МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська політехніка»

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Том 12, № 3

Volume 12, No. 3

Одеса – 2022
Odesa – 2022

Журнал внесений до переліку наукових фахових видань України (технічні науки) згідно наказу Міністерства освіти і науки України № 463 від 25.04.2013 р. Перереєстровано на категорію «Б» за фахами 121, 122, 125, 151 згідно наказу МОН України № 1473 від 26.11.2020 р.

Виходить 4 рази на рік

Заснований Одеським національним політехнічним університетом у 2011 році

Свідоцтво про державну реєстрацію КВ № 17610 - 6460Р від 04.04.2011р.

Published 4 times a year

Founded by Odesa National Polytechnic University in 2011

Certificate of State Registration КВ № 17610 - 6460Р of 04.04.2011

Друкується за рішенням редакційної колегії та Вченої ради Національного університету «Одеська політехніка»

Оригінал-макет виготовлено редакцією журналу

Адреса редакції: просп. Шевченка, 1, Одеса, 65044, Україна
Телефон: +38 048 705 8506
Web: www.immm.op.edu.ua (immm.opu.ua) E-mail: immm.ukraine@gmail.com

Editorial address: 1 Shevchenko Ave., Odesa, 65044, Ukraine
Tel.: +38 048 705 8506
Web: www.immm.op.edu.ua (immm.opu.ua) E-mail: immm.ukraine@gmail.com

ЗМІСТ/CONTENTS

DOI 10.15276/imms.v12.no3.137
UDC 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 12 (2022), No. 3, pp. 137-143

IMPROVEMENT OF THE PSEUDORANDOM KEY SEQUENCES GENERATION ALGORITHM BASED ON CELLULAR AUTOMATON AND MANY-VALUED LOGIC BENT-SEQUENCES

M.V.Khymenko, A.V.Sokolov

National Odesa Polytechnic University
Shevchenko Ave., 1 Odesa, 65044, Ukraine, radiosquid@gmail.com

One of the most important cryptographic structures, which is the basis of modern information protection systems, is cryptographically protected generators of pseudo-random key sequences, which are used in a wide variety of tasks, starting from the creation of initialization vectors, key information, and formation of the steganographic path, ending with their operation as the most important basic component of full-fledged stream cryptographic algorithms. Many of the available today algorithms of pseudo-random key sequences generators are characterized either by a quite complex software implementation structure or by insufficient cryptographic security, which makes urgent the task of developing effective cryptographically protected pseudo-random key sequences generators with a high level of stochastic quality. This paper proposes a scheme for an efficient pseudo-random key sequences generator based on a cellular automaton, as well as on such many-valued logic perfect algebraic constructions as IV-sets of quaternary bent-sequences with the maximum level of nonlinearity distance. The proposed generator is characterized by a significant complexity of the relationship between the output bits of the pseudo-random sequence and the elements of the short key on the basis of which they are generated, which determines the high level of its cryptographic security, while the number of protection levels of the proposed generator is easily scalable if necessary. Having only two binary linear feedback shift registers in the proposed scheme makes it adaptable to software implementation. The research performed made it possible to establish that the pseudo-random sequences generated by the proposed generator correspond to all stochastic tests from the NIST set, which makes it possible to recommend it for use in practice.
Keywords: pseudo-random key sequences generator, bent-sequence, cellular automaton.

Introduction and statement of the problem

The pseudo-random key sequences generator (PRKSG) is one of the most important cryptographic structures, which finds its numerous applications in modern information protection systems: starting from the generation of various initialization vectors, ending with full-fledged use as the main element of a stream ciphers, or in units for determining the steganographic path in steganographic algorithms. Such a considerable demand for PRKSG leads to significant attention of modern researchers to the problems of developing PRKSG, which is characterized by high cryptographic security, high stochastic quality of generated pseudo-random sequences, as well as significant performance.

Despite the fact that today there are many methods for estimating the stochastic quality of a PRKSG, the set of NIST [1] stochastic tests is generally accepted, so the compliance of PRKSG with these tests is an indicator of its high stochastic quality.

Today there are many schemes for PRKSG construction, among which a special place is occupied by PRKSG based on perfect algebraic constructions. Thus, the work [2] presents a scheme of the PRKSG based on linear feedback shift registers (LFSR) and dual pairs of bent-sequences, which is characterized by the correspondence with a set of stochastic tests [3], as well as a set of NIST stochastic tests, as it was proved in [4]. Nevertheless, despite the high cryptographic and stochastic quality of the PRKSG [3], it

is not devoid of disadvantages related to the fact that the use of LFSR is not always desirable on modern devices during the software implementation of the PRKSG and may lead to a decrease in its overall performance. This circumstance led to the creation of a modification of this PRKSG [5], based on the application of cellular automaton [6], which allowed a significant increase in its performance, however, as shown in [4], it reduced the level of stochastic quality of generated pseudorandom sequences, which complicates its application in practice.

As the performed research shows, this shortcoming can be eliminated by using such many-valued logic perfect algebraic constructions as the quaternary bent-sequences, the definition of which was proposed in [7].

The *purpose* of this paper is to develop a high-speed, stochastically, and cryptographically high-quality PRKSG based on cellular automaton and IV-set of quaternary bent-sequences.

Quaternary bent-sequences

The basis for the development of the proposed modification of the generator of pseudorandom key sequences is bent-sequences of quaternary logic, which were first defined in [7], after which the research of their full class was performed in [8]. Let us introduce the basic definitions we need.

Definition 1 [9]. A mapping $\{0,1,2,3...,q-1\}^k \to \{0,1,2,3...,q-1\}$ is called a function of a q-valued logic (hereinafter referred to as a q-function).

The most common way of defining a q-function is the truth table. In addition to the way of representation of q-functions with help of the truth tables over the alphabet $\{0,1,...,q-1\}$, exponential truth tables presented above the alphabet $z_k = e^{j\frac{2\pi}{q}k}$, $k \in \{0,1,...,q-1\}$ are also considered.

In the case of 4-functions, the alphabet of the considered vectors will consist of the following values $\{0 \quad 1 \quad 2 \quad 3\} \to \{z_0 \quad z_1 \quad z_2 \quad z_3\} \to \{e^{j\frac{2\pi}{4}\cdot 0} \quad e^{j\frac{2\pi}{4}\cdot 1} \quad e^{j\frac{2\pi}{4}\cdot 2} \; e^{j\frac{2\pi}{4}\cdot 3}\}$.

Definition 2 [9]. The coefficients of the Vilenkin-Chrestenson transform of a function of q-valued logic is the vector obtained by multiplying its truth table of length N by a complex conjugate of the Vilenkin-Chrestenson matrix

$$\Omega_A = A \cdot \overline{V}_N, \tag{1}$$

while in the quaternary case, the Vilenkin-Chrestenson matrix is constructed in accordance with the following recurrence rule

$$V_{4^{k+1}} = \begin{bmatrix} V_{4^k} & V_{4^k} & V_{4^k} & V_{4^k} \\ V_{4^k} & V_{4^k}+1 & V_{4^k}+2 & V_{4^k}+3 \\ V_{4^k} & V_{4^k}+2 & V_{4^k} & V_{4^k}+2 \\ V_{4^k} & V_{4^k}+3 & V_{4^k}+2 & V_{4^k}+1 \end{bmatrix}, \tag{2}$$

where "+" is the addition operation, matrices V are presented in symbolic form, i.e., the summation is performed relative to indices z_i.

Definition 3 [8]. For a Vilenkin-Chrestenson matrix of order $N = q^k$, where q is a prime, a bent-sequence is a sequence $H = [h_0, h_1, \cdots, h_i, \cdots, h_{N-1}]$ over the alphabet $h_i \in \{e^{j\frac{2\pi}{q}\nu}\}, \nu = 0,1,...,q-1$ if it has a uniform absolute values of the Vilenkin-Chrestenson spectrum, which can be represented in matrix form

$$\left|\Omega_B(\omega)\right| = \left|H \cdot \overline{V}_N\right| = const, \quad \omega = \overline{0, N-1}, \tag{3}$$

where V_N is the Vilenkin-Chrestenson matrix of order N over the alphabet $h_i \in \{e^{j\frac{2\pi}{q}\nu}\}, q = 0,1,...,q-1$.

Since bent-sequences are unbalanced by their construction, for their practical application in cryptographic issues, the concept of a *q*-set of bent-sequences is most often used, the definition of which is introduced in [8].

Definition 4 [8]. A set of q q-ary bent-sequences is called a *q*-set if the concatenation of its truth tables is balanced, i.e., $K^0 = K^1 = ... = K^{q-1}$.

In [8], it is shown that the complete set of quaternary bent-sequences of length $N = 16$ and cardinality $J = 200704$ can be classified into 4428 different IV-sets.

He proposed PRKSG scheme

In the proposed PRKSG scheme, two LFSR are used to form the initial state of the cellular automaton with the number of states of each cell $q = 4$. The size of the used cellular automaton is $n = 16$, while the radius of the neighborhood is chosen as equal to $r = 2$. The IV-set of quaternary bent-sequences is used as the evolution rule. After a given number of steps of evolution $t = 7$ is performed, the data in the register of the cellular automaton enters the pseudo-random bit generation block, which decides the value of the output pseudo-random bit. The scheme of operation of the proposed PRKSG is presented in Fig. 1.

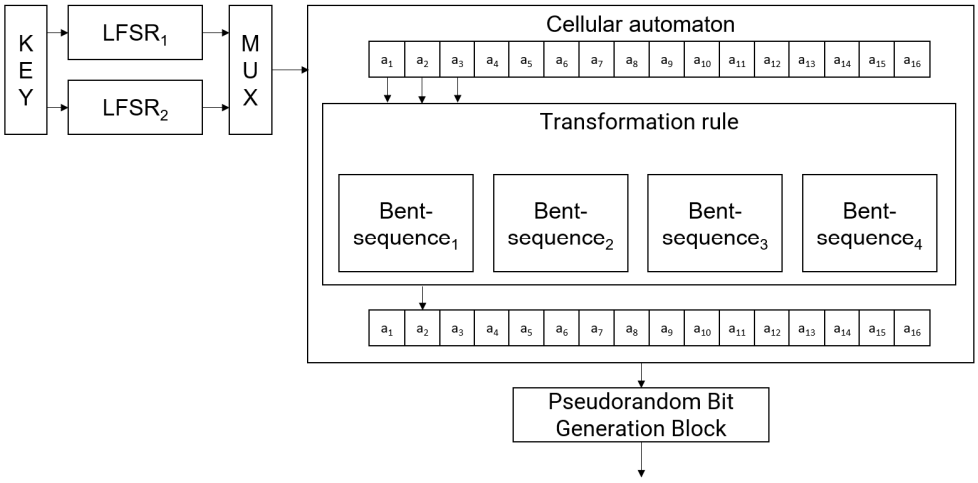


Fig. 1. Scheme of the proposed PRKSG

Let us explain in specific steps the algorithms of the proposed PRKSG, the scheme of which is shown in Fig. 1.

Initialization algorithm of the PRKSG

Step 1. Select 2 primitive irreducible polynomials $f_1(x)$ and $f_2(x)$, and to ensure the best stochastic and cryptographic properties of the PRKSG, the degrees of the selected polynomials must be mutually prime $\mathrm{GCD}(\deg\{f_1(x)\}, \deg\{f_2(x)\}) = 1$.

Step 2. Construct on the basis of selected primitive irreducible polynomials LFSR_1 and LFSR_2, the initial states of which are considered as the cryptographic key of the generator.

Step 3. In accordance with **Definition 4**, select the IV-set of quaternary bent-sequences, which are a nonlinear element of the generator.

Algorithm for generating a bit of a pseudo-random sequence

Step 1. Using $LFSR_1$ and $LFSR_2$, generate the next 16 bits of two pseudo-random sequences, which must then be multiplexed into 16 elements of the quaternary sequence $[a_1\ a_2\ a_3\ a_4\ a_5\ a_6\ a_7\ a_8\ a_9\ a_{10}\ a_{11}\ a_{12}\ a_{13}\ a_{14}\ a_{15}\ a_{15}]$ — the initial state of the cellular automaton.

Step 2. The evolution rule is applied $t=7$ times to each element of the cellular automaton sequence. For each element of the sequence $a_i, i=1,2,...,16$, a triplet of elements $\{a_{(i-1)\bmod 16}, a_i, a_{(i+1)\bmod 16}\}$ is considered, where the element $a_{(i+1)\bmod 16}$ determines the index of the quaternary bent-sequence in the IV-set, while the elements $a_{(i-1)\bmod 16}, a_i$ determine the index of the element of the selected quaternary bent-sequence, the value of which will be used in the next step of evolution.

Step 3. After $t=7$ steps of the evolution iterations of the cellular automaton, the j-th bit of the pseudorandom sequence is calculated as

$$g_j = \left(\sum_{h=1}^{16} a_h\right) \bmod 2. \tag{4}$$

The results of testing

The results of testing of the proposed PRKSG are given for the following initial data. The following primitive irreducible polynomials are used to construct $LFSR_1$ and $LFSR_2$

$$\begin{cases} f_1(x) = x^{83} + x^{46} + x^{45} + x + 1; \\ f_2(x) = x^{31} + x^{21} + x^{12} + x^3 + x^2 + x + 1, \end{cases} \tag{5}$$

while the following initial states are selected

$$\begin{cases} \alpha_1 = \{11111111111101011111110111111111111111111111 \\ \qquad\qquad 11111111111001111101011011010010110100\}; \\ \alpha_2 = \{10011010111110010011100010110 00\}. \end{cases} \tag{6}$$

Thus, with other non-secret parameters, the value of protection levels number of the PRKSG will be equal to $\Psi = 2^{83}2^{31} = 2^{114}$, which is considered as sufficient. It is obvious that the value of protection levels number can be easily scaled, if necessary, by choosing primitive irreducible polynomials for $LFSR_1$ and $LFSR_2$ of the necessary degree.

The following set is selected as the IV-set of quaternary bent-sequences

$$\begin{array}{ll} H_1 = \{0331132333230113\}; & H_3 = \{3220301121111013\}; \\ H_2 = \{3222302222103101\}; & H_4 = \{3221020030012000\}. \end{array} \tag{7}$$

For the purposes of experimental research of the stochastic properties of the proposed PRKSG, the 5 000 000 bits of pseudorandom sequence were generated based on the initial data (5), (6), and (7), which were presented in the form of an image shown in Fig. 2.

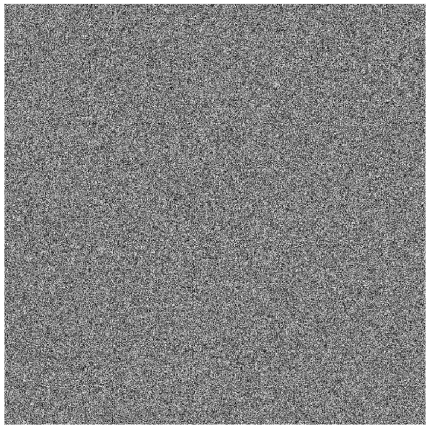


Fig. 2. Graphical representation of a pseudo-random sequence generated by the developed PRKSG

In the Table 1, we present the results of the research of compliance of the developed PRKSG with NIST test set [1].

Table 1

The results of testing the developed PRKSG by the set of NIST tests set

No.	Test	P-value	Pass rate
1	Monobit test	0.8279	✓
2	Frequency within block test	0.9050	✓
3	Runs test	0.6788	✓
4	Longest run ones in a block test	0.3916	✓
5	Binary matrix rank test	0.9980	✓
6	DFT test	0.4676	✓
7	Non overlapping template matching test	1	✓
8	Overlapping template matching test	0.2565	✓
9	Maurers universal test	0.1880	✓
10	Linear complexity test	0.3440	✓
11	Serial test	0.0490	✓
12	Approximate entropy test	0.1002	✓
13	Cumulative sums test	0.4000	✓
14	Random excursion test	0.3192	✓
15	Random excursion variant test	0.2170	✓

Analysis of the data presented in Table 1 allows us to draw a conclusion about the full compliance of the sequences generated by the developed PRKSG with the set of NIST tests, which confirms its high effectiveness. We also note that the high degree of complexity of the relationship between key elements and the generated gamma allows us to draw a conclusion about the high level of cryptographic strength of the developed generator. Thus, the developed generator can be recommended for use in practical applications.

Conclusions

Let us note the main results of the performed research:

1. The scheme of an effective PRKSG based on a cellular automaton and IV-set of quaternary bent-sequences, including two LFSR, is proposed. The proposed scheme is characterized by the simplicity of software implementation, as well as a high level of cryptographic strength in terms of the complexity of the relationship between the elements of the short key and the generated bits of the output sequence. The value of protection levels number of the developed generator is easily scalable and in the considered example is equal to $\Psi = 2^{114}$, which is sufficient.

2. Performed research of the proposed PRKSG showed its full compliance with all stochastic quality tests of the NIST set, which is a confirmation of the high effectiveness of the developed generator and allows us to recommend its use in practical applications.

References

1. A statistical test suite for random and pseudorandom number generators for cryptographic applications. Gaithersburg, MD : U.S. Dept. of Commerce, Technology Administration, National Institute of Standards and Technology, 2000. 153 p.
2. Mazurkov M. I., Sokolov A. V., Barabanov N.A. The key sequences generator based on bent functions dual couples. *Proceedings of Odesa Polytechnic University*. 2013. No. 3. P. 150-156.
3. Ivanov M. A., Chugunkov I. V. Theory, application and evaluation of the quality of generators of pseudo-random sequences. Moscow: KUDITS-OBRAZ, 2003. 240 p.
4. Sokolov A.V., Khimenko M.V. Testing key sequence generators based on perfect algebraic constructions. *Science and social life of Ukraine in the era of global challenges for humanity in the digital era. International scientific-practical conference on the occasion of the 30th anniversary of the declaration of independence of Ukraine and the 25th anniversary of the adoption of the Constitution of Ukraine.* Odesa: Helvetyka Publishing House, 2021. Vol. 1, P. 610-613.
5. Sokolov A.V. The cellular automata key sequences generator. *Proceedings of the ONPU*, 2014. No. 1(43). P. 180-186.
6. Szaban M., Seredynski F. Cryptographically Strong S-Boxes Based on Cellular Automata. *Lecture Notes in Computer Science*. 2008. Vol. 5191. P. 478-485.
7. Schmidt K. Quaternary Constant-Amplitude Codes for Multicode CDMA. *IEEE International Symposium on Information Theory*. Nice. 2007. P. 2781-2785.
8. Sokolov A.V. Properties of the full class of quaternary bent-functions of two variables. *Journal of Discrete Mathematical Sciences and Cryptography*. 2022. Vol. 25, No. 8. P. 2569-2582.
9. Sokolov A.V., Zhdanov O.N. Cryptographic constructions based on many-valued logic functions. Monograph. Scientific thought, 2020. 192 p.

УДОСКОНАЛЕННЯ АЛГОРИТМУ ГЕНЕРАЦІЇ ПСЕВДОВИПАДКОВИХ КЛЮЧОВИХ ПОСЛІДОВНОСТЕЙ НА ОСНОВІ КЛІТИННОГО АВТОМАТУ І БЕНТ-ПОСЛІДОВНОСТЕЙ БАГАТОЗНАЧНОЇ ЛОГІКИ

М.В. Хименко, А.В. Соколов

Національний університет «Одеська політехніка»
Україна, Одеса, 65044, пр-т Шевченка, 1, radiosquid@gmail.com

Одним із найважливіших криптографічних конструктів, що лежить в основі сучасних систем захисту інформації, є криптографічно захищені генератори псевдовипадкових ключових послідовностей, які застосовуються у найрізноманітніших задачах, починаючи від створення векторів ініціалізації, ключової інформації та формування стеганошляху, закінчуючи їх роботою у складі повноцінних потокових криптографічних алгоритмів, для яких вони складають найважливіший компонент. Наявні на сьогоднішній день генератори псевдовипадкових ключових послідовностей характеризуються або досить складною для програмної реалізації структурою, або недостатньою криптографічною захищеністю, що робить актуальною задачу розробки ефективних криптографічно захищених генераторів псевдовипадкових ключових послідовностей, що володіють високим рівнем стохастичної якості. У даній статті запропоновано схему ефективного генератора псевдовипадкових ключових послідовностей на основі клітинного автомату, а також таких досконалих алгебраїчних конструкцій багатозначної логіки, як IV-набори четвіркових бент-

послідовностей, що володіють максимальним рівнем дистанційної нелінійності. Запропонований генератор характеризується значною складністю взаємозв'язку вихідних бітів псевдовипадкової послідовності та елементів короткого ключа, на основі якого вони генеруються, що обумовлює високий рівень його криптографічної стійкості, при цьому число рівнів захисту запропонованого генератора є легко масштабованим в разі необхідності. Наявність у запропонованій схемі лише двох двійкових регістрів зсуву з лінійним зворотним зв'язком робить її адаптованою до програмної реалізації. Проведені дослідження дозволили встановити, що генеровані запропонованим генератором псевдовипадкові послідовності відповідають всім стохастичним тестам з набору NIST, що дозволяє рекомендувати його для використання на практиці.

Ключові слова: генератор псевдовипадкових ключових послідовностей, бент-послідовність, клітинний автомат.

DOI 10.15276/imms.v12.no3.144
UDC 517:532.516.001.57

Informatics and Mathematical Methods in Simulation
Vol. 12 (2022), No. 3, pp. 144-153

RESEARCH OF SOLVABILITY OF TASK OF AUTHENTICATION OF WATER-OIL MIXTURES ON THE PARAMETERS OF TUNING OF MATHEMATICAL MODEL

S.A. Polozhaenko, F.G. Garaschenko, L.L. Prokofieva

National Odesa Polytechnic University
Shevchenko ave., 1, Odesa, Ukraine; e-mail: sanp277@gmail.com

The formulation of the problem is set by the parametric identification for oil-water reservoirs in the case when one of the fluids being filtered is anomalous. Therewith, the identification problem is defined as an optimal control problem reduced to finding the extremum of the quality criterion (functional). The conditions of the existence and uniqueness of the solution to identify the mathematical model adjustment are obtained alongside with the differentiability of the quality criterion, and therefore the corresponding theorems are proved. Solving the problems of modelling and identifying anomalous diffusion processes is associated with a number of fundamental difficulties, both staging and computational. In this sense, it should be noted, in particular: the non-linear nature of the processes under study; the complexity of the geometry of the spatial modelling area and its boundaries; limitedness of the vector of measurements of the state space of the process and the number of points of application of control actions; high dimensions of the resulting finite-dimensional analogues of the mathematical model (MM). Mathematical methods for describing anomalous diffusion processes with a multiplicative representation of state functions, as well as for the case of multicomponent diffusing systems, have not received sufficient development. These problems require not only development, but also the development of new methods for studying anomalous diffusion processes. The pronounced direction of the development of anomalous diffusion processes determines the adequacy of their mathematical formalization based on the apparatus of variational inequalities.

Keywords: mathematical model, variational inequalities, mathematical method, modeling and identifying.

Introduction

The solution of the problem of modeling water-oil fields assumes that the values of the coefficients of the differential operators of these variational inequalities are known, which, in turn, are determined by the physical parameters of the modeling environment. For fluid mechanics problems, these are: porosity and permeability. However, when solving practical problems, quite often the values of these parameters are not known in advance, and, therefore, the functions describing them are not a priori set, or, in other words, the coefficients of the differential operators of the corresponding MM are not determined. This circumstance makes it necessary to formulate and solve the problems of identifying the parameters of the physical medium that precede the solution of the problems of controlling the processes under study (and if the coefficients of the initial MM are not completely determined, then the modeling problems).

It should be pointed out that the identified parameters can be not only functions of spatial coordinates, but also of the desired functions reservoir pressure and water saturation.

Note that the problems of identifying the parameters of the pore medium were previously solved for oil and oil and gas reservoirs (for example, [1, 3]. However, these problems were solved based on the assumption of ideal fluid filtration. In the case of filtration of liquids that do not obey the Darcy law, a number of important aspects arise that qualitatively change the formulation of the identification problem:

1. From the interaction with a porous medium having specific physical and chemical parameters, the filtering liquid can acquire an anomalous character, which requires the use of adequate MM when solving practical problems.

2. The result of solving the problem of modeling an oil reservoir can be the achievement of a limiting pressure gradient, which leads to the subsequent formulation and solution of the problem of determining stagnant zones, as well as their physical parameters.

3. In the case of multiphase filtration, which differs in that the filtering fluid only partially obeys the Darcy law (when a viscous fluid is displaced by a viscous fluid), the general identification problem is divided into particular problems of determining parameter fields for zones of predominant rheology of anomalous and viscous fluids, which, in the general case, they can have different formulations. In this case, it should also be taken into account that the space of states of a multiphase fluid is characterized by fields of two functions: and .

4. The water-driven regime of oil field development, when presented in the form of MM, is clearly non-linear, which, in turn, leads to a non-trivial formulation of the identification problem, when the desired parameter fields are found in the class of non-linear functions.

Purpose of the work

The purpose of the work is to obtain conditions for solving the problem of parametric identification of water-oil mixtures when presenting mathematical models of the latter in the form of variational inequalities.

Main part

In the practice of the geophysical research and oil production the spatial soil medium denotes the layer, which in addition to the geological components of different types of rocks, the horizons of groundwater and fluid minerals, in particular, also includes a number of technological components, such as production and injection wells etc. The reservoir porosity and permeability of its material should be considered as the most important geological characteristics. These characteristics determine, respectively, the relative share of the amount of space occupied by the rock itself, and the penetrating ability of the medium for the intrastratal fluid - phase to be infiltrated (filtrated) through it. It should be noted that the filtering intrastratal fluids in terms of the hydrodynamic theory can be regarded as viscous (ideal), obeying a linear Darcy law of motion, or as viscoplastic (abnormal) whose motion can not be described within the bounds of the mentioned law. [1] Viscoplasticity should be understood in terms of compressibility, which is specified by the oil complex fractional composition in particular. The most common technological mode of oil production is artificially created pressure by pumping water into the injection wells. This filtering is called viscoplastic rheology of viscoplastic (oil) and viscous (water) fluids [1]. The mathematical model (MM) of a physical process in the case of the collaborative filtering of viscoplastic and viscous fluids in the reservoir system can be represented as follows [2,3] (here and hereafter the index or parameters of summation will be denoted by $i, j, j_1, j_2, \ldots$ will be for the corresponding variables):

$$-\frac{m\partial S_2}{\partial t}(v - S_2) - \int_\Omega \sum_{i=1}^{n}\left[k_1 \frac{\partial^2 P}{\partial z_i^2}|v|\right]dz + \int_\Omega \sum_{i=1}^{n}\left[k_1 \frac{\partial^2 P}{\partial z_i^2}|S_2|\right]dz \geq \frac{1}{h}\sum_{j=1}^{K_1}\zeta_j(z)Q_{1_j}(t) \quad \forall v, S_2 \in K \tag{1}$$

$$-\frac{m\partial S_2}{\partial t} - \int_\Omega \sum_{i=1}^{n}\left(k_2 \frac{\partial^2 P}{\partial z_i^2}\right)dz = \frac{1}{h}\sum_{j=1}^{K_2}\zeta_j(z)Q_{2_j}(t) \tag{2}$$

$$P(0,z) = P_0(z) \quad S_2(0,z) = S_{2_0}(z) \tag{3}$$

$$\frac{\partial S_2(t,z)}{\partial \eta} \geq 0;\ S_2(t,z) < S_{2_{\max}} \tag{4}$$

$$\frac{\partial S_2(t,z)}{\partial \eta} = 0;\ S_2(t,z) \geq S_{2_{\max}} \qquad (5)$$

where $P = P(t,z)$ — the distributed function of intratrastal pressure; $S_2 = S_2(t,z)$ — the distributed function of of water saturation; $v = v(t,z)$ — the distributed test function (with respect to the function of water saturation); $P_0(z)$, $S_{2_0}(z)$ — the initial values of the functions, of the intrastratal pressure and of water saturation respectively; $S_{2_{\max}}$ — the maximum value of water saturation; $k_1 = k_1(z)$, $k_2 = k_2(z)$ — the reservoir permeability of the material for the corresponding phase (index 1 — oil, index 2 — water); $m = m(z)$ — the porosity of the reservoir material; h — the bulk of reservoir rock; $Q_{1_j}(t)$, $Q_{2_j}(t)$ — the consumption function of the corresponding phases (debits); $\zeta_j(t)$ — the function determining the nature of fluid withdrawal from the j-th hole; K_1, K_2 — a number of production and injection wells, respectively; Ω — the spatial region where a physical process is developing; t — temporal value; z — spatial value; K — the functional space of the function definition for water saturation respectively; n — the number of spatial variables; η — normal to the boundary G of the spatial domain Ω.

Solving the direct problem of the research, i.e., tasks of modeling, filtration processes described by the system of the form (1) — (5) suggests that the values of coefficients of the differential operators for the corresponding expressions, defined by the physical parameters of the medium are known — in this case by the porosity $m(z)$ and permeability of the reservoir $k_l(z)\ (l = 1,2)$. However, in practice, quite often the values of these parameters are not known and, therefore, the functions describing them are not specified a priori, and , or in other words, the coefficients the differential operators for the corresponding MM are not defined. The given circumstance conditions the necessity to formulate and solve the identification problems of the parameters in the physical environment (inverse problems) - the porosity and permeability of the preceding the solution for managing the process being investigated, and, if the coefficients of the original MM are not completely defined, then the modeling problems as well. Therewith, the porosity and permeability are the parameter settings for the MM of the physical process studied.

The problems of identification of the parameters for the reservoir system have been, for example, earlier solved for oil and oil-gas reservoir [4]. However, their decision was made on the assumption of ideal filtering liquids. In case of abnormal fluid filtration, a number of important aspects qualitatively change the problem of identification:

— interacting with a porous medium, with specific physical and chemical parameters the filtering fluid can acquire anomalous character that requires the use of adequate MM for solving practical problems;

— the result of solving the problem for water-oil reservoir simulation can be considered when the intrastratal pressure achieves the limiting gradient that leads to the subsequent formulation and solution of problem of determining the therein dead zones, as well as the problem of identification of the physical parameters in the reservoir;

— in case of the multiphase filtration the filterable mixture of anomalous and ideal fluids only partially obeys Darcy's law: for example, when displacing viscoplastic fluid with viscous fluid, the general problem of identification is divided into individual tasks of determining the zones of the parameter fields in preferential rheology of anomalous and viscous fluids that, in general, can have a different setting;

— MM of water drive in oil field development has a clearly pronounced non-linear character, which, in its turn, results in setting a non-trivial problem of

identification and finds the required parameter fields in the class of nonlinear functions when being solved.

In what follows, the problem of identification of the filtration processes in porous media will refer to the determination of the fields of the porosity parameters $m(z)$ and permeability of the medium $k_l(z)\,(l=1,2)$ based on the results of measuring the intrastratal pressure $P(t,z)$ and flow rates $Q_j(t)$ in the system of wells which cover the reservoir.

The formalized statement of problem of identifying the anomalous fluids of the filtration processes in porous media as an optimization problem is offered. Let $m'(z)$ and $k_l'(z)\,(l=1,2)$ are the exact values of porosity parameters and permeability of the medium, respectively. For the j-th well in the time interval $t\in(0,t_k)$, the measured intrastratal pressure $P(t,z)$ of the filterable fluid is indicated through

$$F_j^P(t)=\int\limits_{\Omega_j}P'(t,z)dz+\varepsilon_j^P(t),\ j=1,...,(K_1+K_2) \tag{6}$$

and water saturation $S_2(t,z)$ in the reservoir through

$$F_j^S(t)=\int\limits_{\Omega_j}S_2{}'(t,z)dz+\varepsilon_j^S(t),\ j=1,...,(K_1+K_2) \tag{7}$$

where $P'(t,z)$, $S_2{}'(t,z)$ are the values of the intrastratal pressure and water saturation, determined in accordance with a mathematical model for the exact type (1) — (5) of the parameter values $m'(z)$ and $k_l'(z)\,(l=1,2)$; $\varepsilon_j^P(t)$ and $\varepsilon_j^S(t)$ — are respectively, the measurement error of the intrastratal pressure and water saturation in the j-th well. [4]

The functionals are introduced into consideration

$$J_1[m(z),k_1(z)]=\sum_{j=1}^{K_1+K_2}\left\{\int\limits_{T_j}\left[P'(t,z_j,m,k_1)-F_j^P(t)\right]^2dt+\int\limits_{T_j}\left[S_2{}'(t,z_j,m,k_1)-F_j^S(t)\right]^2dt\right\} \tag{8}$$

$$J_2[m(z),k_2(z)]=\sum_{j=1}^{K_1+K_2}\left\{\int\limits_{T_j}\left[P'(t,z_j,m,k_2)-F_j^P(t)\right]^2dt+\int\limits_{T_j}\left[S_2{}'(t,z_j,m,k_2)-F_j^S(t)\right]^2dt\right\} \tag{9}$$

where T_j is the period of time when the measurement $F_j^P(t)$ and $F_j^S(t)$, is done.

Since the exact values of the pressure $P'(t,z_j,m,k_1)$ and $P'(t,z_j,m,k_2)$, as well as the water saturation $S_2{}'(t,z_j,m,k_1)$ and $S_2{}'(t,z_j,m,k_2)$ included in the expressions (8), (9), are physically the same value i.e. mathematically $J_1=J_2$), then only one of the functionals, e.g. J_1, will be taken into account in the subsequent arguments.

One possible approach to the solution of formulated problem of identification is representing it in the form of an optimal control problem. Quality criterion for this can be a functional (8), and the problem itself in terms of the optimization will be as follows: to determine $\hat{m}(z)$, $\hat{k}_1(z)$ for which

$$J_1(\hat{m},\hat{k}_1)\le J_1(m,k_1)\ \forall(m(z),k_1(z))\in\Lambda_d, \tag{10}$$

where Λ_d is the admissible domain to determine the parameter fields $m(z)$, $k_1(z)$.

The aim to qualitatively analysis the problem of identification for water-oil reservoirs by the parameters of the MM settings in the work conducted is studying the existence and uniqueness of problem solving (10), as well as establishing the fact of differentiability of the functional $J_1[m(z),k_1(z)]$ in (8) by the of porosity and permeability parameters. In this regard, the following theorems are formulated and proved.

Theorem 1. For a set of functions defined by (6), (7) and the admissible domain of the parameters $\forall\Lambda_d^m$, $\Lambda_d^k \in \Lambda_d$, the problem (10) has, at least, one solution, and this solution is the only one.

Proof. Given the physical meaning of the operators and domain of admissible values of variables included in the system (1) — (5), their affiliation the corresponding class of spaces is written as

$$P(t,z) \in L^2(\Omega) = H(\Omega);\ \ S_2(t,z) \in L^2(\Omega) = H(\Omega);$$

$$\frac{1}{h}\sum_{j=1}^{K_1}\zeta_j(z)Q_{1_j}(t) = f_1(t,z) \in L^2(\Omega);\ \ \frac{1}{h}\sum_{j=1}^{K_{21}}\zeta_j(z)Q_{2_j}(t) = f_2(t,z) \in L^2(\Omega);$$

$$\int_\Omega \sum_{i=1}^{n}\left[k_1\frac{\partial^2 P}{\partial z_i^2}|v|\right]dz = A_1'(P,v,t,z) \in L^2(\Omega);$$

$$\int_\Omega \sum_{i=1}^{n}\left[k_1\frac{\partial^2 P}{\partial z_i^2}|S_2|\right]dz = A_1'(P,S_2,t,z) \in L^2(\Omega);$$

$$\sum_{i=1}^{n}\left(k_1\frac{\partial^2 P}{\partial z_i^2}\right) = A_1''(P,t,z) \in L^2(\Omega),$$

where $L^2(\Omega)$ is space of square-integrable functions.

Let a given functional space is $W^P = H^1(\Omega);\ W^S = H^1(\Omega);\ H(\Omega) = L^2(\Omega)$, where $H^1(\Omega)$ is Sobolev space of order 1, defined as follows

$$H^1(\Omega) = \left\{\omega|\omega \in L^2(\Omega);\ \frac{\partial\omega}{\partial z_i} \in L^2(\Omega),\ i = 1,2\right\}.$$

It is assumed that there are sets of elements in spaces W^P and W^S, which are generated by a basis for which the following relations are true

$$\left(\left(w_j^P,\omega\right)\right) = \beta_j^P\left(w_j^P,\omega\right)\ \forall w^P \in W^P;\ \forall j = 1,2,...,q,$$

$$\left(\left(w_j^S,\omega\right)\right) = \beta_j^S\left(w_j^S,\omega\right)\ \forall w^S \in W^S;\ \forall j = 1,2,...,q.$$

Since the original system (1) — (5) is infinite, which is impossible to obtain an analytical solution for, it is necessary to pass to a discrete space for its numerical implementation. Then for the discrete space $W: W_n = \{w_1, w_2, ..., w_n\}$ the system, defining the problem (1) — (5) is written

$$-\left(\frac{m\partial S_2}{\partial t}, w_j^S\right)\left(v - S_2, w_j^S\right) - A_1'\left(P_q,v,t,z,w_j^P\right) + A_1'\left(P_q,v,t,z,w_j^P\right) \ge f_1\left(z,w_j^P\right);\qquad j = 1,2,...,q \tag{11}$$

$$\left(\frac{m\partial S_2}{\partial t}, w_j^S\right) - A_1''\left(P_q,t,z,w_j^P\right) = f_2\left(z,w_j^P\right);\ j = 1,2,...,q \tag{12}$$

$$\overline{P_q}(0) = \overline{P_{0_q}} \to P_0 \in L^2(\Omega);\ \overline{S_{2q}}(0) = \overline{S_{2_{0_q}}} \to S_{2_0} \in L^2(\Omega) \tag{13}$$

where the set $\left\{P_q(t,z), S_{2_q}(t,z)\right\}$ is the approximate solution of (1) — (5), represented as

$$\overline{P}_j(t,z) = \sum_{j=1}^{q}\beta_j^P(t)w_j^P;\ \overline{S_2}_j(t,z) = \sum_{j=1}^{q}\beta_j^S(t)w_j^S,\ \forall t \in [0,t_q];$$

$\beta_j^P(t)$ and $\beta_j^S(t)$ are the weighting coefficients

The resulting solution is local because it is valid only on the local interval $t \in [0,t_q]$, and t_q is a discrete analog of t_k. It should be proved that $t_q = t_k$, i.e., that the local solution can be extended to the whole-time interval $\forall t \in [0,t_k]$.

For this purpose, the termwise multiplication of the derivatives of j-th dynamics ratios (11), (12) by $\beta_j^P(t)$ and $\beta_j^S(t)$, respectively, as well as their summation is performed, and as result the system of equations has the form of

$$-\left(\frac{m\partial S_{2q}(t,z)}{\partial t}, S_{2q}(t,z)\right)\left(v - S_{2q}(t,z)\right) - A_1'\left(P_q(t,z), v, P_q(t,z)\right) + \\ + A_1'\left(P_q(t,z), S_{2q}(t,z), P_q(t,z)\right) \geq f_1\left(z, P_q(t,z)\right) \quad (14)$$

$$\left(\frac{m\partial S_{2q}(t,z)}{\partial t}, S_{2q}(t,z)\right) - A_1''\left(P_q(t,z), P_q(t,z)\right) = f_2\left(z, P_q(t,z)\right) \quad (15)$$

$$P_q(0) = P_0;\ S_{2_q}(0) = S_{2_0} \quad (16)$$

where it turns out that the solution of $\{P(t,z), S_2(t,z)\}$ systems (1) — (5) exist in the whole interval $[0,t_k]$, i.e. $t_q = t_k$.

Next, some operators Y^P and Y^S are introduced that perform projection H on W^P and H on W^S in n-dimensional space of R^n for the norms of $\|P_q(t,z)\|$ and $\|S_{2_q}(t,z)\|$. Then, the expressions of the dynamics (11), (12) can be represented as

$$-Y^P\frac{m\partial S_2}{\partial t} \geq Y^P A_1'\left(P_q, v, z\right) - Y^P A_1'\left(P_q, S_2, z\right) + Y^P f_1(t), \quad (17)$$

$$Y^S\frac{m\partial S_2}{\partial t} = Y^S A_1''\left(P_q, z\right) + Y^S f_2(t) \quad (18)$$

and here (17) and (18) are performed in the spaces of W^P and W^S almost for all $t \in (0,t_k)$. The above arguments imply that the operators $Y^P A_1'\left(P_q, v, z\right), Y^P A_1''\left(P_q, z\right)$ belong to the space boundary of $L^2\left(0,t_k,W^P\right)$, and the operator of $Y^P A_1'\left(P_q, S_2, z\right)$ — to the space boundary $L^2\left(0,t_k,W^S\right)$.

Finally, it follows that the required solution of $\{P(t,z), S_2(t,z)\}$ can be obtained from the approximate of $\{P_q(t,z), S_{2_q}(t,z)\}$, and thus the following conditions for convergence are taken into account:

— $P_q \to P$ in the space of $L^2\left(0,t_k,W^P\right)$ and $S_{2_q} \to S_2$ in the space of $L^2\left(0,t_k,W^S\right)$ — *weak*;

— $\frac{m\partial S_{2_q}}{\partial t} \to \frac{m\partial S_2}{\partial t}$ in the space of $L^2\left(0,t_k,W^S\right)$ — *weak*;

— $P_q \to P$ in the space of $L^\infty\left(0,t_k,W^P\right)$ and $S_{2_q} \to S_2$ in the space of $L^\infty\left(0,t_k,W^S\right)$ — *weak*.

Therefore, the implemented limiting transition is the proof that the set of $\{P(t,z), S_2(t,z)\}$ provided by the specified conditions of convergence, is a solution of the (1) — (5) system for the parameters of $(m(z), k_1(z)) \in \Lambda_d$.

The next phase of the qualitative analysis is the proof of the uniqueness of the problem solving of (1) — (5). Suppose that (1) — (5) has two solutions, defined by the set of $\{P^1(t,z), S_2^1(t,z)\}$ and $\{P^2(t,z), S_2^2(t,z)\}$. Then it may also be assumed that for each point of the domain Ω there are numbers

$$\eta^P = P^1(t,z) - P^2(t,z);\ \eta^S = S_2^1(t,z) - S_2^2(t,z).$$

Replacing in terms of the systems dynamics of (1) — (5) the functions of $P(t,z)$, $S_2(t,z)$respectively by $P^1(t,z)$, $S_2^1(t,z)$ and $P^2(t,z)$, $S_2^2(t,z)$, it is possible to get two systems where the termwise subtraction will lead to the result

$$\left(\frac{m\partial\eta^S}{\partial t}\right)(v-\eta^S)-\left[A_1'(P^1,v,t,z)-A_1'(P^2,v,t,z)\right]+\left[A_1'(P^1,S_2,t,z)-A_1'(P^2,S_2,t,z)\right]\geq 0 \quad (19)$$

$$\left(\frac{m\partial\eta^S}{\partial t}\right)-\left[A_1''(P^1,t,z)-A_1''(P^2,t,z)\right]=0 \quad (20)$$

$$\eta^P(0)=0;\ \eta^S(0)=0 \quad (21)$$

The expressions in square brackets in (19) and (20), based on the definition of the operators $A_1'(\cdot)$ and $A_1''(\cdot)$, can be presented as

$$A_1'(P^1,v,t,z)-A_1'(P^2,v,t,z)=\int_\Omega\sum_{i=1}^n\left\{k_1\frac{\partial^2}{\partial z_i^2}\left[\beta(P^1)-\beta(P^2)\right]|v|\right\}dz\ ,$$

$$A_1'(P^1,S_2^1,t,z)-A_1'(P^2,S_2^2,t,z)=\int_\Omega\sum_{i=1}^n\left\{k_1\frac{\partial^2}{\partial z_i^2}\left[\beta(P^1)-\beta(P^2)\right]|S_2^1-S_2^2|\right\}dz\ ,$$

$$A_1''(P^1,t,z)-A_1''(P^2,t,z)=\sum_{i=1}^n\left\{k_1\frac{\partial^2}{\partial z_i^2}\left[\beta(P^1)-\beta(P^2)\right]\right\}dz\ .$$

Thus the system (19) — (21) can be presented as

$$\begin{aligned}&|S_2^1-S_2^2|\left(\frac{m\partial\eta^S}{\partial t}\right)(v-\eta^S)-\int_\Omega\sum_{i=1}^n\left\{k_1\frac{\partial^2}{\partial z_i^2}\left[\beta(P^1)-\beta(P^2)\right]|P^1-P^2||v|\right\}dz+\\&+\int_\Omega\sum_{i=1}^n\left\{k_1\frac{\partial^2}{\partial z_i^2}\left[\beta(P^1)-\beta(P^2)\right]|P^1-P^2||S_2^1-S_2^2|\right\}dz\geq 0\end{aligned} \quad (22)$$

$$|S_2^1-S_2^2|\left(\frac{m\partial\eta^S}{\partial t}\right)-\sum_{i=1}^n\left\{k_1\frac{\partial^2}{\partial z_i^2}\left[\beta(P^1)-\beta(P^2)\right]|P^1-P^2|\right\}dz=0 \quad (23)$$

$$\eta^P(0)=0;\ \eta^S(0)=0 \quad (24)$$

It is obvious that implementing the conditions of the system (22) — (24) is possible only under the condition that $P^1(t,z)=P^2(t,z)$, $S_2^1(t,z)=S_2^2(t,z)$ which proves the uniqueness of the solution of initial problem (1) — (5).

Thus, there is the solution of the problem in $L^2(\Omega)\bigcap L^\infty(0,t_k,H)$ and it is unique.

Now the differentiability of the functional (10) in the form of proving the following theorem is under study.

Theorem 2. For $(m(z),k_1(z))\in\Lambda_d$ the functional (10) has a weak derivative Λ_d (i.e., the derivative in the sense of Gateaux) in the domain R^n.

Proof. The functional derivative $J_1[m(z),k_1(z)]$ is defined as

$$\begin{aligned}&\delta J_1(m,k_1)=\int_\Omega\delta m(z)\left\{\left[\frac{\partial\left[P(t,z_j,m,k_1)-F_j^P(t)\right]}{\partial t}+\right.\right.\\&\left.\left.+\frac{\partial\left[S_2(t,z_j,m,k_1)-F_j^S(t)\right]}{\partial t}\right]\cdot p^*dt\right\}dz+\int_\Omega\delta k_1(z)\left\{\sum_{j=1}^{K_1+K_2}\left[\frac{\partial\left[P(t,z_j,m,k_1)-F_j^P(t)\right]}{\partial z_j}+\right.\right.\\&\left.\left.+\frac{\partial\left[S_2(t,z_j,m,k_1)-F_j^S(t)\right]}{\partial z_j}\right]\cdot\frac{\partial p^*}{\partial z_j}dt\right\}dz\end{aligned} \quad (25)$$

where $\{P(t,z), S_2(t,z)\}$ is the solution of the problem (1) — (5), and $p^*(t,z)$ is the solution of the adjoint system of the form

$$-m(z)\frac{\partial p^*}{\partial t}(v-S_2)-\left[A_1'(P,v,t,z)+A_1'(P,S_2,t,z)\right]\sum_{i=1}^{n}\left[k_1(z)\frac{\partial p^*}{\partial z_i}\right]\geq 0 \qquad (26)$$

$$-m(z)\frac{\partial p^*}{\partial t}-A_1''(P,t,z)\sum_{i=1}^{n}\left[k_1(z)\frac{\partial p^*}{\partial z_i}\right]=0 \qquad (27)$$

$$\frac{\partial p^*(t,z)}{\partial t}=0 \quad \Sigma=\partial\Omega\times(0,t_k) \qquad (28)$$

$$p^*(t_k,z)=0 \ \text{ for } \ \Omega \qquad (29)$$

The conjugate function satisfies the following conditions

$$p^*(t,z)\in L^2(0,t_k,H(\Omega))\bigcap L^\infty(0,t_k) \quad \frac{\partial p^*(t,z)}{\partial t}\in L^2(\Omega) \qquad (30)$$

Assuming that $(m(z),k_1(z))\to P(t,z)$ and $(m(z),k_1(z))\to S_2(t,z)$ are continuous on Λ_d and, consequently, have weak derivatives (ie, derivatives in the sense Gato) on $L^2(\Omega)$, we can prove that the criterion $J_1[m(z),k_1(z)]$ (8) is also Gateaux-differentiable, and its derivative Λ_d is

$$\delta J_1=-\int_0^{t_k}\int_\Omega\left[e^P(t,z)\delta P(t,z)+e^S(t,z)\delta S_2(t,z)\right]dz\,dt,$$

where

$$e^P(t,z)=-2\sum_{j=1}^{K_1+K_2}\left\{\frac{1}{|z_j|}\int_\Omega\left[P(t,z_j,m,k_1)-F_j^P(t)\right]dz\right\};$$

$$e^S(t,z)=-2\sum_{j=1}^{K_1+K_2}\left\{\frac{1}{|z_j|}\int_\Omega\left[S_2(t,z_j,m,k_1)-F_j^S(t)\right]dz\right\},$$

$\delta P(t,z)$ and $\delta S_2(t,z)$ — respectively increment of functions $P(t,z)$ and $S_2(t,z)$.

For the functions $\delta P(t,z)\in L^2(\Omega)$ and $\delta S_2(t,z)\in L^2(\Omega)$, given the accepted symbols, the expressions of the systems dynamics can be written

$$\left(\frac{\delta m(z)\partial\delta S_2}{\partial t}\right)(\delta v-\delta S_2)-A_1'(\delta P,\delta v,t,z)+A_1'(\delta P,\delta S_2,t,z)=$$

$$=\left(\frac{\delta m(z)\partial\delta S_2}{\partial t}\right)(\delta v-\delta S_2)-\int_\Omega\sum_{i=1}^{n}\left[\delta k_1(z)\frac{\partial\delta P}{\partial z_j}|\delta v|\right]dz+$$

$$\int_\Omega\sum_{i=1}^{n}\left[\delta k_1(z)\frac{\partial\delta P}{\partial z_j}|\delta S_2|\right]dz\leq f(t,z) \qquad (31$$

$$\left(\frac{\delta m(z)\partial\delta S_2}{\partial t}\right)-A_1''(\delta P,t,z)=\left(\frac{\delta m(z)\partial\delta S_2}{\partial t}\right)-\sum_{i=1}^{n}\delta k_1(z)\frac{\partial^2\delta P}{\partial z_j^2} \qquad (32)$$

Next, the function $\rho(t,z)\in L^2(\Omega)$ which can be defined by the following system is introduced into consideration

$$\left.\begin{array}{c}\left(\dfrac{m\partial\rho}{\partial t}\right)-A_1'(\rho,v,t,z)+A_1'(\rho,S_2,t,z)=\displaystyle\int_\Omega\left(e^P\rho+e^S\rho\right)dt;\\ \rho(t_k)=0,\end{array}\right\} \qquad (33)$$

and this system has a unique solution (which follows from the proof of Theorem 1), satisfying the conditions

$$\left.\begin{array}{c}\rho \in L^2(\Omega)\bigcap L^\infty(0,t_k,H),\\ \dfrac{\partial\rho}{\partial t}\in L^2(\Omega).\end{array}\right\} \tag{34}$$

Using the expressions (31) — (34) the following can be obtained

$$\delta J_1=\left(\delta m(z)\frac{\partial\delta S_2}{\partial t}\right)(\delta v-\delta S_2)-\int\limits_\Omega\sum_{i=1}^{n}\left[\delta k_1(z)\frac{\partial\delta P}{\partial z_j}|\delta v|\right]dz+\int\limits_\Omega\sum_{i=1}^{n}\left[\delta k_1(z)\frac{\partial\delta P}{\partial z_j}|\delta S_2|\right]dz \tag{35}$$

By equating in turn $p^*=\delta S_2$ и $p^*=\delta P$, the inequality (26) can be obtained from (35) and the relation (30) from (33). In addition, (35) results from (25). Hence Theorem 2 is proved.

We can write the derivative $J_1(m,k_1)$ by the parameters in the form of $m(z)$ and $k_1(z)$

$$\delta J_1=J_1(m,k_1)[\delta m(z),\delta k_1(z)]=\int\limits_\Omega\left[\delta m(z)\frac{\partial J_1(m,k_1)}{\partial m(z)}+\delta k_1(z)\frac{\partial J_1(m,k_1)}{\partial k_1(z)}\right]dz,$$

Where

$$\frac{\partial J_1(m,k_1)}{\partial m(z)}=\int\limits_0^{t_k}\frac{\partial S_2(t,z)}{\partial t}[v-S_2(t,z)]p^*(t,z)dt \tag{36}$$

$$\frac{\partial J_1(m,k_1)}{\partial k_1(z)}=\int\limits_0^{t_k}\left[A_1{}'(P,v,t,z)+A_1{}'(P,S_2,t,z)\right]\sum_{i=1}^{n}\frac{\partial P(t,z)}{\partial z_i}\frac{\partial p^*(t,z)}{\partial z_i}dt \tag{37}$$

The relations (36), (37) are convenient for the numerical calculation of the gradient of the functional $J_1[m(z),k_1(z)]$ while writing the optimization problem in the form (10).

A qualitative analysis of the problem of identification for water-oil reservoirs by the porosity and permeability parameters, which are the parameter settings of the MM for filtering process of the anomalous fluid, showed that there is a solution for the formulated problem of identification in the optimization setting and it is unique. In addition, the quality criteria in the formulated optimization problem is differentiable with respect to identifiability of the porosity and permeability parameters, which means the possibility to achieve extremum in its decision. In other words, a quality criterion for the optimization problem can be minimized by MM settings, and the initial problem of identification for water-oil reservoirs is the correct solution.

Conclusion

The statement of the problem of parametric identification of MM of multicomponent anomalous diffusion processes in the form of an optimal control problem is carried out.

A qualitative study of the problem of parametric identification of MMs of multicomponent anomalous diffusion processes has been carried out, during which existence and uniqueness theorems for the optimization problem posed have been proved. The differentiability of the accepted quality criterion with respect to the MM settings is also proved.

An approach to solving the problem of parametric identification of MMs of multicomponent anomalous diffusion processes, presented in an optimization formulation, is proposed. The approach is based on the procedure of the gradient

projection method. The possibility of applying the proposed approach to solving problems both in linear and non-linear formulations is substantiated.

References

1. Бернадинер М.Г., Ентов В.М. Гидродинамическая теория фильтрации аномальных жидкостей. М.: Наука, 1975. 199с.
2. Положаенко С.А. Оптимизационный подход к исследованию моделей объектов, представленных в виде вариационных неравенств. *Автоматика, автоматизация, электротехнические комплексы и системы*. 2002. № 1. С. 6–12.
3. Положаенко С.А. Математические модели процессов течения аномальных жидкостей. *Моделювання та інформаційні технології: Зб. наук. пр*. К.: ІПМЕ, 2001. Вип. 9. С. 14 – 21.
4. Ажогин В.В., Згуровский М.З. Автоматизированное проектирование математического обеспечения АСУ ТП. К.: Вища школа, 1986. 334с.

ДОСЛІДЖЕННЯ МОЖЛИВОСТІ РОЗВ'ЯЗУВАННЯ ЗАДАЧІ ІДЕНТИФІКАЦІЇ ВОДОНАФТОВИХ СУМІШЕЙ ПО ПАРАМЕТРАХ НАЛАШТУВАННЯ МАТЕМАТИЧНОЇ МОДЕЛІ

С.А. Положаєнко, Ф.Г. Гаращенко, Л.Л. Прокофьєва

Національний університет «Одеська політехніка»
пр-т Шевченка, 1, Одеса, Україна; ; e-mail: sanp277@gmail.com

Виконано постановку задачі параметричної ідентифікації для водо-нафтових пластів у випадку, коли одна з рідин, що фільтрується, має аномальний характер. При цьому задачу ідентифікації сформульовано як задачу оптимального управління, що зводиться до відшукання екстремуму критерію якості (функціонала). Одержано умови існування та єдиності розв'язку задачі ідентифікації за параметрами налаштування математичної моделі, а також диференційованості критерію якості, у зв'язку з чим доведено відповідні теореми. Розв'язок задач моделювання та ідентифікації аномальних процесів дифузії пов'язане з низкою важливих складностей як постановочного, так і обчислювального характеру. У цьому сенсі слід зазначити, зокрема: нелінійний характер досліджуваних процесів; складність геометрії просторової області моделювання та її границь; обмеженість вектора вимірювань простору станів процесу та числа точок прикладення управляючих впливів; високі розмірності результуючих кінцевовимірних аналогів математичної моделі (ММ). Не набули достатнього розвитку математичні методи опису аномальних дифузійних процесів при мультиплікативному представленні функцій стану, а також для випадку багатокомпонентних дифузних систем. Зазначені проблеми потребують як розвитку, так і розробки нових методів дослідження аномальних дифузійних процесів.Різко виражена спрямованість розвитку аномальних дифузійних процесів зумовлює адекватність їх математичної формалізації на основі апарату варіаційних нерівностей.

Ключові слова: математична модель, варіаційні нерівності, математичний метод, моделювання та ідентифікація.

DOI 10.15276/imms.v12.no3.154
UDC 004.9

Informatics and Mathematical Methods in Simulation
Vol. 12 (2022), No. 3, pp. 154-161

INTELLIGENT SYSTEM FOR ASSESSING AND FORECASTING THE RISK OF FAILURE OF COMPONENTS OF A COMPLEX TECHNICAL SYSTEM

A.V. Vychuzhanin

National Odesa Polytechnic University,
Ave.. Shevchenko, 1, Odesa, 65044, Ukraine; e-mail: v.v.vychuzhanin@op.edu.ua

The complexity of the composition and the increase in the number of technical systems lead to an increase in the intensity of their failures. As a result, there is a need to repair the equipment of complex technical systems, leading to system downtime. The search for failed components and the elimination of their failures contributes to an increase in the safety level of operation of complex technical systems. Diagnostics and prediction of failures of components of automated systems and mechanisms (subsystems, elements, intersystem and interelement connections) in real operation to find and eliminate the causes of failures remains an urgent task. The operational reliability of restored complex technical systems and their components is effectively achieved by the strategy of operating systems with technical condition monitoring based on technical diagnostic systems. Reducing failures and man-made risks in the operation of complex technical systems is facilitated by predicting their technical condition based on diagnostics. The article presents an intelligent system that operates using the developed model for assessing and predicting the risk of failure of components of a complex technical system using the example of a ship power plant. Building a model taking into account the hierarchical levels of subsystems (components), intersystem (interelement) connections of an intelligent system is based on the use of a priori information about failures of components of complex technical systems. The model connects the types of technical condition of components and diagnostic features of systems in the form of the risk of their failures. The use of a posteriori inference in Bayesian belief networks makes it possible to determine the risk of system component failures, taking into account the incoming diagnostic information and information about component failures. In order to build and research a diagnostic Bayesian network model of an intelligent system for assessing the risk of failures for a system for diagnosing and predicting the technical condition of the components of a complex technical system consisting of numerous variables, the software product GeNIe was used. The results of studies of the model for assessing and predicting the risk of failure of components of a complex technical system confirmed the possibility of predicting the risk of failure of components and the system as a whole.

Keywords: complex technical system, components, diagnostics, prediction, failure risk assessment, intelligent system, Bayesian belief network

Introduction

The complexity of the composition and the increase in the number of technical systems installed at various facilities lead to an increase in the intensity of their failures. As a result, there is a need to repair the equipment of the systems, which leads to its downtime.

When designing, manufacturing and operating complex technical systems (CTS), reliability is ensured by methods and means specific to each stage of the "life cycle" of systems. The operational reliability of the restored CTS and their components is effectively achieved by the strategy of operating systems with technical condition monitoring based on technical diagnostic systems [1-5]. The reduction of failures and man-made risks during the operation of CTS is facilitated by the prediction of their technical condition based on diagnostics.

Currently, the volume of implementation of automation, digitalization and artificial intelligence technologies in various industries continues to grow. For example,

in accordance with the requirements of the Register of Maritime Navigation, all modern ships must be equipped with automation systems for technical means using digital technologies, as well as artificial intelligence technologies [2,6-10]. Such systems should constantly monitor the components of the ship's CTS, analyze trends in changing the operating modes of the equipment of the systems, perform emergency transfers and provide decision support. To implement such a technology, appropriate algorithmic and software tools are needed to provide diagnostics, forecasting the technical state of systems, and support for decision-making that is adequate to the goal. The diagnostic algorithms used, as a rule, are based on the tolerance control of individual diagnostic parameters. At the same time, the volume of measuring and diagnostic information, the number of connections, dependencies of diagnostic features and types of technical states of systems can be significant. In theory, engineering practice, various methods are used to assess the risk of failure of CTS components.

An example of the application of risk theory is the logical development of a probabilistic approach for assessing the risk of failures [11,12]. With a probabilistic approach, the level of reliability is selected depending on the possible consequences of damage (failure) of system components. In this regard, the assessment of the risk of CTS failures lies in the unacceptable probability of their damage. However, the negative consequences of a failure in systems are often taken into account intuitively, implicitly, by taking certain values of the probability of failure-free operation or the safety factor of system components.

In artificial intelligence, various models of knowledge representation are actively developing. Bayesian belief networks (BBN) are a promising mathematical tool that can be used, in relation to diagnostic tasks, to take into account both the causal relationship between the types of CTS technical condition and diagnostic features, and the arrival of new information in the form of statistical data or predictive estimates. Bayesian networks allow combining a priori (initial) knowledge about an object with experimental data to obtain an a posteriori estimate [13,14].

Forecasting the state of CTS plays an important role in planning their operation. It is assumed that the actual technical condition of an object can be assessed by the results of monitoring its parameters, and predicting their changes allows the object to be operated until signs of a dangerous decrease in reliability appear. There are efficient algorithms and forecasting methods. Artificial intelligence models, in particular, neural networks, are being actively developed to solve forecasting problems [15,16]. However, the main problem for the productive operation of a neural network is the need for a significant amount of statistical data, which is difficult to obtain in real conditions due to a number of reasons (high cost of the systems under study, high costs for testing, limited time, etc.). The lack of a clear understanding in the choice of neural network architecture for solving various types of problems (pattern recognition, approximation, prediction, etc.) and areas of application also complicates their application.

The conceptual basis for the intellectualization of the solution of interrelated problems of diagnostics, forecasting and decision support is traditional for the class of unstructured and poorly formalized tasks: the impossibility of obtaining complete and objective information for making adequate decisions and the resulting need to involve informal (subjective, heuristic) information; the presence of uncertainty in the initial data, as well as the presence of ambiguity (multiple options) in the process of finding a solution; the need to develop and justify the desired solutions to the problem inconditions of strict time constraints, which are determined by the course of controlled processes; the need to correct and introduce additional information into the process of finding solutions, the interactive (dialogue, human-machine) nature of the logical inference of solutions. Taking these factors into account forces us to abandon traditional algorithmic methods and models of decision-making and management and move on to

intelligent technologies. Combined with the tasks of diagnosing and predicting, the task of modeling the behavior of the CTS acts as a source of data on the state of the object at the stages of system testing.

Thus, during the operation of CTS, an urgent task remains the improvement of methods and models aimed at accurate and prompt assessments, management of the risk of failures of CTS components.

Objective

The aim of the work is to improve the reliability of CTS operation based on the use of an intelligent system for assessing and predicting the risk of failures of components and systems as a whole.

Main part

Currently, Bayesian belief networks are actively developing in the field of modeling and knowledge representation [13,14]. When solving the problems of diagnosing CTS, BBN allow taking into account both the dependence between the types of technical systems and diagnostic features, taking into account the reliability of their checks, and the results of checking diagnostic features, data on failures of CTS components.

The model of an intelligent syste m for assessing and predicting the risk of failure of components of a complex technical system in the form of a BBN can be written as:

<M,S,R,L> (1)

where *M* - is the set of subsystems (elements) of the CTS; *S* - a set of intersystem (interelement) links of CTS; *R* - a set of diagnostic assessments of the risk of failures of subsystems (elements), intersystem (interelement) links of CTS; *L* - mapping of connections between the sets *M, S* and *R*, based on the CTS diagnostic model.

The set of subsystems (elements) of ship CTS, taking into account the hierarchical levels of subsystems (elements), is determined by:

$$M = \{\upsilon_{i_{S(E)}}^{<j_{S(E)}>} \mid i_{S(E)} = \overline{1, I_{S(E)}}; j_{S(E)} = \overline{0, J_{S(E)}}\}, \quad (2)$$

where $\upsilon_{i_{S(E)}}^{<j_{S(E)}>}$ - is the state of each subsystem (element) of the CTS; $i_{S(E)}$ - number of subsystem (element) of CTS; $j_{S(E)}$ - number of the hierarchical level of the subsystem (element) of the CTS; $I_{S(E)}$ - number of subsystems (elements) of CTS; $J_{S(E)}$ - number of hierarchical levels of subsystems (elements) of CTS

The state of each subsystem (element) of the CTS:

$$\upsilon_{i_{S(E)}}^{<j_{S(E)}>} = \{F_{\upsilon_{n_{S(E)}}}, F_{\upsilon_{i_{S(E)}}}, a_{\upsilon_{in_{S(E)}}}, a_{\upsilon_{on_{S(E)}}}\}, \quad (3)$$

where $F_{\upsilon_{n_{S(E)}}}$ - is the nominal performance of the subsystem (element) of the STS; $F_{\upsilon_{i_{S(E)}}}$ - operability of a subsystem (element) in case of its partial loss; $a_{\upsilon_{in_{S(E)}}}, a_{\upsilon_{on_{S(E)}}}$ - intersystem (interelement) connections incoming and outgoing to subsystems (elements), *in, on* – sequence number of incoming and outgoing intersystem (interelement) connections.

A set of intersystem (interelement) links of CTS:

$$S = \{\omega_{c,h}^{<b,q>} \mid c = \overline{1, C}; h = \overline{1, H}; b = \overline{1, B}; q = \overline{1, Q}\}, \quad (4)$$

where $\omega_{c,h}^{<b,q>}$ - is the state of each intersystem (interelement) connection; *c* – number of intersystem communication; *h* - is the number of the interelement bond; b is the number of the hierarchical level of intersystem communication; *q* - is the number of the hierarchical level of the interelement connection; *C* - is the number of intersystem connections; *H* - is the number of interelement bonds; *B* - is the number of hierarchical levels of intersystem links; *Q* - is the number of hierarchical levels of interelement connections

The state of each intersystem (interelement) connection

$$\omega_{c,h}^{<b,q>} = \{F_{\omega_{cn}}; F_{\omega_{cp}}; F_{\omega_{hn}}; F_{\omega_{hp}}\}, \tag{5}$$

where $F_{\omega_{cn}}$ - is the nominal performance of intersystem connections; $F_{\omega_{cp}}$ - operability of intersystem communication in case of its partial loss; $F_{\omega_{hn}}$ - nominal performance of the interelement connection; $F_{\omega_{hp}}$ - operability of intersystem communication in case of its partial loss.

A set of diagnostic assessments of the risk of failures of subsystems (elements), intersystem (interelement) links of CTS:

$$\begin{gathered} R < P, Y > \\ R_m = \{r_m \mid m = \overline{1, M}\}, \\ R_s = \{r_s \mid s = \overline{1, S}\}, \end{gathered} \tag{6}$$

where *M, S* - are determined based on the failure trees, presented as a set of risk of failures of subsystems (elements) and intersystem (interelement) links, taking into account their failure probabilities (*P*) and damages from failures (*Y*); r_m - risk of failures of subsystems (elements) of CTS; r_s - risk of failures of intersystem (interelement) connections.

The initial data for constructing a model of an intelligent system for assessing and predicting the risk of failures of components of a complex technical system on the example of a ship power plant (SPP) [17], based on a dynamic BBN, are: SPP scheme; the principle of operation of the SPP; probability of failures of CTS components.

The construction and study of the BBN of the probability of loss of working capacity, assessments of the risk of failures of CTS components was carried out using the GenNIe software product [18]. It is a fully portable C++ class library that implements graphical decision theory methods such as the Bayesian network. jobs and impact diagrams that are directly amenable to inclusion in intelligent systems. Its Windows user interface, Genie is a versatile and user-friendly development environment for graphical decision theory models. modeling tools into intelligent systems. The use of the GenNIe environment allows diagnosing each component of the CTS. Perform a regression analysis of the influence of each parent element of the network on its corresponding child element. Implement a graphical display of the results of predicting the risk assessment of failures of CTS components. Calculate the value of the probability of loss of performance, damage and risk assessments of failures of CTS components. When modeling the BBN of the SPP (Fig. 1), for various values of the probability (risk) of failure of the input element, the values of the probability (risk) of failures, the performance of the components of the SPP for 20,000 hours of its operation are determined. Symbols of the elements of the SPP are given in Table 1. The operating

state and failure, for example, of the SSV subsystem for the risk of failure at the input element of the SPP 0.014 is shown in Fig.2.

Table 1

Symbols of the components of the SPP

Component name	Symbol	Failure risk value
Input element	VHOD	0,26
Manual control of the main engine	RUGD	0,035
Compressed air system	SSV	0,047
Control system for propulsion and steering complex (PSC)	SUDRK	0,081
Boiler plant	KU	0,13
Ship power plant	SE	0,09
Fire fighting system	PS	0,01
Main engine	GD	0,16
Remote automated control system of the main engine	DAU	0,01
Ballast drainage system	BOS	0,019
Transfer of power from the main engine to the propeller	PM	0,003
Emergency drive PSC	AP	0,01

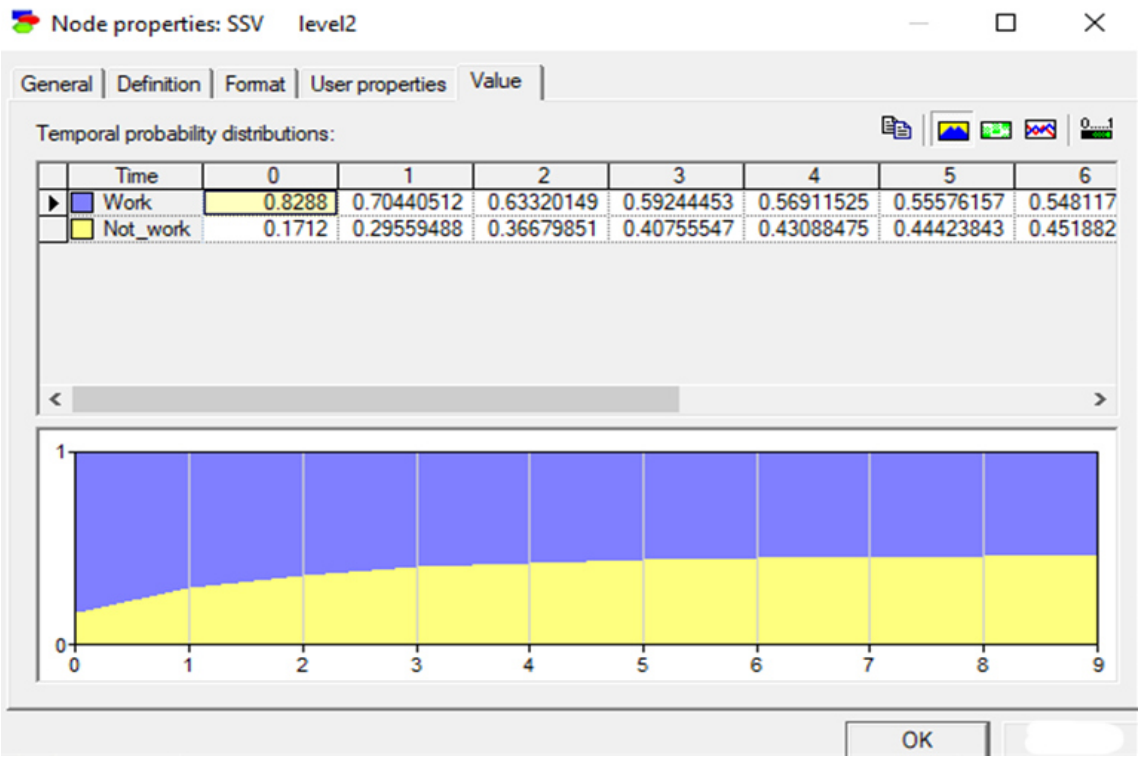


Fig.1. Operating state and failure of the SSV subsystem for the risk of failure at the input element of the SPP 0.014

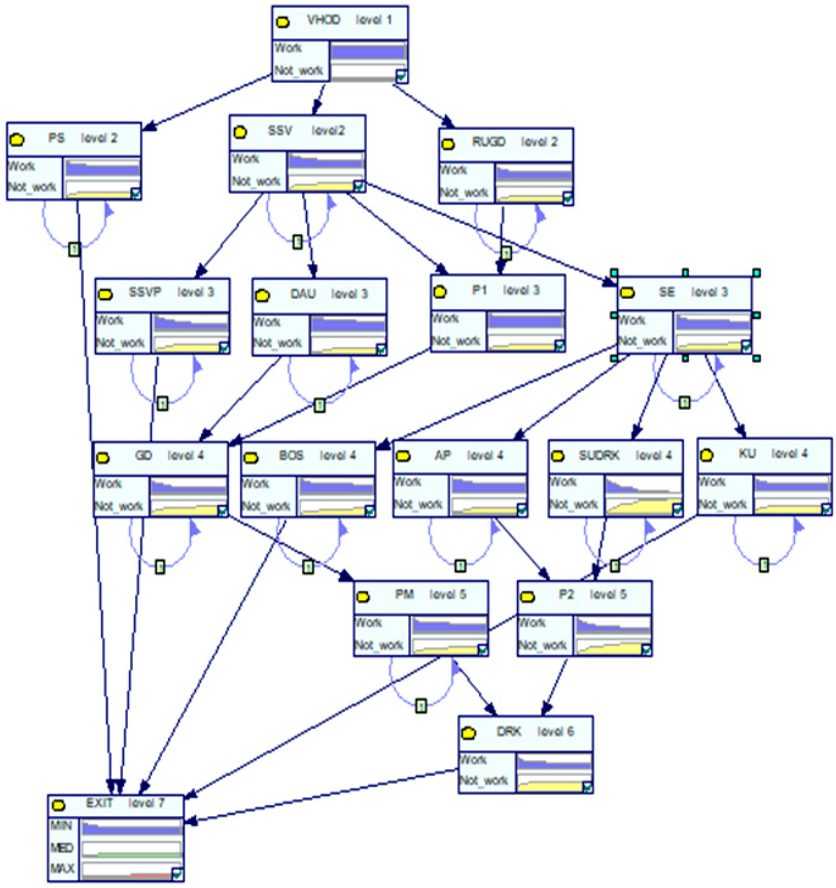


Fig.2. BBN SPP in the GeNIe environment when searching for the causes of failures at the risk of failure of the input component

From the retrospective analysis of the research results in the simulation of the SPP, the components that affect the overall performance of the system are identified. In the study of emergency situations, the analysis of incidents in the CTS, the main goal is to determine the cause of the accident. It follows from the research results that the maximum non-operating state during the operation of the SPP is 20,000 hours. corresponds to the SUDRK complex (Fig. 2). Because Since the SUDRK complex is dependent at the level of the hierarchical structure of the SPP, it is necessary to check the complex in order to find the cause of its failure.

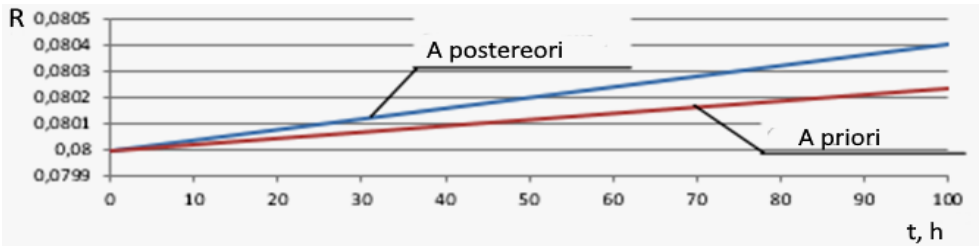


Fig.3. A posteriori and a priori estimates of the risk of failure power plant compressed air systems

The purpose of using the BBN in assessing both the probability of loss of performance and the risk of failure of the elements of the CTS components is an a posteriori conclusion. The a priori data are dynamically recalculated and form a posterior failure risk estimate, which is a priori information, to process the new information. The a posteriori conclusion is based on the procedures for analyzing the data obtained as a

result of using the BBN. When implementing this approach in research, modeling using a priori and a posteriori data, the subsystems of the power plant are determined that have the greatest impact on the performance of the main engine and the operation of the entire system for various periods of time. Figure 3 shows a priori and a posteriori data and studies of the compressed air system for 100 hours of SPP operation. The risk of system failure increased slightly, changing from 0.08 to 0.085.

Conclusions

Application of the research results of the developed model for the purpose of a retrospective analysis of emergency situations at CTS makes it possible to improve the reliability of systems operation by solving the problem of determining their causes. The application of the developed model, taking into account the hierarchical levels of subsystems (components), intersystem (interelement) connections for an intelligent system for assessing and predicting the risk of failures of components of a complex technical system when searching for the causes of failures of CTS components, allows:

• control the values of the risk of failures of the system components upon receipt of information about failures;

• predict trends in the risk of failures of CTS components, taking into account changes in the risk of failures of individual components in order to select a strategy for their recovery.

References

1. ISO 13381-1:2015 Condition monitoring and diagnostics of machines. Part 1: General guidelines. 2015. 21p.
2. Vychuzhanin V.V., Rudnichenko N.D. Metody informatsionnykh tekhnologiy v diagnostike sostoyaniya slozhnykh tekhnicheskikh sistem. Monografiya. Odesa: Ekologiya, 2019. 178 p.
3. Vyuzhuzhanin V.V., Rudnichenko N.D., Shibaeva N.O. Data Control in the Diagnostics and Forecasting the State of Complex Technical Systems. *Herald of Advanced Information Technology.* 2019. Vol.2. No.2. P.183-196.
4. Vyuzhuzhanin V., Gritsuk I. The Complex Application of Monitoring and Express Diagnosing for Searching Failures on Common Rail System Units DP. *SAE International*. 2018. 9.10. 2018-01-1773.
5. Vychuzhanin V., Rudnichenko N. Complex Technical System Condition Diagnostics and Prediction Computerization. *CMIS-2020 Computer Modeling and Intelligent Systems*. 2020. P.1-15.
6. Andersen B.A. Diagnostic System for Remote Real-Time Monitoring of Marine Diesel-Electric Propulsion Systems. Leipzig, 2011. 45 p.
7. Sorensen A. J. Marine Control Systems Propulsion and Motion Control of Ships and Ocean Structures. Trondheim, Norway: Department of Marine Technology NTNU, 2013. 537 p.
8. Zhang P., GaoCao Z., Dong L. Marine Systems and Equipment Prognostics and Health Management. *Systematic Review from Health Condition Monitoring to Maintenance Strategy. Machines.* 2022. No.10. P.72. URL: https://doi.org/10.3390/machines10020072.
9. Vychuzhanin V., Rudnichenko N. Devising a method for the estimation and prediction of technical condition of ship complex systems. *Eastern-European Journal of Enterprise Technologies*. 2016. V. 84. No. № 6/9. P. 4-11.
10. Lazakis I. Advanced ship systems condition monitoring for enhanced inspection, maintenance and decision making in ship operations. *Transportation Research Procedia.* 2016. No. 14. P. 1679 – 1688.
11. Vychuzhanin V., Rudnichenko N. Assessment of risks structurally and functionally complex technical systems. *Eastern-European Journal of Enterprise Technologies.*

2014. Vol.1. No.2. P.18-22. URL: https://doi.org/10.15587/1729-4061.2014.19846.
12. Zhang M., Montewka J., Manderbacka T., Kujala P., Hirdaris S. A Big Data Analytics Method for the Evaluation of Ship – Ship Collision Risk Reflecting Hydrometeorological Conditions. *Reliability Engineering & System Safety.* 2021. V.213. 107674. URL: https://doi.org/10.1016/j.ress.2021.107674.
13. Jensen F.V. Bayesian Networks and Decision Graphs. Berlin: Springer, 2007.457 p.
14. Wang C.R., Guan C. A Bayesian Inference-Based Approach for Performance Prognostics Towards Uncertainty Quantification and Its Applications on the Marine Diesel Engine. *ISA Trans.* 2021. V.118, P.159–173.
15. Lan F., Jiang Y. Performance Prediction Method of Prognostics and Health Management of Marine Diesel Engine. *Proceedings of the 2020 3rd International Conference on Applied Mathematics, Modeling and Simulation, Shanghai*, China, 20–21 September 2020. Bristol, UK: IOP Publishing, 2020. Vol. 1670.
16. Chenguang Y., Jing N. Neural Network for Complex Systems: Theory and Applications. 2018 | Article ID 3141805 |URL: https://doi.org/10.1155/2018/3141805
17. Boullosa-Falces D., Barrena J.L.L. Monitoring of fuel oil process of marine diesel engine. *Appl. Therm. Eng.* 2017. P. 127, 517–526.
18. Genie Backup Manager. URL:zoolz.com/genie9/

ІНТЕЛЕКТУАЛЬНА СИСТЕМА ОЦІНКИ І ПРОГНОЗУВАННЯ РИЗИКУ ВІДМОВ КОМПОНЕНТІВ СКЛАДНОЇ ТЕХНІЧНОЇ СИСТЕМИ

А.В. Вичужанін

Національний університет «Одеська політехніка»
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: v.v.vychuzhanin@op.edu.ua

Складність складу та збільшення кількості технічних систем призводять до зростання інтенсивності їх відмов. В результаті виникає необхідність ремонту обладнання складних технічних систем, що веде до простоїв систем. Пошук компонентів, що відмовили, та усунення їх відмов сприяє підвищенню рівня безпеки експлуатації складних технічних систем. Діагностика та прогнозування відмов компонентів автоматизованих систем та механізмів (підсистем, елементів, міжсистемних та міжелементних зв'язків) у реальних експлуатації для пошуку та усунення причин відмов залишається актуальним завданням. Експлуатаційна надійність складних технічних систем, що відновлюються, та їх компонентів ефективно досягається стратегією експлуатації систем з контролем технічного стану на основі систем технічної діагностики. Зменшенню відмов та техногенних ризиків під час експлуатації складних технічних систем сприяє прогнозування їх технічного стану на основі діагностики. У статті наведено інтелектуальну систему, що функціонує з використанням розробленої моделі оцінки та прогнозування ризику відмов компонентів складної технічної системи на прикладі суднової енергетичної установки. Побудова моделі з урахуванням ієрархічних рівнів підсистем (компонентів), міжсистемних (міжелементних) зв'язків інтелектуальної системи ґрунтується на використанні апріорної інформації про відмови компонентів складних технічних систем. Модель пов'язує види технічного стану компонентів та діагностичні ознаки систем у вигляді ризику їх відмов. Використання апостеріорного висновку в байєсівських мережах довіри дозволяє визначати ризик відмов компонентів системи з урахуванням діагностичної інформації, що надходить, та інформації про відмови компонентів. З метою побудови та досліджень діагностичної байєсівської мережевої моделі інтелектуальної системи оцінки ризику відмов для системи діагностики та прогнозування технічного стану компонентів складної технічної системи, що складається з численних змінних, застосовано програмний продукт GeNIe. Отримані результати досліджень моделі оцінки та прогнозування ризику відмов компонентів складної технічної системи підтвердили можливість прогнозувати значення ризику відмов компонентів та системи загалом.

Ключові слова: складна технічна система, компоненти, оцінка ризику відмови, інтелектуальна система, байєсовська мережа довіри, діагностика, прогнозування.

DOI 10.15276/imms.v12.no3.162
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 12 (2022), No. 3, pp. 162-172

ДОСЛІДЖЕННЯ ПАРАМЕТРІВ ПЕРЕТВОРЕНИХ БЛОКІВ ЦИФРОВОГО ЗОБРАЖЕННЯ ДЛЯ ВИЯВЛЕННЯ ПОРУШЕННЯ ЙОГО ЦІЛІСНОСТІ

І.І. Бобок

Національний університет «Одеська Політехніка»,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: onu_metal@ukr.net

Проблема виявлення порушення цілісності інформаційного контенту є одною з основних проблем сучасної інформаційної безпеки. Несанкціоноване змінений інформаційний контент при його використанні з нерозважальною метою може привести до критично негативних наслідків як для окремих людей, підприємств, банків, фірм, так і до катастрофічних наслідків для людства в цілому, якщо кібератаки будуть спрямовані на сферу військової галузі, енергетики, хімічної промисловості тощо. Світова наукова спільнота приділяє багато уваги проблемі виявлення порушень цілісності інформаційних контентів, зокрема цифрових зображень, що розглядаються в роботі, але остаточного розв'язку ця проблема не має, задача удосконалення підходів та методів експертизи цілісності цифрових контентів залишається актуальною. Метою роботи є дослідження можливостей удосконалення існуючого підходу до виявлення несанкціонованих змін цифрових зображень, заснованого на аналізі сингулярних чисел і сингулярних векторів блоків відповідної матриці, шляхом дослідження властивостей блоків, отриманих з використанням різноманітних перетворень, що відрізняються від запропонованих раніше. Досліджені властивості блоків, отриманих шляхом загальної симетризації, а також шляхом запропонованих перетворень, результатом яких є несиметричні матриці, що можуть використовувати довільну кількість m матриць-множників. Встановлено, що для підвищення ефективності підтвердження збереження цілісності зображення має сенс використовувати симетризовані блоки при m=2, несиметризовані - при m=3, але з урахуванням пріоритетності виявлення саме порушення цілісності в загальному випадку перевагу треба віддати перетворенню симетризації з m=2.

Ключові слова: цілісність цифрового зображення, порушення цілісності, сингулярне число, сингулярний вектор, чутливість до збурюючих дій.

Вступ

Проблема виявлення порушення цілісності інформаційного контенту є одною з основних проблем сучасної інформаційної безпеки [1,2]. Несанкціоновано змінений інформаційний контент при його використанні з нерозважальною метою може привести до критично негативних наслідків як для окремих людей, підприємств, банків, фірм в вигляді компрометації персональних даних, матеріального, економічного збитку [3,4], так і до катастрофічних наслідків для людства в цілому, якщо кібератаки будуть спрямовані на сферу військової галузі, енергетики, хімічної промисловості тощо, що може поставити під загрозу життя людей в усьому світі. Інформація на сьогоднішній день стає найдорожчим і найзатребуванішим товаром [5].

Світова наукова спільнота приділяє багато уваги проблемі виявлення порушень цілісності інформаційних контентів, зокрема цифрових зображень (ЦЗ), що відбуваються в результаті різноманітних збурних дій [6-8], але остаточного розв'язку ця проблема не має. Більше того, на погляд автора, вона принципово взагалі не може бути вирішеною остаточно, оскільки розвиток інформаційних технологій, теорії інформаційної безпеки приводе до удосконалення способів та методів, що використовуються для несанкціонованих змін контентів, а методи виявлення – це, як правило, відповідь на нові «виклики». Тому задача

удосконалення підходів та методів експертизи цілісності цифрових контентів, зокрема ЦЗ, що і розглядаються в роботі, сьогодні і завтра залишаться актуальними.

Нещодавно в роботах [9-14] був запропонований новий підхід до вирішення проблеми виявлення порушення цілісності ЦЗ/кадрів цифрового відео, заснований на аналізі властивостей сингулярних чисел (СНЧ) і сингулярних векторів (СНВ) $l\times l$-блоків матриці цифрового контенту, отриманих шляхом стандартної розбивки його матриці [15], що є результатом нормального сингулярного розкладання [10]:

$$B = U\Sigma V^T, \quad (1)$$

де B – $l\times l$-блок, U, V – ортогональні $l\times l$-матриці, стовпці яких $u_1,\ldots,u_l$ і $v_1,\ldots,v_l$ – відповідно ліві (лексикографічно додатні) і праві СНВ B, $\Sigma = diag\left(\sigma_1(B),\ldots,\sigma_l(B)\right)$, $\sigma_1(B)\geq\ldots\geq\sigma_l(B)\geq 0$ – СНЧ B.

В межах підходу було первісно встановлено [9-10], що для більшості блоків більшості оригінальних ЦЗ має місце співвідношення:

$$\angle\left(u_1,\bar{\sigma}\right)\approx\angle\left(v_1,\bar{\sigma}\right)\approx\angle\left(n^O,e_1\right), \quad (2)$$

де $\bar{\sigma}=\sigma/\|\sigma\|$, $\sigma=\left(\sigma_1(B),\sigma_2(B),\ldots,\sigma_l(B)\right)^T\in R^l$ – вектор СНЧ B, $\|\sigma\|$ – норма σ, $\angle\left(u_1,\bar{\sigma}\right)$, $\angle\left(v_1,\bar{\sigma}\right)$ - величини кутів між векторами u_1 і $\bar{\sigma}$, v_1 і $\bar{\sigma}$ відповідно, $n^O=\left(1/\sqrt{l},1/\sqrt{l},\ldots,1/\sqrt{l}\right)^T\in R^l$ - n-оптимальний вектор простору R^l, $e_1=(1,0,\ldots,0)\in R^l$ - перший вектор стандартного базису R^l, $\angle\left(n^O,e_1\right)$ - кут між векторами n^O,e_1.

Удосконалення підходу [11-14] привело до встановлення факту, що співвідношення

$$\angle\left(u_1,\bar{\bar{\sigma}}\right)\approx\angle\left(v_1,\bar{\bar{\sigma}}\right)\approx\angle\left(n^O,e_1\right), \quad (3)$$

де $\bar{\bar{\sigma}}=\left(\sigma_1^2(B),\sigma_2^2(B),\ldots,\sigma_l{}^2(B)\right)^T\Big/\left\|\left(\sigma_1^2(B),\sigma_2^2(B),\ldots,\sigma_l{}^2(B)\right)^T\right\|$, виконується для більшості блоків оригінального ЦЗ, отриманих шляхом стандартної розбивки його матриці, при цьому рівність в (3) має місце для більшої кількості блоків більшої кількості оригінальних ЦЗ, ніж в (2).

Згаданий підхід добре зарекомендував себе при застосуванні в задачах стеганоаналізу, зокрема універсального, при виявленні результатів накладання різноманітних шумів, розмиття ЦЗ, виявленні блокової обробки, локальних порушень цілісності зображення тощо. Враховуючи це, а також те, що результати його роботи при реалізації в конкретних експертних методах не є абсолютними, тобто такими, що взагалі не можна покращити, актуальним є питання удосконалення цього підходу для підвищення ефективності відповідних експертних методів, що на ньому базуються.

Метою роботи є дослідження можливостей удосконалення підходу виявлення порушень цілісності ЦЗ, заснованого на аналізі СНЧ і СНВ блоків матриці ЦЗ, шляхом дослідження властивостей блоків, отриманих з використанням перетворень, що відрізняються від запропонованих раніше [11-14].

Основний матеріал

Перетвореннями блоку B, що використовувалися при удосконаленні [11-14] експертного підходу, заснованому на аналізі СНЧ і СНВ блоків матриці ЦЗ, були дві симетризації у вигляді:

$$B\to BB^T,\ B\to B^TB,$$

які приводили до підвищення ефективності експертизи цілісності, в порівнянні з аналізом параметрів поданого блоку B, завдяки тому, що СНЧ $\sigma_i\left(BB^T\right)$, $\sigma_i\left(B^TB\right)$,

$i=\overline{1,l}$, матриць BB^T, B^TB відрізнялися від СНЧ B відповідно до співвідношення: $\sigma_i\left(BB^T\right)=\sigma_i\left(B^TB\right)=\sigma_i^{\,2}(B)$, а СНВ BB^T, B^TB, що одночасно були і власними векторами, співпадали з лівими, правими СНВ B відповідно.

Симетризація блоку в загальному вигляді може бути представлена наступним чином:

$$B\to BB^TBB^T...BB^T,\qquad B\to B^TBB^TB...B^TB, \tag{4}$$

де кількість множників-матриць в правих частинах перетворень (4) дорівнює $2k$, $k\in N$, N – множина натуральних чисел. Дійсно, якщо є деяка симетрична матриця $A=A^T$, то множення її на себе довільну кількість разів залишить результуючу матрицю симетричною: $\left(AA...A\right)^T=A^TA^T...A^T=AA...A$. В нашому випадку: $A=BB^T$, $A=B^TB$. Виникає питання: чи приведе до наступного покращення експертного підходу аналіз блоків ЦЗ, отриманих за допомогою перетворень (4) з $k>1$?

Твердження 1. Для матриць (4) мають місце наступні співвідношення:

$$\sigma_i\left(BB^T...BB^T\right)=\sigma_i\left(B^TB...B^TB\right)=\sigma_i^{\,2k}\left(B\right),i=\overline{1,l}, \tag{5}$$

ліві і праві СНВ матриці $BB^TBB^T...BB^T$, що одночасно є її власними векторами, співпадають з лівими СНВ матриці B, а ліві і праві СНВ матриці $B^TBB^TB...B^TB$, що одночасно є її власними векторами, співпадають з правими СНВ матриці B.

Доказ. Покажемо, що для матриці $BB^TBB^T...BB^T$ має місце наступне співвідношення:

$$\underbrace{BB^TBB^T...BB^T}_{2k\ множників}=U\Sigma^{2k}U^T. \tag{6}$$

Скористаємося для цього принципом математичної індукції. Використовуючи (1), для k=1 отримаємо:

$$BB^T=U\Sigma^2U^T. \tag{7}$$

Припустимо, що для деякого $k=n$ рівність (6) доведена, тобто $\underbrace{BB^TBB^T...BB^T}_{2n\ множників}=U\Sigma^{2n}U^T$. Перевіримо (6) для $k=n+1$, використовуючи припущення індукції і (7):

$$\underbrace{BB^TBB^T...BB^T}_{2(n+1)\ множників}=\underbrace{BB^TBB^T...BB^T}_{2n\ множників}BB^T=U\Sigma^{2n}U^TBB^T=U\Sigma^{2n}U^TU\Sigma^2U^T=U\Sigma^{2(n+1)}U^T.$$

Таким чином, співвідношення (6) має місце для $\forall k\in N$.

Аналогічним чином, використовуючи рівність, отриману за допомогою (1):

$$B^TB=V\Sigma^2V^T, \tag{8}$$

можна показати, що для матриці $B^TBB^TB...B^TB$ має місце наступне співвідношення:

$$\underbrace{B^TBB^TB...B^TB}_{2k\ множників}=V\Sigma^{2k}V^T. \tag{9}$$

Співвідношення (6), (9), враховуючи властивості матриць U,V,Σ, визначених для (1), є нормальними спектральними (одночасно і сингулярними) розкладаннями для матриць $BB^TBB^T...BB^T$, $B^TBB^TB...B^TB$ відповідно, з чого випливає рівність (5) і висновок твердження для їх СНВ.

Відповідність між СНЧ поданої і перетвореної матриці блоку B, аналогічна (5), буде мати місце і в випадку перетворень матриці виду:

$$B\to BB^TBB^T...BB^TB,\qquad B\to B^TBB^TB...B^TBB^T, \tag{10}$$

де кількість множників-матриць в правих частинах перетворень (10) дорівнює $2k$+1, $k\in N$. Для (10) має місце наступне твердження.

Твердження 2. Для матриць (10) мають місце співвідношення:

$$\sigma_i\left(BB^T...BB^TB\right)=\sigma_i\left(B^TB...B^TBB^T\right)=\sigma_i^{\,2k+1}(B),\ \ i=\overline{1,l}\,, \tag{11}$$

ліві і праві СНВ матриці $BB^TBB^T...BB^TB$ співпадають відповідно з лівими і правими СНВ матриці B, а ліві і праві СНВ матриці $B^TBB^TB...B^TBB^T$ співпадають з правими і лівими СНВ матриці B відповідно.

Доказ. Аналогічно доказу твердження 1 з використанням співвідношень (7), (8) та наступних, отриманих з урахуванням (1): $BB^TB=U\Sigma^3V^T$, $B^TBB^T=V\Sigma^3U^T$.

Позначимо вектори СНЧ матриць $BB^TBB^T...BB^T$, $B^TBB^TB...B^TB$, $B^TBB^TB...B^TBB^T$, $BB^TBB^T...BB^TB$ наступним чином:

$$\sigma_{B^TB...B^TB}=\left(\sigma_1\left(B^TB...B^TB\right),...,\sigma_l\left(B^TB...B^TB\right)\right)^T=\left(\sigma_1^{2k}(B),...,\sigma_l^{\,2k}(B)\right)^T=\sigma_{BB^T...BB^T}=\sigma_{(B)^{(2k)}}$$

$$\sigma_{B^TB...B^TBB^T}=\left(\sigma_1\left(B^TB...B^TBB^T\right),...,\sigma_l\left(B^TB...B^TBB^T\right)\right)^T=\left(\sigma_1^{2k+1}(B),...,\sigma_l^{\,2k+1}(B)\right)^T=\sigma_{BB^T...BB^TB}=\sigma_{(B)^{(2k+1)}}$$

В блоках оригінального ЦЗ має місце співвідношення:

$$\sigma_1(B)>>\sigma_2(B)\geq...\geq\sigma_l(B)\geq 0\,. \tag{12}$$

При піднесенні до ступеня $2k/2k+1$ СНЧ B при обчисленні СНЧ матриць (4), (10) відповідно до (5), (11) зменшаться малі (менші 1) і збільшаться великі (більші 1) значення, ще більше відокремивши максимальне СНЧ від усіх інших. При нормуванні векторів $\sigma_{(B)^{(2k)}}$, $\sigma_{(B)^{(2k+1)}}$, результатом чого буде вектор

$$\bar{\sigma}^{(2k)}=\sigma_{(B)^{(2k)}}\Big/\left\|\sigma_{(B)^{(2k)}}\right\|,\ \bar{\sigma}^{(2k+1)}=\sigma_{(B)^{(2k+1)}}\Big/\left\|\sigma_{(B)^{(2k+1)}}\right\|,$$

перші компоненти $\bar{\sigma}^{(2k)}$, $\bar{\sigma}^{(2k+1)}$ виявляться ближчими до одиниці, ніж перші компоненти вектора $\bar{\sigma}$, а останні можуть виявитися значно ближче до 0, ніж останні компоненти $\bar{\sigma}$, що приводить до наступного твердження, що є узагальненням висновків, представлених в [11,14].

Твердження 3. Для блоків оригінального ЦЗ, отриманих в результаті стандартної розбивки його матриці, має місце співвідношення

$$\angle\left(e_1,\bar{\sigma}^{(p)}\right)<\angle\left(e_1,\bar{\sigma}^{(m)}\right)<\angle\left(e_1,\bar{\sigma}\right), \tag{13}$$

якщо $p>m$.

Доказ. Нехай $\alpha=\angle\left(e_1,\bar{\sigma}\right)$, тоді [11,14]:

$$cos\,\alpha=\frac{\sigma_1(B)}{\sqrt{\sigma_1^{\,2}(B)+\sigma_2^{\,2}(B)+...+\sigma_l^{\,2}(B)}}\,.$$

Нехай $\beta_m=\angle\left(e_1,\bar{\sigma}^{(m)}\right)$. Тоді

$$cos\,\beta_{(m)}=\frac{\sigma_1^{\,m}(B)}{\sqrt{\sigma_1^{\,2m}(B)+\sigma_2^{\,2m}(B)+...+\sigma_l^{\,2m}(B)}}\,. \tag{14}$$

Права частина (13) при $m>1$ випливає з відповідного твердження [11,14]. Ліву частину (13) отримаємо шляхом піднесення лівої і правої частин (14) у квадрат і розгляду оберненого до отриманого значення:

$$\frac{1}{cos^2\beta_{(m)}}=\frac{\sigma_1^{\,2m}(B)+\sigma_2^{\,2m}(B)+...+\sigma_l^{\,2m}(B)}{\sigma_1^{\,2m}(B)}=1+\left(\frac{\sigma_2(B)}{\sigma_1(B)}\right)^{2m}+...+\left(\frac{\sigma_l(B)}{\sigma_1(B)}\right)^{2m} \tag{15}$$

Кожен дріб в правій частині (15) задовольняє умові:

$$0\leq\frac{\sigma_i(B)}{\sigma_1(B)}<1,\ i=\overline{2,l}\,.$$

Враховуючи властивості показникової функції з основою, що менше одиниці, маємо при $p > m$:

$$\left(\frac{\sigma_i(B)}{\sigma_1(B)}\right)^{2p} < \left(\frac{\sigma_i(B)}{\sigma_1(B)}\right)^{2m}, i = \overline{2,l}, \quad (16)$$

З (16) випливає:

$$\frac{1}{cos^2\beta_{(p)}} < \frac{1}{cos^2\beta_{(m)}} \quad \Rightarrow \quad cos^2\beta_{(m)} < cos^2\beta_{(p)}.$$

З урахуванням того, що СНЧ будь-якої матриці є нечутливими до збурних дій, тобто кути $\beta_{(p)}, \beta_{(m)}$ - гострі, маємо:

$$\beta_{(p)} < \beta_{(m)},$$

що й потрібно було довести.

В [12], враховуючи актуальність оцінки чутливості для параметрів, що аналізуються в межах підходу, що розглядається, для виявлення порушення цілісності ЦЗ, було показано, що нормований вектор СНЧ $\bar{\sigma}$, що відповідає $l \times l$ – блоку B, будучи нечутливим, має більшу чутливість до збурних дій, ніж також нечутливий нормований вектор $\bar{\bar{\sigma}}$ СНЧ матриці BB^T ($B^T B$). Узагальненням цього є наступне твердження.

Твердження 4. Чутливість нормованого вектора $\bar{\sigma}^{(m)}$ є меншою за чутливість $\bar{\sigma}$ і спадає зі зростанням *m*.

Доказ. Доведення першої частини твердження аналогічне [12]. Нехай в результаті збурної дії блок B зазнав збурення ΔB, результатом чого є збурений блок $\overline{B}$ з СНЧ $\sigma_i(B + \Delta B), i = \overline{1,l}$. Для відповідних перетворених блоків (4) або (10) збурення відіб'ється на векторі $\bar{\sigma}^{(m)}$, який в результаті стане $\bar{\sigma}_{зб}^{(m)}$ і буде обчислюватися наступним чином:

$$\bar{\sigma}_{зб}^{(m)} = \frac{\left(\sigma_1^m(B + \Delta B), \ldots, \sigma_l^m(B + \Delta B)\right)}{\sqrt{\sigma_1^{2m}(B + \Delta B) + \ldots + \sigma_l^{2m}(B + \Delta B)}} \quad (17)$$

Оцінимо чутливість $\bar{\sigma}^{(m)}$ за допомогою кута повороту $\gamma_{(m)}$ між векторами $\bar{\sigma}^{(m)}$ і $\bar{\sigma}_{зб}^{(m)}$ (17):

$$cos(\gamma_{(m)}) = \frac{\left(\bar{\sigma}^{(m)}, \bar{\sigma}_{зб}^{(m)}\right)}{\left\|\bar{\sigma}^{(m)}\right\| \left\|\bar{\sigma}_{зб}^{(m)}\right\|} = \frac{\sigma_1^m(B)\sigma_1^m(B + \Delta B) + \ldots + \sigma_l^m(B)\sigma_l^m(B + \Delta B)}{\sqrt{\sigma_1^{2m}(B) + \ldots + \sigma_l^{2m}(B)}\sqrt{\sigma_1^{2m}(B + \Delta B) + \ldots + \sigma_l^{2m}(B + \Delta B)}}, \quad (18)$$

де $(\cdot,\cdot)$ – скалярний добуток векторів-аргументів.

Перетворену відповідно з (4) або (10) матрицю блоку *B* будемо позначати $(B)^{(m)}$, де *m* вказує на кількість використаних при перетворенні матриць-множників. Нехай $p > m$, тобто $p = m + c$, де $c > 0$, $cos(\gamma_{(p)})$ визначимо відповідно до (18). Тоді:

$$\frac{cos(\gamma_{(p)})}{cos(\gamma_{(m)})} = \frac{\left(\sigma_1^{m+c}(B)\sigma_1^{m+c}(B + \Delta B) + \ldots + \sigma_l^{m+c}(B)\sigma_l^{m+c}(B + \Delta B)\right)}{\sqrt{\sigma_1^{2(m+c)}(B) + \ldots + \sigma_l^{2(m+c)}(B)}\sqrt{\sigma_1^{2(m+c)}(B + \Delta B) + \ldots + \sigma_l^{2(m+c)}(B + \Delta B)}} \times$$
$$\times \frac{\sqrt{\sigma_1^{2m}(B) + \ldots + \sigma_l^{2m}(B)}\sqrt{\sigma_1^{2m}(B + \Delta B) + \ldots + \sigma_l^{2m}(B + \Delta B)}}{\left(\sigma_1^m(B)\sigma_1^m(B + \Delta B) + \ldots + \sigma_l^m(B)\sigma_l^m(B + \Delta B)\right)}.$$

Враховуючи співвідношення між матричною нормою Фробеніуса і складовими сингулярного спектру матриці [12], останнє співвідношення можна представити у вигляді:

$$\frac{cos\left(\gamma_{(p)}\right)}{cos\left(\gamma_{(m)}\right)}=\frac{\left(\sigma_1{}^{m+c}(B)\sigma_1{}^{m+c}(B+\Delta B)+\ldots+\sigma_l{}^{m+c}(B)\sigma_l{}^{m+c}(B+\Delta B)\right)}{\left\|(B)^{(m+c)}\right\|_F\left\|(B+\Delta B)^{(m+c)}\right\|_F}\times$$

$$\times\frac{\left\|(B)^{(m)}\right\|_F\left\|(B+\Delta B)^{(m)}\right\|_F}{\left(\sigma_1{}^{m}(B)\sigma_1{}^{m}(B+\Delta B)+\ldots+\sigma_l{}^{m}(B)\sigma_l{}^{m}(B+\Delta B)\right)}. \qquad (19)$$

Враховуючи, що норма Фробеніуса добутку матриць не перевищує добутку норм множників [16], а також, що норми поданої і транспонованої матриці співпадають, з (19) отримуємо:

$$\frac{cos\left(\gamma_{(p)}\right)}{cos\left(\gamma_{(m)}\right)}\geq\frac{\left(\sigma_1{}^{m+c}(B)\sigma_1{}^{m+c}(B+\Delta B)+\ldots+\sigma_l{}^{m+c}(B)\sigma_l{}^{m+c}(B+\Delta B)\right)}{\left\|(B)^{(m)}\right\|_F\left\|(B+\Delta B)^{(m)}\right\|_F\left\|(B)^{(c)}\right\|_F\left\|(B+\Delta B)^{(c)}\right\|_F}\times$$

$$\times\frac{\left\|(B)^{(m)}\right\|_F\left\|(B+\Delta B)^{(m)}\right\|_F}{\left(\sigma_1{}^{m}(B)\sigma_1{}^{m}(B+\Delta B)+\ldots+\sigma_l{}^{m}(B)\sigma_l{}^{m}(B+\Delta B)\right)}=$$

$$=\frac{\left(\sigma_1{}^{m+c}(B)\sigma_1{}^{m+c}(B+\Delta B)+\ldots+\sigma_l{}^{m+c}(B)\sigma_l{}^{m+c}(B+\Delta B)\right)}{\left(\sigma_1{}^{m}(B)\sigma_1{}^{m}(B+\Delta B)+\ldots+\sigma_l{}^{m}(B)\sigma_l{}^{m}(B+\Delta B)\right)\left\|(B)^{(c)}\right\|_F\left\|(B+\Delta B)^{(c)}\right\|_F}\geq \qquad (20)$$

$$=\frac{\left(\sigma_1{}^{m+c}(B)\sigma_1{}^{m+c}(B+\Delta B)+\ldots+\sigma_l{}^{m+c}(B)\sigma_l{}^{m+c}(B+\Delta B)\right)}{\left(\sigma_1{}^{m}(B)\sigma_1{}^{m}(B+\Delta B)+\ldots+\sigma_l{}^{m}(B)\sigma_l{}^{m}(B+\Delta B)\right)\|B\|_F^c\|B+\Delta B\|_F^c}\geq$$

$$\geq\frac{\sigma_1{}^{m+c}(B)\sigma_1{}^{m+c}(B+\Delta B)}{\left(\sigma_1{}^{m}(B)\sigma_1{}^{m}(B+\Delta B)+\ldots+\sigma_l{}^{m}(B)\sigma_l{}^{m}(B+\Delta B)\right)\|B\|_F^c\|B+\Delta B\|_F^c}.$$

Враховуючи (12), визначення спектральної матричної норми [16], порівнянність спектральної матричної норми і норми Фробеніуса для блоку оригінального ЦЗ [12], з (20) отримуємо:

$$\frac{cos\left(\gamma_{(p)}\right)}{cos\left(\gamma_{(m)}\right)}\geq$$

$$\geq\frac{\sigma_1{}^{m+c}(B)\sigma_1{}^{m+c}(B+\Delta B)}{\left(\sigma_1{}^{m}(B)\sigma_1{}^{m}(B+\Delta B)+\ldots+\sigma_l{}^{m}(B)\sigma_l{}^{m}(B+\Delta B)\right)\|B\|_F^c\|B+\Delta B\|_F^c}\approx\frac{\sigma_1{}^{m+c}(B)\sigma_1{}^{m+c}(B+\Delta B)}{\sigma_1{}^{m}(B)\sigma_1{}^{m}(B+\Delta B)\|B\|_F^c\|B+\Delta B\|_F^c}=$$

$$=\frac{\|B\|_2^{m+c}\|B+\Delta B\|_2^{m+c}}{\|B\|_2^{m}\|B+\Delta B\|_2^{m}\|B\|_F^c\|B+\Delta B\|_F^c},$$

тобто

$$\frac{cos\left(\gamma_{(p)}\right)}{cos\left(\gamma_{(m)}\right)}\geq 1,$$

що й потрібно було довести.

Оскільки при перетвореннях (4), (10) СНВ перетворених матриць відповідають СНВ блоку B, то їх реакція на збурюючу дію ΔB в межах B і перетворених матриць буде визначатися однаково.

З доведених вище тверджень випливає істинність

Твердження 5. Для блоку B зображення пара векторів $u_1,\overline{\sigma}^{(m)}$ є більш стійкою до збурних дій, ніж пара $u_1,\overline{\sigma}$ у тому розумінні, що в результаті

збурюючої дії величина кута між $u_1, \overline{\sigma}^{(m)}$ збуриться менше, ніж між $u_1, \overline{\sigma}$, при цьому ця стійкість буде зростати разом зі зростанням m.

З врахуванням вищенаведеного має місце наступна теорема.

Теорема. Співвідношення

$$\angle\left(u_1, \overline{\sigma}^{(m)}\right) \approx \angle\left(v_1, \overline{\sigma}^{(m)}\right) \approx \angle\left(n^O, e_1\right), \tag{21}$$

виконується для більшості блоків оригінального ЦЗ, отриманих шляхом стандартної розбивки його матриці, при цьому рівність в (21) має місце для більшої кількості блоків більшої кількості оригінальних ЦЗ при $m > 2$, ніж при $m = 2$.

Таким чином, з точки зору отриманих теоретичних результатів, використання перетворень (4), (10) для $k > 1$ очікувано повинно дати підвищення ефективності методів експертизи цілісності ЦЗ, що базуються на підході, який розглядається в роботі, в частині підтвердження збереження зображеннями цілісності.

Для практичної перевірки висновку теореми був проведений обчислювальний експеримент, в якому було задіяно 1000 ЦЗ розміром 400×400 пікселів: 500 ЦЗ з бази NRCS [17], 500 ЦЗ з бази img_Nikon_D70s [18].

Ілюстрація, яка має типовий характер, і підтверджує висновок теореми, наведена на рис.2 для ЦЗ (рис.1), $l = 4$.

Рис.1. Тестове ЦЗ

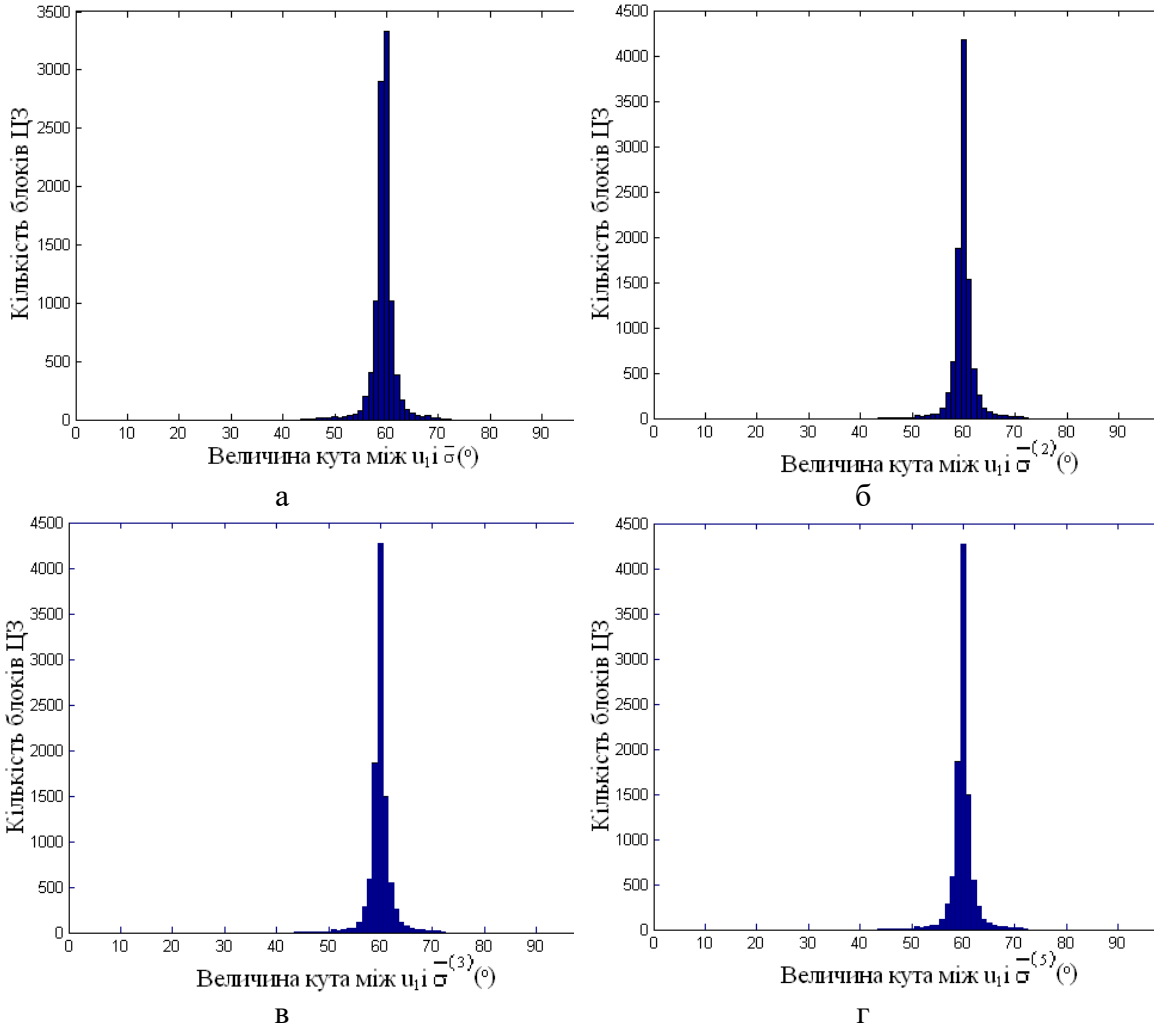


Рис.2. Ілюстрація виконання співвідношення (21) для оригінального ЦЗ при різних значеннях m: а – аналізуються вектори $u_1, \bar{\sigma}$; б - вектори $u_1, \bar{\sigma}^{(2)}$; в - вектори $u_1, \bar{\sigma}^{(3)}$; г - вектори $u_1, \bar{\sigma}^{(5)}$

Як видно з рис.2(б,в,г), характер змін гістограми хоча і відповідає теоремі (збільшення значення в моді, яка співпадає з $\angle\left(n^O, e_1\right)$), але кількісно ці зміни при $m > 2$ є незначними, аж до непомітних (порівн. рис.2(в), рис.2(г)). Це має пояснення. Дійсно, починаючи з деякого значення $m > 2$, відокремленість максимального СНЧ блоку $(B)^{(m)}$ стає настільки великою, що при нормуванні відповідного вектору СНЧ отримується вектор e_1, і подальше підвищення ступеня m тут вже нічого не змінює для ступеня близькості нормованого вектора СНЧ і e_1. Найбільший ефект тут досягається при переході від аналізу векторів $u_1, \bar{\sigma}$ до векторів $u_1, \bar{\sigma}^{(2)}$. Але, як показує обчислювальний експеримент, для підвищення ефективності при встановленні оригінальності ЦЗ (зниженні помилок 2-го роду для відповідних експертних методів) має сенс використовувати $m = 3$.

Підвищення стійкості пари векторів $u_1, \bar{\sigma}^{(m)}$ разом зі зростанням m має і негативні наслідки в світлі проблеми, що розглядається. Дійсно, зниження чутливості до збурних дій сприяє підвищенню ефективності виявлення ЦЗ, цілісність яких порушена не була, але це зниження дещо ускладнює виявлення змінених ЦЗ. Дійсно, чим стійкіша пара $u_1, \bar{\sigma}^{(m)}$, тим менше вона «реагує» на будь-

яку збурну дію, утруднюючи пошук властивостей відповідних гістограм, які і вказують на це порушення, що знайшло своє підтвердження на практиці в результаті обчислювального експерименту, в якому були задіяні 1000 ЦЗ, описаних вище. Ілюстрація цьому наведена на рис.3 для того ж ЦЗ (рис.1), яке використовувалося в оригінальному вигляді на рис.2. В якості збурної дії тут використовувалось накладання гауссівського шуму з нульовим математичним очікуванням і D=0.005.

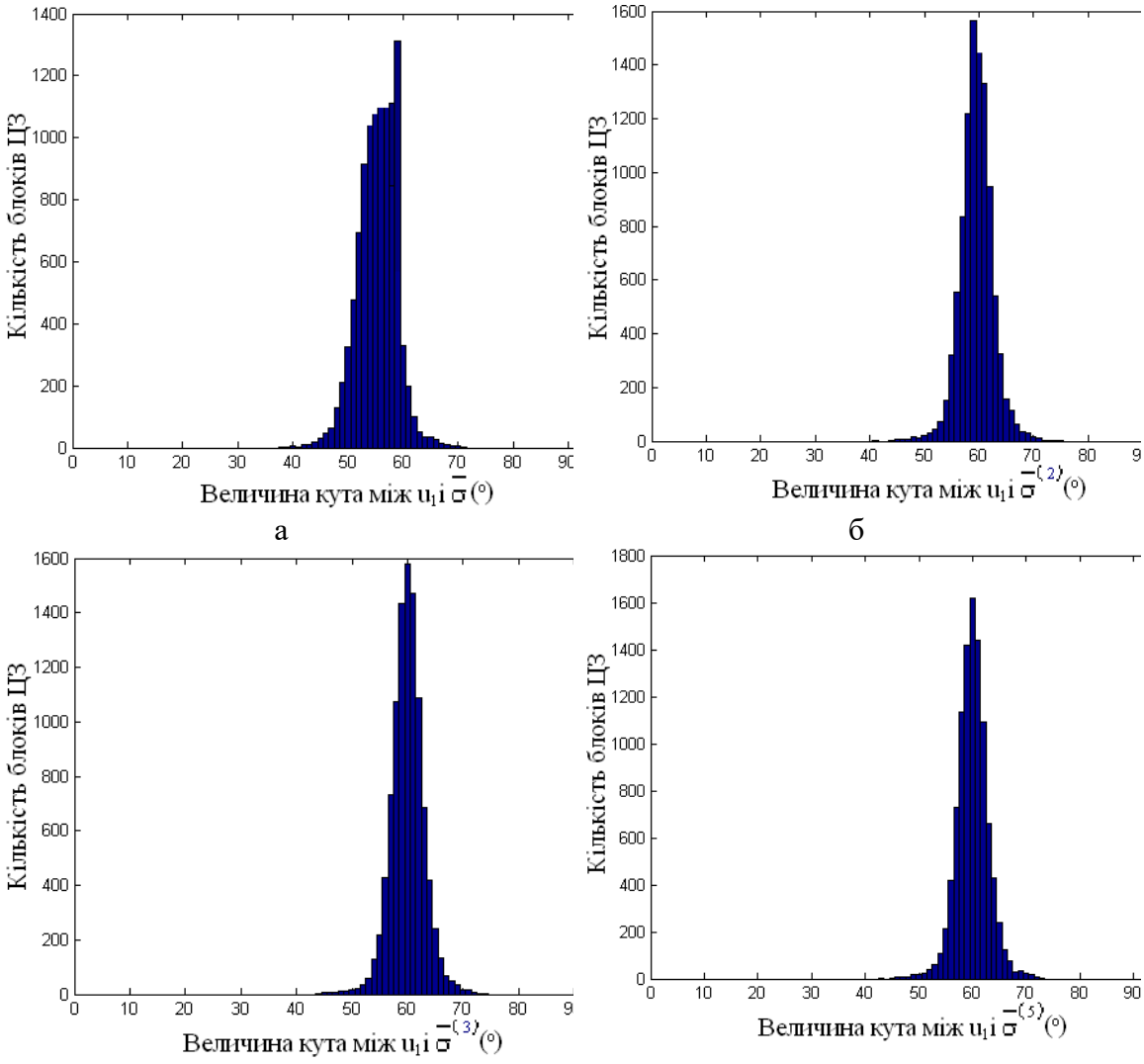


Рис.3. Гістограми значень кутів (21) для ЦЗ, цілісність якого порушена: а – аналізуються вектори $u_1, \bar{\sigma}$; б - вектори $u_1, \bar{\sigma}^{(2)}$; в - вектори $u_1, \bar{\sigma}^{(3)}$; г - вектори $u_1, \bar{\sigma}^{(5)}$

Найзначнішою тут є реакція пари векторів $u_1, \bar{\sigma}$ і $u_1, \bar{\sigma}^{(2)}$, яка приводить до зміни положення моди гістограми в результаті збурення ЦЗ, а при $m > 2$, мода не змінює своє положення відносно того, яким воно було для оригінального ЦЗ. І хоча гістограми оригінального і збуреного ЦЗ навіть при співпадінні моди значно відрізняються (порівн. рис.2(в) і 3(в); рис.2(г) і 3(г)): значення гістограми в моді менше для збуреного ЦЗ майже в 3 рази, велика кількість блоків збуреного ЦЗ має кут між $u_1, \bar{\sigma}^{(m)}$, $m > 2$, близький до моди, що є очікуваним і випливає з [11-14], але при відсутності гістограми відповідного оригінального ЦЗ, що є стандартною

ситуацією на практиці при проведенні експертизи цілісності, встановити її порушення буде тут складніше, ніж у випадку $m = 2$. Підвищення стійкості пари $u_1, \overline{\sigma}^{(m)}$, що має місце зі зростанням *m*, є очевидним і у випадку ЦЗ, цілісність якого порушена: мода не тільки не зсувається з місця $\angle\left(n^O, e_1\right)$, але й значення гістограми в моді зростає (див.рис.3(в, г)).

Таким чином, на практиці не має сенсу підвищувати значення *m* більше двох, що, підвищуючи обчислювальну складність процесу експертизи ЦЗ, принципово не зможе покращити ефективність експертних методів, заснованих на розглянутому підході, зменшуючи кількість помилок другого роду при очікуваному збільшенні кількості помилок першого роду.

Висновки

В роботі проаналізовані різноманітні перетворення матриці блока ЦЗ з метою їх використання для підвищення ефективності експертизи цілісності ЦЗ, що базується на аналізі властивостей СНЧ і СНВ блоків матриці контенту, отриманих шляхом її стандартної розбивки. Встановлено, що для підвищення ефективності підтвердження збереження цілісності ЦЗ має сенс використовувати перетворення виду (4) при *m*=2, виду (10) при *m*=3, але з урахуванням пріоритетності виявлення саме порушення цілісності в загальному випадку перевагу треба віддати перетворенню (4) з *m*=2.

Список літератури

1. Пирцхалава Л.Г. Информационное противоборство в современных условиях. К.: ЦП Компринт, 2019. 226 с.
2. Appari A., Johnson M.E. Information security and privacy in healthcare: current state of research. *International Journal of Internet and Enterprise Management*. 2010. 6(4). P. 279–314
3. Shabtai A., Elovici Y., Rokach L. A Survey of Data Leakage Detection and Prevention Solutions. Boston: Springer, 2012. 100 p.
4. Mazurczyk W. Information Hiding in Communication Networks: Fundamentals, Mechanisms, Applications, and Countermeasures /. Hoboken: Wiley, 2016. 296 p.
5. Heatherly R., Kantarcioglu M., Thuraisingham B. Preventing private information inference attacks on social networks. *IEEE Transactions on Knowledge and Data Engineering*. 2013. 25(8). P. 1849–1862.
6. Задірака, В.К. Сучасні методи розв'язання задач інформаційної безпеки. *Вісник НАН України*. 2014. 5. С. 65–69.
7. Milov O. Development of methodology for modeling the interaction of antagonistic agents in cybersecurity systems. *Восточно-Европейский журнал передовых технологий*. 2019. 2(9). С. 56–66.
8. Uliyan D.M. Image region duplication forgery detection based on angular radial partitioning and Harris key-points. *Symmetry*. 2016. 8(7). 62.
9. Kobozeva A.A., Bobok I.I., Garbuz A.I. General principles of integrity checking of digital images and application for steganalysis. *Transport and Telecommunication Journal*. 2016. 17(2). P. 128–137.
10. Кобозева, А.А. Основы общего подхода к разработке универсальных стеганоаналитических методов для цифровых изображений. *Праці Одеського політехнічного університету*. 2014. 2. С. 136–146.
11. Бобок И.И. Теоретическое развитие общего подхода к проблеме выявления нарушений целостности цифровых контентов, основанного на анализе полного набора формальных параметров. *Інформатика та математичні методи в моделюванні*. 2017. 7(3). С. 170–177.

12. Бобок І.І. Дослідження властивостей формальних параметрів цифрового зображення в умовах порушення його цілісності. *Сучасна спеціальна техніка*. 2017. 4(51). С. 6–16.;
13. Бобок І.І Розвиток загального підходу до проблеми виявлення порушень цілісності цифрових зображень. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2017. 2(34). С. 78–88.
14. Бобок І.І. Розвиток теоретичних основ підходу до проблеми виявлення порушень цілісності цифрового зображення. *Перспективні напрями захисту інформації*: матеріали V Всеукр. наук.-практ. конф. Одеса, 2019. С. 17–19
15. Гонсалес Р., Вудс Р. Цифровая обработка изображений. М.: Техносфера, 2006. 1070 с.
16. Деммель Д. Вычислительная линейная алгебра: теория и приложения. М.: Мир, 2001. 430 с.
17. NRCS Photo Gallery // United States Department of Agriculture. URL: https://www.nrcs.usda.gov/wps/portal/nrcs/main/national/newsroom/multimedia/
18. Gloe T., Böhme R. The “Dresden Image Database” for benchmarking digital image forensics. *Proceedings of the 2010 ACM Symposium on Applied Computing (SAC ’10)*. New York, 2010. P. 1585–1591.

INVESTIGATION OF THE PARAMETERS OF THE CONVERTED BLOCKS OF A DIGITAL IMAGE TO DETECT VIOLATIONS OF ITS INTEGRITY

I.I. Bobok

National Odesa Polytechnic University, ave. Shevchenko, 1, Odesa, 65044, Ukraine
onu_metal@ukr.net

The problem of detecting the integrity violations of information content is one of the main problems of modern information security. Unauthorized modified information content when used for non-entertainment purposes can lead to critically negative consequences for individuals, enterprises, banks, firms, and catastrophic consequences for humanity as a whole if cyber-attacks are directed at the military, energy, chemical industry, etc. The world scientific community pays a lot of attention to the problem of detecting the integrity violations of information content, in particular digital images considered in the work, but this problem does not have a final solution, the task of improving approaches and methods of examination of the integrity of digital content will remain relevant. The aim of the work is to investigate the possibilities of improving the existing approach to detecting unauthorized changes of digital images, based on the analysis of singular values and singular vectors of the blocks of the corresponding matrix, by studying the properties of the blocks obtained using various transformations that differ from those proposed earlier. The properties of the blocks obtained by general symmetrization, as well as by the proposed transformations, which result in asymmetric matrices that can use an arbitrary number of m matrix-multipliers, are investigated. It has been established that to increase the effectiveness of confirming the integrity of the image, it makes sense to use symmetric blocks at m=2, non-symmetrized blocks at m=3, but taking into account the priority of detecting integrity violations, in the general case preference should be given to the symmetrization transformation with m=2.

Keywords: digital image integrity, integrity violation, singular value, singular vector, sensitivity to disturbances

DOI 10.15276/imms.v12.no3.173
УДК 681.514:621.029

Informatics and Mathematical Methods in Simulation
Vol. 12 (2022), No. 3, pp. 173-181

УДОСКОНАЛЕННЯ МЕТОДУ ВИЯВЛЕННЯ ТА ЛОКАЛІЗАЦІЇ ОБЛАСТЕЙ КЛОНУВАННЯ В ЦИФРОВИХ ЗОБРАЖЕННЯХ

Р.І. Васалатій, В.І. Матрос, О.Ю. Лебедєва, Д.А. Маєвський

Національний університет «Одеська Політехніка»,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: vasroma4@gmail.com, matros.s.od@gmail.com

Розглядається удосконалення методу виявлення та локалізації областей клонування в цифрових зображеннях. Значну роль у сучасному світі відіграють цифрові сигнали, зокрема, цифрові зображення, що використовуються у науці, медицині, судових розглядах, пресі тощо. Сьогодні камера є у кожного, якщо подія значуща, то у вашому розпорядженні опиняться тисячі фотографій. Проте змінити фотографію дуже просто. Це можуть зробити навіть любителі. Часто такі фальсифікації практично неможливо виявити неозброєним оком. Однією з найчастіше використовуваних операцій під час фальсифікації цифрових зображень є операція клонування, у ході якої відбувається заміна частини цифрового зображення, частиною того ж цифрового зображення. В роботі розглядається метод виявлення та локалізація областей клонування на основі коефіцієнту кореляції Пірсона. У базовому методі використовуються блоки розміром 8x8 як компроміс між часом обробки зображення та точністю виявлення областей клонування. Збільшення розміру блоку дозволить прискорити роботу базового методу. Іншим направленням удосконалення методу виявлення та локалізації клонованих блоків можна вважати використання маркерів. Маркери – це заздалегідь визначені пікселі в блоку, які використовуються для визначення перспективності блоку для виявлення області клонування. В роботі запропоновано маркери для квадратних блоків та блоків складної форми. Під блоками складної форми в роботі прийняти блоки які складаються з відповідного набору пікселів, які використовуються для виявлення та локалізації областей клонування. Наводяться основні кроки удосконаленого методу виявлення та локалізації областей клонування в цифрових зображеннях. Оцінку ефективності удосконаленого методу виявлення та локалізації областей клонування виконано у вимірюванні часу виявлення та локалізації областей клонування до удосконалення та після.

Ключові слова: зображення, фальсифікація зображень, виявлення клонування областей, блоки складної форми.

Вступ

Суспільство вступило у період свого розвитку, який на загальну думку можна назвати інформаційним. Процес впровадження нових інформаційних технологій у всі сфери життя суспільства немислимий без вирішення питань інформаційної безпеки, зокрема питань, пов'язаних із забезпеченням/виявленням порушень цілісності цифрових контентів.

У сучасному цифрові технології стали невід’ємною частиною життя людини. У сервісі Google Images на сьогоднішній день можна знайти більше 136 мільярдів фотографій. Кожен рік по всьому світу роблять приблизно 1,72 трильйони фотографій. Кожен день користувачі інтернету діляться між собою 3,2 мільярдами зображень. Через це в інтернеті легко зіткнутися з фальсифікованими зображеннями, навіть у довірених новинних виданнях, оскільки у вільному доступі знаходяться такі графічні редактори, як Adobe Photoshop, Figma, GIMP та Photo Pos Pro.

У наш час цифрові зображення (ЦЗ) можуть бути просто змінені за допомогою комп’ютерів та редагування фотографій, тощо. Ці зміни вплинуть на достовірність зображень у законодавстві, політиці, ЗМІ, промисловості та

медицині.

Фальсифікація – це маніпуляції з цифровим зображенням, щоб приховати певну значущу або корисну інформацію зображення. Виявлення фальсифікації цифрових зображень є однією з найбільш критичних аналітичних практик у наш час. Через це зростає необхідність у ефективних методах виявлення фальсифікованого зображення.

Однією з найчастіше використовуваних операцій під час фальсифікації цифрових зображень, реалізованої у всіх графічних редакторах, є операція клонування, у ході якої відбувається заміна частини (частин) цифрового зображення, частиною (частинами) того ж цифрового зображення.

Через загальнодоступність програмного забезпечення, що дозволяє обробляти і редагувати ЦЗ, а також у зв'язку з різноманітністю способів їх фальсифікації, зростає необхідність у вдосконаленні існуючих та розробці нових методів виявлення порушення цілісності ЦЗ, що є обов'язковою складовою частиною будь-якої сучасної комплексної системи захисту інформації. Тому зростає актуальність методів виявлення порушення цілісності цифрових зображень.

Постановка задачі та мети дослідження

У роботі буде розглядатись фальсифікація цифрових зображень методом клонування, яку можна реалізувати у будь-якому графічному редакторі за допомогою інструментів виділення області, копіювання або за допомогою інших інструментів. Так в графічному редакторі Adobe Photoshop для цих цілей можна використовувати такі інструменти як Штамп (Clone Stamp), Пензель відновлення (Healing Brush) і Латка (Patch). Для більш вдалого клонування зловмисники також можуть використовувати Гумка (Erase) и Розмиття (Blur) для «замітання слідів» своєї фальсифікації.

Метою роботи є підвищення ефективності методу виявлення та локалізації областей клонування в цифрових зображеннях шляхом його модифікації, заснованої на використанні маркерів.

Для досягнення поставленої мети необхідно вирішити такі завдання:

- огляд методів та засобів виявлення та локалізації областей клонування в цифрових зображеннях;
- проаналізувати метод виявлення та локалізації областей клонування в цифрових зображеннях та провести вибір маркерів для блоків, які використовуються для виявлення областей фальсифікації;
- вибір виду складних блоків для виявлення областей клонування;
- удосконалення методу виявлення та локалізації областей клонування в цифрових зображеннях;
- програмна реалізація удосконаленого методу виявлення та локалізації областей клонування в цифрових зображеннях та оцінити його ефективність.

Під ефективністю в цій роботі будемо розуміти зменшення часу роботи методу виявлення та локалізації областей клонування в цифрових зображеннях.

Основна частина

Для захисту та виявлення порушення цілісності ЦІ створюються відповідні методи та алгоритми, які поділяються на дві великі категорії: активні, пасивні. В активних методах деяка інформація попередньо впроваджується у ЦІ. Пасивні методи дозволяють підтвердити цілісність ЦІ або виявити її порушення без впровадження додаткової інформації. У роботі розглядатимутися пасивні методи.

Виходячи з найчастіших операцій, що здійснюються засобами графічних редакторів над цифровими зображеннями під час їх фальсифікації, за способом створення ці фальсифікації можна розбити на такі категорії:

- клонування – коли одна область зображення копіюється і вставляється в іншу область цього зображення;
- фотомонтаж – коли використовуються частини двох чи кількох зображень для створення нового зображення;
- обробка – коли зображення або його частини піддаються таким операціям, як зміна масштабу, поворот, розмиття, зміна яскравості, кольору тощо.

При підробці областей клонування одна частина зображення копіюється та вставляється в інше місце того самого зображення, щоб приховати інформацію або змінити значення зображення [1]. Отже, між оригінальною та клонованою областю існує сильна кореляція, яку можна використовувати як доказ для виявлення підробки копіювання-переміщення.

Існують різні методів виявлення областей клонування, які спираються на різні компоненти, наприклад яскравість пікселей або сингулярні числа, різні ускладнення, наприклад фальсифікація без додаткової обробки або зі збереженням у форматі з втратами. Кожен метод виявлення залежить від поставленої задачі: чи то обробити якомога швидше, чи то обробити якомога точніше.

Одним з перспективних для удосконалення та модифікації методів виявлення клонованих областей є метод виявлення на основі коефіцієнту кореляції Пірсона.

Коефіцієнт кореляції Пірсона (позначають «r») – в статистиці, показник кореляції (лінійної залежності) між двома змінними X та Y, який набуває значень від −1 до +1 включно [2]. Він широко використовується в науці для вимірювання ступеня лінійної залежності між двома змінними.

Коефіцієнт кореляції Пірсона між двома змінними дорівнює сумі добутків відхилень, поділеній на добуток їх стандартних відхилень. Нехай, є дві вибірки $x^m = (x_1, \ldots, x_m)$, $y^m = (y_1, \ldots, y_m)$, тоді коефіцієнт кореляції Пірсона розраховують за формулою 1:

$$r_{xy} = \frac{\sum_{i=1}^{m}(x_i - \bar{x})(y_i - \bar{y})}{\sum_{i=1}^{m}(x_i - \bar{x})^2 \sum_{i=1}^{m}(y_i - \bar{y})^2} \quad (1)$$

де $\bar{x}$, $\bar{y}$ – вибіркові середні x^m і y^m.

Для представлення цифрового зображення розміром $n \times m$ пікселів в роботі використовується: $n \times m$ – матриці R, G, B (колірна схема RGB); $n \times m$ – матриця яскравості Y (колірна схема YUV).

У роботі [3] пропонується метод виявлення областей клонування шляхом використання коефіцієнта Пірсона який має наступні кроки:

1. Перевести зображення з режиму RGB до YUV.
2. Ініціалізувати область, що треба виявити *Res* = ⦰ та розбити матрицю яскравості цифрового зображення на множину квадратних блоків, що перетинаються, $C = \{c_1, c_2, \ldots, c_s\}$, $\bigcup_{i=1}^{s} c_i = Y$, розміром $p \times p$ (тут кожний наступний блок відрізняється від попереднього зсувом на 1 піксель вправо, вліво, вниз та угору).
3. Кожний блок c_i, i = 1, …, s розглянути в парі з усіма c_j, j = i+1, …, s, відповідно. Для кожної пари розраховується коефіцієнт кореляції Пірсона.
   3.1 Якщо кореляція дорівнює 1, то блоки c_i та c_j – це оригінальний та клонований, після чого до результату додаються обидва блоки: *Res = Res* ∨ *ci* ∨ *cj*.
   3.2 Якщо кореляція не дорівнює одиниці, то перейти до наступної пари блоків.
4. Вивести знайдену область Res.

Ілюстративний приклад роботи описаного базового методу виявлення та локалізації областей клонування представлений на рисунку 1.

а б в

Рис. 1. Результат роботи методу виявлення та локалізації областей клонування: оригінальне зображення (а); фальсифіковане (б); результат виявлення стандартними блоками (в)

У базовому методі використовуються блоки розміром 8x8 через компроміс між часом обробки зображення та точністю виявлення областей клонування. Хоча зменшення розміру блоку дозволяє уточнювати область фальсифікації, чим більше зменшується розмір блоку, тим більше буде кількість помилок другого роду. Збільшення розміру блоку прискорює роботу базового методу.

Іншим направленням удосконалення методу виявлення та локалізації клонованих блоків можна вважати використання маркерів. Маркери – це заздалегідь визначені пікселі обох блоків, які будуть зрівнюватись. Для квадратних блоків різних розмірів в роботі було запропоновано використовувати кутові пікселі у якості маркерів (рис. 2)**Ошибка! Источник ссылки не найден.**.

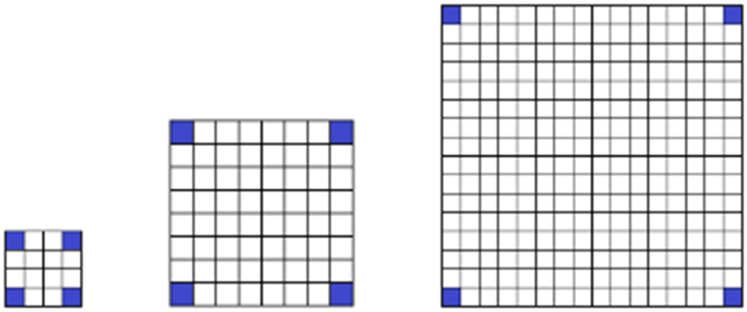


Рис. 2. Маркери блоку квадратної форми розміру 4x4, 8x8, 16x16

Для блоків, розміром 4x4 в якості маркеру для цілого блока беруться лише 4 значення яскравості, що відповідають пікселям, які знаходяться в кутах блоку. Це значно підвищить ефективність роботи алгоритму виявлення областей клонування, але якщо брати блоки розміром 16x16, виявлена область клонування буде меншою, ніж є насправді. Оптимальним є використання маркерів для квадратних блоків розміром 8x8.

Перед тим як вирахувати коефіцієнт кореляції при порівнянні двох блоків, будемо порівнювати між собою маркери блоків. Якщо маркери у двох блоків співпадають, то припускаємо, що маємо справу зі схожими (клонованими та оригінальними) блоками та тільки тоді будемо вираховувати коефіцієнт кореляції для остаточного підтвердження цього припущення.

Тоді удосконалений метод для виявлення та локалізації областей клонування буде мати наступні шаги:

1. Ініціалізувати область, що треба виявити $res = \emptyset$ та розбити матрицю яскравості Y цифрового зображення на множину блоків, що перетинаються,

розміром $p \times p$ пікселей $C = \{c_1, c_2, \dots, c_s\}$ таких, що: $\bigcup_{i=1}^{s} c_i = Y$, (тут кожний наступний блок c_i відрізняється від попереднього c_{i-1} зсувом на 1 піксель вправо, вліво, вниз та угору).

2. Кожний блок $c_i,\ i = 1, \dots, s$, розглянути в парі з усіма $c_j,\ j = i + 1, \dots, s$, відповідно. Для кожної пари:

2.1 Для кожної пари блоків c_i та c_j:

2.2 Отримати набори маркерів mc_i та mc_j. Якщо маркери mc_i не дорівнюють mc_j, то розглядати наступну пару блоків. Інакше виконати наступні шаги:

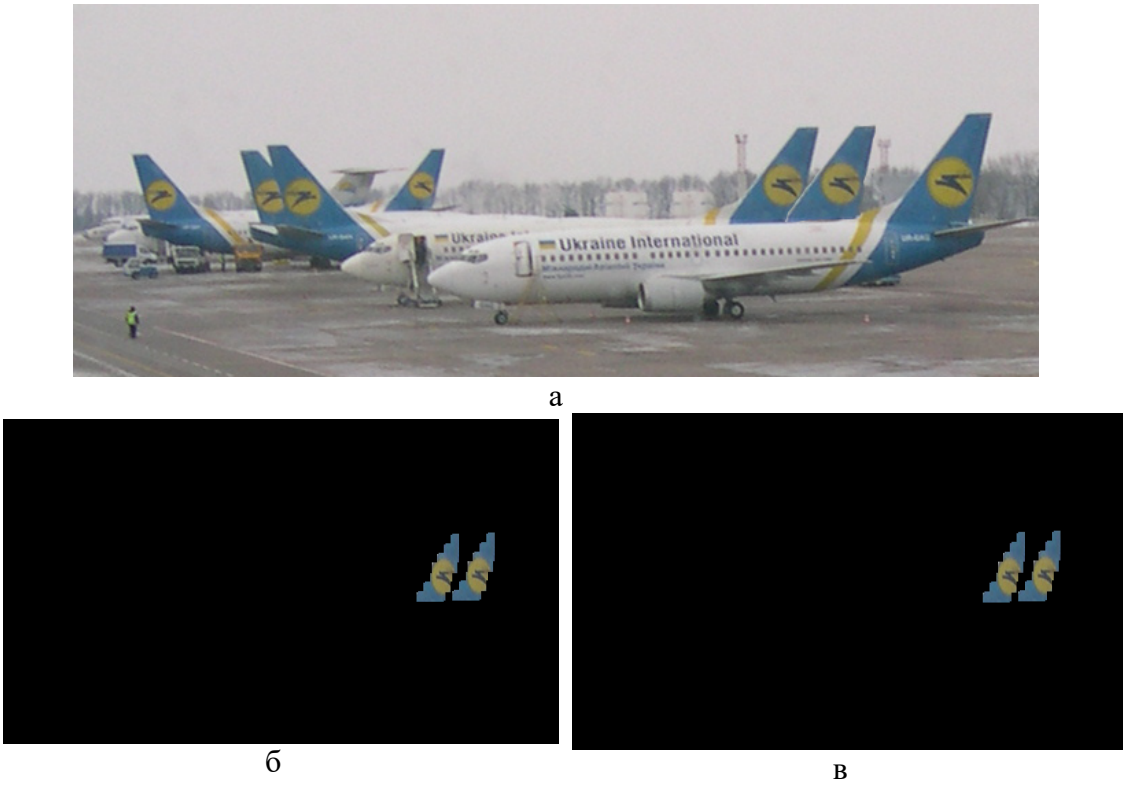
2.2.1 Розрахувати коефіцієнт кореляції: $cor = correlation(c_i, c_j)$.

2.2.2 Якщо $cor = 1$, то блоки c_i и c_j являються оригінальним та клонованим,

$res = res \cup\ c_i \cup c_j$.

3. Вивести знайдену область res.

Розглянемо приклад результату роботи удосконаленого методу. Знайдені клоновані області при запусках без використання маркерів та з використанням маркерів будуть однакові (рисунок 3).



а б в

Рис. 3. Результат роботи алгоритму: зображення, що обробляється (а); пошук по блокам без використання маркерів (б); пошук по блокам з використання маркерів (в)

Оцінку ефективності удосконаленого методу виявлення та локалізації областей клонування виконано у вимірюванні часу виявлення та локалізації областей клонування до удосконалення та після. Нижче в таблиці 1 наведені дані експерименту для деяких зображень при використанні блоків 8x8.

Таблиця 1

Дані експериментів при використанні блоків 8x8

№ зображення	Розмір зображення	Час роботи базового методу (годин:мінут:секунд)	Час роботи удосконаленного методу (годин:мінут:секунд)
1	240 x 480	00:09:44	00:00:54
2	272 x 400	00:21:59	00:00:49
3	320 x 880	00:47:52	00:03:51
4	320 x 832	00:39:43	00:03:27
5	272 x 704	00:21:00	00:01:49
6	320 x 480	00:14:30	00:01:11
7	880 x 512	02:03:02	00:10:07
8	240 x 512	00:08:28	00:00:44
9	240 x 352	00:05:41	00:00:23
10	176 x 352	00:02:17	00:00:11

Маркери можна використовувати не тільки для квадратних блоків, а і для блоків різної форми. В роботі також розглядалися блоки складної форми. Під блоками складної форми будемо розуміти блоки які складаються з відповідного набору пікселів, які використовуються для виявлення та локалізації областей клонування.

В роботі проводився експеримент з використанням блоків складної форми розміром 16x16. В експерименті використовувались складні блоки різних форм. За результатом експерименту було вирішено залишити для виявлення областей клонування 3 блоки (рисунок 4), де сірим позначені пікселі, що використовуються.

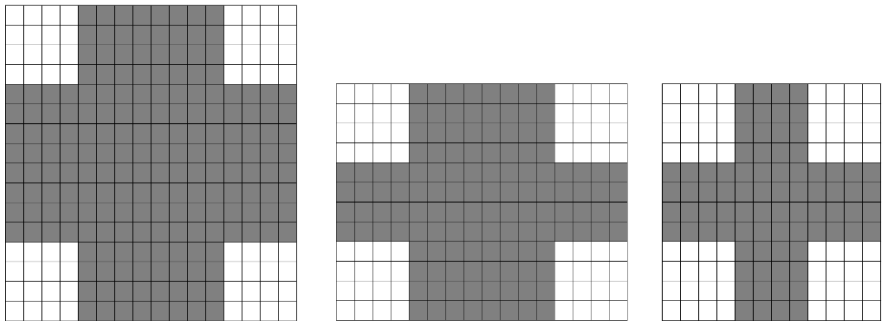


Рис. 4. Типи блоків складної форми

Блок А залишився 16x16. Розмір блоку В змінився на 16x12, а блоку С – на 12x12. Кутові пікселі в блоках прибрані, щоб краще відстежувати нерівні контури області клонування.

Проводився експеримент на цифрових зображеннях з використанням обраних типів блоків. Результати роботи використання блоків складної форми для виявлення та локалізації областей клонування продемонстровані на рисунку 5.

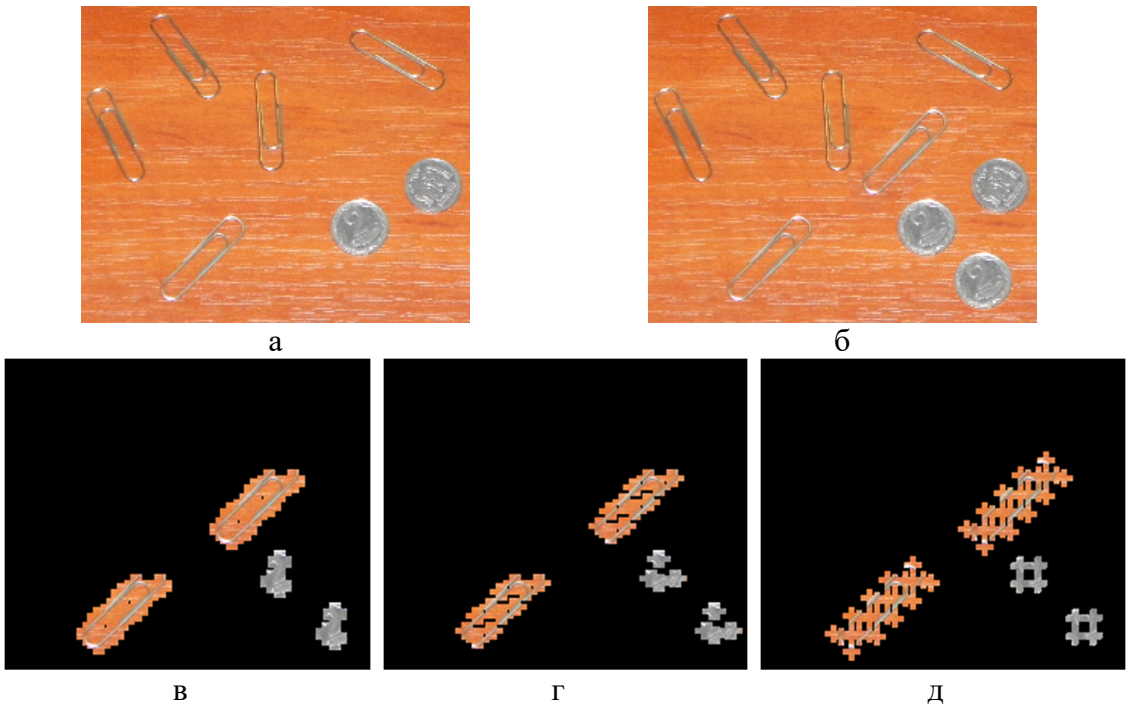


Рис. 5. Результат виявлення областей клонування з використанням складних блоків: оригінальне зображення (а); фальсифіковане (б); складними блоками типу A (в); складними блоками типу B (г); складними блоками типу C (д);

Оскільки ці блоки краще себе проявляють на периметрі області клонування, то, щоб уникнути пустих дир, що будуть утворені через відсутність кутових пікселів блоку, то у подальшому до методу необхідно додати додаткову перевірку. Якщо коефіцієнт кореляції між двома складними блоками дорівнюватиме одиниці, то буде проведена додаткова перевірка на кореляцію, використовуючи вже квадратні блоки того ж розміру.

Для обраних блоків складної форми було вирішено використовувати маркери, які продемонстровано на рисунку 6.

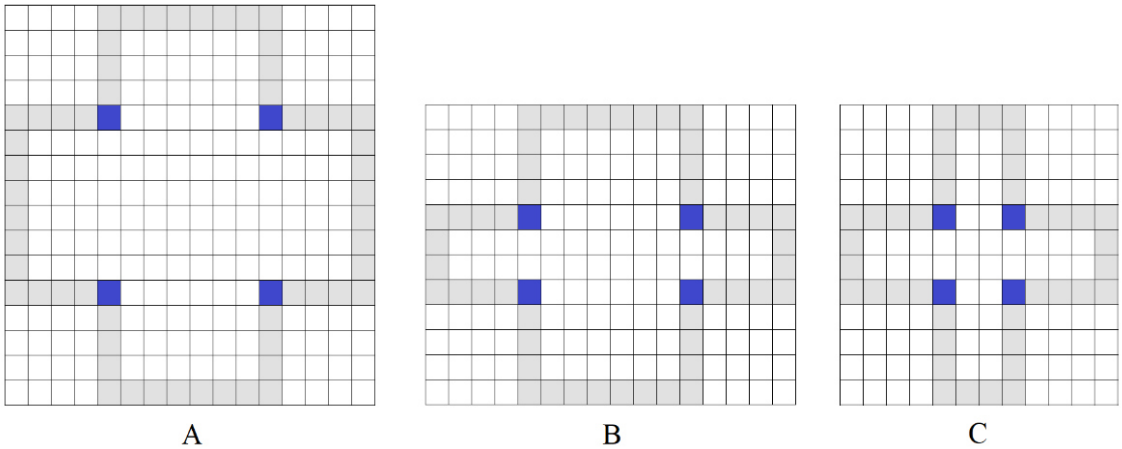


Рис. 6. Маркери блоків складної форми

Результати експериментів з використання блоків складної форми наведені нижче у таблиці 2 та 3.

Таблиця 2

Час роботи методу без маркерів при використанні блоків складної форми у форматі (ГГ:ХХ:СС)

Номер зображення	Розмір	Час роботи				
		квадратні блоки 8x8	квадратні блоки 16x16	блок складної форми типу A	блок складної форми типу B	блок складної форми типу C
1	301x235	0:03:08	0:01:36	0:01:44	0:01:49	0:02:26
2	352x176	0:02:27	0:01:17	0:01:13	0:01:29	0:01:56
3	256x208	0:01:56	0:00:57	0:01:07	0:01:07	0:01:27
4	216x216	0:01:30	0:00:40	0:00:47	0:00:47	0:01:09
5	704x272	0:25:06	0:12:25	0:17:40	0:17:10	0:18:05
6	880x320	1:02:02	0:26:20	0:44:54	0:37:54	0:43:31
7	832x320	0:49:50	0:23:19	0:28:38	0:28:03	0:41:06
8	512x240	0:11:34	0:04:57	0:06:39	0:06:01	0:09:58

Як можна побачити, навідмінно від квадратних блоків, при використанні складних блоків обробка проходить значно швидше. При тому чим більше розмір зображення, тим більша буде різниця часу обробки.

Таблиця 3

Час роботи методу з маркерами при використанні блоків складної форми у форматі (ГГ:ХХ:СС)

Номер зображення	Розмір	Час роботи				
		квадратні блоки 8x8	квадратні блоки 16x16	блок складної форми типу A	блок складної форми типу B	блок складної форми типу C
1	301x235	0:00:14	0:00:03	0:00:03	0:00:04	0:00:06
2	352x176	0:00:16	0:00:02	0:00:04	0:00:05	0:00:07
3	256x208	0:00:11	0:00:02	0:00:03	0:00:03	0:00:05
4	216x216	0:00:09	0:00:01	0:00:02	0:00:02	0:00:04
5	704x272	0:01:53	0:00:26	0:00:27	0:00:37	0:00:51
6	880x320	0:04:07	0:00:56	0:01:06	0:01:24	0:01:54
7	832x320	0:03:45	0:00:50	0:00:56	0:01:12	0:01:41
8	512x240	0:00:45	0:00:10	0:00:11	0:00:14	0:00:21

Висновки

За результатами аналізу методу виявлення та локалізації областей клонування в цифрових зображеннях був проведений вибір маркерів для квадратних блоків та блоків складної форми, які можуть використовуватися для виявлення областей фальсифікації.

Удосконалено метод виявлення та локалізації областей клонування шляхом використання маркерів в процесі виявлення областей клонування, що дозволило прискорити час роботи методу.

Список літератури

1. Rani P., Rani J. Copy-move morgery attack detection in digital images. International *Journal of Engineering Research and Technology IJERT*. 2015. V.4. Is.6. P. 118-132.
2. Коефіцієнт_кореляції_Пірсона. Матеріал з вікіпедії – вільної енциклопедії. URL: https://uk.wikipedia.org/wiki/Коефіцієнт_кореляції_Пірсона
3. Лебедева, Е.Ю., Лебедев Ю.Ф. Исследование метрик используемых при обнаружении клонированных участков изображений в задачах выявления фальсификаци. *Вісник національного технічного університету ХПІ.* 2011. №35. С.25 – 31.

IMPROVEMENT OF THE METHOD OF DETECTION AND LOCALIZATION OF CLONING AREAS IN DIGITAL IMAGES

R. Vasalatiy, V. Matros, O. Lebedieva, D. Majevsky

National Odesa Polytechnic University, ave. Shevchenko, 1, Odesa, 65044, Ukraine
e-mail: vasroma4@gmail.com, matros.s.od@gmail.com

The paper considers the improvement of the method of detection and localization of cloning areas in digital images. A significant role in the modern world is played by digital signals, in particular, digital images used in science, medicine, court proceedings, the press, etc. Today, everyone has a camera, if the event is significant, you will have thousands of photos at your disposal. However, changing the photo is very easy. Even amateurs can do it. Often, such falsifications are almost impossible to detect with the naked eye. One of the most commonly used operations in the forgery of digital images is the cloning operation, in which a part of a digital image is replaced by a part of the same digital image. The paper considers the method of detection and localization of cloning regions based on the Pearson correlation coefficient. The basic method uses 8x8 blocks as a compromise between image processing time and the accuracy of cloning region detection. Increasing the block size will speed up the base method. Another way to improve the method of detecting and locating cloned blocks is to use markers. Markers are predefined pixels in a block that are used to define the perspective of the block to identify the cloning area. Markers for square blocks and blocks of complex shape are proposed in the work. Blocks of a complex shape in the work are considered to be blocks consisting of a suitable set of pixels, which are used to detect and localize areas of cloning. The main steps of the improved method of detection and localization of cloning regions in digital images are presented. Evaluation of the effectiveness of the improved method of detection and localization of cloning areas was performed by measuring the time of detection and localization of cloning areas before and after improvement.

Keywords: image, image falsification, area cloning detection, blocks of complex shape.

DOI 10.15276/imms.v12.no3.182
УДК 519.242:519.25

Informatics and Mathematical Methods in Simulation
Vol. 12 (2022), No. 3, pp. 182-192

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ПРИЙНЯТТЯ РІШЕНЬ В ФОРМУВАННІ ЄДИНОЇ БАЗИ ДАНИХ ОБ'ЄКТІВ-АНАЛОГІВ ДОСЛІДЖУВАНОГО ОБ'ЄКТА

Н. М. Єршова

Придніпровська державна академія будівництва та архітектури
м. Дніпро, 49000, вул. Чернишевського, 24 а E-mail:
nersova107@gmail.com

Експеримент посідає особливе місце серед способів отримання інформації про внутрішні взаємозв'язки явищ у природі та техніці. Відповідно ускладненню досліджуваних процесів та явищ зростають витрати на апаратуру та проведення експерименту. У ході випробувань збирається велика кількість експериментальних даних, що потребують обробки та аналізу. При цьому тривалість аналізу, осмислення результатів випробувань та їхнього обліку для коригування характеристик нових виробів дуже значна. Під час проведення спостережень чи експерименту дуже важливо відібрати методи та інструментальні засоби обробки даних експерименту. Незважаючи на те, що починаючи з 2001 року в багатьох роботах доводиться ефективність пакету аналізу Excel для обробки даних експерименту, досі в науковій та навчальній літературі використовується при обробці даних спостережень та експерименту обчислення розрахункових значень критеріїв рівності дисперсій та середніх за формулами, а вибір їх критичних значень за таблицями. Іншою проблемою є формування вибірки з вибірок різного обсягу прямим розрахунком за формулами навіть у середовищі Excel. У даній роботі пропонується методика дисперсійного аналізу однорідності вибірок різного обсягу з використанням інструментів пакету аналізу Excel. Інструмент «Описова статистика» виконує статистичну обробку багатовимірних вибірок різного обсягу та видає значення 13 параметрів, у тому числі: середнє значення, мода, медіана, ексцес, асиметричність, дисперсія та обсяг вибірки. За цією інформацією легко визначити розрахункове та критичне значення статистик. Критичне значення критеріїв визначаються за допомогою статистичних функцій майстра функцій. Вихідна інформація інструменту «Однофакторний дисперсійний аналіз» містить розрахункове та критичне значення F – критерію Фішера, що дозволяє легко перевірити однорідність вибірок рівного обсягу. Методика значно спрощує процедуру формування єдиної бази даних об'єктів-аналогів досліджуваного об'єкта.

Ключові слова: експеримент, обробка даних, дисперсійний аналіз, формування вибірки, вибірки різного обсягу, пакет аналізу Excel.

Вступ

В багатьох роботах доводиться ефективність пакету аналізу Excel для обробки даних експерименту, але досі в науковій та навчальній літературі використовується при обробці даних спостережень та експерименту обчислення розрахункових значень критеріїв рівності дисперсій та середніх за формулами, а вибір їх критичних значень за таблицями. Іншою проблемою є формування вибірки з вибірок різного обсягу прямим розрахунком за формулами. У даній роботі пропонується методика дисперсійного аналізу однорідності вибірок різного обсягу з використанням інструментів пакету аналізу Excel. Інструмент «Описова статистика» виконує статистичну обробку багатовимірних вибірок різного обсягу та видає значення 13 параметрів, у тому числі: середнє значення, мода, медіана, ексцес, асиметричність, дисперсія та обсяг вибірки. За цією інформацією легко визначити розрахункове та критичне значення статистик. Критичне значення критеріїв визначаються за допомогою статистичних функцій

майстра функцій. Вихідна інформація інструменту «Однофакторний дисперсійний аналіз» містить розрахункове та критичне значення F – критерію Фішера, що дозволяє легко перевірити однорідність вибірок рівного обсягу. Методика значно спрощує процедуру формування єдиної бази даних об'єктів-аналогів досліджуваного об'єкта.

Аналіз останніх досліджень і публікацій

Експеримент посідає особливе місце серед способів отримання інформації про внутрішні взаємозв'язки явищ у природі та техніці. Відповідно ускладненню досліджуваних процесів та явищ зростають витрати на апаратуру та проведення експерименту. У ході випробувань збирається велика кількість експериментальних даних, що потребують обробки та аналізу. При цьому тривалість аналізу, осмислення результатів випробувань та їхнього обліку для коригування характеристик нових виробів дуже значна. Під час проведення спостережень чи експерименту дуже важливо відібрати методи та інструментальні засоби обробки даних експерименту. Незважаючи на те, що починаючи з 2001 року в роботах [5-6, 10] доводиться ефективність використання пакету аналізу Excel для обробки даних експерименту, до цих пір у науковій та навчальній літературі при обробці даних спостережень та експерименту використовується обчислення розрахункових значень критеріїв рівності дисперсій та середніх за формулами, а вибір їх критичних значень за таблицями [1, 4, 7, 9].

Іншою проблемою є формування вибірки з вибірок різного обсягу прямим розрахунком за формулами навіть в середовищі Excel. Постає питання, чи не можна спростити цю процедуру? Виявляється, можна, якщо для цього використовувати інструмент «Описова статистика» пакету аналізу.

Мета роботи

Отже метою даної роботи є розробка методики дисперсійного аналізу однорідності вибірок різного обсягу з використанням инструменту «Описова статистика» пакету аналізу Excel.

Основна частина

Методи дисперсійного аналізу дозволяють формувати єдину базу даних об'єктів-аналогів та оцінювати величину впливу конкретних факторів на досліджувану результативну ознаку.

Під час експерименту для кожного об'єкту часто можна зміряти (отримати) значення декількох ознак. У результаті виходить багатовимірна вибірка. Смисл обробки багатовимірних вибірок полягає у встановленні зв'язків між ознаками. Для цього їх ділять на ознаки факторні і результативні. Факторна ознака викликає зміну інших, пов'язаних з ним, ознак. Результативна ознака змінюється під дією факторних ознак. Дисперсійний аналіз призначений для кількісного дослідження впливу факторних ознак на результативну ознаку у разі малих вибірок.

Для порівняння впливу факторних ознак на результативну ознаку необхідний певний статистичний матеріал – кожному рівню фактора повинна відповідати певна вибірка значень результативноъ ознаки. Статистичний матеріал зручно представляти у вигляді таблиці 1. Перш ніж судити про кількісний вплив фактора, необхідно встановити наявність такого впливу. Можливо, розбіжність значень результативної ознаки для різних рівнів фактора пояснюється дією чистої випадковості.

Загальне число спостережень $n = n_1 + n_2 + ... + n_p$.

Таблиця 1

Матриця експериментів для однофакторного аналізу

	Рівні фактора (Номер вибірки)			
	1	2	…	p
Значення результативної ознаки	x_{11} x_{21} … $x_{n_1 1}$	x_{12} x_{22} … $x_{n_2 2}$		x_{1p} x_{2p} … $x_{n_p p}$
Обсяг вибірки	n_1	n_2		n_p

На статистичній мові це припущення означає перевірку однорідності всіх вибірок таблиці 1, тобто перевірку приналежності всіх значень результативної ознаки однієї генеральної сукупності. Основною процедурою дисперсійного аналізу є перевірка цієї гіпотези за допомогою статистичних критеріїв.

Допустимо фактор A має p різних рівнів, на кожному з яких виконано n спостережень. Отже, спостерігалося $N = pn$ значень x_{ij} ознаки (властивості) X, де i - номер спостереження ($i = 1,2,...,n$), j - номер рівня фактора ($j = 1,2,...,p$).

Існують поняття [8]:

- загальна сума квадратів - сума квадратів відхилень всіх можливих значень ознаки від їх загального середнього значення

$$S = \sum_{i=1}^{n}\sum_{j=1}^{p}(x_{ij} - \overline{X})^2; \tag{1}$$

- сума квадратів між групами або за факторами - зважена сума квадратів відхилень середніх значень за групами від загального середнього значення

$$S_1 = n\sum_{j=1}^{p}(\overline{x}_j - \overline{X})^2; \tag{2}$$

- сума квадратів усередині груп - сума квадратів відхилень можливих значень ознаки кожної групи (рівня фактора) від середнього значення цієї групи

$$S_2 = \sum_{i=1}^{n}\sum_{j=1}^{p}(x_{ij} - \overline{x}_j)^2, \tag{3}$$

де $\overline{x}_j, \overline{X}$ - відповідно середнє значення групи і загальне середнє значення результативної ознаки, що визначаються за формулами

$$\overline{x}_j = \frac{\sum_{i=1}^{n} x_{ij}}{n}; \quad \overline{X} = \frac{\sum_{j=1}^{p} \overline{x}_j}{p}. \tag{4}$$

Для оцінки впливу фактора слід розкласти загальну суму квадратів на складові: суму квадратів між групами (за факторами) і суму квадратів усередині груп. Отже

$$S = S_1 + S_2. \tag{5}$$

Сума S_1 відображає вплив на результативну ознаку рівнів фактора, а сума S_2 - вплив погрішностей вимірювань. Оскільки $S_2 = S - S_1$, то суму S_2 називають ще залишковою сумою квадратів.

Суми квадратів S, S_1, S_2 ділені на відповідні числа ступенів свободи, дають три незміщені оцінки дисперсії σ^2 генеральної сукупності:

$$s^2 = \frac{S}{N-1}; \tag{6}$$

$$s_1^2 = \frac{S_1}{p-1}; \tag{7}$$

$$s_0^2 = \frac{S_2}{p(n-1)} = \frac{S_2}{N-p}. \tag{8}$$

Перша оцінка називається загальною оцінкою дисперсії (або вибірковою дисперсією), друга – оцінкою дисперсії за факторами (оцінкою дисперсії між групами або факторної дисперсією) і третя – залишковою оцінкою дисперсії (оцінкою дисперсії усередині груп або залишковою дисперсією).

Для порівняння дисперсій двох вибірок використовують F – критерій Фішера. Визначають розрахункове значення F – критерію у вигляді відношення більшої дисперсії до меншої

$$F = \frac{s_1^2}{s_2^2}\ . \tag{9}$$

Критичне значення - критерію (F_{kp}) обчислюємо за допомогою статистичної функції F .ОБР.ПХ(α; m_1; m_2). Число ступенів свободи приймають відповідно $m_1 = n_1 - 1; m_2 = n_2 - 1$, де n - обсяг вибірки. Гіпотеза про рівність дисперсій підтверджується, якщо $F \le F_{kp}$.

Для порівняння двох вибіркових середніх використовують t – статистику. Після перевірки гіпотези про рівність двох вибіркових дисперсій, обчислюють загальну дисперсію двох вибірок та розрахункове значення t – статистики за формулами:

$$s^2 = \frac{m_1 s_1^2 + m_2 s_2^2}{m}; \tag{10}$$

$$t = \frac{(\overline{X}_1 - \overline{X}_2)\sqrt{n_1 n_2 /(n_1 + n_2)}}{s}\ . \tag{11}$$

Критичне значення t - статистики (t_{kp}) визначаємо за допомогою статистичної функції СТЬЮДЕНТ.ОБР.2Х(α; m). Число ступенів свободи $m = m_1 + m_2$. Гіпотеза про рівність середніх значень підтверджується, якщо $|t| \le t_{kp}$.

На основі дисперсійного аналізу можна приймати рішення у багатьох галузях науки та практики. Особливо це важливо при створенні нових матеріалів, виробів, технологічних процесів та ін., коли є мало інформації про властивості об'єкта, що досліджується.

В даній статті розглядаються інформаційні технології прийняття рішень при формуванні єдиної бази даних об'єктів-аналогів досліджуваного об'єкта.

Мала вибірка містить мало інформації про цікаву властивість. Для отримання більш надійних висновків потрібно об'єднати малі вибірки в одну, але при цьому необхідно встановити їх однорідність.

Коли фактор приймає тільки два значення, тоді в розпорядженні дослідника є дві вибірки, що відповідно характеризують зміну результативної ознаки в залежності від зміни рівня фактора. В цьому випадку процедуру факторного аналізу називають перевіркою однорідності двох вибірок. При цьому в залежності від типу даних розрізняють дві ситуації:

– вибірки незалежні, коли вимір значень ознаки проводиться на

різних, досить однорідних об'єктах;

– вибірки представляють собою парні спостереження, коли безліч об'єктів зафіксовано, а спостереження проводяться в різні моменти часу.

Складність проведення дисперсійного аналізу залежить від обсягу вибірок. Якщо об'єднуються кілька вибірок одного обсягу, то легко перевірити їхню однорідність за допомогою інструмента «Однофакторний дисперсійний аналіз» пакета аналізу. У разі вибірок різного обсягу виникає проблема. До цього часу доводять однорідність вибірок різного обсягу безпосереднім розрахунком за формулами (1)-(11). Критичні значення критеріїв визначають за таблицями.

Доведемо шляхом моделювання можливість поєднання вибірок різного розміру за допомогою інструмента «Описова статистика» пакета аналізу.

Моделювання однорідності незалежних вибірок

В якості прикладу дисперсійного аналізу однорідності вибірок у випадку нерівного числа спостережень за факторами розглянемо дані спостережень терміну служби електричних ламп [8].

Приклад 1. Для виготовлення кожної партії ламп взято дріт різних сортів, інші умови виробництва були однакові. Потрібно встановити однорідність партій ламп між собою за терміном служби.

Вихідна інформація та результати розрахунку за формулами (1)..(11) представлені у табл.2.

Таблиця 2

Дисперсійний аналіз однорідності партій електричних ламп

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	формування вибірки з вибірок різного обсягу															
2		термін служби електричних ламп														
3	номер партії	1	2	3	4											
4	X1j	1,6	1,58	1,46	1,51			Xij-Xcp				(Xij-Xcp)^2				
5	X2j	1,61	1,64	1,55	1,52			-0	-0,06	-0,181	-0,13081	0,002	0,004	0,033	0,017	
6	X3j	1,65	1,64	1,6	1,53			-0	-0	-0,091	-0,12081	9E-04	7E-07	0,008	0,015	
7	X4j	1,68	1,7	1,62	1,67			0,01	-0	-0,041	-0,11081	8E-05	7E-07	0,002	0,012	
8	X5j	1,7	1,75	1,64	1,6			0,04	0,06	-0,021	0,029188	0,002	0,004	4E-04	9E-04	
9	X6j	1,72		1,66	1,68			0,06	0,11	-8E-04	-0,04081	0,004	0,012	7E-07	0,002	
10	X7j	1,8		1,74				0,08		0,019	0,039188	0,006		4E-04	0,002	
11	X8j			1,82		SSj		0,16		0,099		0,025		0,01		
12	Sj	11,8	8,31	13,1	9,51	42,67				0,179				0,032		S
13	nj	7	5	8	6	Xcp						0,039	0,019	0,085	0,048	0,192
14	Xjcp	1,68	1,66	1,64	1,585	1,641										
15	Xjcp-Xcp	0,04	0,02	-0	-0,06											
16	(Xjcp-Xcp)^2	0	0	0	0,003	S1	S2									
17	nj*(Xjcp-Xcp)^2	0,01	0	0	0,019	0,032	0,16									
18						s1^2	s0^2									
19						0,011	0,007									
20	n	p	m1	m2	m											
21	26	4	3	22	25											
22	alfa	F	Fkp													
23	0,05	1,46	3,05													

В результаті розрахунку за формулами отримали $F < F_{kp}$, тобто немає причин відкидати гіпотезу щодо однорідності терміну служби електроламп.

Вихідна інформація інструменту «Описова статистика» для даного прикладу наведена в таблиці 3.

Таблиця 3

Статистична обробка вибірок

1		*2*		*3*		*4*	
Среднее	1,68	Среднее	1,662	Среднее	1,61	Среднее	1,585
Стандартная	0,026095	Стандартная	0,02905	Стандартная	0,03331	Стандартная	0,031278
Медиана	1,68	Медиана	1,64	Медиана	1,62	Медиана	1,565
Мода	#Н/Д	Мода	1,64	Мода	#Н/Д	Мода	#Н/Д
Стандартное	0,069041	Стандартное	0,06496	Стандартное	0,088129	Стандартное	0,076616
Дисперсия в:	0,004767	Дисперсия в	0,00422	Дисперсия в	0,007767	Дисперсия в	0,00587
Эксцесс	0,265861	Эксцесс	-0,4379	Эксцесс	0,881162	Эксцесс	-2,34249
Асимметричн	0,650875	Асимметрич	0,24878	Асимметрич	-0,4234	Асимметрич	0,40824
Интервал	0,2	Интервал	0,17	Интервал	0,28	Интервал	0,17
Минимум	1,6	Минимум	1,58	Минимум	1,46	Минимум	1,51
Максимум	1,8	Максимум	1,75	Максимум	1,74	Максимум	1,68
Сумма	11,76	Сумма	8,31	Сумма	11,27	Сумма	9,51
Счет	7	Счет	5	Счет	7	Счет	6

Вихідна інформація щодо дисперсійного аналізу вибирається з таблиці 3 і зводиться в таблицю 4. Дисперсійний аналіз однорідності вибірок різного обсягу виконується шляхом перевірки однорідності двох вибірок, одна з яких - перша партія ламп. Другою вибіркою послідовно є: друга, третя та четверта партії ламп (таблиця 5).

Таблиця 4

Зведення вихідних даних

	V	W	X	Y
17	партії	дисперсія	середня	обсяг
18	1	0,00476667	1,68	7
19	2	0,00422	1,662	5
20	3	0,00776667	1,61	8
21	4	0,00587	1,585	6

Таблиця 5

Дисперсійний аналіз однорідности вибірок

	V	W	X	Y	Z
23	alfa=	0,05			
24	партії 1-2	F	Fkp	дисперсія	tkp
25		1,129541864	6,16313228	0,004538889	2,22814
26		m1		t	
27		6		0,456290187	
28		m2		m	
29		4		10	
30	партії 1-3	F	Fkp	дисперсія	tkp
31		1,629370629	4,28386571	0,006366667	2,17881
32		m1		t	
33		6		-1,695080656	
34		m2		m	
35		6		12	
36	партії 1-4	F	Fkp	дисперсія	tkp
37		1,231468531	4,38737419	0,005275897	2,20099
38		m1		t	
39		5		-2,350868854	
40		m2		m	
41		6		11	

Порівняння розрахункових значень критеріїв з відповідними критичними значеннями показує, що для всіх поєднань партій ламп $F < F_{kp}$ і $t \le t_{kp}$.

Для доказу достатньо використати F – критерій. Отже, вибірки однорідні і можуть бути об'єднані в одну вибірку обсягом 26 елементів.

Моделювання однорідності парних спостережень

Приклад 2 [10]. Є вибірки, що містять вартість 1 м^2 внутрішньої площі об'єктів нерухомості у місті N за 1998-2000 р. р. Необхідно виконати дисперсійний аналіз із метою перевірки однорідності вибірок.

Вихідні дані та результати дисперсійного аналізу в середовищі ЕТ за формулами наведені в таблиці 6.

Отримано $F < F_{kp}$, тобто аналізовані вибірки однорідні.

Для підтвердження цього розглянемо додатково можливість об'єднання вибірок, отриманих в результаті парних спостережень. Виконаємо дисперсійний аналіз вибірок за 1998 та 1999 роки. Вони мають однаковий обсяг – 26 спостережень.

Зведення дисперсійного аналізу, що отримано за допомогою інструменту «Однофакторний дисперсійний аналіз», представлено у таблиці 7.

В результаті дисперсійного аналізу отримано $F < F_{kp}$, тобто вибірки за 1998 та 1999 роки однорідні.

Покажемо можливість об'єднання вибірок різного обсягу – вибірки за 1999 та 2000 роки. Вихідна інформація інструмента «Описова статистика» наведена в табл. 8.

Таблиця 6

Дисперсійний аналіз однорідності вибірок у середовищі ЕТ

	A	B	C	D	E	F	G	H	I	J	K
1	формування вибірки з вибірок різного розміру										
2		оцінка об'єктів нерухомості									
3	рік оцінки	1998	1999	2000		Xij-Xcp			(Xij-Xcp)^2		
4		75,92	84,352	91,8		-22,6261	-14,1941	-6,74608	511,939	201,472	45,5096
5		117,318	77,844	90,561		18,7719	-20,7021	-7,98508	352,385	428,576	63,7615
6		90,254	84,352	70,053		-8,29208	-14,1941	-28,4931	68,7585	201,472	811,855
7	вартість 1м^2	88,958	149,152	98,368		-9,58808	50,6059	-0,17808	91,9312	2560,96	0,03171
8	внутрішньої	100,743	55,031	109,603		2,19692	-43,5151	11,0569	4,82647	1893,56	122,256
9	площі	86,522	119,997	111,352		-12,0241	21,4509	12,8059	144,578	460,142	163,992
10		76,98	149,152	133,252		-21,5661	50,6059	34,7059	465,096	2560,96	1204,5
11		147,115	87,98	95,366		48,5689	-10,5661	-3,18008	2358,94	111,642	10,1129
12		71,005	135,026	128,222		-27,5411	36,4799	29,6759	758,511	1330,78	880,66
13		114,415	73,594	66,016		15,8689	-24,9521	-32,5301	251,823	622,606	1058,21
14		114,423	88,822	126,799		15,8769	-9,72408	28,2529	252,077	94,5577	798,228
15		95,031	63,649	101,016		-3,51508	-34,8971	2,46992	12,3558	1217,81	6,10052
16		37,7	77,874	89,627		-60,8461	-20,6721	-8,91908	3702,25	427,335	79,5499
17		110,341	72,935	90,033		11,7949	-25,6111	-8,51308	139,12	655,927	72,4725
18		72,379	68,051	98,267		-26,1671	-30,4951	-0,27908	684,716	929,95	0,07788
19		124,033	103,055	165,528		25,4869	4,50892	66,9819	649,583	20,3304	4486,58
20		92,27	109,923	95,301		-6,27608	11,3769	-3,24508	39,3891	129,434	10,5305
21		136,626	110,65	65,948		38,0799	12,1039	-32,5981	1450,08	146,505	1062,63
22		187,005	71,069	115,067		88,4589	-27,4771	16,5209	7824,98	754,99	272,941
23		152,979	79,207	101,137		54,4329	-19,3391	2,59092	2962,94	374	6,71288
24		156,401	92,418	98,454		57,8549	-6,12808	-0,09208	3347,19	37,5533	0,00848
25		43,208	137,198	63,15		-55,3381	38,6519	-35,3961	3062,3	1493,97	1252,88
26		29,336	99,033	80,464		-69,2101	0,48692	-18,0821	4790,03	0,23709	326,962
27		35,483	99,148	154,443		-63,0631	0,60192	55,8969	3976,95	0,36231	3124,47
28		52,771	141,003	82,74		-45,7751	42,4569	-15,8061	2095,36	1802,59	249,832
29		49,176	113,967	73,919		-49,3701	15,4209	-24,6271	2437,4	237,805	606,493
30				107,458				8,91192			79,4224
31				83,558				-14,9881			224,642
32				126,977				28,4309			808,317
33				88,272				-10,2741			105,557

Продовження табл. 6

34				115,554				17,0079			289,269	
35				107,558				9,01192			81,2148	
36				110,997				12,4509			155,025	
37				79,999				-18,5471			343,994	
38				111,731				13,1849			173,842	
39				70,165				-28,3811			805,486	
40				104,15				5,60392			31,404	
41				187,315				88,7689			7879,92	
42				135,36	SSj			36,8139			1355,26	S
43	Sj	2458,39	2544,48	4025,58	9028,45				42435,5	18695,5	29050,7	90181,8
44	nj	26	26	39	Xc						s^2=	1002,02
45	Xcpj	94,5535	97,8647	103,22	98,5461							
46	Xcpj-Xcp	-3,99254	-0,68138	4,67392								
47	(Xcpj-Xcp)^2	15,9404	0,46428	21,8456	S1							
48	nj*(Xcpj-Xcp)^2	414,449	12,0714	851,977	1278,5							
49				s1^2	639,249							
50				S2	s0^2							
51				88903,3	1010,26							
52	n	p	m1	m2	m							
53	91	3	2	88	90							
54	alfa	F	Fkp									
55	0.05	0.63275	3.10007									

Результати статистичної обробки вибірок показують, що вартість 1 м^2 внутрішньої площі об'єктів нерухомості підпорядковується нормальному закону розподілу, оскільки середнє значення, мода та медіана мають один порядок, а значення ексцесу та асиметричності близькі до нуля.

Таблиця 7

Дисперсійний аналіз однорідности вибірок

Однофакторный дисперсионный анализ						
ИТОГИ						
Группы	*Счет*	*Сумма*	*Среднее*	*Дисперсия*		
1998	26	2458,392	94,5535385	1680,84294		
1999	26	2544,482	97,8646923	747,3383157		
Дисперсионный анализ						
Источник вариации	*SS*	*df*	*MS*	*F*	*P-Значение*	*F критическое*
Между группами	142,529	1	142,528617	0,117395369	0,733313031	4,034309546
Внутри групп	60704,5	50	1214,09063			
Итого	60847,1	51				

Таблиця 8

Статистична обробка вибірок

	M	N	O	P	Q	R
21	1998		1999		2000	
22	Среднее	94,5535	Среднее	97,8646923	Среднее	103,22
23	Стандартная ошибка	8,04039	Стандартная ошибка	5,36132273	Стандартная ошибка	4,362050996
24	Медиана	91,262	Медиана	90,62	Медиана	98,454
25	Мода	#Н/Д	Мода	84,352	Мода	#Н/Д
26	Стандартное отклонение	40,9981	Стандартное отклон	27,3374892	Стандартное отклон	27,24099974
27	Дисперсия выборки	1680,84	Дисперсия выборки	747,338316	Дисперсия выборки	742,0720669
28	Эксцесс	-0,38574	Эксцесс	-0,7318968	Эксцесс	1,535417751
29	Асимметричность	0,31284	Асимметричность	0,54675199	Асимметричность	1,043068369
30	Интервал	157,669	Интервал	94,121	Интервал	124,165
31	Минимум	29,336	Минимум	55,031	Минимум	63,15
32	Максимум	187,005	Максимум	149,152	Максимум	187,315
33	Сумма	2458,39	Сумма	2544,482	Сумма	4025,58
34	Счет	26	Счет	26	Счет	39

У таблиці 9 виконано дисперсійний аналіз вибірок різного обсягу. Обчислено розрахункові та критичні значення F - критерію Фішера та t - статистики Стьюдента за 1999 та 2000 р.р.

Таблиця 9

Дисперсійний аналіз вибірок різного обсягу

	M	N	O	P	Q	R
40	дисперсія		alfa		Fkp	F
41	744,1785664		0,05		1,798312276	1,007096681
42	t	tkp	m1	m2	m	
43	0,775368492	1,99834	25	38	63	

У результаті дисперсійного аналізу однорідності вибірок за 1999 та 2000 роки встановлено, що $F < F_{kp}$. Отже, ці вибірки однорідні.

Аналіз дисперсійного аналізу, що наведено у таблиці 6, показує однорідність трьох вибірок різного обсягу. Тобто можна спростити процедуру проведення дисперсійного аналізу даних спостережень, якщо використовувати інструмент «Описова статистика» пакету аналізу.

Алгоритм методики дисперсійного аналізу з використанням инструментів пакету аналізу Excel

Допустимо є кілька вибірок різного обсягу, серед яких є дві вибірки рівного обсягу.

1. Зробити розміщення інформації на робочому аркуші ЕТ в такий спосіб, щоб вибірки рівного обсягу перебували на початку таблиці (табл. 6).

2. Перевірити однорідність цих вибірок за допомогою інструмента «Однофакторний дисперсійний аналіз».

3. Виконати статистичну обробку всіх вибірок, використовуючи інструмент «Описова статистика» (табл. 8).

4. За підсумками аналізу числових характеристик досліджуваної ознаки перевірити її підпорядкування нормальному закону розподілу.

5. Скласти таблицю вихідних даних щодо дисперсійного аналізу вибірок різного обсягу, у якій першої вибіркою буде остання з вибірок рівного обсягу. Вона вважається базовою і з нею порівнюються інші вибірки різного обсягу (табл. 4).

6. Виконати дисперсійний аналіз однорідності вибірок різного обсягу (табл. 5). Для цього достатньо визначити розрахункове та критичне значення F – критерію Фішера та переконатися в тому, що всі вибірки належать єдиній генеральній сукупності.

Висновки

1. Вихідна інформація інструменту «Однофакторний дисперсійний аналіз» пакету аналізу містить розрахункове та критичне значення F – критерію Фішера, що дозволяє легко перевірити однорідність вибірок рівного обсягу.

2. Інструмент «Описова статистика» пакету аналізу виконує статистичну обробку багатовимірних вибірок різного обсягу та видає значення 13 параметрів, у тому числі: середнє значення, мода, медіана, ексцес, асиметричність, дисперсія та обсяг вибірки. За цією інформацією легко визначити розрахункове та критичне значення статистик. Критичні значення критеріїв визначаються за допомогою статистичних функцій майстра функцій.

3. Розроблено методику проведення дисперсійного аналізу однорідності вибірок різного обсягу за допомогою інструменту «Описова статистика» пакету аналізу, що значно спрощує процедуру формування вибірки.

Список літератури

1. Вознесенский В. А., Ляшенко Т. В., Огарков Б. Л. Численные методы решения строительно-технологических задач на ЭВМ. К.: Выща школа, 1989. 328 с.
2. Гарькина И. А., Данилов А. М., Прошин А. П., Бормотов А. Н. Применение математических методов в строительном материаловедении. Пенза: ПГАСА, 1999. 204 с.
3. Гарькина И. А., Данилов А. М., Прошин А. П. Математические методы синтеза строительных материалов. Пенза: ПГАСА, 2001. 106 с.
4. Дворкин Л. И., Шамбан И. Б. Проектирование составов бетона с применением математического моделирования. К.: УМК ВО, 1992. 44 с.
5. Ершова Н. М., Деревянко В. Н., Тимченко Р. А., Шаповалова О. В. Обработка данных средствами Excel при планировании эксперимента: учеб. пособие для вузов Д.: ПГАСА, 2012. 350 с.
6. Ершова Н. М. Дисперсионный анализ данных наблюдений. Днепропетровск: ПГАСА, 2010. 80 с.
7. Красовский П. С. Исследование и оптимизация свойств строительных материалов с применением элементов математической статистики: Учебное пособие. Хабаровск: ДВГУПС, 2004. 128 с.
8. Митропольский А. К. Техника статистических вычислений. М.: Главная редакция физико-математической литературы издательства «Наука», 1971.576 с.
9. Пінчук С. Й. Організація експерименту при моделюванні та оптимізації технічних систем: навч. посібник для студ. ВНЗ. Д.: Дніпро-VAL, 2009.289с.
10. Сивец С. А. Статистические методы в оценке недвижимости и бизнеса. Учебно-практическое пособие по статистике для оценщиков. Запорожье, 2001. 320 с.

INFORMATION TECHNOLOGIES FOR DECISION-MAKING IN FORMATION UNIFORM DATABASE OF ANALOGUE OBJECTS OF THE RESEARCHED OBJECT

N. M. Yershova

Prydniprovska State Academy of Civil Engineering and Architecture, 24-a, Chernyshevskyi St., Dnipro, 49600, Ukraine, E-mail:nersova107@gmail.com

The experiment occupies a special place among the ways of obtaining information about the internal interconnections of phenomena in nature and technology. According to the increasing complexity of the processes and phenomena under research, the expense of equipment and the experiment increase. A large amount of experimental data is collected during the tests and requires processing and analysis. At the same time, the duration of analysis, comprehension of the test results and their consideration in order to adjust the new products' characteristics is significant. It is very important to select methods and means of processing experimental data during conducting an observation or experiment. Since 2001, many publications proved the effectiveness of the Excel analysis tool package for the experimental data processing. Despite this, in the observational and experimental data processing, the calculation of values for the equality of variances criteria and averages under formulas is still used in scientific and educational literature, and to select their critical values in the tables. Another problem is the sample formation of different sample sizes under direct calculation using formulas, even in Excel. This article proposes a variance analysis methodology of homogeneity for samples of different sizes, using the "Descriptive statistics" tool of the Excel analysis tool package. The "Descriptive Statistics" tool performs statistical processing of multivariate samples of various sizes and outputs the values of 13 parameters, including: mean, mode, median, kurtosis, asymmetry, variance, and sample size. Based on this information, it is easy to determine the estimated and critical value of statistics. The critical value of the criteria is determined using the statistical functions of the function wizard. The initial information of the "Univariate analysis of variance" tool contains the calculated and critical value - Fisher's test, which allows you to easily check the homogeneity of samples of equal volume. The technique significantly simplifies the procedure of forming a single database of objects-analogues of the object under study.

Keywords: experiment, data processing, variance analysis, sample formation, samples of different sizes, Excel analysis package.

DOI 10.15276/imms.v12.no3.193
УДК 621.391

Informatics and Mathematical Methods in Simulation
Vol. 12 (2022), No. 3, pp. 193-201

РОЗРАХУНОК ЦИФРОВИХ ФІЛЬТРІВ В СЕРЕДОВИЩІ MATLAB

С. О. Клімович, В. В. Кузавков

Військовий інститут телекомунікацій та інформатизації імені Героїв Крут
м. Київ, Україна; e-mails: robota_ks@ukr.net, nevse@ukr.net

Цифрові фільтри застосовуються в системах цифрової обробки сигналів (ЦОС) для вирішення двох основних задач: розділення (двох і більше сигналів) та відновлення сигналів, які були спотворені. Задача відновлення сигналів вирішується у тих випадках, коли первинний сигнал реєструється у спотвореному вигляді. Такі задачі можуть вирішуватись програмними та апаратними методами. В системах радіозв'язку при передачі (прийманні) інформації, первинний сигнал, який реєструється від джерела, окрім коливань, які обумовлені інформаційною складовою, буде вміщувати складові обумовлені іншими фізичними процесами. Фільтр повинен забезпечувати таке розділення корисного сигналу і завади, після котрого відбудеться безпомилкове приймання переданої інформації та (або) визначення параметрів завади (навмисного або природнього походження).

Якщо відома імпульсна характеристика системи, можливо вирахувати її реакцію на сигнал довільної форми. Для цього вхідний сигнал представляється у вигляді сукупності імпульсних сигналів з одиничним нульовим відліком, кожний з яких може розглядатися як одиничний імпульс помножений на деяку величину зсунуту по часу. Реакція системи на кожний вхідний імпульс отримується шляхом підсилення та зсуву імпульсної характеристики системи. Сигнали складної форми розкладаються на прості складові за допомогою імпульсної декомпозиції. В наслідок чого загальна реакція системи на вхідний сигнал обраховується шляхом додавання реакцій системи на усі компоненти декомпозиції окремо.

В статті, на основі білінійного z-перетворення, проведено аналіз електричних фільтрів які можливо застосовувати в цифрових засобах зв'язку спеціального призначення.

Метою дослідження є створення програмної складової, яка б забезпечила можливість автоматичного розрахунку параметрів з метою побудови ЦФ з певними параметрами. Хід виконання розрахунку наведено у вигляді опорного алгоритму з низкою вхідних даних та обмежень. Основні характеристики цифрового фільтра (характеристика загасання та фазова характеристика) визначаються та візуалізуються в програмному середовищі Matlab через створену програмну складову розрахунку ЦФ.

Ключові слова: нормована частота, коефіцієнт пропорційності, z-перетворення, функція Золотарьова – Кауєра, Чебишева, Батерворта.

Вступ

Для вирішення поставлених задач обробки сигналів можливо використовувати аналогові фільтри, проте цифрові фільтри дозволяють досягнути високої точності, а також характеристик які значно перевищують аналогові пристрої [1]. Реалізація аналогових фільтрів, як правило, найбільш вигідна з фінансової точки зору. Також ці фільтри мають більш високу швидкодію та більш широкий динамічний діапазон по амплітуді та частоті. В свою чергу цифрові фільтри перевершують аналогові за точністю відтворення частотних характеристик. У зв'язку з цим значно відрізняються підходи до розрахунку і проектування аналогових та цифрових фільтрів. Для аналогових фільтрів важливо врахувати обмеження, обумовлені елементною базою, такі як стабільність та точність параметрів пасивних компонентів схеми. Цифрові фільтри, як правило, дозволяють досягнути заданої точності, тому першочерговим значенням

отримують проблеми пов’язані з обмеженістю динамічного діапазону. Розрахунки фільтрів зручно проводити в спеціалізованих математичних програмах, однією з яких є Matlab, котра вже має набір відповідних функцій та значно полегшує обрахунки.

Огляд літератури

Аналіз останніх публікацій свідчить, що розрахунок (проектування) цифрових та аналогових фільтрів на етапі апроксимації є процесом знаходження передаточної функції. В літературі [2–6] розглядається метод розкладання апроксимуючої функції в ряд Фур’є, а також знаходження передаточної функції за відомими часовими характеристиками, де не наведено програмований метод розрахунку. В літературі [7–10] зазначено такі методи апроксимації для рекурсивних ЦФ: узгодженого z-перетворення; білінійного перетворення; інваріантності імпульсної характеристики, при цьому не наведена програма розрахунку ЦФ. В літературі [11] не наведено програмної складової розрахунку білінійного z-перетворення ЦФ з деталізованим відображенням практичної реалізації. Варто зазначити, що розрахунки ЦФ з використанням білінійного z-перетворення є громіздкими та потребують значного часу, при цьому автоматизація (створення програмної складової) розрахунку ЦФ з використанням білінійного z-перетворення має складний характер побудови та розглянута не в повному обсязі.

Виклад основного матеріалу

Найважливішим поняттям для цифрової обробки сигналів та цифрових фільтрів є дельта-функція $\delta(t)$ або функція Дірака, котра представляє собою нескінченно вузький імпульс з безкінечною амплітудою, розташованою при нульовому значенні аргументу функції [1]. При цьому площа імпульсу рівна одиниці. Дельта-функцію неможливо реалізувати фізично, однак вона дуже важлива для теоретичного аналізу сигналів та систем. Для дискретних систем використовується поняття дискретної дельта-функції $\delta(n)$. Вона називається одиничним імпульсом або одиничним відліком, представляючи собою сигнал в котрому нульовий відлік має значення одиниці, а всі інші рівні нулю.

Наступним важливим поняттям є імпульсна характеристика системи $h[n]$, яка представляє собою реакцію системи на одиничний імпульс. Якщо дві системи мають будь-які різності то їх імпульсні характеристики будуть різнитися. Сигнали складної форми можливо розкласти на прості складові за допомогою імпульсної декомпозиції. Імпульсний сигнал котрий являється компонентом розкладання при імпульсній декомпозиції може бути представлений як одиничний імпульс зсунутий на відповідну величину по часовій вісі та помножений на значення відліку вихідного сигналу в цей самий момент часу. Таким чином, якщо відома імпульсна характеристика системи, можливо вирахувати реакцію системи на сигнал довільної форми. Для цього вхідний сигнал шляхом декомпозиції представляється у вигляді сукупності імпульсних сигналів з одиничним нульовим відліком, кожний з яких може розглядатися як одиничний імпульс помножений на деяку величину зсунуту по часу. Реакція системи на кожний вхідний імпульс отримується шляхом відповідного підсилення та зсуву імпульсної характеристики системи. В результаті чого загальна реакція системи на вхідний сигнал обраховується шляхом додавання реакцій системи на усі компоненти декомпозиції окремо. Обрахунок вихідного сигналу за вхідним сигналом та імпульсною характеристикою виконується за допомогою операції згортки $(*)$. Для обрахунку вихідного сигналу $y(n)$ необхідно визначити згортку відповідно до виразу (1):

$$y[n] = x[n] \times h[n], \tag{1}$$

де: $x[n]$ – вхідний сигнал; $h[n]$ – імпульсна характеристика.

Графічний приклад обрахунку згортки для фільтра нижніх частот представлений на рисунку 1.

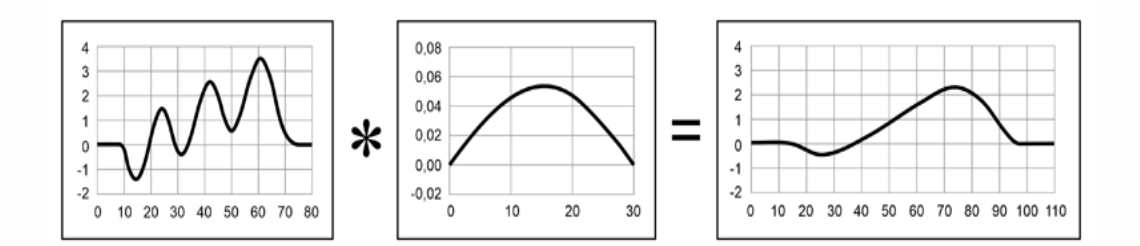


Рис. 1. Згортка для фільтру нижніх частот. Згортка будь-якого сигналу з одиничним імпульсом відповідає самому сигналу: $x[n]\times\delta[n]=x[n]$.

Якщо змінити одиничний імпульс помноживши його на постійний множник отримаємо систему котра працює в якості підсилювача або атенюатора в залежності від величини множника. Таким чином, властивість згортки дозволяє проектувати цифрові фільтри з широким набором властивостей.

Цифрові фільтри поділяються на два види – фільтри з кінцевою імпульсною характеристикою (КІХ) або нерекурсивні та фільтри з нескінченною імпульсною характеристикою (НІХ) або рекурсивні [1].

Приклад структури КІХ-фільтру наведено на рисунку 2.

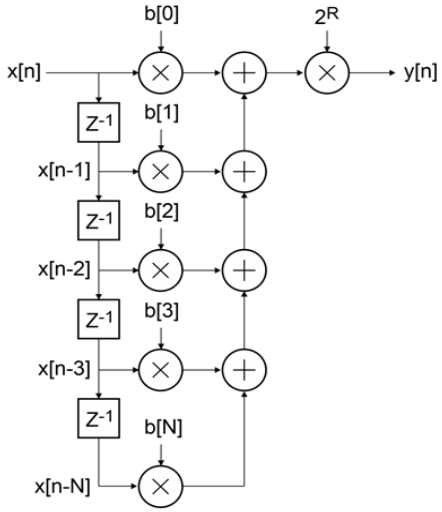


Рис. 2. Структура КІХ фільтру

Робота КІХ-фільтру описується виразом:

$$y(n)=b_0x(n)+b_1x(n-1)+...+b_px(n-p)\,. \qquad (2)$$

Вираз (2) відображає згортку вхідного сигналу з набором коефіцієнтів фільтра.

КІХ-фільтри мають високу стійкість та дозволяють отримувати довільні амплітудно-частотну характеристику та фазо-частотну характеристику. Проте вони споживають більше обчислювальних ресурсів в порівнянні з НІХ – фільтрами та мають більші часові затримки.

Приклад структури НІХ-фільтру наведено на рисунку 3, а його функціонування описується виразом:

$$y(n)=b_0x(n)+b_1x(n-1)+...+b_px(n-p)-a_1y(n-1)-a_2y(n-2)-...-a_qy(n-q).$$

НІХ-фільтри мають наступні переваги: висока швидкодія та низька собівартість в порівнянні з КІХ-фільтрами, наявність аналогових прототипів.

Недоліками є те, що амплітудно-частотну характеристику (АЧХ) необхідно вибирати з існуючих реальних фільтрів-прототипів.

Розглянемо приклад проектування КІХ-фільтру з використанням віконної функції Хеммінга (3).

На першому етапі визначаємось з ідеальною АЧХ фільтру.

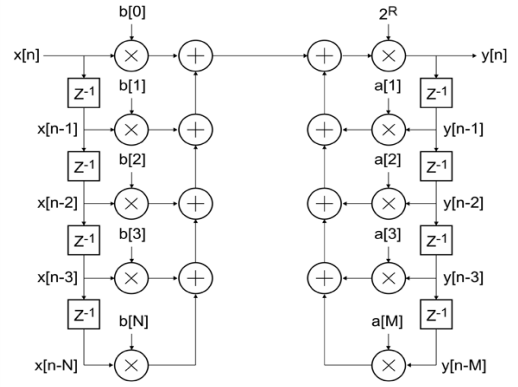


Рис. 3. Структура НІХ-фільтра

АЧХ ідеального фільтру має коефіцієнт передачі рівний нулю в смузі завади та одиниці в смузі пропускання корисного сигналу. Відповідно до частоти дискретизації формула АЧХ виглядає наступнім чином:

$$D_p(f) = \begin{cases} 1, & 0 \le f \le f_{\text{с.п.}}, \\ 0, & f_{\text{с.з.}} \le f \le \dfrac{f_{\text{д}}}{2}, \end{cases}$$

де: $f_{\text{с.п.}}$ – гранична частота смуги пропускання; $f_{\text{с.з.}}$ – гранична частота смуги затримки; $f_{\text{д}}$ – частота дискретизації.

Використовуємо віконну функцію Хеммінга:

$$\omega_k = \begin{cases} 0{,}54 - 0{,}46 \cdot \cos\left(\dfrac{2\pi k}{N-1}\right), & 0 \le k \le N-1, \\ 0, & k < 0, \quad k > N-1, \end{cases} \tag{3}$$

де: N – число коефіцієнтів фільтра.

КІХ-фільтр може бути заданий коефіцієнтами імпульсної характеристики {h(n)}. Коефіцієнти нерекурсивного фільтру відповідають відлікам імпульсної характеристики кола.

Для обрахунку коефіцієнтів імпульсної характеристики необхідно обрахувати зворотне дискретне перетворення Фур'є:

$$h(n) = \frac{1}{N} \sum_{k=0}^{N-1} H(k) \cdot e^{\frac{j2\pi nk}{N}}.$$

При цьому відбувається множення кожного відліку вихідної імпульсної функції на відлік віконної функції з тим самим порядковим номером (k):

$$h_{\omega k} = h_k \cdot \omega_k. \tag{4}$$

У відповідності до (4) отримуємо набір коефіцієнтів для проектування КІХ-фільтру. Для побудови реальної АЧХ фільтру здійснюється пряме дискретне перетворення Фур'є.

Здійснення розрахунків параметрів фільтру за наведеним прикладом із застосуванням програмного середовища Matlab ускладнено. Тому розглянемо інший варіант обчислення параметрів фільтру на основі z-перетворення:

$$z = e^{pT}; \; z^{-1} = e^{-pT}.$$

Розрахунок ЦФ базується на використанні передаточної функції відповідного фільтра-прототипа нижніх частот. Період дискретизації (T) обирається відповідно до теореми відліків (теорема Котельникова) [4]:

$$T = \frac{1}{2 f_{max}},$$

де f_{max} – максимальна частота у спектрі сигналу, який передається.

Метою дослідження є створення програмної складової, яка б забезпечила можливість автоматичного розрахунку параметрів з метою побудови ЦФ з певними параметрами.

Для пояснення програмної складової та ходу виконання процесів розрахунку в роботі наводяться основні етапи опорного алгоритму (рис.6):

введення початкових даних;

знаходження коефіцієнта пропорційності;

знаходження нормованої частоти затримки аналогового ФНЧ-прототипу і порядку фільтра;

отримання знаменника нормованої передаточної функції аналогового ФНЧ-прототипу;

знаходження передаточної функції ЦФ з використанням білінійного z-перетворення.

Для функціонування програмної складової потрібні наступні вхідні дані: $\omega_{\text{п}}$ – гранична частота смуги пропускання, $\omega_{\text{з}}$ – гранична частота смуги затримки, T – період дискретизації, Δa – нерівномірність загасання в смузі пропускання, a_0 – загасання в смузі затримки, вид апроксимації.

До обмежень відносимо відповідність отриманого порядку фільтра:

$$n_{\min} \geq n_{\text{пот}} \geq n_{\max} \qquad (5)$$

Розв’язання задачі розрахунку ЦФ на основі Matlab розділено на етапи:

1. Розрахунок коефіцієнта пропорційності:

$$K = \operatorname{ctg} \frac{\omega_{\text{п}} \cdot T}{2}.$$

2. Розрахунок нормованої частоти затримки аналогового ФНЧ-прототипу:

$$\Omega_{\text{з}} = K \operatorname{tg} \frac{\omega_{\text{з}} \cdot T}{2}.$$

3. Розрахунок порядку фільтра (при використанні функції Батерворта):

$$n \geq \frac{\lg \dfrac{10^{0,1 a_0} - 1}{10^{0,1 \Delta a} - 1}}{2 \lg \Omega_{\text{з}}}.$$

4. Перевірка виконання умови (5). При виконанні зазначеної умови відбувається перехід до блоку 5 алгоритму. В іншому випадку – до блоку 8 алгоритму.

5. Розрахунок знаменника нормованої передаточної функції аналогового ФНЧ-прототипу $H(\lambda)$ (коефіцієнти якої знаходять в таблицях за відомими: загасанням, порядком фільтра та видом апроксимації):

$$H(\lambda) = C(\lambda - \alpha_1)(\lambda^2 - 2\alpha_1 \lambda + \nu_2), \; \nu_2 = \alpha_2{}^2 + \beta_2{}^2; \; \lambda = \frac{j\omega}{\omega_{\text{п}}}.$$

де C – коефіцієнт з довідника [12].

6. Розрахунок передаточної функції ЦФ низьких частот з використанням білінійного z-перетворення $k\dfrac{1-z^{-1}}{1+z^{-1}}$:

$$K(\lambda)=\frac{1}{H(\lambda)}. \tag{6}$$

7. Розрахунок характеристики загасання (рис. 4) та фазової характеристики (рис. 5).

Визначення характеристики загасання ФНЧ:

$$a(\Omega)=20\lg C+10\lg[(\Omega^2+\alpha_1{}^2)^2]+10\lg\cdot[\alpha_2{}^2+(\Omega-\beta_2)^2]+10\lg[\alpha_2{}^2+(\Omega+\beta_2)^2]$$

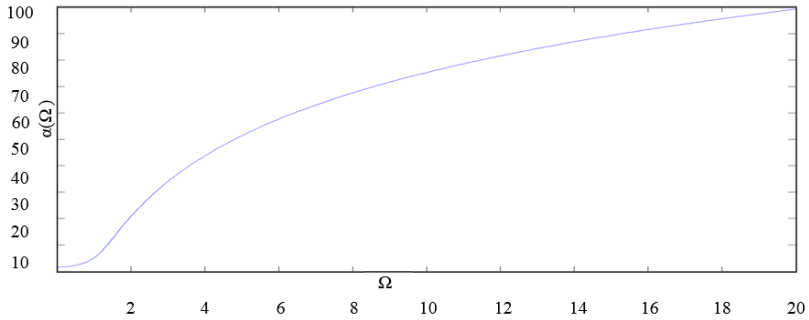


Рис. 4. Графік загасання ФНЧ

Визначення фазової характеристики ФНЧ:

$$\beta(\Omega)=\sum_{\nu=1}^{n_1}arctg\frac{\Omega}{(-a_\nu)}+\sum_{\nu=n_1+1}^{n_2}[arctg\frac{\Omega-\beta_\nu}{(-a_\nu)}+arctg\frac{\Omega+\beta_\nu}{(-a_\nu)}].$$

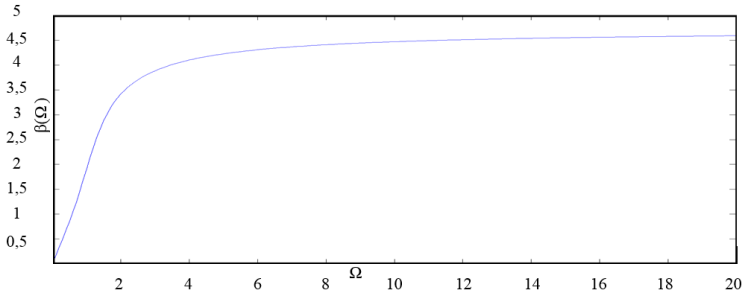


Рис. 5. Графік фазової характеристики ФНЧ

Відповідно до отриманих z-показників та виразу (6) можливо здійснити проектування ЦФ в пакеті Simulink, що являє собою блокове моделювання без використання мови Matlab, що дозволяє відстежити процес обробки даних в часі. Simulink надає можливість побудувати графічні блок-діаграми та дослідити працездатність ЦФ. За рахунок того, що складову Simulink інтегровано в Matlab, результати розрахунку програмної складової ЦФ, які проводилися вище, використаємо для отримання вихідних показників фільтра.

На рис. 6 побудована структурна схема ЦФ.

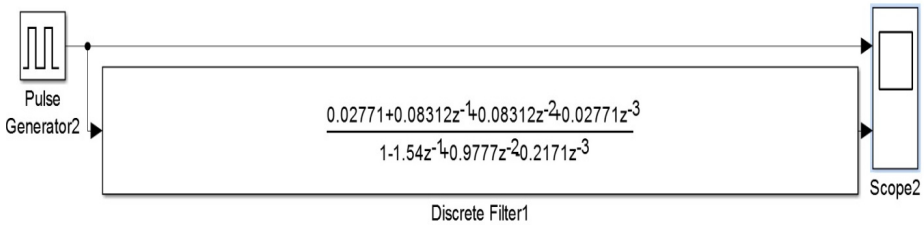
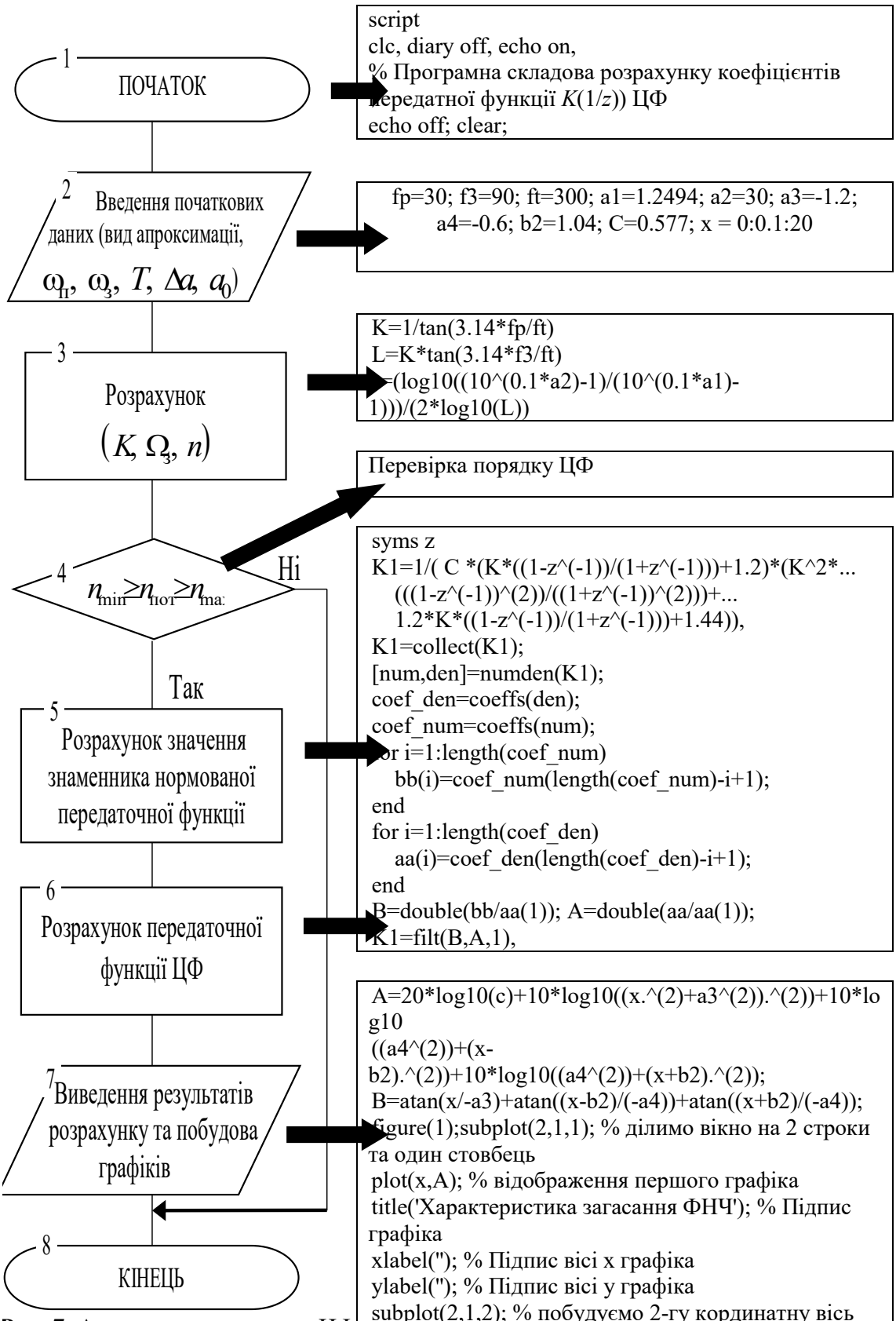


Рис. 6. Структурна схема з Discrete Filter

Етапи та програмна складова розрахунку коефіцієнтів ЦФ відповідно до алгоритму представлена на рис. 7.




```
script
clc, diary off, echo on,
% Програмна складова розрахунку коефіцієнтів
передатної функції K(1/z)) ЦФ
echo off; clear;
```

```
fp=30; f3=90; ft=300; a1=1.2494; a2=30; a3=-1.2;
a4=-0.6; b2=1.04; C=0.577; x = 0:0.1:20
```

```
K=1/tan(3.14*fp/ft)
L=K*tan(3.14*f3/ft)
=(log10((10^(0.1*a2)-1)/(10^(0.1*a1)-
1)))/(2*log10(L))
```

Перевірка порядку ЦФ

```
syms z
K1=1/( C *(K*((1-z^(-1))/(1+z^(-1)))+1.2)*(K^2*...
   (((1-z^(-1))^(2))/((1+z^(-1))^(2)))+...
   1.2*K*((1-z^(-1))/(1+z^(-1)))+1.44)),
K1=collect(K1);
[num,den]=numden(K1);
coef_den=coeffs(den);
coef_num=coeffs(num);
or i=1:length(coef_num)
   bb(i)=coef_num(length(coef_num)-i+1);
end
for i=1:length(coef_den)
   aa(i)=coef_den(length(coef_den)-i+1);
end
B=double(bb/aa(1)); A=double(aa/aa(1));
K1=filt(B,A,1),
```

```
A=20*log10(c)+10*log10((x.^(2)+a3^(2)).^(2))+10*lo
g10
((a4^(2))+(x-
b2).^(2))+10*log10((a4^(2))+(x+b2).^(2));
B=atan(x/-a3)+atan((x-b2)/(-a4))+atan((x+b2)/(-a4));
igure(1);subplot(2,1,1); % ділимо вікно на 2 строки
та один стовбець
plot(x,A); % відображення першого графіка
title('Характеристика загасання ФНЧ'); % Підпис
графіка
xlabel(''); % Підпис вісі x графіка
ylabel(''); % Підпис вісі y графіка
subplot(2,1,2); % побудуємо 2-гу кординатну вісь
plot(x,B); % відображення 2-го графіка в нових
вісях
title('Фазова характеристика ФНЧ');% Підпис
графіка
xlabel(''); % Підпис вісі x графіка
ylabel(''); % Підпис вісі y графіка
```

Рис. 7. Алгоритм розрахунку ЦФ в програмному середовищі Matlab

На рис. 8 відображено властивості блоку ЦФ відповідно до отриманих показників програмної складової.

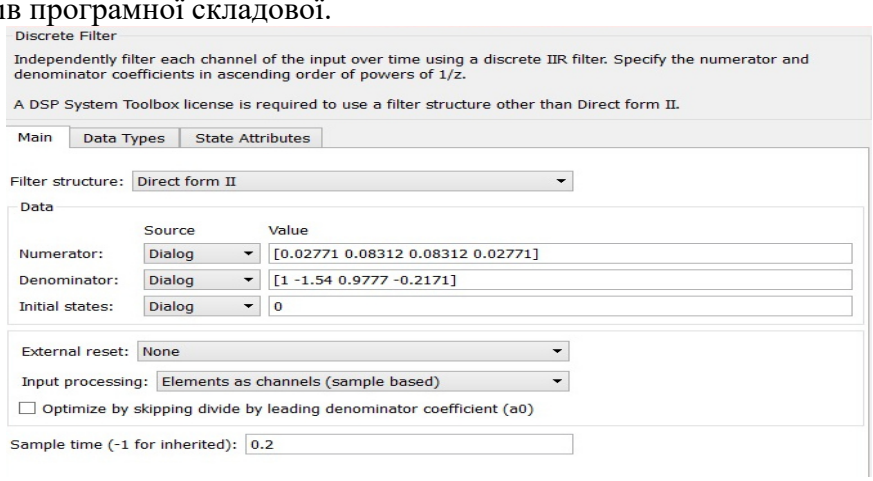


Рис. 8. Властивості блоку Discrete Filter

Перевірку фільтруючої дії ЦФ НЧ продемонструємо при подачі на вхід ЦФ послідовності прямокутних відеоімпульсів.

Отримані сигнали, що надходять на осцилограф (Scope2) з генератору (Pulse Generator2) та ЦФ (Discrete Filter1), зображені на рис. 9.

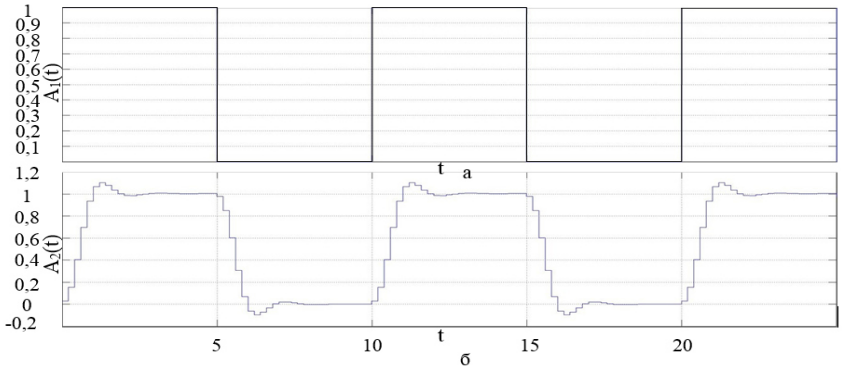


Рис. 9. Результат роботи ЦФ на Scope2

Візуалізація результатів обчислень на основі z-перетворення та алгоритму наведеного на рисунку 6 доводить працездатність запропонованого програмного модуля синтезу ЦФ. Сигнал, отриманий (рис.9,б) відповідає фільтру з “широкою” смугою пропускання (сигнал рис.9,а відповідає ідеальному фільтру з нескінченною смугою).

Висновки

Представлена програмна складова розрахунку ЦФ з використанням Matlab дозволяє визначити основні параметри ЦФ, а саме: коефіцієнт пропорційності; нормовану частоту затримки аналогового ФНЧ-прототипу та порядок фільтру; знаменник нормованої функції аналогового ФНЧ-прототипу та передаточну функцію ЦФ; зменшити час розрахунків та полегшити побудову характеристики загасання та фазової характеристики ЦФ; отримати схему ФНЧ 3-го порядку з можливістю формування збільшеного порядку шляхом нарощування елементів схеми.

Реалізація програмної складової в пакеті Simulink дозволяє здійснити процес компіляції створеного проекту і зменшити витрату часу на проектування ЦФ.

Запропонований підхід для визначення необхідних характеристик (параметрів) фільтрів може бути застосований для фільтрів Батерворта, Чебишева, Золотарьова – Кауера, смугових фільтрів.

Подальшим напрямком досліджень є вирішення задачі реалізації отриманої програмної складової з використанням цифрових сигнальних процесорів.

Список літератури

1. Філатова Г. Є. Проектування цифрових фільтрів. Х.: НТУ «ХПІ», 2017. 120 с.
2. Белодедов М. В. Методы проектирования цифровых фильтров. Волгоград: Издательство Волгоградского государственного университета, 2004. 64 с.
3. Солонина А. И., Арбузов С. М. Цифровая обработка сигналов. Моделирование в MATLAB. СПб.: БХВ-Петербург, 2008. 816 с.
4. Белецкий А.Ф. Теория линейных электрических цепей. М.: Радио и связь, 1986. 544с.
5. Оппенгейм А., Шафер Р. Цифровая обработка сигналов. М., 2006. 856 с.
6. Бойко В. С. Теоритичні основи електротехніки. К., 2004. 268 с.
7. Сериков С. А., Бороденко Ю. Н., Дзюбенко А. А. Методы преобразования и обработки сигналов. Синтез цифровых фильтров. Х., 2008. 60 с.
8. Сергиенко А. Б. Цифровая обработка сигналов : учебник. СПб.: Питер, 2002. 608 с.
9. Баскаков С. И. Радиотехнические цепи и сигналы. М.: Высш. шк., 2003. 462 с.
10. Антонью А. Цифровые фильтры: анализ и проектирование. М.: Радио и связь, 1983. 320 с.
11. Клімович С. О., Мотора Є. М., Боголій С. М. Методика розрахунку цифрових фільтрів на основі MATLAB. *Збірники наукових праць ВІТІ*. 2017. № 4. С. 45-49.
12. Зааль Р. Справочник по расчету фильтров. М.: Радио и связь, 1988. 752 с.

DESIGN OF DIGITAL FILTERS IN THE MATLAB ENVIRONMENT

S. Klimovych, V. Kuzavkov

Military Institute of Telecommunication and Information technologies named after the Heroes of Kruty, Kyiv, Ukraine; e-mails: robota_ks@ukr.net, nevse@ukr.net

Digital filters are used in digital signal processing (DSP) systems to solve two main problems: separation (of two or more signals) and restoration of signals that have been distorted. The task of restoring signals is solved in those cases when the primary signal is registered in a distorted form. Such tasks can be solved by software and hardware methods. In radio communication systems, when transmitting (receiving) information, the primary signal that is registered from the source, in addition to oscillations caused by the information component, will contain components caused by other physical processes. The filter must provide such a separation of the useful signal and the interference, after which the transmitted information will be received without error and (or) the parameters of the interference (intentional or natural origin) will be determined. If the impulse characteristic of the system is known, it is possible to calculate its response to a signal of arbitrary shape. For this, the input signal is represented as a set of pulse signals with a single zero count, each of which can be considered as a single pulse multiplied by some time-shifted value. The response of the system to each input pulse is obtained by amplifying and shifting the impulse response of the system. Signals of complex form are decomposed into simple components using impulse decomposition. As a result, the overall response of the system to the input signal is calculated by adding the responses of the system to all components of the decomposition separately. In the article, on the basis of the bilinear z-transformation, an analysis of electrical filters that can be used in digital means of special purpose communication is carried out. The purpose of the research is to create a software component that would provide the possibility of automatic calculation of parameters in order to build a CF with certain parameters. The progress of the calculation is given in the form of a reference algorithm with a number of input data and restrictions. The main characteristics of the digital filter (attenuation characteristic and phase characteristic) are determined and visualized in the Matlab software environment through the created software component for calculating the digital filter.

Keywords: normalized frequency, proportionality coefficient, z-transformation, Zolotaryov-Kauer, Chebyshev, Butterworth function.

DOI 10.15276/imms.v12.no3.202
УДК 004.4

Informatics and Mathematical Methods in Simulation
Vol. 12 (2022), No. 3, pp. 202-208

РОЗРОБКА МЕСЕНДЖЕРА ДЛЯ ПРИХОВАНОЇ ПЕРЕДАЧІ ПОВІДОМЛЕНЬ

А.В. Павлюк, Н.І. Кушніренко, О.В. Троянський

Національний університет «Одеська Політехніка», просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: infsec2011@gmail.com

Інформація є одним з найцінніших предметів сучасного життя. Одержання доступу до неї з появою глобальних комп'ютерних мереж стало неймовірно простим. У той же час легкість і швидкість такого доступу значно підвищили і загрозу порушення безпеки даних при відсутності засобів щодо їх захисту. Актуальність теми полягає у тому, що в сьогоднішніх реаліях месенджери є невід'ємною частиною життя майже кожної людини на світі, тому безпека особистої інформації має високий пріоритет. Метою роботи є розробка методу приховування повідомлень в наборі послідовних зображень, його програмна реалізація та використання в месенджері. Для досягнення визначеної мети роботі були сформовані наступні задачі: аналіз існуючих популярних месенджерів та їх методів захисту інформації, аналіз актуальності застосування стеганографії в месенджерах; розробка стеганографічного методу приховування повідомлень в наборі послідовних зображень; розробка програмної реалізації запропонованого методу; дослідження стійкості запропонованого методу приховування можливих збурених дій з боку зловмисника; програмна реалізація месенджера, який використовує запропонований метод. Об'єкт дослідження - процес забезпечення безпеки особистої інформації користувача при передачі повідомлень за допомогою месенджерів. Предмет дослідження – методи приховування інформації та алгоритми транспортування повідомлень в месенджерах. Новизна роботи полягає в розробці методу кодування повідомлень за допомогою зображень, який вперше використано в користувацькому месенджері. Розроблений метод приховування повідомлень реалізовано у самостійному програмному продукті для спілкування, крім того його реалізація може бути використана в існуючих месенджерах.

Ключові слова: цифрове зображення, передача повідомлень, потоки даних, метод кодування, месенджер.

Вступ

Завдання надійного захисту авторських прав, прав інтелектуальної власності або конфіденційних даних (які сьогодні в більшості випадків мають цифрової формат) від несанкціонованого доступу є однією з найдавніших і досі невирішених проблем. У зв'язку з інтенсивним розвитком і поширенням технологій, які дозволяють за допомогою комп'ютера інтегрувати, обробляти та синхронно відтворювати різні типи сигналів (так звані мультимедійні технології), питання захисту інформації, представленої в цифровому вигляді, є надзвичайно актуальним.

Переваги подання та передачі даних у цифровому вигляді (простота відновлення, висока потенційна завадостійкість, перспективи використання універсальних апаратних і програмних рішень) можуть бути перекреслені тією легкістю, з якою можливі їх викрадення та модифікація. Тому в усьому світі назріло питання розробки методів та засобів захисту інформації організаційного, методологічного й технічного характеру, серед них – методи криптографії та стеганографії [1-3].

Програми обміну повідомленнями є одними з найпопулярніших програм по всьому світу, про це свідчать результати опитувань [4-5]. Мільйони повідомлень

відправляються користувачами кожен день. Месенджери надають можливість спілкування з будь-якого місця, де є Інтернет, та в будь-який час. З кожним роком популярність месенджерів збільшується, вони стають невід'ємним атрибутом сучасного життя, зростає кількість постійних користувачів. Але зріст попиту на програми спілкування також збільшив і кількість зловмисників, які користуються всіма доступними методами задля викрадення особистої інформації.

Аналіз досліджень та публікацій

Можливість приховувати повідомлення за допомогою стеганографії має соціальні та етичні наслідки, подібні до криптографії. Деякі уряди вжили заходів щодо заборони використання криптографії або певних типів криптографії. Ці заборони часто застосовуються, щоб дозволити органам влади контролювати комунікації. Вважається, що безпека людей потребує обмежень конфіденційності комунікацій. В даний час стеганографічні методи можна використовувати, коли шифрування заборонено.

Стеганаліз, виявлення стеганографічних повідомлень в електронних носіях, часто може розкрити наявність стеганографічних повідомлень. Таким чином, зовнішні сторони (наприклад, уряди) можуть докладати зусиль, щоб виявити та, можливо, відстежити як відправника, так і одержувача стеганографічних повідомлень [6-7].

В Інтернеті можна знайти месенджери, в яких для захисту, а точніше приховування повідомлень, використовується стеганографія. В деяких таких проектах опублікований вихідний код або додаток вже доступний на таких платформах, як Google play.

Програма «Steganography» була розроблена як екзаменаційний проект у Копенгагенській школі дизайну та технологій. Вона використовувала веб-сервіс для функції стеганографії. Пізніше, програму було перенесено на телефон та опубліковано в Google Play з аналогічною назвою відповідно.

Нещодавно з'явилися бот-мережі на основі стеганографії (стего-ботнети), які дозволяють системам виявлення ботнетів виглядати звичним трафіком [8-9]. У стего-ботнетах кожне повідомлення вбудовано в мультимедійний файл, наприклад файл зображення, за допомогою методів стеганографії та розміщується на веб-сайтах служби соціальних мереж (таких як Facebook) або в онлайн-месенджерах (таких як WeChat або KakaoTalk).

Кемпбелл-Мур розробил плагін Secretbook, щоб приховати текстові повідомлення довжиною до 140 символів у зображеннях JPEG у Facebook за допомогою браузера Google Chrome [10-11]. Стаття Бекхузена чудово розкриває проблему стеганографії Facebook і пояснює рішення Кемпбелла-Мура. Коли хтось завантажує зображення на Facebook, воно автоматично стискається. Якщо в зображенні є стеганографія, Facebook спотворює його. Алгоритм Secretbook автоматично стискає зображення JPEG, як це зробив би Facebook, а потім додає приховані дані. Алгоритм також додає надлишковість, тому будь-які спотворення, що залишилися, можна виправити шляхом реконструкції з копій.

Як бачимо, приховання повідомлень є актуальною задачею в сучасному просторі обміну інформацією. Існують різні підходи до застосування стеганографії в процесі передачі повідомлень, це питання достатньо багато досліджується та розробляються контр-методи виявлення та аналізу прихованих повідомлень. Крім того, самі месенджери не приховують інформацію, а тільки передають контейнери в заздалегідь вбудованими даними.

В даній роботі запропоновано власний месенджер для захищеного спілкування користувачів на основі нового метода приховування повідомлень в наборі послідовних зображень.

Мета статті та постановка завдань

Метою роботи є розробка методу приховування повідомлень, його програмна реалізація та використання в месенджері.

Для досягнення визначеної мети в роботі були сформовані для розв'язання наступні задачі:

1. аналіз існуючих популярних месенджерів та їх методів захисту інформації, аналіз актуальності застосування стеганографії в месенджерах;
2. розробка стеганографічного методу приховування інформації в наборі зображень;
3. розробка програмної реалізації запропонованого методу приховування повідомлень;
4. дослідження стійкості запропонованого методу приховування до можливих збурених дій з боку зловмисника;
5. розробка програмної реалізації месенджера, який використовує запропонований метод приховування повідомлень.

Основна частина

В роботі запропоновано новий метод приховування повідомлень за допомогою зображень. Для користуванням методу потрібен приватний ключ і набір випадкових змістовних зображень. В самому месенджеру приватний ключ отримується за допомогою обміну ключами алгоритмом Діффі-Геллмана. Публічні ключі зберігаються на сервері, до якого мають доступ усі автентифіковані користувачі. За допомогою приватного ключа формується спеціальний словник відношення «піксель-символ», який використовується для перетворення повідомлення на набір послідовних зображень. Алфавіт месенджера, який було використано в цій роботі, складається з великих літер англійської абетки («A-Z», всього 26 літер) та символів «.» (точка), «,» (кома), «!» (знак оклику), «?» (знак питання), « » (пробіл). Всього - 31 символ. Для кожного символу з алфавіту месенджера було відведено визначену кількість значень пікселів, а саме:

«A – Z» - 8 значень; «!» - 9 значень; «?» - 9 значень; «,» - 9 значень; «.» - 10 значень;

« » - 11 значень.

Всього – 256 значень, що дорівнює кількості значень, яких може набувати яскравість пікселя. Всі символи згруповані в кортежі: кожен контейнер містить символ у відповідній йому кількості (наприклад, «AAAAAAAA», «BBBBBBBB», …). Такий підхід використано з метою, щоб у подальшому збільшити захист методу від збурених дій (стеганоаналітичних атак), які можуть бути використані по відношенню до зображень, які використовуються як контейнери для передачі повідомлення. Для того, щоб сформувати випадковий словник відношення «піксель-символ», де тепер за символ можна рахувати одразу відрізок символів, використовується бібліотека random в Python. За допомогою методу sample в модулі random формуємо випадкову послідовність вище зазначених кортежів символів, після чого задаємо відповідність значенням пікселів від 0 до 255 відповідно до сформованої випадкової послідовності. Щоб відправник і отримувач повідомлення мали той самий словник відношення «піксель-символ» використовується ключ як seed для модуля random. Такий seed дозволяє використати властивості псевдовипадкового формування послідовностей, тому сформований словник буде однаковий як у відправника, так і в отримувача. Набір випадкових змістовних зображень автоматично завантажується з Інтернету за випадковим пошуковим запитом. Кількість зображень буде становити більш, ніж 200 (в залежності від часу, але не більше 5 хвилин). Завантаження зображень відбувається

за допомогою Google API. Після того, як було підготовлено словник відношення «піксель-символ» та набір зображень, метод приховування повідомлень готовий до кодування тексту. По черзі, починаючи з першого символу, метод перетворює кожен символ на зображення, яке підходить для його кодування. Сам метод нічого не вбудовує в зображення, якщо відповідне до символу зображення було завантажене. В іншому випадку метод змінює лише значення одного пікселя. Через те, що алгоритм використовує для приховування повідомлення лише значення одного пікселя, цей метод є стійким до виявлення наявності вбудовування інформації в зображення стеганоаналізом.

На рисунку 1 схематично відображено загальну схему роботи запропонованого методу приховування повідомлення.

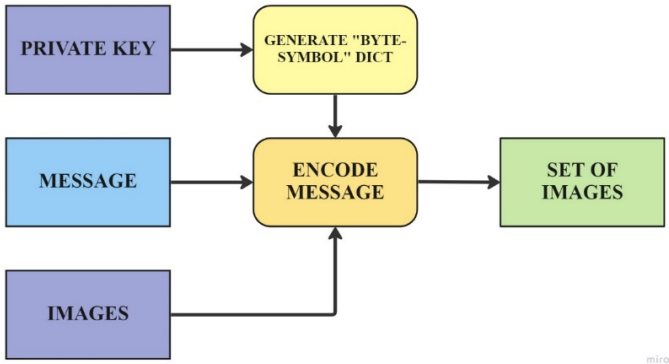


Рис. 1. Загальна схема методу приховування повідомлення в наборі послідовних зображень

Набір зображень відправляється у відповідному порядку отримувачу. Для декодування повідомлення отримувач буде використовувати свій приватний ключ, отриманий за алгоритмом Діффі-Геллмана.

Як і відправник, отримувач спочатку формує словник відношення «піксель-символ» за допомогою приватного ключа. Далі, по черзі, починаючі з першого зображення, починає декодувати повідомлення.

Загальна схема декодування відображена на рисунку 2.

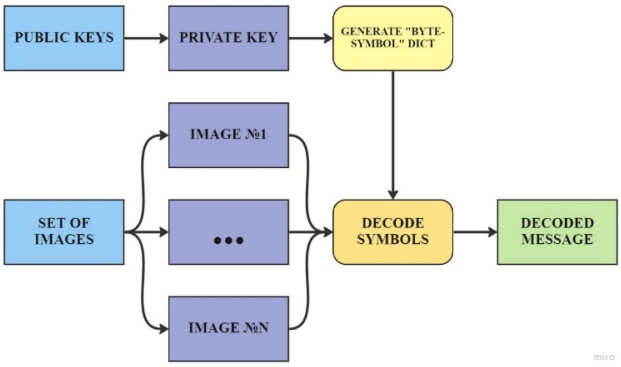


Рис. 2. Загальна схема декодування отриманого повідомлення

Для запропонованого метода було перевірено стійкість до накладення шуму, розмиття та повторного стиснення по відношенню до зображень.

Результати досліджень шумів Гауса та Лапласа на 100-та випадкових зображеннях представлені в таблиці 1.

За результатами перевірки стійкості метода до шуму Гауса можна сказати, що метод є стійким по відношенню до непомітного для користувача шуму. При коефіцієнті до 0.15 зберігається більше, ніж 90% повідомлення.

Таблиця 1

Результати перевірки стійкості метода до шумів Гауса та Лапласа

Коефіцієнт	Кількість успішно декодованих символів	
	Шум Гауса	Шум Лапласа
0.08	96	93
0.1	95	93
0.15	90	93
0.2	86	86
0.3	73	85
0.5	59	77
1	32	50

За результатами перевірки стійкості метода до шуму Лапласа можна сказати, що метод є стійким по відношенню до непомітного для користувача шуму. При коефіцієнті до 0.15 зберігається більше, ніж 93% повідомлення.

Аналогічні дослідження на 100-та зображеннях були проведені для розмиття Лапласа та повторного стиснення алгоритмом JPEG. Висновки по результатам представлені нижче.

За результатами перевірки стійкості метода до розмиття Лапласа можна сказати, що метод є стійким по відношенню до непомітного для користувача розмиття. При коефіцієнті до 1 зберігається більше, ніж 84% повідомлення.

За результатами перевірки стійкості метода до повторного стиснення JPEG можна сказати, що метод є стійким по відношенню до непомітного для користувача стиснення. При коефіцієнті якості до 70 зберігається більше, ніж 84% повідомлення.

Розглянемо роботу месенджера, в якому проведена програмна реалізація розробленого методу.

Щоб увійти в систему користувачу потрібно ввести логін та пароль у поля Login System, які можна побачити на рисунку 3, після чого відправляється пакет з цими даними на сервер.

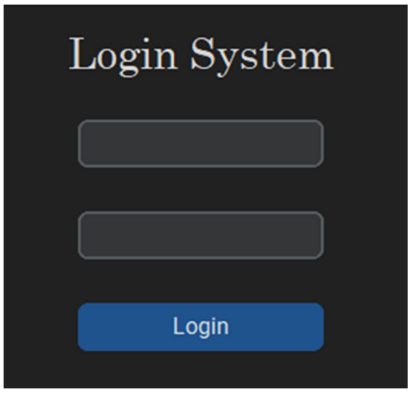


Рис. 3. Вікно авторизації користувача

Після успішної авторизації користувач потрапляє в головне меню месенджера, де він може обрати користувача, додати чи видалити його зі свого списку та відправити обраному співрозмовнику повідомлення.

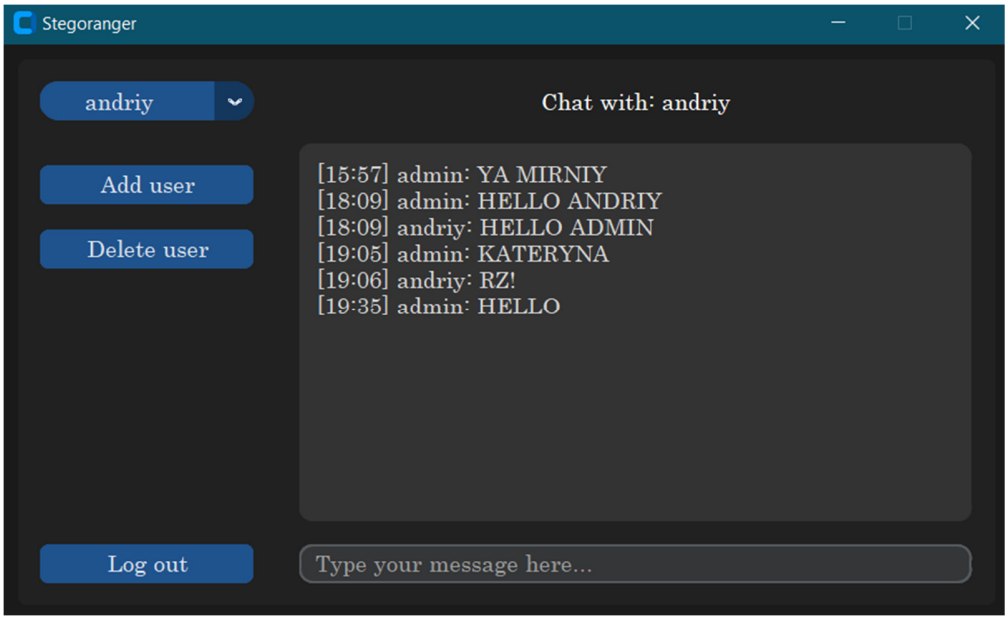


Рис. 4. Загальний інтерфейс месенджера з відкритим чатом

Спілкування між користувачами відбувається через сервер, але на сервері жодне з повідомлень не декодується, а зберігається в тому вигляді, в якому воно було відправлено, тобто у вигляді упорядкованого набору зображень.

Висновки

В роботі доведена актуальність обраної теми, обґрунтована мета розробки методу приховування повідомлень та отримані наступні результати:

1. Розроблено метод приховування повідомлень в наборі послідовних зображень без їх модифікації.
2. Розроблено програмну реалізації запропонованого методу та проведено тестування його стійкості до можливих збурених дій зі сторони зловмисника.
3. Розроблено месенджер з зручним користувацьким інтерфейсом, який використовує запропонований метод.

Запропонований метод приховування інформації також може знайти застосування в інших існуючих месенджерах.

Список літератури

1. Locating Secret Messages in Images», URL: https://www.cs.ucdavis.edu/~davidson/Publications/kddres2004.pdf
2. Мельник С.В., Кондакова С.В. Світові тенденції розвитку цифрової стеганографії в контексті завдань забезпечення інформаційної безпеки держави. *Актуальні проблеми управління інформаційною безпекою держави. Наук.-практ. конф.* К. : Наук.-вид. відділ НА СБ України, 2010. С. 134-138.
3. Кінзерявий О.М. Стеганографічні методи приховування даних у векторні зображення, стійкі до активних атак на основі афінних перетворень: дис. ... канд.

техн.. наук. Спеціальність 05.13.21 – Системи захисту інформації. Київ , 2015, 324 с.
4. WhatsApp, WeChat and Facebook Messenger: global usage of messaging apps and statistics. URL: https://www.messengerpeople.com/global-messenger-usage-statistics/
5. Які мобільні додатки є найбільш популярними? URL: https://www.kiis.com.ua/?lang=ukr&cat=reports&id=1072&page=1
6. Steganalysis Techniques: A Comparative Study. URL: https://scholarworks.uno.edu/cgi/viewcontent.cgi?article=1562&context=td
7. Enhanced PeerHunter: Detecting Peer-to-Peer Botnets Through Network-Flow Level Community Behavior Analysis. URL: https://doi.org/10.1109/TIFS.2018.2881657
8. A Survey on Botnet Detection Techniques. URL: https://doi.org/10.1109/ic-ETITE47903.2020.Id-70
9. Using Facebook for Image Steganography. URL: https://www.researchgate. net/publication/277959373_Using_Facebook_for_Image_Steganography
10. Castiglione A., Cattaneo G., De Santis A. A forensic analysis of images on online social networks. *Third International Conference on Intelligent Networking and Collaborative Systems*, 2011, P. 679-684.

DEVELOPMENT OF A MESSENGER FOR HIDDEN TRANSMISSION OF MESSAGES

A. Pavliuk, N. Kushnirenko, O. Troyanskiy

National Odesa Polytechnic University,
1, Shevchenko Ave., Odesa, 65044, Ukraine; e-mail: infsec2011@gmail.com

Information is one of the most valuable objects of modern life. Accessing it has become incredibly easy with the development of global computer networks. At the same time, the ease and speed of such access significantly increased the threat of data security violations in the absence of means to protect them. The relevance of the topic lies in the fact that in today's realities messengers are an integral part of the life of almost every person in the world, therefore the security of personal information has a high priority. The purpose of the work is to develop a method of hiding messages in a set of sequential images, its software implementation and use in the messenger. To achieve the defined goal, the following tasks were formed: analysis of existing popular messengers and their methods of information protection, analysis of the relevance of steganography in messengers; development of a steganographic method of hiding messages in a set of consecutive images; development of software implementation of the proposed method; study of the resistance of the proposed hiding method to possible disturbed actions by the attacker; software implementation of the messenger that uses the proposed method. The object of the study is the process of ensuring the security of the user's personal information when using messengers. The subject of the research is methods of hiding information and algorithms for transporting messages in messengers. The novelty of the work lies in the development of a method for encoding messages using images, which was first used in a user messenger. The developed method of hiding messages is implemented in an independent software product for communication, in addition, its implementation can be used in other existing messengers.
Keywords: digital image, message transmission, data streams, coding method, messenger.

А.Ю. Прокофьєв

1DOI 10.15276/imms.v12.no3.209
УДК 519.972.5:004.942.001.57

Informatics and Mathematical Methods in Simulation
Vol. 12 (2022), No. 3, pp. 209-218

АНАЛІЗ ПОХИБОК МАТЕМАТИЧНОГО МОДЕЛЮВАННЯ ДИНАМІЧНИХ ОБ'ЄКТІВ, ЯКІ ОПИСУЮТЬСЯ ІНТЕГРАЛЬНИМИ РІВНЯННЯМИ

А.Ю. Прокофьєв

Національний університет «Одеська політехніка»
пр.-т Шевченка, 1, Одеса, 65022, Україна; e-mail: fallbrick1985@gmail.com

Вибір інтегральних рівнянь при математичному моделюванні, в залежності від досліджуваного явища, обумовлено наступними факторами: неможливість складання інших рівнянь (суть — математичних моделей досліджуваних явищ); необхідність зниження мірності рівнянь (тобто кількості незалежних змінних) при розв'язуванні задач для суцільних середовищ; можливість компактного формулювання граничних задач; досягнення спрощень при обчисленнях; можливість простого та природного переходу до систем кінцевовимірних рівнянь (при дискретизації неперервних задач). Слід підкреслити особливу роль інтегральних рівнянь при розв'язуванні граничних задач та аналізі випадкових, в тому числі динамічних процесів. Застосування методу математичного моделювання, який являє собою сукупність прийомів визначення математичних зв'язків між відомими вихідними даними та невідомою характеристикою об'єкта, що досліджується у вигляді інтегральних рівнянь чи перетворень, є важливим не тільки тому, що це питання недостатньо висвітлено в літературі, але також і тому, що своєрідність інтегральних співвідношень та умов їх складання у значній мірі визначають вибір обчислювальних методів та засобів при числовій реалізації. Насамперед зазначена особливість полягає у аналізі точності обчислювальних процедур, які застосовуються в ході математичного моделювання із застосуванням моделей об'єктів у вигляді інтегральних рівнянь, оскільки в якості вхідних даних при цьому використовуються експериментальні дані, точність яких визначається застосованою вимірювальною апаратурою та впливом зовнішніх завад при вимірюваннях. Тому аналіз похибок математичного моделювання динамічних об'єктів на основі моделей у вигляді інтегральних рівнянь має актуальне значення при розв'язуванні більш широких задач моделювання та управління динамічними об'єктами.

Ключові слова: математичне моделювання, інтегральні рівняння, похибка розв'язку, динамічні об'єкти.

Вступ

Застосування інтегральних перетворень та рівнянь дозволяє сформулювати деякі загальні властивості такого способу математичного моделювання:

1. Принципова та практична можливість використання в задачах, що мають стохастичну природу, і в задачах, математичне моделювання яких засновано на оцінці сумарного впливу відомих (шуканих) величин на характеристики, що спостерігаються (досліджуються), причому вказані дані, або їх частина, має експериментальне походження.

2. Висока універсальність математичних співвідношень, які отримуються, що досягається як за рахунок компактного формулювання граничних задач, так і за рахунок того, що до одного і того ж типу інтегральних рівнянь зводяться задачі, кожна з яких може бути описана власним, відмінним від інших, диференціальним рівнянням.

3. Можливість єдинообразного переходу до розрахункових виразів з використанням ефективних прийомів обчислювальної математики.

Невідомим етапом математичного моделювання є використання виразів, що описують явище, яке досліджується, для отримання числових результатів, тобто конкретних відомостей, за ради яких, у багатьох випадках, і проводиться дослідження. Цей етап має назву числової реалізації математичних моделей (ММ) і зводиться до розв'язування рівнянь, які відповідають прийнятій формі математичного моделювання.

Розв'язування практичних задач, сформульованих у вигляді інтегральних рівнянь, потребує застосування *наближених числових методів* розв'язку, для реалізації яких, як правило, необхідно застосування певних (переважно таких, що потребують застосування обчислювальної техніки) засобів обчислювання. Тому, поряд з удосконаленням теорії інтегральних рівнянь, отримали розвиток числові *комп'ютерно-орієнтовані* методи їх розв'язування.

Задача *числової реалізації інтегральних моделей*, з огляду на її складність, неодмінно трансформується в проблему машинної (*комп'ютерної*) реалізації, яка, в залежності від конкретних умов та мети дослідження, може зводитися до сукупності питань вибору та використання обчислювальних методів та засобі, а у багатьох випадках — і до їх розробки. Дійсно, ММ може бути використана для отримання лише числових результатів розв'язку — тоді це *задача обчислення*; для достатньо багатостороннього відтворення та довготривалого відтворення явища або об'єкта, що досліджується, — це *задача моделювання*; для формування управляючих впливів у іншому об'єкті чи явищі — *задача управління*. Часто метою дослідження є спільний розв'язок вказаних задач.

Основою числових розв'язування прикладних задач є досконало розроблені числові методи. Значна кількість та різноманіття цих методів пояснюється намаганням до їх удосконалення та наявністю різних типів рівнянь, неможливістю охоплення яких єдиним універсальним методом є об'єктивним фактом [1 – 3].

Сказане вище дозволяє вважати, що методи математичного моделювання на основі інтегральних рівнянь у сукупності з методами розв'язування (та прикладними програмами) потребують уваги як з точки зору їх розвитку, так і з точки зору застосування.

Враховуючи важливість задач математичного моделювання при розв'язуванні прикладних задач моделювання та управління динамічними об'єктами, окремою важливою проблемою постає оцінка точності отриманих розв'язків, яка напряму пов'язана з аналізом похибок останніх.

Мета роботи

Мета роботи полягає у отриманні аналітичних виразів, які дозволяють апріорно оцінити точність (похибки) процедур математичного моделювання при розв'язуванні прикладних задач моделювання та управління динамічними об'єктами, ММ яких представлено у вигляді інтегральних рівнянь.

Основна частина

Інтегральні рівняння є досить загальною формою математичного опису різних динамічних об'єктів. Лінійні нестаціонарні об'єкти, в загальному випадку, може бути описано лінійним рівнянням Вольтери другого роду

$$y(x)+\int_0^x [K(x,s)\,y(s)]\,ds = f(x), \qquad (1)$$

де $K(x,s)$ — ядро; $f(x)$ — відома функція (права частина); $y(x)$ — шукана функція.

Частинним випадком (1) може бути опис *стаціонарних лінійних* об'єктів у вигляді:

$$y(x)+\int_0^x [K(x-s)\,y(s)]\,ds = f(x), \tag{2}$$

ядро якого залежить від різниці аргументів x та s і, тому називається *різницевим*.

Нелінійні об'єкти може бути описано рівнянням наступного виду:

$$y(x)+\int_0^x \{K(x,s)\,F[y(s)]\}\,ds = f(x) \tag{3}$$

або більш загальним рівнянням

$$y(x)+\int_0^x \{K[x,s,y(s)]\}\,ds = f(x), \tag{4}$$

причому, у випадку стаціонарних об'єктів (як зазначалося — частинного випадку), ядро в рівняннях (3), (4) є різницевим.

При комп'ютерному розв'язуванні рівнянь (1) — (4) за допомогою методів математичного моделювання *актуальною* є задача отримання уявлень щодо можливих *похибок розв'язків*, які неодмінно виникають у зв'язку із застосуванням числових (тобто *наближених*) методів моделювання. Така ж задача є актуальною і при пошуку *управління*, оскільки *синтез управляючих функцій* (суть — *зворотна* задача) ґрунтується на реалізації ММ динамічних (або стаціонарних — у частинному випадку) об'єктів, як етапу такого синтезу.

Відомий ряд робіт [4], в яких розглядаються питання *аналізу точності* розв'язування традиційних для комп'ютерних засобів диференціальних рівнянь. Отримані результати може бути частково використано у застосуванні до інтегральних рівнянь, одначе є також низка *якісних особливостей*, які слід враховувати.

При комп'ютерному розв'язуванні наведених рівнянь (1) — (4), як було зазначено вище, використовують наближені (числові) методи. Одначе, без попередніх спеціальних перетворень, можливе розв'язування лише рівнянь виду:

$$y(x)+\int_0^x \left[a_1 + a_2(x-s)+\ldots+a_n\,\frac{(x-s)^{n-1}}{(n-1)!}\right] y(s)\,ds = f(x), \tag{5}$$

які описують лінійні стаціонарні об'єкти із зосередженими параметрами (ЗП-об'єкти) та еквівалентні диференціальним рівнянням виду

$$\frac{d^n\varphi(x)}{dx^n} + a_1\,\frac{d^{n-1}\varphi(x)}{dx^{n-1}} + \ldots + a_n\varphi(x) = \psi(x), \tag{6}$$

де

$$y(x) = \frac{d^n\varphi(x)}{dx^n}.$$

Права частина (5) визначається функцією $\psi(x)$ та початковими умовами для рівнянь (6).

В якості способу безпосереднього моделювання рівняння (5) зручно прийняти аналогову форму розв'язування рівняння (6), яка полягає у застосуванні замкнутої моделюючої схеми, яка містить послідовний ланцюжок з n інтеграторів.

Якщо розв'язується рівняння (2) з довільним різницевим ядром, то для застосування методу безпосереднього моделювання необхідно виконати попередню апроксимацію ядра.

Слід зазначити, що для лінійних та таких, які добре лінеаризуються, інтегральних рівнянь похибка може виражена за допомогою фундаментальної формули похибок [5]. Дійсно, комп'ютерний розв'язок можна представити таким, що залежить від ряду величин $q_1, q_2, .., q_n$, які характеризують параметри ММ, вхідні впливи тощо, відхилення яких і викликають похибку отримуваного результату. За наявності відхилень реальний розв'язок шляхом розкладання у обмежений ряд Тейлора може бути представлено наступним чином:

$$Y(x, q_1 + \Delta q_1, q_2 + \Delta q_2, ..., q_n + \Delta q_n) \cong Y(x, q_1, q_2, ..., q_n) + \\ + [u_1(x)\Delta q_1 + u_2(x)\Delta q_2 + ... + u_n(x)\Delta q_n], \quad (7)$$

де $u_1(x), u_2(x), ..., u_n(x)$ — коефіцієнти *впливу* або *чутливості*.

Віднімаючи з правої частини (7) точний розв'язок $Y(x, q_1, q_2, ..., q_n)$ — тобто перший доданок — можна записати похибку

$$\Delta Y(x) = u_1(x)\Delta q_1 + u_2(x)\Delta q_2 + ... + u_n(x)\Delta q_n. \quad (8)$$

Таким чином, для достатньо наближеного визначення похибки розв'язку необхідно знати *відхилення* параметрів $q_1, q_2, .., q_n$ (або їх *вірогідніснi характеристики*) та визначити коефіцієнти їх впливу.

Для віднаходження коефіцієнтів чутливості (у випадку лінійного рівняння) можна отримати відповідне рівняння. Будемо вважати, що параметри $q_1, q_2, .., q_n$ визначаються внутрішніми властивостями ММ, тобто входять до ядра рівняння, що розв'язується комп'ютерними засобами, і яке, в такому випадку, має вигляд:

$$Y(x) + \int_0^x [K_м(x, s, q_1, q_2, .., q_n) Y(s)] ds = f(x). \quad (9)$$

Виконуючи диференціювання обох частин (1.49) по параметрах $q_i \ (i = \overline{1, n})$, отримаємо

$$\frac{\partial Y(x)}{\partial q_i} + \int_0^x \left[\frac{\partial K_м(x, s, q_1, q_2, .., q_n)}{\partial q_i} Y(s) \right] ds = 0. \quad (10)$$

Уводячи позначення

$$\frac{\partial Y(x)}{\partial q_i} = u_i(x), \ \frac{\partial K_м(x, s, q_1, q_2, .., q_n)}{\partial q_i} = K'_{м q_i}(x, s, q_1, q_2, .., q_n)$$

отримаємо шукані рівняння:

$$u_i(x) + \int_0^x [K_м(x, s, q_1, q_2, .., q_n) u_i(x)] ds = \\ = -\int_0^x [K'_{м q_i}(x, s, q_1, q_2, .., q_n) Y(s)] ds. \quad (11)$$

В якості функції $Y(s)$ в правій частині (1.51) можна використати наближений розв'язок. Як видно, для визначення коефіцієнтів чутливості можна використати

основну ММ, що реалізується комп'ютерними засобами, оскільки ядро рівняння (11) співпадає з ядром рівняння (1), яке розв'язується.

Таким самим образом можна отримати рівняння чутливості для нелінійного рівняння (1.43). Відповідне йому машинне рівняння має вигляд:

$$Y(x)+\int_0^x \{K_{\text{м}}(x,s,q_1,q_2,\ ..,q_n)F[Y(s)]\}ds = f(x). \tag{12}$$

Диференціювання (12) дає

$$\frac{\partial Y(x)}{\partial q_i}+\int_0^x \left\{\frac{\partial K_{\text{м}}(x,s,q_1,q_2,\ ..,q_n)F[Y(s)]}{\partial q_i}\right\}ds = 0$$

або

$$\frac{\partial Y(x)}{\partial q_i}+\int_0^x \{K'_{\text{м}q_i}(x,s,q_1,q_2,..,q_n)F[Y(s)]+$$

$$+K_{\text{м}}(x,s,q_1,q_2,\ ..,q_n)F'(s)\frac{\partial Y(s)}{\partial q_i}\Big\}ds = 0. \tag{13}$$

Враховуючи уведене раніше позначення для $u_i(x)$, можна отримати:

$$u_i(x)+\int_0^x [K_{\text{м}}(x,s,q_1,q_2,\ ..,q_n)F'(s)u_i(s)]ds =$$

$$=-\int_0^x \{K'_{\text{м}q_i}(x,s,q_1,q_2,\ ..,q_n)F[Y(s)]\}ds;\ \ i=\overline{1,n}. \tag{14}$$

Отримані рівняння чутливості є лінійними, на відміну від вихідного рівняння (3). Для їх розв'язування може бути використано ММ, яка реалізується комп'ютерними засобами, в якій нелінійне перетворення шуканої функції по закону $F[\cdot]$ замінено множенням її на змінний коефіцієнт $F'[\cdot]$. Для відтворення правої частини (14) також можна використати отриману раніше комп'ютерним розв'язуванням функцію $Y(x)$.

Слід зазначити, що загальне рівняння (4) може бути приведено до більш простому виду (3), який допускає *дослідження похибок*.

Якщо функцію $K[x,s,y(s)]$ може бути розкладено у ряд Маклорена [6] по ступенях $x(t)$:

$$K[x,s,y(s)] \cong \sum_{i=0}^{\infty}\frac{K_x^{(i)}[x=0,s,y(s)]}{x!}x^i$$

і ряд збігається в області зміни x та s, то можна виконати наближену заміну

$$K[x,s,y(s)] \cong \sum_{i=0}^{m}\frac{K_x^{(i)}[x=0,s,y(s)]}{x!}x^i;\ \ i=\overline{1,m}$$

та розв'язувати наближене рівняння

$$y(x)+\int_0^x \sum_{i=0}^{m}\frac{K_x^{(i)}[x=0,s,y(s)]}{i!}x^i = f(x).$$

Як і у випадку диференційних рівнянь, для лінійних інтегральних рівнянь можна отримати *рівняння для похибки*. Можна вважати, що при розв'язуванні (1) машинне рівняння має вигляд:

$$\widetilde{y}(x)+\int_0^x\left[\widetilde{K}(x,s)\widetilde{y}(s)\right]ds=\widetilde{f}(x), \tag{15}$$

де ядро $\widetilde{K}(x,s)$ враховує *первинні похибки моделювання* (*методичну* та *інструментальну* похибки) та являє собою суму

$$\widetilde{K}(x,s)=K(x,s)+\Delta K(x,s),$$

права частина $\widetilde{f}(x)$ містить *похибку зовнішнього збудження* та

$$\widetilde{f}(x)=f(x)+\Delta f(x),$$

$\widetilde{y}(x)$ — наближений розв'язок, що визначається співвідношенням

$$\widetilde{y}(x)=y(x)+\Delta y(x),$$

де $\Delta y(x)$ — *сумарна похибка* розв'язку.

Тоді, віднімаючи вираз (1) з (15), можна отримати

$$\Delta y(x)+\int_0^x\left\{\left[K(x,s)+\Delta K(x,s)\right]\left[y(x)+\Delta y(x)\right]-K(x,s)y(s)\right\}ds=\Delta f(x).$$

Розкриваючи дужки під інтегралом і вважаючи похибки $\Delta K(x,s)$ та $\Delta y(x)$ настільки малими, що їх добутком можна знехтувати, отримаємо шукане рівняння

$$\Delta y(x)+\int_0^x\left[K(x,s)\Delta y(s)\right]ds=\Delta f(x)-\int_0^x\left[\Delta K(x,s)y(s)\right]ds. \tag{16}$$

Цим рівнянням для обчислення похибки $\Delta y(x)$ складно скористатися з огляду через невизначеність завдання первинних похибок, яка зазвичай має місце, а також у зв'язку з тим, що замість істинного розв'язку $y(s)$ в правій частині необхідно використовувати наближене. Одначе воно може використовуватися для *якісного дослідження похибок*, оскільки, зокрема, показує що різні складові сумарної похибки можуть бути визначені окремо (залишаючи в правій частині тільки $\Delta f(x)$, можна визначити *наслідкову похибку* результату, а залишаючи лише інтеграл — *похибку моделювання*). Крім того, рівняння для похибки дозволяє виконати *оцінку похибки*.

Зокрема (у вигляді тестової задачі), якщо (x,s) належить області D ($(x,s)\in D$); $0\le x\le a$, $0\le s\le b$ і, при цьому, можна завдати обмеження

$$\max_{(x,s)\in D}\left|K(x,s)\right|\le K,\ \max_{(x,s)\in D}\left|\widetilde{K}(x,s)\right|\le\widetilde{K},\ \max_{(x,s)\in D}\left|\Delta K(x,s)\right|\le\delta,$$

$$\max_{(x,s)\in D}\left|\widetilde{f}(x)\right|\le f,\ \max_{(x,s)\in D}\left|\Delta f(x)\right|\le\eta,$$

то, використовуючи вище наведені результати, можна отримати оцінку

$$\Delta y(x)\le\left[f\,\delta\frac{e^{(K-\widetilde{K})x}-1}{K-\widetilde{K}}+\eta\right]e^{\widetilde{K}x}.$$

При $K=\widetilde{K}$ дана оцінка спрощується :

$$\Delta y(x)\le\left(f\,\delta x+\eta\right)e^{Kx}.$$

Таким чином, з наведеного аналізу випливає, що існує декілька шляхів отримання відомостей щодо *похибок розв'язків інтегральних рівнянь*, які виникають при числовій реалізації їх (як відповідних ММ динамічних об'єктів) із застосуванням комп'ютерно-орієнтованих методів.

В якості прикладного аспекту аналізу похибок наразі розглянемо застосування методу модельних прикладів при реалізації ММ динамічних об'єктів у вигляді інтегральних рівнянь (зокрема, для конкретності викладення — рівнянь Фредгольма першого роду, що, одначе, не знижує загального характеру цього викладення).

Як зазначалося вище, постановка задачі відшукання невідомої характеристики у вигляді (1.41) є некоректною. Не зважаючи на те, що у розвитку теорії наближених методів розв'язування некоректних задач отримано значні конструктивні результати [7], проблема ефективної та формалізованої реалізації методів регуляризації і до тепер залишається ще гострою [8, 9]. Одним з розповсюджених методів при визначенні параметру регуляризації є *метод модельних прикладів*, суть якого викладено, зокрема в [9]. Обґрунтування (з використанням оціночних нерівностей) та процедура методу модельних прикладів полягає в наступному.

Нехай завдано операторне рівняння першого роду, що відповідає (1.41):

$$Ay = f\,,\ y \in Y\,,\ f \in F\,, \tag{17}$$

де y — шуканий, а f — заданий елементи лінійних нормованих просторів Y та F ; A — лінійний безперервний оператор $A : Y \to F$.

Відомо [9] (як зазначалося вище), що задача розв'язування рівняння (17) є некоректною і повинна розв'язуватися певними методами, які набули назву методів регуляризації [8, 9].

Так, в *методі регуляризації Лаврентьєва* [8, 9], замість рівняння (17) розв'язується рівняння

$$\alpha y + Ay = f\,, \tag{18}$$

де α — параметр регуляризації, а в *методі Тихонова* [9], замість (17) розв'язується рівняння

$$\alpha y + A^* Ay = A^* f\,, \tag{19}$$

де A^* — оператор, сполучений з оператором A.

Найбільш трудомісткою та складною є задача визначення параметру α, для розв'язування якої запропоновано декілька методів [9], у тому числі *метод модельних прикладів*.

Визначення 1.1. *Модельним прикладом* (рівнянням) по відношенню до деякої практичної задачі (рівнянню) P називається приклад Q, який має такий самий набір параметрів $M = (m_1, m_2, ..., m_k)$, що і задача P.

Якщо задачу P та приклад Q розв'язувати при одному й тому ж значенні параметра α, то цілком раціонально вважати, що оцінки відносних похибок розв'язків в обох випадках будуть однаковими. Це дає можливість вважати рівняння P та Q, в певному сенсі «близькими», не зважаючи на можливе розходження в правих частинах. Природно, співпадіння оцінок не гарантує рівності відносних похибок $\|\Delta y_P\| / \|y_P\|$ та

$\|\Delta y_Q\|/\|y_Q\|$ відповідних розв'язків (похибки рівні лише у випадку, коли $f_Q(x) = gf_P(x)$, де $g = \text{const} \neq 0$).

Смисл уведення модельного прикладу полягає у можливості мати «близьке» до рівняння, яке розв'язується, інше — з відомим розв'язком y_Q.

Метод модельних прикладів полягає у наступному.

1. Для заданого рівняння P, яке підлягає розв'язуванню, складається штучний модельний приклад Q, в якому задається *точний розв'язок* $y_Q(s)$ такий, щоб функція $f_Q(x)$, яку визначається обчисленням інтегралу в лівій частині рівняння (рівняння *Фредгольма першого порядку*)

$$Ay = \int_a^b [K(x,s)\,y(s)]ds = f(x),\ c \le x \le d\,, \tag{20}$$

де ядро $K(x,s) \in L_K$ та права частина $f(x) \in L_f$ — відомі функції, $y(s) \in Y$ — шукана функція, був би (тобто точний розв'язок $y_Q(s)$), за можливістю, «близьким» до правої частини $f_P(x)$ рівняння P, яке розв'язується (наприклад, з точністю до деякого постійного множника $g = \text{const} \neq 0$). При цьому, будуючи функцію $y_Q(s)$, необхідно враховувати можливу апріорну інформацію щодо шуканої функції $y_P(s)$.

2. До значень $f_Q(x)$ за допомогою генератора випадкових чисел додаються такі похибки, при яких приблизно співпадають величини $\|\Delta f_Q\|/\|f_Q\|$ та $\|\Delta f_P\|/\|f_P\|$ (вочевидь, точної рівності не можна досягнути, оскільки Δf_P на практиці зазвичай відома з похибкою).

3. Шляхом числового розв'язування модельного прикладу Q, відповідно до одного з методів регуляризації (19), (20), для ряду значень α визначається оптимальне значення $\alpha = \alpha_{\text{опт}}$ таке, при якому

$$\|y_{Q_\alpha} - y_Q\| \to \min\,. \tag{21}$$

Тут y_{Q_α} — числовий розв'язок рівнянь регуляризації (20), відповідно за методами Лаврентьєва та Тихонова:

$$\alpha y\left[(x-c)\frac{b-a}{\alpha - c} + \alpha\right] + \int_a^b [K(x,s)\,y(s)]ds = f(x);\ c \le x \le d\,, \tag{22}$$

$$\alpha y(x) + \int_a^b [K(x,s)\,y(s)]ds = \omega(x);\ a \le x \le b\,, \tag{23}$$

де

$$K(x,s) = \int_c^d [K(t,x)\,K(t,s)]dt,\ \ \omega(x) = \int_c^d [K(t,x)\,f(t)]dt\,.$$

4. Віднайдене значення $\alpha_{Q_{\text{опт}}}$, будучи близьким до шуканого $\alpha_{P_{\text{опт}}}$, використовується у подальшому для розв'язування вихідного рівняння P.

Строге математичне обґрунтування методу модельних прикладів ускладнено. Одначе, в прикладному сенсі, метод еталонних прикладів може бути орієнтовано для оперативного розв'язування некоректних задач (особливо *задач управління в реальному масштабі часу*) з однаковими наборами вихідних даних $M = (m_1, m_2, ..., m_k)$. При цьому розв'язування широкого кола практичних задач свідчить про ефективність даного методу. Крім розглянутих, певного поширення при числовій реалізації інтегральних рівнянь, набули методи: резольвент [10], зведення до алгебраїчних рівнянь [11], заміни інтеграла кінцевою сумою [11].

Висновки

Отримано вирази, які визначають похибку розв'язку інтегральних рівнянь, які використовуються в якості математичних моделей при розв'язуванні задач моделювання та управління динамічними об'єктами. Показано, що частинна задача аналізу похибки розв'язку інтегрального рівняння по складності може наближатися до власно первинної задачі моделювання або управління. Також показано, що при обчисленні похибки $\Delta y(x)$ в процесі розв'язування інтегральних рівнянь (як математичних моделей відповідних динамічних об'єктів) слід звертати увагу на невизначеність завдання первинних похибок (похибок вимірювання вхідних даних), що, зазвичай, має місце для прикладних задач.

Одначе, отримані вирази дають змогу виконати якісне дослідження похибок розв'язку інтегральних рівнянь (суть — реалізації моделей динамічних об'єктів), оскільки, зокрема, показують складові сумарної похибки, які, в свою чергу, можна оцінити (обчислити) окремо, та визначити вплив кожної з цих складових на сумарну похибку.

Список літератури

1. Задачін В.М., Конюшенко І.Г. Чисельні методи. Х.: Вид-во ХНЕУ ім. С. Кузнеця, 2014. 180 с.
2. Гончаров О.А. Л. В. Васильєва А. М. Юнда. Чисельні методи розв'язання прикладних задач. Суми: Сумський державний університет, 2020. 142 с.
3. Андрунік В.А., Висоцька В.А., Пасічник В.В. Чисельні методи в комп'ютерних науках. Львів: Новий світ– 200, 2017. 470 с.
4. Третинник В.В., Любашенко Н.Д. Методи обчислень: Чисельні методи алгебри К.: КПІ ім.І.Сікорського, 2019. 139 с.
5. Семенко Л. Г. Информационные технологии. М.: ГП ЦНИИС, 2003. 379 с.
6. Фихтенгольц Г.М. Курс дифференциального и интегрального исчисления. Т.1. М.: ФИЗМАТЛИТ, 2003. 680 с.
7. Кабанихин С.И. Обратные и некорректные задачи. Новосибирск: Сибирское научное издание, 2009. 457 с.
8. Engl H., Hanke M., Neuebauer A. Regularization of Inverse Problems. London: Kluwer, 1996. 376 p.
9. Тихонов А.Н., Арсенин В.Я. Методы решения некорректных задач. М.: Наука, 1979. 288 с.
10. Канунников А. Л. Алгебра. Ч 3 — Метод резольвент Лагранжа. М.: СОЛИС, 2005. 147 с.
11. Корн Г., Корн Т. Справочник по математике для научных работников и инженеров. М.: Физматгиз, 1978. 832 с.

ERROR ANALYSIS OF MATHEMATICAL MODELING OF DYNAMIC OBJECTS WHICH ARE DESCRIBED BY INTEGRAL EQUATIONS

A.Yu. Prokofiev

National Odesa Polytechnic University
Shevchenko ave., 1, Odesa, Ukraine; e-mail: fallbrick1985@gmail.com

The choice of integral equations in mathematical modeling, depending on the investigated phenomenon, is determined by the following factors: the impossibility of compiling other equations (the essence is mathematical models (MM) of the investigated phenomena); the need to reduce the dimensionality of equations (that is, the number of independent variables) when solving problems for continuous environments; the possibility of a compact formulation of boundary problems; achieving simplifications in calculations; the possibility of a simple and natural transition to systems of finite-dimensional equations (when discretizing continuous problems). It should be emphasized the special role of integral equations in solving boundary value problems and analyzing random, including dynamic, processes. The application of the mathematical modeling method, which is a set of techniques for determining mathematical relationships between known initial data and an unknown characteristic of the object under investigation in the form of integral equations or transformations, is important not only because this issue is not sufficiently covered in the literature, but also because the peculiarity of the integral relations and the conditions of their compilation largely determine the choice of computational methods and tools for numerical implementation. First of all, the specified feature consists in the analysis of the accuracy of computational procedures that are used in the course of mathematical modeling using the MM of objects in the form of integral equations, since experimental data are used as input data, the accuracy of which is determined by the used measuring equipment and the influence of external interference during measurements. Therefore, the analysis of errors of mathematical modeling of dynamic objects based on MM in the form of integral equations is of urgent importance in solving broader problems of modeling and control of dynamic objects.

Keywords: mathematical modeling, integral equations, solution error, dynamic objects.

DOI 10.15276/imms.v12.no3.219
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 12 (2022), No. 3, pp. 219-225

МЕТОД СИНТЕЗУ ВИСОКОЯКІСНИХ S-БЛОКІВ НА ОСНОВІ ФУНКЦІЙ БАГАТОЗНАЧНОЇ ЛОГІКИ

В.В. Радуш, А.В. Соколов

Національний університет «Одеська політехніка»
Україна, Одеса, 65044, пр-т Шевченка, 1. radiosquid@gmail.com

Криптографічний S-блок є найважливішим компонентом сучасних шифрів, від якості якого у великій мірі залежить ефективність, криптографічна захищеність та швидкодія шифрів, які на ньому засновані. На сьогоднішній день, через розвиток квантового криптоаналізу, а також появу можливих атак на криптографічні алгоритми шляхом їх опису за допомогою функцій багатозначної логіки, стає актуальним завдання розробки алгоритмів синтезу S-блоків, які були б високоякісними не тільки при їх представленні компонентними булевими функціями, але і при будь-якому іншому представленні компонентними функціями багатозначної логіки. При цьому, більша частина представлених в літературі існуючих методів синтезу S-блоків орієнтована лише на дослідження їх криптографічної якості при представленні компонентними булевими функціями. У даній роботі на основі S-блоків довжини N=16, що відповідають суворому лавинному критерію компонентних булевих та 4-функцій, представлено метод синтезу великої множини потужності J=117588 S-блоків практично цінної довжини N=256, що одночасно відповідають строгому лавинному критерію компонентних булевих функцій, строгому лавинному критерію компонентних 4-функцій, а також критерію кореляційного імунітету компонентних булевих функцій, тобто володіють ідеальними матрицями коефіцієнтів кореляції векторів виходу та входу. Висока криптографічна якість розроблених S-блоків при їх представленні компонентними булевими та 4-функціями дозволяє рекомендувати їх для практичного застосування як у задачах підвищення ефективності існуючих криптоалгоритмів, так і при розробці перспективних шифрів, тоді як потужність класу синтезованих S-блоків дозволяє застосовувати їх у якості довгострокового ключа.

Ключові слова: S-блок, критерій розповсюдження помилки, кореляційний імунітет, функція багатозначної логіки.

Введення і постановка задачі

Одним з найважливіших криптографічних примітивів, що визначає ефективність, рівень криптографічної захищеності, а також швидкодію сучасних симетричних криптоалгоритмів, є S-блок [1]. На сьогоднішній день, чимало публікацій присвячено питанням синтезу S-блоків за критеріями криптографічної якості їх компонентних булевих функцій. Однак, через появу публікацій [2], де зазначаються можливості атак проти криптографічних конструкцій із застосуванням їх опису функціями багатозначної логіки, все більш гостро стає питання про необхідність побудови криптографічних конструкцій із врахуванням їх можливого уявлення функціями багатозначної логіки. Оскільки, найуживанішою довжиною сучасних S-блоків є довжина $N = 256$, йдеться, у першу чергу, про врахування криптографічної якості компонентних булевих функцій, 4-функцій та 16-функцій. Зараз вже створено методи синтезу S-блоків, які характеризуються високою криптографічною якістю як при представленні компонентними булевими функціями, так і компонентними функціями багатозначної логіки. Зокрема, відомий метод синтезу S-блоків, що відповідають суворому лавинному критерію компонентних 4-функцій та критерію максимального лавинного ефекту компонентних булевих функцій [3]. Однак, як показують проведені дослідження,

отримані у роботі [3], результати можуть стати основою для побудови більш досконалих методів синтезу S-блоків, які одночасно відповідатимуть як суворому лавинному критерію компонентних булевих функцій та 4-функцій, так і критерію кореляційного імунітету компонентних булевих функцій, що означає ідеальність їх матриць коефіцієнтів кореляції.

Метою цієї роботи є підвищення криптографічної якості підстановлювальних конструкцій сучасних шифрів шляхом розробки методу синтезу високоякісних S-блоків на основі функцій багатозначної логіки.

Застосовувані критерії криптографічної якості

Розглянемо основні критерії криптографічної якості, у відповідності до яких виконуватиметься синтез S-блоків.

2.1. Суворий лавинний критерій

Визначення відповідності S-блока суворому лавинному критерію при його представленні булевими функціями базується на дослідженні його компонентних булевих функцій за допомогою наступних визначень.

Визначення 1 [4]. Похідною за напрямом $u \in V_k$ булевої функції f називається булева функція

$$D_u f(x) = f(x) \oplus f(x \oplus u), \tag{1}$$

де V_k — лінійний векторний простір двійкових векторів довжини k, $\oplus$ — підсумовування по модулю 2.

Визначення 2 [4]. Булева функція $f(x)$ задовольняє критерію розповсюдження помилки щодо вектора $u \in V_k$ — КР(u) якщо її похідна за напрямом u є збалансованою функцією, тобто

$$p\{f(x) = f(x \oplus u)\} = 0.5. \tag{2}$$

Визначення 3 [4]. Булева функція f задовольняє строгому лавинному критерію (СЛК), якщо вона задовольняє критерію розповсюдження помилки КР(u) щодо всіх векторів ваги Гемінґа 1, тобто

$$p\{f(x) = f(x \oplus u)\} = 0.5, \quad \forall u \in V_k, \quad wt(u) = 1. \tag{3}$$

При представленні S-блока компонентними функціями багатозначної логіки для дослідження його відповідності строгому лавинному критерію відбувається на основі наступних визначень.

Визначення 4 [5]. Вагою $\varpi(u)$ q-значного вектора назвемо кількість його ненульових компонентів.

Визначення 5 [5]. Похідною функції f у напрямку вектора u назвемо функцію

$$D_u f(x) = f(x \underset{q}{\oplus} u) - f(x) \,(\mathrm{mod}\, q), \tag{4}$$

де $\underset{q}{\oplus}$ означає додавання по модулю q.

Визначення 6 [5]. Функція q-значної логіки $f(x)$ задовольняє строгому лавинному критерію, якщо її похідні за напрямами u одиничної ваги $\varpi(u) = 1$ є збалансованими функціями, тобто їх значення $0,1,...,q-1$ приймаються з рівними

ймовірностями: $p(D_u f(x) = i(\mathrm{mod}\, q)) = 1/q$ для всіх $i = 0,1,...,q-1$. Інакше висловлюючись, $K^0 = K^1 = ... = K^{q-1}$, де K^i — кількість наборів значень змінних, у яких похідна набуває значення i.

2.2. Критерій кореляційного імунітету

Визначення відповідності S-блока критерію кореляційного імунітету відбувається шляхом дослідження його компонентних булевих функцій на основі наступних визначень.

Визначення 7 [6]. Підфункцією булевої функції $f(x)$, $x \in V_k$ називається функція f', отримана підстановкою в f констант "0" або "1" замість частини змінних. Якщо підставимо в функцію f константи $\sigma_{i_1},\cdots,\sigma_{i_s}$ замість змінних $x_{i_1},\cdots,x_{i_s}$, відповідно, то отримана підфункція позначається $f^{\sigma_{i_1},\cdots,\sigma_{i_s}}_{x_{i_1},\cdots,x_{i_s}}$. Якщо замість змінної x_i константа не підставлена, то x_i називається вільною змінною.

Визначення 8 [6]. Булева функція $f(x)$, $x \in V_k$ називається кореляційно-імунною порядку m, $1 \le m \le k$, якщо вага Геммінга буде дорівнювати $wt(f') = wt(f)/2^m$, для будь-якої її підфункції f' від $k-m$ змінних.

Визначення кореляційного імунітету тісно пов'язане з такою характеристикою S-блока, як його матриця коефіцієнтів кореляції [7] $R = \left\| \rho_{\nu,\mu} \right\|$, $\nu, \mu = 1,2,...,k$, елементи якої обчислюються відповідно до наступної формули

$$r_{\nu,\mu} = 1 - 2^{-(k-1)} \sum_{z=1}^{N} \left(x_{z,\nu} \oplus y_{z,\mu} \right) = 0, \quad \nu,\mu = \overline{1,k}, \tag{5}$$

де $\{x_i\}$ і $\{y_j\}$ — двійкові вектори входу та виходу S-блока.

Відомо, що якщо всі компонентні булеві функції S-блока є кореляційно імунними порядку $m = 1$, то такий S-блок характеризується ідеальною матрицею коефіцієнтів кореляції, тобто $\rho_{\nu,\mu} = 0$, $\nu, \mu = 1,2,...,k$.

Метод синтезу криптографічно високоякісних S-блоків

Дослідження показали, що побудова S-блоків, що характеризуються високою криптографічною якістю як компонентних булевих функцій, так і компонентних функцій багатозначної логіки, може здійснюватися у рекурентний спосіб.

В якості основи роботи представленого методу застосовується метод побудови S-блоків, що відповідають СЛК компонентних 4-функцій та критерію максимального лавинного ефекту компонентних булевих функцій, який було запропоновано у роботі [3], та який наводимо для повноти викладу матеріалу.

Метод М1

Крок 1. В якості вхідного матеріалу для даного методу буде використовуватися множина S-блоків довжини $N = 16$, що відповідають СЛК 4-функцій, які були побудовані у [5]. Дана множина має потужність $J = 245760$.

Крок 2. Задається функція F_m, яка представляє собою старшу компонентну 4-функцію в розкладанні S-блоку на 4-функції.

Крок 3. Формується множина з 4-х перестановок у відповідності з наступним правилом

$$p_j = x \underset{4}{\oplus} (j \circ d), \quad x = 0,1,...,N-1, \quad j = 0,1,2,3, \tag{5}$$

де d — один з векторів довжини $k = \log_4 N$ з 1 на одній зі своїх позицій, вектор x пробігає четвіркові представлення чисел від 0 до $N-1$, $\underset{4}{\oplus}$ – додавання по модулю 4, $\circ$ — символ поелементного множення четвіркового представлення числа d на значення j.

Крок 5. Збільшуємо довжину S-блоку до значення $4N$ використовуючи наступну конструкцію

$$G_0 = \{S \mid S(p_1) \mid S(p_2) \mid S(p_3)\}. \quad (6)$$

Крок 6. Будуємо новий бієктивний S-блок довжини $4N$, що відповідає суровому лавинному критерію компонентних 4-функцій за наступним правилом

$$S_1 = \{G_1 \cdot 4^k + G_0\}, k = \log_4 N. \quad (7)$$

Проведені експерименти показують, що на основі множини S-блоків довжини $N = 16$, які були отримані в [5], шляхом використання розробленого методу можуть бути отримані S-блоки практично цінної довжини $N = 256$, що відповідають одночасно СЛК компонентних 4-функций та критерію максимального лавинного ефекту булевих функцій.

Варто зазначити, що кількість S-блоків сильно залежить від значення обраних параметрів c_1, c_2, c_3, c_4, а також від обраного вектору напрямку d. Наприклад, нехай задані наступні параметри: довжина S-блоку $N = 256$, параметри $c_1 = 0, c_2 = 1, c_3 = 2, c_4 = 3$ на першій та другій ітерації використання методу, а також значення $d = [0\ 1]$ на першій ітерації використання методу і $d = [0\ 0\ 1]$ на другій ітерації використання методу.

Тоді отримуємо, що з множини $J = 245760$ S-блоків довжини $N = 256$, отриманих на основі множини S-блоків довжини $N = 16$ [5], $J_1 = 3968$ S-блоків одночасно відповідають СЛК компонентних 4-функцій і критерію максимального лавинного ефекту компонентних булевих функцій.

Означена множина S-блоків є основою для побудови високоякісних S-блоків на основі запропонованого у даній роботі Методу М2, який представимо у вигляді конкретних кроків.

Метод М2

Крок 1. Застосовуючи Метод М1 виконати синтез множини з $J_1 = 3968$ високоякісних S-блоків довжини $N = 256$, що відповідають строгому лавинному критерію компонентних 4-функцій та критерію максимального лавинного ефекту компонентних булевих функцій.

Крок 2. Пробігаючи усю множину S-блоків, отриману на *Кроці 1*, виконати їх декомпозицію на компонентні 4-функції. Розкладаючи отримані 4-функції на 2 компонентні булеві функції, виділити з них такі, у яких обидві компонентні булеві функції відповідають умовам СЛК.

Після виконання *Кроку 2* ми отримуємо множину 4-функцій, потужність якої складає 14336 функцій. Одна з таких функцій має наступний вигляд

$$F_{41} = [0, 1, 3, 3, 2, 2, 2, 1, 2, 0, 3, 0, 1, 0, 3, 1, 1, 3, 3, 0, 2, 2, 1, 2, 0, 3, 0, 2, 0, 3, 1, 1, 3, 3, 0, 1, 2, 1, 2, 2, 3, 0, 2, 0, 3, 1, 1, 0, 3, 0, 1, 3, 1, 2, 2, 2, 0, 2, 0, 3, 1, 1, 0, 3, 2, 0, 0, 1, 3, 3, 2, 3, 1, 0, 1, 3, 1, 0, 2, 2, 0, 0, 1, 2, 3, 2, 3, 3, 0, 1, 3, 1, 0, 2, 2, 1, 0, 1, 2, 0, 2, 3, 3, 3, 1, 3, 1, 0, 2, 2, 1, 0, 1, 2, 0, 0, 3, 3, 3, 2, 3, 1, 0, 1, 2, 1, 0, 2, 1, 1, 2, 3, 0, 3, 0, 0, 1, 2, 0, 2, 1, 3, 3, 2, 1, 2, 3, 1, 3, 0, 0, 0, 2, 0, 2, 1, 3, 3, 2, 1, 2, 3, 1, 1, 0, 0, 0, 3, 0, 2, 1, 2, 3, 2, 1, 3, 3, 1, 1, 2, 0, 0, 3, 0, 2, 1, 2, 0, 2, 1, 3, 3, 2, 3, 0, 2, 0, 1, 1, 1, 3, 1, 3, 2, 0, 0, 3, 2, 3, 0, 2, 2, 1, 1, 1, 0, 1, 3, 2, 3, 0, 3, 2, 0, 0, 2, 2, 3, 1, 1, 0, 1, 3, 2, 3, 1, 3, 2, 0, 0, 2, 2, 3, 0, 1, 0, 1, 1, 2, 3, 1, 3, 2, 0, 0, 3]. \quad (8)$$

Крок 3. З отриманої множини 4-функцій, необхідно виділити такі, що є унікальними.

Після проведення даної процедури видалення дублікатів з даної множини отримуємо в решті всього 769 підходящих функцій.

Крок 4. Виконуючи композицію отриманих 4-функцій між собою відповідно до теореми [8], генеруємо множину S-блоків, відбираючи ті, що є бієктивними.

Після виконання *Кроку 4* отримуємо множину, потужність якої складає $J = 117588$ унікальних S-блоків.

В якості прикладу у табл. 1 наведемо один з таких S-блоків.

Таблиця 1

Приклад високоякісного S-блоку, що відповідає СЛК булевих та 4-функцій

S	**00**	**01**	**02**	**03**	**04**	**05**	**06**	**07**	**08**	**09**	**A**	**B**	**C**	**D**	**E**	**F**
00	05	00	0A	7A	5B	A1	C2	65	BF	67	DB	F4	1C	91	EE	BC
01	14	1E	4E	19	B5	D6	79	6F	7B	EF	C8	83	A5	F2	80	20
02	22	52	2D	28	EA	4D	73	89	F3	DC	97	4F	C6	94	34	B9
03	66	31	3C	36	51	47	9D	FE	E0	AB	53	C7	A8	08	8D	DA
04	41	4B	BB	46	E2	03	A6	98	A4	18	35	FC	D2	2F	FD	5D
05	5F	8F	5A	55	17	BA	AC	F6	2C	09	C0	B8	33	C1	61	E6
06	93	6E	69	63	8E	B0	CA	2B	1D	D4	8C	30	D5	75	FA	07
07	72	7D	77	A7	84	DE	3F	92	E8	90	04	21	49	CE	1B	E9
08	88	F8	87	82	40	E7	D9	23	59	76	3D	E5	6C	3E	9E	13
09	CC	9B	96	9C	FB	ED	37	54	4A	01	F9	6D	02	A2	27	70
A	AF	AA	A0	D0	F1	0B	68	CF	15	CD	71	5E	B6	3B	44	16
B	BE	B4	E4	B3	1F	7C	D3	C5	D1	45	62	29	0F	58	2A	8A
C	39	C4	C3	C9	24	1A	60	81	B7	7E	26	9A	7F	DF	50	AD
D	D8	D7	DD	0D	2E	74	95	38	42	3A	AE	8B	E3	64	B1	43
E	EB	E1	11	EC	48	A9	0C	32	0E	B2	9F	56	78	85	57	F7
F	F5	25	F0	FF	BD	10	06	5C	86	A3	6A	12	99	6B	CB	4C

У табл. 2 наведемо значення ваги Гемінґа похідних компонентних булевих функцій S-блока (табл. 1) для всіх векторів u_j одиничної ваги.

Таблиця 2

Відповідність вимогам СЛК компонентних булевих функцій синтезованого високоякісного S-блоку

u_j	$wt(D_{f_1})$	$wt(D_{f_2})$	$wt(D_{f_3})$	$wt(D_{f_4})$	$wt(D_{f_5})$	$wt(D_{f_6})$	$wt(D_{f_7})$	$wt(D_{f_8})$
00000001	128	128	128	128	128	128	128	128
00000010	128	128	128	128	128	128	128	128
00000100	128	128	128	128	128	128	128	128
00001000	128	128	128	128	128	128	128	128
00010000	128	128	128	128	128	128	128	128
00100000	128	128	128	128	128	128	128	128
01000000	128	128	128	128	128	128	128	128
10000000	128	128	128	128	128	128	128	128

Дослідження результатів, представлених у табл. 2 підтверджує відповідність S-блоку, представленого у табл. 1 умовам СЛК компонентних булевих функцій. У табл. 3 представлено значення кількостей K^0, K^1, K^2, K^3 елементів 0, 1, 2, 3 у похідних компонентних 4-функціях S-блока (табл. 1) для всіх векторів u_j одиничної ваги $\varpi(u_j) = 1$.

Таблиця 3

Відповідність вимогам СЛК компонентних 4-функцій синтезованого високоякісного S-блоку

u_j	$f_{41}: K^0 / K^1 / K^2 / K$	$f_{42}: K^0 / K^1 / K^2 / K$	$f_{43}: K^0 / K^1 / K^2 / K$	$f_{44}: K^0 / K^1 / K^2 / K$
0001	64/64/64/64	64/64/64/64	64/64/64/64	64/64/64/64
0002	64/64/64/64	64/64/64/64	64/64/64/64	64/64/64/64
…	…	…	…	…
3333	64/64/64/64	64/64/64/64	64/64/64/64	64/64/64/64

Побудована множина високоякісних S-блоків, зокрема, S-блок, наведений у табл. 1 характеризується також ідеальною матрицею коефіцієнтів кореляції, тобто відповідністю компонентних булевих функцій критерію кореляційного імунітету порядку $m = 1$. Наприклад, матриця коефіцієнтів кореляції S-блоку (табл. 1) має наступний вигляд

$$R = \begin{bmatrix} 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \end{bmatrix}. \qquad (9)$$

Висновки

Відзначимо основні результати проведених досліджень:

1. Запропоновано метод синтезу великої множини з $J = 117588$ криптографічно високоякісних S-блоків довжини $N = 256$, що відповідають суворому лавинному критерію компонентних булевих функцій, суворому лавинному критерію компонентних 4-функцій, а також критерію кореляційного імунітету компонентних булевих функцій, тобто володіють ідеальними матрицями коефіцієнтів кореляції.

2. Актуальна довжина S-блоків $N = 256$, їх відповідність критеріям криптографічної якості як у сенсі представлення булевими функціями, так і у сенсі представлення функціями багатозначної логіки дозволяють рекомендувати їх до практичного застосування як для покращення роботи існуючих шифрів, так і для побудови нових перспективних криптоалгоритмів. При цьому велика потужність множини побудованих S-блоків дозволяє застосовувати їх у якості довгострокового ключа.

Список літератури

1. Соколов А.В. Новые методы синтеза нелинейных преобразований современных шифров. Lap Lambert Academic Publishing, Germany 2015. 100 p.
2. Baigneres T., Stern J., Vaudenay S. Linear cryptanalysis of non-binary ciphers. *International Workshop on Selected Areas in Cryptography*. Springer, Berlin, Heidelberg, 2007. P. 184-211.
3. Sokolov A.V., Radush V.V. A method for synthesis of S-boxes with good avalanche characteristics of component Boolean and quaternary functions. *Journal of Discrete Mathematical Sciences and Cryptography*. 2022. P. 1-12. URL: https://doi.org/10.1080/09720529.2021.1964727
4. Forrié R. The strict avalanche criterion: spectral properties of Boolean functions and an extended definition. *Conference on the Theory and Application of Cryptograph*y. Springer, New York, NY, 1988. P. 450-468.
5. Sokolov A.V., Zhdanov O.N. Strict avalanche criterion of four-valued functions as the quality characteristic of cryptographic algorithms strength. *Siberian Journal of Science and Technology*, 2019. Vol. 20, No. 2. P.183-190.
6. Camion P. On correlation-immune function. *Annual International Cryptology Conference*. Springer, Berlin, Heidelberg, 1991. P. 86-100.
7. Mazurkov M. I. Synthesis method of optimal substitution constructions based on the criterion of zero correlation between the output and input data vectors. *Radioelectronics and Communications Systems*. 2012. Vol. 55. No. 12. P. 533-543.
8. Kim K. Construction of DES-like S-boxes Based on Boolean Functions Satisfying the SAC. *Proc. of Asiacrypt'91*. Springer Verlag, 1991. P. 59-72.

THE METHOD FOR SYNTHESIS OF HIGH-QUALITY S-BOXES BASED ON MANY-VALUED LOGIC FUNCTIONS

V.V. Radush, A.V. Sokolov

National Odesa Polytechnic University
Ukraine, Odesa, 65044, Shevchenko Ave., 1. radiosquid@gmail.com

The cryptographic S-box is the crucial component of modern ciphers which determines their efficiency, cryptographic security, and performance. Today, the development of quantum cryptanalysis, as well as the appearance of possible attacks on cryptographic algorithms by describing them using many-valued logic functions made urgent the task of developing algorithms for the synthesis of S-boxes, which would be characterized by high quality not only when represented by component Boolean functions, but also with any other representation by component functions of many-valued logic. At the same time, most of the existing methods of synthesis of S-boxes presented in the literature are focused only on the research of their cryptographic quality when represented by component Boolean functions. In this paper, on the basis of S-boxes of length N=16, which corresponds to the strict avalanche criterion of component Boolean and 4-functions, we propose a method for synthesis of a set of high cardinality equal to J=117588 of S-boxes of practically valuable length N=256, which simultaneously corresponds the strict avalanche criterion of component Boolean functions, the strict avalanche criterion of component 4-functions, as well as the criterion of correlation immunity of component Boolean functions, i.e., they have ideal matrices of correlation coefficients between output and input vectors. The high cryptographic quality of the developed S-boxes when they are represented by component Boolean and 4-functions makes it possible to recommend them for practical use both in the tasks of increasing the effectiveness of existing cryptographic algorithms and in the development of promising ciphers, while the cardinality of the class of synthesized S-boxes allows them to be used as a long-term key.

Keywords: S-box, error propagation criterion, correlation immunity, many-valued logic function.

DOI 10.15276/imms.v12.no3.226
УДК 004.056

Informatics and Mathematical Methods in Simulation
Vol. 12 (2022), No. 3, pp. 226-235

ЗАХИСТ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ ВІД ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В КОНТЕКСТІ СУЧАСНИХ ГІБРИДНИХ ВІЙН

О.М. Симонова, І.І.Бобок

Національний університет «Одеська політехніка»,
просп. Шевченка, 1, Одеса, 65044,Україна; e-mail: simonova.a.m@ukr.net

Фішинг використовується для розповсюдження шкідливого програмного забезпечення і зараження мереж критичної інфраструктури. Починаючи з 2000 років фішинг набуває популярності у кіберзлочинців. Одну з перших великих, спроб було зроблено 2001 року, коли в хаосі після терактів 11 вересня зловмисники відправили своїм жертвам електронні листи нібито для перевірки їхньої особистості. Отримані дані було використано для крадіжки банківських даних. Електронна пошта стала одним із надійних засобів зв'язку в реальному часі, за допомогою якого величезна кількість людей і організацій обмінюються своїми повідомленнями та даними. Зі значним збільшенням кількості користувачів електронної пошти зловмисники використовують електронну пошту різними способами, щоб спонукати користувачів розкривати свої облікові дані. Прикладом використання електронної пошти для фішингової атаки є розповсюдження вірусу Petya та NotPety у 2017 році, який брав свій початок з української державної енергокомпанії та вважається частиною російсько-української гібридної війни. Питання протидії фішинговим атакам в Україні та у всьому світі загалом залишається гострим. Користувачі Інтернету постійно стикаються зі спробами заволодіння їх даними. Жертвами можуть стати також великі компанії, що, може поставити під загрозу безпеку держави, якщо фішингова атака є частиною кібервійни. У роботі був удосконалений алгоритм виявлення небезпечний електронних листів, який відрізняється від існуючих комплексним підходом аналізу з використанням раніше не застосованим у цьому напрямку методі, що дозволило підвищити ефективність аналізу з коротким часом обчислень. Результати даної роботи можуть бути використані для захисту інформаційно-телекомунікаційних мереж від розповсюдження шкідливого програмного забезпечення та/або витоку даних.

Ключові слова: фішинг, електрона пошта, кіберзбезпека, інформаційна безпека

Вступ

Вид ворожих дій, при якому атакуюча сторона не вдається до класичного військового вторгнення , а пригнічує супротивника, використовуючи комбінацію таємних операцій, диверсій, кібервійни, а також надаючи підтримку. повстанцям, які діяли на території ворога називається гібридною війною. При цьому військові дії можуть взагалі не вестися, і, з формальної точки зору, гібридна війна може відбуватися в мирний час.

Одною з високоефективних форм кіберзлочинності сьогодні є фішинг [2]. Фішинг – це різновид соціальної інженерії, який полягає в наступному: зловмисник-шахрай надсилає електронною поштою повідомлення, призначене для змушення людини розкрити конфіденційну інформацію зловмисникові [1] або розгорнути шкідливе програмне забезпечення в інфраструктурі жертви, поширеним прикладом чого є програми-вимагачі.

Відповідно з Radicati Group [3], загальна кількість користувачів електронної пошти на початку 2021 року становила приблизно 4,1 мільярда, і, за прогнозами, зросте до 4,5 мільярдів до кінця 2025 року, що робить питання боротьби з ним одним з найактуальніших сучасних питань кібербезпеки.

Зловмисники використовують повідомлення електронної пошти з переконливим вмістом як приманку для викрадення особистої інформації користувачів; електронний лист направляє користувача через гіперпосилання на веб-сайт, що належить злочинцям, який візуально копіює офіційний (законний) веб-сайт, де користувачеві пропонують ввести особисту та/або фінансову інформацію. Це дозволяє злочинцям отримати доступ до цієї цінної інформації, яку вони потім використовують для вчинення шахрайства або продажу. Кіберзлочинці також можуть обманом змусити користувачів завантажити шкідливі коди або зловмисне програмне забезпечення шляхом натиснення на посилання, вбудоване в електронний лист.

Актуальність теми роботи полягає у тому, що, незважаючи на існування багатьох методів та підходів для захисту користувачів від фішинг-атак [4-7], ця проблема не є вирішеною повною мірою, а питання захисту у цьому напрямку залишається доволі гострим, зокрема для нашої країни: за даними Національного координаційного центру кібербезпеки у 2021 році в Україні зафіксовано понад 400 тис. випадків фішингових атак [8]

Для боротьби з фішингом поштові клієнти використовують спам-фільтри, які відправляють підозрілі листи в карантин (папки спаму), а не в основну поштову скриньку користувача. Однак ці фільтри не завжди ефективні: з понад 555 000 фішингових листів, проаналізованих компанією хмарної безпеки Avanan в рамках свого Global Phish Report 2019 [9], 25% оминули заходи безпеки Office 365, в результаті чого потрапили до поштових скриньок потенційних жертв.

Мета роботи

Метою роботи є розробка алгоритму захисту пошти від фішингових атак, який може бути імплантовано у сучасний браузер.

Основна частина

Електронний лист складається з двох частин: заголовків та вмісту. У роботі пропонується алгоритм, який би враховував в аналізі на наявність фішингу обидві частини листа, використовуючи гібридний метод аналізу, та реалізація цього алгоритму шляхом створення розширення для браузера під назвою Athena logic.

Підробка електронної пошти – техніка, яка використовується під час атак зі спамом і фішингом, щоб змусити користувачів подумати, що повідомлення надійшло від особи чи організації, яку вони знають або якій можуть довіряти. Під час спуфінгу відправник підробляє заголовки електронної пошти, щоб клієнтське програмне забезпечення відображало шахрайську адресу відправника, яку більшість користувачів сприймають за чисту монету. Якщо вони не перевірять заголовок уважніше, користувачі побачать у повідомленні підробленого відправника. Якщо це ім’я, яке вони впізнають, вони, швидше за все, довірятимуть йому. Тож вони натискатимуть шкідливі посилання, відкриватимуть вкладені файли зловмисного програмного забезпечення , надсилатимуть конфіденційні дані та навіть переведуть корпоративні кошти.

У роботі пропонується проведення аналізу наступних частин заголовків електронного листа для запобігання фішингу:

— Return-Path;
— Reply-To;
— Received-SPF;
— DKIM (Domain Keys Identified Mail).

Адреса електронної пошти Return-Path містить інформацію про статус відправлення. Поштовий сервер зчитує вміст заголовка Return-Path для обробки повідомлень, які не можна доставити або повернути відправнику. Сервер-одержувач використовує це поле для ідентифікації «підроблених» електронних листів: він запитує всі дозволені IP-адреси, пов’язані з доменом відправника, і порівнює їх з IP-адресою автора повідомлення. Якщо вони не знайдуть збігів, лист відправляється в спам.

Адреса електронної пошти в полі Reply-To використовується для надсилання відповіді. У фальшивих електронних листах вона може відрізнятися від адреси відправника.

Received-SPF дозволяє одержувачу перевірити, що електронна пошта, яка нібито походить з певного домену, походить з IP-адреси, дозволеної адміністраторами цього домену. Адміністратор домену зазвичай авторизує IP-адреси, які використовують його власні вихідні MTA, включаючи будь-які проксі-сервери або смарт-хости [10].

При встановленні з'єднання протокол управління трафіком перевіряє IP-адресу відправника MTA і переконується, що віддалений хост доступний. Поштовий сервер-одержувач отримує команду HELO SMTP незабаром після встановлення з'єднання і команду Mail from: на початку кожного повідомлення. Обидва можуть включати в себе доменне ім'я. Верифікатор SPF запитує в системі доменних імен (DNS) відповідний SPF-запис, який, за наявності, ідентифікує IP-адреси, дозволені адміністратором домену. Це поле є дійсним, якщо воно має значення PASS.

DKIM перевіряє зміст повідомлень за допомогою цифрових підписів. Замість цифрових сертифікатів через DNS розповсюджуються ключі перевірки підпису. Таким чином, повідомлення асоціюється з доменним ім'ям.

Адміністратор DKIM-сумісного домену створює одну або більше пар асиметричних алгоритмів шифрування, потім відправляє закриті ключі підписуючим MTA і публікує відкриті ключі в DNS. DNS мітки структуровані у вигляді selector._domainkey.example.com, де селектор вказує пару ключів, а _domainkey - фіксоване ключове слово, за яким слідує назва підписаного домену, щоб публікація перебувала під контролем ADMD цього домену. Безпосередньо перед тим, як вставити повідомлення в транспортну систему SMTP, підписуючий MTA створює цифровий підпис, який охоплює вибрані поля заголовка і тіла (або тільки початок). Підпис повинен включати основні поля заголовка, такі як «Від кого», «Кому», «Дата» і «Тема», а потім додаватися до самого заголовка повідомлення як поле для відстеження.

Повідомлення можуть прийматися і відправлятися будь-якою кількістю ретрансляторів, і на кожному кроці підпис може бути перевірений шляхом отримання відкритого ключа з DNS [11]. Поки посередники не змінюють підписані частини повідомлення, підписи повідомлень DKIM залишаються дійсними. Це поле є дійсним, якщо воно має значення PASS.

Для аналізу вмісту листа у роботі використовується семантичний аналіз для порівняння слів та словосполучень. Порівняння здійснюється за допомогою двох словників: спаму та тональності (настроїв), аналізуючи слова, вирази та символи, як видимі, так і приховані для людського ока, за допомогою різних методів.

У роботі використовується словник OOPSpam та український тональний словник [12], який містить 3442 слова української мови, які мають не нейтральну тональність.

Мета аналізу настроїв полягає в аналізі певної кількості даних, щоб визначити різні почуття, виражені в них. Отримані почуття потім можуть бути предметом статистичних даних щодо загального відчуття спільноти. Прикладом

використання тональності тексту є робота Мангурі та ін. [13], які проводили аналіз настроїв записів користувачів у Twitter щодо спалахів COVID-19 у всьому світі.

Сентимент-аналіз дозволяє аналізувати листи «вимагачі», «жебраки» або «благодійні», які можуть бути надіслані з реальних адрес та не містити жодного посилання. У цьому разі фішери використовують як зброю слова, щоб викликати у жертви конкретні емоції та відчуття. Зазвичай виділяють два види емоцій: позитивні та негативні, виконуючи класифікацію за двома класами, для якої в роботі використовується лексичний аналіз.

Підхід, заснований на лексичному аналізі, полягає у виведенні емоцій, які викликає речення, за допомогою семантичного аналізу слів. Цей підхід включає класифікацію речення за допомогою вже існуючих екземплярів речень, для яких емоції ідентифіковано, для чого використовується словник. Кожне слово тексту зіставляється зі словником; якщо знайдене співпадіння, то тональність тексту зростає.

Словник спаму містить у собі слова та словосполучення з типовою лексикою спаму.

Зміст листа може містити посилання. У цьому випадку метою зловмисника є перенаправлення жертви на певний веб-ресурс, куди зловмисник намагається впровадити шкідливе програмне забезпечення, використовуючи вразливості в самій сторінці або при переході в браузері.

URL-фішинг – це шахрайська практика заманювання людей на фальшиві сайти з переконливим змістом, де вони завантажують шкідливе програмне забезпечення або розкривають конфіденційну інформацію, таку як імена користувачів, паролі та банківські реквізити. Один з найпоширеніших прикладів такої атаки, коли шахраї імітують компанію та надсилають електронного листа з наступним повідомленням: «Ваш обліковий запис заблоковано. Відновити його можна за посиланням». Ошуканий користувач переходить за посиланням і несвідомо завантажує шкідливе програмне забезпечення або переходить на підроблений веб-сайт, який виглядає легітимно. Після переходу за посиланням користувач може стати жертвою різного роду XSS-атак. Суть цих атак полягає у виконанні скрипту в браузері та його подальшій взаємодії з сервером зловмисника. Ці операції відкривають доступ до даних браузера і дозволяють ввести в нього експлойтів, а також викрадати файли cookie, дані авторизації або, наприклад, здійснювати HTTP-запити від імені користувача.

За даними Звіту про розслідування порушень даних [14] близько 91% порушень безпеки починаються з фішингової атаки, і багато з них включають шкідливі посиланням на підроблені сайти.

У роботі URL-адреса аналізується за наступними критеріями:

- наявність символу «@»;
- довжина URL-адреси;
- кількість скісних рисок.

Зловмисники часто використовують подвійні скісні риски, щоб приховати шахрайську частину URL-адреси. Якщо URL-адреса містить забагато символів «/», вона є фішинговою, в іншому випадку - легітимною.

Підрахунок кількості символів в URL-адресі є важливою характеристикою для виявлення шахрайських джерел. Зловмисники використовують довгі URL-адреси, щоб приховати шахрайську частину адреси в адресному рядку. Таким чином, видима частина адресного рядка містить легітимну URL-адресу, яка може вводити в оману. Якщо довжина URL-адреси перевищує 35-символьний ліміт, джерело вважається підозрілим, в іншому випадку джерело легітимне [15].

Символ равлика «@» використовується для перенаправлення трафіку на інший, як правило шахрайський, сайт, доменне ім'я якого одразу супроводжується символом @. Наприклад, http://op.edu.ua@download.file.com перенаправить користувача на download.file.com замість op.edu.ua. Усе, що стоїть перед равликом, відкидається. Як правило, цей синтаксис сьогодні практично не використовується. Так, якщо в адресному рядку з'являється символ "@", то URL-адреса вважається підозрілою, в іншому випадку - легальною.

З урахуванням вищенаведеного пропонується наступний алгоритм захисту електронної пошти від фішингових атак, блок-схема якого наведена на рис. 1.

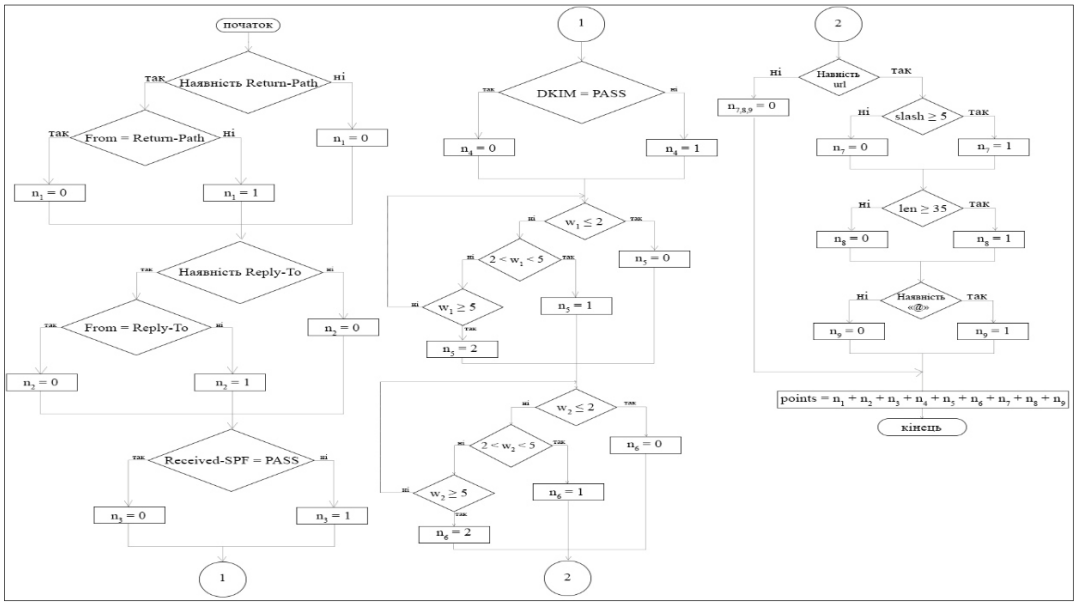


Рис. 1 Блок-схема розробленого алгоритму

Крок 1. Перевірка Return-Path, на виході якої отримуємо n_1 – бали фішингу за рівність *From = Return-Path*. Спочатку перевіряється наявність заголовка Return-Path. У деяких випадках, наприклад, при автоматичному повідомлені від системи безпеки, цей заголовок може бути відсутній. Якщо поле заголовка знайдено, воно зіставляється з полем заголовка From: при співпадінні $n_1 = 0$, якщо збігів не знайдено – $n_1 = 1$.

Крок 2. Перевірка Reply-To, на виході якої отримуємо n_2 – бали фішингу за рівність From = Reply-To. Спочатку перевіряється наявність заголовка Reply-To. Якщо поле заголовка знайдено, воно зіставляється з полем заголовка From: при співпадінні $n_2 = 0$, якщо збігів не знайдено – $n_2 = 1$.

Крок 3. Перевірка заголовка Received-SPF, де отримуємо n_3 – бали фішингу за рівність *Received-SPF = PASS*. При співпадінні $n_3 = 0$, якщо збігів не знайдено – $n_3 = 1$.

Крок 4. Перевірка співпадіння DKIM і PASS (n_4): при співпадінні $n_4 = 0$, якщо збігів не знайдено – $n_4 = 1$.

Після аналізу заголовків, алгоритм переходить до аналізу вмісту листа.

Крок 5. Сентимент аналіз, на виході якого отримаємо n_5 – кількість балів за перевірку листа за словником тональності: кожне слово листа зіставляється зі словником, при виявленні збігів (w_1) відбувається перевірка умов. Якщо збігів менше 2 – $n_5=0$, якщо у діапазоні між 2 та 5 – $n_5=1$, якщо більше 5 – $n5=2$.

Крок 6. Аналіз перевірки листа за словником спаму, на виході якої отримуємо n_6 – кількість балів за перевірку листа за словником спаму. Кожне слово листа зіставляється зі словником, при виявленні збігів (w_2) відбувається

перевірка умов. Якщо збігів менше двох – $n_6=0$, якщо у діапазоні між двома та п'ятьома – $n_6=1$, якщо більше п'яти, то $n_6=2$.

У обох випадках якщо кількість збігів $w_n > 5$, n – номер словника, то бали фішинга дорівнюють 2. Зловмисники мають на меті приховати свою особистість та за допомогою маніпулятивних дій – речень – завдати користувачеві матеріальної або психологічної шкоди. У роботі припускається, що зловмисники можуть використовувати тактики маркетингу для збільшення імовірності ввести потенційну жертву в оману. Однією з таких тактик є метод «холодного листа». Холодний лист – це перший лист, який надсилається потенційному клієнту, тобто перший контакт з людиною. Дослідження [16-17] показали, що ідеальна довжина для листа (щоб він міг вважатися «холодним») варіюється від 50 до 200 слів. На основі цього отримано, що кількість слів-збігів не може перевищувати 10% від загальної кількості слів листа (табл. 1) та обрано середнє значення з можливих.

Таблиця 1

Відсоток збігів w_n

Кількість слів	Відсоток збігів, %
50	10
75	6,7
100	5
125	4
150	3,3
175	2,8
200	2,5

Відповідно до запропонованого алгоритму:

Крок 7. Перевірки на наявність посилань. Якщо посилання не знайдено, то $n_{7,8,9}$ – кількість балів фішингу за кожний критерій, буде дорівнювати 0. У іншому випадку:

7.1. Перевірка URL-посилань на кількість символів «/» – *slash*, на виході якої отримуємо n_7 – кількість балів фішингу за цей критерій. Якщо $slash \geq 5$ – $n_7 = 1$, в іншому випадку – $n_7 = 0$.

7.2. Перевірка URL-посилань на загальну кількість символів (*len*), на виході якої отримуємо n_8. Якщо $len \geq 35$ – $n_8 = 1$, в іншому випадку – $n_8 = 0$.

7.3. Перевірка на наявність в URL символу равлика «@», та, якщо він є, кількість балів за дану перевірку (n_9) дорівнюватиме 1, в іншому випадку – 0.

У таблиці 2 відображена максимальна кількість балів, яку може отримати кожний критерій аналізу окремо.

Таблиця 2

Розподіл балів фішингу

Заголовки					Вміст листа			
Return-Path (n_1)	Reply-To (n_2)	Received-SPF (n_3)	DKIM (Domain Keys Identified Mail (n_4)	Словник тональності тексту (n_5)	Словник «спаму» (n_6)	Наявність посилання		
						Символ @ (n_7)	Кількість // (n_8)	Довжина url (n_9)
1	1	1	1	2	2	1	1	1

Крок 8. Отримання загальної кількості балів: $points = n_1 + n_2 + n_3 + n_4 + n_5 + n_6 + n_7 + n_8 + n_9$, де *points* – загальна кількість балів.

Крок 9. Висновок. Небезпечність листа залежить від кількості балів (табл. 3).

Таблиця 3

Залежність результату перевірки листа від значення загальної кількості балів

Результат	Кількість балів (points)
Небезпечно	points>3
Сумнівно	2 ≤ points ≤ 3
Безпечно	points<2

Користувачі Інтернету можуть використовувати розширення браузера, щоб оптимізувати його використання. Розширення веб-браузера – це доповнення до обраного користувачем веб-переглядача, які можуть вносити зміни на стороні клієнта, щоб змінити спосіб відображення веб-сторінок або надавати користувачеві інструменти, які допомагають йому під час перегляду Інтернету.

Розширення браузера можна використовувати для виявлення різних форм фішингових атак, наприклад, «GoldPhish» — це розширення Internet Explorer, яке використовується для виявлення фішингових веб-сторінок.

Розширення для браузера Athenalogic було розроблено для того, щоб дозволити користувачеві класифікувати електронні листи у своєму клієнті веб-пошти як легітимні або фішингові.

Як показано на рис. 2 станом на жовтень 2022 Google Chrome має 66,7% користувачів по світу [16] та близько 60% в Україні [17] (рис. 3). Саме тому розширення для веб-браузера було розроблено для Chrome, бо він залишається доступним для найбільшої кількості користувачів.

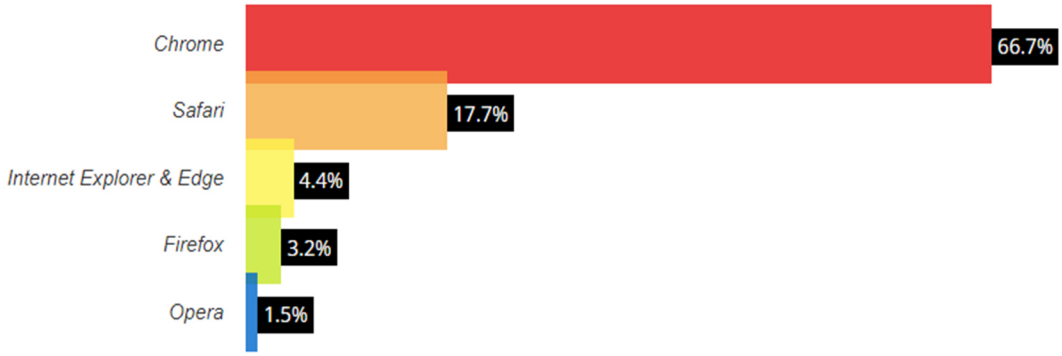


Рис. 2 Статистика популярності браузерів у світі

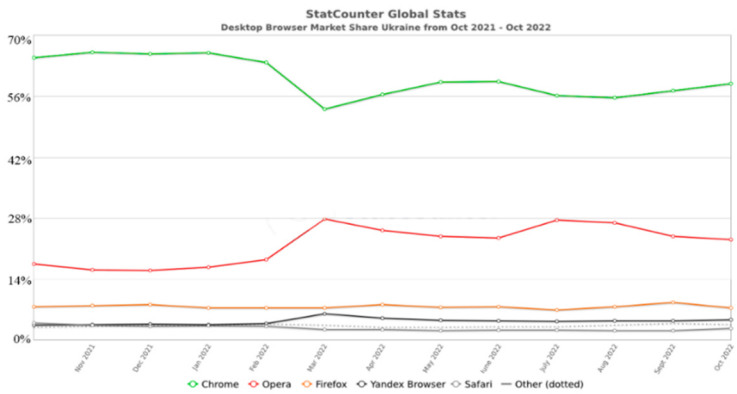


Рис. 3 Статистика популярності браузерів на ПК в України

Athena logic використовує розподіл балів для виявлення фішингових листів. Спочатку розширення аналізує заголовки, при кожному неспівпадінні додаються «бали фішингу» (далі – бали), потім вміст на наявність «спам-слів», слів з позитивним та/або негативним емоційним забарвленням і посилань за описаними вище критеріями.

Для оцінки ефективності розробленого в роботі розширення на практиці, було проведене дослідження, у якому порівнювались п’ять інших розширень (табл. 4, 5) з Athena logic.

Таблиця 4

Порівняння інших додатків для Chrome

Розширення	Опис	Переваги	Недоліки
MailTrout	Використовується метод на основі машинного навчання	Зручність використання; Розширення подається як освітній інструмент, який навчає користувачів самостійно виявляти фішингові електронні листи	Хибні спрацювання; великий час оброблень
Ter7AntiPhishing	Семантичний аналіз з використанням словника	Зручність використання	Малий відсоток вірно визначених фішингових листів; Лише для Gmail
PhishBlock Prediction	Аналізує url-адреси в листах Евристичний метод	Швидкий аналіз	Наявність певного відсотка помилково-позитивних результатів; Не переглядає вміст електронної пошти; Лише для Gmail
Detect spam emails	Семантичний аналіз з використанням словника	Зручність використання	Хибні спрацювання
Email Phishing Tool	Семантичний аналіз з використанням словника Аналізує url-адреси в листах Евристичний метод	Хороші результати на невеликих наборах даних.	Малий відсоток вірно визначених фішингових листів; Малий відсоток визначення фішингових url;

Таблиця 5

Результати дослідження

Розширення	Точність, %
MailTrout	48
Ter7AntiPhishing	31
PhishBlock Prediction	54
Detect spam emails	30
Email Phishing Tool	42
Athena Logic	94

Результати дослідження, представлені у табл. 5, показали ефективність Athena logic, що значно перевищує ефективність аналогів, та довели, що для успішного аналізу для виявлення фішингу, необхідно охоплювати обидві частини електронного листа. Так, розширення Ter7AntiPhishing та Detect spam emails показали низький відсоток точних результатів через залежність від словникового методу: листи з коротким та, на перший погляд, легітимним змістом, але з небезпечними посиланнями, вони виявили як безпечні.

Розширення PhishBlock Prediction безглузде у випадках відсутності у листах посилань. MailTrout у свою чергу сприймає легітимні листи за фішингові.

Висновки

У результаті виконання роботи був запропонований алгоритм виявлення фішингових листів, що використовує гібридний метод аналізу, та розроблена програмна реалізація цього методу у вигляді розширення для браузера Chrome. Розширення браузера можуть діяти як доступні інструменти безпеки, оскільки для використання вони потребують небагато технічних знань і можуть бути легко включені в стандартну онлайн-діяльність людини.

Завдяки своїй простоті створене розширення може бути особливо корисними для тих, хто має незначний досвід користування Інтернетом, і як інструменти безпеки можуть ефективно захистити найбільш вразливі групи.

В результаті порівняльного аналізу ефективності розробленого розширення браузера з існуючими аналогами встановлено, що він перевищує найкращий з існуючих на 40%.

Список літератури

1. Jansson K., Von Solms R., Phishing for phishing awareness. *Behaviour and Information Technology*. 2013.V32, #6, P.584-593
2. Alkhalil Z, Hewage C, Nawaf L., Khan I. Phishing Attacks: *A Recent Comprehensive Study and a New Anatomy*, 2021
3. Radicati S. Email statistics report. The Radicati Group, Inc; 2016.
4. Cisco Advanced Phishing Protection. URL: https://www.cisco.com/c/dam/en/us/products/collateral/security/cloud-email-security/at-a-glance-c45-740894.pdf
5. Office 365 Advanced Threat Protection. URL: https://docs.microsoft.com/ru-ru/microsoft-365/security/office-365-security/office-365-atp
6. Бойл П. Впровадження розширення браузера для виявлення фішингових електронних листів за допомогою обробки природної мови,
7. Gascon, H., Ullrich, S., Stritter, B., Rieck, K. Reading Between the Lines: Content-Agnostic Detection of Spear-Phishing Emails. Research in Attacks, Intrusions, and Defenses. 2018. *Lecture Notes in Computer Science*, Vol 11050. URL:https://doi.org/10.1007/978-3-030-00470-5_4
8. Ради національної безпеки і оборони України, НКЦК: у 2021 році в Україні зафіксовано вже майже 14 мільйонів інцидентів у сфері кібербезпеки. URL: https://www.rnbo.gov.ua/ua/Diialnist/4797.html
9. Global-Phish-Report 2019. URL: https://www.avanan.com/hubfs/2019-Global-Phish-Report.pdf
10. Klensin J. Simple Mail Transfer Protocol, 2008. URL: https://www.rfc-editor.org/info/rfc5321
11. Crocker D. DKIM Frequently Asked Questions. URL: https://www.dkim.org/info/dkim-faq.html
12. Ukrainian tone dictionary. URL: https://github.com/lang-uk/tone-dict-uk

13. Manguri K.N., Ramadhan R.R. Mohammed A.P. Twitter Sentiment Analysis on Worldwide COVID-19 Outbreaks. *Kurdistan Journal of Applied Research*. 2020. P. 54–65. URL: https://doi.org/10.24017/covid.8.
14. Data Breach Investigations Report - Executive Summary, 2017
15. Орунсолу А.А., Содия А.С.. Акинвале А.Т. Прогностическая модель для обнаружения фишинга. *Журнал Университета короля Сауда — компьютерные и информационные науки.* URL:https://doi.org/10.1016/j.jksuci.2019.12.005
16. Renahan M. The Ideal Length of a Sales Email, Based on 40 Million Emails. *HubSpot Blog*. URL: https://blog.hubspot.com/sales/ideal-length-sales-email.
17. Kristensen E. What's the Ideal Email Length?. *The Ecommerce Revenue Engine | Drip*. URL: https://www.drip.com/blog/ideal-email-length.
18. Browser and Platform Market Share, 2022. URL: https:// web.archive.org/web/20221018205527/https://www.w3counter.com/globalstats.php
19. Desktop Browser Market Share Ukraine. 2022. URL: https://gs.statcounter.com/browser-market-share/desktop/ukraine

PROTECTION OF INFORMATION AND TELECOMMUNICATION NETWORKS FROM MALICIOUS SOFTWARE IN THE CONTEXT OF MODERN HYBRID WARS

O.M. Symonova, I.I.Bobok

National Odesa Polytechnic University,
ave. Shevchenko, 1, Odesa, 65044, Ukraine; e-mail: simonova.a.m@ukr.net

Phishing is used to spread malicious software and infect critical infrastructure networks. Since 2000, phishing has been gaining popularity among cybercriminals. One of the first big attempts was made in 2001, when in the chaos after the September 11 attacks, attackers sent their victims e-mails allegedly to verify their identity. The obtained data was used to steal bank data. Email has become one of the reliable means of real-time communication through which a huge number of people and organizations share their messages and data. With the dramatic increase in the number of email users, attackers are using email in a variety of ways to trick users into revealing their credentials. An example of email being used for a phishing attack is the spread of the Petya and NotPety virus in 2017, which originated from a Ukrainian state energy company and is considered part of the Russian-Ukrainian hybrid war. The issue of countering phishing attacks in Ukraine and around the world in general remains acute. Internet users are constantly faced with attempts to get hold of their data. Large companies can also become victims, which can endanger the security of the state if a phishing attack is part of a cyber war. The work included an improved algorithm for detecting dangerous e-mails, which differs from the existing ones by a comprehensive approach to analysis using a previously unapplied method in this direction, which made it possible to increase the efficiency of the analysis with a short calculation time. The results of this work can be used to protect information and telecommunication networks from the spread of malicious software and/or data leakage.

Keywords: phishing, e-mail, cyber security, information security

DOI 10.15276/imms.v12.no3.236
УДК 681.51

Informatics and Mathematical Methods in Simulation
Vol. 12 (2022), No. 3, pp. 236-242

СИНТЕЗ ОДНОВИМІРНИХ СИСТЕМ КЕРУВАННЯ З ВРАХУВАННЯМ ШУМІВ ВИМІРЮВАННЯ

А. О. Стопакевич, О.А. Стопакевич

Державний університет інтелектуальних технологій та зв'язку,
1, Кузнечна, Одеса, 65029, stopakevich@gmail.com
Національний університет «Одеська політехніка»,
1, пр. Шевченка, Одеса, 65044, stopakevich@opu.ua

Мета роботи – розробити новий метод синтезу одновимірних систем автоматичного керування з П, ПІ та ПІД законів керування для статичних й астатичних об'єктів керування, метою якого є мінімізація впливу шуму вимірювань на динамічні властивості системи керування без ускладнення структури каналу керування. Сфера застосування методу – задачі стабілізації певних швидких процесів, які переважну частину свого часу керуються регуляторами в режимі, коли похибка керування близька до похибки вимірювання. Наприклад, це може бути стабілізація температури в теплообміннику чи регулювання витрати (тиску). Поставлена мета досягається шляхом розв'язку наступних задач: 1) розробка правил для регуляторів ПІД-типу для статичних та астатичних об'єктів керування з запізненням, які досягають гарантовану величину відношення вихідної дисперсії до вхідної (за моделлю білого шуму); 2) дослідити правила на моделі технологічного об'єкту, яка враховує особливості роботи засобів автоматизації в каналі керування.. Найбільш істотним результатом роботи є метод, який представляє набір нескладних правил, аналогічних до правил інших відомих методів настройки регуляторів ПІД-типу. Як еталонна модель об'єктів керування розглядається модель в вигляді поєднання ланки (інерційної чи інтегральної) першого порядку з запізненням, при чому метод є придатним й для важкокерованих об'єктів керування, тобто з наявним істотним чи домінуючим запізненням. На прикладі застосування розробленого методу для керування температурою в теплообміннику бражної колони з застосуванням ПІ-регулятора показано, що метод дозволяє знизити дисперсію на чверть у порівнянні з регулятором, отриманим за допомогою програми pidtune. Аналогічні результати досягаються й для інших регуляторів ПІД-типу.

Ключові слова: система керування, одновимірний регулятор, ПІД, білий шум, дисперсія, метод настройки

Вступ

Задача синтезу одновимірних систем керування може включати багато аспектів і є істотно багатокритеріальною [1-5]. Якщо розглядати лінійні моделі об'єктів керування, наприклад в передаточних функціях, то за такими моделями звичайно ставиться задача розробки регулятора, який відповідає певним прямим показникам якості та/або показникам робастності. Найбільш полярними параметрами в межах звичайної постановки задачі синтезу одновимірних САК часто є швидкість перехідних процесів та запас стійкості. За межі звичайної задачі винесено все те, що відноситься до особливостей програмно-технічної реалізації каналу керування, а саме проблема точності цифрової реалізації каналів керування, врахування особливостей роботи виконавчих механізмів та датчиків, чутливість регуляторів до зміни параметрів тощо.

Якщо розглядати типовий випадок одновимірного регулятора – регулятор ПІД-типу, то неповнота звичайної задачі при його застосуванні частіше за все ігнорується чи компенсується певними емпіричними методами. Одним з факторів, який звичайно ігнорується – це шум вимірювання, який присутній в будь-якому каналі керування. В роботі [6] продемонстровано, що наявність шумів вимірювання

в каналі керування робить динаміку системи автоматичного керування (САК) достатньо далекою від модельної за максимальними амплітудами відхилення та інтегральними показниками якості. Це продемонстровано на прикладі ПІ-регулятора для теплообмінного апарату.

Якщо ж додати Д-складову до регулятора, то виникають додаткові проблеми з реалізацією та роботою диференційної складової в реальних контурах керування [7]. Теоретично при керуванні Д-складова може збільшити швидкість перехідних процесів й зменшити коливальність, яку додає І-складова, однак тільки якщо параметр Д-складової підібраний вірно, коливальність може й погіршитись. Тим не менш, при технічній реалізації ці переваги можуть й не спрацювати, оскільки Д-складова буде реагувати на невраховані шуми вимірювання й мати похибку реалізації операції, що замість якісного керування буде лише зношувати виконавчий механізм. Частково проблема нейтралізується шляхом додавання фільтру нижніх частот (інерційну ланку з постійною часу біля $0.1\dot{}\ldots 0.2*T_d$), що робить регулятор постійним коефіцієнтом на високих частотах й може привести до формулювання 4-х параметричної задачі [9] з визначенням бажаної постійної часу фільтру реального диференціатора. Всі поширені правила настройки регуляторів ПІД-типу не застосовують 4-й параметр, як й приладові регулятори чи програмні системи часто не дозволяють його змінювати. Серед популярних методів настройки регуляторів ПІД-типу 4-й параметр дозволяє визначати MATLAB-програма pidtune, але параметри шуму при цьому не задаються. Задача може бути й ускладнена до 5-ти параметрів, якщо також додати параметр порядку знаменника реального диференціатора.

Альтернативний варіант до реального диференціатора запропонований в монографії [2] в якій рекомендується фільтрувати вихід всього ПІД-регулятора інерційною ланкою другого порядку. Фільтрувати можна також й вимірювання, що потенційно може зробити регулятор менш чутливим до шумів й збільшити робастність, але, з іншого боку, це змінює та уповільнює динаміку об’єкту керування (ОК). Це також збільшує кількість необхідний параметрів настройки регулятора.

Показовою є робота [10], у якій проаналізована задача синтезу системи керування з фільтром Баттенворта для сигналу вимірювання

$$F(s) = \frac{1}{0.5 \cdot T_f^2 \cdot s^2 + T_f \cdot s + 1}.$$

Розглядається проблема синтезу ПІ- та ПІД-регуляторів для ОК, представлених моделями в вигляді поєднання інерційної ланки першого порядку з запізненням та більш складними типами моделей. В роботі продемонстровано, що потужний фільтр знижує коливання керуючого впливу коштом зниження якості перехідних процесів, тому вибір постійної часу фільтру – окрема проблема. Більш того, невдалий вибір фільтру викликає додаткові проблеми з робастністю. Цікаво також, що порядок фільтру істотно впливає на динамічні показники системи керування й процедура вибору постійної часу фільтру орієнтується на відношення часу запізнення до постійної часу об’єкту. Зміна динамічних властивостей САК при застосуванням фільтру робить задачу зв’язаною, настройки регулятора треба розраховувати разом з параметрами фільтру. Ускладнення структури регулятора ускладнює також й проблеми цифрової реалізації регулятора, оскільки регулятор необхідно реалізовувати власноруч програмним чином. Крім того, введення фільтру накладає додаткові обмеження на вибір кроку дискретності САК.

У цілому, досвід промислової автоматизації показує що для складних інерційних технологічних процесів проблема врахування шумів звичайно жорстко не стоїть й часто не є першочерговою, так як їх інерційність є часто більшою за інерційність датчика. Звичайно задача керування каналами в таких об’єктах зводиться до застосування ПІ-закону керування для уникнення проблем з

диференційною складовою. Однак в технологічних схемах багатьох технологічних процесів присутні задачі стабілізації певних швидких процесів, які переважну частину свого часу керуються регуляторами в режимі, коли похибка керування близька до похибки вимірювання. Наприклад, це може бути стабілізація температури в теплообміннику чи регулювання витрати (тиску). Як правило, такі процеси описуються доволі точно моделями в вигляді поєднання ланки (інерційної чи інтегральної) першого порядку з запізненням. Для регуляторів таких процесів бажано, щоб вони виконували не тільки стабілізацію, але й були одночасно певним фільтром низьких частот. Однак розв'язувати багатопараметричні задачі для зменшення проблеми впливу шумів для таких простих контурів керування не є розповсюдженою інженерною практикою, більш практичним є спробувати нейтралізувати проблему шумів вимірювання в межах типового ПІД-закону, обравши задачу мінімізації дисперсії шумів як основний критерій синтезу САК.

Мета роботи

Мета роботи – розробити метод настройки регуляторів ПІД-типу, який мінімізує вихідну дисперсію керованої змінної в залежності від вхідної за певним законом. При чому метод не має ставити додаткових вимог: встановлення певних фільтр, перерахунок параметрів моделі та ін. Метод має представляти набір нескладних правил, аналогічних до правил інших відомих методів настройки регуляторів ПІД-типу. Як еталонна модель ОК розглядається модель в вигляді поєднання ланки (інерційної чи інтегральної) першого порядку з запізненням, при чому метод має бути придатним й для важкокерованих ОК, тобто з наявним істотним чи домінуючим запізненням.

Задачі роботи

В роботі будуть розв'язані наступні задачі: 1) розробити правила для регуляторів ПІД-типу, які керують статичними та астатичними ОК з запізненням і досягають гарантовану величину відношення вихідної дисперсії до вхідної (за моделлю білого шуму); 2) дослідити ефективність правил на моделі технологічного об'єкту, яка враховує особливості роботи засобів автоматизації в каналі керування.

Розробка правил настройки для регуляторів ПІД-типу

Правила застосовуються для моделі в вигляді ланки першого порядку з запізненням (FOPDT). Розглядаються як статичні (з самовирівнюванням), так і астатичні (без самовирівнювання) ОК. Відправною базою для розробки правил став удосконалений метод Циглера-Ніколсона [2], який для статичних ОК визначає пропорційну настройку регулятора k_p за фактором, який включає час запізнення τ, постійну часу T та коефіцієнт передачі k моделі ОК. В запропонованому методі фактор має вигляд $\pi \cdot T/(4\cdot\tau)$ для астатичних ОК й $\left(\pi \cdot T/(4\cdot\tau)+0.5\right)/k$ для статичних ОК. Також, основою методу для статичних ОК з ПІ та ПІД регуляторами є експериментально встановлена нами залежність $\omega\cdot\tau = f(T/\tau)$, показана на рис.1.

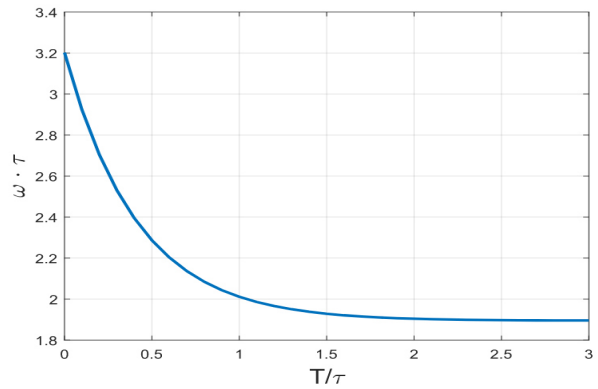


Рис. 1. Залежність $\omega \cdot \tau = f(T/\tau)$

Приведена на рис.1. залежність може бути описана формулою:

$$\omega \cdot \tau = 1.312 \cdot exp(-2.395 \cdot T / \tau) + 1.89 \cdot exp(0.0007932 \cdot T / \tau). \quad (1)$$

Розроблені формули настройки регуляторів ПІД-типу для FOPDT об'єктів при дії випадкових шумів вимірювань з оцінкою їх впливу на дисперсію виходу приведені в табл.1.

Таблиця 1

Розроблені формули настройки регуляторів ПІД-типу для FOPDT об'єктів при дії випадкових шумів вимірювань з оцінкою їх впливу на дисперсію виходу

Регулятор	Об'єкт	Настройка	Дисперсія виходу
k_p	$k \cdot e^{-\tau \cdot s} / (T \cdot s)$	$k_p = \pi \cdot T / (4 \cdot \tau)$	$\sigma_y = \sigma_u / k_p$
k_p	$k \cdot e^{-\tau \cdot s} / (T \cdot s + 1)$	$k_p = \left(\pi \cdot T / (4 \cdot \tau) + 0.5\right) / k$	$\sigma_y = \frac{\sigma_u \cdot k}{1 + k \cdot k_p}$
$k_p + \frac{k_i}{s}$	$k \cdot e^{-\tau \cdot s} / (T \cdot s + 1)$	$k_p = 0.9 \cdot \left(\pi \cdot T / (4 \cdot \tau) + 0.5\right) / k$ $k_i = 0.2 \cdot k_p \cdot \omega$	$\sigma_y = \frac{\sigma_u \cdot k}{1 + k \cdot k_i \cdot T}$
$k_p + \frac{k_i}{s} + k_d \cdot s$	$k \cdot e^{-\tau \cdot s} / (T \cdot s + 1)$	$k_p = 1.2 \cdot \left(\pi \cdot T / (4 \cdot \tau) + 0.5\right) / k$ $k_i = 0.32 \cdot k_p \cdot \omega,$ $k_d = 0.75 \cdot k_p / \omega$	$\sigma_y = \frac{\sigma_u \cdot k}{1 + k \cdot k_p \cdot T}$
$k_p + \frac{k_i}{s}$	$k \cdot e^{-\tau \cdot s} / (T \cdot s)$	$k_p = 0.9 \cdot \pi \cdot T / (4 \cdot \tau),$ $k_i = 0.2 \cdot T / \tau^2$	Залежність не встановлена, застосування не рекомендується
$k_p + \frac{k_i}{s} + k_d \cdot s$	$k \cdot e^{-\tau \cdot s} / (T \cdot s)$	$k_p = 0.3 \cdot \pi \cdot T / \tau,$ $k_i = 0.45 \cdot T / \tau^2,$ $k_d = 0.45 \cdot T$	

Дослідження правил настройки на моделі технологічного процесу

Розглянемо приклад застосування розробленого методу для керування температурою в теплообміннику бражної колони з застосуванням ПІ-регулятора.

Модель каналу «Витрата холодної води (% ходу виконавчого механізму) - температура води, що відходить (°С) має вигляд:

$$P_{\Delta G \to \Delta T_{\text{outer}}} = \frac{-0.285}{268 \cdot s + 1} \cdot e^{-74 \cdot s}$$

Приймемо номінал керованої змінної: 50°С, керуючого впливу: 70%.

Для вимірювання температури виберемо датчик ТСП-012-011 з показником теплової інерції, що дорівнює 15 с.

Виберемо крок дискретності системи керування рівним Δt=1с.

Тип регулятора: ПІ-регулятор виду з методом дискретизації Backward Euler.

Модель САК з датчиком показана на рис. 2.

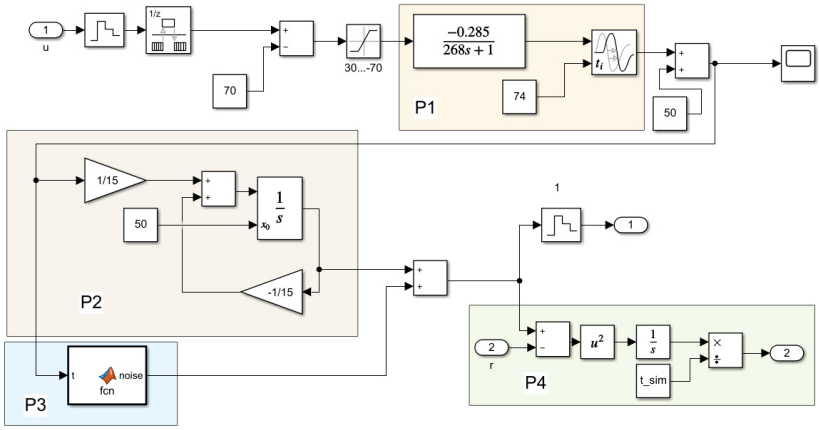


Рис. 2. Структурна схема моделі САК (підсистема Матлаб), яка вміщує модель каналу, датчика та розрахунок дисперсії керованої змінної

Модель об'єкту реалізуємо як підсистему. Входами підсистеми є керуючий вплив з регулятора u й завдання r. Частина P1 моделює динаміку каналу керування в відносних координатах. Частина P2 моделює інерційність давача. Частина P3 моделює похибку давача. Частина P4 розраховує дисперсію керованої змінної. Змінна t_sim визначає час моделювання.

Методика моделювання давача та код моделювання приведено в роботі [6].

Порівняємо метод синтезу, реалізований в функції pidtune (в блоці Simulink PID), та запропонований метод мінімізації дисперсії. Щоб зрівняти шанси регуляторів, зведемо модель об'єкту до FOPDT, оскільки з моделлю давача вона стала моделлю другого порядку. Використавши варіант методу Сімою для отримання FOPDT моделі, отримаємо редуковану модель виду

$$W_r = \frac{-0.285}{239.8006 \cdot s + 1} \cdot e^{-117.1632 \cdot s}.$$

Далі, для спрощення не будемо брати знак мінус в коефіцієнті при синтезі, а врахуємо його в зворотному зв'язку. Функція pidtune для дає такі коефіцієнти: k_p = 4.03, k_i = 0.016. Запропонований метод мінімізації дисперсії дає такі налаштування: k_p = 6.66, k_i = 0.0216.

Промоделюємо дві САК з ПІ-регуляторами й однаковими об'єктами по завданню. Зверху регулятор, що синтезовано pidtune, нижче – методом мінімізації дисперсії. Як бачимо на рис.3, дисперсія в другому випадку на 1/4 менша.

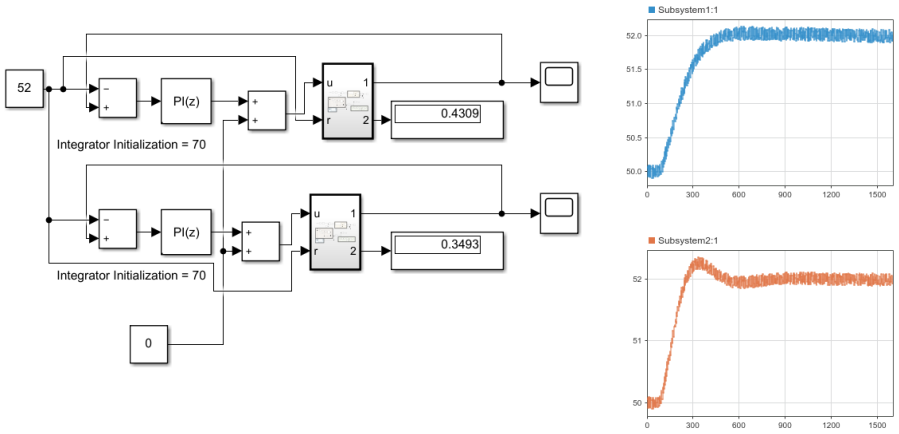


Рис. 3. Модель та результати моделювання двох САК за завданням. Якщо промоделювати за завданням й збуренням одночасно, то тенденція зберігається.

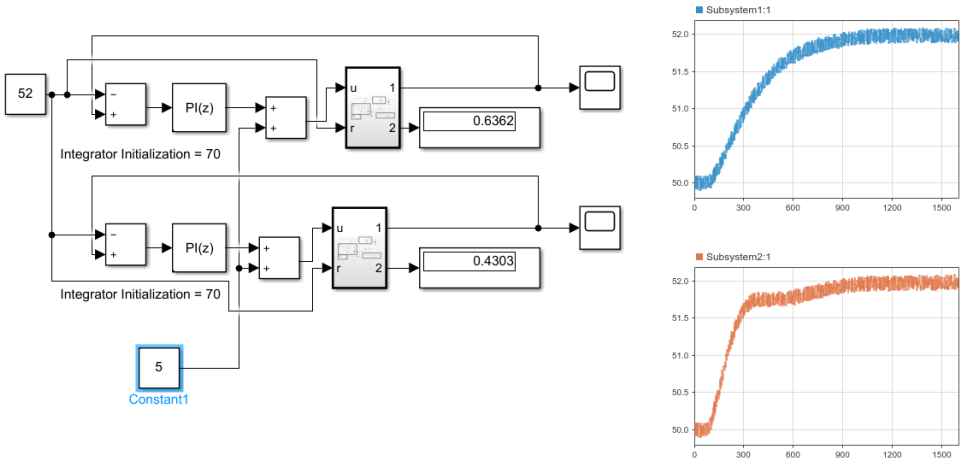


Рис. 4. Модель та результати моделювання двох САК за завданням та збуренням одночасно

Аналогічні до приведених результати досягаються й при використанні інших запропонованих правил.

Висновки

Розроблено метод синтезу одновимірних систем керування з типовими регуляторами ПІД-типу та об'єктів, динаміка яких описуються статичною чи астатичною FOPDT моделлю, який відрізняється тим, що дозволяє врахувати вплив дисперсії вимірювань на дисперсію керованої змінної. Формули метода базуються на врахуванні традиційного для настроювання регуляторів ПІД-типу відношення τ / T . Рекомендована сфера застосування методу – об'єкти з малими збуреннями, похибка керування в яких значної мірою залежить від шуму датчика, який можна оцінити по його нормованій похибці.

Список літератури

1. O'Dwyer A. Handbook of PI and PID Controller Tuning Rules. London : Imperial Colledge Press, 2006.
2. Åström K., Hägglund T. Advanced PID control. Research Triangle Park, NC: ISA, 2006.
3. Стопакевич А.О. Синтез регулятора в дискретному часі з заданим часом встановлення перехідного процесу. *Інформатика та математичні методи в моделюванні*. 2020. Т.10, №3-4. С. 208-221. https://doi.org/10.15276/imms.v10.no3-4.208
4. Stopakevych A., Stopakevych O., Tigariev A., Tigarieva T. A simple method for a precise solution of the digital optimal controllers design problem for SISO objects with delay. *Proceedings of O.S.Popov Odesa National Academy of Telecommunicaions*. 2019. No.2. P. 104-114.
5. Стопакевич А.А. Проектирование робастных регуляторов объектами с большим запаздыванием. *Восточно-европейский журнал передовых технологий*. 2016. Т. 1, №2 (79). С. 48-56. https://doi.org/10.15587/1729-4061.2016.59107
6. Стопакевич А. О. Моделирование погрешности датчика температуры при разработке высокоточных ИУС. *Збірник наукових праць Одеської державної академії технічного регулювання та якості*. 2015. №. 2. С. 85-88.
7. Vilanova R., Visioli A. (eds.). PID Control in the Third Millennium, Advances in Industrial Control. London: Springer-Verlag, 2012.
8. Денисенко В. ПИД-регуляторы: вопросы реализации. *СТА*. 2007. №4. С.86-97

9. Isaksson A.J., Graebe S.F. Derivative filter is an integral part of PID design. *IEE Proceedings - Control Theory and Applications*, 2002. Vol. 149, № 1. P. 41-45. https://doi.org/ 10.1049/ip-cta:20020111
10. Segovia V. R., Hägglund T., Åström K. Measurement noise filtering for PID controllers. *Journal of Process Control*. 2014. Vol. 24, № 4. P. 299–313. https://doi.org/10.1016/j.jprocont.2014.01.017

DESIGN OF SISO CONTROL SYSTEMS ACCOUNTING MEASUREMENT NOISES

Andrii Stopakevych, Oleksii Stopakevych

National University of Intellectual Technologies and Communications,
1, Kuznechna street, Odesa, 65029, Ukraine, stopakevich@gmail.com
National Odesa Polytechnic University,
1, Shevchenko Ave., Odesa, 65044, Ukraine, stopakevich@op.edu.ua

The paper aims to develop a new method of designing one-dimensional automatic control systems with P, PI, and PID control laws. The method scope is static and astatic plants, and it aims to minimize the influence of measurement noise on the dynamic properties of the control system. Achievement of this aim should be without complicating the structure of the control channel. The scope of the method is the problems of stabilization of relatively fast processes, which most of the time are controlled by regulators in the mode when the control error is close to the measurement error. Examples of such problems are: temperature stabilization in a heat exchanger or flow (pressure) control. The goal is achieved by solving the following tasks: 1) to develop rules for PID-type controllers for static and astatic control plants with a dead tune, which achieve a guaranteed value of the ratio of the output dispersion to the input (according to the white noise model); 2) to investigate the rules on the model of the technological plant, which takes into account the peculiarities of the automation in the control channel. The most significant result of the work is a method that represents a set of simple rules similar to the rules of other known methods of tuning PID-type controllers. A plant's reference dynamic mode is supposed in the form of a combination of a first-order aperiodic or integrating link with a dead time link. The method is also suitable for hard-controlled plants with a significant or dominant dead time. An example of the application of the developed method for controlling the temperature in the heat exchanger of a beer distillation column using a PI controller is demonstrated. It is shown that the method allows a reduction of the dispersion by a quarter compared to the controller obtained using the pidtune program. Similar results are achieved for other PID-type controllers.
Keywords. Control system, SISO controller, PID, white noise, dispersion, tuning method.

DOI 10.15276/imms.v12.no3.243
УДК 004.4

Informatics and Mathematical Methods in Simulation
Vol. 12 (2022), No. 3, pp. 243-253

ОРГАНІЗАЦІЯ ДИСТАНЦІЙНОГО ДОСТУПУ ДО КОМП'ЮТЕРНОЇ НАВЧАЛЬНОЇ ЛАБОРАТОРІЇ ЗА ДОПОМОГОЮ ВЕБ-ТЕХНОЛОГІЙ

Г.О. Шеремет, О.А. Стопакевич

Національний університет "Одеська політехніка",
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: sheremet.heorhiy@gmail.com,
stopakevich@op.edu.ua

Зараз у світі відбувається цифрова трансформація суспільства. Більшість видів людської діяльності поступово переносяться у цифровий вимір. Така сфера життя, як освіта не є винятком. З кожним роком студенти все рідше відвідують заняття очно, причиною цього є різні фактори. Виникає необхідність переходу навчальних закладів на дистанційну форму навчання. У зв'язку з цим виникають складнощі у використанні комп'ютерних лабораторій, розташованих в навчальних закладах. Отже, на сьогоднішній день організація дистанційного доступу до комп'ютерів навчальної лабораторій є досить актуальним завданням. Метою роботи є створення системи віддаленого доступу до комп'ютерної навчальної лабораторії з комп'ютера будь-якого користувача по паролю за допомогою web технологій. У статті розглядається процес налаштування серверної частини віртуальної приватної мережі VPN на віртуальному виділеному сервері VPS. Розглянуто послідовність команд у терміналі для встановлення та налаштування серверної частини VPN. Описано процес підключення до віртуальної приватної мережі з комп'ютера навчальної лабораторії та розглянуто послідовність команд у терміналі для встановлення та налаштування клієнтської частини VPN. Розглянуто інсталяцію та налаштування програмного забезпечення для віддаленого доступу на комп'ютерах навчальної лабораторії. Змодельовано віддалений доступ, який надає можливість віддаленого керування комп'ютерною мишею та клавіатурою, віддаленого запуску програмного забезпечення, обміну файлами між комп'ютером студента та комп'ютером навчальної лабораторії.. Стороннє програмне забезпечення, яке використовується при створенні системи віддаленого доступу, є вільно розповсюджуваним та безкоштовним.

Ключові слова: віддалений доступ до комп'ютера, віртуальна приватна мережа, VPN, WireGuard, RustDesk, VPS.

Вступ

Структурні зміни у світовій системі освіти, що відбулися починаючи з другій половині XX століття, зумовлені розвитком науково-технічного прогресу, вплинули на всі сторони життя суспільства. Поява дистанційного навчання не є раптовою подією, за всіх часів потреба у освіті зберігалася високому рівні. Поява інтернету та прискорення темпів наукового прогресу лише сприяли поширення даного формату здобуття освіти. У світлі останніх подій в Україні дистанційне навчання набуває ще більшої актуальності.

Існує безліч готових рішень для віддаленого доступу до комп'ютера. Найпоширеніші і найбільш функціональні з них є платними чи частково платними. У статті розглядається організація дистанційного доступу до комп'ютерної навчальної лабораторії з використанням виключно безкоштовних рішень. При цьому запропоноване рішення є досить функціональним і забезпечує студентів всім необхідним для комфортного використання навчальної лабораторії дистанційно.

Аналіз досліджень та публікацій

Дистанційне навчання в сучасному розумінні сформувалося порівняно нещодавно і тому, беручи до уваги цю новизну, воно орієнтується на передовий

педагогічний і методичний досвід, акумульований різними освітніми інституціями світового простору, на застосовування новітніх і оперативних інформаційно-педагогічних технологій, що окликаються на запити сучасної освіти та соціуму в цілому. Дистанційне навчання – одна із форм навчання, яка виникла й удосконалювалася разом із розвитком інтернет-технологій, і на сьогодні має чіткі характерні ознаки, принципи і певні методичні напрацювання. Дистанційне навчання та освіта із застосуванням дистанційних освітніх технологій набуває все більшого поширення в Україні і здобуває власних рис [**1**].

Коворкінг означає роботу двох або більше людей в одному місці, але не в одній фірмі. Це явище набуло значного розмаху в останні роки, включаючи зростання попиту у великих містах навколо світу та перспективи подальшого зростання в майбутньому. Характеристика фірм, розташованих у коворкінгах здається, змінилися з часом, оскільки сьогодні також зростає кількість великих нетехнологічних фірм, які обирають цей стиль [2].

У цілому нині з підприємницького погляду перебування у коворкінгу позитивно впливає на підприємницьку поведінку. Це засноване в основному на позитивних побічних ефектах та співпраці представників різних професій у рамках коворкінгу, що особливо вигідно молодим фірмам [2,3,4].

Коворкінг явище, яке проникло в організаційні структури, впливає на створення та обмін знаннями, покращує інноваційну поведінку та перебуває під впливом соціальних факторів, а також матеріального оснащення. Середовище, що нагадує коворкінг, робить людей більш щасливими та емоційно здоровими, компанії можуть розглянути можливість застосування набутого досвіду та знань у своїй організації, щоб співробітники з більшою готовністю залишалися з ними [5,6,7].

Мета і задачі роботи

Метою роботи є опис створення системи віддаленого доступу до комп'ютерної навчальної лабораторії з комп'ютера любого користувача по паролю за допомогою web технологій.

Для досягнення поставленої мети розроблена система має відповідати наступним основним вимогам:

- забезпечити реєстрацію та ідентифікацію, доступ по паролю користувачів та адміністраторів системи;
- комп’ютери лабораторії працюватимуть з використанням операційній системи Windows версії не нижче 8х;
- користувачі повинні мати доступ до управління курсором та клавіатурою, реалізувати віддалений запуск програм і отримання результатів їх роботи;
- забезпечити можливість обміну файлами з віддаленим комп’ютером.

Основна частина

Для організації дистанційного доступу до комп'ютерної навчальної лабораторії за допомогою веб-технологій необхідно виконати такі пункти:

1. Налаштувати серверну частину VPN на VPS.
2. Підключитись до VPN з комп'ютерної навчальної лабораторії.
3. Встановити та налаштувати програмне забезпечення для віддаленого доступу на комп'ютерах навчальної лабораторії.
4. Протестувати можливість віддаленого доступу.
5 Моделювання побудованої системи.

Налаштування серверної частини VPN на VPS.

VPN (virtual private network – віртуальна приватна мережа) — це узагальнена назва технологій, які дозволяють створювати віртуальні захищені мережі поверх інших мереж із меншим рівнем довіри. VPN-тунель, який створюється між двома вузлами, дозволяє приєднаному пристрою чи користувачеві бути повноцінним

учасником віддаленої мережі та користуватися її сервісами — внутрішніми сайтами, базами, принтерами, політиками виходу в Інтернет. Безпека передавання інформації через загальнодоступні мережі реалізована за допомогою шифрування, внаслідок чого створюється закритий для сторонніх канал обміну інформацією. Технологія VPN дозволяє об'єднати кілька географічно віддалених мереж (або окремих клієнтів) у єдину мережу з використанням для зв'язку між ними спеціадьних каналів. Багато провайдерів пропонують свої послуги як з організації VPN-мереж для бізнес-клієнтів, так і для виходу в Інтернет. VPN є клієнт-серверною технологією [8].

Виртуальний виділений чи приватний сервер (virtual dedicated VDS or private VPS server) – послуга, у межах якої користувачеві надають віртуальний сервер. Це повноцінна альтернатива фізичного виділеного сервера з великою кількістю переваг, високою стабільністю, простотою в управлінні та налаштуванні, стійкістю до відмов та набагато меншими фінансовими витратами [9].

Можна обрати майже будь-який VPS, наприклад від digitalocean [10]. Операційною системою цього VPS є Ubuntu 22.10.

Для реалізації VPN використаємо WireGuard. WireGuard — це комунікаційний протокол та безкоштовне програмне забезпечення з відкритим вихідним кодом, яке реалізує зашифровані VPN [11]. Розглянемо послідовність команд у терміналі для встановлення та налаштування серверної частини WireGuard.

Оновлюємо сервер:

```
apt update && apt upgrade -y
```

Ставимо wireguard:

```
apt install -y wireguard
```

Генеруємо ключі сервера:

```
wg genkey | tee /etc/wireguard/privatekey | wg pubkey | tee /etc/wireguard/publickey
```

Проставляємо права на приватний ключ:

```
chmod 600 /etc/wireguard/privatekey
```

Перевіримо назву мережного інтерфейсу:

```
ip a
```

Швидше за все, це буде eth0, але можливо й інший, наприклад, ens3 або якось інакше. Ця назва інтерфейсу використовується далі в конфігураційному файлі /etc/wireguard/wg0.conf, який буде створено нижче:

```
vim /etc/wireguard/wg0.conf
```

Вміст файлу wg0.conf

```
[Interface]
PrivateKey = <privatekey>
Address = 10.0.0.1/24
ListenPort = 51830
PostUp = iptables -A FORWARD -i %i -j ACCEPT; iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
PostDown = iptables -D FORWARD -i %i -j ACCEPT; iptables -t nat -D POSTROUTING -o eth0 -j MASQUERADE
```

У рядках PostUp і PostDown використаний саме мережевий інтерфейс eth0. Якщо інший, необхідно замінити eth0 на нього.

Вставляємо замість <privatekey> вміст файлу /etc/wireguard/privatekey

Налаштовуємо IP форвардинг:

```
echo "net.ipv4.ip_forward=1" >> /etc/sysctl.conf
sysctl -p
```

Включаємо systemd демон з wireguard:

```
systemctl enable wg-quick@wg0.service
systemctl start wg-quick@wg0.service
systemctl status wg-quick@wg0.service
```

Створюємо ключі клієнта:

```
wg genkey | tee /etc/wireguard/client_privatekey | wg pubkey | tee /etc/wireguard/ client_publickey
```

Додаємо в конфіг сервера клієнта:

```
vim /etc/wireguard/wg0.conf
[Peer]
PublicKey = <client_publickey>
AllowedIPs = 10.0.0.2/32
```

Замість <client_publickey> — замінюємо вміст файлу /etc/wireguard/ client_publickey

Перезавантажуємо systemd сервіс із wireguard:

```
systemctl restart wg-quick@wg0
systemctl status wg-quick@wg0
```

Підключення до VPN з комп'ютерної навчальної лабораторії

На локальній машині навчальної лабораторії створюємо текстовий файл із конфігом клієнта:

```
[Interface]
PrivateKey = <CLIENT-PRIVATE-KEY>
Address = 10.0.0.3/32
DNS = 8.8.8.8
[Peer]
PublicKey = <SERVER-PUBKEY>
Endpoint = <SERVER-IP>:51830
AllowedIPs = 0.0.0.0/0
PersistentKeepalive = 20
```

Тут <CLIENT-PRIVATE-KEY> замінюємо на приватний ключ клієнта, тобто вміст файлу /etc/wireguard/client_privatekey на сервері. <SERVER-PUBKEY> замінюємо на публічний ключ сервера, тобто вміст файлу /etc/wireguard/publickey на сервері. <SERVER-IP> замінюємо на IP сервер.

Цей файл відкриваємо у Wireguard клієнті (є для всіх операційних систем, у тому числі мобільних) – і тиснемо у клієнті кнопку підключення.

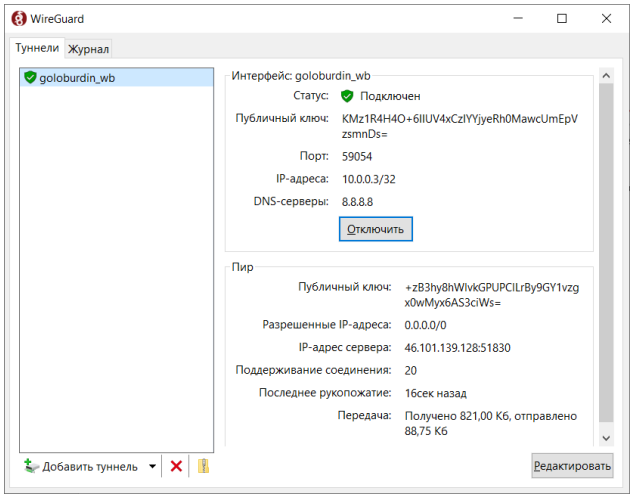


Рис. 1. Підключення до VPN

На цьому налаштування локальної машини навчальної лабораторії закінчено. Тепер вона має вихід в інтернет через білу IP-адресу. Це необхідно для можливості віддаленого доступу.

Встановлення та налаштування програмного забезпечення для віддаленого доступу на комп'ютері навчальної лабораторії.

Для віддаленого доступу використовується програма RustDesk. RustDesk – це безкоштовне програмне забезпечення для віддаленого ПК, створене RustDesk. Ця програма з відкритим вихідним кодом допомагає користувачам отримувати доступ та керувати своїми комп'ютерами. з будь-якого місця. Він служить і клієнтом, і

сервером, тому для його використання немає необхідності використовувати будь-які інші сторонні програми.[12]

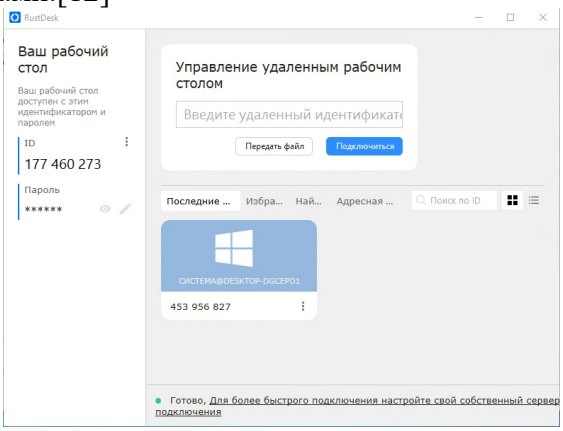


Рис. 2. Інтерфейс RustDesk

Цього достатньо для віддаленого доступу. Єдине, треба переконатися, що служба запущена.

Для віддаленого доступу необхідно надати студентам ID та пароль.

Тестування можливості віддаленого доступу.

Встановлюємо програму RustDesk на комп'ютер. У вікні «Керування віддаленим робочим столом» вводимо ID віддаленого комп'ютера навчальної лабораторії та натискаємо «Підключитися».

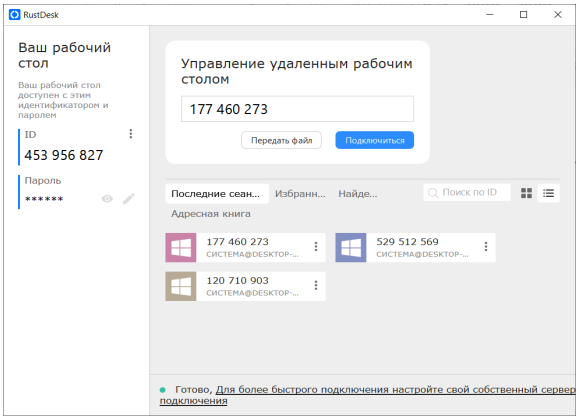


Рис. 3. Підключення до віддаленого комп'ютера

Далі програма попросить надати пароль. Вводимо пароль та натискаємо кнопку «ОК».

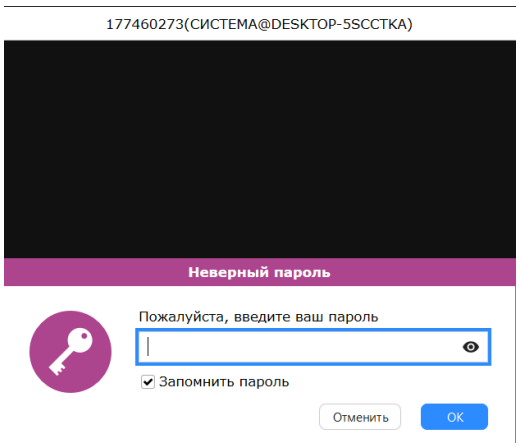


Рис. 4. Вікно введення пароля

Далі отримуємо віддалений доступ.

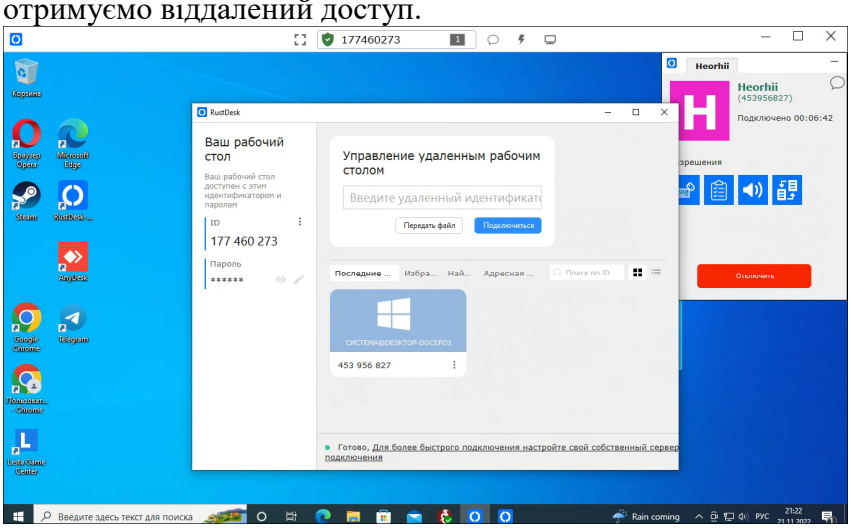


Рис. 5. Вікно віддаленого доступу

Тепер після успішного тестування ми можемо бути впевнені, що це рішення робоче і готове до використання.

Моделювання побудованої системи.

Панель адміністратора має вигляд як представлено рис. 6. У ній адміністратор системи може додавати, редагувати та видаляти комп'ютери.

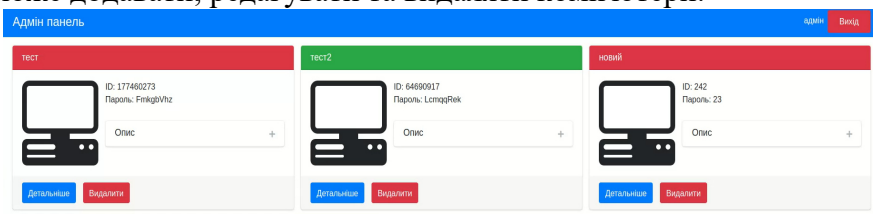


Рис. 6. Панель адміністратора.

Створимо новий комп'ютер з даними, представленими на рис. 7.

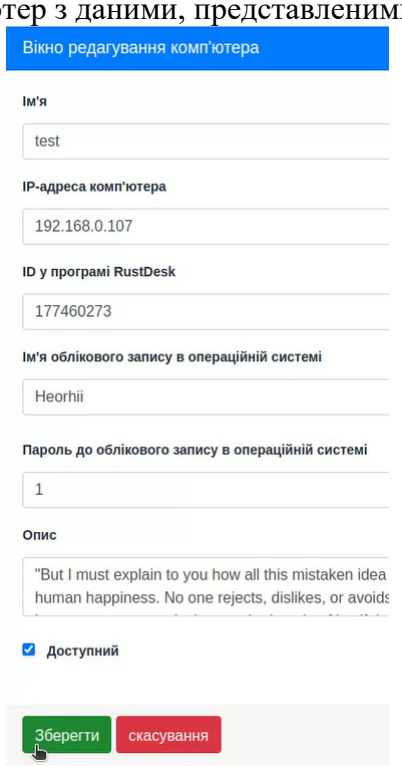


Рис. 7. Вікно редагування комп'ютера.

Тепер комп'ютер з ip-адресою 192.168.0.107 доступний для підключення студентів.

Для реєстрації необхідно надати електронну пошту та придумати пароль. Для користування системою також необхідно підтвердити адресу електронної пошти. Зареєструємось у системі. На рис.8 зображено вікно реєстрації.

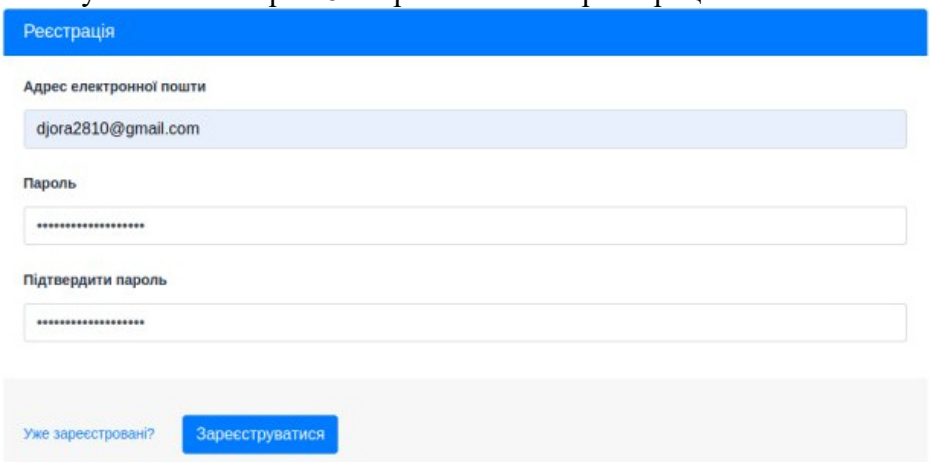


Рис. 8. Вікно реєстрація.

Після реєстрації ми побачимо повідомлення про необхідність підтвердити адресу електронної пошти. На рис.9 зображено Сповіщення.

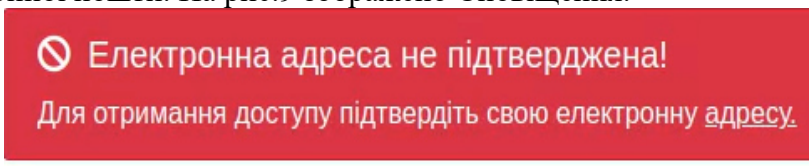


Рис. 9. Сповіщення.

Після підтвердження адреси це повідомлення зникне і ми зможемо скористатися системою. Завершивши реєстрацію, користувач побачить інтерфейс як представлено на рис.10.

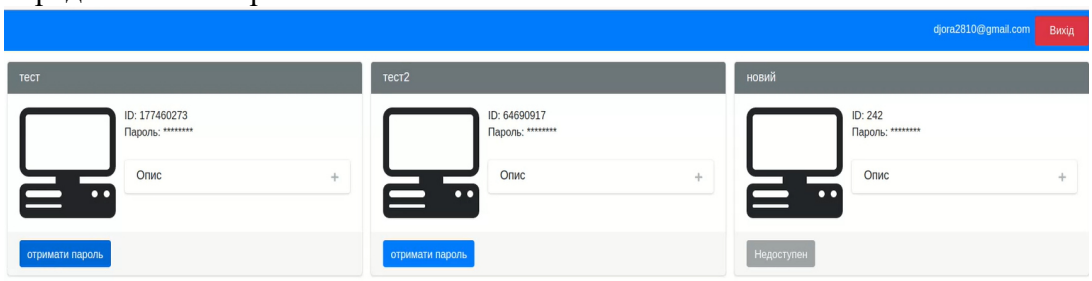


Рис. 10. Інтерфей користувача.

Користувач може вибрати комп'ютер та підключитися до нього. Підключимося до комп'ютера з іменем «test» натиснувши на кнопку «Отримати пароль». Після чого система надасть нам ID та пароль для підключення, як представлено на рис.11.

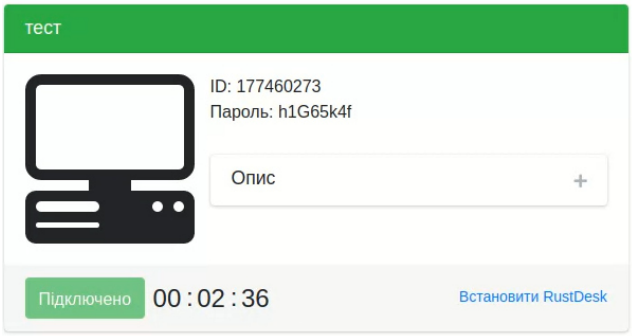


Рис. 11. Отримання пароля.

Далі заходимо в RustDesk і підключаємося за наданим ID, в нашому випадку це 177460273. RustDesk запросить пароль, вводимо раніше отриманий пароль, в нашому випадку це h1G65k4f.

Маючи віддалений доступ до комп'ютера, заходимо в консоль і вводимо команду ipconfig, щоб перевірити ip-адресу і переконатися в тому, що підключилися до потрібного комп'ютера. На рис. 12 зображено вікно віддаленого доступу.

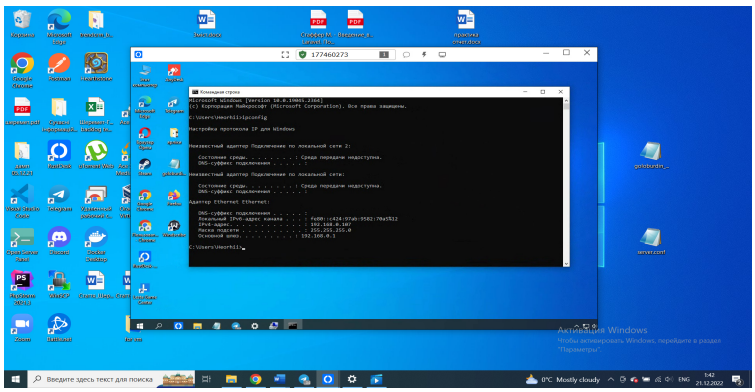


Рис. 12. Вікно віддаленого доступу.

Як видно на малюнку ip-адреса 192.168.0.107. Такий, як ми вказували при створенні комп'ютера в панелі адміністратора. Відтак система працює коректно та готова до використання.

Також у системі існує можливість зайняти чергу у разі коли потрібний нам комп'ютер зайнятий іншим користувачем. Зайнятий комп'ютер виглядає як на рис.13.

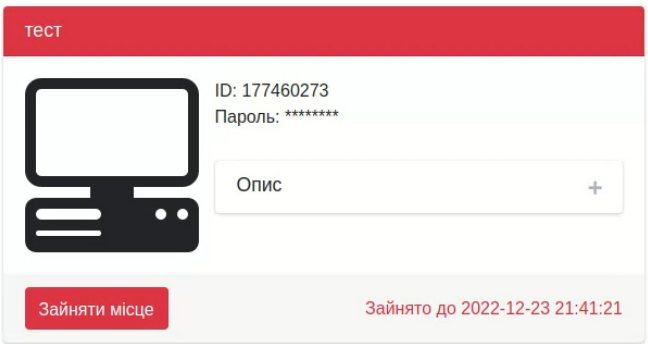


Рис. 13. Зайнятий комп'ютер.

При натисканні на кнопку "Зайняти місце" ми займемо місце в черзі. Перебування у черзі виглядає як представлено рис.14.

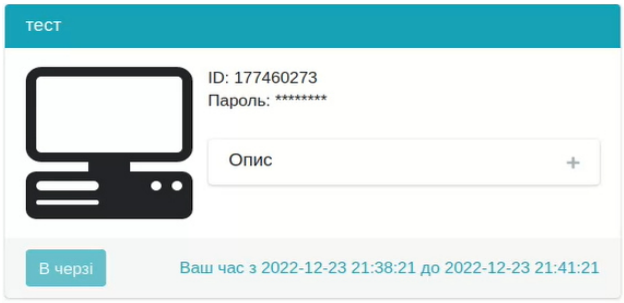


Рис. 14. Знаходження у черзі.

При настанні нашої черги система надасть нам пароль і ми зможемо отримати віддалений доступ.

Висновки

В межах статті виконана мета роботи – описано створення системи дистанційного доступу до комп'ютерної навчальної лабораторії за допомогою web-технологій.

При досягненні поставленої мети в роботі розв'язані наступні задачі:

- розроблено систему реєстрацію та ідентифікацію, доступ по паролю користувачів та адміністраторів системи;
- Розроблена система працює на операційній системи Windows версії не нижче 8х;
- Надана можливість управління курсором та клавіатурою, та віддаленого запуску програм і отримання результатів їх роботи;
- забезпечено можливість обміну файлами з віддаленим комп’ютером.

Проведено аналіз існуючих програм дистанційного доступу до комп'ютерних мереж. Серед них була обрана і взята за основу програма, що найбільш підходить за функціоналом і вимогами.

Розроблено програмний додаток який:

- забезпечує реєстрацію, автентифікацію та авторизацію користувачів у системі;
- надає можливість віддаленого керування курсором та клавіатурою;
- надає можливість віддаленого запуску програмного забезпечення;
- надає можливість обміну файлами між персональним комп'ютером користувача та комп'ютером навчальної лабораторії;
- забезпечує почергове використання комп'ютерів студентами.

Також проведено моделювання роботи системи дистанційного доступу до комп'ютерної навчальної лабораторії. Моделювання продемонструвало основні функції системи та підтвердило її працездатність.

Отримані в даній роботі результати можуть бути корисні не тільки для освіти, а й для дистанційного бізнес – коворкінга у невеликих фірмах, наукових установах. Результати роботи можуть служити основою для подальших розробок у цій галузі.

Список літератури

1. Гнатюк О.В. Дистанційне навчання: проблеми, пошуки, виклики. URL: https://lib.iitta.gov.ua/ Текст.pdf
2. Tim A. Haucke N., Östmarck A. An Analysis of the Co-working Space Industry in Stockholm from an Entrepreneurial Perspective. URL: https://kth.diva-portal.org/smash/get/diva2:1190270/FULLTEXT01.pdf
3. Fahrizal1 A., Jean C., Juan B.M., Ramdhani R., Hadiwirosa S., Hamdi E., Indradewa R., Abadi F. Strategic Formulation Analysis of Coworking Space Businesses Using Containers. URL: https://www.ijrrjournal.com/IJRR_Vol.9_Issue.3_March2022/IJRR022.pdf

4. Endrissat N., Vandelannoitte A.L. From sites to vibes: Technology and the spatial production of coworking spaces. URL: https://hal.archives-ouvertes.fr/hal-03332209/document
5. Kraus S.; Bouncken R.B.; Görmar L.; González-Serrano M.H., Calabuig F. Coworking spaces and makerspaces: Mapping the state of research. URL: https://www.econstor.eu/bitstream/10419/260976/1/1796986151.pdf
6. Hofeditz L., Mirbabaie M., Stieglitz S. Virtually Extended Coworking Spaces? *The Reinforcement of Social Proximity, Motivation and Knowledge Sharing Through ICT*. URL: https://arxiv.org/ftp/arxiv/papers/2012/2012.09538.pdf
7. Roche M., Oettl A., Catalina C. (Co-) Working in Close Proximity. *Knowledge Spillovers and Social Interactions*. URL: https://www.hbs.edu/ris/Publication%20Files/21-024rev2-11-22_4cf1fb54-e60b-41e6-8611-985031c999ba.pdf
8. Вікіпедія. VPN. URL: https://uk.wikipedia.org/wiki/VPN
9. Вікіпедія. Віртуальний виділений сервер. URL: https://uk.wikipedia.org/wiki/Віртуальний_виділений_сервер
10. DigitalOcean. Droplets. URL: https://www.digitalocean.com/products/droplets
11. Вікіпедія. WireGuard. URL: https://ru.wikipedia.org/wiki/WireGuard
12. RustDesk. URL: https://rustdesk.com/

ORGANIZING REMOTE ACCESS TO THE COMPUTER EDUCATIONAL LABORATORY USING WEB TECHNOLOGIES

G.O. Sheremet, O.A. Stopakevich

National Odesa Polytechnic University,
ave. Shevchenko, 1, Odesa, 65044, Ukraine; e-mail: sheremet.heorhiy@gmail.com,
stopakevich@op.edu.ua

Currently, the world is undergoing a digital transformation of society. Most types of human activity are gradually being transferred to the digital dimension. Such a sphere of life as education is no exception. Every year, students attend classes face-to-face less and less, the reason for this is various factors. There is a need for educational institutions to switch to distance education. In this connection, difficulties arise in the use of computer laboratories located in educational institutions. So, today, the organization of remote access to computers of educational laboratories is a very urgent task. The purpose of the work is to create a system of remote access to the computer training laboratory from any user's computer by password using web technologies. The article discusses the process of setting up the server part of a virtual private network VPN on a virtual dedicated VPS server. Considered the sequence of commands in the terminal to install and configure the VPN backend. The process of connecting to a virtual private network from a computer of the educational laboratory is described, and the sequence of commands in the terminal for installing and configuring the VPN client part is considered. The installation and configuration of software for remote access on the computers of the educational laboratory is considered. Remote access is simulated, which provides the possibility of remote control of a computer mouse and keyboard, remote start of software, file exchange between a student's computer and a computer of the educational laboratory. Third-party software used in creating a remote access system is free redistributable and free.
Keywords: remote computer access, virtual private network, VPN, WireGuard, RustDesk, VPS.

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

Том 12, номер 3, 2022. Одеса – 254 с., іл.

ИНФОРМАТИКА И МАТЕМАТИЧЕСКИЕ МЕТОДЫ В МОДЕЛИРОВАНИИ

Том 12, номер 3, 2022. Одесса – 254 с., ил.

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Volume 12, No. 3, 2022. Odesa – 254 p.

Засновник: Національний університет «Одеська політехніка»

Зареєстровано Міністерством юстиції України 04.04.2011р.

Свідоцтво: серія КВ № 17610 - 6460Р

Друкується за рішенням Вченої ради Одеського національного політехнічного університету (протокол № 3 від 27.09.2022)

Адреса редакції: Національний університет «Одеська політехніка»,

проспект Шевченка, 1, Одеса 65044 Україна

Web: www.immm.op.edu.ua (immm.opu.ua)

E-mail: immm.ukraine@gmail.com