ISSN 2519-2310

COMPUTER SCIENCE AND CYBERSECURITY

ISSUE 1(5) 2017

V. N. Karazin Kharkiv National University Publishing

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ УКРАИНЫ
MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені В.Н.КАРАЗІНА
ХАРЬКОВСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ имени В.Н. КАРАЗИНА
V.N. KARAZIN KHARKIV NATIONAL UNIVERSITY

КОМП'ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА
КОМПЬЮТЕРНЫЕ НАУКИ И КИБЕРБЕЗОПАСНОСТЬ
COMPUTER SCIENCE AND CYBERSECURITY
(CS&CS)

Issue 1(5) 2017

Заснований 2015 року

Міжнародний електронний науково-теоретичний журнал
Международный электронный научно-теоретический журнал
International electronic scientific journal

The journal publishes research articles on theoretical, scientific and technical problems of effective facilities development for computer information communication systems and on information security problems based on advanced mathematical methods, information technologies and technical means.

Journal is published quarterly.
Approved for placement on the Internet by Academic Council of the Karazin Kharkiv National University (April 24, 2017, protocol No.6)

Editorial office:
Karazin Kharkiv National University
Svobody sq., 6, office 315a, Kharkiv, 61022, Ukraine
Phone: +38 (057) 705-10-83
E-mail: *cscsjournal@karazin.ua*
Web-page: *http://periodicals.karazin.ua/cscs (Open Journal System)*

Published articles have been internally and externally peer reviewed

TABLE OF CONTENTS

Issue 1(5) 2017

UDC 621.37:621.391

THE METHOD OF PSEUDORANDOM CODES DECODING ON THE BASIS OF THE MODIFIED METHOD OF BRANCHES AND BOUNDARIES

T. Lavrovska, S. Rassomakhin

V. N. Karazin Kharkiv National University, Svobody sq., 4, Kharkov, 61022, Ukraine
lavrovska92@gmail.com, rassomakhin@karazin.ua

Reviewer: Victor Krasnobayev, Dr., Full Professor, V.N. Karazin Kharkiv National University, Svobody sq., 4, Kharkov, 61022, Ukraine;
krasnobayev@karazin.ua

Received on November 2016

Abstract. *Reasons of crisis of error-correcting coding are considered. Underlined the urgency of application of pseudo random codes in modern systems transmission of information. Presented constructive mathematical method of decoding pseudorandom codes based on the use of the method of branches and borders. Is proposed for modification of the classical algorithm of branch and bound. Is proposed, assessment of computing complexity of methods of decoding of pseudorandom codes on basis of the classical and modified algorithm of branches and boundaries is made, and also assessment of computing complexity of the offered method in comparison with exhaustive search method. Program implementation of method of decoding of pseudorandom codes is developed.*

Keywords*: pseudorandom code, branch and bound method, computational complexity, error-correcting coding.*

1 Introduction

Formulation of the problem. Scientific and technical progress in the field of telecommunications in the modern society gives ample opportunities for information exchange. It is a powerful method for development of different information technologies, which strongly enter in daily life of humanity. Business by means of electronic commerce, using Blockchain, application of cloud computing – is not the complete list of achievements of IT area. At the same time the nomenclature and number of technical means of processing and information transfer which work on wireless communication networks are increased from year to year. Therefore, search of new solutions of rational use of frequency and energy resource of transmission channels for creation of the technologies allowing to increase data transmission rate and reduce the required power of transmitters is urgent.

In the theory of information transfer is known the historical role of the methodology based on use of random codes in the proof of fundamental theorems for noisy channels [1,2]. However, proofs on the basis of an random choice of a code usually are called nonconstructive as till today random (pseudorandom) codes (PRC) for support of error correcting and confidentiality of process of information transfer are not used. It is a consequence of absence of acceptable computing complexity of methods of creation and decoding of PRC which provide ability of correction, the close to maximum likelihood.

Implementation of constructive algorithms of creation and processing of PRC can be expected only when using of determinate algorithms of generation of pseudorandom characters of code words. Attractiveness of PRC technologies consist in a possibility of creation of signal and code constructions, which will allow to raise at the same time as the frequency, and energetic efficiency of information transmission systems. However, the main barrier to broad use of PRC is absence of methods of decoding not based on algorithm of exhaustive search.

Computing complexity of the algorithms based on computation of Euclidean distances increases exponentially with increase in block length of a code and in case of required values of block length

is unacceptable. Receiving simple linear algebraic methods of decoding is encountered with difficulties following from nonlinearity of the determined algorithms of generation of the pseudorandom sequence. Thus, the ideas of application of PRC will be applied constructive if develop the linear (linearized) methods of decoding of such codes.

Objective: development of a constructive mathematical method of decoding of PRC on the basis of application of the modified method of branches and boundaries, assessment of computing complexity of operation of decoding and its comparing with exhaustive search algorithms based on use of the rule of maximum likelihood.

MAIN PART

2 Statement of the task of decoding, as main objective of the linear programming

The procedure of obtaining of code book of arbitrary pseudorandom code can be provided as follows. The general flow of binary characters of a source is subject to coding whishes divided on the sequences by length of **k** bits. These sequences are intended for creation of pseudorandom error correcting code. At the same time each combination from **k** binary characters of a source is transferred to decimal value x_0 – sequence number by which is determined appropriate sequence of pseudorandom numbers $x_1, x_2, \ldots, x_{n-1}$, that is x_0 –is ancestor number of the code word $X_j=\left\{x^j_0, x^j_1, \ldots, x^j_{n-1}\right\}$ with appropriate number $j = x^j_0$, $j\in\left[0,\ldots,\left(2^k\text{-}1\right)\right]$. Thus, for each block from **k** binary characters of a source are put in compliance block from **n** not binary numbers of a code. Numbers of code words determine informative parameters of a signal. For example, amplitudes of the quadrature components of subcarrier frequencies [3]. Magnitude

$$R= k/n , \qquad (1)$$

is speed of error correcting code and shows a ratio of amount of information binary characters of the message with amount of not binary characters of a codewhich are used for transmissions on communication link. Speed of a code (1) can be both more and less than one. Reason of this property is ability of a choice of length of the code word PRC irrespective of length of the initial block of binary characters **k**.

On an output of the channel after impact of noise the sequence has an form:

$$X^*_j=X_j+\Xi=\left\{x^j_0+\xi_0, x^j_1+\xi_1,\ldots, x^j_{n-1}+\xi_{n-1}\right\}=\left\{x^*_0, x^*_1,\ldots, x^*_{n-1}\right\},$$

where $\Xi=\left\{\xi_0, \xi_1,\ldots,\xi_{n-1}\right\}$ is vector of coordinates of noise. These codes allow to provide rather low probability of decoding with an error on the block of a code in case of simple increase in block length n if throughput of the channel was not exceeded.

Now pseudorandom codes are not applied in information transmission systems because the known methods of decoding of such codes are based on implementation of the rule of maximum likelihood and are possible only in case of symbol-by-symbol comparing, the received channel word with all possible options which are stored in the receiver. Decoding procedure is based on search of the minimum value of length of the difference vector of Euclidean distances between points X^*_j i X_i:

$$\min\left|X^*_j\text{-}X_i\right|=\sqrt{(x_0{}^{j*}\text{-}x_0{}^{i})^2+\ldots+(x_{n-1}{}^{j*}\text{-}x_{n-1}{}^{i})^2},$$

where $i\in\left[0\ldots\left(2^k\text{-}1\right)\right]$.

Thus, computing complexity of such methods of decoding increases exponentially with length of block code **n**.

For solution of this problem of decoding in case of creation of PRC is offered to use a procedure of computation of characters of code words by recurrent rule of the linear congruent generation

(LCG). This rule allows to linearize the issue of decoding of PRC and essential to reduce its computing complexity. It is possible by replacement of computation Euclidean distances on rule of smallest projections (SP) which are identical on the end result

$$\min\sum_{q=0}^{n-1}\left|x_q^{j*}-x_q^{i}\right|, \quad \text{where} \quad i\in\left[0..\left(2^k-1\right)\right].$$

Using of SP in a complex with method of decoding of PRC on the basis of the modified method of branches and boundaries will allow to provide polynomial computing complexity. Process of obtaining code words PRC on the basis of the linear congruent generation is as follows [3,4]. Each next i number of the pseudorandom sequence of arbitrary **j** code word is generated by the recurrent rule of generation of the sequence of LCG in case x_0^j:

$$x_i^j=(a\cdot x_{i-1}^j+b)\bmod m, \tag{2}$$

where a – multiplicative parameter, b – additive parameter of conversion, *mod* – operation of computation of the module m. Magnitude $m=2^k$ is power of the alphabet of words PRC. For simplification of mathematical calculations the upper index in designation of variables x_i^j will not be used, that is number of the code word is fixed $x_i^j \to x_i$.

In a general view the offered method of decoding of a pseudorandom error correcting code in the conditions of distortions of characters is considered. This method is based on use of a mathematical algorithm of branches and boundaries for directional search of the decision.

Operation of decoding is reached if in the conditions of possible distortions, the ancestor number x_0 of a segment of the pseudorandom sequence (PRS) is correctly defined. Magnitude x_0 (the first number in code word of length **n**) in binary representation correctly defines the transferred binary sequence of a source. For search of number all characters of PRS of a code are used, as all of them are connected to ancestor number a recurrent chain of non-linear computation (2).

Whereas in (2) non-linear operation of computation of the module is used, it is a hindrance to implementation of directional search of the decision. Necessary perform linearization of operation of decoding by introduction of additional integer non-negative numerical parameter y.

Quantitative value y is equal to a multiplier by equivalent linear algebraic operation of computation of the module m. Then mathematical expression (2) changes the next way:

$$x_{i+1}=ax_i+b-y_im, \quad i\in\left[0,\ldots,(n-1)\right]. \tag{3}$$

Mathematical expression (3) is fair only in case of execution of restrictions which follow from a mathematical gist of an algorithm of LCG PRC:

$$0\le y_i\le\left\lfloor\frac{(m-1)a+b}{m}\right\rfloor, \qquad y_i \ - \text{ integer}, \ i\in\left[0,\ldots,(n-2)\right]. \tag{4}$$

For compensating of distortions of arbitrary initial code word of a source **x** in result of summing with elements of a vector of Gaussian random variables Ξ for each of numbers of the code word x_i^*, $i\in[0,\ldots,n-1]$ will be entered couple of auxiliary non-negative variables w_{2i+1}, w_{2i+2}.

This pair characterizes possible double-sided deviations of number x_i^* which are a consequence of action of a vector of a noise Ξ. One variable from this pair enters in calculation with sign "+", it means that it is added to the number distorted by a noise x_i^*, other–with sign «-», it means that it is subtracted from x_i^*. Then for observed code word $X^*=\left\{x^*_0,\ldots,x^*_{n-1}\right\}$ system of equations is formed:

$$\begin{cases} x_0 = x^*_0 - w_1 + w_2; \\ x_1 = x^*_0 - w_3 + w_4; \\ \vdots \\ x_{n-1} = x^*_{n-1} - w_{2n-1} + w_{2n}. \end{cases} \quad (5)$$

In each of the equations (5) one of pair of auxiliary variables **w** with an even or odd index will equal zero because the deviation from action of a noise can be only towards reduction, or towards increase of true number. At the same time variables x_i must satisfy to inequality $0 \le x_i \le (m-1)$. For decision of the task of decoding is planned to use the linear programming (LP), then the left inequality of this restriction (non negativity support) is automatically executed according to terms of the canonical task LP.

Issue LP-in a canonical form requires of representation of all restrictions of area of admissible decisions in the form of equalities. Therefore, for changeover from the right inequality to equality non-negative integer auxiliary variables $\tilde{x}_n, \tilde{x}_{n+1}, \ldots, \tilde{x}_{2n-1}$ is entered:

$$\begin{cases} \tilde{x}_n = (m-1-x^*_0) + w_1 - w_2; \\ \tilde{x}_{n+1} = (m-1-x^*_1) + w_3 - w_4; \\ \vdots \\ \tilde{x}_{2n-1} = \left(m-1-x^*_{\frac{n-1}{2}}\right) + w_{2n-1} - w_{2n}. \end{cases} \quad (6)$$

In case of execution of restrictions (6) is reached execution of the following system of equalities:

$$\begin{cases} x_0 + \tilde{x}_n = m-1; \\ x_1 + \tilde{x}_{n+1} = m-1; \\ \vdots \\ x_{n-1} + \tilde{x}_{2n-1} = m-1. \end{cases} \quad (7)$$

On the basis of (3) and (4) are defined values y_i corresponding to multipliers of equivalent algebraic representation of operation of computation of the module m:

$$\begin{cases} y_0 = \frac{1}{m}(ax^*_0 - x^*_1 + b) - \frac{a}{m}w_1 + \frac{a}{m}w_2 + \frac{1}{m}w_3 - \frac{1}{m}w_4; \\ \vdots \\ y_{n-2} = \frac{1}{m}(ax^*_{n-2} - x^*_{n-1} + b) - \frac{a}{m}w_{2n-3} + \frac{a}{m}w_{2n-2} + \frac{1}{m}w_{2n-1} - \frac{1}{m}w_{2n}. \end{cases} \quad (8)$$

Minimum of objective function **L**, which needs to be provided when decoding PRC according to the rule of the smallest projections considered above, has an appearance:

$$L = \sum_{i=1}^{2n} w_i = w_1 + w_2 + \ldots + w_{2i-1} + w_{2i}. \quad (9)$$

The physical sense of objective function consists in finding of the minimum sum of projections of the ends of the difference vector between a point X^* on an output of noisy channel and a point X of the code book of PRC which is closest to X^*.

Mathematical expressions (5), (6), (8) and (9) represent a canonical statement of the main problem of the linear programming (MPLP). For solution MPLP is applied simplex a method and its implementation in the form of table algorithm. MPLP contains $3n-1$ equations and has $5n-1$ unknown variables 2n variables choosing as the free, and remaining $3n-1$ is as basis variables expressed through free. The free variables are $\underbrace{w_1, \ldots, w_{2n}}_{2n}$.

Then conversions of the equations (5), (6), (8) and (9) gives the following statement of the integer task LP. It is necessary to find the non-negative values of variables x_i, y_j, w_q satisfying to

system of restrictions equalities (5), (6), (8) and providing a minimum of objective function (9). For decision of formulated integer task LP is applied table algorithm of simplex method. On the basis of the received expressions the simplex table is built (Table 1).

Rules of filling of the table are as follows:

– names of basis variables to the first column of basis variables (B.V.)are entered;

– names of the free variables to the first line of the free variables (F.V.) are entered;

– free terms from the equations (5), (6), (8) and (9) are entered to the second column of free terms (S.Ch.);

– starting with the third column are entered coefficients of free variables from the equations (5), (6), (8) and (9) with changing signs on opposite.

Decoding of the code word PRC that was distorted by noises comes down to the correct determination of value x_0 – ancestor number of the code word PRC that correctly defines k bit combination of binary characters of a source.

The initial table contains the basic plan (*a task has variant of solution*), where B.V. values are equal to elements in the corresponding lines of the F.T. column, and values of the free variables are equal to zero. In a line of objective function in the F.T. column is a value of size of objective function. This value is used for realization of directional searching of the decision on a method of branches and borders. Decoding on the basis of a method of branches and borders is iterated that means creation of a tree of decisions with tops of minimum values of basic plans. Route by a tree from initial top to some fixed top determines the admissible sequence of the choice of integer values for task variables. Main goal of decoding by proposed method is receiving integer variables of $\boldsymbol{x}$ and $\boldsymbol{y}$ at minimum possible value of objective function **L**.

Table 1 - The initial simplex table

F.V / B.V.	F. T.	w_1	w_2	w_3	w_4	…	w_{2n-3}	w_{2n-2}	w_{2n-1}	w_{2n}
x_0	x^*_0	1	-1	0	0	…	0	0	0	0
x_1	x^*_1	0	0	1	-1	…	0	0	0	0
⋮	⋮	⋮	⋮	⋮	⋮	…	⋮	⋮	⋮	⋮
x_{n-1}	x^*_{n-1}	0	0	0	0	…	0	0	1	-1
x_n	$\left(m-1-x^*_0\right)$	-1	1	0	0	…	0	0	0	0
x_{n+1}	$\left(m-1-x^*_1\right)$	0	0	-1	1	…	0	0	0	0
⋮	⋮	⋮	⋮	⋮	⋮	…	⋮	⋮	⋮	⋮
x_{2n-1}	$\left(m-1-x^*_{n-1}\right)$	0	0	0	0	…	0	0	-1	1
y_0	$\frac{1}{m}\left(ax^*_0-x^*_1+b\right)$	$\frac{a}{m}$	$-\frac{a}{m}$	$-\frac{1}{m}$	$\frac{1}{m}$	…				
⋮	⋮	⋮	⋮	⋮	⋮	…	⋮	⋮	⋮	⋮
y_{n-2}	$\frac{1}{m}\left(ax^*_{n-3}-x^*_{n-2}+b\right)$					…	$\frac{a}{m}$	$-\frac{a}{m}$	$-\frac{1}{m}$	$\frac{1}{m}$
L	0	-1	-1	-1	-1	…	-1	-1	-1	-1

Formally the method of branches and borders can be described by the sequence of the following stages.

On the first iteration the plan of Table 1 is analyzed on permissibility on the basis of content of cells of a column F.T.. If all elements of column of the free terms are not the negative then the plan is permissible. If all elements of line of objective function **L** (except an element in the F.T. column) are negative, then the plan is optimum.

If any element of F.T. column is negative, plan is not permissible and the table is modified according to an algorithm of the solution of a dual problem of LP. The line with the negative element is allowing. If such lines are several, then the line is chosen which has maximal on an absolute value negative element. In the allowing line is looked for an element which has the negative sign. If such elements are several, then among them is selected maximum on an absolute value. The column which has this element is considered allowing. On crossing of the allowing column and line is an allowing element.

Modification of the table with exchange between couple a "free-basic" variables from headings of allowing line and column and recalculation of maintenance of cells must make for transition to the next plan of task as follows:

- headings of variables which correspond to the allowing column and line are interchanged the position;
- an allowing element changes on inverse;
- elements of an allowing line are divided into the allowing element;
- elements of allowing column are divided into the allowing element and are changed their sign on inverse;
- to all other elements from old table is added multiplication of an element of the allowing line from old table which is in the same column, on an element of the allowing column from new table which is in the same line.

After modification, received table repeatedly is analyzed on permissibility. After obtaining permissible plan, it is analyzed on an optimality.

If in a line of objective function is at least one positive element, then the plan not optimum and the table is modified according to an algorithm of the decision of the direct task LP. Column which has positive element is selected as allowing column. If such elements are several then among them is selected maximum. In the allowing column are analyzed elements which match on a sign with element of F.T. column. If such couples of elements a few, then it is necessary to calculate the relation of the free term to appropriate element of allowing column. The allowing line is the line which has the minimum value of this relation. On crossing of the allowing column and line is an allowing element.

The table is modified and content of cells is recalculated by rules which are considered above. After modification of table, table repeatedly is analyzed on permissibility and optimality. These iterations cyclically repeat till that moment will not be found permissible and optimum plan which is called the basic plan of the task.

Further the received basic plan is analyzed on existence of integral numbers in F.T. column. Variables x_i, $i \in [0,\ldots,(2n-1)]$ and y_j, $j \in [0,\ldots,(n-2)]$ which are contained in the cells of F.T. column must contain integral numbers. The first line which has not integer, specifies the name of the variable (x_i, y_j or w_k) for which will be created an additional constraint of integrality.

For reduction of computing complexity of this method of decoding is offered to use the modified method of branches and boundaries. Gist of this modification consists in provision of priority of the analysis of integrality only of variables $\mathbf{y_j}$. Experimentally proved that when the integrality of those variables provides integrality of other variables of decoding task. This modification significantly reduces the number of iterations of search of the decision, as a result, reduces computing complexity of decoding procedure of PRC. Additional restriction is created by introduction to the basic plan of an additional line for an additional auxiliary basis variable. The mechanism of introduction of additional restrictions in details will be considered below in case of presentation of a specific example of implementation of the decision of the task of decoding. On the basis of additional restrictions is executed branching of a decision tree. Let's assume that for providing of

integrality is selected variable $\mathbf{y_j}$. Area of admissible solutions of zero step of the task breaks on two not crossed subareas for the following step $G_1^{(1)}$ and $G_2^{(1)}$ on the basis of the rule:

$$G_1^{(1)} = \left\{ Y \in G^{(0)}, y_i \le \lfloor y_i \rfloor \right\};$$
$$G_2^{(1)} = \left\{ Y \in G^{(0)}, y_i \ge \lceil y_i \rceil \right\}. \quad (10)$$

The rule (10) means that in new areas value of variable needs to be reduced to the next smaller integer number $\lfloor y_i \rfloor$, or on the contrary, be to increased to the next bigger integer number $\lceil y_i \rceil$. Then, on the technology described above, it is necessary to find sequentially basic plans of tasks for areas $G_1^{(1)}$ and $G_2^{(1)}$. After execution of branching and formation of restrictions, basic plans are analyzed on permissibility and optimality, if necessary is executed modification and recalculation of tables, and also analysis of integrality. Actions is iterated until all elements in lines of the F.T. column will be integers. At the same time some integer variables can be in composition of the free, it means that they are equal to zero.

3 Decoding of PRC on basis of modified method of branches and boundaries

Example of application of offered method for decoding of a pseudo random error correcting code on the basis of use of the modified method of branches and boundaries is considered.

Parameters of a pseudorandom error correcting code are values: k=5; n=5. For LCG technology parameters are selected: $m = 2^k = 32,\ a = 5,\ b = 19$. Sequentially changing numbers of the binary sequences on length $k = 5$ characters $x_0 = 0,1,\ldots,31$ and using the rule (2) for computation of characters of code words and is obtained code book of PRC which is provided in Table 2.

Table 2 – Code sequences of the complete code book of PRC

x_0	X	x_0	X	x_0	X	x_0	X
0	0, 19, 18, 13, 20	8	8, 27, 26, 21, 28	16	16, 3, 2, 29, 4	24	24, 11, 10, 5, 12
1	1, 24, 11, 10, 5	9	9, 0, 19, 18, 13	17	17, 8, 27, 26, 21	25	25, 16, 3, 2, 29
2	2, 29, 4, 7, 22	10	10, 5, 12, 15, 30	18	18, 13, 20, 23, 6	26	26, 21, 28, 31, 14
3	3, 2, 29, 4, 7	11	11, 10, 5, 12, 15	19	19, 18, 13, 20, 23	27	27, 26, 21, 28, 31
4	4, 7, 22, 1, 24	12	12, 15, 30, 9, 0	20	20, 23, 6, 17, 8	28	28, 31, 14, 25, 16
5	5, 12, 15, 30, 9	13	13, 20, 23, 6, 17	21	21, 28, 31, 14, 25	29	29, 4, 7, 22, 1
6	6, 17, 8, 27, 26	14	14, 25, 16, 3, 2	22	22, 1, 24, 11, 10	30	30, 9, 0, 19, 18
7	7, 22, 1, 24, 11	15	15, 30, 9, 0, 19	23	23, 6, 17, 8, 27	31	31, 14, 25, 16, 3

For transmission on the channel is selected code word generated by number $x_0 = 0$ or $X = \{0,19,18,13,20\}$, which as a result of summing with a noise vector Ξ and is changed $X^* = \{0,18,22,15,20\}$. For simplification of an example the numbers of the code word distorted by transmission are rounded to integer values. On the basis of expressions (5), (6), (8) and (9) and according to rules of filling of initial simplex table (Table 1) is formed starting table of this example (Table 3).

Table 3 contains the permissible, optimum basic plan of not integer problem of LP (elements of column FT are not negative, elements of line L – are not positive). However the plan does not meet of condition of integrality (FT column contains in lines $y0 \div y3$ not integer values). According to developed of modified method of branches and borders additional restriction is formed for area $G_1^{(1)}$. Firstly (in the analysis of lines of Table 3 from top to down), not integer variable $y0$ is chosen. That variable $y0$, which is equal in the Table 3 to size 0,0312 will got value of the next smaller integer $\lfloor y0 \rfloor = 0$.

Performance of inequality is required $y0 \le 0$. For formation of a line of constraint for new table it is necessary to execute transition from restriction inequality to restriction equality, by introduction of an additional non-negative variable v: $y0 + v = 0$. Let's express a variable v as basic:

$$v = 0 - y0 . \quad (11)$$

Table 3 – First iteration *(Step 1)*

	FT	w1	w2	w3	w4	w5	w6	w7	w8	w9	w10
x0	0	1	-1	0	0	0	0	0	0	0	0
x1	18	0	0	1	-1	0	0	0	0	0	0
x2	22	0	0	0	0	1	-1	0	0	0	0
x3	15	0	0	0	0	0	0	1	-1	0	0
x4	20	0	0	0	0	0	0	0	0	1	-1
x5	31	-1	1	0	0	0	0	0	0	0	0
x6	13	0	0	-1	1	0	0	0	0	0	0
x7	9	0	0	0	0	-1	1	0	0	0	0
x8	16	0	0	0	0	0	0	-1	1	0	0
x9	11	0	0	0	0	0	0	0	0	-1	1
y0	0,031	0,1562	-0,1562	-0,0312	0,0312	0	0	0	0	0	0
y1	2,718	0	0	0,1562	-0,1562	-0,0312	0,03125	0	0	0	0
y2	3,562	0	0	0	0	0,1562	-0,1562	-0,0312	0,0312	0	0
y3	2,312	0	0	0	0	0	0	0,1562	-0,1562	-0,0312	0,0312
L	0	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1

Definition $y0$ in the form of a linear combination of free variables is set by line $y0$ of Table 3:

$$y_0 = 0,1562w1 - 0,1562w2 - 0,0312w3 - \\ - 0,0312w4 + 0,0312. \quad (12)$$

Using (12) in (11), the equation of additional restriction is created:

$$v = -0,0312 - 0,1562w1 + 0,1562w2 + \\ + 0,0312w3 - 0,0312w4. \quad (13)$$

On the basis of (13) the additional line for a fictitious variable v is entered into the basic plan. As a result size of the table increases, and it is transformed to Table 4.

Table 4 – First iteration *(Step 1)* with additional restriction

	FT	w1	w2	w3	w4	w5	w6	w7	w8	w9	w10
x0	0	1	-1	0	0	0	0	0	0	0	0
x1	18	0	0	1	-1	0	0	0	0	0	0
x2	22	0	0	0	0	1	-1	0	0	0	0
x3	15	0	0	0	0	0	0	1	-1	0	0
x4	20	0	0	0	0	0	0	0	0	1	-1
x5	31	-1	1	0	0	0	0	0	0	0	0
x6	13	0	0	-1	1	0	0	0	0	0	0
x7	9	0	0	0	0	-1	1	0	0	0	0
x8	16	0	0	0	0	0	0	-1	1	0	0
x9	11	0	0	0	0	0	0	0	0	-1	1
y0	0,0312	0,1562	-0,1562	-0,0312	0,0312	0	0	0	0	0	0
y1	2,7187	0	0	0,1562	-0,1562	-0,0312	0,0312	0	0	0	0
y2	3,5625	0	0	0	0	0,1562	-0,1562	-0,0312	0,0312	0	0
y3	2,3125	0	0	0	0	0	0	0,1562	-0,1562	-0,0312	0,0312
v	-0,031	-0,1562	0,1562	0,0312	-0,0312	0	0	0	0	0	0
L	0	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1

Table 4 for subarea $G_1^{(1)}$ contains the impermissible plan because FT column has a negative element. According to the rules described above is necessary to execute the solution of a dual task. Allowing line – a line of restriction v, the allowing column – a column of a variable w1 and the allowing element which is located on crossing of a line v and column w1 are chosen (look at shaded elements in Table 4).

For transition to the permissible plan is necessary to execute modification and recalculation of Table 4 according to rules which were considered above. Modification of the plan gives Table 5.

Table 5 – Modification of initial Table 4 *(Step 1)*

	FT	v	w2	w3	w4	w5	w6	w7	w8	w9	w10
x0	-0,2	6,4	0	0,2	-0,2	0	0	0	0	0	0
x1	18	0	0	1	-1	0	0	0	0	0	0
x2	22	0	0	0	0	1	-1	0	0	0	0
x3	15	0	0	0	0	0	0	1	-1	0	0
x4	20	0	0	0	0	0	0	0	0	1	-1
x5	31,2	-6,4	0	-0,2	0,2	0	0	0	0	0	0
x6	13	0	0	-1	1	0	0	0	0	0	0
x7	9	0	0	0	0	-1	1	0	0	0	0
x8	16	0	0	0	0	0	0	-1	1	0	0
x9	11	0	0	0	0	0	0	0	0	-1	1
y0	0	1	0	0	0	0	0	0	0	0	0
y1	2,7187	0	0	0,1562	-0,1562	-0,0312	0,0312	0	0	0	0
y2	3,5625	0	0	0	0	0,1562	-0,1562	-0,0312	0,0312	0	0
y3	2,3125	0	0	0	0	0	0	0,1562	-0,1562	-0,0312	0,0312
w1	0,2	-6,4	-1	-0,2	0,2	0	0	0	0	0	0
L	0,2	-6,4	-2	-1,2	-0,8	-1	-1	-1	-1	-1	-1

The decision received in Table 5 is analyzed on permissibility. As the plan is not permissible then its modification is executed. As allowing line is selected x0, and allowing the column - w4. Recalculation gives Table 6.

Table 6 – Modification of Table 5 *(Step 1)*

	FT	v	w2	w3	x0	w5	w6	w7	w8	w9	w10
w4	1	-32	0	-1	-5	0	0	0	0	0	0
x1	19	-32	0	0	-5	0	0	0	0	0	0
x2	22	0	0	0	0	1	-1	0	0	0	0
x3	15	0	0	0	0	0	0	1	-1	0	0
x4	20	0	0	0	0	0	0	0	0	1	-1
x5	31	0	0	0	1	0	0	0	0	0	0
x6	12	32	0	0	5	0	0	0	0	0	0
x7	9	0	0	0	0	-1	1	0	0	0	0
x8	16	0	0	0	0	0	0	-1	1	0	0
x9	11	0	0	0	0	0	0	0	0	-1	1
y0	0	1	0	0	0	0	0	0	0	0	0
y1	2,875	-5	0	0	-0,7812	-0,0312	0,0312	0	0	0	0
y2	3,5625	0	0	0	0	0,1562	-0,1562	-0,0312	0,0312	0	0
y3	2,3125	0	0	0	0	0	0	0,1562	-0,1562	-0,0312	0,0312
w1	0	0	-1	0	1	0	0	0	0	0	0
L	1	-32	-2	-2	-4	-1	-1	-1	-1	-1	-1

Table 6 contains permissible and optimum basic plan. This plan is noted on a tree of decisions (Fig. 1) by corresponding top $G_1^{(1)}$ which has value of objective function L=1.

Restriction for area $G_2^{(1)}$ is formed so that the variable $y0$ will got value of the next bigger integer $\lceil y0 \rceil = 1$. For this purpose, performance of inequality $y0 \geq 1$ is required. $y0 \leq 0$. For transition from restriction inequality to restriction equality is entered an additional non-negative variable v: $y0 - v = 0$, or:

$$v = y0 - 1. \quad (14)$$

For designation of an additional variable in (14) is used the same name v, all fictitious variables are auxiliary and their size at achievement of the final decision of a task does not matter. When obtaining of intermediate basic plan any additional fictitious variable is appeared as a part of basic variables of a task (in heading of any line) for reduction of dimension of tables the corresponding line will delete.

Definition $y0$ through values of free variables gives:

$$v = -0,968 + 0,1562w1 - 0,1562w2 - \\ - 0,0312w3 + 0,0312w4, \quad (16)$$

What to allows to enter a line of additional restriction into the Table 7.

Table 7 – The second iteration with additional restriction *(Step 1)*

	FT	w1	w2	w3	w4	w5	w6	w7	w8	w9	w10
x0	0	1	-1	0	0	0	0	0	0	0	0
x1	18	0	0	1	-1	0	0	0	0	0	0
x2	22	0	0	0	0	1	-1	0	0	0	0
x3	15	0	0	0	0	0	0	1	-1	0	0
x4	20	0	0	0	0	0	0	0	0	1	-1
x5	31	-1	1	0	0	0	0	0	0	0	0
x6	13	0	0	-1	1	0	0	0	0	0	0
x7	9	0	0	0	0	-1	1	0	0	0	0
x8	16	0	0	0	0	0	0	-1	1	0	0
x9	11	0	0	0	0	0	0	0	0	-1	1
y0	0,0312	0,1562	-0,1562	-0,0312	0,0312	0	0	0	0	0	0
y1	2,7187	0	0	0,1562	-0,1562	-0,0312	0,0312	0	0	0	0
y2	3,5625	0	0	0	0	0,1562	-0,1562	-0,0312	0,0312	0	0
y3	2,312	0	0	0	0	0	0	0,1562	-0,1562	-0,0312	0,0312
v	-0,968	0,1562	-0,1562	-0,0312	0,0312	0	0	0	0	0	0
L	0	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1

Table 7 for subarea $G_2^{(1)}$ contains impermissible plan, because column FT has negative element. According to the rules described above are chosen as the allowing line – a line of restriction v, and as the allowing column – a column w2. For achievement of permissibility of plan is executed modification of Table 7.

As a result Table 8 is obtained permissible and optimum basic plan of Table 8 is noted on a tree of decisions (Fig. 1) by corresponding top $G_2^{(1)}$ which has value of objective function L = 6,2.

Tops $G_1^{(1)}$ and $G_2^{(1)}$ of first step of the decision, which correspond to Tables 6 and 8 must be branched for the purpose of achievement of integer values of other integer variables.

The choice of the next top (table) among the "hanging" tops of a tree of decisions for the subsequent branching is carried out from the point of view of its greatest prospects. For obtaining next basic plan is chosen table which has the smallest (*among the "hanging" tops*) value of objective function. Then next top of tree of decisions which will be used for branching, is Table 6 with value L = 1.

Table 8 – Modification of Table 7 *(Step 1)*

	FT	w1	v	w3	w4	w5	w6	w7	w8	w9	w10
x0	6,2	0	-6,4	0,2	-0,2	0	0	0	0	0	0
x1	18	0	0	1	-1	0	0	0	0	0	0
x2	22	0	0	0	0	1	-1	0	0	0	0
x3	15	0	0	0	0	0	0	1	-1	0	0
x4	20	0	0	0	0	0	0	0	0	1	-1
x5	24,8	0	6,4	-0,2	0,2	0	0	0	0	0	0
x6	13	0	0	-1	1	0	0	0	0	0	0
x7	9	0	0	0	0	-1	1	0	0	0	0
x8	16	0	0	0	0	0	0	-1	1	0	0
x9	11	0	0	0	0	0	0	0	0	-1	1
y0	1	0	-1	0	0	0	0	0	0	0	0
y1	2,7187	0	0	0,1562	-0,1562	-0,0312	0,0312	0	0	0	0
y2	3,562	0	0	0	0	0,1562	-0,1562	-0,0312	0,0312	0	0
y3	2,312	0	0	0	0	0	0	0,1562	-0,1562	-0,0312	0,0312
w2	6,2	-1	-6,4	0,2	-0,2	0	0	0	0	0	0
L	6,2	-2	-6,4	-0,8	-1,2	-1	-1	-1	-1	-1	-1

On the second step is chosen next not integer variable $y1$ for formation of additional restriction of area $G_1^{(2)}$. So that chosen variable $y1$ is equal in the Table 6 to size 2,875 will have value of the next smaller integer $\lfloor y1 \rfloor = 2$. Additional restriction is formed by an example of expressions (12) and (16) that leads to Table 9.

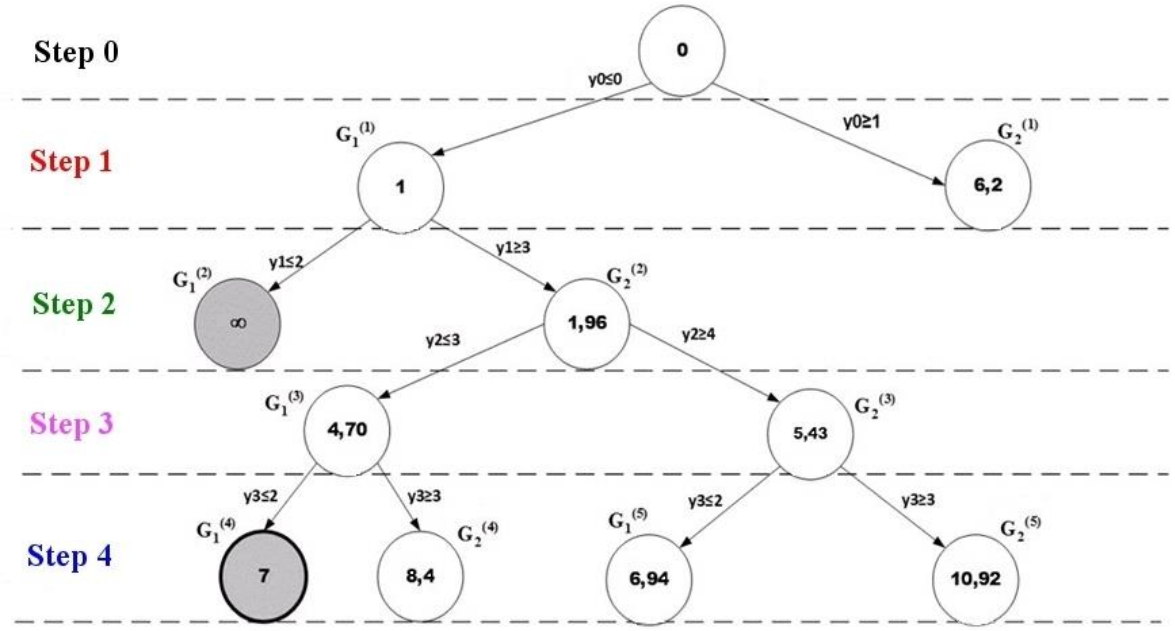


Fig. 1 – The tree of decisions for the modified method of branches and borders

Table 9 for subarea $G_1^{(2)}$ contains impermissible plan, because column FT has negative element. According to the rules described above are chosen as the allowing line – a line of restriction v, and as the allowing column – a column $w6$.

Modification of the table lead to the plan presented in Table 10.

Table 9 – First iteration *(Step 2)*

	FT	v	w2	w3	x0	w5	w6	w7	w8	w9	w10
w4	1	-32	0	-1	-5	0	0	0	0	0	0
x1	19	-32	0	0	-5	0	0	0	0	0	0
x2	22	0	0	0	0	1	-1	0	0	0	0
x3	15	0	0	0	0	0	0	1	-1	0	0
x4	20	0	0	0	0	0	0	0	0	1	-1
x5	31	0	0	0	1	0	0	0	0	0	0
x6	12	32	0	0	5	0	0	0	0	0	0
x7	9	0	0	0	0	-1	1	0	0	0	0
x8	16	0	0	0	0	0	0	-1	1	0	0
x9	11	0	0	0	0	0	0	0	0	-1	1
y0	0	1	0	0	0	0	0	0	0	0	0
y1	2,875	-5	0	0	-0,7812	-0,0312	0,0312	0	0	0	0
y2	3,5625	0	0	0	0	0,1562	-0,1562	-0,0312	0,0312	0	0
y3	2,3125	0	0	0	0	0	0	0,1562	-0,1562	-0,0312	0,0312
w1	0	0	-1	0	1	0	0	0	0	0	0
v	-0,875	5	0	0	0,7812	0,0312	-0,0312	0	0	0	0
L	1	-32	-2	-2	-4	-1	-1	-1	-1	-1	-1

Table 10 contains impermissible plan (*a negative number in a line* $x7$ *of the FT column*). As other numbers in this line are not negative, then continuation of calculations for this table does not make sense, because getting permissible decision is impossible.

Table 10 – Modification of the Table 9 *(Step 2)*

	FT	v	w2	w3	x0	w5	v	w7	w8	w9	w10
w4	1	-32	0	-1	-5	0	0	0	0	0	0
x1	19	-32	0	0	-5	0	0	0	0	0	0
x2	50	-160	0	0	-25	0	-32	0	0	0	0
x3	15	0	0	0	0	0	0	1	-1	0	0
x4	20	0	0	0	0	0	0	0	0	1	-1
x5	31	0	0	0	1	0	0	0	0	0	0
x6	12	32	0	0	5	0	0	0	0	0	0
x7	-19	160	0	0	25	0	32	0	0	0	0
x8	16	0	0	0	0	0	0	-1	1	0	0
x9	11	0	0	0	0	0	0	0	0	-1	1
y0	0	1	0	0	0	0	0	0	0	0	0
y1	2	0	0	0	0	0	1	0	0	0	0
y2	7,937	-25	0	0	-3,9062	0	-5	-0,0312	0,0312	0	0
y3	2,312	0	0	0	0	0	0	0,1562	-0,1562	-0,0312	0,0312
w1	0	0	-1	0	1	0	0	0	0	0	0
w6	28	-160	0	0	-25	-1	-32	0	0	0	0
L	29	-192	-2	-2	-29	-2	-32	-1	-1	-1	-1

Plan of Table 10 is noted on a tree of decisions (Fig. 1) by corresponding top $G_1^{(2)}$ which has value of objective function $L = \infty$. The top $G_1^{(2)}$ is final of branch, and is not subject to further branching.

The next restriction for area $G_2^{(2)}$ is built so that the variable $y1$ will have got value of the next bigger integer number $\lceil y1 \rceil = 3$. Additional restriction was created by an example of expression (16) leads to plan of Table 11. Table 11 contains impermissible plan because FT column has a negative number. According to described above by the rules allowing line and column are additional variables v (*exchange of positions between two additional fictitious variables*).

Table 11 – Second iteration *(Step 2)*

	FT	v	w2	w3	x0	w5	w6	w7	w8	w9	w10
w4	1	-32	0	-1	-5	0	0	0	0	0	0
x1	19	-32	0	0	-5	0	0	0	0	0	0
x2	22	0	0	0	0	1	-1	0	0	0	0
x3	15	0	0	0	0	0	0	1	-1	0	0
x4	20	0	0	0	0	0	0	0	0	1	-1
x5	31	0	0	0	1	0	0	0	0	0	0
x6	12	32	0	0	5	0	0	0	0	0	0
x7	9	0	0	0	0	-1	1	0	0	0	0
x8	16	0	0	0	0	0	0	-1	1	0	0
x9	11	0	0	0	0	0	0	0	0	-1	1
y0	0	1	0	0	0	0	0	0	0	0	0
y1	2,875	-5	0	0	-0,7812	-0,0312	0,0312	0	0	0	0
y2	3,5625	0	0	0	0	0,1562	-0,1562	-0,0312	0,0312	0	0
y3	2,3125	0	0	0	0	0	0	0,1562	-0,1562	-0,0312	0,0312
w1	0	0	-1	0	1	0	0	0	0	0	0
v	-0,125	-5	0	0	-0,7812	-0,0312	0,0312	0	0	0	0
L	1	-32	-2	-2	-4	-1	-1	-1	-1	-1	-1

Modification leads to Table 12.

Table 12 – Modification of Table 11 *(Step 2)*

	FT	v	w2	w3	x0	w5	w6	w7	w8	w9	w10
w4	1,8	-6,4	0	-1	0	0,2	-0,2	0	0	0	0
x1	19,8	-6,4	0	0	0	0,2	-0,2	0	0	0	0
x2	22	0	0	0	0	1	-1	0	0	0	0
x3	15	0	0	0	0	0	0	1	-1	0	0
x4	20	0	0	0	0	0	0	0	0	1	-1
x5	31	0	0	0	1	0	0	0	0	0	0
x6	11,2	6,4	0	0	0	-0,2	0,2	0	0	0	0
x7	9	0	0	0	0	-1	1	0	0	0	0
x8	16	0	0	0	0	0	0	-1	1	0	0
x9	11	0	0	0	0	0	0	0	0	-1	1
y0	-0,025	0,2	0	0	-0,1562	-0,0062	0,0062	0	0	0	0
y1	3	-1	0	0	0	0	0	0	0	0	0
y2	3,5625	0	0	0	0	0,1562	-0,1562	-0,0312	0,0312	0	0
y3	2,3125	0	0	0	0	0	0	0,1562	-0,1562	-0,0312	0,0312
w1	0	0	-1	0	1	0	0	0	0	0	0
v	0,025	-0,2	0	0	0,1562	0,0062	-0,0062	0	0	0	0
L	1,8	-6,4	-2	-2	1	-0,8	-1,2	-1	-1	-1	-1

For disposal of impermissible plan is necessary to execute exchange – values $y0 \leftrightarrow x0$.

This transformation leads to plan which is presented in Table 13.

Table 13 contains permissible and optimum basic plan. Important point is possibility of removal of a line of a fictitious variable v in Table 13 during transition to next basic plan and its place will have used for record of new restriction. The basic plan, which was received in Table 13, is noted by top $G_2^{(2)}$ on a tree of decisions (Fig. 1) and corresponds to value of objective L = 1,96. This top corresponds to the smallest value of objective function among all available "hanging" tops. That's why this top and its Table 13 are chosen for further branching for achievement of integer of value $y2$.

Table 13 – Modification of Table 12 *(Step 2)*

	FT	v	w1	w3	y0	w5	w6	w7	w8	w9	w10
w4	1,8	-6,4	0	-1	0	0,2	-0,2	0	0	0	0
x1	19,8	-6,4	0	0	0	0,2	-0,2	0	0	0	0
x2	22	0	0	0	0	1	-1	0	0	0	0
x3	15	0	0	0	0	0	0	1	-1	0	0
x4	20	0	0	0	0	0	0	0	0	1	-1
x5	30,84	1,28	0	0	6,4	-0,04	0,04	0	0	0	0
x6	11,2	6,4	0	0	0	-0,2	0,2	0	0	0	0
x7	9	0	0	0	0	-1	1	0	0	0	0
x8	16	0	0	0	0	0	0	-1	1	0	0
x9	11	0	0	0	0	0	0	0	0	-1	1
x0	0,16	-1,28	0	0	-6,4	0,04	-0,04	0	0	0	0
y1	3	-1	0	0	0	0	0	0	0	0	0
y2	3,5625	0	0	0	0	0,1562	-0,1562	-0,0312	0,0312	0	0
y3	2,3125	0	0	0	0	0	0	0,1562	-0,1562	-0,0312	0,0312
w1	0,16	-1,28	-1	0	-6,4	0,04	-0,04	0	0	0	0
v											
L	1,96	-7,68	-2	-2	-6,4	-0,76	-1,24	-1	-1	-1	-1

Steps of the decision is repeated to achievement of integer of all elements of the FT column. At the same time perspective and final tops of a tree of decisions gradually are defined. From a step to a step quantity of final (not perspective and not subject to branching) tops begins to increase, and task quickly strives for the only optimum integer decision which corresponds to the smallest achievable value of objective function. Received value L corresponds to the minimum size of the sum of lengths of projections of a vector of hindrance Ξ. It allows of implement offered rule of decoding (SP). Full process of decoding for the reviewed example is illustrated by a tree in fig. 1. The top $G_1^{(4)}$ is final, which corresponds to the plan of the decision presented in Table 14, at the same time value of objective function is equal L = 7. Value of a variable determines the most probable (by MLE) the decoded code word.

Table 14 – Final table *(Step 4)*

	FT	v	w1	w3	y0	v	w6	v	w8	w9	w10
w4	1	0	0	0	0	1	0	0	0	0	0
x1	19	0	0	1	0	1	0	0	0	0	0
x2	18	32	0	5	0	5	0	0	0	0	0
x3	13	160	0	25	0	25	0	32	0	0	0
x4	20	0	0	0	0	0	0	0	0	1	-1
x5	31	0	0	-0,2	6,4	-0,2	0	0	0	0	0
x6	12	0	0	-1	0	-1	0	0	0	0	0
x7	13	-32	0	-5	0	-5	0	0	0	0	0
x8	18	-160	0	-25	0	-25	0	-32	0	0	0
x9	11	0	0	0	0	0	0	0	0	-1	1
x0	0	0	0	0,2	-6,4	0,2	0	0	0	0	0
y1	3	-1	0	0	0	0	0	0	0	0	0
y2	3	0	0	0	0	0	0	-1	0	0	0
y3	2	25	0	3,9062	0	3,9062	0	5	0	-0,0312	0,0312
w2	0	0	-1	0,2	-6,4	0,2	0	0	0	0	0
w5	4	-32	0	-5	0	-5	-1	0	0	0	0
w7	2	-160	0	-25	0	-25	0	-32	-1	0	0
L	7	-192	-2	-30,8	-6,4	-28,8	-2	-32	-2	-1	-1

On Fig. 2 for an example the tree of decisions received by decoding of PRC on the basis of the classical method of branches and borders which does not use priority at search of variables for achievement of integer values is shown. In the analysis of a tree of decisions is seen that the objective of decoding are achieved already at 4-th step, however process of branching continues to the 7th step that is caused by need of check of all "hanging" perspective tops and confirmations of correctness of decoding.

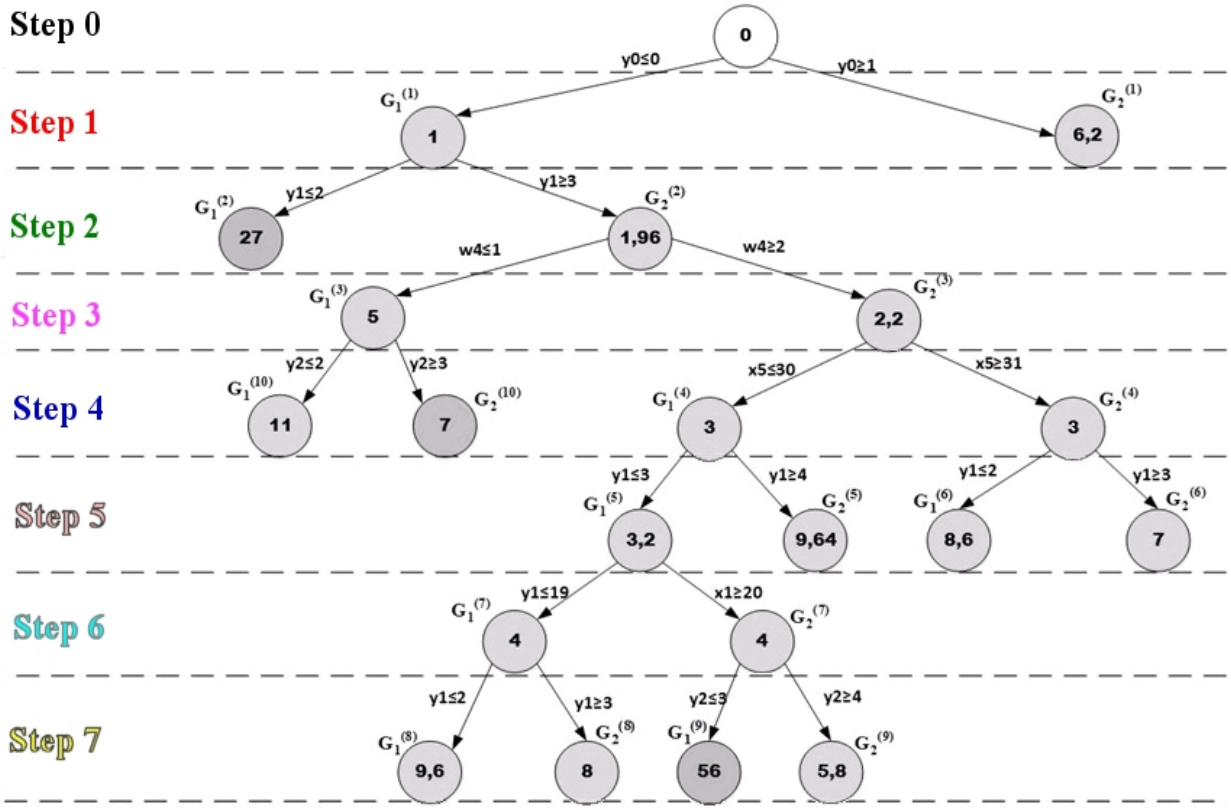


Fig. 2 – Tree of decisions for a classical method of branches and borders

Important result of use of the offered modified method of search of integer variables is that values of objective function in nodes of a tree are increased quicker (at increase of number of step of branching), unlike values by Fig. 2. It allows to conclude that computing complexity of method of decoding of PRC on the basis of the modified method of branches and borders significantly decreases by putting of a priority for achievement of integrality of the variables y performing function of linearization of operations of calculation of the module m. Approximate estimate of increment of computing efficiency in the reviewed example can be defined by simple calculation of the relation of quantity of nodes of trees of the decisions which are shown in Fig. 1 and Fig. 2: $21/11 \approx 1{,}91$.

4 Assessment of computing complexity of decoding of PRC

For confirmation of the fact of receiving a constructive method of decoding of PRC which has polynomial computing complexity is necessary to held comparison with method of simple search. For assessment of computing complexity of decoding of PRC by modified method of branches and borders uses the known result [5] where is described that чтоupper limit of quantity of tops of a tree of decisions for a classical algorithm amount:

$$S \approx N^5 \log_2 N, \qquad (17)$$

where N – effective value of quantity of unknown variables of a task.

The number of elementary operations (multiplication and addition) which are performed at modification one simplex of the table by size of $(3n-1)\cdot(2n)$ cells (as in the example reviewed above) problems of LP, using (17), it is possible to define total of elementary operations for solution of problem of decoding:

$$S=N^5 \log_2 N \cdot 2 \cdot (3n-1) \cdot (2n) \ . \tag{18}$$

It is known [6] that at the solution of problems of linear programming for obtaining of any permissible and optimum basic plan it is necessary to execute, approximately, no more N/2 iterations of recalculation of tables. Therefore final assessment of quantity of executed elementary operations constitutes:

$$\begin{aligned} S&=N^5 \log_2 N \cdot 2 \cdot (3n-1) \cdot (2n) \cdot \frac{N}{2} = \\ &= N^6 \log_2 N \cdot (3n-1) \cdot (2n). \end{aligned} \tag{19}$$

Total of variables of basis task in the starting table constitutes 3n-2, where n - length of block PRC. At branching of nodes of tree of decisions according to the modified method of branches and borders the priority is given to achievement of integer of variables y_i, $i \in [0,\ldots,n-2]$. Achievement of integrality of variables y_i, practically, guarantees achievement of the full solution of a task (*all variables will be integer*). At the same time the quickest approximation to decision is observed (*the decision is reached for smaller quantity of steps*).

Also, variables x and $\tilde{x}$ are a part of basic variables (Table 15). But appeal to lines of these variables at conditions of integrality are executed extremely seldom. For variables x restrictions only are formed in case the corresponding variable is outside the admissible range of values $[0\ldots m-1]$. The probability of this case on condition of uniform distribution of numbers, and an exception of a possibility of emergence in the code word of two identical numbers is equal $2/2^n$ – for variable x and $1/2^n$ – for variable $\tilde{x}$. The corresponding probabilistic weight coefficients which determine the weight of variables x, $\tilde{x}$, y and at calculation of effective quantity of variables N of problem of LP are presented in Table 15 .

Table 15 – Weight coefficients of variables

Quantity of variables	Name and range of placement	Weight coefficients
n	$x_i, i \in [0,\ldots,n-1]$	$2^{-(n-1)}$
n	$\tilde{x}_i, i \in [i,\ldots,2i-1]$	2^{-n}
n-1	$y_i, i \in [2i,\ldots,3i-2]$	1

Using of the weight coefficients presented in Table 15 allow to determine size of effective value of quantity of unknown variables of a task N:

$$N=(n-1)+n \cdot 2^{-n} + n \cdot 2^{-(n-1)}. \tag{20}$$

On the basis of expressions (19) and (20) computing complexity of a method of decoding of PRC on the basis of the modified method of branches and borders is estimated. Results of comparison of computing efficiency of developed decoding method with similar parameter of simple directional search of the decision at decoding of PRC are presented in Fig. 3.

As appears from the dependences presented in Fig. 3 with growth of length of the block computing complexity of directional search of the decision algorithm of decoding grows exponential, and using of the offered decoding method computing complexity grows to polynomial law. With lengths of PRC blocks $n \geq 37$ is reached advantage of offered decoding method on computing complexity comparison with directional search of the decision. For example, with a block length PRC

n = 50 advantage is equal almost 1000, and n = 60 – approximately by 10^6 times. It is confirmation of achievement of the object of this work.

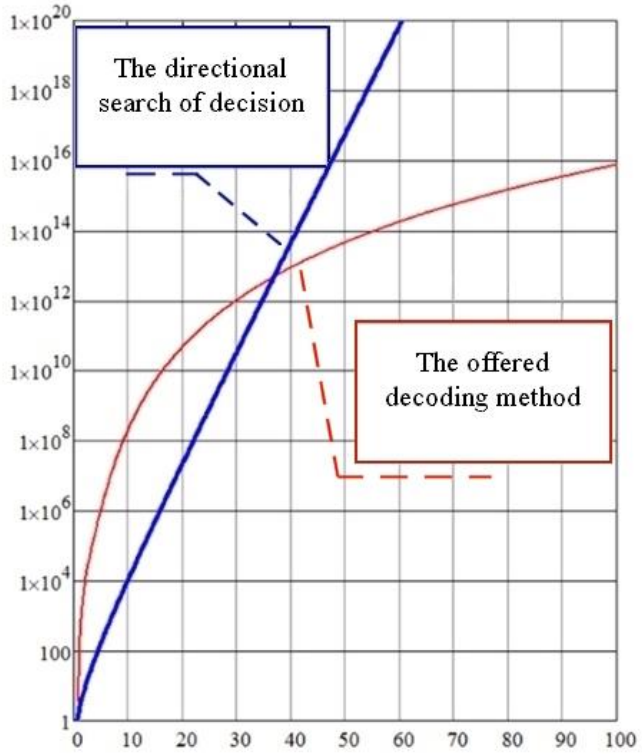


Fig. 3 – Comparison of computational complexity

5 Conclusions

The main result of this article consists in receiving a constructive method of construction and decoding of the LKG pseudorandom codes on the basis of the offered modified mathematical method of branches and borders. The possibility of representation of a problem of decoding in the form of tasks of integer linear programming due to insignificant decrease in objectivity of the rule of definition of the next code word is proved. This result disproves the settled stereotypes concerning a possibility of decoding of random and pseudorandom codes by exclusively methods of directional search of the decision on the basis of the rule of maximum like hood. The offered rule of the smallest projections of different vectors is a basis for linearization of objective function of the decoder. Decrease in objectivity of decoding is compensated by increase of lengths of PRC blocks.

The most acceptable method for the solution of an integer problem of decoding of PRC is the mathematical method of the directed search of the optimal solution – a method of branches and granits. The instrument of linearization of objective function is replacement of nonlinear operation of calculation of the module on its algebraic equivalent. Using of this replacement in the equations of recurrent interrelation of symbols of code words allows to formalize a problem of decoding in the form of an initial problem of integer linear programming.

Modification of a classical method of branches and borders by introduction of a priority of search of integer variables of a task in nodes of branching of a tree of decisions, allows to reduce several times quantity of the steps necessary for obtaining the optimal integer solution of a problem of decoding.

The complex consideration of the main problematic issues connected with creation and processing of pseudorandom codes and also the received strict mathematical solution of a problem of decoding PRC which have done in this work allow to make the reasonable assumption of a possibility of practical realization of PRC technologies in perspective systems of information transfer.

References

[1] Shannon C. E. A Mathematical Theory of Communication / C. E. Shannon // Bell Syst. Tech. J. – 1948. – Vol. 27. – P. 379–423, 623–656. (In English)
[2] Shannon C. E. Communication in the presence of noise / Shannon C. E. // Proc. IRE. – 1949. – Vol. 37. – P. 10 – 21. (In English)
[3] Lavrovskaya T.V. Matematicheskie modeli sluchaynyih i psevdosluchaynyih kodov // T.V. Lavrovskaya, S.G. Rassomahin // Sistemi obrobki Informatsiyi. – 2016. – Vip.9 (146). – S. 55-61. (In Russian)
[4] Lavrovskaya T.V. Fizicheskaya model psevdosluchaynyih kodov v mnogomernom Evklidovom prostranstve / T.V. Lavrovskaya, S.G. Rassomahin // Sistemi Ozbroennya i Viyskova Tehnika. – 2016. – Vip. 3 (47). – S. 79-84. (In Russian)
[5] Nazaryants E.G. Polinomialnaya slozhnost parallelnoy formyi metoda vetvey i granits resheniya zadachi kommivoyazhera // Ya.E. Romm, E.G. Nazaryants // Izvestiya Yuzhnogo federalnogo universiteta. Tehnicheskie nauki. – 2015. – Vip.4 (165). – S. 44. (In Russian)
[6] Akulich I.L. Matematicheskoe programmirovanie v primerah i zadachah: ucheb. posobie dlya studentov ekonom. spets. vuzov / I. L. Akulich – Moskva: Vyissh. Shkola. – 1986. – 319 s. (In Russian)

Рецензент: Віктор Краснобаєв, д.т.н., проф., Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
E-mail: krasnobayev@karazin.ua

Надійшло: Листопад 2016.

Автори:
Таміла Лавровська, аспірантка, Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
E-mail: lavrovska92@gmail.com
Сергій Рассомахін, д.т.н., проф., Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
E-mail: rassomakhin@karazin.ua

Метод декодування псевдовипадкових кодів на основі модифікованого методу гілок і меж.

Анотація: Розглянуто причини кризи завадостійкого кодування. Підкреслюється актуальність застосування псевдовипадкових кодів в сучасних системах передачі інформації. Наведено конструктивний математичний метод декодування псевдовипадкових кодів на основі використання методу гілок і меж. Запропонована модифікація класичного алгоритму гілок і меж. Проведена оцінка обчислювальної складності методів декодування псевдо-випадкових кодів на основі класичного та модифікованого алгоритму гілок і меж, а також оцінка обчислювальної складності запропонованого методу у порівнянні з перебірним алгоритмом. Розроблена програмна реалізація метода декодування псевдовипадкових кодів.

Ключові слова: псевдовипадковий код, метод гілок і меж, обчислювальна складність, завадостійке кодування.

Рецензент: Виктор Краснобаев, д.т.н., проф., Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина.
E-mail: krasnobayev@karazin.ua

Поступила: Ноябрь 2016.

Авторы:
Тамила Лавровская, аспирантка, Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина.
E-mail: lavrovska92@gmail.com
Сергей Рассомахин, д.т.н., проф., Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина.
E-mail: rassomakhin@karazin.ua

Метод декодирования псевдослучайных кодов на основе модифицированного метода ветвей и границ.

Аннотация: Рассмотрены причины кризиса помехоустойчивого кодирования. Подчеркивается актуальность применения псевдослучайных кодов в современных системах передачи информации. Представлен конструктивный математический метод декодирования псевдослучайных кодов на основе использования метода ветвей и границ. Предложена модификация классического алгоритма ветвей и границ. Проведена оценка вычислительной сложности методов декодирования псевдослучайных кодов на основе классического и модифицированного алгоритма ветвей и границ, а также оценка вычислительной сложности предложенного метода по сравнению с переборным алгоритмом. Разработана программная реализация метода декодирования псевдослучайных кодов.

Ключевые слова: псевдослучайный код, метод ветвей и границ, вычислительная сложность, помехоустойчивое кодирование.

UDC 621.391

RESEARCH ALGORITHM OF HIDE THE SPEECH MESSAGING BASED ON THE SPREAD SPECTRUM METHOD

P. Likholob, A. Bukhantsov, A. Vodounou, Ya. Baka

Belgorod State National Research University, Belgorod, Russia
Likholob@bsu.edu.ru, Bukhantsov@bsu.edu.ru, Aaron.Vodounou@gmail.com, BakaYana@mail.ru

Reviewer: Alexandr Kuznetsov Dr., Full Professor, V.N. Karazin Kharkiv National University, Svobody sq., 4, Kharkov, 61022, Ukraine
kuznetsov@karazin.ua

Received on January 2017

***Resume**: In the work the approach, which makes it possible to modify the method of expanding the spectrum for the realization of the reserved coding of voice communication in vocal data, is proposed. The results of investigating the dependence of different estimations on the values of the assigned parameters are represented. The development algorithm can make it possible to increase the effectiveness of the reserved exchange of voice communications, due to the more effective use of reticence and capacity of vocal material. The use of the orthonormalized basis instead of pseudorandom sequence, allows more effectively from the position of the volume of the coded information to use vocal material for the reserved transfer of communication.*

***Key words:** speech signals, steganography, spread spectrum, measures the differences, the correlation coefficient, the mean square error, relative error, the signal-to-noise ratio.*

1 Introduction

For the large commercial and corporate structures, there is a need for accomplishing the protected exchange of the data by those presenting commercial secret. The use of methods steganography of the concealment of the fact of the transmission of information makes it possible to carry out not only protection of business data, but also in particular, it makes it possible to hide the indirect signs of the fact of the realization of negotiations. Most frequently for the transfer of the informational announcements that not containing the numbers is used spoken language. The use of a spoken language as the means of communication is caused, so by simplicity of its perception by man. Further voice communication, the secretly transferred information, registered in the form of the voice signal, and converted into the digital form.

It is worthwhile to note that the often information resources for the reserved transfer of voice communications, by the methods of cryptography are limited. This is caused by the fact that for the concealment of protected voice communication it is necessary to use the data, whose volume several times must exceed the volume of the protected vocal. Therefore, a quantity of methods and algorithms, which it is possible to use for, purposes the reserved transfer of voice communications not great. The development of method and algorithm of those realizing the principles of the reserved transfer of voice communication in vocal data, can make it possible to increase the effectiveness of the reserved exchange of voice communications, due to the more effective use of reticence and capacity of vocal material. By effectiveness in the work is understood, the use of an approach for coding of voice communication with the guarantee of its reticence, which makes it possible to increase the volume of transferred voice communications without the need for an increase in the volume of vocal material. Cryptography of those making it possible to accomplish a reserved transfer of voice communication in vocal data are widely known several methods. To the bases, the method of the least significant bit (LSB) and method of expanding the spectrum (SSp) carry [1,3,6]. Its durability is the main disadvantage in the method of LSB; therefore, wide application obtained the method of expanding spectrum [6]. The essence of method consists in the addition to the section of the initial voice signal of pseudorandom sequence in accordance with the expression [5,7,8]:

$$\vec{y} = \vec{x} + \alpha \cdot e \cdot \vec{u}\ ; \qquad (1)$$

where $\vec{x}$ – the initial section of vocal data; $\vec{u}$ – the section, which corresponds to pseudorandom sequence; α – weight coefficient; e – the code mapping of the binary bit of hidden voice communication, determined from the formula:

$$e = 2\mathrm{e} - 1,\ m = 1,\ldots,M; \tag{2}$$

where e_m – bit of control information in the binary number system $\mathrm{e}_m \in \{0,1\}$; e_m – the code mapping of the binary bit of control information $e_m \in \{-1,1\}$; m – the ordinal number of the bit of control information is m-th. The weight coefficient of αm determines the reticence of system. In the works [9, 10] it's proposed to select equal:

$$\alpha = \langle \vec{x}, \vec{u} \rangle / \|\vec{u}\|^2. \tag{3}$$

The decoding of the bit of control information from the data occurs by determining the sign of the scalar product of the section of the data and of the pseudorandom sequence:

$$\tilde{e} = sign(\langle \vec{y}, \vec{u} \rangle); \tag{4}$$

where $sign(\ )$ – the operation of the isolation of sign.

The use of a large volume of vocal data for the transfer of short voice communication is a drawback in approach described above. This is caused by the fact that in one section of the data coding the one-bit of protected voice communication is possible. With the frequency of discreteness of 48Gts, it is possible to reach the capacity of vocal data of 92 bytes/s. For increasing the capacitance, it is proposed in one section of vocal data to code 4 bytes of information, i.e. to reach the capacity of 3000 bytes/s.

2 Proposed method

Model of the reserved coding:

$$\vec{y}_i = \vec{x}_i + \lambda \cdot w_i \cdot \vec{u}_i - b \cdot \alpha_i \cdot \vec{u}_i,\ i = 1,..,J; \tag{5}$$

where $\vec{x}_i$ – initial section (vocal material); $\vec{y}_i$ – section containing the coded information by steganography (Filled container); α_i – the constant of proportionality, which determines mutual energy pseudorandom sequence and initial section; λ – coefficient determining reticence and the durability of the coded information by steganography; w_i – the secretly coded byte of voice communication; $\vec{u}_i$ – function from the orthogonal basis of Radamacher, illustrated by Fig. 1; M – it corresponds to a quantity of utilized functions.

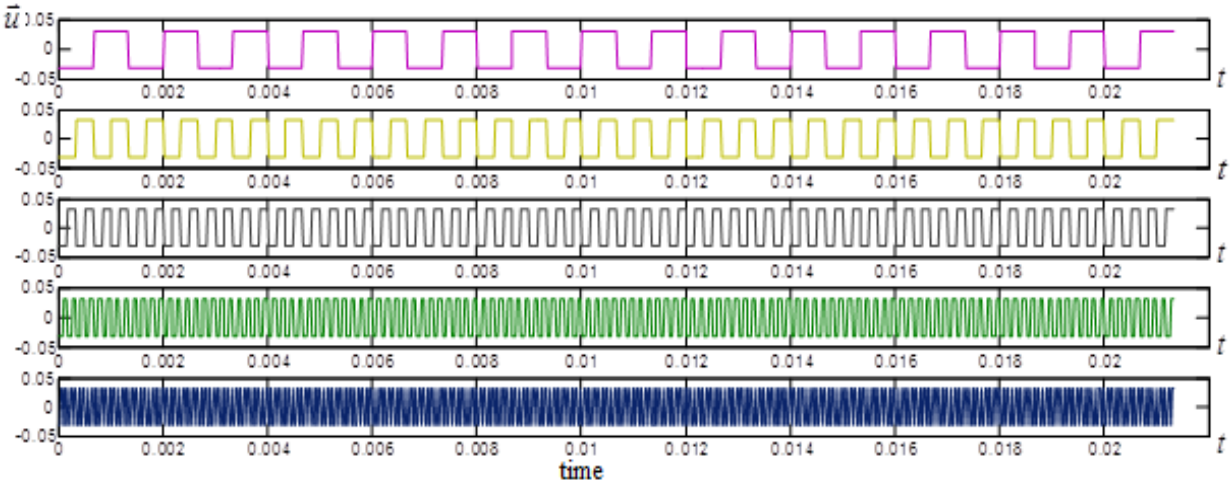


Fig. 1 – Plot of orthogonal basis Rademacher

The decoding of information from filled container occurs, by means of the scalar product of the section of vocal data containing voice communication and corresponding function of the utilized orthogonal basis:

$$\tilde{w}_i = \langle \vec{y}, \vec{u}_i \rangle, \; i = 1,..,J; \tag{6}$$

where $\tilde{w}_i$ – the decoded from the section of voice signal byte of voice communication.

3 Experimental results

For investigating the sensitivity of the measures of the quality of the concealment of information examined, were carried out computational experiments with the use of different sounds of Russian speech. In Fig. 2,3 are represented the sections of the voice signals, which correspond to some sounds of Russian speech, and distribution of their energy on the frequency intervals.

The use of a large volume of vocal data for the transfer of short voice communication is a drawback in approach described above. This is caused by the fact that in one section of the data coding the one-bit of protected voice communication is possible. With the frequency of discreteness of 48Gts, it is possible to reach the capacity of vocal data of 92 bytes/s. For increasing the capacitance, it is proposed in one section of vocal data to code 4 bytes of information, i.e. to reach the capacity of 3000 bytes/s.

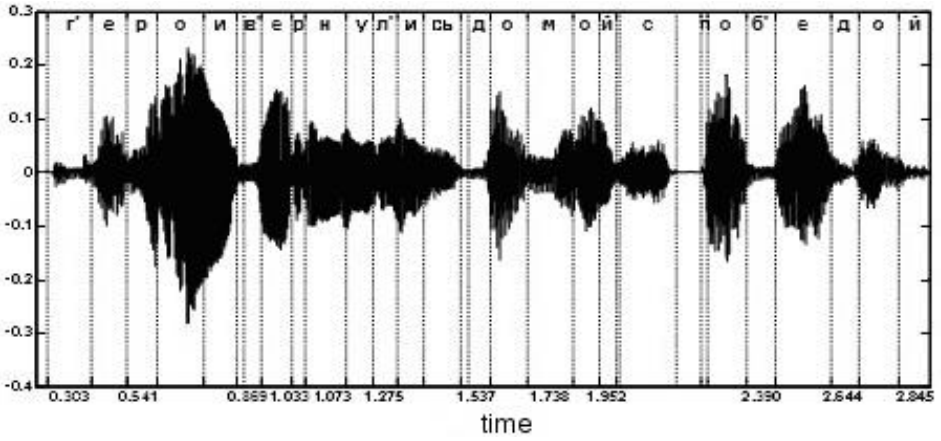


Fig. 2 – An example of digital the original content

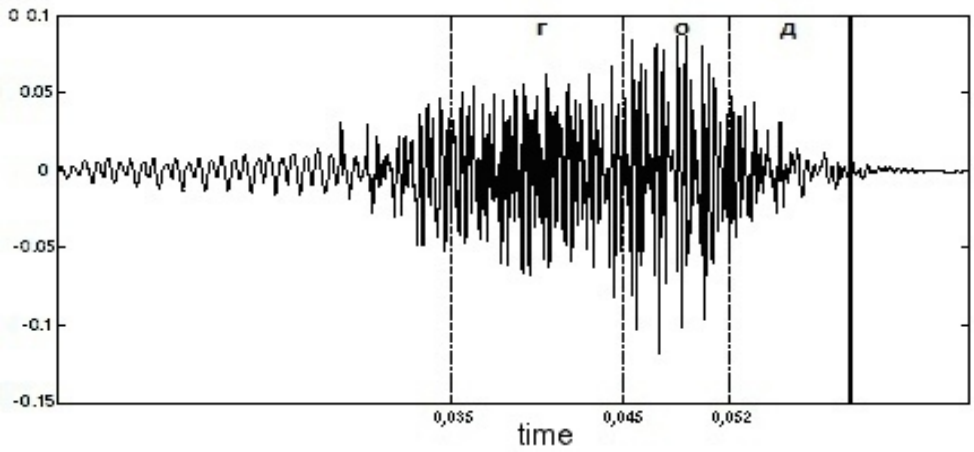


Fig. 3 – An example of hide digital speech audio

In the work are used such estimations of difference as relative error (NSKO), signal to noise ratio (SNR), correlation coefficient (R). Each of these estimations makes it possible to reveal differences in the compared signals [6,7]. In particular, relative error (NSKO) reflects a difference in energy of the sections of signals in the time domain referred to the standard of the initial signal:

$$NSKO = \sum_{n=1}^{N} (x_n - \tilde{x}_n)^2 \Big/ \sum_{n=1}^{N} x_n^{\,2}; \quad (7)$$

where x_n – the value of the amplitude of the initial section of the data; $\tilde{x}_n$ – the value of the amplitude of the section of the data containing additional information, N – quantity of counting of the compared sections of signals.

This measure makes it possible to reveal differences in the envelopes of the amplitudes of the sections of voice signals. The less the changes introduced with the introduction of additional information, the nearer the value of this estimation to zero [1,8,10].

Also to account for the degree of a difference in the initial signal and result of introducing the additional information is used the estimation, sensitive to the time of the recovery of the compared sections of the signals:

$$SNR = 10 \cdot \lg \frac{\sum_{n=1}^{N} x_n^{\,2}}{\sum_{n=1}^{N} (x_n - \tilde{x}_n)^2}; \quad (8)$$

The higher the estimation SNR, the less the changes was introduced. In the case of the equality of two sections (initial and subjected to changes during the coding); the estimation will be equal to infinity (∞). For the evaluation of the degree of the similarity of two sections of the data, frequently is used the evaluation of mutual energy of these signals, determined by correlation coefficient:

$$R = \frac{\sum_{n=1}^{N} \left(x_n - \frac{1}{N} \sum_{n=1}^{N} x_n \right) \cdot \left(\tilde{x}_n - \frac{1}{N} \sum_{n=1}^{N} \tilde{x}_n \right)}{\sqrt{\sum_{n=1}^{N} \left(x_n - \frac{1}{N} \sum_{n=1}^{N} x_n \right)^2 \cdot \left(\tilde{x}_n - \frac{1}{N} \sum_{n=1}^{N} \tilde{x}_n \right)^2}}; \quad (9)$$

The nearer correlation value to one, the higher the similarity of the section of the data containing control information and initial.

Table 1 presents the results of evaluating the measures of difference for all sounds of Russian speech examined. In this case for the analysis the sections of the voice signals, recorded with the frequency of discreteness 8 kHz and code length of 16 bits, were used. For the application of the method of expanding the spectrum voice signals were divided in the sections of identical duration on T=32ms. It is important also to note that the study of the measures in question was accomplished in the implementation of the imposition of noise on the signal in the absence of cross-correlation and use of a weight coefficient of the form:

Table 1 – Evaluation of the differences of the original signal and implementation results using steganographic technique spreading

№		Estimation of reticence PC			Estimation extracted PC		
	b	NSKO	SNR	R	NSKO	SNR	R
1	0	0.1×10^{-6}	69.52	0.9989	171.4	-44.66	0.0107
2	0.5	0.1014	24.19	0.9332	42.76	-32.62	0.0431
3	0.98	0,3825	12,82	0,7158	0.0684	23.29	0.9669
4	0.99	0.3903	12.65	0.7100	0.0171	35.33	0.9915
5	1	0.3981	12.48	0.7043	≈ 0	∞	1

4 Conclusions

The use of the orthonormalized basis instead of pseudorandom sequence, allows more effectively from the position of the volume of the coded information to use vocal material for the reserved transfer of communication. Steganographic coding has a number of stages. The first includes coding

in the orthonormal basis. The second accomplishes adaptive filtration, so that the decoding of communication would possess higher authenticity and it was not subjected to distortions. The third stage is direct coding with the adaptive coefficient. As showed experiments, reticence can be ensured due to the use as the coefficients of those reflecting the value of energy of initial section.

References

[1] Gribunin V.G. Digital steganography. Protection Aspects / V.G. Gribunin, I.N. Wintergrasp, I.V. Turintsev. – Moscow: Solon-Press, 2002. – 261 p.
[2] Zharkikh A.A. The method of steganography based on the direct spread spectrum signal / A.A. Hot, A.V. Gurin, V.Y. Plast // Proceedings of the VII International Scientific and Technical Conference INTERMATIC, 7 – 11 December 2009. Part 4. – Moscow: MIREA, 2009. – P. 78–83.
[3] Zhilyakov E.G. On the Steganography in Voice Data / E.G. Zhilyakov et al. // Asian J. Inf. Technol. – 2016. – Vol. 15. – № 12. – P. 1949–1952.
[4] Konahovich G.F. Computer steganography. Theory and practice / G.F. Konahovich, A.Y. Puzyrenko. – Kiev: MK – Press, 2006. – 288 p.
[5] Fridrich J. Steganography in digital media: Principles, algorithms, and applications / Jessica Fridrich. – Cambridge University Press, 2012. – 441 p.
[6] Furui S. Digital Speech Processing, Synthesis, and Recognition / Sadaoki Furui. – Marcel Dekker, 2001. – 477 p.
[7] Cvejic N. Spread spectrum audio watermarking using frequency hopping and attack characterization / Nedeljko Cvejic, Tapio Seppanen// Signal Processing. – 2004. – Vol. 84. – №11. – P. 207 – 213.
[8] Stanković S. Multimedia signals and systems / S. Stanković, I. Orović, E. Sejdić. – Springer, 2012. – 373 p.
[9] Thierry Dutoit, Ferran Marques. Applied Signal Processing A MATLAB ™- Based Proof of Concept. – Springer, 2009. – 456 p.
[10] Vercoe B.L. Csound: A Manual for the Audio-Processing System / Barry L. Vercoe. – Cambridge: MIT Media Lab, 1995.

Рецензент: Олександр Кузнецов, д.т.н., проф., Харківський національний університет імені В. Н. Каразіна, Харків, Україна. E-mail: kuznetsov@karazin.ua

Надійшло: Січень 2017.

Автори:
Петро Ліхолоб, ст. викладач, кафедра інформаційно-телекомунікаційних систем і технологій, федеральна державна автономна освітня установа вищої освіти «Білгородський державний національний дослідницький університет» (НДУ «БелГУ»), Білгород, Росія.
E-mail: Likholob@bsu.edu.ru

Андрій Буханцов, к.т.н., доцент, кафедра інформаційно-телекомунікаційних систем і технологій, федеральна державна автономна освітня установа вищої освіти «Білгородський державний національний дослідницький університет» (НДУ «БелГУ»), Білгород, Росія.
E-mail: Bukhantsov@bsu.edu.ru

Аарон Водуну, студент, каф. інформаційно-телекомунікаційних систем і технологій, федеральна державна автономна освітня установа вищої освіти «Білгородський державний національний дослідницький університет» (НДУ «БелГУ»), Білгород, Росія.
E-mail: Aaron.Vodounou@gmail.com

Яна Бака, студент, каф. інформаційно-телекомунікаційних систем і технологій, федеральна державна автономна освітня установа вищої освіти «Білгородський державний національний дослідницький університет» (НДУ «БелГУ»), Білгород, Росія.
E-mail: BakaYana@mail.ru

Дослідження алгоритму прихованої передачі мовного повідомлення заснованого на методі розширення спектра.

Анотація. В роботі запропонований підхід, що дозволяє модифікувати метод розширення спектра для здійснення таємного кодування мовного повідомлення в речових даних. Представлені результати дослідження залежності різних оцінок від значень параметрів, що задаються. Розроблений алгоритм дозволяє підвищити оперативність таємного обміну мовними повідомленнями за рахунок більш ефективного використання скритності і таємності мовного матеріалу. Використання ортонормованого базису замість ПСП дозволяє більш ефективно, з позиції обсягу кодованої інформації, використовувати мовний матеріал для прихованої передачі повідомлення.

Ключові слова: мовні сигнали, стеганографія, метод розширення спектра, заходи відмінності, коефіцієнт кореляції, середньоквадратична помилка, відношення сигнал-шум.

Рецензент: Александр Кузнецов, д.т.н., проф., Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина. E-mail: kuznetsov@karazin.ua

Поступила: Январь 2017.

Авторы:

Петр Лихолоб, ст. преподаватель, каф. информационно-телекоммуникационных систем и технологий, федеральное государственное автономное образовательное учреждение высшего образования «Белгородский государственный национальный исследовательский университет» (НИУ «БелГУ»), Белгород, Россия.
E-mail: Likholob@bsu.edu.ru

Андрей Буханцов, к.т.н., доцент, каф. информационно-телекоммуникационных систем и технологий, федеральное государственное автономное образовательное учреждение высшего образования «Белгородский государственный национальный исследовательский университет» (НИУ «БелГУ»), Белгород, Россия.
E-mail: Bukhantsov@bsu.edu.ru

Аарон Водуну, студент, каф. информационно-телекоммуникационных систем и технологий, федеральное государственное автономное образовательное учреждение высшего образования «Белгородский государственный национальный исследовательский университет» (НИУ «БелГУ»), Белгород, Россия.
E-mail: Aaron.Vodounou@gmail.com

Яна Бака, студент, каф. информационно-телекоммуникационных систем и технологий, федеральное государственное автономное образовательное учреждение высшего образования «Белгородский государственный национальный исследовательский университет» (НИУ «БелГУ»), Белгород, Россия.
E-mail: BakaYana@mail.ru

Исследование алгоритма скрытной передачи речевого сообщения, основанного на методе расширения спектра.

Аннотация. В работе предложен подход, позволяющий модифицировать метод расширения спектра для осуществления скрытного кодирования речевого сообщения в речевых данных. Представлены результаты исследования зависимости различных оценок от значений задаваемых параметров. Разработанный алгоритм позволяет повысить оперативность скрытного обмена речевыми сообщениями за счет более эффективного использования скрытности и емкости речевого материала. Использование ортонормированного базиса вместо ПСП позволяет более эффективно, с позиции объема кодируемой информации, использовать речевой материал для скрытной передачи сообщения.

Ключевые слова: речевые сигналы, стеганография, метод расширения спектра, меры различия, коэффициент корреляции, среднеквадратическая ошибка, относительная погрешность, отношение сигнал-шум.

УДК 681.142

МЕТОД КОНТРОЛЯ ДАННЫХ В СИСТЕМЕ ОСТАТОЧНЫХ КЛАССОВ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ ПОЗИЦИОННОГО ПРИЗНАКА НЕПОЗИЦИОННОЙ КОДОВОЙ СТРУКТУРЫ

Виктор Краснобаев[1], Сергей Кошман[2], Алина Янко[3]

[1] Харьковский национальный университет имени В.Н. Каразина, пл. Свободы, 4, г. Харьков, 61022, Украина
krasnobayev@karazin.ua

[2]Харьковский национальный технический университет сельского хозяйства имени Петра Василенка, ул. Алчевских, 44, г. Харьков, 61002, Украина
s_koshman@ukr.net

[3]Полтавский национальный технический университет имени Юрия Кондратюка, пр. Первомайский, 24, г. Полтава, 36011, Украина
al9_yanko@ukr.net

Рецензент: Сергей Кавун, доктор экономических наук, к.т.н., проф., Харьковский институт банковского дела УБД НБУ, пр. Победы, 55, г. Харьков, 61174, Украина.
kavserg@gmail.com

Поступила в январе 2017

Аннотация. *В статье разрабатывается метод контроля данных в системе остаточных классов (СОК), который основан на использовании позиционного признака непозиционной кодовой структуры. Рассмотрены варианты применения предложенного метода контроля данных в СОК, а также примеры конкретного выполнения операции контроля данных в СОК. Приведены данные сравнительного анализа количества оборудования системы контроля в зависимости от величины разрядной сетки компьютерной системы.*

Ключевые слова: *система остаточных классов, достоверность контроля данных, система передачи и обработки данных, позиционный признак непозиционного кода, непозиционная кодовая структура*.

1 Введение

Известно [1], что значительное время контроля данных снижает общую эффективность применения непозиционных кодовых структур (НКС) в системе остаточных классов (СОК), при реализации целочисленных арифметических модульных операций. Существующие методы оперативного контроля компонентов компьютерной системы обработки целочисленных данных (ККС) позволяют существенно снизить время контроля, однако при этом возникла задача повышения достоверности этого контроля [2-4]. Таким образом, актуальны исследования, посвященные решению задача повышения достоверности контроля данных в СОК. Цель статьи – разработка метода повышения достоверности контроля данных в ККС, функционирующей в СОК.

2 Основная часть

Известный метод оперативного контроля данных в СОК основан на получении и использовании так называемого позиционного признака непозиционного кода (ППНК). Данный ППНК является одной из характеристик контролируемой НКС $A=(a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n, a_{n+1})$, представленной в СОК основаниями $\{m_i\}$, $(i=\overline{1,n+1})$, с одним контрольным a_{n+1} остатком по контрольному основанию (модулю) m_{n+1}, при этом $M=\prod_{i=1}^{n} m_i$; $M_0=\prod_{i=1}^{n+1} m_i$. Контроль НКС вида $A=(a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n, a_{n+1})$ осуществляется на основе использования ППНК, который в свою очередь определяется на основе специального кода (СК). В общем виде структура СК

$$K_N^{(n_A)} = \left\{ Z_{N-1}^{(A)}\ Z_{N-1}^{(A)} \dots Z_1^{(A)}\ Z_0^{(A)} \right\} \tag{1}$$

представляет собой последовательность двоичных $Z_K^{(A)}$ $(K = \overline{0, N-1})$ разрядов, состоящую из единиц и только одного нуля, находящегося на n_A –м месте (считая справа, от разряда $Z_0^{(A)}$, налево, до разряда $Z_{N-1}^{(A)}$). Параметр n_A является ППНК непозиционной кодовой структуры $A = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, \dots, a_n, a_{n+1})$ данных, представленных в СОК. Математически параметр n_A представляет собой натуральное число, которое определяет местоположение нулевого двоичного разряда $Z_{n_A}^{(A)} = 0$ в записи СК $K_N^{(n_A)}$. Он определяет номер j_i числового $[j_i \cdot m_i,\ (j_i + 1) \cdot m_i)$ интервала нахождения числа A, т.е. значение n_A с определенной W точностью, которая зависит от значения величины модуля m_i СОК, определяет местоположение числа $A = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, \dots, a_n, a_{n+1})$ на числовой оси $0 \div M_0$. Рассмотрим, процедуру формирования СК $K_N^{(n_A)}$. Для выбранного основания m_i СОК (*правила выбора основания m_i СОК будет изложено ниже*) по значению остатка a_i числа $A = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, \dots, a_n, a_{n+1})$ в блоке констант нулевизации (БКН) ККС определяется константа вида $KH_{m_i}^{(A)} = \left(a_1^{'}, a_2^{'} ..., a_{i-1}^{'}, a_i, a_{i+1}^{'}, ..., a_{n+1}^{'} \right)$. Далее, посредством выбранной константы $KH_{m_i}^{(A)}$ нулевизации осуществляется операция вычитания

$$A_{m_i} = A - KH_{m_i}^{(A)} = \left(a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n, a_{n+1}\right) - \left(a_1^{'},\ a_2^{'},\ ...,\ a_{i-1}^{'},\ a_i,\ a_{i+1}^{'},\ ...,a_n^{'}, a_{n+1}^{'}\right) =$$

$$= \left[a_1^{(1)},\ a_2^{(1)},\ ...,\ a_{i-1}^{(1)},\ 0,\ a_{i+1}^{(1)},\ ..., a_n^{(1)}, a_{n+1}^{(1)} \right].$$

Эта операция соответствует процессу смещению контролируемого числа $A = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, \dots, a_n, a_{n+1})$ на левый край интервала $[j_i \cdot m_i,\ (j_i + 1) \cdot m_i)$ его первоначального (исходного) нахождения. В этом случае $A_{m_i} = j_i \cdot m_i$, т.е. число A_{m_i} кратно значению модуля m_i СОК. Известно, что правильность числа A в СОК определяется его нахождением или нет в числовом информационном $[0, M)$ интервале. Если число A находится вне этого интервала $(A \geq M)$, то оно считается искаженным (неправильным). В этом случае по значению n_A необходимо произвести контроль правильности или нет исходного числа A путем определения факта попадания или непопадания исходного числа A в интервал $[0, M)$. Чтобы определить факт нахождения числа в информационном $[0, M)$ числовом интервале необходимо провести совокупность операций вида

$$A_{m_i} - K_A \cdot m_i = Z_{K_A}^{(A)}. \tag{2}$$

Операции (2) проводиться одновременно и параллельно во времени посредством совокупности из N констант $K_A \cdot m_i$ вида $\left(K_A = \overline{0, N-1}\right)$:

$$\begin{cases} A_{m_i} - 0 \cdot m_i = Z_0^{(A)}, \\ A_{m_i} - 1 \cdot m_i = Z_1^{(A)}, \\ A_{m_i} - 2 \cdot m_i = Z_2^{(A)}, \\ \quad \dots \\ A_{m_i} - (N_i - 2) \cdot m_i = Z_{N-2}^{(A)}, \\ A_{m_i} - (N_i - 1) \cdot m_i = Z_{N-1}^{(A)}, \end{cases} \tag{3}$$

где $N_i = \prod_{\substack{K=1;\\ K\neq i.}}^{n+1} m_K$.

В этом случае СК представится в виде (1), а метод формирования ППНК n_A в СОК представлен на рис. 1.

1	Выбор информационных $\{m_i\}$, $i=\overline{1,n}$, и контрольного $m_K = m_{n+1}(m_i < m_{i+1})$ оснований для представления данных $A=(a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n, a_{n+1})$ в СОК. НОД $(m_i, m_j)=1$, $i \neq j$.
2	Выбор основания $m_i \in \{m_j\}$, $(j=\overline{1,n+1})$ по которому определяется номер j_i числового интервала, $[j_i \cdot m_i,\ (j_i+1)\cdot m_i)$ в котором находится число $A=(a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n, a_{n+1})$.
3	Определение по значению остатка a_i числа $A=(a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n, a_{n+1})$ константы нулевизации вида $KH_{m_i}^{(A)} = (a_1', a_2', ..., a_{i-1}', a_i, a_{i+1}', ..., a_n', a_{n+1}')$.
4	Определение значения $j_i \cdot m_i = A_{m_i} = A - KH_{m_i}^{(A)} = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n, a_{n+1}) - (a_1', a_2', ..., a_{i-1}', a_i, a_{i+1}', ..., a_n, a_{n+1}) = [a_1^{(1)},\ a_2^{(1)},\ ...,\ a_{i-1}^{(1)}, 0, a_{i+1}^{(1)}, ..., a_n^{(1)}, a_{n+1}^{(1)}]$.
5	Определение СК $K_N^{(n_A)} = \{Z_{N-1}^{(A)}\ Z_{N-2}^{(A)} \dots Z_0^{(A)}\}$ в виде $K_{N_i}^{(n_A)} = \{Z_{N_i-1}^{(A)}\ Z_{N_i-2}^{(A)} \dots Z_0^{(A)}\}$. $N = \prod_{\substack{K=1;\\ K\neq i.}}^{n+1} m_K$, $N_i =]M / m_i[$, $M = \prod_{i=1}^{n} m_i$. $A_{m_i} - K_A \cdot m_i = Z_{K_A}^{(A)}$. $\begin{cases} A_{m_i} - 0\cdot m_i = Z_0^{(A)}, \\ A_{m_i} - 1\cdot m_i = Z_1^{(A)}, \\ \quad \dots \\ A_{m_i} - (N-2)\cdot m_i = Z_{N-2}^{(A)}, \\ A_{m_i} - (N-1)\cdot m_i = Z_{N-1}^{(A)}. \end{cases}$
6	Определение ППНК числа $A=(a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n, a_{n+1})$, т.е. определение числового значения n_A для которого $Z_{K_A}^{(A)} = Z_{n_A}^{(A)} = 0$, т.е. $A_{m_i} - n_A \cdot m_i = 0$. При этом $Z_l^{(A)} = 1$, $(A_{m_i} - l\cdot m_i \neq 0;\ \ l \neq n_A)$.

Рис. 1 – Метод формирования ППНК в СОК

В совокупности (3) аналитических соотношений существует единственное значение n_A из (2) для которого $Z_{K_A}^{(A)} = Z_{n_A}^{(A)} = 0$ $(K_A = n_A)$, т.е. $A_{m_i} - n_A \cdot m_i = 0$. Остальные значения (2) равны $Z_l^{(A)} = 1$ $(A_{m_i} - l\cdot m_i \neq 0;\ l \neq n_A)$. В общем случае количество двоичных разрядов в

записи СК $K_N^{(n_A)}$ равно значению N. Однако отметим, что для определения только факта искажения числа A нет необходимости иметь и анализировать всю последовательность из N совокупности значений $Z_{K_A}^{(A)}$ СК $K_N^{(n_A)}$. Для этого достаточно иметь СК $K_{N_i}^{(n_A)}$ длиною всего $N_i =]M / m_i[$ двоичных разрядов (где значение $]M/m_i[$ обозначает целую часть числа M/m_i, его не меньшую, т.е. производится округление числа M/m_i до ближайшего целого в большую сторону).

Этот факт объясняется следующим образом. При проведении процедуры контроля, для установления факта правильности или нет числа $A=(a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n, a_{n+1})$, нет необходимости анализировать все числовые интервалы $[j_i \cdot m_i, (j_i+1)\cdot m_i)$, где находится искажённое число, расположенное вне информационного числового интервала $[0, M)$. В этом случае для установления только факта правильности (или нет) числа A, определение номеров и анализ местоположения этих интервалов $[j_i \cdot m_i, (j_i+1)\cdot m_i)$ не имеют никакого значения. Для контроля НКС A в СОК достаточно знать местоположение нуля в записи (1) СК (знать численное значение n_A) только в числовых интервалах $[j_i \cdot m_i, (j_i+1)\cdot m_i)$, лежащих в информационном числовом интервале $0 \div M$, и в первом, находящимся после значения M, интервале, расположенном на отрезке $0 \div M_0$ (Рис. 2). Для контроля данных $A=(a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n, a_{n+1})$ достаточно знать СК $K_{N_i}^{(n_A)}$ длиною всего $N_i =]M / m_i[$ двоичных разрядов.

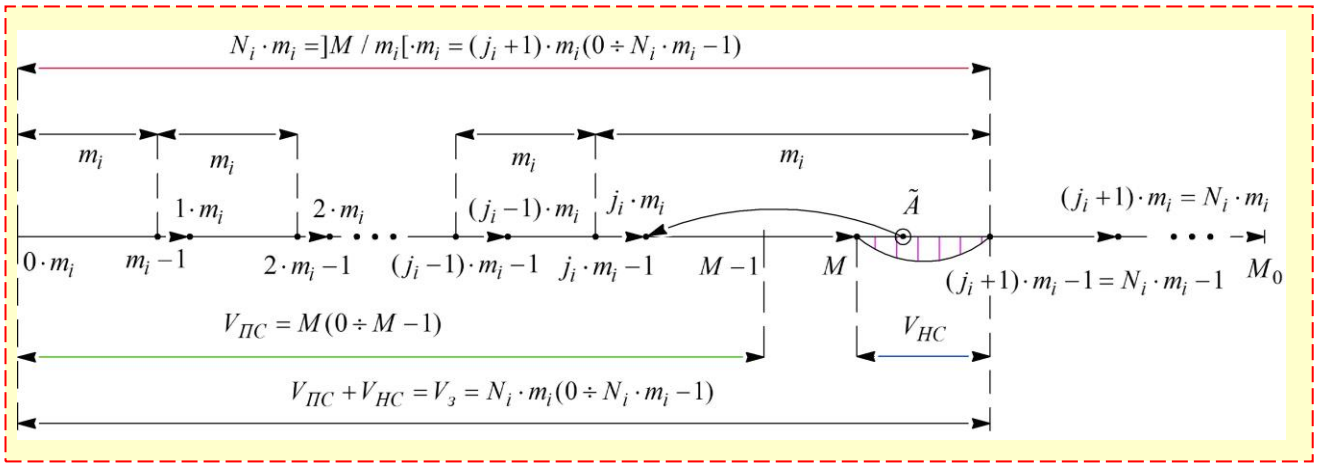


Рис. 2 – Схема контроля данных в СОК для произвольного значения модуля m_i

Таким образом, суть метода контроля данных в СОК состоит в следующем (см. Рис. 3). Для контролируемой НКС $A=(a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n, a_{n+1})$, представленной в СОК, определяется ППНК n_A путем формирования СК $K_{N_i}^{(n_A)} = \left\{ Z_{N_i-1}^{(A)}\ Z_{N_i-2}^{(A)} \ldots Z_1^{(A)}\ Z_0^{(A)} \right\}$ в виде последовательности из N_i двоичных разрядов. Выбор основания m_i СОК производиться специальным образом, в соответствии с определенными критериями.

Исходя из значения остатка a_i числа $A=(a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n, a_{n+1})$, выбирается константа нулевизации вида $KH_{m_i}^{(A)} = \left(a_1', a_2', ..., a_{i-1}', a_i, a_{i+1}', ..., a_n', a_{n+1}'\right)$. Далее проводиться реализация операции $A_{m_i} = A - KH_{m_i}^{(A)}$. Используя N_i констант $K_A \cdot m_i$ $\left(K_A = \overline{0, N_i - 1}\right)$, одновременно проводятся операции вычитания $A_{m_i} - K_A \cdot m_i$, в результате которых образуется значение двоичных разрядов $Z_{K_A}^{(A)}$, т.е. формируется СК $K_{N_i}^{(n_A)}$. Значение ППНК n_A опреде-

ляется из равенства $A_{m_i} - n_A \cdot m_i = 0$.

Рис. 3 – Метод контроля данных в СОК

Процедура контроля числа A состоит в следующем. Если $n_A > N_i$, то считается что число A – неправильное число. В противоположном случае ($n_A \le N_i$) число A – правильное.

Рассмотрим примеры реализации метода контроля для конкретной СОК, которая задана основаниями $m_1 = 3$, $m_2 = 4$, $m_3 = 5$, $m_4 = 7$ и $m_k = m_{n+1} = m_5 = 11$. Данная СОК обеспечивает обработку данных в однобайтовой ($l = 1$) разрядной сетке СПОД. При этом $M = \prod_{i=1}^{4} m_i = 420$, $M_0 = M \cdot m_{n+1} = 4620$. Кроме этого будем считать, что $m_i = 11$. В этом случае $N_i = N_{n+1} =]M / m_i[=]M / m_{n+1}[=]420/11[=]38{,}18[= 39$.

В табл. 1 приведено содержимое БКН СПОД относительно основания $m_K = m_{n+1} = 11$.

Таблица 1 – Константы $KH_{m_{n+1}}^{(A)}$ нулевизации

Остаток $a_к = a_{n+1}$	Константы нулевизации				
	$m_1 = 3$	$m_2 = 4$	$m_3 = 5$	$m_4 = 7$	$m_k = m_5 = 11$
	a'_1	a'_2	a'_3	a'_4	a_5
0000	00	00	000	000	0000
0001	01	01	001	001	0001
0010	10	10	010	010	0010
0011	00	11	011	011	0011
0100	01	00	100	100	0100
0101	10	01	000	101	0101
0110	00	10	001	110	0110
0111	01	11	010	000	0111
1000	10	00	011	001	1000
1001	00	01	100	010	1001
1010	01	10	000	011	1010

Пример 1. Провести контроль данных, представленных в виде $A = (01, 00, 000, 010, 0001)$ при $m_k = m_{n+1} = m_5 = 11$. По значению остатка $a_K = a_{n+1} = a_5 = 0001$ числа A в БКН (Табл. 1) выбирается константа $KH_{m_{n+1}}^{(A)} = (01, 01, 001, 001, 0001)$ нулевизации. Далее определяем $A_{m_{n+1}} = A - KH_{m_{n+1}}^{(A)} = (00, 11, 100, 001, 0000)$. Посредством реализации соотношения (3) форми-

руем СК вида $K_{N_i}^{(n_A)} = K_{39}^{(9)} = \{11...110111111111\}$. Исходя из вида СК и используя выражение $A_{m_{n+1}} - n_A \cdot m_{n+1} = 0$, определяем, что $n_A = 9$ ($A_{m_{n+1}} - n_A \cdot m_{n+1} = 99 - 9 \cdot 11 = 0$), т.е. $Z_{n_A}^{(A)} = Z_9^{(A)}$. Так, как $N_i = 39 > n_A = 9$, то ошибки нет. Проверка: $A = 100 < M = 420$ (число A правильное).

Пример 2. Провести контроль данных $A = (00, 01, 000, 010, 1010)$. По значению $a_5 = 1010$ в БКН (Табл. 1) выбирается константа вида $KH_{m_{n+1}}^{(A)} = (01, 10, 000, 011, 1010)$. Получим, что $A_{m_{n+1}} = A - KH_{m_{n+1}}^{(A)} = (10, 00, 000, 110, 0000)$. Так как $A_{m_{n+1}} - n_A \cdot m_{n+1} = 440 - 44 \cdot 11 = 0$, то СК имеет вид $K_{N_i}^{(n_A)} = K_{39}^{(40)} = \{11...11...11\}$ и $n_A = 40$. Так как $N_i = 39 < n_A = 40$, то ошибка в данных присутствует. Проверка: $A = 450 > M = 420$ (число A неправильное).

Пример 3. Провести контроль данных $A = (01, 11, 010, 000, 1001)$. По значению $a_5 = 1001$ в БКН (Табл. 1) выбирается константа $KH_{m_{n+1}}^{(A)} = (00, 01, 100, 010, 1001)$. Определим что $A_{m_{n+1}} = A - KH_{m_{n+1}}^{(A)} = (01, 10, 011, 101, 0000)$. Так как $A_{m_{n+1}} - n_A \cdot m_{n+1} = 418 - 38 \cdot 11 = 0$, то СК имеет вид $K_{N_i}^{(n_A)} = K_{39}^{(38)} = \{011...11...11\}$ и $n_A = 38$. Исходя из того, что $n_A = 38 < N_i = 39$ делается вывод: число A правильное (не искажено). Однако проверка показывает, что $A = 427 > M = 420$, т.е. A неправильное число (Рис. 4). В этом случае при контроле данных допущена ошибка.

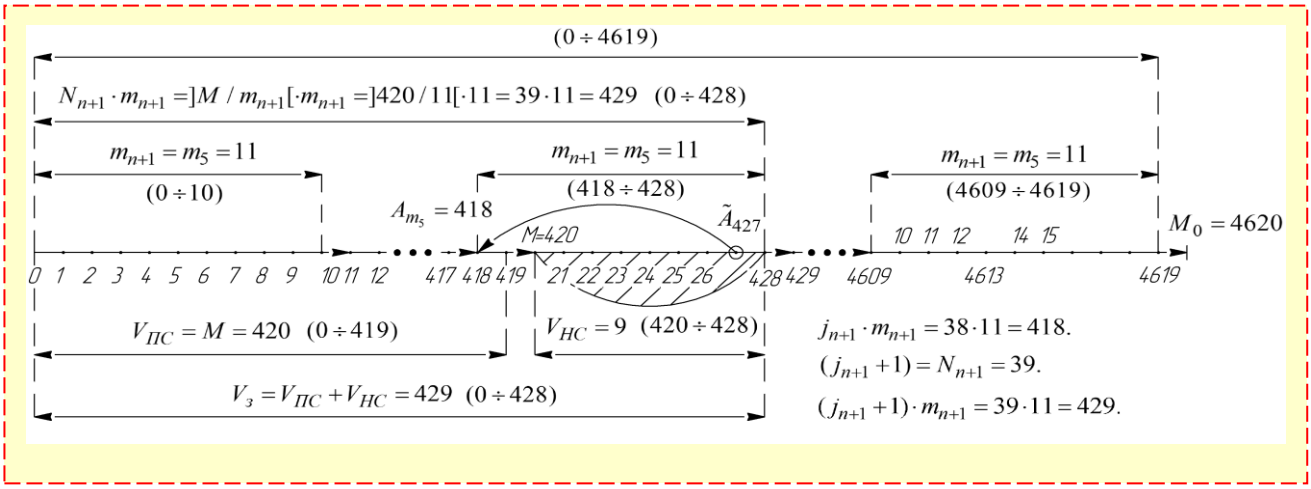


Рис. 4 – Схема контроля данных в СОК для $m_i = 11$

Из примера №3 следует, что применение рассмотренного метода для оперативного контроля данных в СОК не во всех случаях обеспечивает достоверный результат контроля. Действительно, существует совокупность $(j_{n+1} + 1) \cdot m_{n+1} - M$ неправильных $\tilde{A}$ чисел, которые определяются системой контроля (СКН) ККС как правильные, что обуславливает низкую достоверность контроля. Для примера №3, таких чисел будет более 80% (Табл. 2).

Таблица 2 – Совокупность кодовых слов

Числовой диапазон [418, 429)	
Правильные числа A	*Совокупность неправильных $\tilde{A}$ чисел, которые определяются системой контроля СПОД как правильные*
418, 419	420, 421, 422, 423, 424, 425, 426, 427, 428

Таким образом, очевидно, что рассмотренный метод оперативного контроля данных в СОК обеспечивает низкую достоверность контроля [2]. Низкая достоверность контроля данных вызвана наличием ненулевого значения α остатка в выражении

$$\alpha = M_{n+1} / m_{n+1} - [M_{n+1} / m_{n+1}] = M / m_{n+1} - [M / m_{n+1}]. \quad (4)$$

В свою очередь наличие ненулевого $\alpha \neq 0$ остатка определяется фактом не кратности значения M контрольному модулю m_{n+1} СОК, который определяет величину числового интервала $[j_{n+1} \cdot m_{n+1},\ (j_{n+1}+1) \cdot m_{n+1})$ возможного нахождения числа A. В этом случае контроль данных $A = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n, a_{n+1})$ осуществляется на основе использования контрольного m_{n+1} основания СОК, путем формирования СК

$$K_{N_{n+1}}^{(n_A)} = \left\{ Z_{N_{n+1}-1}^{(A)}\ Z_{N_{n+1}-2}^{(A)} \ldots Z_0^{(A)} \right\}. \quad (5)$$

Геометрически низкую достоверность контроля данных можно пояснить следующим образом (Рис. 2). Числовой информационный интервал $[0,\ M = \prod_{i=1}^{n} m_i)$ не вмещает целое число отрезков длинною равных значению $m_i = m_{n+1}$. В этом случае на числовой оси $0 \div M_0$ существует числовой интервал $[j_{n+1} \cdot m_{n+1},\ (j_{n+1}+1) \cdot m_{n+1})$ (или $[(N_{n+1}-1) \cdot m_{n+1}, N_{n+1} \cdot m_{n+1})$ внутри которого находится число M. Поэтому в данном интервале одновременно находится совокупность $(j_{n+1}+1) \cdot m_{n+1}) - M$ неправильных чисел (или $N_{n+1} \cdot m_{n+1} - M$) и совокупность М – $j_{n+1} \cdot m_{n+1}$ правильных чисел (или $M - (N_{n+1}-1) \cdot m_{n+1}$). В процессе контроля данных A, при проведении процедуры нулевизации, все, как неправильные $(j_{n+1}+1) \cdot m_{n+1}) - M$, так и правильные $M - j_{n+1} \cdot m_{n+1}$ числа, смещаются на левый край (к одному правильному числу $j_{n+1} \cdot m_{n+1}$) интервала $[j_{n+1} \cdot m_{n+1},\ (j_{n+1}+1) \cdot m_{n+1})$. В этом случае СКН ККС будет идентифицировать (определять) неправильные $[N_{n+1} \cdot m_{n+1}) - M]$ числа как правильные.

Под достоверностью контроля данных в СОК будем понимать вероятность получения истинного результата операции контроля данных. В качестве показателя для количественной оценки достоверностью контроля данных в СОК можно воспользоваться соотношением

$$P_{дк} = V_{ПС} / V_{OC}, \quad (6)$$

где в общем случае: $V_{ПС} = M$ – количество (от 0 до $M \div 1$) правильных ($A < M$), лежащих в рабочем числовом $[0, M_0)$ диапазоне, кодовых слов для данной СОК; $V_{OC} = (V_{ПС} + V_{HC})$ – общее количество кодовых слов, которые в результате проведения контроля данных считаются правильными; $V_{HC} = (N_i \cdot m_i - M)$ – количество неправильных ($A \geq M$) кодовых слов, которые в результате проведения контроля данных считаются правильными (отметим, что $N_i =]M / m_i[= j_i + 1$.

С учетом вышеизложенного, показатель достоверности (6) определяется соотношением

$$P_{дк} = \frac{M}{M + N_i \cdot m_i - M} = \frac{M}{N_i \cdot m_i}. \quad (7)$$

При равенстве $m_i = m_{n+1}$ имеем, что $V_{HC} = (N_{n+1} \cdot m_{n+1} - M)$. Если $m_i = m_{n+1}$ то выражение (7) примет вид

$$P_{дк} = \frac{M}{M + N_{n+1} \cdot m_{n+1} - M} = \frac{M}{N_{n+1} \cdot m_{n+1}}. \quad (8)$$

Так, как заведомо $N_{n+1} \cdot m_{n+1} > M$ (см. (4), рис. 2, 4), то в этом случае всегда $P_{дк} < 1$.

Если в качестве основания m_i, определяющего величины числовых $j_i \cdot m_i \div (j_i+1)\cdot m_i$ интервалов, возьмём информационное основание СОК, например, $m_i = m_1$, тогда $N_i =]M / m_i[= N_1 =]M / m_1[$ и $N_1 = \prod_{i=2}^{n} m_i$. В этом случае, выражение (7) примет вид

$$P_{дк} = \frac{M}{M + N_1 \cdot m_1 - M} = \frac{M}{N_1 \cdot m_1} = 1. \qquad (9)$$

В этом случае получим, что (см. выражение (4)) всегда $Д = 1$, т.е., при $m_i = m_1$, СКН ККС всегда обеспечивает достоверный результат контроля данных в СОК.

Предлагаемый метод повышения достоверности контроля основан на известном методе оперативного контроля информации в СОК, который, в свою очередь, состоит из процедур получения и использования ППНК [2].

Суть предлагаемого метода повышения достоверности контроля данных в СОК состоит в обеспечении максимальной $P_{дк} = 1$ достоверности контроля данных, путем обеспечения выполнение условия $\alpha = 0$ (см. выражение (4)). В этом случае для вычисления значения $N_i =]M / m_i[$ выбирается модуль m_i, определяющий номер j_i числового интервала $[j_i \cdot m_i,\ (j_i+1)\cdot m_i)$ нахождения числа $A = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n, a_{n+1})$, только из совокупности *n* информационных модулей СОК, которые, естественно, кратны значению *M*. В этом случае $\alpha = M - [M / m_i] \cdot m_i = 0$, что и обеспечивает максимальное значение показателя достоверности контроля $P_{дк} = 1$ (см. выражение (7)).

Приведем пример применения разработанного метода для повышения достоверности контроля данных в СОК.

Пример 4. Из вышеприведенной СОК выбираем, например, информационное основание $m_i = m_1 = 3$ (Рис. 5). При этом $N_i = N_1 = M / m_1 = 4 \cdot 5 \cdot 7 = 140$. В этом случае рабочий числовой $[0, M_0)$ диапазон СОК разбивается на интервалы $[j_1 \cdot m_1, (j_1+1)\cdot m_1)$. Для значения $m_1 = 3$ информационный числовой интервал $[0, M)$ разбивается точно на $N_1 = M / m_1 = 140$ отрезков длиною три единицы каждый (см. Рис. 5). В таблице 3 приведено содержимое БКН относительно основания $m_1 = 3$.

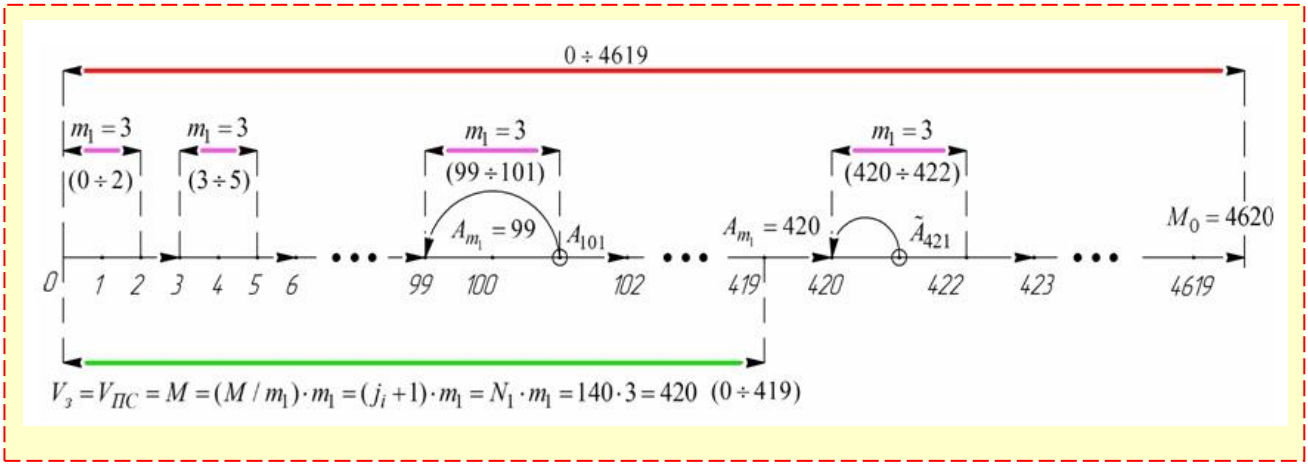


Рис. 5 – Схема контроля данных в СОК для $m_i = 3$

Пусть необходимо провести контроль числа $A = (01, 11, 010, 000, 1001)$. По значению $a_1 = 01$ в БКН (Табл. 3) выбираем константу нулевизации вида $KH_{m_1}^{(A)} = (01, 01, 001, 001, 0001)$.

Таблица 3 – Содержимое БКН для $m_1 = 3$

a_i	Константы				
	$m_1 = 3$	$m_2 = 4$	$m_3 = 5$	$m_4 = 7$	$m_5 = 11$
00	00	00	000	000	0000
01	01	01	001	001	0001
10	10	10	010	010	0010

Далее определяем $A_{m_1} = A - KH_{m_1}^{(A)} = (00, 10, 001, 110, 1000)$.

Если $A_{m_1} - n_A \cdot m_1 = 426 - 142 \cdot 3 = 0$, то СК имеет следующий вид:

$$K_{N_i}^{(n_A)} = K_{140}^{(142)} = \{Z_{139}^{(A)}\ Z_{138}^{(A)} \ldots Z_1^{(A)}\ Z_0^{(A)}\} = \ = \{11...11...11\}.$$

Так как $N_i = 140 < n_A = 142$, то есть ошибка в числе A.

Проверка: $A = 427 > M = 420$. Число $A > M$, т.е. оно неправильное (искажено).

В таблице 4 приведены результаты расчета и сравнительного анализа достоверности контроля данных для различных значений контрольного основания m_{n+1} СОК, которая задана информационными основаниями $m_1 = 3$, $m_2 = 4$, $m_3 = 5$ и $m_4 = 7$.

Таблица 4 – Результат расчёта значений $Д_i$ и $Д_{n+1}$ достоверности контроля в СОК

№ п.п.	m_{n+1}	M	M / m_{n+1}	$]M / m_{n+1}[$	$N_{n+1} =]M / m_{n+1}[\cdot m_{n+1}$	$Д_{n+1}$	$Д_i$, $i = \overline{1,n}$	Выигрыш в [%]
1	11	420	38,2	39	429	0,979	1	2,1
2	13	420	32,3	33	429	0,979	1	2,1
3	17	420	24,7	25	425	0,988	1	1,2
4	19	420	22,1	23	437	0,961	1	3,9
5	23	420	18,2	19	437	0,961	1	3,9
6	29	420	14,4	15	435	0,965	1	3,5

Кроме оперативности контроля данных важной характеристикой ККС является количество оборудования системы контроля. Отметим, что в СОК количество оборудования СКН в основном зависит от количества сумматоров, реализующих операции вида (3).

Таким образом, количество оборудования СКН зависит от величины значения

$$N_i = \prod_{\substack{K=1; \\ K \neq i.}}^{n+1} m_K \quad (i = \overline{1,n}).$$

В этом случае, с учетом требования $\alpha = 0$ и требования не снижения оперативности контроля, для минимизации количества оборудования СКН в СОК необходимо выбрать максимальный по величине информационный модуль. Для упорядоченной ($m_i < m_{i+1}$) СОК это будет основание m_n.

Предварительная оценка количества оборудования для l– байтовой разрядной сетки представления машинного слова ККС может быть проведена посредством значения коэффициента эффективности представленного в виде:

$$K_{эф}^{(l)} = \frac{N_1}{N_n} = \frac{M / m_1}{M / m_n} = \frac{m_n}{m_1}.$$

Приведём пример контроля данных в СОК для значения $m_i = m_n$.

Пример 5. Максимальным из информационных оснований для вышеприведенной СОК является $m_n = m_4 = 7$. При этом $N_i = N_4 = M / m_4 = 3 \cdot 4 \cdot 5 = 60$. Рабочий числовой $[0, M_0)$ диапазон разбивается на интервалы $[j_4 \cdot m_4, (j_4 + 1) \cdot m_4)$, т.е. на $M_0 / m_4 = 4620 / 7 = 660$ отрезков. Для значения $m_4 = 7$ информационный $[0, M)$ интервал разбивается на $N_4 = M / m_4 = 60$ числовых отрезков длинною семь единиц (см. Рис. 6). В таблице 5 приведено содержимое БКН ККС относительно основания $m_4 = 7$.

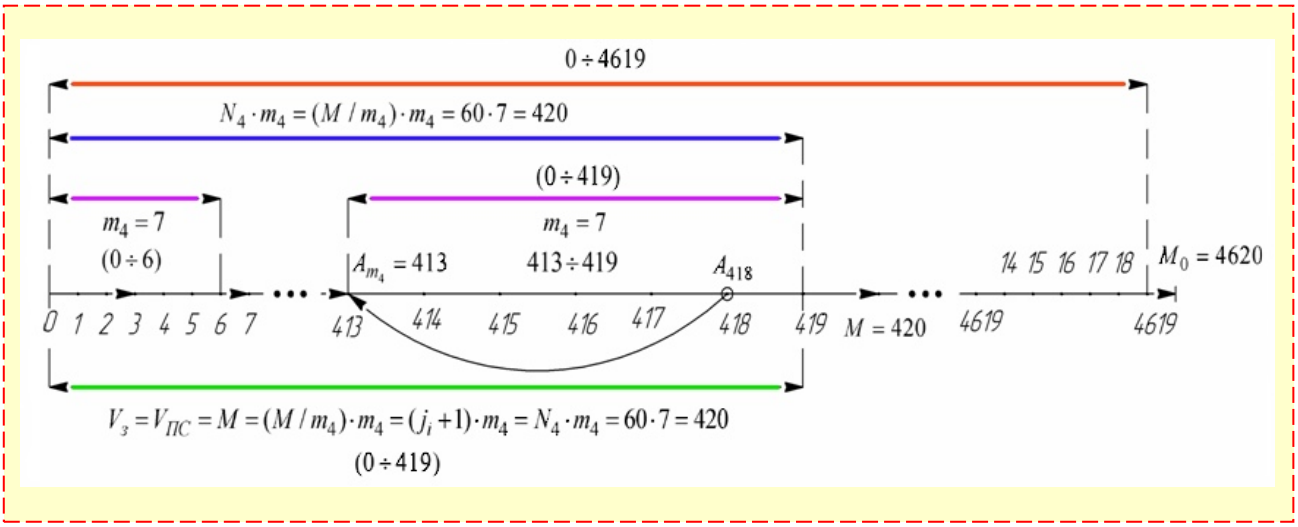


Рис. 6 – Схема контроля данных в СОК для $m_i = 7$

Таблица 5 – Содержимое БКН для $m_4 = 7$

a_4	**Константы**				
	$m_1 = 3$	$m_2 = 4$	$m_3 = 5$	$m_4 = 7$	$m_5 = 11$
000	00	00	000	0000	0000
001	01	01	001	001	0001
010	10	10	010	010	0010
011	00	11	011	011	0011
100	01	00	100	100	0100
101	10	01	000	101	0101
110	11	10	001	110	0110

Пусть необходимо провести контроль числа $A=(01,11,010,000,1001)$. По значению $a_4=000$ в БКН (Табл. 4) выбираем константу $KH_{m_n}^{(A)}=KH_7^{(A)}=(00,00,000,000,0000)$. Далее определяем значение $A_{m_n}=A_7=A-KH_7^{(A)}=(01,11,010,000,1001)$. Посредством реализации соотношений (2) формируем СК вида $K_{N_4}^{(n_A)}=K_{60}^{(61)}=\left\{Z_{59}^{(A)}\,Z_{58}^{(A)}\ldots Z_1^{(A)}\,Z_0^{(A)}\right\}=\{11\ldots11\ldots11\}$. Исходя из вида СК и используя выражение $A_{m_n}-n_A\cdot m_n=0$, определяем, что $n_A=61$ ($A_{m_n}-n_A\cdot m_n=427-61\cdot7=0$). Т.к. $N_4=60<n_A=61$, то ошибка в данных A присутствует.

Проверка: $A=427>M=420$.

В таблице 6 приведены расчетные данные условного количества оборудования системы контроля ККС, функционирующей в СОК, и данные сравнительного анализа сокращения количества оборудования СКН для $m_i=m_n$.

Таблица 6 – Сравнительные данные количества оборудования системы контроля СПОД

Разрядная сетка l - байтовой СПОД (ρ, n, k)	Информационные основания СОК m_i ($i=\overline{1,n}$)	Контрольное m_{n+1} основание СОК	Минимальное информационное m_1 основание СОК	Максимальное информационное m_n основание СОК	$K_{эфф.}^{(l)}$
$l=1$ ($\rho=8$, $n=4$, $k=3$)	$m_1=3$, $m_2=4$, $m_3=5$, $m_4=7$	$m_5=11$	$m_1=3$	$m_4=7$	2,3
$l=2$ ($\rho=16$, $n=6$, $k=4$)	$m_1=2$, $m_2=5$, $m_3=7$, $m_4=9$, $m_5=11$, $m_6=13$	$m_7=17$	$m_1=2$	$m_6=13$	6,5
$l=3$ ($\rho=24$, $n=8$, $k=5$)	$m_1=3$, $m_2=4$, $m_3=5$, $m_4=7$, $m_5=11$, $m_6=13$, $m_7=17$, $m_8=19$	$m_9=23$	$m_1=3$	$m_8=19$	6,3
$l=4$ ($\rho=32$, $n=10$, $k=5$)	$m_1=2$, $m_2=3$, $m_3=5$, $m_4=7$, $m_4=11$, $m_5=13$, $m_6=17$, $m_7=19$, $m_9=23$, $m_{10}=29$	$m_{11}=31$	$m_1=2$	$m_{10}=29$	14,5
$l=8$ ($\rho=64$, $n=16$, $k=6$)	$m_1=3$, $m_2=4$, $m_3=5$, $m_4=7$, $m_5=11$, $m_6=13$, $m_7=17$, $m_8=19$, $m_9=23$, $m_{10}=29$, $m_{11}=31$, $m_{12}=37$, $m_{13}=41$, $m_{14}=43$, $m_{15}=47$, $m_{16}=53$	$m_{17}=59$	$m_1=3$	$m_{16}=53$	17,6

3 Выводы

В данной работе рассмотрен метод повышения достоверности контроля данных в СОК. Представленный метод основан на использовании ППНК n_A, который является одной из характеристик СК. Использование данного метода обеспечивает выбор значения модуля m_i, которое определяет номер числового интервала нахождения НКС, из всей совокупности n возможных информационных оснований СОК. Применение рассмотренного метода обеспечивает получение достоверного результата контроля данных в СОК.

Ссылки

[1] Akushskii I. Ya. Mashinnaya arifmetika v ostatochnykh klassakh / I. Ya. Akushskii, D. I. Yuditskii. – Moskva: Sovetskoe radio, 1968. – 440 s.
[2] Moroz S. A. Metody kontrolya, diagnostiki i korrektsii oshibok dannykh v informatsionno–telekommunikatsionnoi sisteme, funktsioniruyushchei v klasse vychetov / S. A. Moroz, V. A. Krasnobaev // Informacijno–kerujuchi systemy na zaliznychnomu transporti. – 2012. – № 2. – S. 60–78.
[3] Karpenko O. Discrete Signals with Multi – Level Correlation Function / O. Karpenko, A. Kuznetsov, V. Sai, Yu. Stasev // Telecommunications and Radio Engineering. – 2012. – Vol.71. – Issue 1. – P. 91–98.
[4] Stasev Yu.V. Formation of pseudorandom sequences with improved autocorrelation properties / Yu.V. Stasev, A.A. Kuznetsov, A.M. Nosik // Cybernetics and Systems Analysis. – 2007. – Vol.43. – Issue 1. – P. 1–11.

Reviewer: Sergii Kavun, Doctor of Sciences (Economics), Ph.D. (Engineering), Full Prof., Kharkiv Educational and Research Institute of the University of Banking , Kharkiv, Ukraine. E-mail: kavserg@gmail.com

Received: January 2017.

Authors:
Viktor Krasnobayev, Doctor of Sciences (Engineering), Full Prof., V. N. Karazin Kharkiv National University, Kharkov, Ukraine. E-mail: krasnobayev@karazin.ua.
Sergey Koshman, Ph.D., Associate Prof., Kharkov National Technical University of Agriculture named after Peter Vasylenko, Kharkov, Ukraine. E-mail: s_koshman@ukr.net.
Alina Yanko, PhD stud., The Poltava National Technical Yuri Kondratyuk University, Poltava, Ukraine. E-mail: al9_yanko@ukr.net.

The method of a data control in the residual system classes based on use of positional attribute of non-positional code structure.

Abstract. The method of a data control in the residue number system (RNS) are developed in the article, which is based on the use of positional attribute of non-positional code structure. The using variants of the proposed method of data control in the RNS were considered, as well as specific examples of the operation monitoring data in the CRS. The data of comparative analysis of data control amount equipment depending on the word length of the computer system were given.

Keywords: residue number system, the accuracy of the data control, communication data processing system, position indication nonpositional code, nonpositional code structure.

Рецензент: Сергій Кавун, доктор економічних наук, к.т.н., проф., Харківський інститут банківської справи УБС НБУ, Харків, Україна. E-mail: kavserg@gmail.com

Надійшло: Січень 2017.

Автори:
Віктор Краснобаєв, д.т.н. проф., ХНУ імені В. Н. Каразіна, Харків, Україна. E-mail: krasnobayev@karazin.ua
Сергій Кошман, к.т.н., доцент, Харківський національний технічний університет сільського господарства імені Петра Василенка, Харків, Україна. E-mail: s_koshman@ukr.net
Аліна Янко, аспірантка кафедри комп'ютерної інженерії, Полтавський національний технічний університет імені Юрія Кондратюка, Полтава, Україна. E-mail: al9_yanko@ukr.net

Метод контролю даних у системі залишкових класів на основі використання позиційної ознаки непозиційної кодової структури.

Анотація. У статті розробляється метод контролю даних у системі залишкових класів (СЗК), який заснований на використанні позиційної ознаки непозиционної кодової структури. Розглянуто варіанти застосування запропонованого методу контролю даних у СЗК, а також приклади конкретного виконання операції контролю даних у СЗК. Наведені дані порівняльного аналізу кількості обладнання системи контролю в залежності від величини розрядної сітки комп'ютерної системи.

Ключові слова: система залишкових класів, достовірність контролю даних, система передачі та обробки даних, позиційна ознака непозиційного коду, непозиційна кодова структура.

УДК 519.68

ОТ МАТЕМАТИЧЕСКОЙ ЛОГИКИ К ЯЗЫКАМ ПРОГРАММИРОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

В. Куклин

Харьковский национальный университет имени В.Н. Каразина, пл. Свободы, 4, г. Харьков, 61022, Украина
kuklinvm1@gmail.com

Рецензент: Александр Потий, д.т.н., проф., Харьковский национальный университет имени В. Н. Каразина, пл. Свободы, 4, г. Харьков, 61022, Украина.
potav@ua.fm

Поступила в январе 2017

Аннотация. *Рассмотрен процесс становления теории экспертных систем на примере формирования языка программирования искусственного интеллекта ПРОЛОГ. Показан сложный путь осознания проблем искусственного интеллекта и мотивы, которые привели к появлению экспертных систем, построенных на основе математической логики. Обсуждаются основные идеи и процедуры, которые привели к построению сначала отдела математической логики - теории предикатов, представлению процедур этой теории на гиперграфах и затем к созданию языка ПРОЛОГ. Отмечается прогресс в развитии интеллектуальных систем и проблемы, которые стоят перед исследователями.*

Ключевые слова*: теория предикатов, гиперграфы И/ИЛИ, язык программирования ПРОЛОГ.*

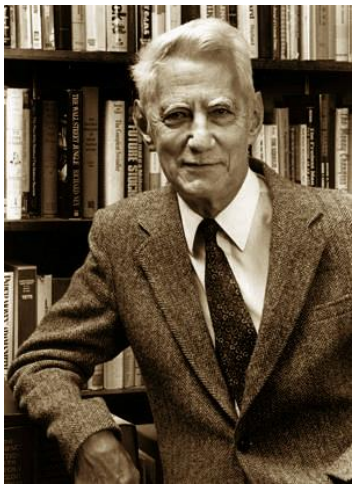
1 Введение

Развитие вычислительной техники стимулировало развитие программного обеспечения, особенно языков программирования высокого уровня. Вообще языки программирования обычно создавали по принципу удобства решения какого-либо класса задач. При этом большинство из них к математике имели весьма отдаленное отношение. Однако для языков искусственного интеллекта ситуация сложилась иначе. Но все по порядку.

Аллен Ньюэлл
(Allen Newell)

Работал в RAND и Университете Карнеги-Меллон. Разработал программмы Logical Theorist (*доказавшую законы из книги Рассела и Уайтхеда «Principia Mathematica»*) и «General Problem Solver» для игры в шахматы. Один из создателей языка IPL.

Клод Э́лвуд Ше́ннон
(Claude Elwood Shannon)



Докторская диссертация в Массачусетском технологическом институте, работа в компании Белл (Bell Labs) и Мичиганском университете. Основатель теории информации и теории автоматов.
Впервые использовал понятие «бит».

Фридрих Людвиг Готлоб Фреге
(Friedrich Ludwig Gottlob Frege)

Вклад Фреге в логику сравнивают с вкладом Аристотеля и К. Геделя. В работе *Begriffsschrift* (Исчисление понятий) Фреге (1879) создал логику предикатов, ввел кванторы и многое другое, что способствовало появлению книги «Principia Mathematica» и теоремы о неполноте Геделя.

Итак, после позднего увлечения шахматами Алленом Ньюэлом, создавшим действующую программу (1954) [1,2] на основе методов Клода Шеннона [3], массово потянулись энтузиасты-последователи. Но о математической логике, которая была давно создана благодаря усилиям Фридриха Готлоба Фреге [4] и его современников, пока никто не вспоминал, что, впрочем, не удивительно. Игры показались интереснее. Однако, пригодный метод для решения задачи создания шахматных программ практически без применения формализма предложил Алан Тьюринг [5]. Не надеясь на математику он вместе с Алонзо Чёрчем считал, что все известные им программы настолько склонны увлекаться собственными действия, что остановить их можно лишь насильственно *(тезис Черча-Тьюринга)*. Потому в программы так часто вводятся операторы и процедуры, сдерживающие прыть машин, которые самозабвенно «роются» в базах данных, в то время, когда пользователю, иной раз, некогда ждать. В результате усилий сотрудников корпорации RAND Джона Шоу и Герберта Саймона, поддерживаемых де Гротом и его коллегами психологами был создан язык ИПЛ (IPL, 1956), предшественник языка ЛИСП *(появился позднее в результате усилий Джона Маккарти (1960))*. Язык ЛИСП - язык обработки списков, был построен на системе лямбда-вычислений А. Черча, как и другие функциональные языки этого семейства, разработанные последователями [6-8].

Алан Тьюринг
(Alan Mathison Turing)

А. Тьюринг внес существенный вклад в основания информатики, разработал теорию и метод взлома немецкого шифратора во время 2-й мировой войны.
Работал в Национальной физической лаборатории и университете Манчестера. Создатель проекта первого компьютера с памятью. Предложил тест своего имени для оценки интеллекта (1950).

Герберт АлександерСаймон
(Herbert A. Simon)

Разработчик теории организации и управления. Один из создателей современной теории управленческих решений *(теория ограниченной рациональности)*.
Профессор компьютерных наук и психологии в Университете Карнеги-Меллона. Нобелевская премия по экономике (1978).

Жак Эрбран
(Jacques Herbrand)

Основные труды в математической логике, теории полей классов, ввел рекурсивные функции, разработал математический метод резолюции.
Теорема Эрбрана о дедукции является результатом диссертации по теории доказательств.

Вообще интересные люди – эти последователи: обыкновенно получив в свое распоряжение новый метод, человек сразу ищет, где бы его применить и как бы его модифицировать, не только для удобства решения нужной проблемы, но и для создания своего собственного творения. При этом последний мотив настолько распространен, что многие научные журналы переполнены вариантами решения задач, которые при ближайшем рассмотрении мало отличаются от самой первой, где собственно и был впервые применен этот тиражируемый метод *(поделки, хотя возможно и небесполезные)*.

Использование формальной логики для создания логического метода «опровержения на основе резолюции» Джоном Робертсоном (1965) оказалось революционным [9, 10].

На основе этого метода, хотя и с целым рядом отличий, был создан язык ПРОЛОГ Алайном Колмраузером, (1971), использующий логику предикатов первого порядка [11]. Кстати, математический метод резолюции был ранее применен юным математиком Жаком Эрбраном [12]. То есть, к началу 70-х годов были созданы языки программирования искусственного интеллекта ЛИСП, ПРОЛОГ, PLANNER, QA4, MACSYMA, REDUCE, TSM и их модификации, ориентированные на выполнение разных задач.

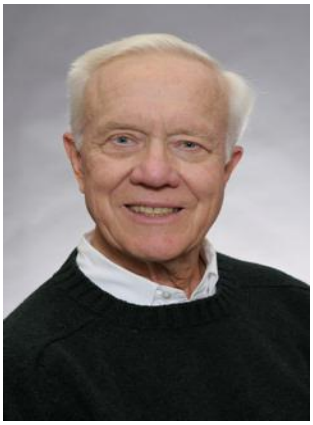
Джон Алан Робинсон
(John Alan Robinson)

Внес определяющий вклад в развитие логического программирования, докторская диссертация в Принстонском университете.
Работал в концерне DuPoint и в университете Райса, где сформулировал практический метод резолюции в логике.

А. Колмерауер
(Alain Colmerauer)

Защитил диссертацию в университете Гренобля.
Работал профессором в университете Монреаля *(где создал Q-system)*, затем в университете Марселя.
Создатель языка ПРОЛОГ.

Нильс Нильсон
(Nils J. Nilsson)



Руководитель Центра искусственного интеллекта Стенфордского университета.
Провел анализ свойств резолюции, выпустил несколько учебников *(в т.ч. «Принципы искусственного интеллекта»)*.

В 70-е годы 20-го века многие ученые и инженеры серьезно занялись отработкой формализма, стандартизованным представлением знаний в символьной форме, понятной машинам. На этом пути стало очевидно, что устройства на базе языков ИИ (искусственного интеллекта) должны сами собирать и обрабатывать информацию, не нуждаясь при этом в традиционных алгоритмах программистов, которые только наполняли бы глобальную базу данных, а что с этими данными делать впоследствии, решала бы уже сама программа. То есть языки программирования ИИ стали кардинально отличаться от обычных языков программирования, ибо в эти языки был встроен механизм решения задач.

Но, главное – это то, что появились языки программирования искусственного интеллекта, основанные на математике. Используя эти языки программирования стало возможным не только просмотреть весь ход решения задачи, но и поправить ее решение, в случае если что-то не нравилось или шло не так.

Другими словами программисты стали видеть, что происходит со знаниями, которые они вводили в память вычислительной машины на всех этапах решения задачи. Это обстоятельство, конечно, отличалось от нейронных систем, где понять, что там «творится» в этом «черном ящике» – нейрокомпьютере, было невозможно. Так как знания в память вычислительной машины вводились на основе данных и оценок экспертов, то и системы стали называть экспертными. Ниже детальнее рассмотрим основные идеи и процедуры, которые позволили создать язык ИИ – ПРОЛОГ.

2 Математическая логика и теория предикатов

Как известно, основой логики является суждение. В математической логике – это последовательность *(важен порядок следования)* квантор, субъект, связка и предикат (лат. *praedicatum* – сказанное). Для связок и кванторов в теории предикатов, которая есть частью математической логики, приняты следующие обозначения.

Таблица 1 – Принятые обозначения

СВЯЗКИ	***КВАНТОРЫ***
$\wedge$, * коньюнкция – И $\vee$, + дизьюнкция – ИЛИ* $\Rightarrow$ импликация – ЕСЛИ...ТО ** -- отрицание - НЕ	$\exists$ *существования* ($\exists$ x - *найдется такой x)* $\forall$ *общности* *(*$\forall$ *x - для каждого x)*

*$\dot{\vee}$ - *возможна дизьюнкция в строго разделительном смысле.*
***ЕСЛИ - антецедент, посылка ТО – консеквент, заключение.*

Таким образом суждение можно записать, например, так

$$(\forall x)\,[СЛОН\,(x),\ \Rightarrow ЦВЕТ\,(x,\ СЕРЫЙ]\,. \qquad (1)$$

Если обозначить символом T истину, а символом F – ложь, то вполне очевидными будут являться утверждения представленные в Табл. 2.

Таблица 2 – Принятые обозначения

$T \vee T$ $T \vee F$ $F \vee F$	*это T* *это T* *это F*
$T \wedge TT \wedge F$ $F \wedge F$	*это T* *это F* *это F*

В табл. 3 приведены не вполне очевидные, но правильные в математической логике утверждения.

Таблица 3 – Пример утверждений

--X1 $\vee$ ***X2***	*эквивалентно*	***X1*** $\Rightarrow$ ***X2***
$-T \vee T$ $-F \vee T$ $-T \vee F$ $-F \vee F$	*это T* *это T* *это F* *это T*	$T \Rightarrow T$ $F \Rightarrow T$ $T \Rightarrow F$* $T \Rightarrow T$
* *Ложно такое утверждение: «из истинного утверждения следует ложное утверждение».*		

В общем случае, можно говорить о трех видах предложений. Это факты, обычные предложения и правила (Табл. 4).

Таблица 4 – Виды предложений

ФАКТЫ Литералы	ПРЕДЛОЖЕНИЯ	ПРАВИЛА
P, P(x)	G(y) $\wedge$ S(z) --D(y) $\vee$ Q(z)	L(y) $\Rightarrow$ H(x)

Важно отметить, что в теории предикатов все связки можно заменить только двумя. Для этого нужно договориться, что все предложения, в которых используется только дизьюнкция и отрицание, должны быть связаны, например, коньюнкцией по умолчанию (так называемая, коньюктивная форма). Т.е. если сформированы два предложения, то их можно переписать в виде одного, поставив между ними связку - коньюнкцию. Возможна и дизьюнктивная форма, когда все предложения содержат только коньюнкцию и отрицание, но при этом по умолчанию связаны дизьюнкцией. Однако это форма менее принята в теории предикатов.

Интересно, что в теории предикатов импликацию заменяют на конъюнкцию, например,

$$\boldsymbol{X1} \Rightarrow \boldsymbol{X2} \text{ эквивалентно } \boldsymbol{--X1} \vee \boldsymbol{X2} \quad (2).$$

Кроме того, существуют и другие виды преобразования предложений, которые используют все связки (представлены ниже). В теории предикатов существует множество устоявшихся формул, подобно тому, как это сделано в элементарной алгебре (Табл. 4-5).

Таблица 5 – Формулы теории предикатов

ПРАВИЛА де МОРГАНА	
$--(X1 \vee X2)$ *эквивалентно* $--X1 \wedge --X2$	$--(X1 \wedge X2)$ *эквивалентно* $--X1 \vee --X2$

Таблица 6 – Формулы теории предикатов

ПРЕОБРАЗОВАНИЕ КВАНТОРОВ ОБЩНОСТИ $\forall$	ПРЕОБРАЗОВАНИЕ КВАНТОРОВ СУЩЕСТВОВАНИЯ $\exists$
$(-- \forall x)[P(x)]$ *эквивалентно* $(\exists x)[--P(x)]$	$--(\exists x)P(x)$ *эквивалентно* $(\forall x)[--P(x)];$

Обычно кванторы переносят в начало предложения и исключают сразу кванторы общности. С кванторами существования сложнее. Для работы с ними используют так называемые сколемовские функции и константы, то есть такие функции и константы, которые наверняка есть, но мы их пока не знаем. Тогда можно заменить квантор существования этими величинами, например, в следующем виде

$$(\forall y)[(\exists x)P(x,y)] \Rightarrow (\forall y)[P(g(y),y)] \ , \quad (3)$$

$$(\exists x)P(x) \Rightarrow P(A), \quad (4)$$

Здесь A и $g(y)$ – сколемовские константа и функция. Используя эти формулы можно преобразовывать сложносочиненные предложения. А процедуры непростых переходов с естественного языка на язык предикатов хорошо представлены в работе [13,14]. Рассмотрим пример преобразования сложносочиненного предложения в три бинарных.

Таблица 7 – Пример преобразования

$(\forall x)\{P(x) \Rightarrow \{(\forall y)[P(y) \Rightarrow P(f(x,y))] \wedge \sim(\forall y)[Q(x,y) \Rightarrow P(y)]\}\}$
$\sim P(x1) \vee \sim P(y) \vee P(f(x1,y))$ $\sim P(x2) \vee Q(x2,g(x2))$ $\sim P(x3) \vee \sim P(g(x3))$

Здесь при записи отдельных предложений *(традиционно для теории предикатов)* меняют аргументы, делая их независимыми. Итак, глобальная база данных состоит из фактов *(литералов)*, предложений и правил (которые можно перевести в предложения) по умолчанию связанных коньюнкцией.

Рассмотрим, как из двух предложений создать новое. Для этого в теории предикатов существует ***процедура и ее результат – резолюция***. Эта процедура является важнейшим механизмом генерации нового знания (см. Табл. 8).

Таблица 8 – Пример резолюции

РЕЗОЛЮЦИЯ - Создание нового предложений из двух	
Резолюция двух предложений $Q \vee P$ и $--P \vee G$ Ставим между предложениями дизъюнкцию $\vee$ $Q \vee P \vee --P \vee G$ Выделяем тавтологию $Q \vee (P \vee --P) \vee G$ Убираем тавтологию* $Q \vee G$.	Эти два предложения можно представить как $Q \vee P$ и $P \Rightarrow G$ при этом P заменяется на G и получаем $Q \vee G$.
* *Всегда без ущерба можно отбросить литерал или часть предложения, если они принимают заведомо истинное значение.*	

Следующей, по порядку, но не по важности процедурой в решении логических задач является ***метод опровержения на основе резолюции***. Опровержение на основе резолюции – это доказательство истинности целевой функции методом «от противного»: Задана целевая функция - в форме предложения или правила (1). Берем ее отрицание (2). Переводим его в форму предложения (3). Применяем резолюцию, то есть получаем все новые и новые предложения…(4). Если в результате подстановок получим пустое предложение, то мы доказали, что целевая функция истинна. Достоинство этого подхода заключается в его простоте и сравнительно коротком пути достижения результата.

Пример. Сформулируем задачу: Если Жора ходит в те же самые места, куда ходит Коля, а Коля в школе, то где же Жора?

$$\text{Факт: } B(KOLIA, SCHOOL); \quad (5)$$

$$\text{Правило: } \forall(x)[B(KOLIA, x) \Rightarrow B(GORA, x)]; \quad (6)$$

$$\text{Цель (вопрос): } (\exists x)B(GORA, x)). \quad (7)$$

На основной вопрос задачи «Где Жора?» можно ответить, если существует решение, иначе говоря, если $(\exists x)B(GORA, x))$ есть следствием начальной базы знаний (аксиом), то есть набора фактов и правил.

Здесь $(\exists x)B(GORA, x))$ - целевое предложение. Его отрицание (см. табл. 6) - это $(\forall x)[\sim B(GORA, x)]$.

Резолюция двух предложений $\sim B(KOLIA, y) \vee B(GORA, y)$ и $B(KOLIA, SCHOOL)$ дает ответ $B(GORA, SCHOOL)$ при унификации $y = KOLIA$.

Унификация – это согласование аргументов двух литералов, для того, чтобы можно было применить резолюцию. Использование резолюции также рассмотрено в работе [15].

Важность унификации при доказательстве теорем впервые подчеркнули авторы работ [16, 17], причем на необходимость согласованности подстановок указывает [17]. Тем не менее, вопрос о единственности решения, оставаясь открытым, вызвал большой интерес математиков, о результатах исследований которых практики мало что знают.

3 Представление теории предикатов на гиперграфах «и/или»

Рассмотрим представление элементов теории предикатов на графах. Родоначальником теории графов считается Л. Эйлер. Но как общемировая наука теория графов начала свое распространение после появления первой монографии на эту тему Д. Конига [18]. Это еще раз подтверждает известный тезис о важности популяризации научных результатов.

Леонард Эйлер (1707-1783)
Leonhard Euler

(портрет кисти Я.Э. Хандманна)

Автор фундаментальных работ по математике, математической физике, механике, оптике, кораблестроению и теории музыки.
Академик Берлинской, Туринской, Лиссабонской и Парижской наук.

Денеш Кёниг (1884-1944)
Kőnig Dénes

Докторская степень (1907). Профессор Будапештского университета. Под влиянием работ Г. Минковского *(Hermann Minkowski)* написал первую монографию по теории графов «Теория конечных и бесконечных графов» (1936).

После появления этой монографии множество исследователей разработали различные виды графов, создали большое число приложений, однако ниже нас будут интересовать такие графы, которые можно использовать для интерпретации теории предикатов. Именно такие разработанные в работах [19] описания гиперграфов И/ИЛИ можно было применять в частности и для теории предикатов.

Использование графов в исчислении предикатов часто позволяет упростить, сократить процедуры и сделать их наглядными. Пример построения графа И/ИЛИ . Важно отметить, что здесь встречается конъюнкция и дизъюнкция. Например, в ПРЯМОЙ СИСТЕМЕ ПРОДУКЦИЙ (то есть решение строится от фактов, используя правила, и достигаются неизвестные нам цели. Здесь дизъюнкция описана к-связками (объединение связок, здесь к = 2), а конъюнкция не использует связок. Факты, например, могут быть описаны сложносочиненным предложением

$$Q(w,A) \wedge [[\sim R(v) \wedge \sim P(v)] \vee \sim S(A,v)] \quad (8)$$

Решением будет множество предложений, конъюнктивно (по умолчанию) связанных между собой) на концевых вершинах графа:

$$Q(w,A), \quad (9)$$

$$\sim R(v) \vee \sim S(A,v) , \quad (10)$$

$$\sim P(v) \vee \sim S(A,v) . \quad (11)$$

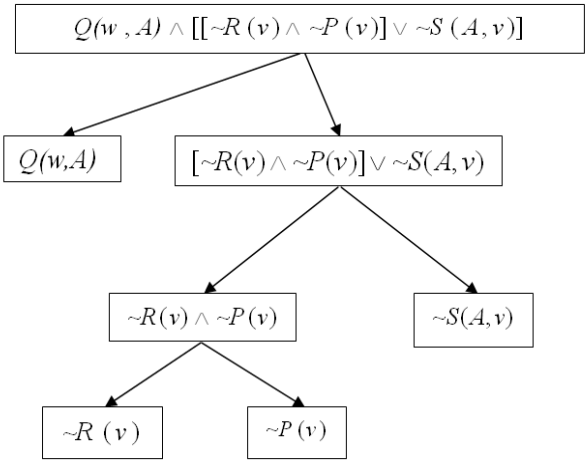


Рис. 1 – Гиперграф утверждений И/ИЛИ *(прямая продукция)*

Однако для наших целей более полезна обратная система продукций В этом случае решение строится от цели (используя правила) и согласуется с фактами, что соответствует в математике доказательству теоремы. Здесь рационально использовать гиперграфы иного вида, где конъюнкция описана k-связками, а дизъюнкция вообще не использует связок. Рассмотрим применение этого подхода на примере.

Докажем цель в следующей теореме:

Факты $R(A)$, (12)

$Q(A)$, (13)

Правила: П1: $R(y) \Rightarrow P(y)$, (14)

П2: $S(z) \Rightarrow P(B)$, (15)

Цель $P(z) \wedge Q(x)$. (16)

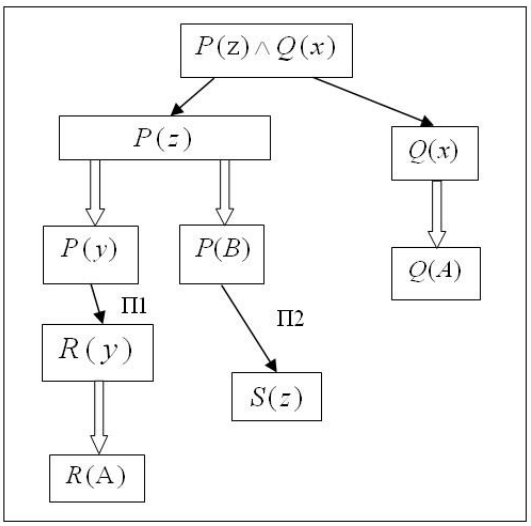


Рис. 2 – Исключение ветви графа при обратной системе продукций

По условиям теоремы две подцели $P(z)$ и $Q(x)$ должны быть непременно достигнуты. Поэтому здесь стоит к-связка (к = 2). Она связывает обе подцели в одну общую цель. В данном случае правила проще применять в виде импликации. Кроме того, правила применяются в обратном порядке, например, к литералу $P(z)$ - применяем развернутое наоборот правило $P(y) \Leftarrow R(y)$ (при условии когда $z = y$). Тогда новая подцель $R(z)$ и при $z = A$ она достигается, так как в базе данных имелся факт $R(A)$.

На правой ветви графа (Рис. 2) подцель $Q(x)$ аналогично достигается при подстановке $x = A$, так как имеется факт $Q(A)$.

Ветвь графа построенная на правиле П2 формируя новую цель $P(B)$, никак не достигается, но поскольку на общее решение это не влияет, то эта ветвь попросту отбрасывается. Решение включает левую и правую ветви графа, а среднюю ветвь, которая не согласуется – попросту удалим.

4 Переход к языку программирования «ПРОЛОГ»

Язык ПРОЛОГ – это язык «наследованный от математики» *(mathematically-derived languages).* Прологовские предложения бывают трех типов: факты, правила и вопросы.

• Факты содержат утверждения, которые являются всегда, безусловно истиной.

• Правила содержат утверждения, истинность которых зависит от некоторых условий.

• С помощью вопросов пользователь может спрашивать систему о том, какие утверждения являются истинными.

Предложения ПРОЛОГа состоят из головы и тела. Тело – это список целей, разделенных запятыми. Факты – это предложения, имеющие пустое тело. Вопросы имеют только тело. Правила имеют голову и (непустое) тело (пример, см. табл. 9).

Таблица 9 – Правила ПРОЛОГа *(пример)*

Предложения ПРОЛОГа	**Голова**	**Тело**
Факты Ф1 Ф2	 Родитель (том, боб) Родитель (боб, пат)	
Правила *пр1* *пр2*	 Предок (X, Z) :- Предок (X, Z) :-	 Родитель (X, Z). Родитель (X,Y), предок (Y, Z).
Вопрос		?- предок (том, пат).

В конце каждого факта точка. Факт - имя собственное. Переменные – имена нарицательные. Дизъюнкция – точка с запятой. Конъюнкция – запятая, имеет приоритет перед дизъюнкцией.

Сопоставление в ПРОЛОГе соответствует действию в логике, называемому унификацией. Существуют некоторые отличия от теории предикатов. Правила используют импликацию (ранее в теории предикатов от импликации уходили, здесь она остается). В ПРОЛОГе всегда применяют обратную продукцию. Рассмотрим процедуру резолюции, то есть создание нового предложения из цели G(A) и правила P(y) $\Rightarrow$ G(y). Здесь голова правила G(y), а тело правила (*условная часть*) P(y). При совпадении цели G(A) и головы правила G(y = A), обе убираются и остается только тело правила с заменой переменной (*конкретизация*). Это эквивалентно процедуре

$$G(x)\big|_{x\to y} \vee G(y) \vee P(y) \Leftrightarrow P(y). \qquad (17)$$

Кванторы представлены не явно. Комментарии: /* Это комментарий */ и % Это тоже комментарий %. Как задают вопросы? а) Простой вопрос: **? - родитель (боб, пат).** б) «Вопрос-ответ» *(это фактически доказательство теорем)*: **? - дед (альфонс, юля)**

-- --> да (18)

Программа начинает с целей и, применяя правила, подменяет текущие цели новыми, до тех пор, пока эти новые цели не окажутся простыми (*заданными*) фактами. То есть это обратная дедукция, ***позволяющая даже в условиях неуверенности в единственности решения, обеспечить выполнение именно указанной задачи.***

Процесс, в результате которого пролог-система устанавливает, удовлетворяет ли объект запросу, часто довольно сложен и включает в себя логический вывод, исследование различных вариантов и, возможно, *возвраты*. Все это делается автоматически самой ПРОЛОГ-системой и по большей части скрыто от пользователя.

Запятая между целями обозначает *конъюнкцию* целей: они *все* должны быть истинными. Однако в ПРОЛОГе возможна и *дизъюнкция* целей: должна быть истинной, *по крайней мере одна* из целей. Дизъюнкция обозначается точкой с запятой. Например: P :- Q; R. читается

так: P – истинно, если истинно Q *или* истинно R. Смысл такого предложения тот же, что и смысл следующей пары предложений**:** P :- Q и P :- R.

Порядок выполнения операций:

P :- Q, R. % P – истинно, если Q и R истинны. Из Q и R следует P %. (19)

Т.е., чтобы решить задачу P, *сначала* решите подзадачу Q, а *затем* – подзадачу R. Чтобы достичь P, *сначала* достигните Q, а *затем* R. Таким образом, различие между "декларативным" и "процедурным" прочтениями заключается в том, что последнее определяет не только логические связи между головой предложения и целями в его теле, но еще и ***порядок***, в котором эти цели обрабатываются. Всякий раз, как рекурсивный вызов процедуры вычислить приводит к неуспеху, процесс вычислений возвращается к ПРОСМОТРУ и продолжается с того предложения C, которое использовалось последним. Поскольку применение предложения C не привело к успешному завершению, пролог-система должна для продолжения вычислений попробовать альтернативное предложение.

В действительности система аннулирует результаты части вычислений, приведших к неуспеху, и осуществляет возврат в ту точку (предложение C), в которой эта неуспешная ветвь начиналась. Когда процедура осуществляет возврат в некоторую точку, все конкретизации переменных, сделанные после этой точки, аннулируются. Такой порядок обеспечивает систематическую проверку пролог-системой всех возможных альтернативных путей вычисления до тех пор, пока не будет найден путь, ведущий к успеху, или же до тех пор, пока не окажется, что все пути приводят к неуспеху.

Рассмотрим на примере, как ПРОЛОГ решает задачу, представленную в табл. 9 [20]. Система попытается достичь этой цели. Для того, чтобы это сделать, она пробует найти такое предложение в программе, из которого немедленно следует упомянутая цель. Очевидно, единственными подходящими для этого предложениями являются *пр1* и *пр2*.

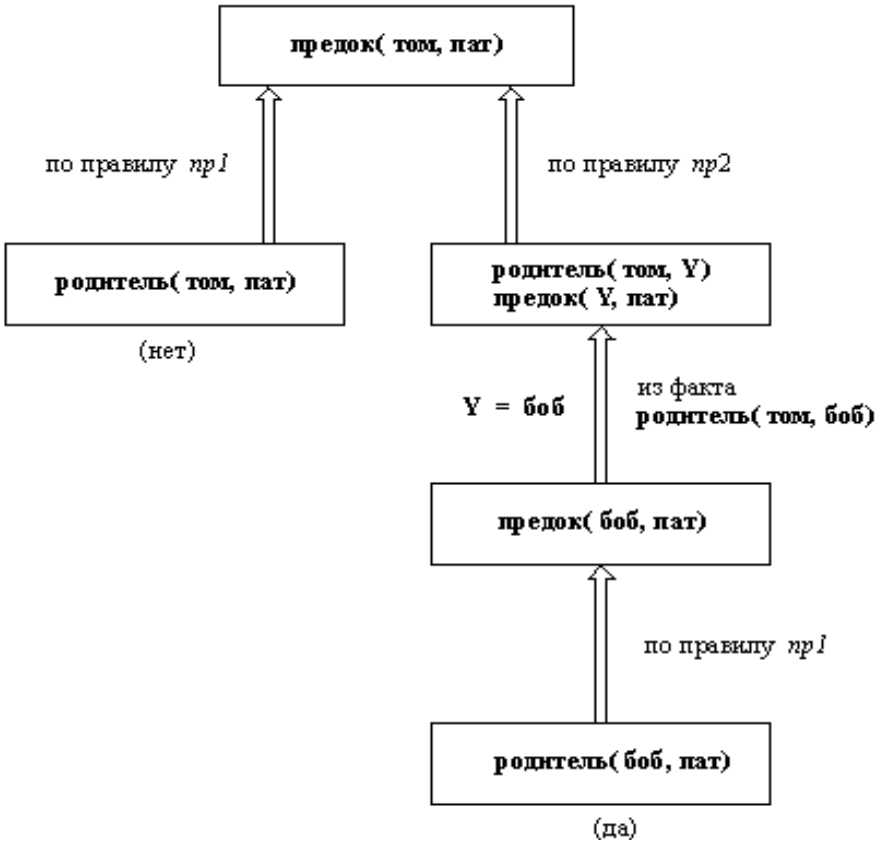


Рис. 3 – Граф задачи табл. 9 *(обратная продукция)*

Вначале система пробует предложение, стоящее в программе первым: **предок (X, Z):- родитель (X, Z)**. Поскольку цель – **предок (том, пат),** подходящие значения переменных **X = том, Z = пат**. Тогда исходная цель **предок (том, пат)** заменяется новой целью: родитель(том, пат). Однако в программе нет фактов и правила, головы которых были бы сопоставимы с целью **родитель (том, пат),** поэтому ***такая цель оказывается неуспешной***. Происходит ***возврат*** к исходной цели, чтобы попробовать второй вариант вывода цели верхнего уровня предок (том, пат).

Используем правило *пр2*. Как и раньше, переменным X и Z приписываются значения: **X = том**, **Z = пат**. В этот момент переменной Y еще не приписано никакого значения. Верхняя цель предок (том, пат) заменяется двумя целями: **родитель (том, Y), предок (Y, пат)**. Теперь перед собой *две* цели, система пытается достичь их в том порядке, каком они записаны. Достичь первой из них легко, поскольку она соответствует факту **родитель (том, боб)** из программы. Процесс установления соответствия – сопоставления (унификация) вызывает **Y = боб**. Тем самым достигается первая цель **родитель (том, боб)**, а оставшаяся превращается (из-за унификации) в **предок (боб, пат).** Для достижения этой цели вновь применяется правило *пр1*. Заметим, что это (второе) применение правила никак не связано с его первым применением. Поэтому система использует новое множество переменных правила всякий раз, как оно применяется. Чтобы указать это, мы переименуем переменные правила *пр1* для нового его применения следующим образом: **предок (X', Z') :-родитель (X', Z')**. Голова этого правила должна соответствовать нашей текущей цели **предок (боб, пат)**. Поэтому **X' = боб, Z' = пат**.

5 Заключение

Если исключить из обсуждения многочисленные победы машин в различных настольных играх, то наиболее интересным было сообщение, что экспертная система сама написала новеллу и эта новелла оказалась в числе десятка выбранных для окончательного конкурса ничего не подозревающим жюри. Правда в проекте, который длился с 2012 года, в компьютер вводились данные о сюжете, и о персонажах, а программа по специальной схеме *(разработанной командой профессора Хитоси Мацубарой из университета "Мирай" в Хакодате)* складывала уже самостоятельно все детали литературной конструкции. Хотя и здесь все как у людей. Вспомните замечательного писателя А. Дюма и в настоящее время немногих явных и множество неявных авторов многочисленных сериалов. Так что технология написания чужими руками придуманного и кратко сформулированного литературного произведения, хоть бы даже машиной, не нова.

Пока системы искусственного интеллекта способны только помочь нам решить некоторые не очень сложные задачи, где скорости реакции машин превосходят скорости реакции человек. Например, роботы в банковской системе позволяют при правильно составленной программе зарабатывать на колебаниях курсов валют и ценных бумаг. Человек вряд ли сможет с ними конкурировать, разве что в ситуациях, когда программы роботов окажутся бессильны. Некоторые виды умственной деятельности также можно переложить на плечи систем искусственного интеллекта. Но пока человеку придется самому справляться с многими задачами, ибо время роботов, способных заменить человека в многообразии жизненной деятельности еще не пришло. Внушает некоторый оптимизм только историческое объединение методов описания экспертных и нейронных систем [21] на базе нечеткой логики [22,23] и набирающий скорость прогресс в создании технических устройств элементов инфраструктуры.

В работе [24] была высказана гипотеза «необходимого развития»: любая эволюционирующая интеллектуальная система (в частности цивилизация или самообучающийся искусственный, или гибридный[1] суперинтеллект), все время усиливает свои интеллектуальные

[1] Возможность формирования планетарного интеллекта на базе глобальной сети, воздействовать на которую человечество не сможет, обсуждалось в работе [24].

ресурсы (т.е. подключаются все новые и новые блоки интеллектуальной сети) растет ее усложнение. И прежний объем обучающих задач и соответственно предложенных решений вскорости окажется недостаточным, в том смысле, что при этом возникают проблемы с формированием производных решений, растут рассогласования, которые воспринимаются как ошибки. Т.е. нарушается устойчивость картины мира. Единственным выходом здесь может быть увеличение объема известных знаний, которые обеспечивают эффективное обучение. Это увеличение может быть обеспечено наукой, расширением горизонта восприятия, доступом к новым источникам, выходом из замкнутого круга прежних понятий и представлений.

Но пока наукой в самом широком смысле вынуждены заниматься люди, пусть даже с помощью множества технических помощников. Смущает явное несоответствие скорости реакции природного нейрона и нейрона искусственной сети, то есть скорости отдельных операций вычислительных систем. Тем не менее скорость получения решения человеком частенько значительно превосходит скорость достижения результата у современных машин. Особенно в условиях одновременного решения многих задач. В чем же дело? Дело скорее всего в том, что мозг человека – это мегапроцессорная система. Одновременное подключение этого гигантского числа процессоров ускоряет получение решения в такое же, если не большее число раз. Поэтому все усилия исследователей полезно применить в области разработки мегапроцессорных систем новых поколений [24,25]. Важно также отметить, что освоение новых знаний у людей происходит порой даже непроизвольно. И когда мы хотим создать искусственную интеллектуальную систему, способную осознавать себя и понимать нас, и намерены заполнить ее базу данных и знаний, вот тут-то и возникают проблемы.

Во-первых, у человека масса знаний, которые он полагает известными (по умолчанию), машине все это надо разжевать и пояснить.

Во-вторых, заполнение базы данных машины должны делать эксперты, а их работа - высокооплачиваемая.

В-третьих, время, которое затрачивается на заполнение баз данных, а также проверку и перепроверку этого заполнения, достаточно значительное. Потому, пока не найдут эффективный машинный способ автоматического заполнения баз данных, или же не обучат эту интеллектуальную систему все это делать самостоятельно, дело быстрее не пойдет.

Самое интересное, что обнаружила цивилизация - это изучение природы и создание новых технологий, многократно усиливающих возможности людей, чтобы еще более успешно познавать мир и создавать то, что превращает жизнь в увлекательную игру. А как известно, ничего так более не привлекает людей, как игры и удовлетворение собственного любопытства, так свойственные природе человека.

Ссылки

[1] Newell A. The chess machine: an example of dealing with a complex task by adaptation / A. Newell // ACM. Proceedings of the 1955 Western joint computer conference. – 1955. – P.101 – 108.

[2] Newell A. GPS, program that simulates human thought / A. Newell, H. Simon // Defense Technical Information Center. – 1961. – Vol.4. – №10. – P. 109 – 124.

[3] Shannon C.E. A Mathematical Theory of Communication / C.E. Shannon // The Bell System Technical Journal. – 1948. – Vol. 27. – P.379 – 423; 623 – 656.

[4] Gotlob F. Izbrannye raboty / Frege Gotlob; Sost. V.V. Anashvili, A.L. Nikiforov; Per. s nem. V.V. Anashvili .– Moskva: Domintellektual, 1997. – 159 s.

[5] Turing A.M. On Computable Numbers, with an application to the Entscheidungsproblem / A.M. Turing // Proc. London Math. Soc. Ser. 2. – 1937. – Vol. 42. – P. 230-265.

[6] Newell A. Programming the Logic Theory Machine / A. Newell, F.C. Shaw // Proceedings of the Western Joint Computer Conference. – 1957. – P. 230-240.

[7] McCarthy J. Lisp 1.5 Programmer's Manual / J. McCarthy, P. Abrahams, D. Edwards et al. – MIT Press, Cambridge, Massachusetts. – 1962.

[8] Church A. Introduction to mathematical logic. Vol.1./ A. Church . – Princeton: Princeton University Press,1956. – 485 p.

[9] Robinson J. A. A Machine-Oriented Logic Based on the Resolution Principle / J. A. Robinson // Communications of the ACM. – 1965. – Vol. 12. – №1. – P. 23-41.

[10] Chang C.L. Symbolic Logic and Mechanical Theorem Proving / C.L. Chang, R.C.T. Lee. – New York: Academic Press,1973. – 331 p.

[11] Colmerauer A. Un système de communication enfrançais / Colmerauer Alain, Henry Kanoui, Robert Pasero et Philippe Roussel // Rapport préliminaire de fin de contrat IRIA, Groupe Intelligence Artificielle, Faculté des Sciences de Luminy, Université Aix-Marseille II, France, 1972.

[12] Herbrand J. Recherches sur la théorie de la demonstration / J. Herbrand // Travaux de la société des Sciences et des Lettres de Varsovie, Class III, Sciences Mathématiques et Physiques. – 1930. – Vol. 33.
[13] Pospesel H. Introdaction to Logic: Predicate Logic. Englewood Cliffs / H. Pospesel. – New Jersey: Prentice – Hall, 1976.
[14] Nil'son N. Printsipy iskusstvennogo intellekta / N. Nil'son; per. s angl. – Moskva: Radio i svyaz', 1985. – 376 s.
[15] Maslov S. An inverse method of establishing deducibility in classical predicate calculus / S. Maslov // Dokl. AN SSSR. – 1964. – Vol. 159. – P. 17–20; Proof-search strategies for methods of the resolution type // Machine Intelligence. – 1971. – N. 6. – P. 77 - 90.
[16] Van Vaalen J. An extension of unification to substitutions with an application to automatic theorem proving / J. van Vaalen // IJCAI. – 1975. – Vol.4. – P. 77–82.
[17] Sickel S. A search technique for clause interconnectivity graphs / S. Sickel // IEEE Trans. On Computers. C-25. – 1976. – № 8. – P. 823–835.
[18] Kőnig D. Theorie der endlichen und unendlichen Graphen / D.Kőnig. – Leipzig: Akademische Verlagsgesellschaf, 1936; per. s angl.: Theory of finite and infinite graphs. – Birkhäuser, 1990.
[19] Martelli A. From dynamic programming to search algorithms with functional costs / A. Martelli, U. Montanari // IJCA. – 1975. – Vol.4. – P.345-350; Optimizing decision trees through heuristically guided search // CACM. – 1978. – Vol.21. – № 12. – P. 1025–1039.
[20] Bratko I. Programmirovanie na yazyke PROLOG dlya iskusstvennogo intellekta / I. Bratko; per. s angl. – Moskva: Mir, 1990. – 560 s.
[21] Jang J.S.R. ANFIS: adaptive-network-based fuzzy inference system / J.S.R. Jang // IEEE transactions on systems, man, and cybernetics. – 1993. – Vol.23. – № 3. – P.665–685.
[22] Zadeh Lotfi A. Fuzzy sets / Lotfi A. Zadeh // Information and Control. – 1965. – Vol.8. – P. 338 – 353; Fuzzy sets and systems // System Theory; Fox J. editor. – Brooklyn, New York: Polytechnic Press, 1965. – P. 29–39.
[23] Kosko B. Fuzzy systems as universal approximation / B. Kosko // IEEE Transactions on Computers. – 1994. – Vol. 43. – № 11. – P. 1329–1333.
[24] Kuklin V. M. Vzglyad na budushchee planetarnoi tsivilizatsii / V. M. Kuklin // Universitates: Nauka i prosveshchenie. – 2003. – № 4 (16). – S. 18–22.
[25] Kuklin V. Will the artificial intelligence help us? / V. Kuklin // COMPUTER SCIENCE AND CYBERSECURITY. – 2016. – Issue 4(4). – P. 35–41 [Electronic Resource]. – Way of access: http://periodicals.karazin.ua/cscs/article/view/8266/7739.pdf.

Reviewer: Alexandr Potii, Dr. of Sciences (Engineering), Full Prof., V. N. Karazin Kharkiv National University, Kharkov, Ukraine.
E-mail: potav@ua.fm

Received: January 2017.

Author:
Vladimir Kuklin, Dr., Full Professor, head of the chair, V.N. Karazin Kharkiv National University, Kharkov, Ukraine.
E-mail: kuklinvm1@gmail.com

From mathematical logic to programming languages artificial intelligence.

Abstract. The paper considers the process of formation of the theory of expert systems on an example of formation of artificial intelligence programming language PROLOG. It showed a difficult path of awareness of artificial intelligence and the motives that led to the emergence of expert systems that are based on mathematical logic. We discuss the basic ideas and procedures that led to the construction of the first department of mathematical logic - predicates theory, representation of procedure on hypergraphs, and then to create a Prolog language. Progress has been made in the development of intelligent systems and the problems faced by researchers are discussed.

Keywords: Theory predicates, hypergraphs AND/OR, Prolog programming.

Рецензент: Олександр Потій, д.т.н., проф., Харківський національний університет імені В.Н. Каразіна, м. Харків, Україна.
E-mail: potav@ua.fm

Надійшло: Січень 2017.

Автор:
Володимир Куклін, д.ф.-м.н., проф., завідувач кафедри, Харківський національний університет імені В.Н. Каразіна, Харків, Україна. E-mail: kuklinvm1@gmail.com

Від математичної логіки до мов програмування штучного інтелекту.

Анотація. Розглянуто процес становлення теорії експертних систем на прикладі формування мови програмування штучного інтелекту ПРОЛОГ. Показаний складний шлях усвідомлення проблем штучного інтелекту і мотиви, які привели до появи експертних систем, побудованих на основі математичної логіки. Обговорюються основні ідеї і процедури, які привели до побудови спочатку відділу математичної логіки - теорії предикатів, поданням процедур цієї теорії на гіперграфах і потім до створення мови ПРОЛОГ. Відзначається прогрес у розвитку інтелектуальних систем та проблеми, що стоять перед дослідниками.

Ключові слова: теорія предикатів, гіперграфи І/АБО, мова програмування ПРОЛОГ.

UDC 004 056 55

PROPOSALS OF COMPARATIVE ANALYSIS AND DECISION MAKING DURING THE COMPETITION REGARDING THE CERTAIN BENEFITS OF ASYMMETRIC POST QUANTUM CRYPTOGRAPHIC PRIMITIVES

I. Gorbenko, Yu. Gorbenko, M. Yesina, V. Ponomar

V.N. Karazin Kharkiv National University, Svobody sq., 4, Kharkov, 61022, Ukraine
gorbenkoi@iit.kharkov.ua; gorbenkou@iit.kharkov.ua; rinayes20@gmail.com; laedaa@gmail.com

Reviewer: Roman Oliynikov, Dr., Full Professor, V.N. Karazin Kharkiv National University, Svobody sq., 4, Kharkov, 61022, Ukraine
roliynykov@gmail.com

Received on February 2017

Abstract. *The paper considers proposals on the implementation of cryptographic primitives comparative analysis and substantiation, development and experimental confirmation of methodical bases application possibilities of system unconditional and conditional criteria selection and application, and methods and technique of comparative analysis and making the decision on asymmetric post quantum cryptographic primitives type directional encryption, and keys encapsulation and electronic signatures mechanisms. Some criteria and indicators that can be used for comparative analysis of properties of the candidates for the post quantum cryptographic primitives are presented. Comparative analysis of the existing mechanisms of perspective electronic signatures in accordance with ISO/IEC 14888-3:2016 standard and some cryptographic primitives that are considered possible to use in the post quantum period is carried out. The results of the cryptographic primitives conducted estimation are presented. Conclusions and recommendations on the use of certain cryptographic primitives estimation methods are made.*

Keywords*: electronic signature mechanisms analysis, weight indices, electronic signature, electronic signature estimation criterion, electronic signature comparison analysis methods.*

1 Introduction

In 2016 there were the series of important events, that have significantly affected to the intensive development of post quantum cryptography. To them should be referred the statement on the Internet – Alfred J. Menezes and Neal Koblitz articles [7], organization and conduction by NSA and NIST USA VII international conference on post quantum cryptography, which took place in February 2016 in Japan [12,14]. An extremely important event was the publication in the USA report «Report on Post – Quantum Cryptography. NISTIR 8105 (DRAFT)» [9], in which fully confirmed the possibility of electronic signatures (ES) asymmetric cryptographic systems successful quantum and the main cryptanalysis, problems and opportunities, and stages of their decision are identified.

NIST USA announced a competition to develop the standards of post quantum asymmetric cryptographic primitives [12], understanding the need to find new electronic signature asymmetric cryptographic primitives and asymmetric end-to-end encryption, which will be relevant and can be applied in post quantum period. The specified one due to two factors. First, there is significant progress in the development of quantum computers, including experimental demonstration of physical qubits realization are carried out, which can be scaled up to larger systems.

Second, likely transition to post quantum cryptography will not be easy, because it is unlikely to be a simple replacement of the current asymmetric cryptographic primitives standards. Significant efforts will be needed to develop, standardize and implement a new post quantum cryptosystems. Therefore, should be a significant transition stage, when as current and post quantum cryptographic primitives are used.

Proposals must be received by NIST to November 30, 2017. Filed proposals received before September 30, 2017 will be considered in terms of fulfillment of requirements completeness, and then pass through the stages of open civil research and standardization according to the announced requirements [12,14]. They shall apply to: directional encryption (E2EE) asymmetric mechanisms, keys encapsulation (KE) and electronic signature (ES). But a preliminary analysis of a creation

condition of a quantum computer and its capabilities in the future also confirms the previous list and essence of requirements announced by NIST.

The specified one, in our view, requires special attention to the selection estimation and comparing crypto primitives criteria and indicators, that would allow to take into account all the announced requirements and, if necessary, extend or narrow them.

The European Union has also started the preparation of a new post quantum standards. A new direction "Quantum-Safe Cryptography" are formed by European Organization for Standardization ETSI in the cluster "Security" [3,10,15]. According to the results of these studies are predicted the groups standards for post quantum period adoption. ETSI has published a group report "Quantum-Safe Cryptography. Quantum-Secure infrastructure" [3], in which fixed bases of perspective infrastructure, provided mechanisms, described primitives types, that will be used. Separately requirements are nominated and estimation criteria are formed for future candidates.

ES and E2EE, and their application mechanisms are allocated among the set of asymmetric cryptographic primitives. The specified one is explained by their wide application in a significant number of applications and potential large losses in case of discrediting ES and E2EE, that are used at present [4-6, 8].

Our experience obtained during the conducting research on projects AES and NESSIE [1,11], and in national standards for hash function DSTU 7564:2014 developing and adopting, and block symmetric encryption algorithm DSTU 7624:2014 [4,8] etc., allows to conclude, that the extremely important problem is substantiation of the estimation criteria system choice and comparison of each cryptographic primitives with other, and development and application the scientifically based techniques of them analysis and comparison in accordance with the nominated requirements. These methods and developed on their basis technique or techniques should take into account all requirements, that are nominated for asymmetric cryptographic primitives and allow to help make the decision about winners based on use the unconditional and conditional criteria system, as partial and integral.

The objective of these proposals are the substantiation, development and experimental confirmation of methodical bases application possibilities of system unconditional and conditional criteria selection and application, and methods and technique of comparative analysis and making the decision on asymmetric post quantum cryptographic primitives type directional encryption, and keys encapsulation and electronic signatures mechanisms.

2 The state of cryptographic primitives comparative analysis techniques development and application

After analysis, it was determined that the first time techniques of estimation and comparative analysis of cryptographic primitives type block symmetric cipher (BSC), streaming symmetric cipher (SSC), electronic signature (ES) and cryptographic protocol were proposed in [22,25], and detailed in [24]. They are based on the use of unconditional and conditional partial and integral criteria system, and indicators, that allow to assess the degree of nominated to the candidate requirements fulfillment. In our opinion the main task of these techniques are the formalization of decision-making processes regarding fulfillment of nominated to them requirements, taking into account the strengths and weaknesses of cryptographic primitives, that are candidates for the post quantum standard, reduce the influence of subjective factors in decision-making,. For example, following techniques can be applied to estimate and compare the ES, E2EE and KE mechanisms, which are the candidates for the post quantum standard in our case.

At the formal level such estimation and comparison techniques ES, E2EE and KE mechanisms can be summarized. But, since to these crypto primitives are nominated different requirements, then for each of the primitives they may be supplemented or simplified and display the entire spectrum of nominated requirements. Also, these techniques can ensure transparency of decision-making, experts independent, and help substantiate making appropriate decisions and confidence in them. Further in research technique we'll mean a fixed set of methods, methods of practice, tested and studied for the expedient implementation of specified work, that leads to a predetermined outcome [24].

In research in the broad sense we'll mean the search of new knowledge or a systematic investigation in order to establish the facts. In a narrow sense this is the scientific method (process) of study anything.

3 Criteria and indexes of cryptographic primitives ES and E2EE estimation

In criterion we'll mean the sign based on which estimate, determination or classification of anything are carried out [24], that is, in fact, we'll mean a measure of estimate. Our previous researchers have allowed to conclude, that cryptographic primitives comparison can be done using two criteria sets: unconditional and conditional [24]. This approach allows to make an estimate and compare the crypto transformations, that are candidates, in 2 stages. This approach is based, in particular, and on taking into consideration or use expert estimates.

At the first stage, at first checked the crypto transform conformity for the partial unconditional criteria system, and then unconditional integral criterion is calculated for each crypto primitive based on partial criteria. At the second stage appropriate estimates are obtained using at first partial conditional criteria system, and then integral conditional criterion is calculated on their base.

This two-step approach allows to reject crypto transformations, that do not meet the unconditional requirements, i.e. requirements, that must be fulfilled unconditionally. Moreover integral unconditional criterion allows to accept the decision regarding each of crypto primitives.

The partial conditional criteria using, and then integral conditional criterion using on their base, allow to estimate the crypto primitive quality in a broad sense, as the quality in average, and then compare crypto primitives, that are candidates for the post quantum algorithm, using the value of the integral criterion for each of crypto primitives. Estimation indexes of ES and E2EE asymmetric crypto transformations by unconditional criteria, that are recommended for use, is given further.

3.1 Unconditional estimation criteria of cryptographic transformations

To unconditional criteria will refer those criteria, which fulfillment is mandatory for cryptographic primitive, that is unconditional. Moreover, in our view, for asymmetric crypto transformations type ES and E2EE you can select the same unconditional criteria system. But this does not preclude the consideration possibilities of requirements features and according to the choice in the analysis and estimation of cryptographic primitives additional partial unconditional criteria. Let's consider and choose at first the partial unconditional criteria system, based on the NIST requirements [12,14].

Requirements analysis, that are nominated by NIST for asymmetric cryptographic transformation type ES and E2EE partial unconditional criteria, our experience in the development and estimation of crypto transformations type ES, BSC, SSC etc. properties [24], achieved results in the practical solution of cryptanalysis problems, including based on quantum cryptanalysis algorithms implementations [24], allow to choose unconditional estimation criteria ES and E2EE at least, listed in Table 1.

As the listed partial criteria are unconditional, then the selection criterion is a logical variable yes/no (1/0), so the unconditional criterion can be written as:

$$(W_1,\ W_2,\ W_3,\ W_4,\ W_5,\ W_6,\ W_7,\ W_8) \in (1,0). \quad (1)$$

In view of described above partial unconditional criteria W1–W8 and condition (1), the crypto transformation compliance function to requirements, that are set out above, written as integral unconditional criterion:

$$fi() = W_1 \wedge W_2\,(W_3) \wedge W_4 \wedge W_5 \wedge W_6 \wedge W_7 \wedge W_8 = W_\delta, \quad (2)$$

where the symbol «∧» indicates the Boolean variables conjunction operation according to (1). It should be noted that in (2) W_3 is taken in parenthesis, that should be used either W_2 or W_3.

Table 1 – Unconditional estimation criteria of ES and E2EE

№	Unconditional criteria	Denotation
1	Reliability, simplicity and transparency of mathematical base (mathematical transformations) used in the implementation of post quantum cryptographic transformations ES and E2EE.	W1
2	Practical security of E2EE type cryptographic transformations in the mechanism "semantically secure encryption" implementation against known attacks using a quantum computer and cryptanalyst access to the 264 selected ciphertexts for security model IND–CCF2.	W2
3	Practical security of ES type cryptographic transformations against known attacks using a quantum computer and cryptanalyst access to the 264 selected ciphertexts for security model EUF–CMA.	W3
4	The validity of real security (stability) ES or E2EE cryptographic transformations against all known and potential cryptanalytic attacks of post quantum period based on the use of common parameters and keys with the necessary size and properties (128-bit keys and more classical stability (safety)).	W4
5	Theoretical security of ES or E2EE type cryptographic transformations in post quantum period against existing force, analytical and special attacks for existing threats models (at least for the model EUF-CMA for ES and IND-CCF2 for E2EE).	W5
6	The possibility of replacing existing standardized cryptographic primitives to the post quantum ones and application in the existing cryptographic systems and protocols in certain conditions and restrictions.	W6
7	Computational efficiency – complexity of direct I_{dir} and reverse I_{rev} cryptographic transformations ES and E2EE, and generating asymmetric key pairs I_{key} is not above polynomial, providing the necessary complexity (performance) values I_{dir}, I_{rev}, I_{key} in practical use in applications with their hardware and software, and program implementation.	W7
8	The performance of limitations for minimum and maximum lengths of private and public key, sizes and unprofitability of ciphertext and ES, the absence of weak private keys for post quantum period security models.	W8

That is, the post quantum cryptographic transformation ES and E2EE quality can be estimated using the integral unconditional criterion – compliance function as integral unconditional criterion

$$f_i() = 1, \tag{3}$$

if cryptographic transformation ES and E2EE corresponds to demanded requirements and

$$f_i() = 0, \tag{4}$$

if cryptographic transformation ES and E2EE does not correspond to demanded requirements.

Thus, according to (1–4) can formalize the decision according to the candidate conformity for post quantum type ES and E2EE cryptographic transformation to nominated for it demands. Thus, if the condition (3) is carried out, the crypto primitive is corresponding to the unconditional requirements, otherwise, that is when we get (4), then the corresponding crypto primitive does not meet the requirements and it is rejected from the further consideration.

3.2 Conditional estimation criteria of cryptographic transformations ES and E2EE

Qualitative and quantitative comparison of type EP and E2EE cryptographic transformations can be carried out using preferences partial conditional and generalized conditional criterion [22, 24, 25]. Table 2 provides a list and designations of estimating partial conditional criteria of type ES and E2EE cryptographic transformations, whose requirements are nominated by NIST [12,14].

Table 2 – Conditional estimation criteria of ES and E2EE

№	Conditional criteria	Denotation
1	Additional security features: - perfect forward secrecy; - resistance to side-channel attack; - resistance to multi-key attacks; - resistance to failures.	K1
2	Stability requirements 1) classic security 128-bit / 64-bit quantum protection (stability reserve AES-128); 2) classic security 128-bit / 80-bit quantum protection (stability reserve SHA-256/ SHA3-256); 3) classic security 192-bit / 96-bit quantum protection (stability reserve AES-192); 4) classic security 192-bit / 128-bit quantum protection (stability reserve SHA-384/ SHA3-384); 5) classic security 256-bit / 128-bit quantum protection (stability reserve SHA2-512, SHA3-512);	K2
3	Additional requirements to stability 6) classic security 512-bit / 256-bit quantum protection (stability reserve SHA-512/ SHA3-512, DSTU 7564: 2014 – 512 bit); 7) classic security 512-bit / from 128-bit to 256-bit quantum protection (stability reserve DSTU 7624:2014 (Kalyna – 512)); 8) classic security 512-bit / quantum protection (stability reserve DSTU 7624:2014 (Kalyna – 512)).	K3
4	Encryption errors. The low percentage of encryption errors.	K4
5	The possibility of multiple E2EE or ES.	K5
6	Flexibility: 1) additional scheme options (optimization, implicit keys exchange etc.); 2) cross-platform; 3) the possibility of parallelization.	K6
7	Correctness verification. Checking the correctness of basic and optimized implementations.	K7

Continuation of Table 2

№	Conditional criteria	Denotation
8	Effectiveness verification: Calculation of time needed for key generation, encryption, decryption, digital signature, signature verification or keys establishing (testing is carried out on optimized versions).	K8
9	Test conditions The main platforms: 1) NIST PQC Reference Platform; 2) Intel x64; 3) Windows or Linux, the GCC compiler; 4) Additional testing of other conditions (8-bit processors, digital signal processors, dedicated CMOS etc.)	K9
10	Possibility and conditions of free distribution post quantum crypto transformations ES or E2EE.	K10
11	Confidence level to the post quantum crypto transformations ES or E2EE at different levels of use.	K11
12	Perspective and justification the use of post quantum crypto transformations ES or E2EE.	K12

As basic components of the generalized preferences criterion proposed to use such partial conditional criteria as shown in Table 2.

4 The partial unconditional criteria and integral unconditional criterion calculation

At the first stage the estimation and verification of post quantum crypto primitives ES and E2EE mechanisms is carried out by partial unconditional criteria and integral unconditional criterion. Partial unconditional criteria are defined by the data, given in Table 1. Estimates are made using the criteria given in Table 1, using the expert estimates methods. Unconditional criteria values are received as a result of expert estimates

$$(W_1, W_2(W_3), W_4, W_5, W_6, W_7, W_8), \quad (5)$$

that take the binary values 1 or 0 (yes/no). Integral unconditional criterion is determined based on these values according to (2)

$$f(W_1, W_2(W_3), W_4, W_5, W_6, W_7, W_8) \quad (6)$$

In the integral unconditional criterion $f() = 1$ post quantum cryptographic primitive passes the test and verification, otherwise, in the integral unconditional criterion $f() = 0$, it is rejected and is not considered further.

Introduced so integral criterion allows to establish, whether the considered type ES or E2EE crypto transformation is responded to nominated unconditional requirements. In case of positive estimation ES or E2EE by integral unconditional criterion, their subsequent comparison and estimation can be made on the basis of partial conditional criteria and as a result, integral conditional criteria [20]. It should be noted that in (5) and (6) W_3 is taken in parenthesis, that should be used either W_2 or W_3.

5 Expert estimation methods

In expert estimates understand the search method and the result of applying the method, that obtained based on the use of personal expert opinion or collective expert group opinion, and a set of logical and mathematical procedures aimed at obtaining information from specialists, its analysis and generalization in order to prepare and making rational decisions [19, 20].

5.1 The expert estimations method application

Application of the expert estimates method generally associated with the implementation of the experts selection procedures, the experts selection and establishment the expert opinion consistency degree.

Expert estimation methods used in situations, when the choice, substantiation and estimation of decisions cannot be made based on accurate calculations [19].

The expert estimates results statistical processing similar to measurement results statistical processing. On the expertise reliability significantly influenced such factors as the expert group size, the experts competence level, the questions composition, offered to experts, etc. [19].

Individual expert estimates also bear the stamp of chance; mood, health, environment, and knowledge and expert experience.

5.2 The experts selection procedure

Expert – a competent person to produce the estimate, that has special experience in a particular area and participating in the research as sources of information [19].

Among the a priori estimation methods of experts quality are the widespread self-concept methods as the most simple in mathematical terms. In this methods group, each expert evaluates himself on any scale – point or verbal-numerical. One of the main problematic tasks by this estimation is the problematic task of same understanding the scales grading by experts.

A variety of self-assessment is a differential method, which usually the estimate is given by the two criteria groups, that characterize expert acquaintance with expertise objects and by criteria, and expert introduce with the main information sources in this area.

It is possible to determine the level of expert competence in mutual estimation. In a simpler case, each expert from the given experts group indicates the list of experts, whom he considers as competent in this area. Coefficient expert competence is defined as the ratio of the lists number, in which is given expert, to the total lists number. This method allows to receive the increased experts estimates.

Another approach consists in the mutual estimating by experts of each other: q_{ij} – estimate in points of the i-th expert. The combination of these estimates forms the definitely orderly matrix. The consistent application of the same procedure to this matrix and interim values vector of competence estimates, obtained in the previous step, gives the finite values vector of experts competency estimates in the result [19]. Another approach based on the fact, that the expert competence must be estimated by how its assessment coordinated with estimates of most.

An effective means of experts estimating is the test method. It is important the following testing moments [19]:

1 - test should be designed for specific expertise objects;

2 - it is necessary the scale, that allows to determine the expert estimates accuracy degree;

3 - the probability of random guessing the true estimate by expert in text experiment should be sufficiently small.

In the case of test method can achieve the simplification, if it is enough data about results of specialist participation in similar expertise. In this case, about the expert competence can be judged on relative to the number of "accurate" estimates are made by him, to the total number of estimates are rendered by him.

Thus, there are several possible experts choice variants. Variant choice depends on how accurate should be estimate and on the complexity of the estimation procedure.

5.3 The experts selection

Depending on the problem task scale, that is solved, the expertise organization is carried out by a person, who makes the decision or management group is designed by him. The selection of quantitative and qualitative experts composition is carried out based on the analysis of problem task breadth, required estimates reliability, experts characteristics and resource costs [19].

The latitude of solved problematic task determines the need for involvement in expertise specialists from different fields. However, the minimum number of experts is determined by quantity of various aspects and directions, that need to be taken into account when deciding the problematic task.

The reliability of experts group estimates depends on the knowledge of individual experts and the number of experts in the group.

The spending resources on the expertise is proportional to the number of experts. Usually to the estimation are attached 5–12 experts [19]. Characteristics of the experts group are determined by the individual experts characteristics: competence, creativity, relevance to the expertise, conformity, thinking constructive, collectivism, self-criticism [19].

Competence – the degree of expert qualification in a particular field of knowledge.

Conformity – propensity to authorities influence.

Relevance to the expertise – negative or passive specialist attitude to solve the problematic task, high employment and other factors significantly effect to the experts functions performance.

Thinking constructive – pragmatic aspect of thinking.

Collectivism – should be taken into consideration during the open discussions.

Self-criticism –it is manifested in the self-concept degree of own competence and taking into account other experts opinions and decision making of this problematic task.

5.4 The expert opinions coherence degree establishing

In case of participation in the survey several experts, discrepancies in their estimates are inevitable, but the value of this difference is important. Group estimate can be considered sufficiently reliable only on condition of good coordination the individual professionals responses.

For analysis of estimates scatter and coherence used statistical characteristics – the measures of scatter or statistical variation [19,21].

5.5 The algorithms ES and E2EE estimation by conditional criteria

In case of a positive estimate of cryptographic transformation ES or E2EE by integral unconditional criterion, further comparison and estimation can be made based on determination the conditional criteria (Table 2) and their comparison by integral conditional criterion.

The main method of calculating the integral conditional criterion value is the partial conditional criteria clotting in integral conditional criterion. As the main methods of partial conditional criteria clotting can choose the analytic hierarchy process based on pairwise comparisons or method of determining the weight indices [20].

6 The analytic hierarchy process based on pairwise comparisons and features of its application for estimation ES and E2EE

For application the analytic hierarchy process must choose conditional criteria and indicators system for getting the values according to conditional criteria. With this set of indicators, means the use of conditional criteria can calculate the integral conditional criteria value and, as a result, make the ES or E2EE comparison by conditional integral criterion.

The method pairwise comparison essence consists in the following [2,20]. The set of pairwise comparisons matrices is constructed. Pairwise comparisons are carried out in terms of the dominance one element over another. Obtained opinions are expressed in integers, taking into account the scale, for example, the used nine.

6.1 The essence and conditions of use the pairwise comparisons method in cryptography

In pairwise comparison the expert compares researched objects of their importance in pairs, sets the most important object in each pair. All possible objects pairs expert represents in a record of each combination (object 1–object 2, object 2–object 3, etc.) or in the matrix form [18,20].

The method of pairwise comparisons is very simple and it allows to explore a large number of objects (compared, for example, by ranking method) and with greater accuracy [20].

Let $E_1,E_2,...,E_n$ – plenty of n elements (alternatives) and $v_1,v_2,...,v_n$ – according to their weight or intensity. Let's compare pairwise weight or intensity of each element with weight or intensity of any other element of the set relative to the total for them property or goal (relative to the element–"father").

When constructing a pairwise comparisons matrix for all criteria is necessary to determine the coherence ratio [20] for each criteria as follows.

The estimate of the eigenvector component calculated by the formula:

$$q_i = (W_{yi} \times W_{yi+1} \times \ldots \times W_{yn})^{\frac{1}{n}}. \quad (7)$$

Normalized estimate of priority vector calculated by the formula:

$$r_i = q_i \div z, \quad (8)$$

where z – matrix coherence ratio, calculated by the formula:

$$z = \sum_{i=1}^{n} q_i \ . \quad (9)$$

Matrix coherence ratio value is in the range $[0, \sum_{i=1}^{n} q_{i\max}]$, where $q_{i\max}$ – the maximum possible eigenvector component estimate value for selected case.

Let's further consider the results of cryptographic primitives estimation by this estimation method on the ES ISO/IEC 14888-3:2016 algorithms example.

7 Method and suggestions of the estimation and ES comparative analysis based on the weight indices

7.1 General formulation of the comparative analysis problem

The other class of clotting partial conditional criteria in the integral conditional criterion methods are formalized methods based on defined weight indices. Preliminary analysis is shown that most of them can be applied essentially to clotting the private conditional indicators [13,16,20,21]. Let's consider them on an example ES algorithms ISO/IEC 14888-3:2016 similarly as in section 6 (it is clear for what reasons cannot be considered post quantum crypto primitives ES and E2EE, because they do not exist in the approved form).

Let need to estimate the ES set according to the specified standard [4,5], which consists of:

1) k ES algorithms, which is necessary to estimate;
2) m indicators, by which each of ES alternatives are estimated;
3) n experts, which conducts ES estimation.

As partial indicators can be used indicators similar to partial conditional criteria specified above.

We can distinguish the following methods of weight indices:

- weight indices and ES estimation using the Fishburn scale;
- weight indices and ES estimation based on the ranking method;
- weight indices and ES estimation based on the points attribution method;
- weight indices and ES estimation based on the numerical method.

Let's consider and compare the mentioned methods by an integral conditional criteria ultimately.

7.2 The method of determining weight indices and ES estimation using the Fishburn scale

In the method of weight indices and ES estimation using the Fishburn scale the following steps are carried out.

1. Every indicator x_i, $i=1,...,m$ is assigned an estimation of its importance. Then the system of weights is constructed so that [20,21]

$$\begin{cases} \sum_{i=1}^{m} a_i = 1, \\ a_i \geq 0, i = 1,....,m \end{cases}, \quad (10)$$

where a_i – i-th indicator weights, i – indicator number, m – indicators quantity.

2. Indicators are ranked by the importance decreasing of each, so that:

$$x_1 \succ x_2 \succ x_3 \succ ... \succ x_i \succ ... \succ x_m .$$

3. Weight indices using the Fishburn scale are determined:

$$a_i = \frac{2 \cdot (m - i + 1)}{m \cdot (m+1)}. \quad (11)$$

4. The weight indices value and their average value are entered in Table 3, where $\overline{a_i}$ – weight indices arithmetic average for the i-th indicator, and $w_i = \overline{a_i}$ – weight indices values.

Table 3 – The weight indices value and their average value

Indicators / Experts	x_1	x_2	…	x_m
1	a_{11}	a_{12}	…	a_{1m}
2	a_{21}	a_{22}	…	a_{2m}
…	…	…	…	…
n	a_{n1}	a_{n2}	…	a_{nm}
w_i	w_1	w_2	….	w_m

7.3 The method of determining weight indices and ES estimation based on the ranking method

In the method of weight indices and ES estimation based on the ranking method the following steps are carried out.

1. The most important indicator corresponds to rank (estimate) m, the following – (m-1) and etc., the rank equals to 1, is the least important indicator. Then, the weight indices are determined by the formula [16,20]:

$$w_j = \frac{r_j}{\sum_{j=1}^{m} r_j}, \quad j = 1,...,m, \quad (12)$$

x_m – m-th indicator, r_j – j-th rank (estimate), n – experts quantity, m – indicators quantity.

2. Results of the experts survey are written in Table 4. In the penultimate string of this table ranks sum (estimates) is written, that have been exposed by experts, and in the last string of table indicators weight indices values are recorded. According to the estimation rules in accordance with specified method, we build the table for indicators and tables for all ES algorithms.

Table 4 – The weight indices value

Experts \ Indicators	x_1	x_2	…	x_m
1	r_{11}	r_{12}	…	r_{1m}
2	r_{21}	r_{22}	…	r_{2m}
…	…	…	…	…
n	r_{n1}	r_{n2}	…	r_{nm}
$r_j = \sum_{i=1}^{n} r_{ij}$	r_1	r_2	…	r_m
w_j	w_1	w_2	….	w_m

7.4 The method of determining weight indices and ES estimation based on the points attribution method

1. In method of determining weight indices and ES estimation based on the points attribution method first experts, depending on the importance indicator, give grades from 0 to 10, whereby it is permitted to estimate the indicator importance by fractional values, as well as the various indicators can attribute the same points [13,16,20].

2. It is determined the each indicator weight, calculated by each expert [20]:

$$r_{ij} = \frac{h_{ij}}{\sum_{j=1}^{m} h_{ij}}, \tag{13}$$

where r_{ij} – j-th indicator weight, defined by i-th expert, h_{ij} – i-th expert point, exhibited j-th indicator, n – experts quantity, m – indicators quantity.

3. The final indicators weight indices are determined by the formula [20]:

$$w_j = \frac{\sum_{i=1}^{n} r_{ij}}{\sum_{j=1}^{m}\sum_{i=1}^{n} r_{ij}}. \tag{14}$$

All obtained values are entered to the table (Table 5).

7.5 The method of determining weight indices and ES estimation based on the numerical method

The method of weight indices and ES estimation based on numerical method is implemented so.

1. For each indicator is calculated the relative scatter ratio by the formula [20]:

$$\delta_i = \frac{x_{i\max} - x_{i\min}}{x_{i\max}}, \tag{15}$$

where $x_{i\max}$, $x_{i\min}$ - in accordance with the max and min i-th indicator value, m - indicators quantity.

Table 5 – The weight indices value

Indicators / Experts	x_1	x_2	…	x_m	$\sum_{j=1}^{m} h_{ij}$	Indicators weights r_{i1}	r_{i2}	…	r_{im}
1	h_{11}	h_{12}	…	h_{1m}	$\sum_{j=1}^{m} h_{1j}$	$r_{11}=\frac{h_{11}}{\sum_{j=1}^{m} h_{1j}}$	$r_{12}=\frac{h_{12}}{\sum_{j=1}^{m} h_{1j}}$	…	$r_{1m}=\frac{h_{1m}}{\sum_{j=1}^{m} h_{1j}}$
2	h_{21}	h_{22}	…	h_{2m}	$\sum_{j=1}^{m} h_{2j}$	$r_{21}=\frac{h_{21}}{\sum_{j=1}^{m} h_{2j}}$	$r_{22}=\frac{h_{22}}{\sum_{j=1}^{m} h_{2j}}$	…	$r_{2m}=\frac{h_{2m}}{\sum_{j=1}^{m} h_{2j}}$
…	…	…	…	…	…	…	…	…	…
n	h_{n1}	h_{n2}	…	h_{nm}	$\sum_{j=1}^{m} h_{nj}$	$r_{n1}=\frac{h_{n1}}{\sum_{j=1}^{m} h_{nj}}$	$r_{n2}=\frac{h_{n2}}{\sum_{j=1}^{m} h_{nj}}$	…	$r_{nm}=\frac{h_{nm}}{\sum_{j=1}^{m} h_{nj}}$
					$\sum_{i=1}^{n} r_{ij}$	$r_1=\sum_{i=1}^{n} r_{i1}$	$r_2=\sum_{i=1}^{n} r_{i2}$	…	$r_m=\sum_{i=1}^{n} r_{im}$
					w_j	$w_1=\frac{r_1}{\sum_{j=1}^{m} r_j}$	$w_2=\frac{r_2}{\sum_{j=1}^{m} r_j}$		$w_m=\frac{r_m}{\sum_{j=1}^{m} r_j}$

2. The indicators value is determined by any of the above methods.

3. The weight indices get the most important value for those indicators, those relative scatter is more significant. All obtained data are entered to the table (Table 6).

Table 6 – The weight indices value

Indicators / Estimation	x_1	x_2	…	x_m
$x_{i\min}$	$x_{1\min}$	$x_{2\min}$		$x_{m\min}$
$x_{i\max}$	$x_{1\max}$	$x_{2\max}$		$x_{m\max}$
δ_i	δ_1	δ_2	….	δ_m
w_i	w_1	w_2	….	w_m

4. The indicators values are found by any one of the above methods.

$$w_i = \frac{\delta_i}{\sum_{i=1}^{m} \delta_i}. \qquad (16)$$

7.6 The ES mechanisms research results analysis according to the conditional integral criteria

The listed above results were obtained by selected ES algorithms estimation methods. The comparison of ES algorithms was made based on expert estimates. After that calculations were made by aforementioned methods.

It is believed that the results of ES algorithms estimation by various methods of weight indices were obtained almost identical – almost the same ES algorithms order from the best to the worst.

Numeric scatter of weight indices values for one algorithm is negligible, only numeric values for ES algorithms IBS-1,2 in the analytic hierarchy process based on pairwise comparisons different from weight indices values for these ES algorithms by other estimation methods. This is conditioned by more strong influence of subjective expert opinion on estimates result in a certain method. Table 7 shows the results of ES algorithms estimation by all estimation methods. Figure 1 shows graphically the results of ES algorithms estimation by various methods.

Table 7 – The results of ES algorithms estimation

Pairwise comparisons method	Methods of determining weight indices			
	using the Fishburn scale	based on the ranking method	based on the points attribution method	based on the numerical method
IBS-1 – 0,256 IBS-2 – 0,256 EC-KCDSA – 0,144 EC-GDSA – 0,125 EC-DSA – 0,099 EC-SDSA – 0,048 EC-FSDSA – 0,048 EC-RDSA – 0,025	IBS-1 – 0,159 IBS-2 – 0,159 EC-DSA – 0,15 EC-GDSA – 0,147 EC-KCDSA – 0,142 EC-FSDSA – 0,118 EC-SDSA – 0,117 EC-RDSA – 0,106	IBS-1 – 0,147 IBS-2 – 0,147 EC-KCDSA – 0,143 EC-GDSA – 0,142 EC-DSA – 0,139 EC-FSDSA – 0,115 EC-SDSA – 0,111 EC-RDSA – 0,103	IBS-1 – 0,137 IBS-2 – 0,137 EC-RDSA – 0,132 EC-FSDSA – 0,128 EC-DSA – 0,127 EC-SDSA – 0,127 EC-GDSA – 0,126 EC-KCDSA – 0,124	IBS-1 – 0,15 IBS-2 – 0,15 EC-DSA – 0,144 EC-GDSA – 0,141 EC-KCDSA – 0,138 EC-FSDSA – 0,126 EC-SDSA – 0,123 EC-RDSA – 0,109

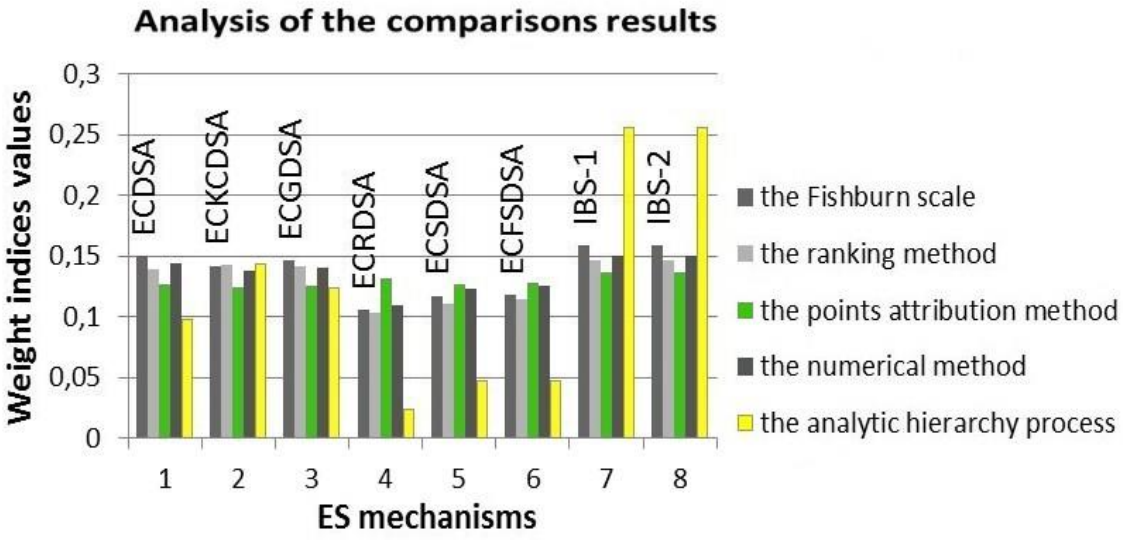


Fig. 1 – The results of ES algorithms estimation by different methods

Table 8 shows the averaged results of ES algorithms estimation by all estimation methods. Figure 2 shows graphically the averaged results of ES algorithms estimation by various methods.

Table 8 – The averaged results of ES algorithms estimation

Algorithm	Averaged estimate	Algorithm	Averaged estimate
EC-DSA	0,1318	EC-SDSA	0,1052
EC-KCDSA	0,1382	EC-FSDSA	0,107
EC-GDSA	0,1362	IBS-1	0,1698
EC-RDSA	0,095	IBS-2	0,1698

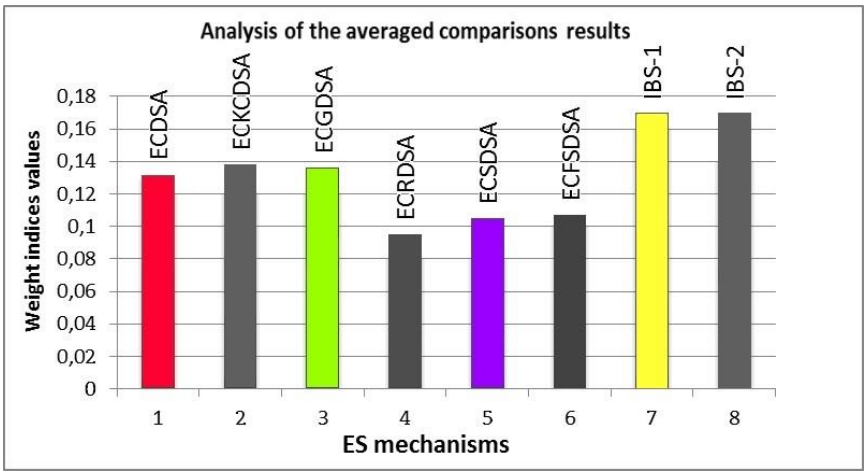


Fig. 2 – The averaged results of ES algorithms estimation by different methods

8 Features and requirements for cryptographic primitives in post quantum period

8.1 Intruder and threats models in the post quantum period

The analysis are showed, that a quantum computer can be considered as the basic intruder model, and methods and algorithms, that implemented on quantum computers – as threats models.

In our opinion the second problem task is successfully solved. So today there are quantum methods and developed based on these algorithms that allow to carry out attacks on asymmetric cryptosystem RSA, DSA, ECC and NTRU [24]. These include, first of all, should be referred quantum algorithms such as [24]: Grover quantum algorithm; Shor factorization algorithm; Shor algorithm for discrete logarithm; Wang algorithms etc.

Given the haste, with which USA and EU have started to build post quantum computers, and advances in this direction, it'll appear immediately in an explicit form after some time. So in the "1000-qubits" computer qubits actually are organized in clusters of 8 qubits each.

8.2 Preliminary analysis of asymmetric post quantum crypto transformations

In the Table 9 are shown general characteristics of mathematical apparatus, on which ES mechanisms are based, using which can be developed quantum-protected ES algorithms [3,12,14,23,24].

Shown in the table 10 ES mechanisms are proposed by ETSI for further study and research as possible candidates for quantum-protected ES circuits. Analysis of the data, that is given in the Tabl. 9,10, allows to conclude about advantages and disadvantages of some crypto transformations.

Table 9 – Directions of quantum-protected asymmetric algorithms

Cryptography scheme	Signature	Encryption	Key size	Data type	Core Ops.	Cryptographic Maturity
Hash-Based	Yes	No	≈ 20	Hash out.	Hashing	High
Multivariate Quadratic	Yes	No	≈ 10k	GF(2m)	Matrix LSE	Low, medium schemes
L-B: NTRU General lattice	Maybe Maybe	Yes Yes	< 0.1k ≈ 100k	Zq GF(2m)	Matrix mult. Medium	Medium Medium
Code-Based	Expensive	Yes	≈ 100k	GF(2m)	Matrix mult.	High, with prec. to impl.

Table 10 – Comparison of key lengths and signatures for quantum-protected ES algorithms

Type	Scheme	Security *(Bits)*	Public key *(Bytes)*	Signature *(Bytes)*
Lattice	Lyubashevsky	-------	1 664	2 560
	NTRU-MLS	128	988	988
	Aguilar et al	128	1 082	1 894
	Guneysu te al	80	1 472	1 120
	BLISS	128	896	640
MQ	Quartz	80	72 237	16
	UOV	128	413 145	135
	Cyclic-UOV	128	60 840	135
	Rainbow	128	139 363	79
	Cyclic-Rainbow	128	48 411	79
Code	Parallel-CFS	120	503 316 480	108
	Cayrel et al	128	10 920	47 248
	RankSign	130	7 200	1 080
	Cyclic-RankSign	130	3 538	1 080
Hash	Merkle	128	32	1 731
	Leighton-Micali	128	20	668
	XMSS	256	64	8 392
	SPHINCS	256	1 056	41 000
Isogeny	Jao-Soukharev	128	768	1 280
	Sun-Tian-Wang	128	768	16

8.3 Substantiation parameters and keys in comparing

The preliminary results of available post quantum algorithms comparison have been obtained during the study. Restrictions were used due to lack of complete information. Table 11 presents some comparison parameters and properties.

Table 11 – Indexes and properties of post quantum crypto primitives

Parameters/ Algorithms	Crypto-graphy stability	The public key length	The private key length	The signature length	Direct conversion speed	Reverse conversion speed
	1	*2*	*3*	*4*	*5*	*6*
1. NTRU	128	988	256	988-	0,5	0,02
2. BLISS	128	896	256	640	0,02	0,02
3. Quartz	80	72237	3000	16	2	0,05
4. XMSS	128	1700	280	2083	2	0,2
5.SPHINCS	128	1056	1088	41000	2	0,2
6.RankSign	130	7200	21600	1080	0,02	0,02
7. Jao-Souk	128	768	768	1280*	5	5

Note: *Cryptography strong is given in bits, data size – in bytes, and the transformations speed – as a coefficient relative to speed of corresponding RSA algorithm transformation with a key length of 4096 bits.*

8.4 Comparative estimation of the using cryptographic algorithms

Table 12 is given the result of determining the weighting indexes according to expert estimates for the electronic signature mechanisms for standard automated systems cryptography *(number from Table 11)*.

Table 12 – The weights indices of standard signature mechanisms

Criteria	1	2	3	4	5	6
1	0,263	0,181	0,123	0,072	0,181	0,181
2	0,203	0,281	0,065	0,105	0,143	0,203
3	0,138	0,232	0,054	0,083	0,138	0,354
4	0,134	0,229	0,075	0,134	0,075	0,353
5	0,153	0,089	0,058	0,274	0,153	0,274
W	0,178	0,202	0,075	0,134	0,138	0,273

The level of estimates consistency is 0,3, which satisfies the requirements. BLISS algorithm has a level 0,763, XMSS – 0,237 after conducting estimates.

In the table 13 is given the result of determining weight indices of encryption mechanisms in cloud environment.

Table 13 – The encryption weights indices for cryptography in the cloud

Criteria	1	2	3	4	5	6
1	0,319	0,068	0,068	0,182	0,182	0,182
2	0,233	0,055	0,082	0,164	0,233	0,233
3	0,329	0,064	0,107	0,107	0,196	0,196
4	0,243	0,056	0,084	0,135	0,242	0,242
5	0,246	0,062	0,062	0,140	0,246	0,246
W	0,274	0,061	0,081	0,146	0,220	0,220

The level of estimates consistency is 0,3, which satisfies the requirements. NTRU algorithm has a level 0,685, Jao-Sukharev – 0,315 after conducting estimates.

9 Conclusions

1. In comparing post quantum algorithms it is proposed to use the system of unconditional and conditional partial and integral criteria. To unconditional criteria will refer those criteria, which fulfillment is mandatory for cryptographic primitive, that is unconditional. Conditional is called criteria, which performance for any ES is carried out by only defined condition.
2. The researches results are showed, that as the main criterion for integral estimation can be recommended to use the integral unconditional criterion, that is derived based on partial unconditional criteria. If at least one partial criterion does not meet conditions, then this ES is rejected.
3. To determine the integral conditional criterion regarding ES standard is possible to use several methods, such as: analytic hierarchy process based on pairwise comparisons and method of determining weight indices.
4. Conducted analysis and studies allowed to compare the properties of selected estimation methods, and to identify the advantages and disadvantages of each method. To obtain the final

result by this method, it is necessary to multiply the level 1 priorities vector and acquired values level 1 matrix, and ranging obtained numerical values from the highest to the lowest.

5. In post quantum period as the basic model infringer can be considered a quantum computer, and as the basic model of threats – methods and algorithms of quantum cryptanalysis.
6. Table 9 shows general characteristics of mathematical apparatus, on which ES mechanisms are based. Tables 12 and 13 are shown the results of weight indices determination according to expert estimates for post quantum crypto primitives that are presented in Table 11.
7. In general, according to the results of the comparative analysis we can conclude, that the best choice among all candidates is the choice of algorithms that use lattices. The disadvantage of these algorithms is that according to recent studies, these algorithms have reduced complexity for quantum attack "meeting in the middle", but this complexity is satisfactory for minimal requirements. So these algorithms are the best choice for the transitional period, which will give the time with sustainable algorithms to search the further improve decisions of these algorithms, or search of other options.

References

[1] AES: the Advanced Encryption Standard [Electronic Resource]. – Way of access: https://competitions.cr.yp.to/aes.html. – Title from the screen.

[2] Analytic hierarchy process [Electronic Resource]. – Way of access: https:// en.wikipedia.org/wiki/ Analytic_hierarchy_ process. – Title from the screen.

[3] ETSI GR QSC 001 V.1.1.1 (2016-07). Quntum-Safe Cryptography (QSC); Quantum-safe algorithmic framework [Electronic Resource]. – Way of access: https://portal.etsi.org/webapp/workProgram/Report_WorkItem.asp?wki_id=46690. – Title from the screen.

[4] Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms: ISO/IEC 14888-3 (Edition 2 (2006-11-15)): 2006. – 68 p.

[5] Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms: ISO/IEC 14888-3 (Edition 3): 2016. – 130 p.

[6] Kalyna [Electronic Resource]. – Way of access: http://www.slideshare.net/oliynykov/kalyna. – Title from the screen.

[7] Koblitz N. A riddle wrapped in an enigma / Neal Koblitz, Alfred J. Menezes [Electronic Resource]. – Way of access: https://eprint.iacr.org/2015/1018.pdf. – Title from the screen.

[8] Kupyna [Electronic Resource]. – Way of access: https://ru.wikipedia.org/wiki/Kupyna. – Title from the screen.

[9] Chen L. Report on Post-Quatum Cryptography. NISTIR 8105 (DRAFT) / Lili Chen, Stephen Jordan, Yi-Kai-Liu et al. [Electronic Resource]. – Way of access: http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf. – Title from the screen.

[10] Mosca M. Setting the Scene for the ETSI Quantum-safe Cryptography Workshop / M. Mosca // E-proceedings of "1st Quantum-Safe-Crypto Workshop", Sophia Antipolis, Sep. 26-27, 2013 [Electronic Resource]. – Way of access: http://docbox.etsi.org/Workshop/2013/201309_CRYPTO/eproceedings_Crypto_2013.pdf. – Title from the screen.

[11] NESSIE: New European Schemes for Signatures, Integrity, and Encryption [Electronic Resource]. – Way of access : https://competitions.cr.yp.to/nessie.html. – Title from the screen.

[12] Post-quantum crypto project [Electronic Resource]. – Way of access: http://csrc.nist.gov/groups/ST/post-quantum-crypto/index.html. – Title from the screen.

[13] Procedures for Determining the Weights of Selection Factors in the Weighted-Matrix Delivery Decision [Electronic Resource]. – Way of access: http://www.tcrponline.org/PDFDocuments/tcrp_rpt_131AppF.pdf. – Title from the screen.

[14] Proposed Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process [Electronic Resource]. – Way of access: http://csrc.nist.gov/groups/ST/post-quantum-crypto/documents/call-for-proposals-draft-aug-2016.pdf. – Title from the screen.

[15] Quantum Safe Cryptography and Security. An introduction, benefits, enablers and challenges // ETSI White Paper. – 2015. – No. 8 [Electronic Resource]. – Way of access: http://www.etsi.org/images/files/ETSI White Papers / Quantum Safe Whitepaper.pdf. – Title from the screen.

[16] Roszkowska E. Rank ordering criteria weighting methods – a comparative overview / Ewa Roszkowska // Optimum. Studia ekonomiczne. – 2013. – № 5 (65). – P. 14–33 [Electronic Resource]. – Way of access: http:// repozytorium. uwb.edu.pl /jspui/bitstream/ 11320/2189/1/02_Ewa%20ROSZKOWSKA.pdf. – Title from the screen.

[17] Saaty T. L. Decision making with the analytic hierarchy process / Thomas L. Saaty // Int. J. Services Sciences. – 2008. – Vol. 1. – №1. – P. 83 – 98 [Electronic Resource]. – Way of access: http://www.colorado.edu/geography/leyk/geog_5113/ readings/saaty_2008.pdf. – Title from the screen.

[18] Saaty T. L. The Analytic Hierarchy Process / T. L. Saaty. – New York: McGraw Hill, 1980. – 278 p.

[19] The methods of expert estimations [Electronic Resource]. – Way of access: http://books forstudy.com/19650323/ ekonomika/metodi ekspertnih otsinok.htm. – Title from the screen.

[20] Yesina M. Methods of cryptographic primitives comparative analysis / Maryna Yesina, Yurij Gorbenko // Inżynier XXI wieku ("Engineer of XXI Century" – the VI Inter University Conference of Students, PhD Students and Young Scientists: University of Bielsko-Biala, Poland, December 02, 2016). – Bielsko-Biała: Wydawnictwo Naukowe Akademii Techniczno-Humanistycznej w Bielsku-Białej, 2016. – P. 451–462.

[21] Zhukova O. V. Fishburne's method and the classical method of pharmacoeconomic analysis in the evaluation of antibiotic treatment of acute and recurrent bronchitis in children / Olga V. Zhukova, Tatjana M. Konyshkina, Svetlana V. Kononova // Int. J. Pharm. Science. – 2015. – Vol. 7. – Issue 11. – P. 185–190 [Electronic Resource]. – Way of access: http://innovareacademics.in/journals/index.php/ijpps/article/view/7770/5973. – Title from the screen.
[22] Andreichikov A. V. Analiz, sintez, planirovanie reshenii v ekonomike / A. V. Andreichikov, O. N. Andreichikova. – Moskva: Finansy i statistika, 2002. – 359 s.
[23] Gorbenko I. D. Postkvantova kryptografija ta mehanizmy i'i' realizacii' / I.D. Gorbenko, O.O. Kuznecov, O.V. Potij ta in. // Radiotehnika. – 2016. – Vyp. 186. – S. 32–52.
[24] Gorbenko Ju. I. Metody pobuduvannja ta analizu kryptografichnyh system: monografija. / Ju. I. Gorbenko. – Kharkiv: Fort, 2015. – 959 s.
[25] Orlovskii S. A. Problemy prinyatiya reshenii pri nechetkoi iskhodnoi informatsii / S. A. Orlovskii. – Moskva: Nauka, 1981. – 208 s.

Рецензент: Роман Олійников, д.т.н., проф., Харківський національний університет імені В.Н. Каразіна, м. Харків, Україна. E-mail: roliynykov@gmail.com

Надійшло: Лютий 2017.

Автори:
Іван Горбенко, д.т.н., проф., лауреат Державної премії України, Харківський національний університет імені В.Н. Каразіна, Харків, Україна. E-mail: gorbenkoi@iit.kharkov.ua
Юрій Горбенко, к.т.н., ХНУ імені В.Н. Каразіна, Харків, Україна. E-mail: gorbenkou@iit.kharkov.ua
Марина Єсіна, аспірантка, ХНУ імені В.Н. Каразіна, Харків, Україна. E-mail: rinayes20@gmail.com
Володимир Пономар, аспірант, ХНУ імені В.Н. Каразіна, Харків, Україна. E-mail: laedaa@gmail.com

Пропозиції з виконання порівняльного аналізу та прийняття в процесі конкурсу рішень щодо переваг певних асиметричних пост квантових криптографічних примітивів.

Анотація. У роботі розглянуто пропозиції із виконання порівняльного аналізу криптографічних примітивів та обґрунтування, розроблення та експериментальне підтвердження можливостей застосування методичних основ вибору та застосування системи безумовних та умовних критеріїв, а також методів та методики порівняльного аналізу та прийняття рішень щодо асиметричних пост квантових криптографічних примітивів типу направлений шифр, а також алгоритмів інкапсуляції ключів та електронних підписів. Наведено певні критерії та показники, що можуть бути використані при порівняльному аналізі властивостей кандидатів у пост квантові криптографічні примітиви. Проведено порівняльний аналіз існуючих перспективних механізмів електронних підписів згідно стандарту ISO/IEC 14888-3:2016 та деяких криптографічних примітивів, що вважаються можливими до застосування у пост квантовий період. Наведено результати оцінювання криптографічних примітивів. Зроблено висновки та надано рекомендації із застосування методів оцінки визначених криптографічних примітивів.

Ключові слова: аналіз алгоритмів ЕП, вагові коефіцієнти, електронний підпис, критерій оцінки ЕП, методи порівняльного аналізу ЕП.

Рецензент: Роман Олейников, д.т.н., проф., Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина. E-mail: roliynykov@gmail.com

Поступила: Февраль 2017.

Авторы:
Иван Горбенко, д.т.н., проф., лауреат Государственной премии Украины, Харьковский национальный университет имени В. Н. Каразина, Украина. E-mail: gorbenkoi@iit.kharkov.ua
Юрий Горбенко, к.т.н., ХНУ имени В. Н. Каразина, Харьков, Украина. E-mail: gorbenkou@iit.kharkov.ua
Марина Есина, аспирантка, ХНУ имени В. Н. Каразина, Харьков, Украина. E-mail: rinayes20@gmail.com
Владимир Пономарь, аспирант, ХНУ имени В. Н. Каразина, Харьков, Украина. E-mail: Laedaa@gmail.com

Предложения по выполнению сравнительного анализа и принятия в процессе конкурса решений относительно преимуществ определенных асимметрических пост квантовых криптографических примитивов.

Аннотация. В работе рассмотрены предложения по выполнению сравнительного анализа криптографических примитивов и обоснование, разработка и экспериментальное подтверждение возможностей применения методических основ выбора и применения системы безусловных и условных критериев, а также методов и методики сравнительного анализа и принятия решений относительно асимметричных пост квантовых криптографических примитивов типа направленный шифр, а также алгоритмов инкапсуляции ключей и электронных подписей. Приведены определенные критерии и показатели, которые могут быть использованы при сравнительном анализе свойств кандидатов в пост квантовые криптографические примитивы. Проведен сравнительный анализ существующих перспективных механизмов электронных подписей согласно стандарту ISO/IEC 14888-3: 2016 и некоторых криптографических примитивов, которые считаются возможными к применению в пост квантовый период. Приведены результаты оценивания криптографических примитивов. Сделаны выводы и даны рекомендации по применению методов оценки определенных криптографических примитивов.

Ключевые слова: анализ алгоритмов ЭП, весовые коэффициенты, электронная подпись, критерий оценки ЭП, методы сравнительного анализа ЭП.

Vesa A. Niskanen
Ph.D., Adjunct Professor,
Department of Economics & Management, University of Helsinki,
P.O. Box 27 (Latokartanonkaari 9), 00014 Helsinki, Finland
E-mail: vesa.a.niskanen@helsinki.fi

Igor Romenskiy
Doktor für physikalische-mathematische Wissenschaften, GFaI Gesellschaft zur Förderung angewandter Informatik e.V.,
Volmerstraße 3, 12489 Berlin, Deutschland
E-mail: iromensky@mail.ru

Alexey Stakhov
Doctor of Sciences (Engineering), Full Professor,
Academicians of the Academy of Engineering Sciences of Ukraine,
International Club of the Golden Section,
6 McCreary Trail, Bolton, Ont., L7E 2C8, Canada
E-mail: goldenmuseum@rogers.com

Vadim Geurkov
Ph.D., Associate Professor,
Department of Electrical and Computer Engineering Ryerson University,
Victoria St., 350, Toronto, Ontario, M5B 2K3, Canada
E-mail: vgeurkov@ee.ryerson.ca

Fionn Murtagh
Ph.D., Professor,
Department of Computing and Mathematics, University of Derby,
Kedleston Road, Derby DE22 1GB, UK
Email: f.murtagh@derby.ac.uk
Department of Computing, Goldsmiths,
University of London,
New Cross, London SE14 6NW, UK
E-mail: f.murtagh@gold.ac.uk

C. Pandu Rangan
Ph.D., FNAE, Senior Professor,
Department of Computer Science and Engineering,
Indian Institute of Technology,
Madras, Chennai, 600036, India
E-mail: prangan55@gmail.com

Håvard Raddum
Ph.D.,
Simula Research Laboratory, P.O. Box 134, 1325 Lysaker, Norway
E-mail: haavardr@simula.no

Oleksandr Kazymyrov
Ph.D.,
EVRY Norge AS,
Snarøyveien 30A, Fornebu, 1360, Norway
E-mail: oleksandr.kazymyrov@evry.com

Mikołaj Karpiński
Doctor of Sciences (Engineering), Full Professor,
University of Bielsko-Biala,
Willowa St., 2, 43-309, Bielsko-Biala, Poland
E-mail: mkarpinski@ath.bielsko.pl

Веса А. Нисканен
доктор філософії, ад'юнкт професор,
департамент економіки та менеджменту, Університет Гельсінкі,
P.O. Бокс 27 (Латокартанонкаарі 9), 00014 Гельсінкі, Фінляндія
E-mail: vesa.a.niskanen@helsinki.fi

Ігор Роменський
доктор фізико-математичних наук,
GFaI - Спілка з просування прикладної інформатики,
Фольмерштрассе 3, 12489 Берлін, Німеччина
E-mail: iromensky@mail.ru

Олексій Стахов
доктор технічних наук, професор, академік Академії інженерних наук України,
Міжнародний Клуб Золотого Перетину,
6 МаккКрері Трейл, Болтон, Онтаріо, L7E 2C8, Канада
E-mail: goldenmuseum@rogers.com

Вадим Геурков
доктор філософії, доцент,
факультет електротехніки та обчислювальної техніки університету Раєрсон,
350 Вікторія-стріт, Торонто, Онтаріо, M5B 2K3, Канада
E-mail: vgeurkov@ee.ryerson.ca

Фінн Мерта
доктор філософії, професор,
факультет обчислювальної математики університету Дербі,
Кедлестон Роад, Дербі DE22 1GB, Великобританія
Email: f.murtagh@derby.ac.uk
факультет обчислень Голдсмітського коледжу Лондонського університету,
Нью-Крос, Лондон SE14 6NW, Великобританія
E-mail: f.murtagh@gold.ac.uk

С. Панду Ранган
доктор філософії, FNAE, старший викладач,
факультет комп'ютерних наук та інженерії Індійського технологічного інституту,
Мадрас, Ченнаї - 600036, Індія
E-mail: prangan55@gmail.com

Ховард Радум
доктор філософії,
науково-дослідна лабораторія Симула, P.O. Бокс 134, 1325, Лісакер, Норвегія
E-mail: haavardr@simula.no

Олександр Казіміров
доктор філософії,
EBPI Норге АС,
Снаройвиен 30A, 1360 Форнебу, Норвегія
E-mail: oleksandr.kazymyrov@evry.com

Микола Карпінський
доктор технічних наук, професор,
Університет Бельсько-Бяла,
вул. Віллова 2, 43-309 Бельсько-Бяла, Польща
E-mail: mkarpinski@ath.bielsko.pl

Volodymyr Khoma
Doctor of Sciences (Engineering), Full Professor,
Institute «Automatics and Informatics», The Opole University of Technology,
Prószkowska St., 76, 45-758, Opole, Poland
E-mail: xoma@wp.pl

Joanna Świątkowska
Ph.D., CYBERSEC Programme Director,
Senior Research Fellow of the Kosciuszko Institute,
Feldmana St., 4/9-10, 31-130, Kraków,
Poland
E-mail: joanna.swiatkowska@ik.org.pl

Nick Bilogorskiy
Director of Security Research,
Cyphort, 5451 Great America Parkway, Suite 225,
Santa Clara, California, 95054, USA
E-mail: nick@novaukraine.org

Richard Kemmerer
Ph.D., Professor,
Computer Science Department, University of California,
Santa Barbara, California, 93106, USA
E-mail: kemm@cs.ucsb.edu

Dimiter Velev
Ph.D., Professor,
Department of Information Technologies and Communications, Faculty of Applied Informatics and Statistics, University of National and World Economy,
„8-ми декември“ St., UNSS - Studentski grad, 1700
Sofia, Bulgaria
E-mail: dgvelev@unwe.bg

Robert Brumnik
Ph.D., Professor Assistant,
GEA College, Dunajska cesta 156, 1000 Ljubljana,
Slovenia
Metra Engineering Ltd, Špruha 19, 1236 Trzin, Slovenia
E-mail: robert.brumnik@metra.si

Stephan Dempe
Ph.D., Professor,
Department of Mathematics and Computer Science,
Technical University Bergakademie Freiberg, Germany
Akademischestrafte 6, D-09596, Freiberg,
Germany
E-mail: dempe@math.tu-freiberg.de

Ludmila Babenko
Doctor of Sciences (Engineering), Full Professor,
Institute of Computer Technologies and Information Safety of Southern Federal University
Chekhov St., 2, Taganrog, Rostov obl., Russia
E-mail: blk@tsure.ru

Valerii Zadiraka
Doctor of Sciences (Physics and Mathematics),
Full Professor, Academician of the National Academy of Sciences of Ukraine, Glushkov Institute of Cybernetics (GIC) of National Academy of Sciences of Ukraine,
40 Glushkov av., Kyiv, 03187, Ukraine
E-mail: zvk140@ukr.net

Володимир Хома
доктор технічних наук, професор,
Інститут «Автоматика та інформатика», Технологічний університет Ополе,
76 Пружовська Вулиця, 45-758 Ополе, Польща
E-mail: xoma@wp.pl

Джоана Святковська
доктор філософії, директор програми CYBERSEC,
старший науковий співробітник Інституту Костюшки
вул. Фельдман 4 / 9-10, 31-130 Краків,
Польща
E-mail: joanna.swiatkowska@ik.org.pl

Нік Білогорський
директор з досліджень безпеки,
Цифорт, 5451 Гріт Америка Парквей, Люкс 225,
Санта-Клара, Каліфорнія 95054, США
E-mail: nick@novaukraine.org

Річард Кеммерер
Ph.D., професор,
факультет інформатики, Каліфорнійський університет,
Санта-Барбарі, CA 93106, США
E-mail: kemm@cs.ucsb.edu

Дімітер Велев
доктор філософії, професор,
кафедра інформаційних технологій і комунікацій,
факультет прикладної інформатики та статистики,
Університет національної та світової економіки,
вул. "8-ми декември", UNSS - Студентські град, 1700
Софія, Болгарія
E-mail: dgvelev@unwe.bg

Роберт Брумнік
доктор філософії, доцент,
GEA коледж, Дунайська цеста 156, 1000 Любляна,
Словенія
Метра Інжиніринг ЛТД, Шпруха 19,1236 Тржин,
Словенія
E-mail: robert.brumnik@metra.si

Стефан Демп
доктор філософії, професор,
факультет математики та інформатики, технічний університет Фрайберзької Гірничої Академії,
Німеччина
Akademischestrafte 6, D -09596, Фрайберг, Німеччина
E-mail: dempe@math.tu-freiberg.de

Людмила Бабенко
доктор технічних наук, професор,
Інститут комп'ютерних технологій та інформаційної безпеки Південного федерального університету
вул. Чехова 2, Таганрог, Ростовська обл., Росія
E-mail: blk@tsure.ru

Валерій Задірака
доктор технічних наук, професор,
академік Національної академії наук України,
Інститут кібернетики імені В.М. Глушкова
Національної академії наук України,
проспект Академіка Глушкова, 40, Київ, 03187, Україна
E-mail: zvk140@ukr.net

Ludmila Kovalchuk
Doctor of Sciences (Engineering), Associate Professor,
Department of mathematical methods of information security Institute of Physics and Technology,
National Technical University of Ukraine
"Kyiv Polytechnic Institute"
37, Peremohy av., Kyiv, 03056, Ukraine
E-mail: lusi.kovalchuk@gmail.com

Людмила Ковальчук
доктор технічних наук, доцент,
кафедра математичних методів захисту інформації фізико-технічного інституту
національного технічного університету України «КПІ»,
03056, Київ, пр. Перемоги, 37, НТУУ "КПІ"
E-mail: lusi.kovalchuk@gmail.com

Anton Alekseychuk
Doctor of Sciences (Engineering), Associate Professor,
Department of application of means of cryptographic and technical defense of information, Institute of Special Communication and Information Security,
National Technical University of Ukraine
"Kyiv Polytechnic Institute"
37 Peremohy av., Kyiv, 03056, Ukraine
E-mail: alex-dtn@ukr.net

Антон Олексійчук
доктор технічних наук, доцент,
кафедра застосування засобів криптографічного та технічного захисту інформації Інституту спеціального зв'язку та захисту інформації національного технічного університету України «КПІ»,
03056, Київ, пр. Перемоги, 37, НТУУ "КПІ"
E-mail: alex-dtn@ukr.net

Volodymyr Maxymovych
Doctor of Sciences (Engineering), Full Professor,
Institute of Computer Technologies, Automation and Metrology (ICTA), Lviv Polytechnic National University,
Bandera St., 12, Lviv, 79013, Ukraine
E-mail: vmax@polynet.lviv.ua

Володимир Максимович
доктор технічних наук, професор,
Інститут комп'ютерних технологій, автоматики та метрології Національного університету
«Львівська політехніка»,
вул. Степана Бандери, 12, м. Львів, 79013, Україна
E-mail: vmax@polynet.lviv.ua

Oleksiy Borysenko
Doctor of Sciences (Engineering), Full Professor,
Sumy State University,
Rymskogo-Korsakova St., 2, Sumy, 40007, Ukraine
E-mail: 5352008@ukr.net

Олексій Борисенко
доктор технічних наук, професор,
Сумський державний університет,
вул. Римського-Корсакова, 2, 40007 Суми, Україна
E-mail: 5352008@ukr.net

Anatoliy Biletsky
Doctor of Sciences (Engineering), Full Professor,
Institute of Air Navigation, National Aviation University,
Kosmonavta Komarova av., 1, Kyiv, 03058, Ukraine
E-mail: abelnau@ukr.net

Анатолій Білецький
доктор технічних наук, професор,
навчально-науковий інститут аеронавігації національного авіаційного університету,
пр. Космонавта Комарова 1, Київ, 03058, Україна
E-mail: abelnau@ukr.net

Serhii Kavun
Doctor of Sciences (Economics), Ph.D. (Engineering),
Full Professor, Department of Information Technologies,
Kharkiv Educational and Research Institute
of the University of Banking,
Peremogy av. 55, Kharkiv, 61174, Ukraine
E-mail: kavserg@gmail.com

Сергій Кавун
доктор економічних наук, кандидат технічних наук,
професор, кафедра інформаційних технологій,
Харківський навчально-науковий інститут
ДВНЗ "Університет банківської справи",
пр. Перемоги 55, м. Харків, 61174, Україна
E-mail: kavserg@gmail.com

Vyacheslav Kharchenko
Doctor of Sciences (Engineering), Full Professor,
Academician of the Academy of Applied Radioelectronics Sciences, N.Ye. Zhukovskiy National Aerospace University – Kharkiv Aviation Institute (KhAI),
17 Chkalov St., Kharkiv, 61070, Ukraine
E-mail: v_s_kharchenko@ukr.net

В'ячеслав Харченко
доктор технічних наук, професор,
академік Академії наук прикладної радіоелектроніки,
Національний аерокосмічний університет
ім. М. Є. Жуковського,
вул. Чкалова, 17, 61070, м. Харків, Україна
E-mail: v_s_kharchenko@ukr.net

Valentin Lazurik
Doctor of Sciences (Physics and Mathematics),
Full Professor, V. N. Karazin Kharkiv National University,
Svobody sq., 4, Kharkiv, 61022, Ukraine
E-mail: vtlazurik@karazin.ua

Валентин Лазурик
доктор фізико-математичних наук, професор,
Харківський національний університет
імені В.Н. Каразіна,
майдан Свободи 4, м. Харків, 61022, Україна
E-mail: vtlazurik@karazin.ua

Volodymyr Kuklin
Doctor of Sciences (Physics and Mathematics), Full Professor, V. N. Karazin Kharkiv National University,
Svobody sq., 4, Kharkiv, 61022, Ukraine
E-mail: kuklinvm1@gmail.com

Володимир Куклін
доктор фізико-математичних наук, професор,
Харківський національний університет
імені В.Н. Каразіна,
майдан Свободи 4, м. Харків, 61022, Україна
E-mail: kuklinvm1@gmail.com

Ivan Gorbenko
Doctor of Sciences (Engineering), Full Professor,
Academician of the Academy of Applied Radioelectronics Sciences, V. N. Karazin Kharkiv National University,
Svobody sq., 4, Kharkiv, 61022, Ukraine
E-mail: gorbenkoi@iit.kharkov.ua

Іван Горбенко
доктор технічних наук, професор, академік Академії наук прикладної радіоелектроніки,
Харківський національний університет
імені В.Н. Каразіна,
майдан Свободи 4, м. Харків, 61022, Україна
E-mail: gorbenkoi@iit.kharkov.ua

Victor Krasnobayev
Doctor of Sciences (Engineering), Full Professor,
Honourable Inventor of Ukraine,
Honourable Radio Specialist of the USSR,
V. N. Karazin Kharkiv National University,
Svobody sq., 4, Kharkiv, 61022, Ukraine
E-mail: krasnobayev@karazin.ua

Віктор Краснобаєв
доктор технічних наук, професор, заслужений винахідник України, почесний радист СРСР,
Харківський національний університет
імені В.Н. Каразіна,
майдан Свободи 4, м. Харків, 61022, Україна
E-mail: krasnobayev@karazin.ua

Irina Lisitska
Doctor of Sciences (Engineering), Full Professor,
Corresponding Member of the Academy of Applied Radioelectronics Sciences,
V. N. Karazin Kharkiv National University,
Svobody sq., 4, Kharkiv, 61022, Ukraine
E-mail: lisitska@karazin.ua

Ірина Лисицька
доктор технічних наук, професор,
член-кореспондент Академії наук прикладної радіоелектроніки, Харківський національний університет імені В.Н. Каразіна,
майдан Свободи 4, м. Харків, 61022, Україна
E-mail: lisitska@karazin.ua

Oleksandr Potii
Doctor of Sciences (Engineering), Full Professor,
Academician of the Academy of Applied Radioelectronics Sciences, V. N. Karazin Kharkiv National University,
Svobody sq., 4, Kharkiv, 61022, Ukraine
E-mail: potav@ua.fm

Олександр Потій
доктор технічних наук, професор,
академік Академії наук прикладної радіоелектроніки,
Харківський національний університет
імені В.Н. Каразіна,
майдан Свободи 4, м. Харків, 61022, Україна
E-mail: potav@ua.fm

Viktor Dolgov
Doctor of Sciences (Engineering), Full Professor,
Academician of the Academy of Applied Radioelectronics Sciences, V. N. Karazin Kharkiv National University,
Svobody sq., 4, Kharkiv, 61022, Ukraine
E-mail: dolgovvi@mail.ru

Віктор Долгов
доктор технічних наук, професор,
академік Академії наук прикладної радіоелектроніки,
Харківський національний університет
імені В.Н. Каразіна,
майдан Свободи 4, м. Харків, 61022, Україна
E-mail: dolgovvi@mail.ru

Roman Oliynikov
Doctor of Sciences (Engineering), Full Professor,
V. N. Karazin Kharkiv National University,
Svobody sq., 4, Kharkiv, 61022, Ukraine
E-mail: roliynykov@gmail.com

Роман Олійников
доктор технічних наук, професор,
Харківський національний університет
імені В.Н. Каразіна,
майдан Свободи 4, м. Харків, 61022, Україна
E-mail: roliynykov@gmail.com

Volodymyr Mashtalir
Doctor of Sciences (Engineering), Full Professor,
V. N. Karazin Kharkiv National University,
Svobody sq., 4, Kharkiv, 61022, Ukraine
E-mail: mashtalir@kture.kharkov.ua

Володимир Машталір
доктор технічних наук, професор,
Харківський національний університет
імені В.Н. Каразіна,
майдан Свободи 4, м. Харків, 61022, Україна
E-mail: mashtalir@kture.kharkov.ua

Grygoriy Zholtkevych
Doctor of Sciences (Engineering), Full Professor,
V. N. Karazin Kharkiv National University,
Svobody sq., 4, Kharkiv, 61022, Ukraine
E-mail: g.zholtkevych@karazin.ua

Oleksandr Oksiiuk
Doctor of Sciences (Engineering), Full Professor,
Taras Shevchenko National University of Kiev
Lomonosova St., 81, Kyiv, 03189, Ukraine
E-mail: o.oksiuk@gmail.com

Serhii Toliupa
Doctor of Sciences (Engineering), Full Professor,
Taras Shevchenko National University of Kiev
Lomonosova St., 81, Kyiv, 03189, Ukraine
E-mail: tolupa@i.ua

Григорій Жолткевич
доктор технічних наук, професор,
Харківський національний університет
імені В.Н. Каразіна,
майдан Свободи 4, м. Харків, 61022, Україна
E-mail: g.zholtkevych@karazin.ua

Олександр Оксіюк
доктор технічних наук, професор,
Київський національний університет імені Т. Шевченка
вул. М. Ломоносова, 81, 03680, м. Київ, Україна
E-mail: o.oksiuk@gmail.com

Сергій Толюпа
доктор технічних наук, професор,
Київський національний університет імені Т. Шевченка
вул. М. Ломоносова, 81, 03680, м. Київ, Україна
E-mail: tolupa@i.ua

Статті пройшли внутрішнє та зовнішнє рецензування.

Наукове видання

КОМП'ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА

Випуск 1(5) 2017

Міжнародний електронний науково-теоретичний журнал

Англійською, українською, російською мовами

Комп'ютерне верстання – Федоренко В.В.

61022, Харків, майдан Свободи, 6
Харківський національний університет імені В.Н. Каразіна

V. N. Karazin Kharkiv National University Publishing