Таблица 4.*** Результат кросс-валидации двухуровневого классификатора

Предполагаемый класс и точность предсказания	Фактический класс				Точность распознавания, %
	1	2	3	4	
Класс 1	14	5	0	0	73,68
Класс 2	6	11	2	2	52,38
Класс 3	0	4	13	4	61,90
Класс 4	0	0	5	14	73,68
Точность предсказания, %	70,00	55,00	65,00	70,00	–

Для анализа точности двухуровневого классификатора также была проведена кросс-валидация (табл. 4).

Точность двухуровневого классификатора составила 65 %, что на 12,5 % (что соответствует десяти примерам) выше точности первичного классификатора.

Заключение

Низкая точность классификатора может быть повышена, если матрица результатов кросс-валидации имеет блочно-диагональную структуру и классификаторы, построенные для каждого блока, имеют более высокую точность, чем исходный классификатор.

Для повышения точности классификатора с результатами кросс-валидации менее 55 % предложена и опробована схема двухуровневого классификатора. На первом этапе строится первичный классификатор, предсказания которого уточняются классификаторами, построенными для диагональных блоков исходной матрицы.

При помощи двухуровневого классификатора точность распознавания степени тяжести ХОБЛ была повышена на 12,5 % и составила 65 %.

Литература

1. **Дюк В., Эмануэль В.** Информационные технологии в медико-биологических исследованиях. — СПб.: Питер, 2003. — 528 с.
2. **Quinlan J. R.** C4.5: Programs for Machine Learning. — Morgan Kaufmann Publishers, 1993. — 302 p.
3. **Воронцов К. В.** Комбинаторный подход к оценке качества обучаемых алгоритмов// Математические вопросы кибернетики. 2004. Т. 13. С. 5–36.
4. **Воронцов К. В.** Лекции по алгоритмическим композициям. http://www.machinelearning.ru/wiki/images/0/0d/Voron-ML-Compositions.pdf (дата обращения: 29.05.2014).
5. **Chapman K. R., Mannino D. M., Soriano J. B.** Epidemiology and Costs of Chronic Obstructive Pulmonary Disease//Eur. Respir J. 2006. Vol. 27. N 1. P. 188–207.
6. **Global** Initiative for Chronic Obstructive Lung Disease — GOLD. http://www.goldcopd.org/uploads/users/files/GOLD_Report_2013.pdf (дата обращения: 29.05.2014).

UDC 004.891.3

Composition of Decision Trees for Severity of Chronic Obstructive Pulmonary Desease Recognition

Omirova N. I.[a], Lecturer, nargiz.eubova@spb-gmu.ru
Paley M. N.[b], Post-Graduate Student, mnpaley@mail.ru
Evsyukova H. V.[b], Dr. Sc., Med., Professor, eevs@yandex.ru
Tishkov A. V.[c], PhD, Phys.-Math., Associate Professor, artem.tishkov@gmail.com
[a]Pavlov First Saint-Petersburg State Medical University, 6/8, L'va Tolstogo St., 197002, Saint-Petersburg, Russian Federation
[b]Saint-Petersburg State University, 7-8, Universitetskaya Emb., 197198, Saint-Petersburg, Russian Federation
[c]Saint-Petersburg Institute for Informatics and Automation of RAS, 39, 14 Line, V. O., 199178, Saint-Petersburg, Russian Federation

Purpose: Chronic obstructive pulmonary disease is one of the most prevalent pulmonary diseases, and spirometry is one of the most important methods to diagnose its severity. Unfortunately, spirometry is not widely available in Russian hospitals and clinics. This paper proposes an algorithm of COPD severity diagnostics without spirometry. **Methods:** As a mathematical framework for the diagnostics, decision trees were chosen. On their base, a two-level compositional classifier was implemented. The primary decision tree provides a preliminary diagnosis refined in the second step by another more specialized decision tree. **Results:** The low accuracy of the classifier can be improved if two conditions are met: the confusion matrix has block-diagonal structure, and the classifiers built for each block have a higher accuracy than the original classifier. In order to improve the cross-validation accuracy of the classifier from less than 55%, a two-level classifier scheme is proposed and tested. First-level classifier is refined by a number of secondary classifiers built for the diagonal blocks of the original confusion matrix. The proposed solution improves the accuracy of the COPD severity diagnostics from 52,5 to 65%. **Practical relevance:** The differential diagnostics of COPD severity can be performed with satisfactory accuracy even in hospitals without spirometry equipment. The proposed method for improving the classifier accuracy can be applied in other diagnostics classifiers, if a set of solvers more competent in narrow areas than the original ones is successfully built.

Keywords — Decision Trees, Compositional Classifiers, Medical Diagnostics, COPD.

References

1. Duke V., Emanuel V. *Informatsionnye tekhnologii v mediko-biologicheskikh issledovaniiakh* [Information Technologies in Biomedical Research]. Saint-Petersburg, Piter Publ., 2003. 528 p. (In Russian).
2. Quinlan J. R. *C4.5: Programs for Machine Learning*. Morgan Kaufmann Publishers, 1993. 302 p.
3. Vorontsov K. V. Combinatorial Approach to Evaluating the Quality of Trained Algorithms. *Matematicheskie voprosy kibernetiki*, 2004, vol. 13, pp. 5–36 (In Russian).
4. Vorontsov K. V. *Lektsii po algoritmicheskim kompozitsiiam* [Lectures on Algorithmic Compositions]. Available at: http://www.machinelearning.ru/wiki/images/0/0d/Voron-ML-Compositions.pdf (accessed 29 May 2014).
5. Chapman K. R., Mannino D. M., Soriano J. B. Epidemiology and Costs of Chronic Obstructive Pulmonary Disease. *Eur. Respir J.*, 2006, vol. 27, no. 1, pp. 188–207.
6. *Global Initiative for Chronic Obstructive Lung Disease — GOLD*. Available at: http://www.goldcopd.org/uploads/users/files/GOLD_Report_2013.pdf (accessed 29 May 2014).

БАЛОНИН Николай Алексеевич

Профессор кафедры вычислительных систем и сетей Санкт-Петербургского государственного университета аэрокосмического приборостроения.
В 1982 году окончил Ленинградский электротехнический институт им. В. И. Ульянова (Ленина) по специальности «Автоматика и телемеханика».
В 2008 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором более 80 научных публикаций, в том числе трех монографий.
Область научных интересов — теория динамических систем, теория идентификации, теория операторов, теория матриц, вычислительные методы, интернет-робототехника, интернет-книги с исполняемыми алгоритмами, научные социальные сети.
Эл. адрес: korbendfs@mail.ru

БРАНИШТОВ Сергей Александрович

Исполняющий обязанности заведующего лабораторией систем логического управления Института проблем управления им. В. А. Трапезникова РАН, Москва.
В 1997 году окончил Чувашский государственный университет по специальности «Электроника и микропроцессорная техника».
В 2009 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором 25 научных публикаций.
Область научных интересов — системы автоматизации, искусственный интеллект, робототехника.
Эл. адрес:
branishtov@mail.ru

ГОРОДЕЦКИЙ Андрей Емельянович

Доктор технических наук, профессор, заведующий лабораторией методов и средств автоматизации Института проблем машиноведения РАН, Санкт-Петербург, заслуженный деятель науки и техники.
В 1965 году окончил Ленинградский политехнический институт им. М. И. Калинина по специальности «Автоматика и телемеханика».
В 1993 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором более 150 научных публикаций и 70 изобретений.
Область научных интересов — математическое моделирование, оптимальное управление, идентификация и диагностика.
Эл. адрес:
gorodetsky@mail23.ipme.ru

БИРИЧЕВСКИЙ Алексей Романович

Аспирант Санкт-Петербургского института информатики и автоматизации РАН.
В 2010 году окончил Сыктывкарский государственный университет по специальности «Комплексная защита объектов автоматизации».
Является автором четырех научных публикаций.
Область научных интересов — информационная безопасность, криптография, безопасность операционных систем, безопасность систем передачи данных.
Эл. адрес: lehabirich@mail.ru

ВОСТРИКОВ Антон Александрович

Доцент кафедры вычислительных систем и сетей Санкт-Петербургского государственного университета аэрокосмического приборостроения.
В 2000 году окончил Санкт-Петербургский государственный университет аэрокосмического приборостроения по специальности «Вычислительные машины, комплексы, системы и сети».
В 2004 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором 45 научных публикаций и двух свидетельств о регистрации программного продукта.
Область научных интересов — распределенные и встраиваемые информационно-управляющие системы, обработка визуальной информации, оптико-информационные системы.
Эл. адрес: vostricov@mail.ru

ГОРСКИЙ Олег Владимирович

Аспирант научно-исследовательского отдела биотехнических проблем Санкт-Петербургского государственного университета аэрокосмического приборостроения.
В 2010 году окончил Санкт-Петербургский государственный университет аэрокосмического приборостроения по специальности «Авиационные приборы и измерительно-вычислительные комплексы».
Является автором семи научных публикаций.
Область научных интересов — бесконтактная передача энергии, имплантируемые системы, медицинское приборостроение.
Эл. адрес: gorskijoleg@gmail.com

ГУСЕЙНОВА
Рена
Омар гызы

Гражданка Азербайджана.
Старший преподаватель кафедры вычислительной техники и программного обеспечения Азербайджанского архитектурно-строительного университета, Баку.
В 1977 году окончила Азербайджанский политехнический институт им. Ч. Ильдрыма по специальности «Электронные вычислительные машины».
Является автором более 20 научных публикаций.
Область научных интересов — информационно-измерительная техника, вычислительная техника, системы управления и контроля.
Эл. адрес:
renahuseynova55@gmail.com

ЗУБОК
Дмитрий
Александрович

Заместитель заведующего кафедрой информационных систем Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики.
В 1996 году окончил Санкт-Петербургский государственный институт точной механики и оптики (технический университет) по специальности «Оптико-электронные приборы и системы».
В 2000 году защитил диссертацию на соискание ученой степени кандидата физико-математических наук.
Является автором 17 научных и учебно-методических публикаций.
Область научных интересов — математическая теория надежности, теория массового обслуживания, рекомендующие системы.
Эл. адрес: zubok@mail.ifmo.ru

КНИГА
Екатерина
Викторовна

Аспирант кафедры машинного проектирования бортовой электронно-вычислительной аппаратуры Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, старший инженер ФГУП «Санкт-Петербургское ОКБ «Электроавтоматика» им. П. А. Ефимова».
В 2012 году окончила Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики по специальности «Управление и информатика в технических системах».
Является автором семи научных публикаций.
Область научных интересов — вычислительные системы интегрированной модульной авионики.
Эл. адрес:
ekovinskaya@gmail.com

ЖАРИНОВ
Игорь
Олегович

Заведующий кафедрой машинного проектирования бортовой электронно-вычислительной аппаратуры Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, руководитель учебно-научного центра ФГУП «Санкт-Петербургское ОКБ «Электроавтоматика» им. П. А. Ефимова».
В 2000 году окончил Санкт-Петербургский государственный университет аэрокосмического приборостроения.
В 2011 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором более 100 научных публикаций.
Область научных интересов — проектирование бортовой вычислительной техники.
Эл. адрес: igor_rabota@pisem.net

ЕВСЮКОВА
Елена
Владимировна

Профессор кафедры госпитальной терапии медицинского факультета Санкт-Петербургского государственного университета.
В 1985 году окончила Первый Ленинградский медицинский институт им. акад. И. П. Павлова по специальности «Врач-лечебник».
В 2002 году защитила диссертацию на соискание ученой степени доктора медицинских наук.
Является автором 140 научных публикаций и одного патента на изобретение.
Область научных интересов — пульмонология и патологическая физиология.
Эл. адрес: eevs@yandex.ru

КОБЯКОВ
Александр
Алексеевич

Заместитель генерального директора ОАО «Концерн «Гранит-Электрон», Санкт-Петербург.
В 1988 году окончил Высшее военно-морское училище радиоэлектроники им. А. С. Попова по специальности «Электронная техника».
Является автором трех научных публикаций.
Область научных интересов — системы представления и обработки информации.
Эл. адрес:
cri-granit@peterlink.ru

КОТЕНКО Игорь Витальевич

Профессор, заведующий лабораторией проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации РАН.
В 1983 году окончил Военно-космическую академию им. А. Ф. Можайского по специальности «Математическое обеспечение автоматизированных систем управления», в 1987 году — Военную академию связи по специальности «Инженерная автоматизированных систем управления».
В 1999 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором более 450 научных публикаций.
Область научных интересов — безопасность компьютерных сетей, обнаружение компьютерных атак, межсетевые экраны, защита от вирусов и сетевых червей и др.
Эл. адрес: ivkote@comsec.spb.ru

МАЯТИН Александр Владимирович

Доцент кафедры информационных систем Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики.
В 2001 году окончил Санкт-Петербургский государственный институт точной механики и оптики (технический университет) по специальности «Профессиональное обучение».
В 2005 году защитил диссертацию на соискание ученой степени кандидата педагогических наук.
Является автором 32 научных публикаций.
Область научных интересов — образовательные технологии, управление информационно-технологической инфраструктурой, операционные системы.
Эл. адрес: mayatin@mail.ifmo.ru

МОНДИКОВА Яна Александровна

Аспирант кафедры автоматизированных систем обработки информации и управления Санкт-Петербургского государственного электротехнического университета «ЛЭТИ».
В 2013 году окончила Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» по специальности «Компьютерная безопасность».
Является автором двух научных публикаций.
Область научных интересов — криптография, алгоритмы шифрования, протоколы электронной цифровой подписи, схемы открытого распределения ключей, компьютерная безопасность.
Эл. адрес: mondikovay@gmail.com

ЛАПШИН Кирилл Владимирович

Начальник научно-исследовательской лаборатории ОАО «Концерн «Гранит-Электрон», Санкт-Петербург.
В 1998 году окончил Санкт-Петербургский государственный университет аэрокосмического приборостроения по специальности «Приборы и системы ориентации, навигации и стабилизации летательного аппарата».
Является автором 14 научных публикаций.
Область научных интересов — системы управления сложными динамическими объектами.
Эл. адрес: kir_i_k@mail.ru

МОЛДОВЯН Николай Андреевич

Профессор, заведующий научно-исследовательским отделом проблем информационной безопасности Санкт-Петербургского института информатики и автоматизации РАН, заслуженный изобретатель РФ.
В 1975 году окончил Кишиневский политехнический институт по специальности «Полупроводниковые приборы».
В 2001 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором более 250 научных публикаций и 60 патентов на изобретения.
Область научных интересов — информационная безопасность, криптография, электронная цифровая подпись, блочные шифры.
Эл. адрес: nmold@mail.ru

НАЗАРОВ Андрей Вячеславович

Начальник кафедры космической радиолокации и радионавигации Военно-космической академии им. А. Ф. Можайского, Санкт-Петербург.
В 1994 году окончил Военно-космическую академию им. А. Ф. Можайского по специальности «Радиоэлектронные системы».
В 2000 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором более 80 научных публикаций.
Область научных интересов — моделирование сложных систем, нейросетевые технологии, техническая диагностика, методы обработки изображений, оптико-информационные системы.
Эл. адрес: naz-av@mail.ru

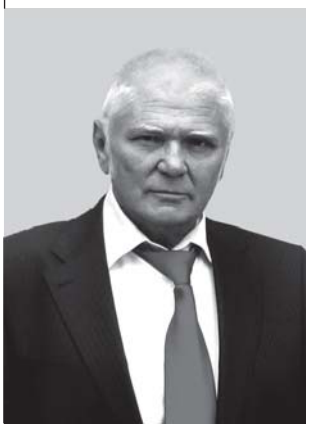
НОВИКОВА Евгения Львовна

Ассистент кафедры информационно-управляющих систем Санкт-Петербургского государственного университета аэрокосмического приборостроения.
В 1973 году окончила Балтийский государственный технический университет «ВОЕНМЕХ» им. Д. Ф. Устинова по специальности «Динамика полета и управление».
Является автором пяти научных публикаций.
Область научных интересов — системный анализ, обработка информации и управление.
Эл. адрес: kir_i_k@mail.ru

ОСИПОВ Василий Юрьевич

Профессор, ведущий научный сотрудник Санкт-Петербургского института информатики и автоматизации РАН.
В 1981 году окончил Высшее военно-морское училище радиоэлектроники им. А. С. Попова по специальности «Радиотехнические средства».
В 2000 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором более 100 научных публикаций.
Область научных интересов — интеллектуальные системы, моделирование, информационная безопасность.
Эл. адрес: osipov_vasiliy@mail.ru

ПАРАМОНОВ Павел Павлович



Советник генерального директора ФГУП «Санкт-Петербургское ОКБ «Электроавтоматика» им. П. А. Ефимова», почетный авиастроитель, заслуженный конструктор РФ.
В 1968 году окончил Ленинградский институт точной механики и оптики по специальности «Инженер-электрик».
В 2004 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором более 200 научных публикаций, в том числе 25 изобретений.
Область научных интересов — разработка систем индикации и средств отображения информации, бортовых цифровых вычислительных машин, навигационных комплексов бортового радиоэлектронного оборудования и др.
Эл. адрес: postmaster@elavt.spb.ru

ОМИРОВА Наргиз Идаят кызы

Преподаватель, заведующая учебной частью кафедры физики, математики и информатики Первого Санкт-Петербургского государственного медицинского университета им. акад. И. П. Павлова, аспирант Санкт-Петербургского государственного университета аэрокосмического приборостроения.
В 2009 году окончила Санкт-Петербургский государственный университет аэрокосмического приборостроения по специальности «Прикладная информатика в экономике».
Является автором пяти научных публикаций.
Область научных интересов — интеллектуальный анализ данных, современные методы статистической обработки медицинских данных.
Эл. адрес: nargiz.eubova@spb-gmu.ru

ПАЛЕЙ Марина Николаевна

Аспирант кафедры госпитальной терапии медицинского факультета Санкт-Петербургского государственного университета.
В 1998 году окончила Санкт-Петербургскую государственную медицинскую академию им. И. И. Мечникова по специальности «Лечебное дело».
Является автором десяти научных публикаций.
Область научных интересов — окислительная модификация белков у больных ХОБЛ.
Эл. адрес: mnpaley@mail.ru

РЫБАЛКИН Михаил Александрович

Аспирант лаборатории теории представлений и динамических систем Санкт-Петербургского отделения Математического института им. В. А. Стеклова РАН.
В 2010 году окончил Санкт-Петербургский государственный политехнический университет по специальности «Математическое и программное обеспечение компьютерных систем».
Является автором четырех научных публикаций.
Область научных интересов — математическое моделирование, полиномиальная алгебра, перестановочные многочлены, методы оптимизации, алгоритмы теории графов.
Эл. адрес: rybalkin@pdmi.ras.ru

СЕБЕРРИ Дженифер Рома

Гражданка Австралии.
Профессор, директор Центра компьютерных исследований безопасности Австралийского государственного университета Волонгонг (Wollongong), основатель школы криптографии Австралии.
В 1966 году получила степень бакалавра в университете Нового Южного Уэльса, в 1969 году — магистра естественных наук в университете Ла Троб, Австралия.
В 1971 году защитила диссертацию на соискание ученой степени доктора наук (PhD).
Является автором более 450 научных публикаций и шести монографий.
Область научных интересов — дискретная математика, комбинаторика, матрицы Адамара, безопасные криптоалгоритмы, передача информации.
Эл. адрес: jennie@uow.edu.au

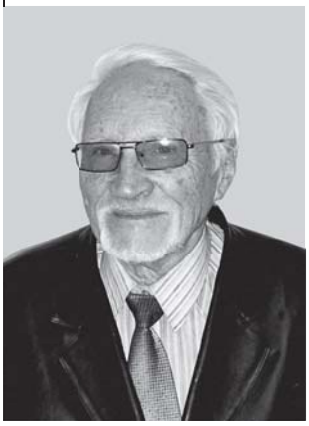
ТАРАСОВА Ирина Леонидовна

Доцент, старший научный сотрудник Института проблем машиноведения РАН, Санкт-Петербург.
В 1978 году окончила Ленинградский политехнический институт им. М. И. Калинина по специальности «Автоматические системы управления».
В 1998 году защитила диссертацию на соискание ученой степени кандидата технических наук.
Является автором более 50 научных публикаций.
Область научных интересов — математическое моделирование, оптимальное управление, идентификация и диагностика.
Эл. адрес: til@msa2.ipme.ru

ТОЛМАЧЕВ Сергей Геннадьевич

Начальник научно-исследовательской лаборатории ОАО «Концерн «Гранит-Электрон», Санкт-Петербург.
В 1980 году окончил Ленинградский электротехнический институт им. В. И. Ульянова (Ленина).
В 1992 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором 25 научных публикаций и трех патентов на изобретения.
Область научных интересов — представление знаний в информационных системах, интеллектуальные методы обработки информации.
Эл. адрес:
cri-granit@peterlink.ru

СОКОЛОВ Михаил Александрович



Профессор кафедры бортовой радиоэлектронной аппаратуры Санкт-Петербургского государственного университета аэрокосмического приборостроения.
В 1947 году окончил Ленинградский институт авиационного приборостроения по специальности «Инженер-электрик по авиационному приборостроению».
В 1972 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором 130 научных публикаций, 50 авторских свидетельств и пяти патентов на изобретения.
Область научных интересов — теория радиолокации и связи, методы проектирования радиоприемных устройств, вычислительные и информационные системы.
Эл. адрес: guap22@mail.ru

ТИШКОВ Артем Валерьевич

Доцент, старший научный сотрудник Санкт-Петербургского института информатики и автоматизации РАН.
В 1996 году окончил Санкт-Петербургский государственный университет по специальности «Программное обеспечение вычислительной техники и автоматизированных систем».
В 1999 году защитил диссертацию на соискание ученой степени кандидата физико-математических наук.
Является автором 62 научных публикаций.
Область научных интересов — медицинская информатика и статистика, поддержка принятия решений в медицинских информационных системах.
Эл. адрес:
artem.tishkov@gmail.com

ТУМЧЕНОК Дмитрий Александрович

Аспирант, инженер-программист лаборатории систем логического управления Института проблем управления им. В. А. Трапезникова РАН, Москва.
В 2013 году окончил Московский государственный технический университет им. Н. Э. Баумана по специальности «Информационные системы и технологии».
Является автором двух научных публикаций.
Область научных интересов — теория графов, теория автоматов, сети Петри.
Эл. адрес:
dmitriy_tumchenok@mail.ru

ФЕДОРЧЕНКО Андрей Владимирович

Младший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации РАН.
В 2014 году окончил Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» по специальности «Компьютерная безопасность».
Область научных интересов — безопасность компьютерных сетей, обнаружение вторжений, вредоносные программы.
Эл. адрес:
fedorchenko@comsec.spb.ru

ЧЕЧУЛИН Андрей Алексеевич

Старший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации РАН.
В 2005 году окончил магистратуру Санкт-Петербургского государственного политехнического университета по специальности «Безопасность и защита информации».
В 2013 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором более 100 научных публикаций.
Область научных интересов — безопасность компьютерных сетей, обнаружение вторжений, анализ сетевого трафика, анализ уязвимостей, интеллектуальный анализ данных.
Эл. адрес:
chechulin@comsec.spb.ru

ШУКАЛОВ Анатолий Владимирович

Генеральный директор ФГУП «Санкт-Петербургское ОКБ «Электроавтоматика» им. П. А. Ефимова».
В 2002 году окончил Санкт-Петербургский государственный университет аэрокосмического приборостроения по специальности «Техническая эксплуатация авиационных электросистем пилотажно-навигационных комплексов».
Является автором более 20 научных и учебно-методических публикаций.
Область научных интересов — проектирование бортовой оптико-электронной и аналого-цифровой вычислительной техники, интегрированная модульная авионика, системы бортовой индикации.
Эл. адрес: aviation78@mail.ru

ЧЕПРУКОВ Юрий Васильевич

Доцент кафедры сервиса инженерных систем и естественнонаучных дисциплин Российского государственного университета туризма и сервиса, филиал в г. Сочи.
В 1976 году окончил Ленинградский политехнический институт им. М. И. Калинина по специальности «Радиофизика и электроника».
В 1991 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором 20 научных публикаций и трех авторских свидетельств на изобретения.
Область научных интересов — теория радиолокации и связи, методы проектирования устройств формирования и обработки сложных сигналов, вычислительные и информационные системы.
Эл. адрес: chuv52@mail.ru

ШИРВАНЯН Артем Мартиросович

Аспирант, инженер-программист лаборатории систем логического управления Института проблем управления им. В. А. Трапезникова РАН, Москва.
В 2013 году окончил Московский государственный технический университет им. Н. Э. Баумана по специальности «Информационные системы и технологии».
Является автором двух научных публикаций.
Область научных интересов — теория графов, теория автоматов, сети Петри.
Эл. адрес:
artshirvanyan@mail.ru

ЯМЩИКОВ Юрий Алексеевич

Инженер-программист ОАО «Концерн «Гранит-Электрон», Санкт-Петербург.
В 2008 году окончил Санкт-Петербургский государственный университет информационных технологий, механики и оптики по специальности «Вычислительные машины, комплексы, системы и сети».
Является автором двух научных публикаций.
Область научных интересов — системный анализ, обработка информации, интеллектуальные технологии управления.
Эл. адрес: gcabman@yandex.ru