МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська політехніка»

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Том 12, № 1-2

Volume 12, No. 1-2

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 Odessa 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., Odessa, 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.no1-2.5
UDC 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 12 (2022), No. 1-2, pp. 5-14

THE STEGANOGRAPHIC METHOD WITH MULTIPLE ACCESS BASED ON FREQUENCY-SPATIAL MATRICES

A.V.Sokolov

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

The solution to some practical tasks with the help of steganography requires the organization of multiple access to a steganographic information transmission channel. At the same time, existing developments imply the use of MC-CDMA technology to solve these tasks, which has a strictly predetermined number of shared channels, requires the simultaneous embedding of additional information delivered from all users and is disintegrated with the applied steganographic algorithm. In this paper, a full-fledged steganographic method, with multiple access based on the use of frequency-spatial matrices has been developed. In the developed method, two code attributes are allocated to each user: frequency and spatial, on the basis of which codewords that are used to transmit information are generated. The total number of registered users operating in the system based on the proposed steganographic method can reach the value of J=4800, while the total number of users simultaneously transmitting information can reach the value of N=100 while supporting the practically acceptable system parameters. At the same time, the embedding of additional information by the users occurs independently of each other at any time convenient to them. To ensure the largest number of simultaneously operating users and minimize the level of intra-system interference, an S-code of spatial arrangements, as well as an F-code of frequency arrangements based on the Reed-Solomon code, are proposed. The proposed steganographic method with multiple access is characterized by flexibility in the allocation of resources of the steganographic channel: if necessary, the throughput of the steganographic channel can be increased with a decrease in PSNR values, or, conversely, the reliability of perception of the steganographic message can be increased by reducing the number of users simultaneously operating in the system.

Keywords: steganography, code control, multiple access, code division of channels, frequency-spatial matrices.

Introduction and statement of the problem

The development of modern information security systems, in addition to cryptographic tools, involves the active introduction and use of the steganographic component, which allows not only to make confidential information unreadable by unauthorized users but also to hide the very fact of its transmission.

In addition to the well-known steganographic methods, which have such properties as simplicity of algorithmic implementation [1…3], minimization of distortions introduced into the container image [4, 5], resistance to various types of attacks against the additional information (lossy compression attacks, noise, blurring) [6…8], the current stage of development of steganography is characterized by the emergence of steganographic methods with multiple access.

Thus, in [9] it is proposed to use the MC-CDMA (Multi-Code Code Division Multiple Access) technology based on the orthogonal Walsh-Hadamard transform to organize multiple access. The disadvantages of this technology include the fact that the number of users is strictly predetermined and equal to $N = 2^k = 2, 4, 8, 16, \ldots$, as well as the disintegration of multiple access technology with the steganographic method used, i.e., MC-CDMA technology does not show exactly how the embedding and extraction of additional information should be performed.

As the performed research has shown, the possibility of overcoming these shortcomings of using MC-CDMA technology in steganographic applications lies in the development of new classes of steganographic structures labelled as frequency-spatial codes, which imply the

possibility of multiple access within a common steganographic channel by using two attributes: frequency and spatial.

The *purpose* of this paper is to develop a steganographic method with multiple access based on frequency-spatial matrices.

The main idea of the developed method

The main orthogonal transform used in the proposed method is the Walsh-Hadamard transform [10], the one-dimensional version of which can be written as

$$V = YH_N, \tag{1}$$

where Y is a row vector of length N, H_N is a Walsh-Hadamard matrix of order $N = 2^k$, which can be constructed in accordance with the Sylvester construction

$$H_{2^k} = \begin{bmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{bmatrix}, \; H_1 = 1. \tag{2}$$

The two-dimensional version of the Walsh-Hadamard transform is determined using the following relationship

$$W = H'_N X H'^T_N, \tag{3}$$

where $H'_N = \frac{1}{N} H_N$, and X is a matrix of size $N \times N$.

The proposed steganographic method uses the relationship established in [11] between the two-dimensional and one-dimensional Walsh-Hadamard transform: up to a coefficient $1/N$, the two-dimensional Walsh-Hadamard transform (3) can be represented through the one-dimensional Walsh-Hadamard transform using the following relation $\tilde{W} = \tilde{Y}H_{N^2}$, where the operator $\tilde{A}$ denotes the representation of matrix A of order $N \times N$ as a row vector of length N^2 by sequential concatenation of its rows.

The basis of the operation of the proposed steganographic method is the linearity property of the Walsh-Hadamard transform, on the basis of which, by setting special properties of the embedded data, it is possible to selectively influence one or another transformant of the Walsh-Hadamard transform of the resulting steganographic message [11]. Indeed, if X is a container, D is additional information, and M is a steganographic message, then

$$\begin{gathered} \tilde{M} = \tilde{X} + \tilde{D}; \\ \tilde{M}H_{N^2} = \tilde{X}H_{N^2} + \tilde{D}H_{N^2}. \end{gathered} \tag{4}$$

Thus, by performing preliminary encoding of information using a special form of codewords matrices, we can get a targeted impact on one or another Walsh-Hadamard transformant of the original container image. Codewords affecting the corresponding Walsh-Hadamard transformants (*n*,*m*), as well as their corresponding frequency components $f_i, i = 1,2,...,16$ are presented in Table 1.

Let us consider the essence of the idea of the steganographic method based on frequency-spatial matrices. The operations of embedding and extraction of additional information in this method are based on dividing the image on the blocks Q_k of size $\mu \times \mu = 16 \times 16$. Each of the obtained blocks is divided into 16 more blocks q_i, $i = 1,2,...,16$ of size 4×4

$$Q_k = \begin{array}{|c|c|c|c|} \hline q_1 & q_2 & q_3 & q_4 \\ \hline q_5 & q_6 & q_7 & q_8 \\ \hline q_9 & q_{10} & q_{11} & q_{12} \\ \hline q_{13} & q_{14} & q_{15} & q_{16} \\ \hline \end{array}. \tag{5}$$

Table 1

Codewords for targeted influence for each of the Walsh-Hadamard transformants

$T^{+}_{4,(1,1)} \leftrightarrow f_0$	$T^{+}_{4,(1,2)} \leftrightarrow f_1$	$T^{+}_{4,(1,3)} \leftrightarrow f_2$	$T^{+}_{4,(1,4)} \leftrightarrow f_3$
$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \end{bmatrix}$	$\begin{bmatrix} 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$
$T^{+}_{4,(2,1)} \leftrightarrow f_4$	$T^{+}_{4,(2,2)} \leftrightarrow f_5$	$T^{+}_{4,(2,3)} \leftrightarrow f_6$	$T^{+}_{4,(2,4)} \leftrightarrow f_7$
$\begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 \end{bmatrix}$	$\begin{bmatrix} 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \end{bmatrix}$
$T^{+}_{4,(3,1)} \leftrightarrow f_8$	$T^{+}_{4,(3,2)} \leftrightarrow f_9$	$T^{+}_{4,(3,3)} \leftrightarrow f_{10}$	$T^{+}_{4,(3,4)} \leftrightarrow f_{11}$
$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 \end{bmatrix}$	$\begin{bmatrix} 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \\ -1 & 1 & -1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 \\ -1 & -1 & 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \\ -1 & 1 & 1 & -1 \end{bmatrix}$
$T^{+}_{4,(4,1)} \leftrightarrow f_{12}$	$T^{+}_{4,(4,2)} \leftrightarrow f_{13}$	$T^{+}_{4,(4,3)} \leftrightarrow f_{14}$	$T^{+}_{4,(4,4)} \leftrightarrow f_{15}$
$\begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \\ -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 \\ -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 \end{bmatrix}$	$\begin{bmatrix} 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \\ -1 & 1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$

The division of user channels is performed based on two properties: frequency and spatial. In other words, to each user 2 codewords are allocated: the S-code codeword of the spatial arrangement and the F-code codeword of the frequency arrangement. At the same time, the codeword of the S-code determines the numbers of blocks q_i into which this user can embed information, while the codeword of the F-code determines those Walsh-Hadamard transformants into which this user can embed information using codewords, presented in Table 1.

Construction of codewords of the S-code of spatial arrangements

To solve the problem of constructing S-codes of spatial arrangements, each codeword of which contains 16 binary components that show whether the given spatial component is active (the value of the element of the codeword is $s_i = 1$) or passive (the value of the element of the codeword is $s_i = 0$), an approach based on exhaustive search has been adopted. In our case, in order to maximize the number of simultaneously operating users, as well as to ensure the highest reliability of perception, codewords of the S-code of spatial arrangements of Hamming weight $wt(\{s_i\}) = 4$ are preferred. The total number of binary vectors of length $N = 16$ and weight $wt(\{s_i\}) = 4$ is determined by the number of 4-permutations of 16 i.e. $C_{16}^{4} = 1820$ and constitute a code with the number of overlaps of active components $\lambda \le 3$.

To solve the problem of minimizing intra-system interference caused by the interference of codewords from different users, it is necessary, based on the full code of the length $N = 16$ and weight $wt(\{s_i\}) = 4$, to construct a spatial arrangements S-code, the codewords of which are characterized by the number of overlaps of active components $\lambda \le 1$.

As experiments show, the cardinality of the constructed code will depend on the order in which codewords are chosen during its construction. Let's use the following approach:

Step 1. We fix the first four possible codewords of the full code of length $N=16$ and weight $wt(\{s_i\})=4$, which have the number of overlaps of active components $\lambda=0$. Thus, by connecting new users with help of these codewords, we will ensure the complete absence of intra-system interference

$$S'=\begin{bmatrix}\{s_{1,i}\}\\ \{s_{2,i}\}\\ \{s_{3,i}\}\\ \{s_{4,i}\}\end{bmatrix}=\begin{bmatrix}\{1111000000000000\}\\ \{0000111100000000\}\\ \{0000000011110000\}\\ \{0000000000001111\}\end{bmatrix}, i=1,...,16. \quad (6)$$

Step 2. Sampling codewords from the full set of vectors of length $N=16$ and weight $wt(\{s_i\})=4$, we build 16 more codewords that have the number of overlaps $\lambda\le 1$ between themselves and relative to codewords (6). As a result, we obtain the following ensemble of cardinality $J_S=20$

$$S=\begin{bmatrix}\{s_{1,i}\}\\ \{s_{2,i}\}\\ \{s_{3,i}\}\\ \{s_{4,i}\}\\ \{s_{5,i}\}\\ \{s_{6,i}\}\\ \{s_{7,i}\}\\ \{s_{8,i}\}\\ \{s_{9,i}\}\\ \{s_{10,i}\}\\ \{s_{11,i}\}\\ \{s_{12,i}\}\\ \{s_{13,i}\}\\ \{s_{14,i}\}\\ \{s_{15,i}\}\\ \{s_{16,i}\}\\ \{s_{17,i}\}\\ \{s_{18,i}\}\\ \{s_{19,i}\}\\ \{s_{20,i}\}\end{bmatrix}=\begin{bmatrix}\{1111000000000000\}\\ \{0000111100000000\}\\ \{0000000011110000\}\\ \{0000000000001111\}\\ \{1000100010001000\}\\ \{0100010001001000\}\\ \{0010001000101000\}\\ \{0001000100011000\}\\ \{0010010010000100\}\\ \{0001100001000100\}\\ \{1000000100100100\}\\ \{0100001000010100\}\\ \{0001001010000010\}\\ \{0010000101000010\}\\ \{0100100000100010\}\\ \{1000010000010010\}\\ \{0100000110000001\}\\ \{1000001001000001\}\\ \{0001010000100001\}\\ \{0010100000010001\}\end{bmatrix}, i=1,...,16, \quad (7)$$

which will be used as the S-code.

Construction of the codewords of the F-code of frequency arrangements

As a basis for constructing the F-code of frequency arrangements in this paper we use doubly cyclic Reed-Solomon (RS) codes [12]. In order to maximize the number of users who can simultaneously operate in a steganographic channel, it is rational to use all available frequency components. For this purpose, to construct frequency arrangements, we use the second-order RS-code in the extended Galois field $GF(2^4)$, which has the following characteristics: codeword length $N=15$, number of information bits $K=2$, code distance $d=N-K+1=15-2+1=14$.

Note that Galois field $GF(2^4)$ has two isomorphic representations, which are determined by two primitive irreducible polynomials $h_1(x)=x^4+x+1$ and $h_2(x)=x^4+x^3+1$. However, from the point of view of the technique for constructing a steganographic method with multiple access, the choice of a specific isomorphism of the Galois field is not of decisive importance, therefore, we will use the arithmetic of the extended Galois field, defined by the primitive irreducible polynomial $h_1(x)$. In this case, the addition and multiplication table in the field $GF(2^4)$ will take the form

+	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	D
0	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	1	0	3	2	5	4	7	6	9	8	B	A	D	C	F	E
2	2	3	0	1	6	7	4	5	A	B	8	9	E	F	C	D
3	3	2	1	0	7	6	5	4	B	A	9	8	F	E	D	C
4	4	5	6	7	0	1	2	3	C	D	E	F	8	9	A	B
5	5	4	7	6	1	0	3	2	D	C	F	E	9	8	B	A
6	6	7	4	5	2	3	0	1	E	F	C	D	A	B	8	9
7	7	6	5	4	3	2	1	0	F	E	D	C	B	A	9	8
8	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7
9	9	8	B	A	D	C	F	E	1	0	3	2	5	4	7	6
A	A	B	8	9	E	F	C	D	2	3	0	1	6	7	4	5
B	B	A	9	8	F	E	D	C	3	2	1	0	7	6	5	4
C	C	D	E	F	8	9	A	B	4	5	6	7	0	1	2	3
D	D	C	F	E	9	8	B	A	5	4	7	6	1	0	3	2
E	E	F	C	D	A	B	8	9	6	7	4	5	2	3	0	1
F	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0

×	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2	0	2	4	6	8	A	C	E	3	1	7	5	B	9	F	D
3	0	3	6	5	C	F	A	9	B	8	D	E	7	4	1	2
4	0	4	8	C	3	7	B	F	6	2	E	A	5	1	D	9
5	0	5	A	F	7	2	D	8	E	B	4	1	9	C	3	6
6	0	6	C	A	B	D	7	1	5	3	9	F	E	8	2	4
7	0	7	E	9	F	8	1	6	D	A	3	4	2	5	C	B
8	0	8	3	B	6	E	5	D	C	4	F	7	A	2	9	1
9	0	9	1	8	2	B	3	A	4	D	5	C	6	F	7	E
A	0	A	7	D	E	4	9	3	F	5	8	2	1	B	6	C
B	0	B	5	E	A	1	F	4	7	C	2	9	D	6	8	3
C	0	C	B	7	5	9	E	2	A	6	1	D	F	3	4	8
D	0	D	9	4	1	C	8	5	2	F	B	6	3	E	A	7
E	0	E	F	1	D	3	2	C	9	7	6	8	4	A	B	5
F	0	F	D	2	9	6	4	B	1	E	C	3	8	7	5	A

(8)

Taking the value of the primitive element $\theta = 2$, we construct a generating RS-code polynomial in the Galois field $GF(2^4)$

$$g(z) = \prod_{i=1}^{d-1}(z-\theta^i) = \prod_{i=1}^{13}(z-2^i) =$$

$$(z+2)(z+4)(z+8)(z+3)(z+6)(z+12)(z+11)(z+5)(z+10)(z+7)(z+14)(z+15)(z+13) = \quad (9)$$

$$= 2+6z+14z^2+13z^3+11z^4+7z^5+12z^6+9z^7+3z^8+4z^9+10z^{10}+5z^{11}+8z^{12}+z^{13}.$$

Based on the obtained generating polynomial, we write the generating matrix of the RS-code

$$G = \begin{bmatrix} 2 & 6 & 14 & 13 & 11 & 7 & 12 & 9 & 3 & 4 & 10 & 5 & 8 & 1 & 0 \\ 0 & 2 & 6 & 14 & 13 & 11 & 7 & 12 & 9 & 3 & 4 & 10 & 5 & 8 & 1 \end{bmatrix}, \quad (10)$$

the first row of which is the base codeword, on the basis of which, using the properties of double cyclicity of RS-codes, it is possible to construct all other codewords by applying the operation of cyclic shift in time and cyclic shift in frequency (using Galois field $GF(2^4)$ arithmetic). In this case, the total number of codewords of the F-code of frequency arrangements constructed by us is defined as

$$J = q(q-1) = 16 \cdot 15 = 240. \quad (11)$$

In view of the fact that the length of each frequency arrangement in accordance with the construction of the steganographic method should be $n = 4$, we will truncate each codeword of the RS-code to the specified length, the resulting codewords are presented in Table 2. At the same time, for brevity, the codewords are written in hexadecimal form.

Table 2

Truncated codewords of the RS-code in the Galois field $GF(2^4)$

26ED	6EDB	EDB7	DB7C	B7C9	7C93	C934	934A	34A5	4A58	A581	5810	8102	1026	026E
37FC	7FCA	FCA6	CA6D	A6D8	6D82	D825	825B	25B4	5B49	B490	4901	9013	0137	137F
04CF	4CF9	CF95	F95E	95EB	5EB1	EB16	B168	1687	687A	87A3	7A32	A320	3204	204C
15DE	5DE8	DE84	E84F	84FA	4FA0	FA07	A079	0796	796B	96B2	6B23	B231	2315	315D
62A9	2A9F	A9F3	9F38	F38D	38D7	8D70	D70E	70E1	0E1C	E1C5	1C54	C546	5462	462A
73B8	3B8E	B8E2	8E29	E29C	29C6	9C61	C61F	61F0	1F0D	F0D4	0D45	D457	4573	573B
408B	08BD	8BD1	BD1A	D1AF	1AF5	AF52	F52C	52C3	2C3E	C3E7	3E76	E764	7640	6408
519A	19AC	9AC0	AC0B	C0BE	0BE4	BE43	E43D	43D2	3D2F	D2F6	2F67	F675	6751	7519
AE65	E653	653F	53F4	3F41	F41B	41BC	1BC2	BC2D	C2D0	2D09	D098	098A	98AE	8AE6
BF74	F742	742E	42E5	2E50	E50A	50AD	0AD3	AD3C	D3C1	3C18	C189	189B	89BF	9BF7
8C47	C471	471D	71D6	1D63	D639	639E	39E0	9E0F	E0F2	0F2B	F2BA	2BA8	BA8C	A8C4
9D56	D560	560C	60C7	0C72	C728	728F	28F1	8F1E	F1E3	1E3A	E3AB	3AB9	AB9D	B9D5
EA21	A217	217B	17B0	7B05	B05F	05F8	5F86	F869	8694	694D	94DC	4DCE	DCEA	CEA2
FB30	B306	306A	06A1	6A14	A14E	14E9	4E97	E978	9785	785C	85CD	5CDF	CDFB	DFB3
C803	8035	0359	3592	5927	927D	27DA	7DA4	DA4B	A4B6	4B6F	B6FE	6FEC	FEC8	EC80
D912	9124	1248	2483	4836	836C	36CB	6CB5	CB5A	B5A7	5A7E	A7EF	7EFD	EFD9	FD91

Superposition of S-code and F-code codewords

In order to maximize the number of available divided communication channels in a common steganographic channel, the proposed method uses the rule of superposition of the codewords of the S-code of spatial arrangements and the F-code of frequency arrangements by superimposing the frequency components of the F-code on the active positions of the S-code.

Thus, the total number of users who can be registered and theoretically simultaneously transmit information in the steganographic channel is

$$J = J_S J_F = 20 \cdot 240 = 4800 . \quad (12)$$

Let's consider a specific example. Let the S-code codeword $\{s_{1,i}\} = \{1111000000000000\}$ is allocated to user A_1, as well as the F-code codeword $C_1 = \{26ED\} = \{2 \quad 6 \quad 14 \quad 13\}$. To obtain codewords T^+ and T^- used for the embedding of information symbols “0” and “1”, respectively, the user performs a superposition of the S-code and F-code codewords allocated to him, for which he follows the following algorithm:

Step 1. Represent the codeword of the S-code as a matrix of size 4×4 by sequentially filling its rows.

Step 2. Sequentially write in the active positions of the matrix obtained at *Step 1* the frequency components, the indices of which are determined by the values of the F-code codeword.

Performing *Step 1* and *Step 2* of the presented algorithm for our example, we obtain the following construction

$$T^{+\prime} = \begin{bmatrix} f_2 & f_6 & f_{14} & f_{13} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}. \quad (13)$$

Step 3. Substitute specific codewords $T_{4,(n,m)}$ presented in Table 1 based on their correspondence to frequency components f_i. In this case, instead of the values "0" in the matrix (13), zero matrices of size 4×4 are substituted. As a result, we obtain a codeword for encoding the character "0" by this user.

Step 4. To obtain a codeword T^-, we invert the codeword T^+ obtained in *Step 3*.

In the case of our example, we get the following codewords T^+ and T^-

$$T^+ = \left[\begin{array}{cccc} \begin{matrix} 1&1&-1&-1 \\ 1&1&-1&-1 \\ 1&1&-1&-1 \\ 1&1&-1&-1 \end{matrix} & \begin{matrix} 1&1&-1&-1 \\ -1&-1&1&1 \\ 1&1&-1&-1 \\ -1&-1&1&1 \end{matrix} & \begin{matrix} 1&1&-1&-1 \\ -1&-1&1&1 \\ -1&-1&1&1 \\ 1&1&-1&-1 \end{matrix} & \begin{matrix} 1&1&-1&-1 \\ 1&1&-1&-1 \\ 1&1&-1&-1 \\ 1&1&-1&-1 \end{matrix} \\ \hline \begin{matrix} 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \end{matrix} & \begin{matrix} 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \end{matrix} & \begin{matrix} 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \end{matrix} & \begin{matrix} 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \end{matrix} \\ \hline \begin{matrix} 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \end{matrix} & \begin{matrix} 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \end{matrix} & \begin{matrix} 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \end{matrix} & \begin{matrix} 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \end{matrix} \\ \hline \begin{matrix} 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \end{matrix} & \begin{matrix} 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \end{matrix} & \begin{matrix} 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \end{matrix} & \begin{matrix} 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \end{matrix} \end{array}\right], \quad T^- = \left[\begin{array}{cccc} \begin{matrix} -1&-1&+1&+1 \\ -1&-1&+1&+1 \\ -1&-1&+1&+1 \\ -1&-1&+1&+1 \end{matrix} & \begin{matrix} -1&-1&+1&+1 \\ +1&+1&-1&-1 \\ -1&-1&+1&+1 \\ +1&+1&-1&-1 \end{matrix} & \begin{matrix} -1&-1&+1&+1 \\ -1&-1&+1&+1 \\ +1&+1&-1&-1 \\ +1&+1&-1&-1 \end{matrix} & \begin{matrix} -1&-1&+1&+1 \\ +1&+1&-1&-1 \\ +1&+1&-1&-1 \\ -1&-1&+1&+1 \end{matrix} \\ \hline \begin{matrix} 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \end{matrix} & \begin{matrix} 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \end{matrix} & \begin{matrix} 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \end{matrix} & \begin{matrix} 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \end{matrix} \\ \hline \begin{matrix} 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \end{matrix} & \begin{matrix} 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \end{matrix} & \begin{matrix} 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \end{matrix} & \begin{matrix} 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \end{matrix} \\ \hline \begin{matrix} 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \end{matrix} & \begin{matrix} 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \end{matrix} & \begin{matrix} 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \end{matrix} & \begin{matrix} 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \end{matrix} \end{array}\right]. \quad (14)$$

The obtained codewords T^+ and T^- are used for the embedding of information symbols “0” and “1”, respectively.

The algorithms for embedding and extraction of additional information

Each user embeds information independently of other users at a time that is convenient for him. Consider the algorithms for information embedding and extraction.

The algorithm for information embedding

Step 1. A unique code $\{\{s_{z_1,i}\}, C_{z_2}\}$ consisting of the codeword of the S-code of spatial arrangements and the codeword of the F-code of frequency arrangements is allocated to the each of the users of the steganographic system.

Step 2. Based on the set $\{\{s_{z_1,i}\}, C_{z_2}\}$, taking into account (5), as well as codewords $f_i, i = 1,2,...,16$, each user generates codewords T^+ and T^-, with the help of which the information will be transmitted.

Step 3. Each user A_z splits the container image into the blocks of size $\mu \times \mu = 16 \times 16$ and embeds one bit $d_{z,k}$ of additional information into each of the container blocks X_k by applying the summation operation, i.e., each steganographic message block is calculated as

$$M_k = X_k + D_k. \tag{15}$$

The algorithm for information extraction

Step 1. The user who received the steganographic message splits it into blocks M_k of size $\mu \times \mu = 16 \times 16$, each of which is sequentially processed in order to extract a bit of information $d_{z,k}$ consigned for this user.

Step 2. The user finds the difference matrix Δ_k between each block of the received steganographic message M_k and the container image X_k.

Step 3. Each block of the difference matrix Δ_k is divided by the user into 16 subblocks of size $\frac{\mu}{4} \times \frac{\mu}{4} = 4 \times 4$ in accordance with construction (5). From the received subblocks, the user selects those whose number corresponds to the position numbers of the codeword of the S-code of spatial arrangements belonging to this user $\{s_{z_1,i}\}$, on which it takes the value 1 (when it is represented as a matrix of size 4×4 by sequentially filling of its rows). In view of the fact that all codewords of the S-code have weight $w = 4$, each of the users at this step chooses four subblocks of size 4×4. The user represents each of the received subblocks as a vector $\{\delta_{z,i}\}, i = 1,2,...,16$ of length $4^2 = 16$ by successive concatenation of its rows.

Step 4. In accordance with the code of frequency arrangements C_{z_2} allocated to this user, he selects the rows of the Walsh-Hadamard matrix H_{16}, which are designated as $\{h_{z,1}\}, \{h_{z,2}\}, \{h_{z,3}\}, \{h_{z,4}\}$.

Step 5. The user A_z calculates the vector P according to the following formula

$$\begin{gathered} P_{z,k} = [p_1 \quad p_2 \quad p_3 \quad p_4], \\ p_i = \sum_{k=1}^{\mu^2} \delta_{j,k} h_{j,k}, i = \{1,2,3,4\}. \end{gathered} \tag{16}$$

Step 6. The user calculates the data bit consigned for him, embedded in the block M_k using the following formula

$$d_{z,k} = sign\left(\sum_{i=1}^{4} p_i \right). \tag{17}$$

Characteristics of a steganographic method with multiple access based on frequency-spatial matrices

To estimate the level of perturbation of the container image when additional information is embedded into it using the proposed steganographic method, we use the difference indicator PSNR, which is defined as

$$\mathrm{PSNR} = 20 \lg\left(\frac{255}{\sqrt{\mathrm{MSE}}} \right), \tag{18}$$

where

$$\mathrm{MSE} = \frac{1}{nm}\sum_i \sum_j \left| X(i,j) - M(i,j) \right|^2 , \tag{19}$$

where n and m represent the size of the original message.

By construction of the proposed steganographic method, it becomes clear that the PSNR of a steganographic message will depend on the number of users in the system simultaneously transmitting information, as well as on the type of S-code and F-code codewords allocated to them. When connecting users in the order of presentation of codewords (7) and Table 2, the graph of PSNR dependence on the number of users simultaneously functioning in the system, will have the form shown in Fig 1.

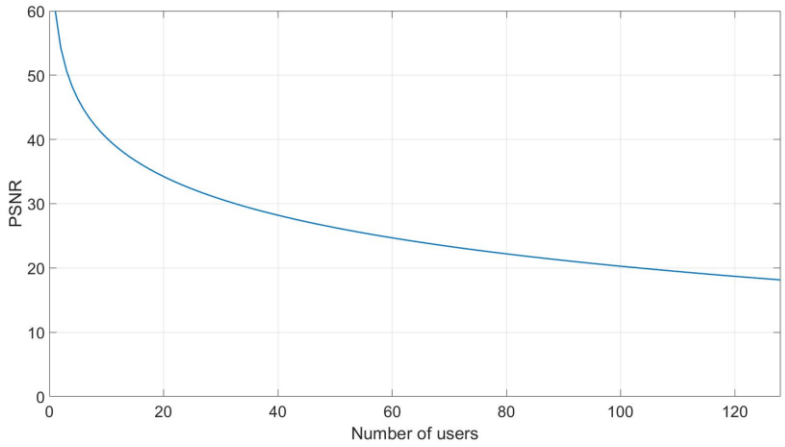


Fig. 1. Dependence graph of the PSNR of a steganographic message on the number of users simultaneously transmitting information using the steganographic channel

Analysis of the data presented in Fig. 1 shows that with the number of users simultaneously transmitting information $N \le 32$, it is possible to achieve a PSNR value of more than 30 dB. With the simultaneous operation of $N \le 100$ users, the PSNR level of the steganographic message does not fall below 20 dB. In view of the fact that the codewords of the S-code of spatial arrangements (7) allow no more than one overlap in space, as well as the codewords of the F-code of frequency arrangements (Table 2) allow no more than one overlap in frequency, the occurrence in the steganographic system of intra-system interference is inevitable. The level of intra-system interference will be directly proportional to the number of users simultaneously transmitting information. It is also clear that the level of intra-system interference will depend on the specific codewords of the S-code and F-code of users who are currently transmitting information through the steganographic channel.

Fig. 2 shows a graph of the dependence of the number of errors in the steganographic channel arising due to the action of intra-system interference on the number of simultaneously operating users when they are connected in the order in which codewords are presented in (7) and Table 2.

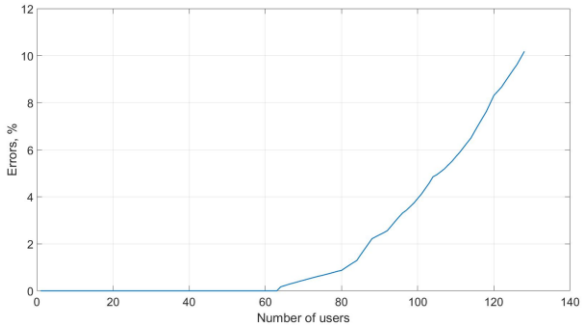


Fig. 2. Graph of the dependence of the number of errors in the steganographic channel arising due to the action of intra-system interference on the number of simultaneously operating users

Analysis of the data presented in Fig. 2 shows that with the selected order of connection of users for their number $N \le 64$, there are no intra-system interference, as a result of which all

information is transmitted without distortion. In the case of the number of users $N \le 100$, the number of errors that occur due to intra-system interference does not exceed the level of 4%, which is acceptable.

Conclusions

We note the main results of the research:

1. A full-fledged steganographic method with multiple access based on frequency-spatial matrices is proposed, which provides separate embedding (or its absence) of information by each user at any time convenient for them. Dividing of user channels is performed according to two properties: spatial and frequency, based on S-codes of spatial arrangements and F-codes of frequency arrangements. In this paper, we construct an S-code of spatial arrangements of cardinality $J_S = 20$ with the property of no more than one overlap, as well as an F-code of frequency arrangements based on the Reed-Solomon code of cardinality $J_F = 240$ in the Galois field $GF(2^4)$, which also has the property of no more than one overlap.

2. The possible total number of registered in the steganographic system with multiple access users is equal to $J = 4800$, while the characteristics of the developed steganographic method directly depend on the number of users simultaneously transmitting information. So, with the number of users simultaneously transmitting information $N \le 32$, the PSNR value does not exceed the level of 30 dB, while with the number of users $N \le 64$ there is no intra-system interference.

3. The proposed steganographic method with multiple access is characterized by flexibility in the distribution of steganographic channel resources: if necessary, the throughput of the steganographic channel can be increased with a decrease in PSNR values, or, conversely, the reliability of perception of a steganographic message can be increased by reducing the number of users simultaneously operating in the system. In this case, the embedding of information into the container by each of the users, occurs independently.

References

1. Astuti Y. P. et al. Simple and secure image steganography using LSB and triple XOR operation on MSB. *International Conference on Information and Communications Technology (ICOIACT). IEEE*. 2018. P. 191-195.

2. Su A., Ma S., Zhao X. Fast and secure steganography based on J-UNIWARD. *IEEE Signal Processing Letters*. 2020. Vol. 27. P. 221-225.

3. Li W. et al. Shortening the cover for fast JPEG steganography. *IEEE Transactions on Circuits and Systems for Video Technology*. 2019. Vol. 30. No. 6. P. 1745-1757.

4. Singh N. High PSNR based image steganography. *Int J Adv Eng Res Sci (IJAERS)*. 2019. Vol. 6, No. 1. P. 109-115.

5. Krishnaveni N., Periyasamy S. Image steganography using LSB embedding with chaos. *International Journal of Pure and Applied Mathematics*. 2018. Vol. 118, No. 8. P. 505-509.

6. Qiao T. et al. Robust steganography resisting JPEG compression by improving selection of cover element. *Signal Processing*. 2021. Vol. 183. P. 108048.

7. Zhu Z. et al. Robust steganography by modifying sign of DCT coefficients. *IEEE Access*. 2019. Vol. 7. P. 168613-168628.

8. Bao Z. et al. A robust image steganography on resisting JPEG compression with no side information. *IETE Technical Review*. 2018. Vol. 35, No. sup1. P. 4-13.

9. Sheidaeian H., Zolfaghari B., Zobeiri M. An Efficient and Secure Approach to Multi-User Image Steganography Using CRC-Based CDMA. *International Conference on Signal Acquisition and Processing. Singapore*. 2011. Vol. 2. P. 1-5.

10. Horadam K. J. Hadamard matrices and their applications. Princeton university press, 2012. 280 p.

11. Kobozeva A. A., Sokolov A. V. Robust Steganographic Method with Code-Controlled Information Embedding. *Problemele Energeticii Regionale.* 2021. Vol. 52, No. 4. P. 115-130.

12. Mazurkov M. I., Broadband Radio Communication Systems. Odessa: Science and Technology, 2010. 340 p.

СТЕГАНОГРАФІЧНИЙ МЕТОД З МНОЖНИМ ДОСТУПОМ НА ОСНОВІ ЧАСТОТНО-ПРОСТОРОВИХ МАТРИЦЬ

А.В. Соколов

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

Вирішення низки завдань із застосуванням стеганографії вимагає організації множинного доступу до стеганографічного каналу передачі інформації. При цьому існуючі розробки мають на увазі використання технології MC-CDMA, яка характеризується строго регламентованою кількістю каналів, що розділяються, вимагає одночасного вбудовування інформації від усіх абонентів, а також є дезінтегрованою із застосованим стеганографічним алгоритмом. У цій статті розроблено повноцінний стеганографічний метод з множинним доступом, заснований на застосуванні частотно-просторових матриць — кожному користувачеві виділяються дві кодові ознаки: частотна і просторова, на основі яких відбувається генерація кодових слів, що застосовуються для передачі інформації. Загальна кількість абонентів, зареєстрованих у працюючій на основі запропонованого стеганографічного методу системі, може досягати J=4800, у той час як загальна кількість абонентів, що одночасно передають інформацію, може досягати значення N=100 при практично прийнятних параметрах системи. При цьому вбудовування інформації абонентами відбувається незалежно один від одного в будь-який зручний для них час. Для забезпечення найбільшої кількості абонентів, що одночасно працюють, а також з метою мінімізації рівня внутрішньосистемних перешкод, запропоновано S-код просторових розстановок, а також F-код частотних розстановок на основі коду Ріда-Соломона. Розроблений стеганографічний метод з множинним доступом характеризується гнучкістю в розподілі ресурсів стеганоканалу: у разі необхідності пропускну спроможність стеганоканалу може бути збільшено зі зменшенням значень PSNR, або ж, навпаки, може бути збільшена надійність сприйняття стеганоповідомлення за рахунок зменшення кількості абонентів, що одночасно працюють.

Ключові слова: стеганографія, кодове управління, множинний доступ, кодовий розподіл каналів, частотно-просторові матриці.

DOI 10.15276/imms.v12.no1-2.15
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 12 (2022), No. 1-2, pp. 15-22

РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЗБЕРІГАННЯ ТА ЗАХИСТУ ДАНИХ ДЛЯ ПРИВАТНОГО ТА КОРПОРАТИВНОГО ЗАСТОСУВАННЯ

Б.В.Гаврилюк, В.В. Зоріло, Н.І.Кушніренко, О.Р.Осколкова

1, пр.Шевченка, Національний університет «Одеська політехніка», 65044, Одеса
vikazorilo@gmail.com, whiteswanhelena@gmail.com

Кажуть, що найкращий менеджер паролів – це наш мозок. У цьому твердженні є сенс, але іноді наш мозок не справляється, доводиться задіяти зовнішні ресурси. Кількість паролів на одного користувача зростає з кожним роком: нові соціальні мережі, нові банківські рахунки, нові реєстрації в різних сервісах, акаунти на різних сервісах (телевізійних, музичних, послуги інтернет-провайдерів тощо). За правилами інформаційної безпеки користуватись одним паролем для різних клієнтських сервісів не є раціональним, тому що якщо зловмисники зможуть, наприклад, підібрати пароль до вашої електронної пошти, вони спробують застосувати його і до інших ваших застосунків на кшталт інтернет-банкінг та інше. Сучасна людина розуміє, що для кожного сервісу потрібен свій унікальний пароль. Пароль має бути надійним, містити певну кількість символів, де серед цифр та літер надійність пароля підвищують спеціальні символи та зміни регістрів. Запам'ятати все це важко. Але запам'ятати один пароль – цілком під силу більшості з нас. Вибрати зручний та надійний менеджер паролів – непросте завдання. Ви маєте дійсно довіряти сервісу. Зрештою, саме він зберігатиме ваші секретні дані. В роботі протестовано два десятки менеджерів паролів і вибрано одинадцять, які є найкращими з погляду функціональності, безпеки та зручності. Проте кожен з відомих менеджерів не враховує індивідуальні особливості користувачів і потребує доповнень згідно їх потреб. Тому створення програмного забезпечення для зберігання паролів у зашифрованому вигляді є актуальним. Доступ до зашифрованих паролів може відбуватися через той один пароль, який необхідно запам'ятати. Такі програмні за стосунки було створено у даній роботі з урахуванням потреб корпоративного та приватного користування.

Ключові слова: захист даних, парольний менеджер, шифрування, криптографія.

Вступ

Причинами цього дослідження стала проблема зі зберіганням великої кількості паролів. Безліч паролів було безповоротно втрачено і доводилося створювати нові і знову втрачати. Тому постало питання зберігання всіх паролів, бажано в одному надійному місці.

Для позбавлення цієї проблеми було вирішено використовувати існуючі рішення – «менеджери паролів» або у разі, якщо існуючі рішення не підійдуть, створення свого програмного продукту.

Навіть найкращий у світі менеджер паролів буде марним, якщо він не відповідає конкретним потребам або просто занадто складний у використанні. Ось чому не слід поспішати і завантажувати менеджер паролів №1, представлений у будь-якому топ-листі – проведемо дослідження існуючих рішень.

Потрібно бути впевненим, що рішення має достатній функціонал і необхідну кількість одночасних підключень. Крім того він має мати зручний інтерфейс.

Більшість менеджерів паролів пропонують однаковий набір функцій: синхронізація, генерація паролів та двофакторна автентифікація. Для вибірки використовувалися такі критерії. Шифрування: все, що менше 256-бітного шифру AES військового рівня, є неприпустимим. Додаткові можливості: сканування даркнета, U2FA, VPN або безпечний чат – ось лише деякі з прикладів, які надають додаткову цінність продукту. Багатофакторна автентифікація: на додаток до власного

автентифікатора хороший менеджер паролів повинен пропонувати кілька інших. Біометричні дані (Touch ID та Face ID) також повинні працювати на всіх пристроях. Імпорт та експорт: від менеджера паролів не так багато користі, як від неможливості імпортувати ваше сховище з іншої служби чи браузера. Експорт також важливий у випадку, якщо ви вирішите змінити менеджер паролів. Програми та розширення для браузерів: чим більше тим краще. Співвідношення ціна-якість. Служба підтримки клієнтів: онлайн-чат або підтримка по телефону – ознака якісного обслуговування. Те саме стосується доступності 24/7.

Огляд сучасних рішень

На сьогоднішній день існує безліч програм, які мають певну систему авторизації. Важливою метою є зберігання та забезпечення захисту тих даних, що стосуються авторизації певної людини чи підприємства.

До основної мети забезпечення та зберігання даних відноситься наявність усіх доступів до систем, які має певна людина чи організація. Важливо зберігати усю інформацію щодо авторизації до різних систем. Адже втрата конфіденційної інформації конкретного користувача або підприємства може призвести до дуже тяжких та іноді до незворотних наслідків. Для вирішення даного питання використовують спеціально призначені системи для збереження парольної інформації користувача або цілого підприємства. Так як існує багато систем, які спрямовані на вирішення даного питання, перед користувачем або організацією постає вибір: яку саме систему варто обрати. Для того, щоб обрати одну з систем, необхідно провести аналіз та огляд сучасних систем, що спрямовані на вирішення даного питання. Існують наступні програми, які надають можливість користувачам зберігати свої парольні дані:

1) LastPass
2) Dashlane
3) 1Password
4) Bitwarden
5) Keeper
6) NordPass
7) Enpass
8) RoboForm
9) RememBear
10) Zoho Vault
11) Passbolt

LastPass – надійний менеджер паролів. Він є однією з найдешевших систем у використанні (3 долари на місяць).

Цей менеджер паролів використовує багатофакторну автентифікацію (MFA), яка може змінюватись від «вашого пристрою» (смартфон) до біометричних даних (відбиток пальця). Можливе використання не тільки власного автентифікатора, але й автентифікатора від YubiKey, Sesame, Google або Microsoft.

Цей менеджер паролів можна встановити на всіх основних платформах і в багатьох браузерах. LastPass має розширення для Chrome, Firefox, Safari, Opera, Edge та Edge Legacy. Але в той же час він не підтримує Vivaldi або Brave. У цій системі присутні функції автозаповнення та автозбереження.

Користуватися даною системою можна і безкоштовно, але в такому випадку користувач не матиме можливості використовувати весь функціонал системи. Без платної підписки користувачеві не доступні такі функції як: оперативне спілкування з техпідтримкою, функція аварійного доступу (коли користувач може надати довіреній особі своє сховище з паролями), обмін паролем через мережу з іншими користувачами, не доступна опція багатофакторної автентифікації для захисту парольних даних. При цьому для звичайного користувача захист даних здійснюється 256-бітовим шифруванням.

Dashlane підтримує три методи аутентифікації, перший з яких – двофакторна аутентифікація (2FA). Це чудовий спосіб захистити обліковий запис, навіть якщо хтось отримає ваш майстер-ключ. Другим фактором може бути інформація, яку знаєте тільки ви (PIN-код), або ваш смартфон або біометрична інформація (наприклад, Face ID).

Преміум-план доступний за ціною $4,99 і пропонує універсальну двофакторну автентифікацію (U2FA). Це безпечніша версія 2FA, в якій пристрій USB або NFC можна підключити до будь-якого комп'ютера для миттєвого доступу до ваших паролів. У той же час U2FA простіша у використанні, пристрій обмінюється даними з комп'ютером за протоколом HID.

Також є біометричний логін, який можна використовувати замість майстер-паролю. Dashlane підтримує як Touch ID, так і Face ID, тому все залежить від пристрою користувача.

Цей менеджер паролів простий у встановленні та використанні, працює на всіх основних платформах і має розширення для браузерів Chrome, Firefox, Safari, Internet Explorer та Edge. Можна імпортувати паролі з більшості браузерів, за винятком мобільних.

Наступним у списку можливостей Dashlane йде сканер даркнета. За бажанням користувача система може використовувати електронну пошту, щоб перевірити, чи немає витоків паролів чи банківських реквізитів. Враховуючи, що кожен день з'являються мільйони нових записів, сканер даркнета може стати чудовим інструментом для запобігання крадіжці особистих даних. Також є вбудований VPN.

1Password – потужний інструмент для зберігання, створення та керування паролями користувача або організації.

Для роботи потрібен майстер-пароль, проте замість цього можна використовувати біометричний логін, як використовується відбиток пальця або обличчя. Інший варіант 2FA – використовувати телефон користувача для створення одноразового пароля.

Крім всіх основних платформ, 1Password підтримує Chrome OS та командний рядок. Що стосується розширень браузера, можливо обрати Chrome, Firefox, Edge та Brave.

Цей менеджер паролів має автозаповнення та синхронізує дані користувача на всіх пристроях. Це також спрощує обмін паролями рахунок створення гостьових облікових записів. 1Password не має обмежень на кількість людей, які можуть користуватися вашим обліковим записом, що робить його доступним для використання у рамках підприємства.

У 1Password має функцію під назвою: «Сторожова вежа». Це веб-сканер, однак він також перевіряє, чи підтримує веб-сайт 2FA і чи використовує HTTPS. А також має функцію «Режим подорожі». Вона потрібна для приховування конфіденційної інформації на телефоні. Якщо користувач втрате телефон або хтось викраде його, можливо можете бути впевненим, що вся особиста інформація в безпеці.

Перейти до 1Password дуже просто, адже у системі можливо імпортувати дані з Chrome, звичайного CSV та інших популярних менеджерів паролів, включаючи LastPass та Dashlane.

Увесь функціонал системи доступний для використання з платною підпискою: 2,99 долара на місяць для одного користувача та є тарифний план на 5 користувачів, який коштує 4,99 долара на місяць.

Програма Bitwarden допомагає зберігати та обмінюватися конфіденційними даними з будь-якого пристрою. Програмою користуються по всьому світу, тому що вона працює 40 мовами. У сервісі можна створювати унікальні паролі, а постійний аудит безпеки робить Bitwarden надійним менеджером для зберігання паролів.

Keeper надає персональне сховище кожному користувачу для того, щоб зберігати та управляти власними паролями, файлами, обліковими даними тощо. Дане сховище представлене у зашифрованому вигляді.

Keeper — надійний та безпечний менеджер паролів, який використовує підхід із нульовою довірою. Це означає, що дані користувача зашифровані не на сервері, а на пристрої, і тільки ви можете їх розшифрувати.

Усі менеджери паролів мають двофакторну автентифікацію, а в Keeper їх безліч. Можливо використовувати SMS, автентифікатор Google та Microsoft (TOTP), RSA SecurID, Duo Security, U2F (YubiKey) та KeeperDNA. Останній є запатентованим варіантом 2FA, який дозволяє біометричну автентифікацію за допомогою смартфона або розумного годинника.

У Keeper є програми для Windows, macOS, Linux, Android та iOS. Щодо розширень браузера, вони використовуються лише для автоматичного заповнення облікових даних. Звичайно, це покращує сумісність - так званий KeeperFill працює з Chrome, Firefox, Opera, Edge та IE.

Цей менеджер паролів є багатофункціональним. Деякі функції недоступні в жодному іншому менеджері паролів. Наприклад, KeeperChat – безпечна система обміну повідомленнями із самознищуючими повідомленнями та медіа-галереєю для приватних фотосесій та музичних кліпів. Або Security Audit, який перевіряє всі паролі користувача, оцінює їхню надійність і пропонує змінити слабкі. Також є сканер даркнета під назвою Breach Watch, який перевіряє, чи не були викрадені імена користувачів чи паролі.

Keeper підтримує імпорт даних з Dashlane, 1Password, ZOHO та інших менеджерів паролів. Що стосується браузерів, можна імпортувати їх з Chrome, Firefox, Opera, Edge і навіть з Internet Explorer. Доступний експорт до PDF, CSV або JSON.

Безкоштовної версії немає. Середня ціна Keeper складає 2,91 долара США на місяць за річної оплати. Проте KeepChat та моніторинг Dark Web вимагають додаткових витрат. Крім того, існують особисті, сімейні, студентські, ділові та корпоративні плани, тому остаточна ціна залежить від цілі використання системи.

Основні функції та параметри додатку. Keeper надає персональне сховище кожному користувачу для того, щоб зберігати та управляти власними паролями, файлами, обліковими даними тощо. Дане сховище представлене у зашифрованому вигляді. Існує можливість автоматичного заповнення паролів. Кількість даних, які можна зберігати у додатку, не обмежуються. Він надає функції консолі адміністратора, контроль версій, рольовий доступ та історію записів та звітування.

Програма спрямована на те, щоб зберігати паролі та особисту інформацію. Keeper працює на будь-якому мобільному пристрої та ПК, де можливе створення власного зашифрованого сховища. Сервіс швидко вигадує нові та надійні паролі та одночасно застосовує їх до підключених облікових записів у додатках та на веб-сайтах. Крім паролів, у менеджері зберігають паспортні дані, посвідчення водія, важливі фотографії, документи та інші типи файлів.

Диспетчер паролів NordPass є частиною пакету онлайн безпеки, який включає шифратор NordLocker і NordVPN.

NordPass використовує майстер-пароль для захисту сховища користувача та синхронізує всі дані між пристроями. Також можна використовувати Touch ID або Face ID (тільки для iOS). Для двофакторної автентифікації знадобиться додаток для автентифікації та електронний лист, на який буде надіслано шестизначний код.

Цей менеджер паролів може працювати на Windows, MacOS, Linux, Android та iOS. Також можливо встановити розширення NordPass у Chrome, Firefox, Safari, Opera, Brave, Vivaldi та Edge.

NordPass враховує всі особливості та потреби користувача. Можливо генерувати паролі та оцінювати їхню надійність, використовувати автозаповнення та автозбереження, а також ділитися обліковими даними для входу.

NordPass має деякі унікальні особливості. Користувачеві надається можливість впорядкувати дані в папках для полегшення доступу та використовувати OCR для автоматичного сканування текстової інформації з кредитних карток, документів та фотографій. Крім того, автономний режим дозволить користувачу отримати доступ до свого сховища, навіть якщо немає підключення до Інтернету.

NordPass також пропонує безліч можливостей для імпорту паролів. Сюди входять найпопулярніші менеджери паролів, крім Zoho Vault, та найпопулярніші браузери, крім Safari. Проте, користувачеві доведеться вручну перевіряти, чи експортований файл відповідає критеріям NordPass.

NordPass пропонує шифрування XChaCha20 наступного покоління з використанням Argon 2 для отримання ключів.

NordPass має відмінну службу підтримки, яка включає цілодобовий чат, електронну пошту і базу знань, що постійно зростає.

Безкоштовна версія потужна, але дозволяє використовувати лише один активний пристрій та не передбачає можливість безпечного обміну та довірених контактів. Коштує 2,49 доларів США на місяць (при покупці на 2 роки).

Enpass – це мінімалістичний менеджер паролів. Він є крос-платформний, але насамперед призначений для автономного використання. Користувач може налаштувати параметри синхронізації між різними пристроями за допомогою сторонніх платформ хмарного хостингу, таких як OneDrive, Dropbox, iCloud і т.д.

Enpass захищає ідентифікаційні дані користувача, інформацію про кредитну картку та багато іншого. Для захисту паролів використовується інструмент моніторингу. Він допомагає оцінити надійність паролів і змінити їх у разі повторного використання пароля. Також є генератор паролів find-secure.

Шифрування даних виконується за допомогою шифру AES-256 з розширенням SQLCIPHER.

Програма безкоштовна, якщо використовуватимете тільки настільну версію. Якщо потрібно перемикатися між настільними та мобільними обліковими записами, користувачу необхідна сплатити ліцензію.

RoboForm - один із найстаріших менеджерів паролів. Він існував ще до того, як менеджери паролів стали важливими продуктами безпеки. Цільова аудиторія - бізнес. Розробники пропонують самостійний хостинг для безкоштовних користувачів, але якщо обрати преміум-план, користувач зможе використати їхню безшовну синхронізацію. Це означає, що користувач, що придбав преміум-план може отримати доступ до всіх паролів на всіх своїх пристроях.

RoboForm має кілька функцій, які можуть бути корисними. Він має стандартний генератор паролів із змінними, які можна змінити.

Також можливо поділитись своїми обліковими даними з іншими користувачами RoboForm. Є також класичні менеджери паролів, такі як безпечне хмарне сховище та спільні папки.

Всі дані, які користувач завантажує, захищені шифруванням AES-256.

Ціна на преміум-опцію починається з 1,66 долара на місяць під час оплати кожні п'ять років.

RememBear – це менеджер паролів, який зберігає, синхронізує та генерує паролі. Також можливо зберігати нотатки, кредитні картки та логіни, які пізніше можна використовувати для автозаповнення. Як і всі інші програми, RememBear підтримує двофакторну автентифікацію та біометрію (відбиток пальця та обличчя).

Даний сервіс має програми для Windows, macOS, Android та iOS. Існують також розширення для браузерів Chrome, Firefox та Safari, але вони не є автономними.

RememBear також може імпортувати із Chrome, з 1Password та LastPass.

Безкоштовна версія демонструє лише частину функцій RememBear. З безкоштовною версією не можливо створити резервну копію своїх паролів, тобто доведеться зберігати другу копію в іншому місці. Крім того, синхронізація між пристроями не дозволена. У тому числі безкоштовна версія не має пріоритетної підтримки, тому отримання відповіді може забрати деякий час.

RememBear коштує від 2,5 доларів на місяць.

Більшість найкращих менеджерів паролів орієнтовані на споживача. Навіть якщо вони мають бізнес-рішення, сегмент B2C збільшує їх дохід. Це не стосується Zoho Vault, яке знаходиться десь між споживачем та бізнесом. Компанія позиціонує Vault як менеджер паролів для команд.

Zoho Vault не має класичного інсталятора, замість цього використовується веб-додаток. Але є клієнти для Android та iOS. Що ж до розширень для браузера, то вибір досить широкий. Можливо обрати з Chrome, Firefox, Safari, Edge, Brave та Vivaldi.

Деякі менеджери паролів є частиною пакету онлайн-безпеки, який включає VPN або інструмент для шифрування файлів. Zoho має величезний список додатків, які інтегруються з Vault, що є лише одним з безлічі доступних сервісів. Крім того, цей менеджер паролів пропонує єдиний вхід для Office 365, Windows AD, Dropbox та ZenDesk.

Цей менеджер паролів підтримує понад 400 сайтів. Zoho Vault має складну систему обміну паролями, яка надає користувачу багаторівневі фільтри, доступ з обмеженням часу і підтвердження або відгук одним клацанням миші.

Можливо імпортувати в Zoho Vault з більш ніж 20 додатків та браузерів, включаючи Dashlane, LastPass, 1Password та Keeper. Проте, імпорт із Safari або Edge недоступний. Експорт доступний або у простому .csv, або у форматі, що відповідає формату Zoho Vault.

Сервіс використовує шифрування військового рівня та архітектуру з нульовим рівнем довіри. Майстер-пароль користувача захищений алгоритмом PBKDF2, який надає йому більшої надійності.

Zoho Vault пропонує підтримку через email, через форму зворотного зв'язку або по телефону.

Дана система має застарілий інтерфейс веб-застосунку, що може перешкоджати якісному та швидкому користування системою.

Вартість ліцензії сягає 3,6 доларів на місяць, з цим можна отримати можливість використовувати п'ять пристроїв для кожного облікового запису на додаток до спільних папок та звітів про доступ за паролем.

Passbolt — один із небагатьох менеджерів паролів із відкритим вихідним кодом. Він призначений для підприємств та промислових підприємств.

Passbolt вимагає використання майстер-паролю у поєднанні із закритим ключем.

Основним недоліком є залежність від закритого ключа чи ключової фрази. Якщо користувач втрачає будь-кого з них, сховище стане недоступним. Незважаючи на те, що це найбезпечніший метод налаштування, йому не вистачає зручності для користувача. Крім того, для зміни ключової фрази, знадобиться базове розуміння роботи з кодом.

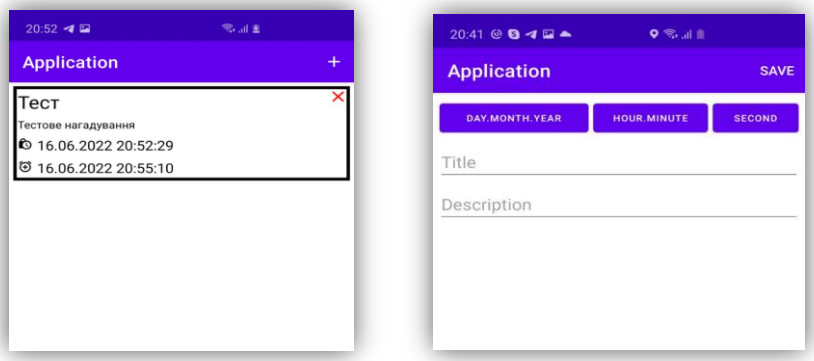
Сервери Passbolt не мають доступу до даних у вигляді відкритого тексту. Паролі завантажуються у хмару лише у зашифрованому вигляді.

Passbolt може бути абсолютно безкоштовним способом керування паролями, хоча це не найзручніший менеджер паролів для не надто технічно підкованих користувачів.

У ході огляду та аналізу існуючих аналогів, які є одними з найкращих рішень на сьогоднішній момент, немає жодного лідера, що не мав би певних недоліків.

Розробка

Для покращення даних аналогів була реалізована розробка нового застосунку, який спрямований на вирішення задач підприємства. Однією з головних задач для даного програмного застосунку є авторизація певного користувача в системі, зберігання та керування парольною інформацією. Для даного застосунку був вирішений недолік, що характерний для кожної з систем, а саме: це можливість користуватися повним функціоналом системи без придбання платної ліцензії. У якості удосконалення застосунку була запроваджена та реалізована система нагадувань, що дозволяє користувачеві створювати власні робочі нагадування. Під час огляду сучасних рішень проблеми, було виявлено, що в жодної з системи немає даного функціоналу, який дозволяв би користувачу створювати власні нагадування та визначати їх час надходження у вигляді сповіщення. Даний функціонал є дуже важливим аспектом для роботи підприємства, адже він забезпечує виконання робочих процесів вчасно, що допомагає підприємству будувати якісну онлайн-інфраструктуру бізнесу.
Інтерфейс програми показано на рисунку 1.



а) системи нагадування б) створення запису

Рис.1. Інтерфейс

Відпрацювання нагадування у вигляді push-сповіщення показано на рис. 2.

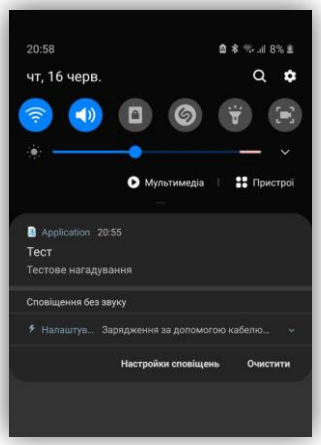


Рис. 2. Відпрацювання нагадування

Переваги розробленого застосунку у порівнянні з існуючими аналогами полягають у наявності системи корпоративних нагадувань. Застосунок має зручний та зрозумілий для користувача інтерфейс. Можливе автономне використання функціоналу нагадувань; додаток є безкоштовним та не потребує придбання ліцензії.

Висновки

У статті виконано фундаментальний огляд найкращих існуючих менеджерів паролів на думку авторів. Кожен з 11 менеджерів паролів унікальний і вибір того, який краще використовувати залежить тільки від користувача: його потреб і фінансових можливостей. Також з даного огляду можна побачити, що в кожній системі є власні переваги та недоліки. Розробка індивідуальних менеджерів згідно з цим є актуальною задачею. Згідно з цим була проведена розробка нового програмного застосунку, який удосконалює існуючі системи та задовольняє саме ті потреби організації, що не наявні у повному складі в жодній із наведених систем.

Список літератури

1. Dashlane URL: https://www.dashlane.com
2. NordPass URL: https://nordpass.com/?gclid=CjwKCAjwh-CVBhB8EiwAjFEPGe6X3Ez9NDz7tjHQspDReZASWuyQRWECogirTWCpGYhulGZxsWC2WxoCkOsQAvD_BwE
3. 1Password URL: https://1password.com/ru/
4. Keeper URL: https://www.keepersecurity.com/ru_RU/
5. Enpass URL: https://www.enpass.io
6. RoboForm URL: https://www.roboform.com/ru
7. LastPass URL: https://www.lastpass.com
8. RememBear URL: https://www.remembear.com
9. Zoho Vault URL: https://www.zoho.com/vault/
10. Passbolt URL: https://www.passbolt.com
11. Bitwarden URL: https://bitwarden.com

DEVELOPMENT OF DATA STORAGE AND PROTECTION SOFTWARE FOR PRIVATE AND CORPORATE APPLICATIONS

B.V. Gavrilyuk, V.V. Zorilo, N.I. Kushnirenko, O.R. Oskolkova

1, Shevchenko Ave., National Odessa Polytechnic University, 65044, Odesa Ukraine
vikazorilo@gmail.com, whiteswanhelena@gmail.com

It is said that the best password manager is our brain. This statement makes sense, but sometimes our brain does not cope, we have to use external resources. The number of passwords per user is growing every year: new social networks, new bank accounts, new registrations in various services, accounts on various services (television, music, Internet service providers, etc.). According to the rules of information security, using the same password for different client services is not rational, because if attackers can, for example, choose a password for your e-mail, they will try to apply it to your other applications such as Internet banking and more. Modern man understands that each service needs its own unique password. The password must be strong, contain a certain number of characters, where among the numbers and letters the reliability of the password is increased by special characters and case changes. It's hard to remember. But remembering one password is beyond the power of most of us. Choosing a convenient and reliable password manager is not an easy task. You really have to trust the service. In the end, it is he who will store your confidential information. In this paper, two dozen password managers were tested and eleven were selected, which are the best in terms of functionality, security and convenience. However, each of the well-known managers does not take into account the individual characteristics of users and needs additions according to their needs. Therefore, the creation of software for storing passwords in encrypted form is relevant. Encrypted passwords can be accessed through the one password you need to remember. Such relationship software was created in this paper, taking into account the needs of corporate and private use.

Keywords: data protection, password manager, encryption, cryptography.

DOI 10.15276/imms.v12.no1-2.23
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 12 (2022), No. 1-2, pp. 23-28

ІНФОРМАЦІЙНА СИСТЕМА НОРМАТИВНОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ПІДПРИЄМСТВ

В. П. Галицький, О. А. Стопакевич

Національний університет «Одеська політехніка»
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: val.gal1969@ukr.net, stopakevich@gmail.com

Зараз склалася ситуація, коли розроблено значна кількість міжнародних стандартів, які забезпечують потреби майже всіх галузей інформаційної та кібербезпеки. Але, в той же час, дуже значна частина підприємств і організацій майже всіх напрямків і галузей не відповідає вимогам цих стандартів, як мінімум в Україні. Більш того, дуже значна більшість керівників підприємств не володіють змістом цих стандартів. Приведено короткий опис системи менеджменту інформаційної системи на базі міжнародних стандартів ISO/IEC 27000, вимоги до її функціонування. Розроблена нова інформаційна система нормативного забезпечення кібербезпеки підприємств, яка забезпечує доступ до бази даних, що містить таблиці термінів з кібербезпеки та міжнародних стандартів з менеджменту інформаційної безпеки. Програмне забезпечення інформаційної системи складається з виконавчого файлу, написаного мовою програмування Python з графічним інтерфейсом. Для того, щоб систему використати її потрібно запустити під операційною системою Windows, але її можна легко адаптувати під любу операційну систему, де встановлено Python. Бажано, щоб комп'ютер був під'єднаний до Інтернету. При кожному виклику програми проходить перевірка на оновлення бази даних на web-сторінці програми та, при необхідності, інформаційна система завантажує оновлену базу даних клієнту. Зміну інформації в базі даних здійснює адміністратор програми. Якщо web-сторінка програми не знаходиться, програма працює без оновлення. Використання розробленої «Інформаційної системи нормативного забезпечення кібербезпеки підприємств» має дати змогу підвищити правову грамотність в сфері кібербезпеки та інформаційної безпеки у керівництва підприємств та працівників, яких це стосується. А також сприятиме впровадженню ефективного менеджменту, який буде якісно впливати на кінцевий результат підприємства. Система може бути корисна для викладачів та студентів учбових закладів, які пов'язані з кібербезпекою.

Ключові слова: Інформаційна безпека, кібербезпека, кіберпростір, програмне забезпечення, стандарт, ISO/IEC 27000.

Вступ

Зараз склалася ситуація, коли розроблена значна кількість міжнародних стандартів, які забезпечують потреби майже всіх галузей інформаційної та кібербезпеки. Але, в той же час, дуже значна частина підприємств і організацій майже всіх напрямків і галузей не відповідає вимогам цих стандартів, як мінімум в Україні. Більш того, дуже значна більшість керівників підприємств не знають про зміст цих стандартів.

За створення, впровадження, перевірку (аудит) та експлуатацію єдиної системи інформаційної та кібербезпеки відповідає менеджмент інформаційної безпеки (ІБ) та відповідна група міжнародних стандартів. Тут потрібно пояснити, що стандарти регламентують поведінку менеджменту не в економіці, а саме в створенні єдиної системи інформаційної і кібербезпеки.

Зародження перших принципів менеджменту інформаційної безпеки відбулося наприкінці 1980-х років у Великобританії, коли Міністерство торгівлі та промисловості ініціювало створення робочої групи, яка мала на меті розробити найкращі практики щодо забезпечення інформаційної безпеки. Як результат роботи у 1989 році було опубліковано перший стандарт PD 0003 *Практичні правила управління ІБ*. У 1995 році Британським інститутом стандартів (British Standards Institution) було прийнято

національний стандарт BS 7799-1 з тою ж назвою, який описував 10 областей та 127 механізмів, які були необхідними для побудови системи менеджменту інформаційної безпеки (СМІБ). Друга частина цього стандарту – BS 7799-2 *СМІБ. Вимоги та настанови щодо застосування* – з'явилася у 1998 році та містила вимоги до загальної моделі побудови СМІБ, а також набір інших обов'язкових вимог, на відповідність яким повинна була проводиться обов'язкова сертифікація. Це період початку активного розвитку системи сертифікації в галузі менеджменті безпеки. В кінці 1999 року експерти Міжнародної електротехнічної комісії IEC (International Electrotechnical Commission) та представники Міжнародної організації зі стандартизації (International Organization for Standardization) заявили, що в рамках існуючих стандартів відсутній спеціалізований стандарт менеджменту ІБ. У результаті взявши за основу BS 7799-1 було прийнято відповідний міжнародний стандарт ISO / IEC. Згодом обидві частини стандарту BS 7799 були переглянуті та адаптовані до міжнародних стандартів систем управління якістю ISO / IEC 9001 та екологією ISO / IEC 14001, а через рік стандарт BS 7799-1 був прийнятий як міжнародний стандарт ISO / IEC 17799-2000 *Інформаційні технології. Практичні правила управління ІБ* [1]. У 2008 року Національний Банк України почав застосовувати вимоги міжнародного стандарту на практиці та зобов'язав всі місцеві банки виконувати його вимоги, створюючи систему менеджменту інформаційної безпеки на основі стандартів безпеки ISO. Оскільки у складі ISO / IEC відповідальність за розробку сімейства міжнародних стандартів з менеджменту ІБ несе підкомітет №27, нумерація даного сімейства стандартів починається з 27000.

Короткий опис системи менеджменту ІБ

Відповідно до стандартів ISO 27000, цілі захисту інформаційної безпеки включають три основні аспекти.

1. Конфіденційність: конфіденційну інформацію можуть переглядати та розголошувати лише уповноважені особи. Тому доступ до цієї інформації має бути належним чином захищений. Конфіденційність порушується, наприклад, якщо зловмисник може підслуховувати комунікації.

2. Цілісність: інформація повинна бути захищена від невиявлених маніпуляцій, щоб зберегти її точність і повноту. Цілісність порушується, якщо, наприклад, зловмисник може змінити дані дослідження без виявлення.

3. Доступність: інформація, послуги або ресурси мають бути доступними для використання для законних користувачів у будь-який час. Доступність може бути порушена, наприклад, через DDoS-атаку, яка навмисно перевантажує системи.

4. Інші аспекти – це автентичність, підзвітність, відданість і надійність.

Ступінь досягнення інформаційної безпеки можна визначити на основі того, наскільки цілі захисту виконуються.

Позначення міжнародних стандартів менеджменту інформаційної безпеки має формат

ISO/IEC nnnnn :yyyy заголовок,

де nnnnn – номер стандарту, yyyy – рік опублікування, заголовок – предмет стандартизації.

ISO зараз налічує 157 національних членів із 195 країн світу.

Серія ISO/IEC 27000, на основі якої розроблятимемо інформаційну систему, містить рекомендації щодо менеджменту інформаційної безпеки, менеджменту ризиків та впровадження засобів контролю в контексті загальної системи менеджменту інформаційної безпеки (СМІБ). Серія застосовується до організацій будь-яких форм і розмірів, також охоплюють не тільки питання конфіденційності, а й технічної безпеки.

В поняття підприємство вкладатимемо більш широкий сенс, в нього входитимуть не тільки юридичні особи, а і фізичні (приватні підприємці, тощо), приватні особи. Великі підприємства можуть дозволити собі мати в штаті фахівця з кібербезпеки, а в деяких випадках і цілі відділи. А що робити приватному підприємцю?

Деяку допомогу йому може дати «Інформаційна система нормативного забезпечення в кібербезпеці». В цій системі він знайде всі стандарти, а також тлумачення визначень, які використовуються в стандартах СМІБ. Так, наприклад, слово «атака» в тлумачному словнику має два визначення, які геть не схожі на визначення згідно стандарту ISO/IEC 27000 і це потрібно розуміти.

СМІБ – це документована система менеджменту, яка складається з набору засобів контролю безпеки, які захищають конфіденційність, доступність і цілісність активів від загроз і вразливостей; це системний підхід до розробки, впровадження, функціонування, моніторингу, аналізу, забезпечення та покращення інформаційної безпеки організації для досягнення бізнес-цілей. Розробляючи, впроваджуючи, керуючи та підтримуючи СМІБ, організації можуть захистити свої особисті та конфіденційні дані від компрометації, розкрадання чи нищення [2].

СМІБ ґрунтується на оцінці ризиків та рівнях прийнятності рішень організації, встановлених таким чином, щоб результативно обробляти ризики та управляти ними. Успішна реалізація СМІБ можлива за умови аналізу вимог щодо захисту інформаційних активів та застосування засобів управління для забезпечення захисту цих інформаційних активів відповідно до ситуації. Також чинниками, які сприяють успішній реалізації системи управління інформаційної безпеки є [3]: усвідомлення необхідності забезпечення інформаційної безпеки; призначення відповідальності за інформаційну безпеку; поєднання зобов'язань керівництва з інтересами заінтересованих сторін; підвищення значення соціальних цінностей; оцінка ризику, що визначає відповідні засоби управління для забезпечення прийнятних рівнів ризику; безпека як невід'ємний елемент інформаційних мереж та систем; активне попередження та виявлення інцидентів інформаційної безпеки; забезпечення комплексного підходу до управління інформаційною безпекою; постійна переоцінка рівня інформаційної безпеки та внесення змін за потреби.

Ефективне впровадження СМІБ є дуже складним процесом, при імплементації якого потрібно враховувати наступні кроки [4]:

1. Визначення обсягу послуг. Керівництво компанії має чітко визначити сфери застосування, цілі та межі СМІБ.

2. Визначення активів, які повинні бути захищені СМІБ. Це можуть бути інформація, програмне забезпечення, послуги та фізичні активи, такі як комп’ютери, кваліфікація, навички та досвід співробітників, а також інші нематеріальні активи, такі як репутація та репутація. Головна мета на даному етапі визначити критично важливі для бізнесу активи, від яких залежить виживання компанії.

3. Визначення та оцінка ризиків. Для кожного активу, який варто захищати, мають бути ідентифіковані та класифіковані потенційні ризики на основі юридичних вимог або вказівок щодо відповідності. Організації повинні визначити, який вплив мав би кожен ризик, якщо було б порушено конфіденційність, цілісність і доступність, або яка ймовірність виникнення ризиків, для того, щоб оцінити, які ризики є прийнятними, наприклад, з огляду на очікувану суму заподіяної шкоди, і які необхідно усунути за будь-яку ціну.

4. Визначення заходів. На основі попередньої оцінки ризику повинні бути обрані та впроваджені відповідні технічні та організаційні заходи для пом’якшення чи уникнення ризику. Це включає визначення чітких компетенцій та відповідальності.

5. Перевірка ефективності: застосовані та впроваджені заходи необхідно постійно контролювати та регулярно перевіряти на ефективність, наприклад, шляхом аудитів.

6. Внесення покращення. Якщо перевірка запроваджених заходів виявляє недоліки або були виявлені нові ризики, процес СМІБ необхідно запустити знову з самого початку. Таким чином, СМІБ можна постійно адаптувати до мінливих умов або вимог, постійно покращуючи інформаційну безпеку в компанії.

За допомогою СУІБ інформаційну безпеку можна систематично впроваджувати в усій компанії та забезпечувати дотримання всіх необхідних стандартів безпеки. Цей комплексний профілактичний підхід має ряд переваг [2]:

1. СМІБ гарантує, що власні інформаційні активи (наприклад, інтелектуальна власність, дані персоналу або фінансові дані), а також дані, довірені клієнтами або третіми сторонами, будуть належним чином захищені від будь-яких загроз.

2. Використовуючи СМІБ для того, щоб зробити інформаційну безпеку невід'ємною частиною своїх бізнес-процесів, компанії можуть постійно підвищувати рівень безпеки та зменшувати ризики інформаційної безпеки. Таким чином вони протидіють ризику інцидентів безпеки, які порушують безперервність бізнесу.

3. Застосовуються суворі вимоги до відповідності, особливо в дуже регульованих секторах, таких як фінанси або критична інфраструктура. Порушення законодавчих норм і договірних угод можуть призвести до великих штрафів. Завдяки СМІБ компанії гарантують, що вони відповідають всім нормативним та договірним вимогам, що також надає їм більшу операційну та юридичну визначеність.

4. Сертифікуючи свої СУІБ, компанії можуть перевіряти третім сторонам, що конфіденційна інформація обробляється безпечно. Це сприяє кращому зовнішньому іміджу та формуванню довіри, що, у свою чергу, означає конкурентну перевагу.

5. Структурована координація та орієнтоване на ризики планування заходів у СУІБ допомагає розставляти пріоритети, ефективно використовувати ресурси та інвестувати в потрібних місцях. Таким чином, після початкових додаткових витрат накладні витрати можна скоротити в довгостроковій перспективі.

Інформаційна система

Інформаційна система нормативного забезпечення складається з бази даних, яка вміщує таблиці термінів з кібербезпеки та міжнародних стандартів з менеджменту інформаційної безпеки. Програмне забезпечення інформаційної системи складається з виконавчого файлу, написаного мовою програмування Python з графічним інтерфейсом. Вікно для роботи з термінами показано на рис.1. Для переходу на форму слід натиснути вкладку **Термін**.

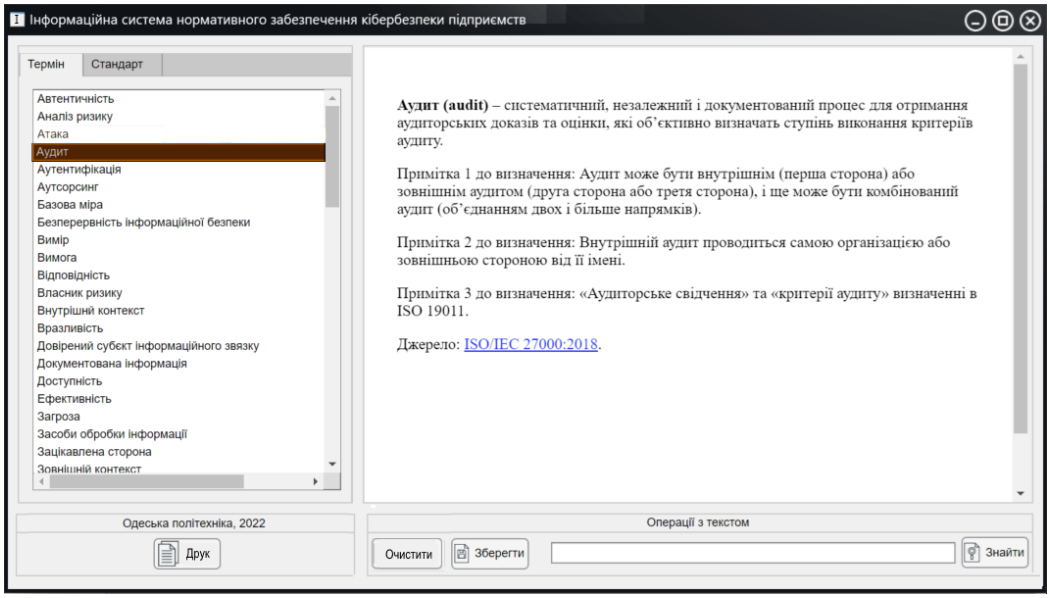


Рис.1. Вікно для роботи з термінами

Зліва в вікні можна вибрати термін, який інтересує користувача. При натисканні на термін у вікні справа з'явиться пояснення терміну, взяте із стандартів по менеджменту інформаційної безпеки серії 27000. Якщо користувач бажає знайти будь-який набір символів в тексті пояснення терміну треба ввести цей набір символів у поле знизу вікна

на натиснути кнопку **Знайти.** Якщо є бажання скопіювати чи роздрукувати виведений текст з допомогою стандартного діалогу Windows, треба натиснути кнопки **Зберегти** або **Друк**. Для того, щоби очистити поле пояснення терміну треба натиснути кнопку **Очистити**

Вікно для роботи з стандартами показано на рис.2. Для переходу на форму слід натиснути вкладку **Стандарт**. Зліва в вікні можна вибрати стандарт по менеджменту інформаційної безпеки серії 27000, який інтересує користувача. При наведені на термін у вікні справа з'явиться повний текст стандарту, взятий із стандартів по менеджменту інформаційної безпеки серії 27000 та двох законів України, які торкаються інформаційної безпеки. Подальша робота з вікном повністю аналогічна роботі з попереднім вікном.

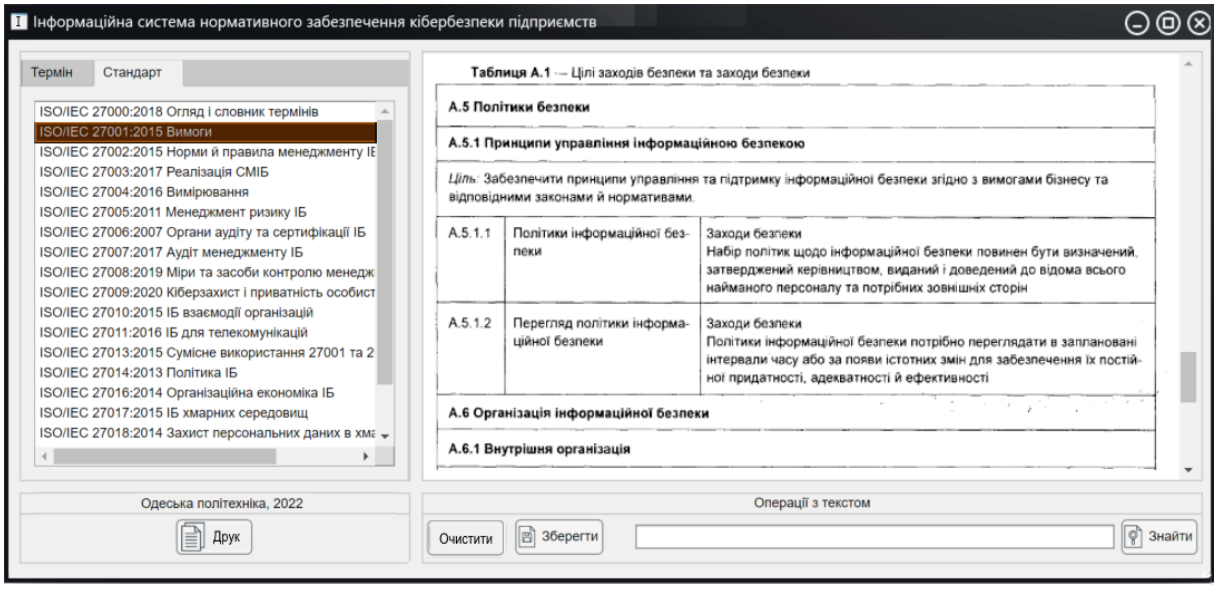


Рис.2. Вікно для роботи з стандартами

Для того, щоб дану систему використати її потрібно запустити на комп'ютер з операційною системою Windows, але її можна легко адаптувати під любу операційну систему, де встановлено Python. Бажано, щоб комп'ютер був під'єднаний до Інтернету. При кожному виклику програми проходить перевірка на оновлення бази даних на web-сторінці програми та, при необхідності, Інформаційна система загружає оновлену базу даних клієнту. Зміну інформації в базі даних здійснює адміністратор програми. Якщо web-сторінка програми не знаходиться, програма працює без оновлення.

Висновок

Використання розробленої «Інформаційної системи нормативного забезпечення кібербезпеки підприємства» має дати змогу підвищити правову грамотність в сфері кібербезпеки та інформаційної безпеки у керівництва підприємств та працівників, яких це стосується. А також впровадженню ефективного менеджменту, який буде якісно впливати на кінцевий результат підприємства. Система може бути корисна для викладачів та студентів учбових закладів, які пов'язані з кібербезпекою.

Список літератури

1. Kissel. Computer Security Division, Information Technology Laboratory. Revision 2. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2013.
2. Золотар О.О. Інформаційна безпека людини: теорія і практика. Київ: АртЕк, 2018. 446 с.
3. Поздняков А.И. Основы теории национальной безопасности. Альманах Пространство и Время. 2013. Т. 2. Вып. 1. 17 с.
4. Танцюра М.Ю. Забезпечення ефективності системи інформаційного забезпечення підприємства: автореф. дис. канд. екон. наук: 08.00.04. Сімферополь, 2012.

INFORMATION SYSTEM FOR ENTERPRISES CYBER SECURITY NORMATIVE SUPPORT

V.P. Halytsky, O.A. Stopakevych

National Odessa Polytechnic University,
Shevchenko Ave., 1, Odessa, 65044, Ukraine; e-mail: val.gal1969@ukr.net

Now the situation has arisen, when a significant number of international standards have been developed and provided almost all areas of information and cyber security. But, at the same time, a very significant part of enterprises and organizations of almost all directions and industries do not meet the requirements of these standards, at least in Ukraine. Moreover, a very significant majority of managers of these enterprises do not know the content of these standards. A brief description of the management system of the information system based on international standards ISO/IEC 27000, requirements for its operation, is provided. The developed information system for regulatory support of cyber security of enterprises consists of a database that contains tables of cyber security terms and international standards for information security management. Information system software consists of an executable file written in the Python programming language with a graphical interface. In order to use the system, it needs to be run under a Windows operating system, but it can be easily adapted to any operating system where Python is installed. It is preferable that the computer is connected to the Internet. Each time the program is called, the database update is checked on the program web page and, if necessary, the Information System downloads the updated database to the client. The program administrator changes the information in the database. If the web page of the program is not achievable, the program works without updating. The use of the developed "Information system for regulatory support of cyber security of enterprises" should make it possible to increase legal literacy in the field of cyber security and information security among the management of enterprises and employees affected by it. And also, the implementation of effective management, which will have a qualitative impact on the final result of the enterprise. The system can be useful for teachers and students of educational institutions that are related to cyber security.

Keywords: Information security, cyber security, cyberspace, software, standard, ISO/IEC 27000

.

DOI 10.15276/imms.v12.no1-2.29
УДК 004.056.53: 004.77

Informatics and Mathematical Methods in Simulation
Vol. 12 (2022), No. 1-2, pp. 29-39

ВИЯВЛЕННЯ ВТОРГНЕНЬ В МЕРЕЖУ ІНТЕРНЕТУ РЕЧЕЙ ШЛЯХОМ АНАЛІЗУ НАЯВНОСТІ АНОМАЛІЙ В МЕРЕЖЕВОМУ ПОТОЦІ ТРАФІКУ AAA ПРОТОКОЛІВ

Л.Ю. Гальчинський

Національний Технічний Університет України «КПІ» імені Ігоря Сікорського
просп. Перемоги, 37, Київ, 02056 Україна; e-mail: hleonid@gmail.com

Одним з найпотужніших трендів інноваційних змін у сучасному світі зараз є Інтернет речей IoT. І хоча цей тренд по-суті тільки на початковому етапі, він вже грає помітну роль в сучасному світі, у сучасній цивілізації. Можна впевнено прогнозувати подальше розширення сфер його застосування. Проте поява цього феномена супроводжується, також, появою пов'язаних з цим проблем. В першу чергу це стосується кіберзагроз, які можуть принести значну шкоду як самим мережам Інтернету речей, так і людям, що користуються цими мережами. Відповідно виникає необхідність у засобах боротьби з цими загрозами. Це складна проблема, яка, в першу чергу, вимагає розробку методів та технологій виявлення такого роду загроз. При цьому ще не склалися чіткі поняття про релевантні рішення для кіберзахисту різних об'єктів застосувань IoT, особливо там, де фінансові можливості обмежені. Тому актуальним є дослідження щодо знаходження рішень, які можуть бути прийнятними для порівняно малобюджетних об'єктів. Метою роботи є отримання методу виявлення вторгнень в мережу IoT, шляхом виявлення аномалій в мережевому потоці трафіку AAA протоколів. Ця проблема ускладнюється тим, що знайдене рішення має відповідати основним політикам безпеки. Проведене нами дослідження показало, що таке рішення принципово можливе шляхом використання можливостей AAA протоколу RADIUS та використання машинного навчання. Методи машинного навчання були перевірені на датасеті UNSW_NB15. Для проведення машинного навчання була проведена попередня обробка з метою нормалізації та стандартизації даних. Комп'ютерні експерименти дозволили перевірити придатність виявлення набору кібератак для різних моделей машинного навчання. Було показано, що сформульований підхід має потенціал для використання у практичних розробках виявлення вторгнень в мережі IoT.

Ключові слова: Інтернет речей, IoT, аномалії у мережевому потоці, AAA протоколи, метод аналізу ієрархій, машинне навчання, датасет

Вступ

Інтернет речей IoT став помітним трендом у сучасному світі, керованому технологіями. Інтернет речей поширюється на різні сфери — від розумних переносних пристроїв до розумних міст, від сфери побуту до промислових застосувань. За оцінками Gartner на 2020 рік Інтернет речей (IoT) мав складати до 26 мільярдів встановлених одиниць, а постачальники продуктів і послуг Інтернету речей мали отримати додатковий дохід, що перевищує 300 мільярдів доларів [1].

Однак цей процес породжує також і складні проблеми, зокрема безпекові. Різноманітні пристрої мають доступ один до одного через віртуальну приватну мережу. Ці комунікаційні процеси дуже вразливі до атак [2].

Основні методи атак на IoT мережі включають атаки типу «відмова в обслуговуванні» (DoS), підробка даних та моніторинг мережі [3].

Зараз методи виявлення вторгнень поділяються на виявлення вторгнень на основі хоста та виявлення вторгнень на основі мережі.

Існує значний корпус досліджень, які висвітлюють питання виявлення вторгнень в мережу на основі виявлення аномалій в мережевому потоці. В цих дослідженнях пропонуються різноманітні моделі виявлення та аналізу аномалій, такі як глибинна

нейронна мережа [3], мережа Маркова [4], метод зворотного поширення помилки [5], об'єднання інформації на основі графу атаки та аналіз основних компонентів [6].

Проте на даний час за даними існуючих досліджень проблема виявлення аномалій мережевого трафіку IoT пристроїв все ще далека від остаточного вирішення. В першу чергу це обумовлено різноманітністю мережевого трафіку різних пристроїв Інтернету речей, гетерогенністю пристроїв в мережах IoT та мережевого середовища, слабкою захищеністю пристроїв тощо. Важливим фактором також є можливості суб'єктів, що використовують мережі IoT, оскільки впровадження систем безпеки може бути досить витратним і дорога система кіберзахисту може бути суб'єкту не по кишені.

В даній роботі основний фокус уваги зосереджено на ефективності та простоті впровадження запропонованого рішення виявлення вторгнень у вже існуючі мережі пристроїв Інтернету речей на основі аналізу даних обліку AAA протоколів в реальному часі.

Аналіз досліджень і публікацій

Проведено багато досліджень по всьому світу щодо безпеки різноманітних IoT інфраструктур, в основному зосереджені на виявленні шкідливого коду та мережевих атак [7].

Для досягнення швидкого виявлення атак зловмисного коду автори в [8] запропонували безпечну та захищену конфіденційну схему агрегації, що ґрунтується на адитивному гомоморфному шифруванні та операціях перешифрування проксі в криптосистемі Paillier.

У роботі [9] автори використовували дизассемблер і метод статистичного аналізу для боротьби з виявленням шкідливого коду. Наразі, згідно статистичних даних, головною точкою входу хакерів для здійснення атаки на мережу IoT, особливо на IIoT, є розумний лічильник.

Механізм виявлення вторгнення відстежує події, що відбуваються в розумному лічильнику, і аналізує їх. Після атаки або виявлення потенційної загрози безпеці механізм виявлення вторгнення видає сигнал тривоги, щоб система та менеджери застосували відповідні механізми реагування.

Зі збільшенням об'єму трафіку IoT та шумів, метод виявлення аномалій, що ґрунтується на традиційному машинному навчанні, стикається з проблемами низької точності та низької надійності вилучення ключових ознак, що знижує продуктивність виявлення атак мережевих атак. Тому зараз активно розвивається метод виявлення аномалій, що ґрунтується на глибокому навчанні [10,11].

Ряд дослідників звернули увагу на організаційні аспекти впровадження систем кіберзахисту для мереж IoT. Зокрема в роботі [12] запропоновано систему виявлення аномалій та ідентифікації пристроїв розумних будинків із застосуванням колективної комунікації. Суть нового підходу в організації безпеки розумних будинків, яке передбачає їх об'єднання у кластери, що дає можливість не тільки об'єднати ресурси власників для впровадження системи захисту, але ще й отримати більш високий рівень достовірності виявлення вторгнень. Якщо це можливо, то це безумовно слушна ідея.

Мета і задачі дослідження

Метою роботи є отримання методу виявлення вторгнень в мережу IoT, на основі виявлення аномалій в мережевому потоці для суб'єкта, який, не маючи значних ресурсів, бажає отримати систему захисту мережі IoT, що задовольняла б вимогам більшості політик безпеки.

Шляхів вирішення проблеми захисту від вторгнень декілька.

1. Самостійна розробка. Це досить довгий і витратний шлях, що передбачає створення команди аналітиків, програмістів та IT- спеціалістів.
2. Послуги спеціалізованих організацій, які надають всі необхідні послуги разом. На перший погляд це виглядає більш ефективним, У такому разі умовна компанія лише налаштовує в своїй мережі переадресацію пакетів в оточення спеціалізованої компанії, де

спеціалізована компанія їх аналізує та надсилає звіт про можливі вторгнення. Проте тут можуть стати на заваді політики безпеки, які можуть забороняти третім сторонам мати повне бачення всього, що відбувається у внутрішній мережі компанії.

3. Придбання IDS або IPS. Таке рішення однак потребує значних витрат на впровадження. Навіть, якщо використовувати рішення з відкритим кодом, такі як Snort, Suricata або Bro IDS.

Мета цього дослідження полягає, у знаходженні можливостей рішення, яке не буде потребувати від умовної компанії значних бюджетних та часових витрат, а також не буде суперечити більшості політик безпеки.

Основна частина

У сучасних корпоративних мережах для розмежування доступу до мережі переважно використовують AAA (authentication, authorization, accounting) сервери [13]. Враховуючи цю обставину, в даній роботі пропонується наступне рішення: вже існуючі AAA сервери налаштувати для перенаправлення запитів обліку на вже розгорнуті та налаштовані AAA сервери. Ці AAA сервери роблять попередню обробку даних обліку, стандартизовану для всіх інфраструктур, та завантажують оброблені дані в центр обробки даних. В центрі обробки отримані дані аналізуються у реальному часі методами машинного навчання, та у випадку виявлення аномалій надсилається відповідне повідомлення.

Фактично, запропоноване рішення не буде потребувати практично жодних додаткових бюджетних витрат, а тільки незначні витрати часу для налаштування переадресації даних обліку на AAA сервері. У той же час дані обліку вже мають стандартизований формат для будь-якого пристрою, відповідно попередня обробка даних буде однаковою для будь якої інфраструктури.

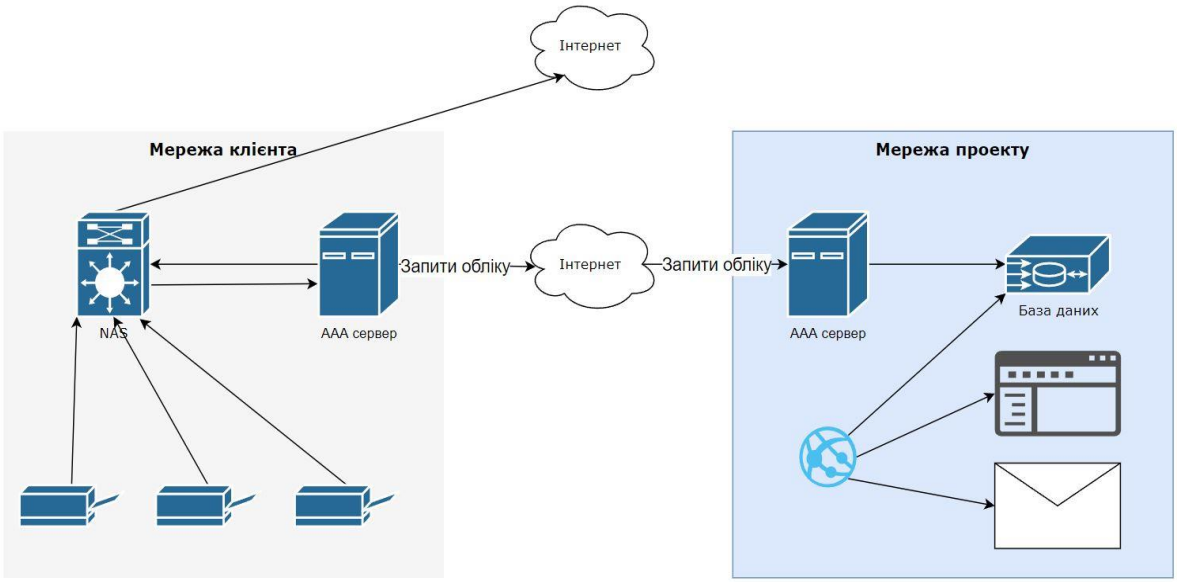


Рис.1. Загальна архітектура запропонованого рішення

AAA сервер підключений до Active Directory Domain Services компанії і коли користувач підключається до мережі зі своїми обліковими даними, мережева система зберігання даних(Network attached storage) NAS перенаправляє цей запит на AAA сервер, а сервер в свою чергу перевіряє чи є такий користувач в директорії і відповідно дозволяє або забороняє доступ до мережі. IoT-пристрої також підключаються до мережі через AAA сервери, однак оскільки далеко не завжди для є них можливість ввести логін та пароль, вони підключаються через MAC автентифікацію. Автентифікація пристроїв відбувається на основі їх фізичних MAC-адрес.

Ключовим моментом тут є те, що ААА сервери призначені для збору даних про використання мережі кожним окремим пристроєм. Однак в даній роботі пропонується використовувати дані обліку для виявлення аномалій.

Подальша конкретизація запропонованого рішення потребує вибору ААА протоколу з множини можливих та вибір методу визначення аномалій. Оскільки ці етапи не взаємопов'язані їх можна вирішувати послідовно.

У сучасних мережах використовують два основних рішення для ААА: Remote Authentication Dial-In User Service (RADIUS) та Cisco's Terminal Access Controller TACACS+ протоколи. Існує ще й третій ААА-протокол, відомий як DIAMETER, який переважно використовується мобільними операторами. Далі коротко охарактеризуємо ці рішення. Функціональні можливості ААА протоколів приведені в табл.1

Таблиця 1

Функціональні можливості ААА протоколів

Протокол / Функція	**RADIUS**	**TACACS+**	**Diameter**
Автентифікація	Автентифікація здійснюється шляхом дешифрування пакета запиту доступу NAS, автентифікації джерела NAS та перевірки параметрів запиту доступу до файлу користувача. Потім сервер повертає одну з трьох відповідей автентифікації: access-accept; access -reject; access-challenge.	Має три типи пакетів: Start, Continue, Reply. Клієнт починає автентифікацію з пакета «Start», який описує тип автентифікації, яку потрібно виконати. Для простих типів автентифікації, таких як PAP, пакет також може містити ідентифікатор користувача та пароль. Сервер відповідає типом пакету «Reply».	Клієнт (тобто NAS) надсилає запит на автентифікацію серверу, що містить команду AA-Request (AAR), ідентифікатор сеансу (session-ID), адресу та ім'я хоста клієнта, за якими слідують ім'я та пароль користувача та значення стану.
Авторизація	Авторизація не є окремою функцією в протоколі RADIUS, вона є просто частиною відповіді автентифікації. Коли сервер RADIUS перевіряє запит на доступ, він повертає клієнту NAS усі атрибути підключення, зазначені у файлі користувача.	Авторизація в TACACS+ здійснюється за допомогою пар атрибут / значення запиту (Request) та відповіді (Response) для встановлення прав доступу та привілеїв, зворотного виклику, фільтрації вхідних і вихідних пакетів та ін.	Запити на авторизацію мають виконуватися протягом існуючого сеансу; їх не можна використовувати для ініціювання сеансів, але їх можна пересилати за допомогою проксі-сервера Diameter.
Облікові можливості	Облік RADIUS збирає дані для статистичних цілей, моніторингу пристроїв в мережі, а також використовується для точного виставлення рахунків користувачам.	На додачу до стандартних облікових даних, які підтримує RADIUS, TACACS має можливість запису подій, яка може записувати зміни на системному рівні прав доступу або привілеїв.	Перевищує облікові можливості RADIUS і TACACS+, за рахунок опцій моніторингу подій, періодичні звіти, передачу записів у реальному часі та інші
Додаткові можливості	Дозволяють виконувати роль проксі-сервера для запитів клієнтів, пересилаючи їх на сервери в інших доменах автентифікації. Пересилання може ґрунтуватися на ряді критеріїв, включаючи іменований або номерний домен. Це особливо корисно, коли єдиний модемний пул є спільним для відділів або організацій.	Розширені функцій автентифікації та авторизації TACACS в чому вони значно покращені відносно функцій протоколу RADIUS завдяки двом спеціальним можливостями: рекурсивним пошуком і викликом (callout).	Підтримку декілька конфігурацій проксі, включаючи дві моделі RADIUS і дві додаткові моделі брокерів.

Порівняння ААА-протоколів

Клієнтами ААА-серверів є пристрої доступу до мережі (NAS). Вони передають інформацію про користувача на сервер ААА і діють відповідно до відповідей, які повертає сервер. Сервери отримують запити на підключення користувача, автентифікують користувача і повертають NAS інформацію про конфігурацію, необхідну для надання послуг користувачеві. Ця інформація може включати транспортні параметри, параметри протоколу, додаткові вимоги автентифікації (зворотній виклик, SecureID), директиви авторизації (дозволені послуги, застосування фільтрів) та вимоги до обліку. Ці функціональні якості притаманні усім трьом з перелічених ААА-протоколів. Проте існують і суттєві відмінності. Далі охарактеризуємо їх базові функції: Авторизація; Автентифікація; Облік; Додаткові можливості.

Вибір ААА протоколу для запропонованого рішення

Кожен з трьох розглянутих ААА протоколів має свої переваги та недоліки, тому їх досить складно порівнювати. Який з них обрати для реалізації запропонованого рішення? Наприклад, переваги протоколу Diameter в розширюваності та чотири варіанти проксування запитів, не є такими значущими, коли умовна компанія просто хоче налаштувати безпечний доступ до мережі. Коли адміністратор мережі компанії хоче налаштувати безпечний мережевий доступ до ресурсів, то його мало хвилює посилені можливості розширюваності та переадресації. Він бажає, щоб працювала автентифікація і авторизація, тут і зараз, і бажано без глибокого занурення в конфігураційні файли, що власне і потрібно для мережі IoT. Тому треба обрати критерії, на основі яких можна об'єктивно обрати ААА протокол, який би найкраще відповідав би даній задачі. На наш погляд такими критеріями можуть слугувати наступні характеристики: можливості переадресації запитів; детальність обліку; швидкість; підтримка виробниками мережевого обладнання; розповсюдженість. Даний набір критеріїв дозволяє оцінювати різні аспекти застосування ААА протоколів в мережах, зокрема і в мережах IoT. Відтак, якщо кожний з критеріїв оцінити кількісно, то ми зможемо об'єктивно оцінити кожний з протоколів і зробити обґрунтований вибір. Однак, при цьому ми маємо справу з багатокритеріальною задачею. І тому маємо застосувати релевантний метод для її розв'язку. Для обґрунтування вибору протоколу був застосований метод аналізу ієрархій(MAI). Метод аналізу ієрархій являє собою метод прийняття рішень ієрархічної композиції задачі та експертного рейтингування. Після того, як ієрархія побудована, особи, що приймають рішення, систематично оцінюють різні її елементи, порівнюючи їх один з одним попарно, з огляду на їх вплив на елемент над ними в ієрархії. Суть MAI полягає в поєднанні експертних оцінок та строгим формальним алгоритмом визначення кращого вибору з можливих. В ролі експертів виступали мережеві адміністратори компаній, в яких використовувались описані вище ААА протоколи.

Побудова ієрархії.

На рис. 2. представлена побудована MAI ієрархія для вирішення задачі вибору кращого ААА протоколу для цілей даної роботи.

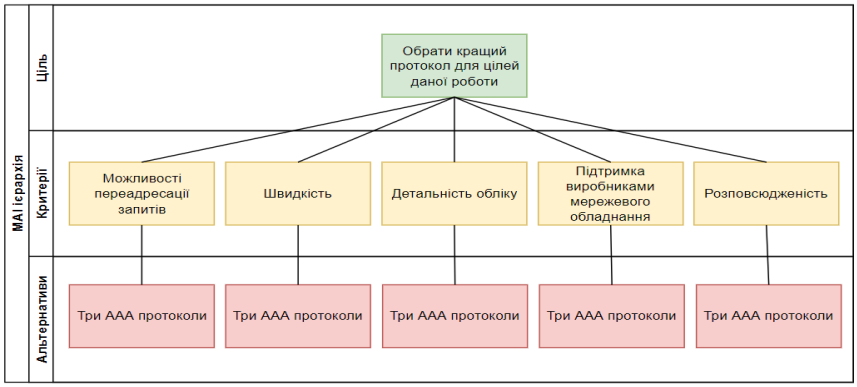


Рис. 2. MAI ієрархія для задачі вибору ААА протоколу

Далі було здійснено порівняння критеріїв по шкалі відношень Сааті щодо того, наскільки вони на думку експертів важливі.

На основі суджень експертів, представлених в табл. 2, було визначено пріоритети для критеріїв, за якими будуть порівнюватися кожен трьох протоколів

Таблиця 2

Результати попарних порівнянь критеріїв експертами

Критерій – Критерій	Можливості пере-адресації запитів	Детальність обліку	Швидкість	Підтримка виробниками мережевого обладнання	Розповсю-дженість
	1	2	3	4	5
1	1	2	5	1/3	1/5
2	1/2	1	4	1/5	1/7
3	1/5	1/4	1	1/7	1/7
4	3	5	7	1	2
5	5	7	7	1/2	1

Далі було здійснено попарне порівняння всіх трьох AAA протоколів за визначеними критеріями. На основі даних, отриманих на кроках попарного порівняння, було сформовано глобальні пріоритети для кожної з альтернатив. Їх загальна сума становить 1, тобто спочатку була проведена процедура нормування. Кожна альтернатива має глобальний пріоритет, що відповідає її «відповідності» всім судженням експертів щодо розглянутих критеріїв. Глобальні пріоритети всіх альтернатив представлені в Табл.3.

Таблиця 3

Глобальні пріоритети всіх альтернатив

Критерій Прлтокол	Можливості переадресації запитів	Детальність обліку	Швид-кість	Підтримка виробниками мережевого обладнання	Розповсю-дженість	Глобальний пріорітет
RADIUS	0.037	0.008	0.023	0.305	0.258	**0.631**
TACACS+	0.010	0.018	0.004	0.061	0.077	0.170
Diameter	0.084	0.057	0.010	0.027	0.022	0.200

RADIUS протокол з глобальним пріоритетом 0.631 краще за інші протоколи підходить для цілей даної роботи.

Експериментальні дослідження

З метою оцінювання ефективності виявлення аномалій на основі використання AAA протоколів було проведено серію випробувань. Спочатку необхідно провести дослідження придатністі пакетів обліку RADIUS-протоколу для для тренування моделей машинного навчання по виявленню аномалій в трафіку повідомлень. Для тестування було використано датасет UNSW_NB15-dataset [13] з набором шкідливого ПЗ та зразки їх трафіку та нешкідливого ПЗ. Далі також були протестовані різні моделі машинного навчання з метою оцінки якості розпізнавання аномалій.

Набори даних NIDS можна концептуалізувати як реляційні дані, які можна вважати табличними даними, тобто наборами записів даних (також визначених як вектори, події, зразки або спостереження), кожен з яких складається зі колонок (тобто атрибутів/областів) з різними типами даних, такими як цілі, з плаваючою точкою, бінарні або категоріальні дані. У випадку вхідних багатоваріантних даних, те, чи є їхні характеристики однаковими чи різними типами даних, визначає застосовність методів виявлення аномалій для їх обробки. Формат пакету RADIUS-протоколу[14] показано на Рис.3.

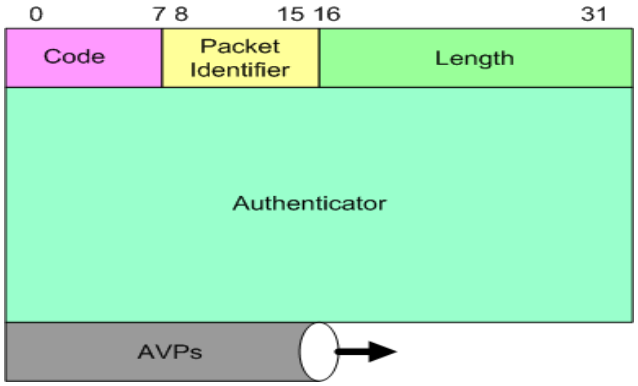


Рис. 3. Формат пакету RADIUS

Атрибути RADIUS містять конкретні відомості про аутентифікацію, авторизацію, облік і конфігурацію для запиту та відповіді. Атрибути обмінюються між NAS і сервером. Кожен атрибут пов'язаний з набором властивостей, які визначають, як його інтерпретувати. Найважливішою властивістю є тип даних, який оголошує тип даних, які ідентифікує атрибут (рядок символів, ціле число, IP-адреса або вихідні двійкові дані). Інформація, яка передається разом із запитом, упакована в набір пар атрибут/значення (AV-пари, або AVP), які складаються з номерів атрибутів та пов'язаних із ними даних. Таким чином, RFC 2865 (Стандартний трек) визначає аутентифікацію та авторизацію, а облікова частина визначена в інформаційних RFC 2866 і 2869. Є ще багато атрибутів.

Не всі поля в цьому наборі даних відповідають полям пакетів обліку RADIUS-протоколу. В наборі даних UNSW_NB15 наявні поля, які неможливо буде отримати зі стандартного трафіку обліку RADIUS. Відповідно для навчання моделі такі поля не будуть використовуватись. Необхідно врахувати, що цей датасет фактично являє собою набір перехоплених пакетів, а облік RADIUS відображає статистичні дані про використання мережі певним пристроєм за певний час. Тому для забезпечення можливості коректного тренування моделей машинного навчання треба провести попередню обробку датасету UNSW_NB15. Попередня обробка включає такі операції, як очищення даних, дедуплікація, агрегація та нормалізація даних. В кінцевому рахунку ми отримуємо нормалізовані і стандартизовані дані представлені на рис. 4.

	dur	spkts	dpkts	sbytes	dbytes	rate	sttl	dttl	sload	dload	-
0	-0.208678	-0.130765	-0.165331	-0.046480	-0.098409	-0.002151	0.722026	-0.751628	0.590935	-0.27285	-
1	-0.208679	-0.130765	-0.165331	-0.039194	-0.098409	0.210460	0.722026	-0.751628	4.363255	-0.27285	-
2	-0.208679	-0.130765	-0.165331	-0.043188	-0.098409	0.678204	0.722026	-0.751628	4.220037	-0.27285	-
3	-0.208679	-0.130765	-0.165331	-0.044155	-0.098409	0.470318	0.722026	-0.751628	2.850314	-0.27285	-
4	-0.208678	-0.130765	-0.165331	-0.037100	-0.098409	0.054546	0.722026	-0.751628	4.198501	-0.27285	-

Рис. 4. Нормалізовані дані з датасету UNSW_NB15

Для проведення машинного навчання необхідно підібрати набір параметрів датасету який би дозволив досягнути компроміс між можливостями формату обліку протоколу RADIUS та достатньо високим рівнем виявлення аномалій в мережі IoT. В першу чергу це можна зробити за рахунок виключення суттєво скорельованих показників. Пороговою величиною такого вилучення в даному дослідженні була значення кореляції 0,5 за Пірсоном. Наприклад, розрахунок кореляції показав, що між spkts та sloss, dpkts (кількість пакетів відправлених до джерела) та dbytes (від призначення до вихідних байтів транзакції), tcprtt та ackdat (час встановлення TCP-з'єднання, час між пакетами SYN_ACK та ACK) перевищують 0,9, і існує тривала позитивна кореляція. З іншого боку кореляція між показниками spkts і state, dbytes і tcprtt менше 0,1.

Крім того, методика машинного навчання говорить що кращий результат буде тоді, коли ентропія, тобто перемішаність ознак буде якомога меншою. Кількісним показником перемішаності служить домішка Джині(DS).

$$DS = 1 - \sum_{i=1}^{n} p_i^2 \quad (1)$$

де p_i - частоти представників різних ознак.

Домішка Джині говорить нам про «забрудненість» множини вибору. Знижуючи домішку Джіні, ми можемо з упевненістю зробити висновок, що чистота буде більше, а отже, вищий шанс на однорідність множини. Чим менше значення домішки Джині для ознаки, тим менше забрудненість об'єкта в наборі даних і тим буде краще навчальний ефект для ознаки.

Процедура відбору ознак була проведена у два етапи. На першому етапі були відібрані всі ознаки з пороговим значенням коефіцієнта кореляції 0,5. На другому етапі були залишені саме ті з них, які мали відповідне менше значення домішки Джині.

В результаті процедури відбору з набору даних UNSW_NB15 в даній роботі було обрано наступні ознаки для подальшого навчання моделі:

- dur - тривалість з'єднання;
- sload - кількість вихідних бітів в секунду (вхідне навантаження);
- dload - кількість вихідних бітів в секунду (вихідне навантаження);
- dpkts - кількість пакетів від пункту призначення до джерела;
- spkts - кількість пакетів від джерела до призначення.

Характерно, що всі ці атрибути визначаються авторами дата сету як основні.

Експерименти, представлені у цій роботі, проведено на Dell Inspiron 15 3000, завантаженому з операційною системою Windows 10 з процесором: AMD A6-6310 1800 МГц 1,80 ГГц. Моделі ML будуються, навчаються, оцінюються та тестуються на базі бібліотек Scikit-Learn,pandas Python. Для формування навчальної та тестової вибірок було було налаштовано як навчальний набір та набір для тестування, а саме, UNSW_NB15_training-set.csv та UNSW_NB15_testing-set.csv відповідно. Кількість записів у навчальному наборі становить 175 341 запис, а у тестовому наборі – 82 332 записів різних типів, атакуючих та звичайних.

Об'єктами для виявлення були наступні різновиди атак:
Fuzzers; Analysis; Backdoors; DoS; Exploits; Generic; Reconnaissance; Shellcode; Worms

Для ідентифікації атак були обрані наступні алгоритми:
Дерево рішень; Random Forest; Багатошаровий перцептрон; Gradient Boosting;
Classifier Support; Vector Classifier

Для верифікації точності моделей використовувся метод перехресної перевірки. Під час навчання моделі набір даних розбивався на рівні апроксимовані сегменти. Потім кожен сегмент використовувався для перевірки точності моделі, а інші сегменти використовувалися для навчання. Процедура повторюється поки всі сегменти набору даних не будуть використані для перевірки точності.

Для об'єктивної оцінки ефективності алгоритмів машинного навчання в даній роботі була використана класична тріада з трьох показників: кількість правильних відповідей (Precision); повнота (recall); F-міра – поєднує повноту та влучність.Precision можна інтерпретувати як частку об'єктів, названих класифікатором позитивними і при цьому дійсно позитивними, а recall показує, яку частку об'єктів позитивного класу з усіх об'єктів позитивного класу знайшов алгоритм.

Результат та обговорення

Були проведені комп'ютерні розрахунки для кожної з моделей машинного навчання для розпізнавання кожної з визначених атак. В таблиці надані результати оцінки

ефективності алгоритмів навчання за значенням F-міри, як агрегованого критерія якості. F-міра (в загальному випадку) є середнє гармонійне precision і recall.

Таблиця 4

Результати перевірки точності

Алгоритм машинного навчання – Назва атаки	Дерево рішень	Random Forest	Багатошаровий перцептрон	Gradient boosting classifier	Support vector classifier
Analysis	0,19	0,19	0,1	0,8	0,1
Backdoor	0,14	0,15	0,11	0,10	0,1
DoS	0,33	0,27	0,2	0,13	0,1
Exploits	0,69	0,72	0,72	0,73	0,69
Fuzzers	0,61	0,65	0,58	0,59	0,42
Generic	0,99	0,99	0,99	0,99	0,98
Normal	0,92	0,93	0,92	0,91	0,87
Reconnaissance	0,82	0,83	0,82	0,83	0,58
Shellcode	0,6	0,67	0,61	0,59	0,0
Worms	0,49	0,23	0,19	0,52	0,0

Для побудованих моделей був застосований метод перехресної перевірки, а також був визначений середній час класифікації. Всі отримані результати представлені в таблиці.

Таблиця 5

Порівняння моделей

Назва алгоритму	F-міра (%)	FPR (%)	Точність (перехресна перевірка) (%)	Час навчання (с)	Час класифікації (мкс)
Дерево рішень	80.9	21.1	80,53	**27,6**	**0,99**
Random Forest	82,6	19,2	82,48	143,6	23,38
Багатошаровий перцептрон	**83,7**	**18,3**	**83,24**	1082,8	2,54
Gradient Boosting Classifier	82	19,9	81,8	3323,1	25,9
Support Vector Classifier	76,8	25,7	76,54	715,1	0,89

Аналіз табл. 5 показує, що два методи навчання: Random Forest та багатошаровий перцептрон має певну перевагу у порівнянні з іншими методами. Причому багатошаровий перцептрон має кращі результати по точності. Однак він поступається в швидкості навчання дереву рішень.

Отримані у цьому дослідженні результати дозволяють стверджувати про можливість виявлення вторгнень в мережі IoT на основі виявлення аномалій шляхом аналізу трафіка за AAA протоколом та дозволяють окреслити практичне рішення для захисту мережі IoT. Очевидно, в подальшому необхідно буде дещо покращити точність виявлення аномалій.

Програмний продукт на основі мікросервісної архітектури буде поставлятися користувачам як SaaS. Ядром цього мікросервісу є авторська програма[15], яка відповідає за обробку пакетів і взаємодію з мережею.

Висновки

У роботі проведені дослідження пошуку підходу виявлення кібератак на мережі IoT на основі аналізу аномалій в трафіку AAA протоколів. В процесі дослідження були:

- проведено аналіз можливостей існуючих протоколів дозволив сформулювати критерії якості для задач виявлення аномалій;
- поставлена і вирішена задача вибору найбільш прийнятного AAA протоколу методом аналізу ієрархій;
- попередня обробка даних датасету UNSW_NB15 з метою використання даних для машинного навчання шляхом проведення двохетапної процедури відбору ознаки, що дало можливість нормалізувати та стандартизувати дані для подальшого машинного навчання;
- проведено комп'ютерні експерименти, в якому було перевірено можливості різних методів машинного навчання для виявлення 9 різновидів кібератак, зафіксованих в дата сеті;
- запропоновано програмне рішення поставленої проблими у вигляді мікросервісної архітектури.

Найкращі результати по критерію точності показали методи: Багатошаровий персептрон та Random Forest. Точність з врахуванням перехресної перевірки складає 83.24%, що говорить про потенційну можливість реалізації підходу виявлення вторгнень в мережу IoT шляхом виявлення аномалій в трафіку за протоколом RADIUS.

Зазначимо, що проведені дослідження не можна вважати завершеними, але дають підставу стверджувати про перспективу подальших досліджень у цьому напрямку.

Список літератури

1. Gartner Says 6.4 billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015". Gartner. 2015. 10 November.

2. MAC Authentication Bypass (MAB). URL: https://networklessons.com/ cisco/ccie-routing-switching-written/mac-authenticationbypass-mab.

3. Nasim B. M., Jelena M., Vojislav B. M., Hamzeh K. A framework for intrusion detection system in advanced metering infrastructure. 2014. P. 195–205.

4. Deep learning. URL: https://en.wikipedia.org/wiki/Deep_learning.

5. Markov random field. URL: https://en.wikipedia.org/wiki/Markov_random_field.

6. Backpropagation. URL: https://en.wikipedia.org/wiki/Backpropagation.

7. Park Y., Nicol D.M., Zhu H. Prevention of Malware Propagation in AMI. Proceedings of the IEEE International Conference on Smart Grid Communications. 2013. P. 474–479.

8. Neetesh S., Bong J. C., Santiago G. Secure and Privacy-Preserving Concentration of Metering Data in AMI Networks. Proceedings of the 2017 IEEE International Conference on Communications (ICC). 2017.

9. Euijin C., Younghee P., Huzefa S., Identifying malicious metering data in advanced metering infrastructure. Proceedings of the 2014 IEEE 8th International Symposium on Service Oriented System Engineering, 2014. P. 490–495

10. DoS and DDoS vulnerability of IoT: A review. URL: https:// www.researchgate.net/publication/39862422_DoS_and_DDoS_vulnerability_of_IoT_A_review.

11. Fernandes G., Rodrigues J. J. P. C., Carvalho L. F., Al-Muhtadi J. F, Proenca M. L.

A Comprehensive Survey oon Network Anomaly Detection. Telecommunication Systems. 2019. V. 70. No. 3. P. 447–489.

12. Нічепорук, А., Нічепорук, А., Савенко, О., & Казанцев, А. An Intelligent System For Detecting Anomalies and Identifying Smart Home Devices Based on the Collective Communication. Electrotechnic and Computer Systems. 2021. No. 34(110). P.50-61.

13. Nour M. Designing an Online and Reliable Statistical Anomaly Detection Framework for Dealing with Large High-Speed Network Traffic. Diss. University of New South Wales, Canberra, Australia.

14. RADIUS. URL: https://en.wikipedia.org/wiki/RADIUS.

15. Нікітін Є.Є., Гальчинський Л.Ю. Комп'ютерна програма «Radius сервер на платформі .NET». Свідоцтво про реєстрацію авторського права на твір №109412. від 12 листопада 2021.

DETECTION OF INTRUSIONS INTO THE INTERNET OF THINGS NETWORK BY ANALYZING THE PRESENCE OF ANOMALIES IN THE NETWORK TRAFFIC FLOW OF AAA PROTOCOLS

L.Yu. Galchynsky

National Technical University of Ukraine "KPI" named after Igor Sikorsky
ave. Peremohy, 37, 02056 Ukraine; e-mail: hleonid@gmail.com

Today, one of the most powerful trends in innovative change in the modern world is the Internet of Things IoT. And although this trend is essentially only at an early stage, it already plays a significant role in the modern world, in modern civilization. It is safe to predict that further expansion of its scope. However, the emergence of this phenomenon is also accompanied by the emergence of related problems. This is especially true of cyber threats, which can cause significant harm to both the Internet of Things itself and the people who use those networks. Accordingly, there is a need for means to combat these threats. This is a rather complex problem, which primarily requires the development of methods and technologies for detecting such threats. At the same time, there are no clear concepts of relevant solutions for cyber security of various IoT applications, especially where financial resources are limited. Therefore, research is currently relevant to find solutions that may be acceptable for relatively low-budget facilities. The aim of the work is to obtain a method for detecting intrusions into the IoT network by detecting anomalies in the network traffic flow of AAA protocols. This problem is complicated by the fact that the solution found must comply with basic security policies. The study conducted in this paper showed that such a solution is possible in principle by using the capabilities of the AAA RADIUS protocol and the use of machine learning. Machine learning methods were tested on the UNSW_NB15 dataset. For machine learning, pre-processing was performed to normalize and standardize the data. Computer experiments have tested the suitability of detecting a set of cyberattacks for different models of machine learning. It was shown that the formulated approach has the potential to be used in practical developments to detect intrusions in the IoT network.

Keywords: Internet of Things, malicious intrusion into the network, anomalies in the network flow, AAA protocols, method of analysis of hierarchies, NIDS data sets, machine learning methods, UNSW_NB15.

DOI 10.15276/imms.v12.no1-2.40
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 12 (2022), No. 1-2, pp. 40-45

ВИЯВЛЕННЯ ФАЛЬСИФІКАЦІЇ ЦИФРОВОГО ЗОБРАЖЕННЯ, ВИКОНАНОЇ МЕТОДОМ ADOBE PHOTOSHOP «ЛАТКА»

М.В. Гонтар, В.В.Зоріло, О.Ю.Лебедєва

1, пр.Шевченка, Національний університет «Одеська політехніка», 65044, Одеса
vikazorilo@gmail.com, whiteswanhelena@gmail.com

Сьогодення все активніше змушує нас дбати про свою інформаційну безпеку. Події у світі і в Україні, інформаційні, гібридні війни, кібервійни – це те, що стало нашою повсякденною реальністю, і те, що спонукає шукати нові та вдосконалювати існуючі методи і засоби захисту інформації. Одне з питань захисту інформації – захист графічного контенту від порушень його цілісності. Порушення цілісності цифрових зображень можливо виконувати великим різноманіття інструментів графічних редакторів. Зокрема, такий інструмент графічного редактора Adobe Photoshop «латка» - зручний спосіб виконати фальсифікацію світлини, якому у відкритому друці на даний час не приділяється уваги. Тож необхідність виявлення даного інструменту стала підставою для описаних в даній статті експериментів. Мета даної роботи – підвищення ефективності виявлення підробок світлин, виконаних засобами інструменту Adobe Photoshop «Латка», шляхом розробки алгоритму. В роботі проведено обчислювальний експеримент з використанням 100 цифрових зображень, до яких було застосовано обробку інструментом «латка». На основі обчислювального інструменту було розроблено алгоритм, який показав себе як ефективний у випадках, коли зображення після фальсифікації збережено у форматах з втратами і без втрат. В більшості випадків вдалося виявити наявність порушення цілісності у випадку, коли вона дійсно мала місце, і встановити факт відсутності обробки інструментом «латка», коли його дійсно не було.
Ключові слова: порушення цілісності інформації, захист інформації, клонування, латка, алгоритм.

У сучасному світі світлини стали невід’ємною частиною кожної людини. Вже давно соціальні мережі, інтернет-магазини та інші цифрові методи взаємодії між людьми стали дуже розвиненими, і це супроводжується використанням великої кількості світлин. Вони зустрічаються нам на кожному кроці. Кожен день безліч користувачів передивляються фото друзів, рідних та близьких. Підтвердженням цьому стали соціальні мережі Instagram, Facebook та інші. Реальність така, що фотокамера є у кожної сучасної людини як мінімум у складі смартфону. Ми непомітно для себе фіксуємо різні моменти нашого життя. Це призводить до того, що у нашому розпорядженні опиняються тисячі фотографій.

Висока доступність програмних засобів редагування цифрових зображень – графічних редакторів, зокрема, Adobe Photoshop – призводить до того, що будь-який користувач може підробити тим чи іншим чином зображення, використати підробку з метою дезінформації задля отримання власної користі в тому числі. Наприклад, можна підробити номер автомобіля та на сайті авто-інтернет-магазину чи на інших ресурсах спробувати використати дані фото задля власної наживи. Операції, які для цього часто використовують, такі як «Штамп» графічного редактора Adobe Photoshop, на сьогоднішній день можливо виявити різними методами [1-7]. Однак сучасні версії цього графічного редактора дозволяють виконувати клонування з можливістю адаптації клонованої частини в контексті від оточуючої сцени. Для цього можна використати інструмент «Латка». Виявленню даного інструмента у відкритому друці не приділяється уваги.

Мета роботи – підвищення ефективності виявлення підробок світлин, виконаних засобами інструменту Adobe Photoshop «Латка», шляхом розробки алгоритму.

В наш час засоби смартфонів як правило виробляються та зберігаються фотографії в форматі JPEG, професійне обладнання дозволяє користувачам зберігати фотографії без втрат, наприклад, у форматі BMP, щоб цифрове зображення в результаті мало найкращу можливу якість.

Зараз існує багато програмного забезпечення, завдяки якому можна редагувати цифрові зображення, такі як Adobe Lightroom, Affinity Photo, PhotoLab тощо. Але найпопулярнішим із великого вибору програм є Adobe Photoshop, який надає можливість використовувати гнучкі налаштування, завдяки яким редагувати фото можна як вам заманеться.

Використання інструменту «Штамп» дуже просте, для цього потрібно на панелі інструментів обрати «Штамп» (рис.1), та затиснувши клавішу Alt клацнути лівою кнопкою миші по області, яку хочемо скопіювати (рис.2).

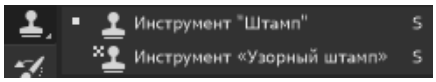


Рис. 1. Інструмент «Штамп»

Рис. 2. Вибір області для копіювання

Далі відпускаємо клавішу Alt і наводимо курсор на те місце, куди хочемо перенести (клонувати) об’єкт (рис. 3).

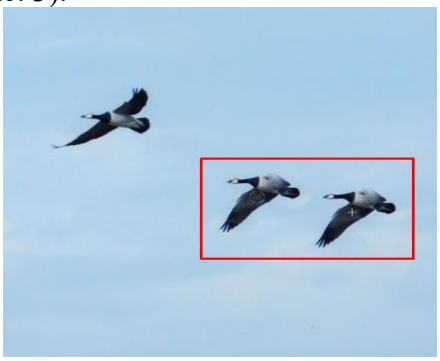


Рис. 3. Копіювання об’єкту

Завдяки цьому можна приховувати недоліки на зображені або робити більшу кількість об’єктів.

Далі ми розглянемо копіювання методом використання «Латки». Він знаходиться також на панелі інструментів (рис. 4).

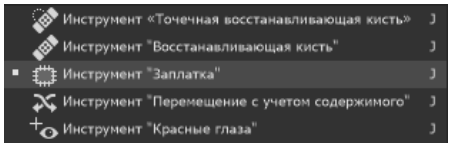


Рис. 4. Вибір інструмента «Латка»

Щоб скопіювати певну область, потрібно її виділити і натиснути клавішу M, після чого виділити область для копіювання (рис. 5) та перетягнути ЇЇ на потрібне місце (рис.6).

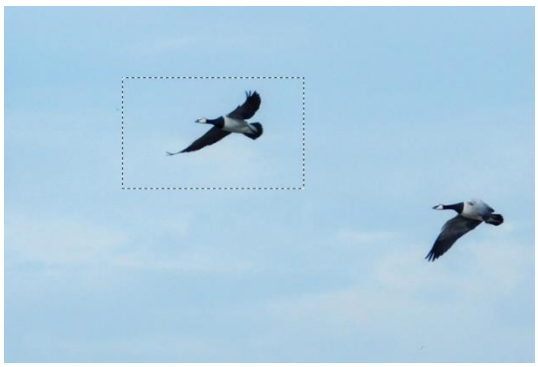


Рис. 5. Виділення об’єкту

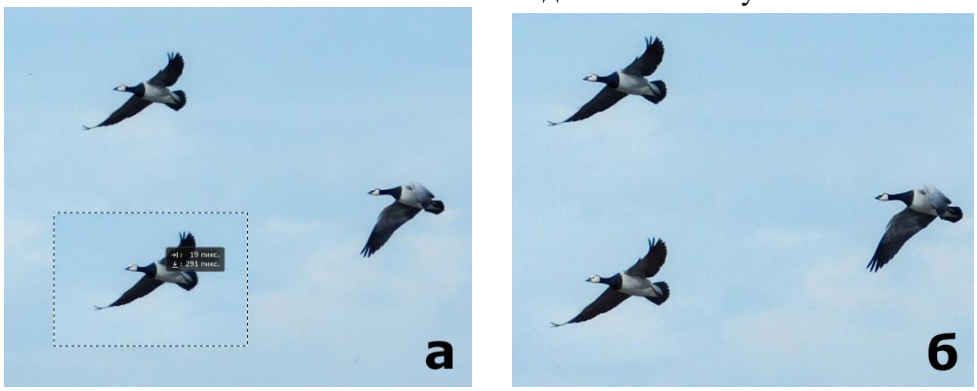


Рис. 6. Копіювання об’єкту інструментом «Латка»

Основна відмінність представлених способів копіювання у тому, що при використанні «штампу» об’єкт копіюється без змін. А при використані «Латки» перенесений об’єкт підлаштовує значення пікселів копійованої області для її органічного вбудовування в іншу частину зображення відповідно контексту.

На рисунку 7 представлений один і той же блок 3×3, але після використання методу «Латка» міняються кольори пікселів.

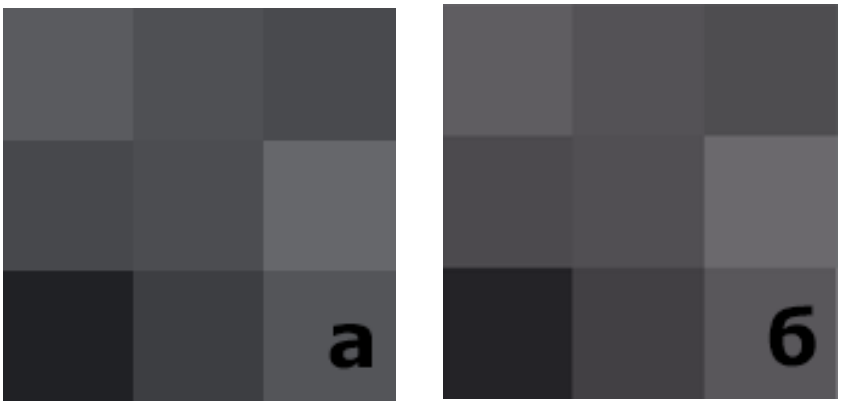


Рис. 7. Зміна кольорів копійованої області зображення після використання інструменту «Латка»

Цей ефект спостерігається по краях копійованої області і зменшується при просуванні до її центру. При достатніх розмірах області, що копіюється, в середині цієї області велика імовірність знайти однакові блоки. Зазвичай різні методи виявлення клонування й інших порушень цілісності використовують розбиття зображення на блоки 8×8, що можуть перетинатись чи не перетинатись. Крім того стандарт стиснення зображень JPEG також використовує розбиття на блоки такого розміру. Однак при виявленні «латки» розбиття на блоки 8×8 дало велику кількість помилок 1 роду. Виявлення фальсифікації було можливим лише при зберіганні без втрат та при розмірах фальсифікації, порівняних з половиною самого зображення. Тож було проведено експеримент з блоками різних розмірів, в ході якого встановлено, що оптимальним є використання блоків розміром 3×3.

Отже, основна задача алгоритму виявлення латки полягає у розбитті матриці зображення на блоки розміром 3×3, що перетинаються, та знайти серед них попарно однакові. Розглянемо роботу даного алгоритму на прикладі фальсифікації, виконаної над зображенням на рисунку 8 (оригінал). Фальсифіковано номер автомобіля інструментом «латка», а саме замість цифри 8 вставлено цифру 0 (рис.9).

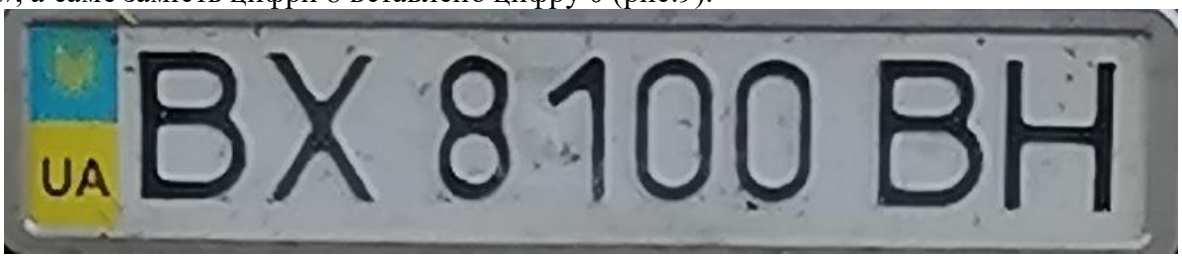


Рис. 8. Оригінальне зображення

Рис. 9. Приклад копіювання об’єкту

Результат було збережено у форматі з втратами jpg з високим ступенем якості та у форматі без втрат bmp. Результати роботи алгоритму для формату з втратами представлено на рисунку 10, для формату буз втрат – на рисунку 11.

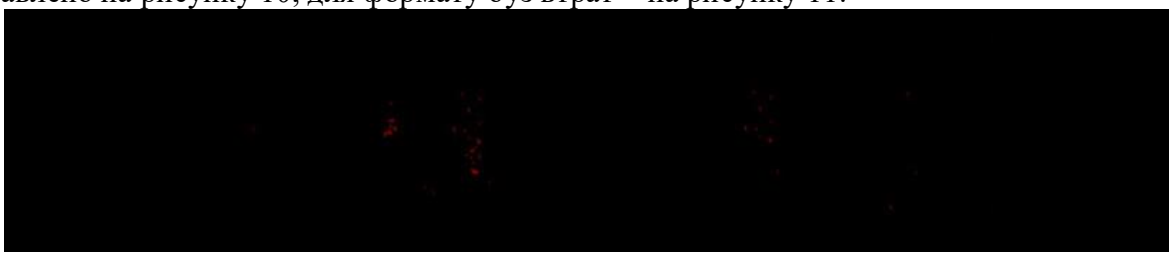


Рис. 10. Результат перевірки виявлення копіювання

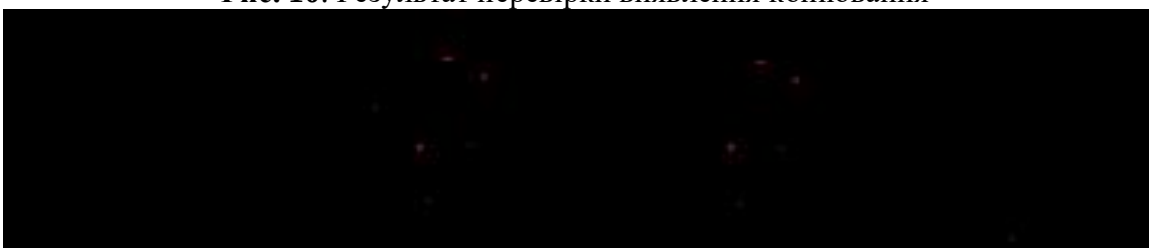


Рис. 11. Результат перевірки виявлення копіювання на зображенні без втрат

В обох випадках копійовані «латкою» області було виявлено: на місці, що відповідають образу і прообразу фальсифікації, знайдено ідентичні блоки (виділено червоним кольором). Однак, як і можна було очікувати, при збереженні з втратами виникають хибні тривоги (помилки 2 роду). Однак при виділенні сукупностей ідентичних блоків, які мають однакове розташування всередині сукупності відносно один одного, можна підвищити ефективність виявлення «латки» при збереженні у форматі з втратами. Тож на основі отриманих результатів алгоритм виявлення «латки» матиме додатковий етап у вигляді виділення зв’язних областей, виділені блоки в яких розміщені ідентично. Основні кроки алгоритму наступні.

Основні кроки алгоритму виявлення клонування, заснованого на аналізі сингулярних чисел блоків його матриці, представлені нижче. Нехай F – матриця зображення розмірів m×n.

1. Розбити матрицю F ЦЗ на 3×3-блоки $F_{ij}, i = 1,2\ldots,(n-2), j = 1,2\ldots,(m-2)$, що перетинаються так, аби кожний блок відрізнявся від сусіднього на один рядок (стовпець).

2. Побудувати матрицю S, елементи s_{ij} якої дорівнюють 1 (замалювати червоним), якщо блоки мають однакові значення пікселів, і 0 (замалювати чорним) – якщо різні ($i = 1,2\ldots,(n-2)$, $j = 1,2\ldots,(m-2)$).

3. Серед блоків, позначених цифрою 1, виділити зв'язні області з однаковим розташуванням виділених елементів, аби відрізнити фальсифіковані частини від хибних тривог.

Після цього ефективність алгоритму в термінах помилок першого та другого роду отримана такою, як її представлено в таблиці 1.

Таблиця 1

Результат експерименту

Формат	Помилки 1 роду	Помилки 2 роду
JPEG	6%	16%
BMP	4%	10%

Експеримент проведено із використанням 100 зображень. Таким чином можемо бачити, що розроблений алгоритм дійсно є ефективним як для зображень, збережених після фальсифікації у форматі з втратами, так і без втрат.

Висновки. Виявленню різних способів фальсифікації цифрових зображень у відкритому друці присвячено багато робіт, однак виявленню одного з можливих сучасних інструментів, - інструмент «латка» графічного редактора Adobe Photoshop, - навпаки, не приділяється уваги попри його популярність серед графічних маніпуляторів. Особливістю даного інструменту є подібність до інструменту «штамп» того ж редактора з відмінністю у підлаштуванні клонованої ділянки до частини фото, в якій вона опинилась. В даній роботі розроблено алгоритм виявлення даного порушення цілісності, який є ефективним як для зображень, збережених у форматі з втратами, так і для зображень без втрат.

Список літератури

1. Langille A. Gong M. An efficient match-based duplication detection algorithm. Canadian Conference on Computer and Robot Vision. 2006 P.64.

2. Luo W., Huang J. Qiu G. Robust detection of region duplication forgery in digital images. International Conference on Pattern Recognition. 2006. P.746–749.

3. Pan X, Lyu S. Region duplication detection using image feature matching

4. IEEE Transactions on Information Forensics and Security. 2010. Vol.5(4). P.857-867.

5. Wang J., Liu G., Li H., Dai Y., Wang Z. Detection of image region duplication forgery using model with circle block. International Conference on Multimedia Information Networking and Security. 2009. 25–29.

6. Shivakumar B.L.. Baboo S.S. Detection of Region Duplication Forgery in Digital Images Using SURF. IJCSI International Journal of Computer Science Issues. 2011. Vol.8. Issue 4. No1. P.199-205.

7. Зорило В.В. Методы повышения эффективности выявления нарушения целостности цифрового изображения. Інформаційна безпека. 2012. №1(7) . С.8.

8. Зоріло В.В. Метод підвищення ефективності виявлення порушення цілісності цифрового зображення: Дисертаційна робота кандидата технічних наук: 05.13.21. К., 2013. 127с.

DIGITAL IMAGE FALSIFICATION DONE BY METHOD OF ADOBE PHOTOSHOP PATCH

M.V.Gontar, V.V.Zorilo, O.Yu.Lebedeva

1, Shevchenko Ave., National Odessa Polytechnic University, 65044, Odesa Ukraine
vikazorilo@gmail.com, whiteswanhelena@gmail.com

Today, more and more actively forces us to take care of our information security. Events in the world and in Ukraine, information, hybrid wars, cybercrimes are what have become our everyday reality, and what prompts us to look for new and improve existing methods and means of information protection. One of the issues of information protection is the protection of graphic content from violations of its integrity. Violation of the integrity of digital images can be done with a wide variety of graphic editor tools. In particular, such a tool of the Adobe Photoshop graphic editor "patch" is a convenient way to falsify a photo, which is currently not paid attention to in the open press. Therefore, the need to identify this tool became the basis for the experiments described in this article. The purpose of this work is to improve the effectiveness of detecting fake photos made using the Adobe Photoshop tool "Patch" by developing an algorithm. In the work, a computational experiment was carried out using 100 digital images, which were processed with the "patch" tool. Based on the computational tool, an algorithm was developed that proved to be effective in cases where the image after falsification is saved in lossy and lossless formats. In most cases, it was possible to detect the presence of a violation of integrity in the case when it really took place, and to establish the fact of the absence of processing with the "patch" tool, when it really was not.
Keywords: violation of information integrity, information protection, cloning, patch, algorithm.

DOI 10.15276/imms.v12.no1-2.46
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 12 (2022), No. 1-2, pp. 46-52

ВИЯВЛЕННЯ ЧАСТИН ЦИФРОВОГО ЗОБРАЖЕННЯ, ЗМЕНШЕНИХ ПІСЛЯ ФАЛЬСИФІКАЦІЇ

В.В. Гулич, В.В. Зоріло, О.Ю.Лебедєва

1, пр.Шевченка, Національний університет «Одеська політехніка», 65044, Одеса
vikazorilo@gmail.com, whiteswanhelena@gmail.com

В час, коли використання цифрового контенту у всіх сферах життя неспинно зростає, можливість перевірки автентичності цифровіх файлів, зокрема, цифрових зображень, є вкрай важливою в галузі захисту інформації від порушень цілісності. В інформаційній війні повсякчас використовують фотофейки для досягнення певних, нерідко злочинних цілей. Як суспільство в цілому, так і окремі індивіди мають дбати про інформаційну безпеку та захищати свій інформаційний простір від неперевіреної інформації. Сучасні методи виявлення порушень цілісності графічної інформації певною мірою вирішують деякі питання інформаційної безпеки, однак, вони не є універсальними і часто потребують розвитку, вдосконалення, додаткових досліджень тощо. Так, існуючі методи виявлення такого поширеного способу фальсифікації зображень, як масштабування, є ефективними лише у випадках, коли фальсифікована частина збільшується, разом з цим при зменшенні частини зображення вони не є ефективними. Більше того, у відкритому друці проблема виявлення зменшених масштабованих частин зображення не висвітлена. Тому мета даної роботи - підвищення ефективності виявлення масштабування як фальсифікації цифрового зображення шляхом розробки алгоритму для детектування масштабування з від'ємним коефіцієнтом. В даній роботі проведено адаптацію метода аналізу рівня помилок для виявлення зменшених частин цифрового зображення. Ефективність адаптованого методу в термінах помилок 1 і 2 роду склала: помилки 1 роду – 2%, 2 роду – 7%. Крім того встановлено, що даний метод також є ефективним при виявленні одночасно масштабованих (зменшених) і переміщених частин цифрового зображення. Даний метод виявляє артефакти (помилки) на цифровому зображенні, які виникають при зменшенні його частини – фальсифікована ділянка має вищу високочастотну складову, ніж решта зображення, що підсилюється під впливом стиснення після збереження фальсифікації у форматі з втратами.

Ключові слова: виявлення фальсифікацій, цифрова криміналістика, масштабування.

Вступ

Сучасний світ дедалі більше стає залежним від зображень. Оскільки передача та засвоєння інформації відбувається значно легше за допомогою цифрового графічного контенту. Тому одним з головних питань постає оригінальність цього контенту, адже існує безліч способів фальсифікувати його, наприклад, клонування областей зображення, ретушування та накладання фільтрів, додавання сторонніх об'єктів до зображення та масштабування областей на зображенні.

Часто масштабування частин зображення застосовують під час його підробки як з додатнім (збільшення), так і з від'ємним (зменшення) коефіцієнтом. В той час як збільшенню у відкритому друці приділяється чимало уваги (ефективно себе показали методи, засновані на аналізі нульових сингулярних чисел блоків цифрового зображення), проблема зменшення взагалі не висвітлена. Відомі з відкритого друку методи виявлення масштабування не дають результатів при масштабуванні з від'ємним коефіцієнтом.

Мета даної роботи – підвищення ефективності виявлення масштабування як фальсифікації цифрового зображення шляхом розробки алгоритму для детектування масштабування з від'ємним коефіцієнтом.

Матеріали та методи

У той час, коли при збільшенні частини цифрового зображення відбувається додавання пікселів в збільшувану частину, яке виконується методом інтерполяції значень існуючих пікселів, при зменшенні частини зображення навпаки кількість пікселів зменшується, а розрахунок нових значень для пікселів, що лишилися, відбувається таким чином, аби зберегти інформативність підроблюваної частини. Якщо у першому випадку ставало більше низьких частот (фонових частин зображення), то у другому випадку контури стануть «щільнішими», збільшиться високочастотна складова зменшуваної частини, що в комбінації із стисненням після фальсифікації призведе до виникнення артефактів, або помилок. Виявлення артефактів, що виникають під час збереження зі стисненням, можна виконати методом Error lever analysis (ELA) [1].

В 2010 році П. Рінгвуд створив сервіс в вигляді веб-сайту під назвою «errorlevelanalysis.com». Але в 2012 році автор зачинив сайт. Після чого Hacker Factor відтворили веб-сайт Рінгвуда [2]. На сайті було створено алгоритм, який оцінює потенційний рівень помилок зображення в форматі JPEG, тобто вимірюється кількість змін під час повторного зберігання (рис. 1 – на зображення був доданий напис).

Рис. 1. Результат роботи алгоритму аналізу рівня помилок

Оскільки при редагуванні зображення змінені частини будуть мати потенційно збільшений рівень помилок, який не є характерним для більшої (нефальсифікованої) частини зображення, то даний алгоритм буде вказувати на наявність фальсифікації в конкретному місці.

Результати та обговорення

База для обчислювального експерименту по перевірці гіпотези щодо збільшеного рівня помилок в масштабованій частині зображення складається з 100 зображень з відкритого телеграм-каналу «Збройні Сили України. Війна з окупантами» [3]. Всі зображення мають різний розмір, роздільну здатність. Після цього всі зображення редагуються за допомогою графічного редактора Adobe Photoshop 2022.

Алгоритм редагування зображень такий.

1. Завантажуємо зображення і обираємо для нього профіль кольорів «Без змін».
2. За допомогою інструменту «Виділення об’єктів» виділяємо потрібний об’єкт на зображенні.
3. Копіюємо об’єкт на новий шар.
4. Робимо невидимим новий шар.
5. На оригінальному шарі знову обираємо об’єкт, що був скопійований на попередньому кроці.
6. Виконуємо заливку виділеної області «Права кнопка миші-Виконати заливку». Параметри заливки: зміст – з урахуванням змісту, режим накладання – нормальний.
7. Обираємо попередньо перенесений туди шар з об’єктом оригінального зображення та робимо його видимим.

8. Виконуємо масштабування об’єкту за допомогою трансформації. Комбінація клавіш Ctrl+T. Трансформуємо (зменшуємо) до потрібного вигляду в залежності від контексту.
9. Зберігаємо отримане зображення у форматі JPEG (параметри JPEG: якість – найкраща. Допустимі втрати 1% – менше виставити неможливо).

Пункт 6 – важливий етап виконання підробки. Заливка дозволяє виконати заповнення обраної частини зображення таким змістом, який схожий з суміжними ділянками зображення. Для отримання найкращих результатів обрана область повинна захоплювати область, яку ми хочемо відтворити на фінальному зображенні. Результат такої роботи показано на рисунку 1.

Рис. 2. Оригінальне (ліворуч) та фальсифіковане (праворуч) зображення

На фальсифікованому зображенні було зменшено чоловіка праворуч від танка. Для фальсифікованої частини відбулося збільшення високочастотної складової за рахунок маніпуляції із розміром цієї області, що саме по собі буде відрізняти цю частину від решти зображення, а в комбінації із стисненням при збереженні з втратами має проявитися ефект збільшення рівня помилок.

Основні кроки алгоритму виявлення фальсифікації наступні.

1) Завантажити зображення у форматі JPEG.
2) Виконати пере збереження даного зображення з завчасно визначеними втратами, які встановлюються вручну.
3) Розрахувати абсолютну (по модулю) попіксельну різницю між двома зображеннями, а саме початковим та збереженим із втратами.
4) Сформувати зображення з отриманої матриці різниці. Варто виділити, що мінімальна різниця буде сягати чисел, які будуть близькими до 0.
5) Знайти максимальні значення пікселів в кожному рядку матриці.
6) Серед мінімальних значень в рядках матриці знайти максимальне (k).
7) Розрахувати коефіцієнт за формулою: $255/k$.
8) Посилити яскравість всього зображення за допомогою визначеного коефіцієнту множенням його на кожен піксель зображення.
9) На отриманому зображенні виділити частини, що принципово відрізняються від решти зображення. Це і буде фальсифікація.

А на рисунку 3 представлено результати роботи алгоритму з тестовим зображенням, показаним на рисунку 1.

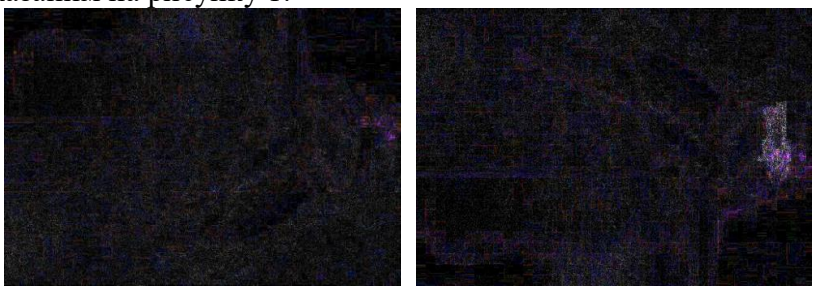


Рис. 3. Результат роботи алгоритму для оригіналу (ліворуч) та підробки (праворуч)

Як бачимо, на фальсифікованому зображенні явно виділена область масштабування, що є типовим результатом для даного експерименту (табл.1).

Таблиця 1

Результати роботи алгоритму пошуку масштабованого об'єкту

	Помилки 1 роду	Помилки 2 роду
Тестові зображення	2%	7%

Аналізуючи таблицю можна вважати, що при обробці оригінального зображення їх більшість не має жодних артефактів, що свідчить про те, що зображення не піддавалися редагуванню шляхом масштабування, а саме – зменшення. Артефакти присутні на 7% оригінальних зображень, що можна трактувати як похибку при зберіганні чи, можливо, зменшення всього зображення за допомогою сторонніх програм. Оскільки це може посилити контрастні контури, роблячи їх набагато яскравішими на виході. На зображеннях з масштабованою областю алгоритм ідентифікував її на 98% зразків.

Також було проведено експеримент не лише з масштабованими, а з масштабованими і одночасно переміщеними об’єктами на зображенні. Масштабування об’єкту відбувається за таким самим алгоритмом, а для його переміщення потрібно просто перетягнути об’єкт у графічному редакторі.

На рисунку 4 наведено оригінальне та фальсифіковане зображення. Фальсифікація була створена за допомогою масштабування та переміщення об’єкту.

Рис. 4. Оригінальне (ліворуч) та сфальсифіковане (праворуч) зображення

З рисунку 4 видно, що на фальсифікованому зображенні було зменшено чоловіка, який стоїть в лівій частині зображення, але його було ще й переміщено з лівої в праву частину зображення та розташовано перед військовою автівкою. Результат перевірки фото алгоритмом представлено на рисунку 5.

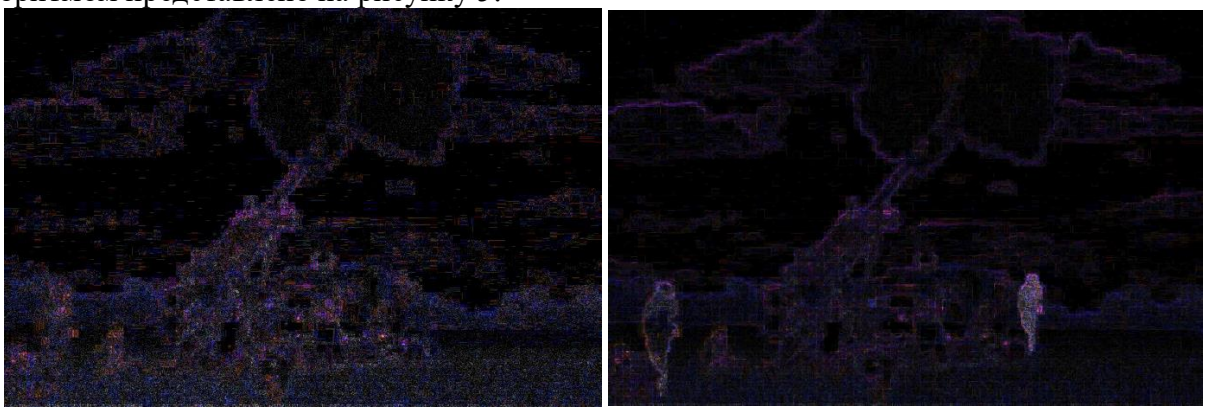


Рис. 5. Результат роботи алгоритму з фальсифікацією масштабування та переміщення

Як бачимо, оригінальне зображення містить однотонні контури зображення без видимих артефактів, що свідчить про те, що зображення є оригінальним. Зображення з правого боку має артефакти в зоні об’єкту, який було масштабовано та переміщено. Крім того, частина зображення, з якої було переміщено обєкт та в якій було виконано заливку, також виділена контуром. Результати даного експерименту показано в таблиці 2.

Таблиця 2

Результати роботи алгоритму при пошуку масштабовано-переміщеного об’єкту

Зображення	Помилки 1 роду	Помилки 2 роду
Тестові зображення	0%	0%

Після проведення другого експерименту може виникнути думка, що зазначеним методом також можна виявити клонування без масштабування. Третьою частиною експерименту стало виявлення клонування частин зображення. Клонування об’єкту відбувається за рахунок інструменту «Штамп», який дає змогу копіювати зміст з вихідної ділянки та використовувати його на інших ділянках зображення. Послідовність дій для клонування об’єкту за допомогою даного інструменту:

На рисунку 6 зображено оригінальне зображення та зображення з клонованою областю за допомогою інструменту «штамп».

Рис. 6. Оригінальне та фальсфіковане зображення

Тепер протестуємо алгоритм на цих зображеннях та перевіримо наявність артефактів, тим самим встановимо, чи фіксує алгоритм такі види фальсифікацій, як клонування. Роботу алгоритму з даними зображеннями буде представлено на рисунку 7.

Рис. 7. Результати роботи алгоритму на оригінальному (ліворуч) та фальсифікованому (праворуч) зображеннях

Розглядаючи отримані результати, можна зробити висновок, що алгоритм не може виявити клонування об’єктів, виконане за допомогою інструменту «штамп». В таблиці 3 наведено результати експерименту.

Таблиця 3

Результати роботи алгоритму пошуку клонованих областей зображення

Зображення	Помилки 1 роду	Помилки 2 роду
Тестові зображення	80%	7%

Результати експерименту вказують на те, що даний алгоритм не може виявити фальсифікацію клонування об’єктів.

Отож підсумок за даними результатами полягає в тому, що алгоритм аналізу рівня помилок дійсно може допомогти при аналізі зображень, які могли бути фальсифіковані методами масштабування та масштабування і переміщення об’єкту на зображенні. Саме тому було вирішено інтегрувати даний алгоритм в телеграм-бота.

Висновки

В даній роботі було проведено аналіз сучасного стану проблеми виявлення фальсифікації цифрового зображення. Серед сучасних методів виявлення основних способів підробити зображення було виділено методи виявлення клонування, ретушування та масштабування. Встановлено, що проблема виявлення масштабування має рішення, коли мова йде про збільшення частини зображення. В цей самий час зменшенню частин зображення у відкритому друці не приділяється уваги, а існуючі методи ефективні лише для виявлення збільшення.

Оскільки при зменшенні частини цифрового зображення відбувається зміна значень пікселів зони, що зменшується, та зони навколо неї, це призводить до виникнення артефактів масштабування, або до зростання рівня помилок. До виявлення слідів цих артефактів в роботі адаптовано метод, заснований на аналізі рівня помилок, який раніше застосовували для виявлення ретушування.

Даний метод показав спроможність виявляти фальсифіковані частини зображення, які було піддано зменшенню. Він також показав високу ефективність, коли зменшену частину було переміщено. Даний метод не ефективний у виявленні переміщення без зменшення, а також у виявленні збільшення частини зображення.

Ефективність методу з врахуванням обмежень його застосування: помили першого роду 2%, помилки другого роду 7%.

Список літератури

1. Експертиза фотографій: виявлення маніпуляцій з фотошопом за допомогою аналізу рівня помилок. URL: https://resources.infosecinstitute.com/topic/error-level-analysis-detect-image-manipulation/

2. Що таке фотофорензика? URL: https://fotoforensic.com/faq.php# What%20is %20 FotoForensics

3. Збройні сили України. Війна з окупантами. URL: https://t.me/zsuwar

DETECTION OF DIGITAL IMAGE PARTS REDUCED AFTER FORGERY

V.V.Gulich, V.V. Zorilo, O.Yu.Lebedeva

1, Shevchenko Ave., National Odessa Polytechnic University, 65044, Odesa, Ukraine
vikazorilo@gmail.com, whiteswanhelena@gmail.com

At a time when the use of digital content in all spheres of life is constantly growing, the ability to verify the authenticity of digital files, in particular digital images, is extremely important in protecting information from integrity violations. In the information war, photo fakes are always used to achieve certain, often criminal, goals. Both society as a whole and individuals must take care of information security and protect their information space from unverified information. Modern methods of detecting violations of the integrity of graphic information to some extent address some issues of information security, however, they are not universal and often require development, improvement, additional research and so on. Thus, existing methods for detecting such a common method of image falsification as scaling are effective only in cases where the falsified part is enlarged, however, when reducing part of the image, they are not effective. Moreover, in open printing the problem of detecting reduced scalable parts of the image is not covered. Therefore, the aim of this work is to increase the efficiency of scaling detection as digital image falsification by developing an algorithm for detecting scaling with a negative coefficient. In this paper, the method of error level analysis is adapted to detect reduced parts of the digital image. The efficiency of the adapted method in terms of errors of the 1st and 2nd kind was: errors of the 1st kind - 2%, 2nd kind - 7%. In addition, it has been found that this method is also effective in detecting simultaneously scalable (reduced) and moved parts of a digital image. This method detects artifacts (errors) in the digital image, which occur when reducing its part - the falsified area has a higher high-frequency component than the rest of the image, which is amplified under the influence of compression after saving the falsification in a lossy format.
Keywords: detection of falsifications, digital criminal science, scaling

DOI 10.15276/imms.v12.no1-2.53
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 12 (2022), No. 1-2, pp. 53-64

ВИЯВЛЕННЯ ФОТОПІДРОБОК, ВИКОНАНИХ ЗАСОБАМИ НЕЙРОННИХ МЕРЕЖ

Є.В. Тимофеєв, В.В. Зоріло

1, пр.Шевченка, Національний університет «Одеська політехніка», 65044, Одеса
vikazorilo@gmail.com, timofeevzhenya2107@gmail.com

Глибоке навчання є ефективною та корисною технікою, яка широко застосовується в різних областях, включаючи комп'ютерний зір, машинний зір та обробку природної мови. Deepfake використовує технологію глибокого навчання, щоб маніпулювати зображеннями та відео людини, які люди не можуть відрізнити від реальних. Deepfake зазвичай створюють двома способами. Перший спосіб – за допомогою генеративної змагальної мережі, або GAN, яка використовує дві окремі нейронні мережі, які працюють разом, навчаючись вивчати характеристики реальних зображень, щоб вони могли створювати переконливі фотопідробки. Другий спосіб – за допомогою алгоритму штучного інтелекту (ШІ), який має назву інкодер і працює шляхом запуску знімків облич двох людей через інкодер для знаходження схожості між цими знімками та запуску декодера, який отримує зображення обличчя та міняє їх місцями. Досягнення в області Deepfake однаково вражають і турбують. У чужих руках ця технологія може бути використана для поширення дезінформації та підриву суспільної довіри майже як науково-фантастичний тип крадіжки особистих даних, коли ви можете змусити будь-кого сказати що завгодно. У зв'язку з цим можна констатувати, що задача детектування Deepfake є дуже важливою та потребує застосування нових для цієї галузі досліджень, розробки нових алгоритмів детектування Deepfake та вдосконалення вже існуючих методів. Отже, метою цієї роботи є створення системи виявлення порушень цілісності медіа файлів, виконаних за технологією Deepfake. В роботі виконано вибір нейронної мережі та її навчання на спеціально створеній базі, що дало можливість виявляти Deepfake як у цифрових зображеннях, так і в цифрових відеозаписах.
Ключові слова: deepfake, виявлення фальсифікацій, цифрова криміналістика, нейронна мережа.

Вступ

На перший погляд технологія Deepfake може здаватися веселим, навіть корисним інструментом. Навіть високобюджетні фільми використовують технологію Deepfake, щоб повернути молодші версії улюблених персонажів. Але переваги цієї технології мінімальні в порівнянні з потенційною небезпекою, яку вона несе. Сьогодні ця технологія використовується для створення порнографії, фейкових новин, містифікацій, знущань, фінансового шахрайства тощо. У березні 2022 року діпфейк президента України Володимира Зеленського, який закликає своїх солдатів скласти зброю, потрапив на зламаний український новинний веб-сайт, а потім став вірусним, перш ніж було визнано, що він є фейком. Хоча точні збитки від цього інциденту залишаються невідомими, він продемонстрував одне з найнебезпечніших застосувань цієї технології. Якби це відео не було швидко позначено як фейк, воно могло б призвести до втрат і змінити хід конфлікту. Цю ж технологію можна використовувати як форму фішингу на робочому місці. Хоча хакери зазвичай використовують текстову переписку, щоб, наприклад, видавати себе за вашого боса чи колегу, тепер хакери можуть зателефонувати вам у Zoom, видавати себе за вашого боса та змусити вас придбати предмети або передати конфіденційну інформацію.

Опис технології Deepfake

Термін «Deepfake» походить від «Deep Learning» (Глибоке навчання) і «Fake» (Фейк), і він описує конкретні фотореалістичні відео або зображення, створені за підтримки глибокого навчання. Це слово було названо на честь анонімного користувача Reddit наприкінці 2017 року, який застосував методи глибокого навчання, щоб замінити обличчя людини в порнографічних відео, використовуючи обличчя іншої людини, і

створив фотореалістичні підроблені відео. Для створення таких підроблених відео використовувалися дві нейронні мережі: генеративна мережа та дискримінаційна мережа з технікою FaceSwap. Генеративна мережа створює підроблені зображення за допомогою кодера та декодера. Дискримінаційна мережа визначає автентичність знову створених зображень. Комбінація цих двох мереж називається Генеративною змагальною мережею (GAN).

Генеративні змагальні мережі (GAN) – це алгоритмічні архітектури, які використовують дві нейронні мережі, налаштовуючи одну проти іншої (тому «змагальні»), щоб генерувати нові синтетичні екземпляри даних, які можуть передаватись як реальні дані. Вони широко використовуються при генерації зображень, відео та голосу.

GAN були представлені в статті Яна Гудфеллоу [1] та інших дослідників з Університету Монреаля, включаючи Йошуа Бенджіо, у 2014 році. Згадуючи GAN, керівник дослідження ШІ Facebook Янн Лекун назвав змагальне навчання «найцікавішою ідеєю за останні 10 років у Машинному Вченні».

Потенціал GAN як для добра, так і для зла величезний, оскільки вони можуть навчитися імітувати будь-який розподіл даних. Тобто GAN можна навчити створювати світи, моторошно схожі на наш, у будь-якій області: зображення, музика, мова, проза. У певному сенсі вони художники-роботи. Але їх також можна використовувати для створення підробленого медіа-контенту, і вони є технологією, що лежить в основі Deepfake.

GAN працює наступним чином. Одна нейронна мережа, яка називається генератором, генерує екземпляри даних, а інша (дискримінатор) оцінює їх на достовірність; тобто дискримінатор вирішує, чи входить кожен екземпляр даних, який він переглядає, до фактичного набору даних для навчання, чи ні.

Наприклад, ми збираємось генерувати рукописні цифри, подібні до тих, що містяться в наборі даних MNIST [2], який береться з реального світу. Метою дискримінатора, коли він показує екземпляр із справжнього набору даних MNIST, є розпізнавання тих, які є автентичними. Тим часом генератор створює нові синтетичні образи, які передає дискримінатор. Це робиться в надії, що вони будуть визнані справжніми, навіть якщо вони підроблені. Мета генератора – генерувати прохідні рукописні цифри: брехати, не будучи спійманим. Мета дискримінатора – ідентифікувати зображення, яке надходить від генератора, як підробку. Ось кроки, які виконують GAN (рис.1).

1. Генератор приймає випадкові числа і повертає зображення.
2. Це згенероване зображення подається в дискримінатор разом із зображеннями, взятими з фактичного набору даних.
3. Дискримінатор бере як реальні, так і підроблені зображення та повертає ймовірність, число від 0 до 1, де 1 означає, що фото достовірне, а 0 вказує на підробку.

Отже, маємо подвійний цикл зворотного зв’язку: дискримінатор знаходиться в циклі зворотного зв’язку з реальним зображенням. Генератор знаходиться в петлі зворотного зв'язку з дискримінатором.

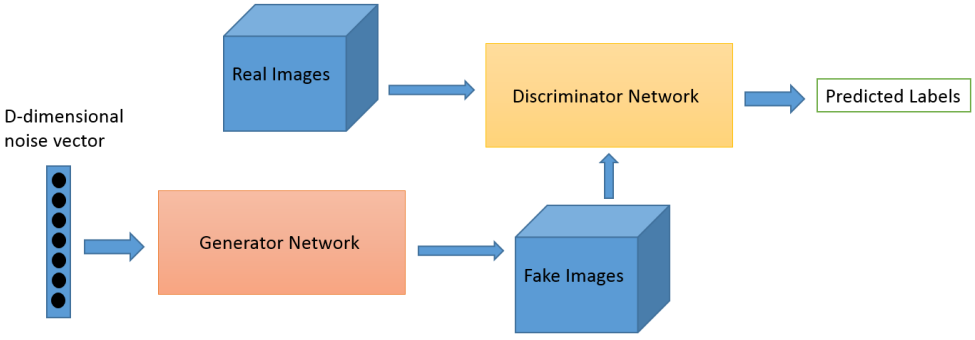


Рис. 1. Схема GAN

Буде корисним порівняти генеративні змагальні мережі з іншими нейронними мережами, такими як автокодери та варіаційні автокодери.

Автокодери кодують вхідні дані як вектори [3]. Вони створюють приховане або стиснене представлення необроблених даних. Вони корисні для зменшення розмірності; тобто вектор стискає вихідні дані в меншу кількість помітних вимірів. Автокодери можна об'єднати з так званим декодером, який дозволяє відновлювати вхідні дані на основі їх прихованого представлення.

Варіаційні автокодери – це генеративний алгоритм, який додає додаткове обмеження для кодування вхідних даних. Варіаційні автокодери здатні як стискати дані, як автокодер, так і синтезувати дані, як GAN. Однак, хоча GAN генерує дані з дрібними деталями, зображення, створені варіаційними автокодерами, мають тенденцію бути більш розмитими.

Методи детектування Deepfake

Протягом останніх років методи глибокого навчання успішно застосовуються для виявлення підроблених зображень. Однак сучасні методи глибокого навчання зображення не можуть бути безпосередньо застосовані для виявлення підроблених відео через наявність значної втрати інформації кадру після стиснення відео. Методи виявлення діпфейків можна поділити на дві основні категорії: ті, що працюють завдяки біологічному аналізу поодиноких осіб та ті, що працюють завдяки аналізу просторових і часових особливостей відео.

Біологічний аналіз поодиноких осіб. Юезен Лі [4] розробив метод, заснований на нейронній мережі для виявлення діпфейку у відео. Цей метод передбачає моргання очей для виявлення підроблених відео. Він використовує згорткову нейронну мережу з рекурсивною нейронною мережею для виявлення фізіологічних сигналів, таких як рух очей і моргання. Потім модель використовує двійковий класифікатор для визначення стану закритих і відкритих очей. Цей підхід перевірено за допомогою набору даних під назвою «eye-blinking» (моргання очей), який сканується з Інтернету. Результати експерименту демонструють ефективність запропонованого підходу у виявленні підроблених зображень.

Інші біологічні сигнали, такі як серцебиття, як було показано, є надійним провісником для реального відео. Ціфці та інші розробив модель на основі генеративної змагальної мережі (GAN), яка може виявляти джерело діпфейку, аналізуючи його сигнали [5]. Запропонована модель починається з кількох мереж детекторів, де вхідним сигналом для цієї моделі є реальне відео. Потім пара реалістичного відео та підробленого відео призначається іншому шару, який називається реєстрацією, який витягує цікаві ділянки обличчя і біологічні сигнали для створення клітин фото плетизмографії (ФПГ). Тут осередки ФПГ є просторово-часовими вікнами, які містять кілька облич, витягнутих за допомогою детектора облич. Останній шар відповідає за класифікацію відео як підробленого чи справжнього. Автори використали кілька загальнодоступних наборів даних для перевірки своєї моделі. Результат показує, що моделі активують точність 97,3% у виявленні діпфейків.

Аналіз просторових і часових ознак. Більшість сучасних методів виявлення діпфейків використовують лише один відеокадр [6]. Фактично, маніпуляції з відео можна виконувати з кількома функціями на рівні кадру. Останнім часом багато досліджень показали, що аналіз тимчасової послідовності між кадрами може успішно допомогти відрізнити реальне відео від підробленого. У цій роботі автори представили тимчасову модель для виявлення фейкових відео. У моделі спочатку використовується згорткова нейронна мережа для виділення ознак кадру. Згодом ці ознаки передаються на шар ДКЧП (довгої короткочасної пам'яті) для аналізу тимчасової послідовності зміни обличчя між Нарешті, функція softmax використовується для класифікації відео як реального чи підробленого. Для оцінки було зібрано колекцію з 600 відео з кількох веб-сайтів. Результати експерименту свідчать про ефективність цієї моделі для виявлення діпфейків.

На основі попередньої версії Cycle-GAN [7] було представлено новий підхід під назвою Recycle-GAN [8], який використовує умовні генеративні змагальні мережі для злиття просторових і часових даних. Результати оцінки показують, що поєднання просторових і часових обмежень може дати ефективний результат. Крім того, також було запропоновано новий підхід, заснований на рекурентній згортковій мережі [9]. Підхід складається з двох етапів аналізу: етап обробки обличчя з подальшим виявленням діпфейку. Під час обробки, кадрування та вирівнювання обличчя витягується за допомогою мережі просторового трансформатора. Потім вихідні дані з попередніх етапів передаються для виявлення діпфейку за допомогою рекурентної згорткової мережі, де аналізується тимчасова інформація по кадрах.

Вибір та навчання нейронної мережі

Глибокі нейромережі є областю машинного навчання, яке невпинно розвивається. Розвиток цього напряму призвів до появи великої кількості алгоритмів, побудованих на глибокому навчанні. Нейромережі використовують усі основні алгоритми для генерації підробних зображень.

Нейронні мережі відображають поведінку людського мозку, дозволяючи комп'ютерним програмам розпізнавати закономірності та вирішувати загальні проблеми в області ШІ, машинного навчання та глибокого навчання.

Нейронні мережі, також відомі як штучні нейронні мережі (ШНМ) або змодельовані нейронні мережі (ЗНМ), вони лежать в основі алгоритмів глибокого навчання. Штучні нейронні мережі (ШНМ) складаються з шарів вузлів, що містять вхідний шар, один або кілька прихованих шарів і вихідний шар (рис.2).

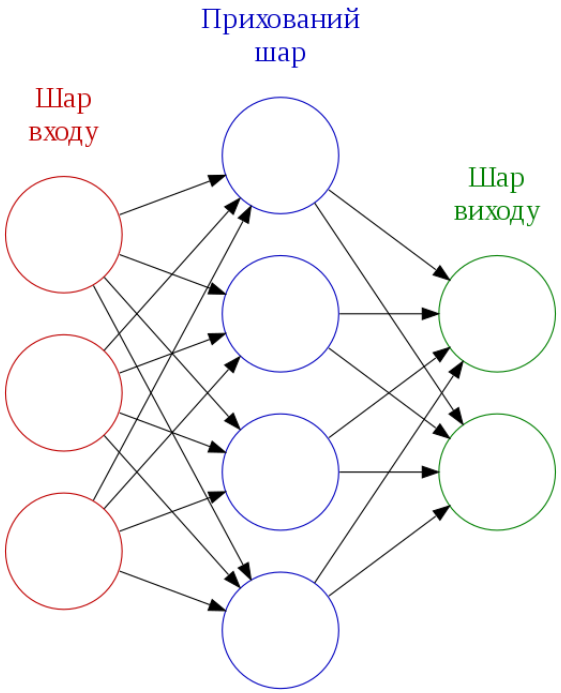


Рис.2. Структура нейронної мережі

Кожен вузол або штучний нейрон з'єднується з іншим і має відповідну вагу та поріг. Якщо вихід будь-якого окремого вузла перевищує вказане порогове значення, цей вузол активується, надсилаючи дані на наступний рівень мережі. В іншому випадку дані не передаються на наступний рівень мережі.

Нейронні мережі покладаються на навчальні дані, щоб з часом покращувати свою точність. Однак, як тільки ці алгоритми навчання будуть максимально налаштовані на точність, вони стануть потужними інструментами в інформатиці та штучному інтелекті,

що дозволить нам класифікувати дані з високою швидкістю. Однією з найвідоміших нейронних мереж є пошуковий алгоритм Google.

Інформація протікає через нейронну мережу двома способами. Коли вона навчається (тренується) або працює нормально (після навчання), шаблони інформації надходять у мережу через вхідні блоки, які запускають шари прихованих блоків, а ті, у свою чергу, надходять до вихідних блоків. Ця поширена конструкція називається мережею прямого зв'язку. Не всі блоки працюють постійно. Кожен блок отримує вхідні дані від одиниць зліва, і вхідні дані помножуються на вагу з'єднань, по яких вони рухаються. В кожному блоці необхідно знайти суму всіх вхідних даних, які він отримує таким чином, і (у найпростішому типі мережі), якщо сума перевищує певне порогове значення, блок запускає одиниці, до яких він підключений (ті, що праворуч).

Щоб нейронна мережа навчалася, має бути задіяний елемент зворотного зв'язку. Нейронні мережі тренуються за допомогою процесу зворотного зв'язку, який називається зворотним поширенням. Це включає порівняння результату, який виробляє мережа, з результатом, який вона повинна була генерувати, після чого відбувається використання різниці між ними для зміни ваги зв'язків між одиницями в мережі. З часом зворотне розповсюдження змушує мережу вчитися, зменшуючи різницю між фактичним і передбачуваним виходом до точки, де передбачуване і фактичне значення точно збігаються.

Згорткові нейронні мережі (ЗНМ) (рис.3) зазвичай використовуються для розпізнавання зображень, візерунків та/або комп'ютерного зору, тому для детектування Deepfake буде застосовуватися саме цей тип нейронних мереж.

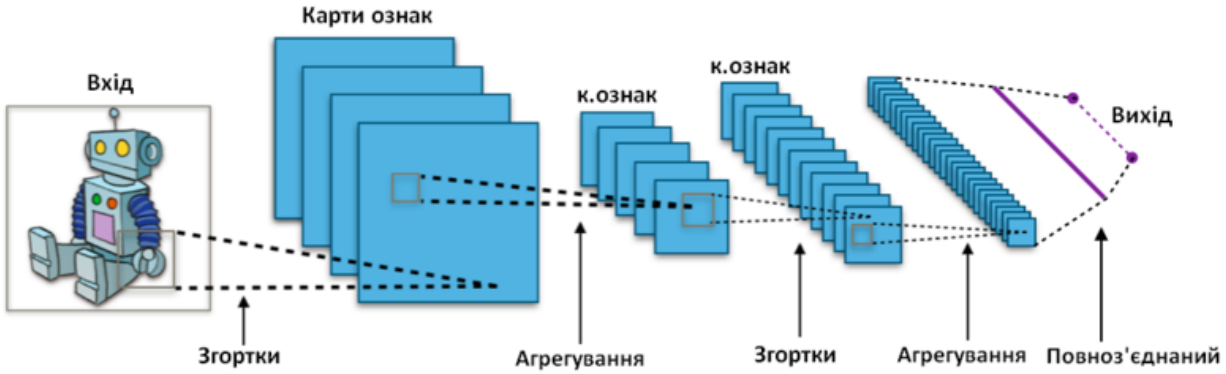


Рис.3. Структура згорткової нейронної мережі

Ці мережі використовують принципи лінійної алгебри, зокрема множення матриці для визначення шаблонів у зображенні. Вони мають три основних типи шарів, а саме:

- згортковий шар;
- об'єднуючий шар;
- повнозв'зний шар.

З кожним шаром ЗНМ збільшується у своїй складності, ідентифікуючи більші частини зображення. Більш ранні шари зосереджені на простих елементах, таких як кольори та краї. Коли дані зображення просуваються через шари ЗНМ, вона починає розпізнавати більші елементи або форми об'єкта, поки нарешті не ідентифікує передбачуваний об'єкт.

Припустимо, що вхідним буде кольорове зображення, яке складається з матриці пікселів у 3D. Це означає, що вхідні дані будуть мати три виміри – висоту, ширину та глибину – які відповідають RGB-зображенню. Згортковий шар має детектор особливостей, також відомий як ядро або фільтр, який переміщається по сприйнятливих полях зображення, знаходячи особливості. Цей процес відомий як згортка.

Детектор особливостей – це двовимірний (2-D) масив ваг, який представляє частину зображення. Хоча вони можуть відрізнятися за розміром, розмір фільтра зазвичай є матрицею 3×3; це також визначає розмір рецептивного поля. Потім фільтр застосовується до області зображення, і між вхідними пікселями та фільтром обчислюється скалярний добуток. Цей скалярний добуток потім подається у вихідний масив. Після цього фільтр зміщується на один крок, повторюючи процес, поки ядро не охопить усе зображення. Остаточний вихід із ряду точкових добутків із входу та фільтра відомий як карта ознак, карта активації або згорнута функція.

Шар об’єднання, також відомий як знижувач дискретизації, зменшує розмірність, зменшуючи кількість параметрів у вхідних даних. Подібно до згорткового шару, шар об’єднання застосовує фільтр по всьому зображенню, але різниця в тому, що цей фільтр не має жодних ваг. Замість цього ядро застосовує функцію агрегації до значень у сприйнятливому полі, заповнюючи вихідний масив.

Назва повнозв'язного шару влучно описує себе. У повнозв’язному шарі кожен вузол вихідного шару підключається безпосередньо до вузла попереднього шару. Цей шар виконує завдання класифікації на основі ознак, витягнутих через попередні шари та їх різні фільтри.

Для детектування Deepfake була обрана модель нейронної мережі (рис.4) ,заснована на статті, опублікованій Даріусом Афчаром та ін. у 2018 році [10]. Це двійковий класифікатор, побудований як відносно неглибока згорткова нейронної мережі, навчена класифікувати зображення на один із двох класів. Один клас відноситься до «реальних» зображень (зображення реальних людей), а інший – до «підроблених» зображень (зображень, створених Deepfake ШІ).

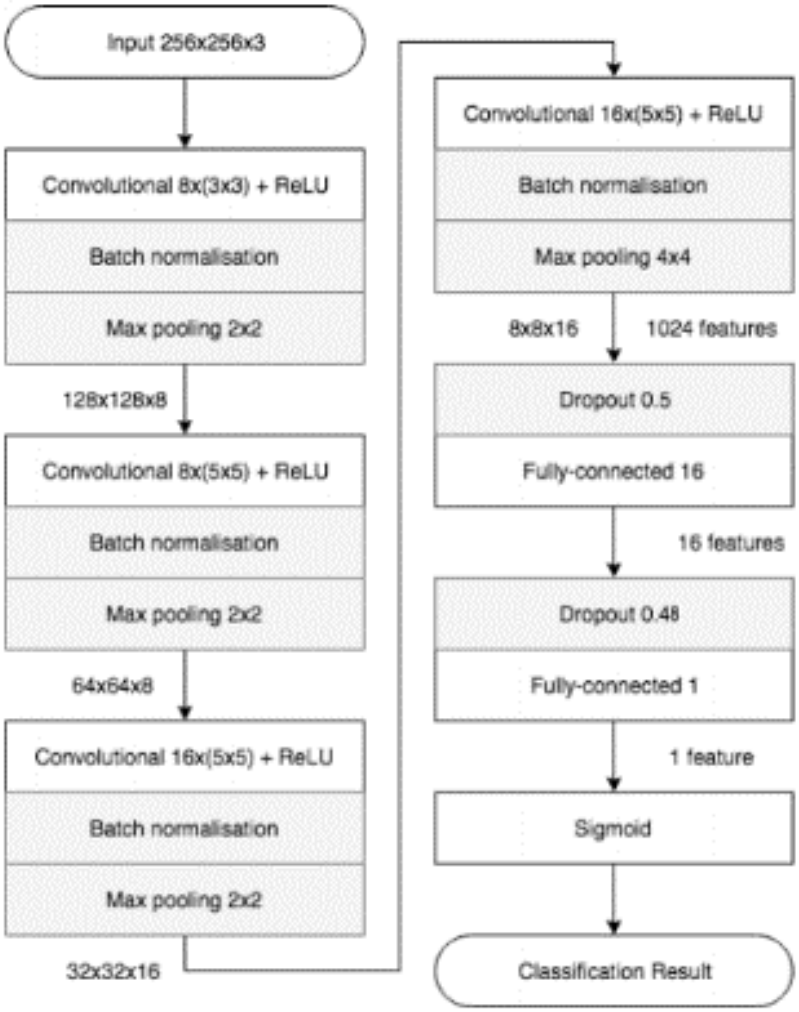


Рис.4. Модель нейронної мережі

− Вхідний шар 3×256×256, який приймає розмір зображення та кількість кольорових каналів.

− Згортковий шар із 8 фільтрами, розміром 3×3 і кроком 1, за яким слідує максимальний об'єднуючий шар розміром 2×2.

− Згортковий шар із 8 фільтрами розміром 5×5 і кроком 1, за яким слідує максимальний об'єднуючий шар розміром 2×2.

− Два згорткових шари з 16 фільтрами розміром 5×5 і кроком 1, за якими слідують максимальні шари об'єднання з вікном об'єднання 2×2.

− Повнозв'язний шар з 16 нейронами.

− Повністю підключений вихідний шар з одним блоком і сигмовидною активацією [11].

Згортковий шар, представлений conv2d, є найважливішою частиною нейронної мережі. Тут встановлюється розмір та кількість фільтрів, які використовуватимуться у згортці. Кожен фільтр є окремим елементом зображення, наприклад, горизонтальна лінія. Під час згортки цей фільтр проходить по зображенню, щоб оцінити, якою мірою певні області цього зображення відповідають фільтру. Після згорткового шару слідує шар пакетної нормалізації. Пакетна нормалізація – це новий метод підвищення швидкості та стабільності нейронних мереж. Він працює шляхом нормалізації вхідних даних для кожного шару мережі, що зменшує взаємозалежність між параметрами даного шару та вхідним розподілом наступного шару. Ця взаємозалежність називається внутрішнім коваріантним зрушенням і надає дестабілізуючу дію на процес навчання. Останній шар наших згорткових блоків – це шар пулу. Саме на рівні пулу значно зменшується розмірність даних, що значно прискорює обчислення. У даній моделі використовується максимальний пул цього шару, що означає зменшення області значень пікселів до максимального значення цієї області. Незважаючи на те, що ця архітектура ретельно дотримується, були проведені експерименти з різними функціями активації. Зокрема, крім використання стандартної активації ReLU також були проведені експерименти з ELU [12] та LeakyReLU [13].

ReLU є функцією активації вибору, оскільки немає очевидного ризику «мертвих нейронів» [14] . Крім того, існує активація LeakyReLU після повністю підключеного шару з 16 одиниць. За цим немає жодної видимої причини, крім того, що використовує газета.

Dropout – випадання, додається після повністю підключеного шару з 16 нейронами для боротьби з перенавчанням. Перенавчання – одна з проблем глибоких нейронних мереж (Deep Neural Networks, DNN), яка полягає в наступному: модель добре пояснює лише приклади з навчальної вибірки, адаптуючись до навчальних прикладів, замість того, щоб вчитися класифікувати приклади, що не брали участь у навчанні (втрата здатності до узагальнення). За останні роки було запропоновано безліч рішень проблеми перенавчання, але одне з них перевершило всі інші, завдяки своїй простоті та чудовим практичним результатам; це рішення – Dropout. Головна ідея Dropout – замість навчання однієї DNN навчити ансамбль кількох DNN, а потім усереднити отримані результати. Нейромережі для навчання створюються за допомогою виключення з нейронної мережі (dropping out) нейронів із ймовірністю p, таким чином, ймовірність того, що нейрон залишиться в мережі, становить q=1-p. «Виключення» нейрона означає, що при будь-яких вхідних даних або параметрах він повертає 0. Виключені нейрони не роблять свій внесок у процес навчання на жодному з етапів алгоритму зворотного поширення помилки (backpropagation); тому вимкнення хоча б одного нейрона рівносильне навчанню нової нейронної мережі.

Flatten (згладжування) – це перетворення даних в одновимірний масив для введення їх у наступний шар. Вирівнюються вихідні дані згорткових шарів, щоб створити один довгий вектор ознак. І це пов'язано з остаточною моделлю класифікації, яка

називається повністю зв’язаним шаром. Іншими словами, відбувається переміщення всіх піксельних даних в один рядок і з’єднання з останнім шаром.

Dense (повнозв’язний шар) – це простий шар нейронів, в якому кожен нейрон отримує вхідні дані від усіх нейронів попереднього шару, тому його називають щільним. Повнозв’язний шар використовується для класифікації зображень на основі вихідних даних із згорткових шарів. Робота одного нейрона. Шар містить кілька таких нейронів.

Для навчання нейронної мережі був використаний набір даних діпфейків, який складався з зображень, які були вилучені зі 175 відео, знятих з популярних платформ діпфейків, та модифікований, а саме з кожного зображення було вилучено обличчя і таким чином був створений новий набір даних для навчання нейронної мережі. Для вилучення облич використовувався метод HOG (гістограми орієнтованих градієнтів), який є дескриптором ознак і використовується в технологіях комп’ютерного зору та обробці зображень з метою виявлення об’єктів. Ця техніка підраховує кількість напрямків градієнта в локальних областях зображення. Дескриптор HOG фокусується на структурі або формі об’єкта. Це краще, ніж будь-який інший дескриптор ознак, оскільки він використовує величину градієнта, а також кут градієнта для обчислення ознак. Для областей зображення він генерує гістограми, використовуючи величину та орієнтацію градієнта. Градієнти розраховуються в межах розподілення зображення на блоки. Блок розглядається як піксельна сітка, в якій градієнти складаються з величини і напрямку зміни інтенсивності пікселя всередині блоку.

Модифікація набору даних була зроблена для збільшення якості навчання нейронної мережі. Фінальний набір даних складає 11780 зображень, які діляться на реальні зображення та діпфейки. Вхідними даними є зображення розміром 256×256×3, де 256×256 – висота і ширина зображення в пікселях, 3 – кількість кольорових каналів. Приклад оригінального зображення та зображення після модифікації можна подивитися на рис.5.

а) оригінальне зображення

б) модифіковане зображення

Рис. 5. Приклад зображень

Для навчання був використаний оптимайзер Adam – один із найефективніших алгоритмів оптимізації у навчанні нейронних мереж. Він поєднує в собі ідеї RMSProp та оптимізатора імпульсу [15] .

Після аналізу великої кількості тестувань на меншому наборі даних, який складав 1000 зображень, при швидкості навчання рівній 0.001 та чотирьох епохах було ідентифіковано, що найкращі результати у тренуванні та тестуванні показала модель нейронної мережі, де шар Dropout змінений з 0,5 до 0,48. Архітектура модифікованої моделі знаходиться на рис.6.

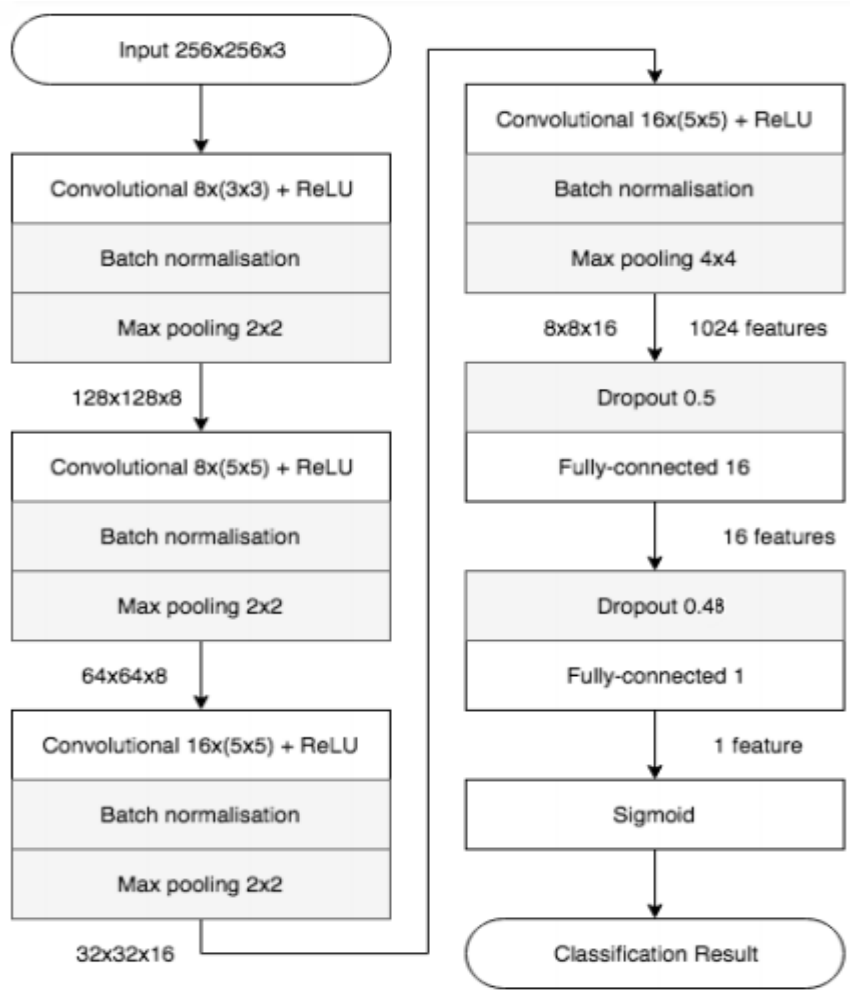


Рис.6. Змінена модель нейронної мережі

А саме після другої епохи була встановлена максимальна точність підтвердження (validation accuracy) – 98,57% та мінімальна втрата підтвердження (validation loss) – 1,26%. В той час на моделі нейронної мережі [1]: максимальна точність підтвердження (validation accuracy) – 97,58% та мінімальна втрата підтвердження (validation loss) – 1,93%. Графік навчання моделі [1] знаходиться на рис.7, а модифікованої моделі на рис.8.

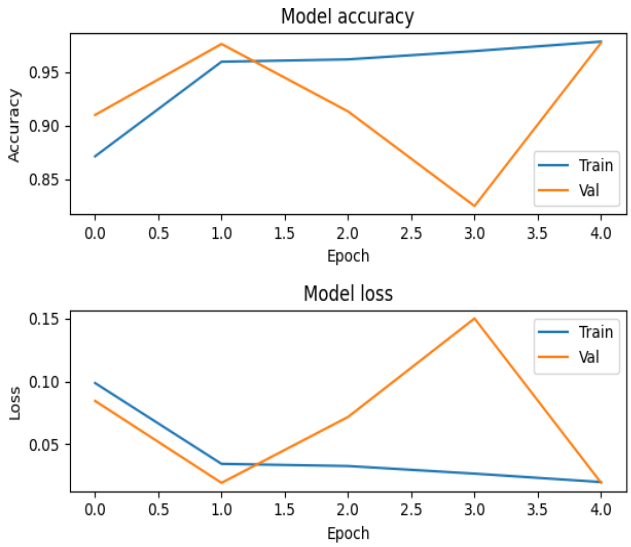


Рис. 7. Графік тестового навчання моделі нейронної мережі [1]

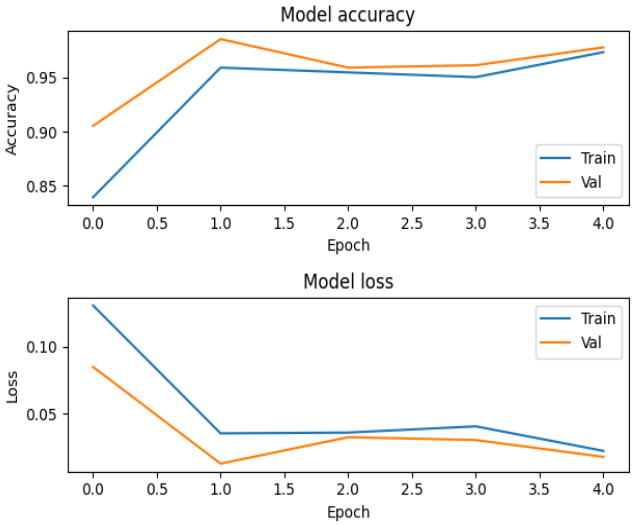


Рис.8. Графік тестового навчання модифікованої моделі нейронної мережі

При більшому розмірі набору даних, а саме – 11780 зображень, при швидкості навчання рівної 0.001 та 30 епохах у модифікованій моделі найкращий результат було отримано на 28-й епосі. Результат навчання моделі можна побачити у таблиці 1, а графік навчання на рис 9.

Таблиця 1

Результат навчання моделі модифікованої моделі нейронної мережі

loss	2,44%
acc	96,89%
val_loss	7,34%
val_acc	91,17%

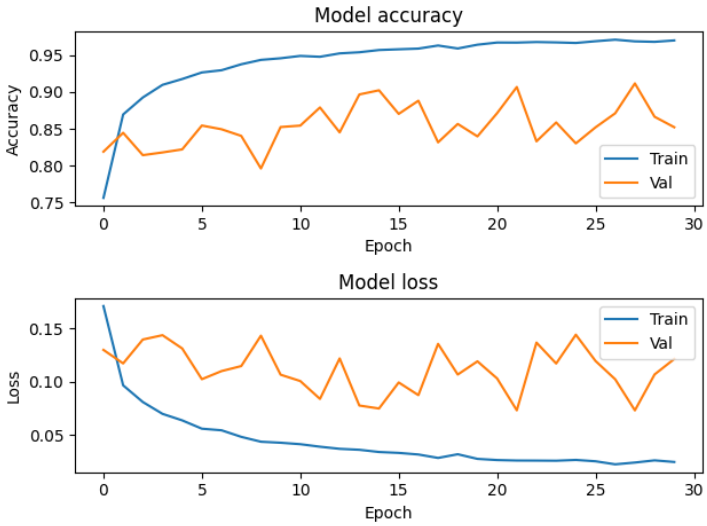


Рис.9. Графік тестового навчання модифікованої моделі нейронної мережі

Точність класифікації створеної моделі є 91,17%, що є досить великим показником, але крім того, завдяки модифікації набору даних вдалося підвищити точність класифікації зображень, які не входять до використаного для навчання моделі набору даних.

Висновки. В роботі представлено алгоритм детектування Deepfake за допомогою згорткової нейронної мережі. Точність класифікації створеної моделі є 91,17%, що є досить великим показником, але крім того, завдяки модифікації набору даних вдалося підвищити точність класифікації зображень, які не входять до використаного для

тестування моделі набору даних. Предметом подальшого розвитку даної роботи є вдосконалення нейромережі за рахунок збільшення набору даних для навчання.

Список літератури

1. Generative Adversarial Networks. URL: https://arxiv.org/abs/1406.2661
2. MNIST URL: https://paperswithcode.com/dataset/mnist.
3. Holländer B. (2020) Autoencoders: Overview of Research and Applications. URL: https://towardsdatascience.com/autoencoders-overview-of-research-and-applications-86135f7c0d35 ?gi=1b7b6132aae
4. Li Y., Chang M.C., Lyu S. In Ictu Oculi: Exposing AI Generated Fake Face Videos by Detecting Eye Blinking. *IEEE International Workshop on Information Forensics and Security (WIFS)*. 2018. P. 1-7.
5. Ciftci U.A., Demir I., Yin, L. How Do the Hearts of Deep Fakes Beat? Deep Fake Source Detection via Interpreting Residuals with Biological Signals. *IEEE International Joint Conference on Biometrics (IJCB)*, 2020, P.1-10.
6. Lima O., Franklin S., Basu S., Karwoski B., George A. Deepfake Detection Using Spatiotemporal Convolutional Networks. 2020. URL: https://www.researchgate.net/publication/342520585_Deepfake_Detection_using_Spatiotemporal_Convolutional_Networks
7. Zhu J.Y., Park T., Isola P., Efros A.A. (2017) Unpaired Image-to-Image Translation Using Cycle-Consistent Adversarial Networks. *IEEE International Conference on Computer Vision*. 2017, P. 2223-2232.
8. Bansal A., Ma S., Ramanan D., Sheikh Y. (2018) Recycle-GAN: Unsupervised Video Retargeting. *European Conference on Computer Vision*. 2018. P.119-135.
9. Sabir E., Cheng J., Jaiswal A., AbdAlmageed W., Masi I., Natarajan P. Recurrent Convolutional Strategies for Face Manipulation Detection in Videos. *CVPR Workshops*. 2019
10. Afchar D et al. Mesonet: a compact facial video forgery detection network. URL: https://arxiv.org/abs/1809.00888
11. Функції активації нейромережі URL: https://neurohive.io/ru/osnovy-data-science/activation-functions/
12. Clevert D.A, Unterthiner T., Hochreiter S. (). Fast and Accurate Deep Network Learning by Exponential Linear Units (ELUs). 2015. URL: https://doi.org/10.48550/arXiv.1511.07289
13. Maas A.L. Rectifier Nonlinearities Improve Neural Network Acoustic Models. 2013. URL: https://ai.stanford.edu/~amaas/papers/relu_hybrid_icml2013_final.pdf
14. Оссовский С. Нейронные сети для обработки информации. М.: Финансы и статистика, 2002. 344 с.
15. Реалізація та порівняння оптимізаторів моделей у глибокому навчанні URL: https://habr.com/ru/company/skillfactory/blog/525214/

DETECTION OF PHOTO FORGERY PERFORMED BY TOOLS OF NEURAL NETWORKS

V.V. Zorilo, E.V. Timofeev

1, Shevchenko Ave., National Odessa Polytechnic University, 65044, Odesa Ukraine
vikazorilo@gmail.com, timofeevzhenya2107@gmail.com

Deep learning is an effective and useful technique that is widely used in a variety of fields, including computer vision, machine vision, and natural language processing. Deepfake uses deep learning technology to manipulate images and videos of a person that people cannot distinguish from real ones. Deepfake is usually created in two ways. The first way is through a generative competition network, or GAN, which uses two separate neural networks that work together to learn how to study the characteristics of real images so that they can create compelling photo fakes. The second way is with an artificial intelligence (AI) algorithm called an encoder, which works by running pictures of two people's faces through an encoder to find similarities between those pictures and running a decoder that takes a face image and swaps them. The achievements in the field of Deepfake are equally impressive and disturbing. In someone else's hands, this technology can be used to spread misinformation and undermine public confidence almost as a sci-fi type of identity theft, when you can get anyone to say anything. In this regard, it can be stated that the task of Deepfake detection is very important and requires the application of new research in this area, the development of new algorithms for Deepfake detection and improvement of existing methods. Therefore, the purpose of this work is to create a system for detecting violations of the integrity of media files made by Deepfake technology. The work selected the neural network and its training on a specially created basis, which made it possible to detect Deepfake in both digital images and digital videos.
Keywords: deepfake, detection of falsifications, digital criminal science, neural network.

DOI 10.15276/imms.v12.no1-2.65
УДК 681.5.015:004.681

Informatics and Mathematical Methods in Simulation
Vol. 12 (2022), No. 1-2, pp. 65-72

МІНІМІЗАЦІЯ ПОМИЛОК ПРИ ФУНКЦІОНУВАННІ У СИСТЕМАХ УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ

М.В. Капустян[1], В.А. Кудінов[2], В.О.Хорошко[3]

[1]Хмельницький національний університет, вул. Інститутська, 11, Хмельницький, 29000, Україна; email: kapustian.mariia@gmail.com

[2]Національна академія внутрішніх справ, пл. Солом'янська, 1, Київ-ДСП, 03035, Україна; e-mail: kudinov_va@ukr.net

[3]Національний авіаційний університет, просп. Любомира Гузера, 1, Київ, 03058, Україна; e-mail: professor_va@ukr.net

У статті розглянуто властивості векторної цільової функції для мінімізації інтегрованої квадратичної оцінки помилки системи управління кіберзахистом. На відміну від традиційного завдання функції інтегральних квадратичних оцінок (ІКО) тільки в області стійких систем управління, пропонована векторна цільова функція визначається в усьому просторі варійованих параметрів. Запропоновано покроковий підхід встановлення достатньої кількості обмежень для переходу в область визначення ІКО і раціональний механізм його реалізації у вигляді пріоритетної оптимізації векторної цільової функції з використанням операції порівняння її значень. Розроблено алгоритми модифікованих методів Хука-Дживса і Нелдера-Міда для оптимізації векторних функцій. Основна відмінність запропонованих модифікованих методів оптимізації векторних функцій від методів мінімізації скалярних функцій полягає у використанні бінарних операцій порівняння значень векторних функцій. Застосування методів оптимізації векторної цільової функції дозволяє в єдиному обчислювальному процесі перейти з будь-якої початкової точки пошуку допустимих параметрів системи управління кіберзахистом інформаційних ресурсів в область стійкості системи управління і знайти в ній мінімум ІКО.

Ключові слова: інтегральні квадратичні оцінки (ІКО), оптимізація векторної цільової функції, системи управління кіберзахистом, стійкі системи управління.

Вступ

Управління кібербезпекою є невід'ємною частиною управління будь-якою системою чи об'єктом, оскільки для них інформація стала таким самим ресурсом, як матеріальні, фінансові, трудові та інші ресурси. Тому до управління кібербезпекою використовуються процесний, системний та ситуаційний підходи, як і до будь-якої іншої системи управління. Однак, як з'ясувалося, особливості самої інформації та інформаційних технологій потребують зовсім інших методів, засобів і заходів для їх захисту. Отже управління кібербезпекою є тією сферою, необхідність теоретичного та практичного вивчення якої стала очевидною. Перші дослідження в цій області почалися наприкінці 1980-х рр., а до кінця 1990-х рр. з'явилися перші національні й міжнародні стандарти (ISO/IEC 17799). Однак стандарти в області управління кібербезпекою не вирішують усіх проблем. Навпаки, завдання управління кібербезпекою ускладнюються разом із усе більш інтенсивним використанням інформаційних комп'ютерних технологій практично в усіх сферах людської діяльності. Це обумовлює необхідність узагальнення досвіду управління кібербезпекою, розробки теорії, вирішення практичних аспектів управління кібербезпекою.

Необхідно відзначити й те, що лише кілька років назад, говорячи про управління кібербезпекою, мали на увазі лише рівень великої організації. Останнім часом усе частіше мова йде про управління безпекою регіональних і національних інформаційних

інфраструктур, усе частіше виникає потреба в забезпеченні та управлінні кібербезпекою на середніх, малих підприємствах та в некомерційних організаціях.

Таким чином, забезпечення інформаційної безпеки є необхідною умовою функціонування будь-якої компанії, а створення політики безпеки - одна з перших вимог до організації інформаційної безпеки підприємства.

У зв'язку з розширенням сфери використання інформаційних систем й їхнього ускладнення, проблема забезпечення інформаційної безпеки загострюється. Безпеку вже неможливо забезпечити одним лише набором технічних засобів і підтримувати тільки силами підрозділу безпеки. Відсутність регулярної оцінки інформаційних ризиків, недостатня інформованість співробітників про правила роботи із інформацією, що захищається, і дотриманні режиму інформаційної безпеки, відсутність формалізованої класифікації інформації зі ступеня її критичності й уявлень про те, скільки коштують інформаційні активи, - все це може звести нанівець зусилля компанії по забезпеченню інформаційної безпеки. З підвищенням ролі інформаційних систем у підтримці основних бізнесів-процесів компанії до цих проблем додаються питання забезпечення безперервності функціонування бізнесу в критичних ситуаціях. Ігнорування проблем інформаційної безпеки, практика "латанія дір" сьогодні можуть обійтися компанії дуже дорого. Вирішити ці питання можна шляхом побудови ефективної системи управління кібербезпекою (СУКБ).

Завданнями СУКБ є систематизація процесів забезпечення ІБ, розміщення пріоритетів компанії в області ІБ, досягнення адекватності системи інформаційної безпеки існуючим ризикам, досягнення її "прозорості". Останнє особливо важливо, тому що дозволяє чітко визначити, як взаємозалежні процеси й підсистеми інформаційної безпеки, хто за них відповідає, які фінансові й людські ресурси необхідні для їхнього забезпечення й т.д. Створення СУКБ дозволяє також забезпечити ефективне відстеження змін, внесених у систему інформаційної безпеки, відслідковувати процеси вироблення та виконання політики безпеки, ефективно управляти системою в критичних ситуаціях.

У цілому, процес управління безпекою відповідає за планування, виконання, контроль і технічне обслуговування всієї інфраструктури безпеки. Організація цього процесу ускладнюється також тією обставиною, що забезпечення інформаційної безпеки пов'язане з виникненням помилок як не навмисних, так і навмисних, які впливають на захищеність інформаційних ресурсів. Тому необхідно оцінювати ризики, які виникають при експлуатації систем управління та мінімізувати їх.

У світовій практиці є розроблені моделі систем управління ІБ, наприклад, "Information Security Management Maturity Model" (ISM3 від ISECOM) або "The Systems Security Engineering Capability Maturity Model" або стандарт NIST SP800-33. Існує також ряд міжнародних стандартів. Однак пряме використання цих моделей і стандартів утруднене. Вони або занадто конкретизовані, а в будь-якій організації, як правило, уже існує певна система процесів, ролей, організаційно-розпорядницьких документів інформаційної безпекою, які необхідно інтегрувати в систему управління кібербезпекою. При цьому не визначаються пріоритети, так званої "ваги директив", які звичайно застосовуються в стандартах аудита. Або, навпаки, рекомендації носять занадто загальний характер. Наприклад, стандарти містять або набір контрольних директив, або загальний підхід до систем менеджменту, тобто визначають, що потрібно зробити, але не визначають, як це зробити.

Завдання визначення оптимальних показників якості систем управління кіберзахистом інформаційних ресурсів автоматизованих систем є однією з найважливіших проблем проектування комплексних систем захисту інформації. Це зумовлено складністю подібних систем, наявністю безлічі варійованих параметрів, складністю обчислення показників якості. Такі показники задаються у вигляді інтегральних квадратичних оцінок (ІКО) помилки системи управління захистом [1]. Проблема полягає в тому, що існуючі чисельні методи їх мінімізації такі, як методи Хука-Дживса і Нелдера-Міда [3; 8-10],

орієнтовані на єдиний (скалярний) параметр, що впливає на ІКО, тоді як в реальних системах таких параметрів може бути декілька і в сукупності вони утворюють векторний параметр. Здійснювати оптимізацію одночасно за всіма параметрами дуже складно, тому перспективним вважається покроковий підхід [6; 11], коли оптимізація виконується послідовно за параметрами. При цьому повинні неухильно задовольнятися обмеження на стійкість системи шляхом оптимізації векторної цільової функції, алгоритми обчислення якої розроблені в частині 1 статті [1].

Метою роботи є розробка методів покрокового підходу до мінімізації інтегральної квадратичної оцінки помилки системи управління кіберзахистом з областю визначення, обмеженій умовами стійкості.

Основна частина

Нехай передавальна функція системи управління залежить від вектору варійованих параметрів $x \in R^p$:

$$w(x,s)=\frac{\beta(x,s)}{\alpha(x,s)};\ \alpha(x,s)=\sum_{i=0}^{n}\alpha_i(x)s^{n-i};\ \beta(x,s)=\sum_{i=0}^{m}\beta_i(x)s^{m-i};\ \alpha_n=\beta_m. \quad (1)$$

Їй відповідає перехідна функція $y(x,t): y(x,0)=0;\ y(x,\infty)=1$. Похибка управління визначається як зважена сума відхилення $z(x,t)=y(x,\infty)-y(x,t)$ та її похідних $z_t^{(k)}(x,t)$:

$$e(x,t)=\sum_{k=o}^{l} w_k \cdot z_t^{(l-k)}(x,t), \quad (2)$$

де $w_k, k=\overline{0,l};\ l\le n-m;\ w_0=1$ – вагові коефіцієнти.

Як показано в [11], інтегральна квадратична оцінка (ІКО) похибки управління системою обчислюється за формулою:

$$I(x)=\frac{1}{2\pi j}\int_{-j\infty}^{j\infty}\frac{\delta(x,s)\cdot\delta(x,-s)}{\alpha(x,s)\cdot\alpha(x,-s)}\,ds, \quad (3)$$

де $\delta(x,s)=\left[\alpha(x,s)-\beta(x,s)\cdot w(s)\right]/s;\ w(s)=\sum_{k=0}^{l} w_k\cdot s^{l-k}$.

ІКО визначається в області стійкості $D\subset R^p$, яка з використанням елементів першого стовпця визначника Рауса $\rho_k=\alpha_k^k,\ k=\overline{0,n}$, задається умовами

$$\alpha_i(x)>0,\ i=\overline{0,n};\ \rho_k(x)>0,\ k=\overline{2,n-1}. \quad (4)$$

Цим нерівностям відповідають області виконання обмежень

$$\Omega_1=\left\{x\middle|\alpha_i(x)>0,\ i=\overline{0,n}\right\};\ \Omega_k=\left\{x\middle|\rho_k(x)>0\right\},\ k=\overline{2,n-1}. \quad (5)$$

Складемо з них систему квазідопустимих областей $D_1=\Omega_1,\ D_k=D_{k-1}\bigcap\Omega_k,\ k=\overline{2,n-1}$, з яких за допомогою різниць множин побудуємо області рівнів обмежень

$$H_0=R^p\setminus D_1;\ H_k=D_k\setminus D_{k+1},\ k=\overline{1,n-1};\ H_{n-1}=D_{n-1}. \quad (6)$$

Ступінь порушення першої групи нерівностей (відповідно до [1]) зобразимо штрафною функцією

$$P(x)=\sum_{i=0}^{n}\max\left\{-\alpha_i(x),0\right\}. \quad (7)$$

Для оцінки ступеня порушення усіх умов стійкості системи управління в [11] сформована векторна цільова функція:

$$F(x)=\begin{cases}(0;P(x)), & x\in H_0;\\ (k;-\rho_{k+1}(x)), & x\in H_k,\ k=\overline{1,n-2};\\ (n-1;I(x)), & x\in H_{n-1};\end{cases} \quad (8)$$

і розроблений алгоритм її обчислення. Властивості цієї функції зумовлені властивостями областей D_k, які утворюють систему вкладених областей: $D_{n-1} \subseteq D_{n-2} \subseteq \ldots \subseteq D_1 \subseteq R^p$. Оскільки $D_k \subset \Omega_j$, $j = \overline{1,k}$, то чим більше значення індексу квазідопустимої області k, тим більше виконано в ній умов (обґрунтовані у [1]). У області D_{n-1} мають бути виконані усі умови стійкості. Області рівнів обмежень (відповідно до [1]) мають властивості $H_k \subset D_k, k = \overline{1,n-1}; H_j \bigcap H_k = \varnothing,\ j \neq k; D = H_{n-1}$, тому області рівнів ділять увесь простір варійованих параметрів на n областей: $R^p = H_0 \bigcup H_1 \bigcup \ldots \bigcup H_{n-1}$.

Перша складова (8) – функція рівня – відображає приналежність її аргументів певної області рівня і являє собою лічильник числа виконаних обмежень, вона кусочно-постійна і може набувати значень від 0 до $n-1$. Друга складова – функція штрафу – представляє поза області стійкості штрафну функцію порушеного обмеження. У області стійкості ця складова співпадає з ІКО. Векторна функція (8) враховує особливості завдання оптимізації – ієрархію обмежень в процесі обчислення ІКО.

Розробимо покроковий підхід мінімізації ІКО за допомогою функції (8), яка враховує умови стійкості (4). Нехай $x \in H_0$, тоді в силу (6) $\exists i \in \overline{\{0,n\}}, \alpha_i(x) \leq 0$. У області H_0 мірою цього порушення обмеження є функція штрафу (42), яка убуває у напрямі межі наступної області H_1, в якій має місце нерівність $\rho_2(x) \leq 0$. Мірою цього порушення обмеження служить функція штрафу $-\rho_2(x)$, що убуває у напрямі межі області H_2 і т.д. У будь-якій непорожній області рівня $H_k, k = \overline{1,n-2}$ мірою порушення обмеження є відповідна функція штрафу $-\rho_{k+1}(x)$. Крок переходу з області H_k в область H_{k+1} полягає в мінімізації функції штрафу (8) в області H_k. При такій мінімізації чергове обмеження задовольняється, функція (8) зростає і починається наступний крок методу. Враховуючи обмежену кількість областей рівнів, перехід з будь-якої початкової точки в область стійкості виконається не більше ніж за $n-1$ кроків.

Для реалізації покрокового підходу оптимізуватимемо векторну функцію $F(x)$ з урахуванням пріоритету її складових: першу складову, що має пріоритет, необхідно максимізувати, а другу складову – мінімізувати. Завдання оптимізації векторної цільової функції (8) з урахуванням пріоритету її складових позначимо $vecopt\ F(x)$. Для визначення кращих значень векторної функції застосуємо операцію порівняння її значень. Оскільки першу проекцію векторної функції (8), що має пріоритет, необхідно збільшувати, а другу – зменшувати, то два значення векторної цільової функції $U = (U_1, U_2)$ і $V = (V_1, V_2)$ порівняємо бінарною операцією «краще» $\prec$:

$$U \prec V = \begin{cases} 1, & якщо\ (U_1 > V_1) \vee (U_1 = V_1) \wedge (U_2 < V) \\ 0, & якщо\ (U_1 < V_1) \vee (U_1 = V_1) \wedge (U_2 \geq V) \end{cases} \quad (9)$$

Сенс цієї операції полягає в тому, що при різних перших складових векторної функції (8) в двох точках кращою вважається та, в якій перша складова, що має пріоритет, набуває більшого значення. При рівних значеннях першої складової кращою вважається та точка, в якій друга складова набуває меншого значення. Операцію (9) можна реалізувати за наступним алгоритмом.

Алгоритм 1. Порівняння значень векторної функції. Вхідні параметри: U, V – значення векторної функції. Вихідний параметр: B – бульовий результат порівняння.

Крок 1. Покласти $B := 0$.

Крок 2. Якщо $U_1 > V_1$, покласти $B := 1$ і перейти до кроку 5.

Крок 3. Якщо $U_1 < V_1$, перейти до кроку 5.

Крок 4. Якщо $U_2 < V_2$, покласти $B := 1$.

Крок 5. Кінець.

Для кількісної реалізації покрокового підходу модифікуємо прямі методи безумовної мінімізації функцій (методи Хука-Дживса і Нелдера-Міда) [8-10]. Зобразимо алгоритм модифікованого методу Хука-Дживса для оптимізації векторних функцій.

Алгоритм 2. Вхідні параметри: x – початкова точка, ε – допустима погрішність, $F(x)$ – векторна функція, $R(x, F_x)$ – функція досліджуючого пошуку. Вихідні параметри: x, F_x – краща точка пошуку і значення векторної функції в ній.

Крок 1. Покласти $F_x := F(x); \delta := 2$ (δ – крок досліджуючого пошуку).

Крок 2. Якщо $\delta < \varepsilon$, перейти до кроку 10.

Крок 3. Покласти $\delta := \delta/2$.

Крок 4. Покласти $(y, F_y) := R(x, F_x)$.

Крок 5. Якщо $(F_y \prec F_x)$, перейти до кроку 2.

Крок 6. Вирахувати $z := 2y - x; F_z := F(z)$.

Крок 7. Покласти $x := y; F_x := F_y$.

Крок 8. Вирахувати $(y, F_y) := R(z, F_x)$.

Крок 9. Якщо $(F_y \prec F_x)$, перейти до кроку 6, інакше – до кроку 2.

Крок 10. Кінець.

Тут (x, F_x) – краща точка попередньої інтеграції і значення функції в ній, (y, F_y) – краща точка досліджуючого пошуку і значення функції в ній, (z, F_z) – точка пошуку за зразком і значення функції в ній. На кроці 1 обчислюється значення цільової функції в початковій точці та ініціалізується крок досліджуючого пошуку. На кроці 2 перевіряється критерій зупину. Кроки 3-9 реалізують ітераційний цикл методу. На кроці 3 зменшується крок досліджуючого пошуку, а на кроці 4 здійснюється досліджуючий пошук типу 1. На кроці 5 порівнюються значення векторної функції в кінцевій точці досліджуючого пошуку типу 1 і базовій точці. На кроці 6 виконують пошук за зразком. На кроці 7 замінюється базова точка. На кроці 8 здійснюється досліджуючий пошук типу 2. На кроці 9 порівнюються значення векторної функції в кінцевій точці досліджуючого пошуку типу 2 і в новій базовій точці. Модифікований метод Хука-Дживса відрізняється від методу мінімізації скалярної цільової функції кроками 5 і 9, на яких замість операції «менше» застосовується операція «краще» (9). Модифікований досліджуючий пошук, що реалізовує функцію $R(x, F_x)$, представимо алгоритмом.

Алгоритм 3. Вхідні параметри: (x, F_x) – базова точка, δ – крок пошуку, $F(x)$ – векторна функція. Вихідні параметри: (y, F_y) – краща точка пошуку.

Крок 1. Покласти $n := \dim x; y := x; F_y := F_x; u := y; i := 1$.

Крок 2. Вирахувати $u_i := y_i + \delta; F_u := F(u)$.

Крок 3. Якщо $(F_u \prec F_y)$, покласти $y_i := u_i; F_y := F_u$ і перейти до кроку 6.

Крок 4. Вирахувати $u_i := y_i - \delta; F_u := F(u)$.

Крок 5. Якщо $(F_u \prec F_y)$, покласти $y_i := u_i; F_y := F_u$, інакше – $u_i := y_i$.

Крок 6. Якщо $i < n$, покласти $i := i + 1$ і перейти до кроку 2.

Крок 7. Кінець.

У цьому алгоритмі n – розмірність вектору змінних, i – номер змінної. На кроці 1 ініціалізюються параметри досліджуючого пошуку. Кроки 2-6 складають ітераційний цикл методу. На кроці 2 виконується досліджуваний пошук в позитивному напрямі. На кроці 3 порівнюються значення векторної функції в поточній точці пошуку і в кращій точці. Після

невдалого пошуку в позитивному напрямі кроком 4 виконується досліджуючий пошук в негативному напрямі. На кроці 5 порівнюються значення векторної функції в поточній точці пошуку і в кращій точці. На кроці 6 перевіряється критерій зупину. Операція «краще» для значень векторної функції в цьому алгоритмі застосовується на кроках 3 і 5.

Пошук мінімуму функції методом Нелдера-Міда залежить від результату порівняння значень цільової функції в різних точках пошуку при визначенні кращої або гіршої вершини, розтягуванні або стискуванні багатогранника [6; 8-10]. Для застосування цього методу в оптимізації векторних цільових функцій порівняння значень скалярної цільової функції замінимо порівнянням значень векторних функцій (9). Модифікований метод Нелдера-Міда представимо наступним алгоритмом.

Алгоритм 4. Вхідні параметри: x – початкова точка, $F(x)$ – векторна функція, ε – допустима погрішність. Вихідні параметри: (x, F_x) – краща точка пошуку і значення векторної функції в ній.

Крок 1. Покласти $n := \dim x; m := n+1; \delta := 1; j := 1; P_m := x$.

Крок 2. Вирахувати $F_m := F(x)$.

Крок 3. Покласти $P_j := x; P_{ij} := x_j + \delta$.

Крок 4. Вирахувати $F_j := F(P_j)$.

Крок 5. Якщо $j < n$, покласти $j := j+1$ і перейти до кроку 3.

Крок 6. Якщо $\delta < \varepsilon$, перейти до кроку 29.

Крок 7. Покласти $l := m; F_x := F_m; h := m; F_w := F_m; j := 1$.

Крок 8. Якщо $F_j \prec F_x$, покласти $F_x := F_j; l := j$.

Крок 9. Якщо $F_w \prec F_j$, покласти $F_w := F_j; h := j$.

Крок 10. Якщо $j < n$, покласти $j := j+1$ і перейти до кроку 8.

Крок 11. Покласти $x := P_l; w := P_h$.

Крок 12. Вирахувати $\delta := \max\left|P_{ij} - x_i\right|$.

Крок 13. Вирахувати $c := \left(\sum_{j=1}^{m} P_j - w\right)\Big/ n$.

Крок 14. Вирахувати $y := 2c - w; F_y := F(y)$.

Крок 15. Якщо $F_y \prec F_x$, перейти до кроку 16, інакше – до кроку 19.

Крок 16. Вирахувати $z := 2y - c; F_x := F(z)$.

Крок 17. Якщо $F_z \prec F_y$, покласти $P_h := z; F_h := F_z$, інакше – $P_h := y; F_h := F_y$.

Крок 18. Перейти до кроку 6.

Крок 19. Покласти $j := 1$.

Крок 20. Якщо $j \neq h$ і $F_y \prec F_j$, покласти $P_h := y; F_h := F_y$ і перейти до кроку 6.

Крок 21. Якщо $j < m$, покласти $j := j+1$ і перейти до кроку 20.

Крок 22. Якщо $F_y \prec F_w$, покласти $w := y; F_w := F_y$.

Крок 23. Вирахувати $z := 0,5(w+c); F_z := F(z)$.

Крок 24. Якщо $F_z \prec F_w$, покласти $P_h := z; F_h := F_z$ і перейти до кроку 6.

Крок 25. Покласти $j := 1$.

Крок 26. Якщо $j \neq l$, вирахувати $P_j := 0,5(P_j + x); F_j := F(P_j)$.

Крок 27. Якщо $j < m$, покласти $j := j+1$ і перейти до кроку 26.

Крок 28. Перейти до кроку 26.

Крок 29. Кінець.

У цьому алгоритмі m означає кількість вершин багатогранника; δ – його розмір; P_j, F_j – вершина з номером j і значення векторної функції в ній; x, l, F_x – краща вершина, її індекс і значення векторної функції в ній; w, h, F_w – гірша вершина, її індекс і значення векторної функції в ній; c – центр тяжіння вершин за винятком гіршої; y і F_y – точка віддзеркалення і значення векторної функції в ній; z і F_z – точка розтягування або стискування і значення векторної функції в ній. Кроки 1 і 2 ініціалізують параметри та формують початкову вершину. Кроки 3-5 формують початковий багатогранник. Кроки 6-28 складають ітераційний цикл методу. На кроці 6 перевіряється критерій зупину. Кроки 7-11 визначають кращу і гіршу вершини. Крок 12 обчислює розмір багатогранника. На кроці 13 обчислюється центр вершин багатогранника, за винятком гіршої вершини. На кроках 14-21 виконуються віддзеркалення і розтягування багатогранника, а на кроках 22-28 – стискання і редукція багатогранника.

Висновки

1. У статті розглянуто властивості векторної цільової функції для мінімізації інтегрованої квадратичної оцінки помилки системи управління кіберзахистом. На відміну від традиційного завдання функції ІКО тільки в області стійких систем управління, пропонована векторна цільова функція визначається в усьому просторі варійованих параметрів.

2. Запропоновано покроковий підхід встановлення достатньої кількості обмежень для переходу в область визначення ІКО і раціональний механізм його реалізації у вигляді пріоритетної оптимізації векторної цільової функції з використанням операції порівняння її значень.

3. Розроблено алгоритми модифікованих методів Хука-Дживса і Нелдера-Міда для оптимізації векторних функцій. Основна відмінність запропонованих модифікованих методів оптимізації векторних функцій від методів мінімізації скалярних функцій полягає у використанні бінарних операцій порівняння значень векторних функцій.

4. Застосування методів оптимізації векторної цільової функції дозволяє в єдиному обчислювальному процесі перейти з будь-якої початкової точки пошуку допустимих параметрів системи управління кіберзахистом інформаційних ресурсів в область стійкості системи управління і знайти в ній мінімум ІКО.

Список літератури

1. Капустян М.В., Пархуць Л.Т., Хорошко В.О. Аналіз методів складання оптимальних розкладів роботи складних систем. *Інформація та математичні методи в моделюванні*. 2012. Т.2, №1, С. 467-57.

2. Лапко А.П., Крохов С.В., Ченцов С.И., Фельдман Д.А. Обучающие системы обработки информации и принятия решений. Новосибирск: Наука, 1996. 284 с.

3. Современна теория систем управления / Под ред. К.Т. Леондеса. М: Мир, 2000. 521 с.

4. Fuller A. The replacement of saturation constrains by energy constrains in control optimization theory. *International Journal of Control*. 1997. № 3. P. 201-277.

5. Головкин Б.А. Расчёт характеристик и планирования процессов. М.: Радио и связь, 2003. 274 с.

6. Кудинов В.А., Пархуць Л.Т., Хорошко В. А. Методика системного проектирования корпоративных сетей. *Вісник ДУІКТ*. 2005.Т.3. №3-4. С. 184-186.

7. Острем К. Ю. Введение в стохастическую теорию управления. М.: Мир, 1973. 322 с.

8. Химмельблау Д. Прикладное нелинейное программирование. М.: Наука, 2005. 536 с.

9. Хеллман О. Введение в теорию оптимального поиска. М.: Радио и связь, 2003. 284 с.

10. Хоменюк В. Б. Элементы теории многоцелевой оптимизации. М.: Наука, 1983. 254 с.

11. Майника Э. Алгоритмы оптимизации на сетях и графах. М.: Мир, 1981. 324 с.

MINIMIZATION OF ERRORS DURING FUNCTIONING IN CYBER SECURITY MANAGEMENT SYSTEMS

M.V. Kapustian[1], V.A. Kudinov[2], V.O. Khoroshko[3]

[1]Khmelnytskyi National University, Instytutska Str., 11, Khmelnytskyi, 29000, Ukraine; email: kapustian.mariia@gmail.com

[2]National Aviation University, Lubomir Huser Ave., 1, Kyiv, 03058, Ukraine; e-mail: professor_va@ukr.net

[3]National Academy of Internal Affairs, Solomyanska Sq., 1, Kyiv-DSP, 03035, Ukraine; e-mail: kudinov_va@ukr.net

The article considers the properties of a vector objective function to minimize the integrated quadratic error estimation of the cybersecurity management system. In contrast to the traditional task of the integral quadratic estimation (IQE) function only in the field of stable control systems, the proposed vector objective function is determined in the whole space of variable parameters. A step-by-step approach of establishing a sufficient number of constraints for the transition to the scope of IQE and a rational mechanism for its implementation in the form of priority optimization of the vector objective function using the operation of comparing its values.

Algorithms of modified Hooke-Jeeves and Nelder-Mead methods for optimization of vector functions are developed. The main difference between the proposed modified methods for optimizing vector functions from methods for minimizing scalar functions is the use of binary operations to compare the values of vector functions. The use of methods for optimizing the vector objective function allows in a single computational process to move from any starting point of search for acceptable parameters of the cybersecurity management system of information resources to the area of management system stability and find a minimum of IQE.

Keywords: integral quadratic estimation (IQE), vector objective function optimization, cybersecurity management system, stable control systems.

DOI 10.15276/imms.v12.no1-2.73
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 12 (2022), No. 1-2, pp. 73-83

АВТОМАТИЗАЦІЯ КОНФІГУРУВАННЯ БЕЗПЕЧНОГО ПІД'ЄДНАННЯ ДО КОРПОРАТИВНИХ МЕРЕЖ

П.Ю. Паталашко, Н.І. Кушніренко

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

Зі стрімким розвитком сфери інформаційних технологій виникає потреба в захисті інформації та в безпечному передаванні її через глобальну мережу. Актуальним об'єктом дослідження є проблема інформаційної безпеки, її систематизація, виявлення джерел інформаційних загроз, показників, критеріїв та стандартів. Проблема забезпечення безпеки інформації саме на стадії транспортування через мережу Інтернет має досить великий пріоритет для досліджень і створення різних підходів для її вирішення. Технологія віртуальних приватних мереж VPN була створена через потребу в об'єднанні комп'ютерних мереж між собою використовуючи безпечний канал зв'язку через мережу з меншим показником довіри. З пункту №1 в пункт №2 необхідно передати дані таким чином, щоб до них неможливо було отримати доступ третім особам, і тільки адресат, якому вони передбачалась, мав змогу їх отримати та використати. Цілком реальна і практична проблема, актуальність якої зростає з кожним роком розвитку інформаційних технологій, на яку націлена технологія віртуальних приватних мереж. Ще однією вагомою причиною для використання технології VPN є стрімкий розвиток і зростання популярності хмарних сервісів. Необхідно вирішити проблему безпечного доступу працівників та з'єднання двох або більше мереж між собою через мережу Інтернет, не збільшуючи при цьому рівень загрози у зв'язку з неминучим проходженням інформації через неї. Розроблений програмний продукт може бути рекомендований для використання на практиці при реальних потребах компаній, які використовують постачальника хмарних послуг Amazon Web Services для автоматизованої організації безпечного з'єднання з внутрішніми мережами. Також дана розробка може виступати основою для втілення аналогічних рішень, які задовольняють умови кожного користувача індивідуально, оскільки кодова база буде спільною для будь-якого постачальника.
Ключові слова: віртуальні приватні мережі, передача даних, організація безпечного з'єднання, протоколи тунелювання, хмарні сервіси, AWS.

Вступ

Зараз технологія VPN є стандартом в сфері інформаційних технологій для об'єднання декількох пунктів зв'язку між собою. В якості пунктів зв'язку можуть виступати окремі робочі станції, вузли, сегменти мереж або цілі мережі. У випадку з транспортуванням інформації між мережами, в якості безпечного рішення проблеми передачі може використовуватись виділений фізичний канал зв'язку. Але імплементація такого підходу не є тривіальною і потребує витрат на організацію та підтримку функціонування. Більш простим і дешевим рішенням є використання вже існуючих фізичних каналів зв'язку, будь то створена попередньо корпоративна мережа або мережа Інтернет. Але у той же час інформація буде направлена по логічно відділеному від решти з'єднань «тунелю», який буде створюватись лише між відправником і одержувачем. Уся інформація, що проходить через такий тунель, буде зашифрована, а відновлення до первозданного виду відбувається шляхом розшифрування на стороні отримувача.

Основними проблемами підходу зі створенням VPN-тунелю є досить важке налаштування серверу і створення та менеджмент конфігурацій клієнтів. Для коректної роботи не достатньо лише згенерувати дані для входу клієнта, але й занести відповідні записи до певних файлів серверу, перезавантажити програмну частину. Зі збільшенням клієнтів, значно збільшується і складність підтримки серверу. Враховуючи, що системному адміністратору доводиться робити усі дії вручну, це може погіршити загальну безпеку через можливість впливу людського фактору. Тому актуальним завданням є повна автоматизація усіх мануальних кроків, від створення і налаштування серверу до додавання конфігурацій клієнтів, які можуть бути використані для безпечного під'єднання по шифрованому тунелю одразу після отримання.

Мета і задачі дослідження

Метою роботи є підвищення рівню безпеки і автоматизації створення під'єднання до внутрішніх корпоративних мереж шляхом розробки спеціалізованого програмного продукту, зокрема сфокусованого на хмарних технологіях. За рахунок такого підходу підвищиться рівень безпеки і автоматизації організації з'єднання, та сильно знизяться ризики людського фактору і витрати часу при конфігуруванні власноруч. В процесі виконання даної роботи необхідно розв'язати наступні задачі:

– розглянути і проаналізувати різні підходи до організації зв'язку між сегментами мереж, визначити загрози інформації при передачі;

– провести аналіз та порівняння сучасних протоколів тунелювання;

– обрати необхідні компоненти AWS для створення серверу;

– створити схему топології мережі;

– розробити програмний продукт для повної автоматизації конфігурації VPN-серверу і клієнту.

Основна частина

Коли виникає необхідність безпечного об'єднання двох пунктів для передачі інформації по мережі, в доступності є достатньо великий вибір засобів. Все залежить від можливостей, здібностей, фінансів та наявності обладнання у компанії. Наприклад, створення фізичного каналу зв'язку власноруч можливий використовуючи наступі способи:

– Ethernet - це скручена пара. До 100 метрів. Максимум у будівлі або між сусідніми будівлями. Швидкість з'єднання 1 Гбіт/с [1].

– Wi-fi. Відстань залежить від реалізації: можливо досягти продуктивності на 40 км, використовуючи потужні спрямовані антени. В середньому до 5 км з прямим видимістю. Швидкість залежить від стандарту та використаної відстані [1].

– Оптичне волокно. 1 Гб/с (рішення для 10 та 100 ГБ/с коштуватимуть забагато при критерії "ціна - якість"). Відстань залежить від багатьох факторів: від кількох кілометрів до сотень. Потрібні координації щодо прокладання кабелю, кваліфікованого персоналу для будівництва та обслуговування [1].

Загалом, кожен випадок є індивідуальним і вимагає свого підходу. При такому способі організації з'єднання для компанії усе прозоро – використання власної окремої фізичної лінії для передачі інформації без обмежень.

Іншим варіантом є оренда каналу зв'язку у постачальника. При необхідності стабільний канал до іншого міста є найпоширенішим і надійним варіантом. Провайдер може надати можливість доєднатися до своєї точки зв'язку.

Тунель через публічну мережу – ще одне альтернативне рішення. Якщо обидва умовні вузли зв'язку мають доступ до Інтернету, найдешевший і найлегший у підтримці спосіб - побудувати тунель між цими двома точками. Для цього необхідно мати публічні адреси на обладнанні, на якому він реалізується.

Звичайно, у кожного з вищенаведених способів об’єднання є свої недоліки. Завданням є не тільки створити зв’язок між клієнтами, сегментами мереж, або забезпечити віддаленого досупу. Не менш важливим фактором для урахування при налаштуванні середи для обміну інформацією є, власне, безпека цієї самої інформації. В цьому плані ідеального рішення немає і ніколи не буде. В будь-якому моменті існування інформації вона є вразливю до різного роду атак.

В Інтернет-просторі існує велика кількість різних загроз цілісності, доступності і конфіденційності інформації. В розрізі дослідження розглядаються загрози даним в процесі передачі. Типи кібератак «Людина посередині» (MITM) відносяться до порушень кібербезпеки, які дають можливість зловмиснику підслуховувати дані, що пересилаються між двома людьми, мережами або комп’ютерами [2]. Це називається атакою «людина посередині», оскільки зловмисник розташовується «посередині» або між двома сторонами, які намагаються спілкуватися. Під час атаки MITM обидві залучені сторони відчувають, що спілкуються, як зазвичай. Але особа, яка фактично надсилає повідомлення, має можливість незаконно модифікувати повідомлення або отримати доступ до нього, перш ніж воно досягне місця призначення.

Перехоплення сесії є також поширеним способом отримання несанкціонованого доступу. Зловмисник отримує контроль сеансу спілкування між клієнтом і сервером. Комп’ютер, який використовується для атаки, замінює свою адресу Інтернет-протоколу (IP) на адресу клієнтського комп’ютера, і сервер продовжує сеанс, не підозрюючи, що спілкується зі зловмисником, а не з клієнтом [3]. Цей вид атаки ефективний, оскільки сервер використовує IP-адресу клієнта для перевірки його особистості. Якщо IP-адреса зловмисника введена на початку сеансу, сервер може не підозрювати порушення, оскільки він уже задіяний у довіреному з’єднанні.

Описані загрози конфіденційності і цілісності інформації мають прямий вплив на надійність, якість та коректне функціонування інфраструктури, що лежить в основі майже усіх сфер діяльності, включаючи освіту, банківську справу, бізнес і медицину. Будь-яка компанія обов’язково стикається з питанням передачі інформації між своїми філіалами, офісами або організації доступу для співробітників віддалено. Фізично дані в такому випадку передаються через недостовірні канали зв'язку, тому потенційний зловмисник має можливість перехопити і використовувати інформацію.

Технологія VPN (Virtual Private Network), на основі якої можливо з’єднати декілька мереж в одну, при цьому забезпечити гнучкість та одночасно високу швидкість передачі даних, а головне - безпеку при обміні інформацією [4]. Користь від VPN полягає у зниженні вартості, збільшення масштабованості та продуктивності без погіршення безпеки [5]. Технологія VPN дає змогу вирішити наступні завдання:

конфіденційність – третя особа не повинна мати можливості скопіювати дані або ознайомитися з інформацією, що передається через спільну мережу;

– автентифікація – перевірка того, чи відправник пакетів є справжнім пристроєм, а не таким, що використовується зловмисником;

– цілісність даних – перевірка, при якій з'ясовується, чи не змінювався пакет при передачі;

– пересилання недостовірної інформації – третя особа не повинна мати можливості копіювати пакети даних, надіслані справжнім відправником, а потім пересилати ці пакети, видаючи себе за справжнього відправника.

Для об’єднання декількох мереж в одну віртуальну мережу використовуються спеціальні віртуальні виділені канали. Для створення подібних з’єднань використовується механізм тунелювання. Ініціатор тунелю інкапсулює пакети локальної мережі в нові IP-пакети,

які містять в своєму заголовку адресу ініціатора тунелю та адресу точки закінчення тунелю. При отриманні подібного пакету, кінцевий користувач проводить зворотній процес розшифрування отриманого пакету.

Для того щоб досягти конфіденційності при передаванні інформації, потрібно використовувати певний алгоритм шифрування, при цьому він має буди аналогічний як для відправника, так і для отримувача, та лише вони повинні мати інформацію про те який саме використовуються алгоритм, також володіти ключем для шифрування та розшифрування трафіку. Протоколи шифрування можуть бути різними, все залежить від того який протокол тунелювання використовується.

Існує багато характеристик VPN-протоколів. Вони різняться за кількістю підтриманих алгоритмів шифрування, швидкістю з'єднання, гнучкістю налаштувань і складністю конфігурування. Згідно з дослідженням двома найпоширенішими протоколами для організації VPN являються IPsec (IP Security) та OpenVPN. Відносно нове рішення під назвою Wireguard розробляється для заміни обох попередніх протоколів, при цьому претендуючи на кращу продуктивність [6]. Дані протоколи були взяті до огляду через відкритість їх коду. IPsec і OpenVPN на даний момент є відкритими стандартами для створення VPN-рішень.

OpenVPN - протокол VPN на основі SSL, оскільки він використовує протоколи SSL і TLS для захищеного з'єднання. OpenVPN може бути налаштований для використання попередньо розділених ключів та сертифікатів. Ці функції, як правило, не доступні іншими VPN на основі SSL. Крім того, OpenVPN використовує віртуальний мережевий адаптер пристрій tun або tap як інтерфейс між програмним забезпеченням і операційною системою. Увесь трафік проходить через одне з'єднання UDP або TCP. Канал управління шифрується і захищається за допомогою SSL і TLS каналів, також дані шифруються за допомогою протоколу шифрування користувача. Стандартний протокол - UDP, порт - 1194.

Перевагами OpenVPN є простота установки конфігурації та можливість встановлення в обмежених мережах, включаючи мережі NAT. Крім того він включає в себе функції безпеки, які надають схожий рівень захищеності, як і у VPN на основі IPSec, включаючи підтримку для різних користувачів механіз аутентифікації. Повний перелік налаштувань доступний через веб-інтерфейс серверу, де можна робити усі необхідні дії.

Недоліки OpenVPN полягають у відсутності його масштабованості та залежності від встановлення клієнтського програмного забезпечення. Зокрема, драйвер інтерфейсу tap для Microsoft Windows часто викликав проблеми розгортання, коли випускалася нова версія операційної системи.

Офіційним стандартом IEEE/IETF для безпеки IP є IPSec. Офіційно зареєстровано як RFC2411. Також вбудований у стандарт IPv6. IPSec функціонує на другому і третьому рівні моделі OSI мережної мережі. IPSec включає поняття політики безпеки, що робить даний протокол надзвичайно гнучким та потужним, але при цьому важко налаштовується та налагоджується. Безпека політики дозволяє адміністратору шифрувати трафік між двома кінцевими точками на основі параметрів, таких як IP-адреса джерела та IP-адреса призначення, а також між вихідним та кінцевим портами TCP або UDP. IPSec можна налаштувати на використання попередньо розділених ключів або сертифікатів для захисту підключення VPN. Крім того, він використовує сертифікати X.509, одноразові паролі, протоколи імен користувача або пароль для аутентифікації VPN-з'єднання.

Існує два режими роботи в IPSec: тунельний режим та транспортний режим. Транспортний режим найчастіше використовується в поєднанні з тунелюванням другого рівня (L2TP). L2TP протокол виконує автентифікацію користувача. Клієнти IPSec, вбудовані в операційні системи, зазвичай використовують IPSec з L2TP. У VPN-клієнту, вбудованого у Microsoft Windows, за замовчуванням використовується протокол IPSec з L2TP, але його можна змінити.

Переваги стандарту IPSec - це його безпека, хороша підтримка з боку різних постачальників та платформ, включаючи маршрутизатори xDSL та Wi-Fi, гнучкість його налаштувань. Даний протокол став золотим стандартом для впровадження в корпоративні мережі. Програмне забезпечення IPSec входить до складу операційних систем, а також брандмауерів, маршрутизаторів.

Недоліками IPSec є складне налаштування, погана інтеграція з мережами NAT. Також багато організацій реалізували розширення до стандарту, які робить його більш складним для того, щоб з'єднати дві кінцеві точки IPSec від різних модифікованих версій протоколу.

Відносно новим VPN-протоколом, який має на меті створення простої та ефективної реалізації віртуальної приватної мережі, є Wireguard. В основі створення даного протоколу лежить ідея увібрати в себе безпеку стандарту IPsec, і зробити процес налаштування легшим, ніж OpenVPN, в той же час не втрачати швидкість роботи з'єдання. Мета дизайну - мати загальну пряму конфігурацію, схожу до SSH, тобто криптографію асиметричного ключа. Wireguard використовує найсучасніші криптографічні алгоритми, такі як:

- Curve25519 для обміну ключами;
- ChaCha20 і Poly1305 для симетричного шифрування;
- SipHash для ключів хеш-таблиць;
- BLAKE2s для функції криптографічного шифрування.

На даний момент протокол використовує лише UDP, порт за замовчуванням - 51280. WireGuard було надіслано в 2020 на перевірку для додавання в ядро Linux. Після успішного аудиту його було включено до ядра починаючи з версії 5.6 [7].

Переваги протоколу полягають у легкості налаштування як серверу, так і клієнтської частини. Він майже не має впливу на швидкість передачі інформації, при цьому використовує стійкі криптографічні алгоритми для шифрування [8]. На рис.1 приведений тест швидкості протоколів з офіційної веб-сторінки.

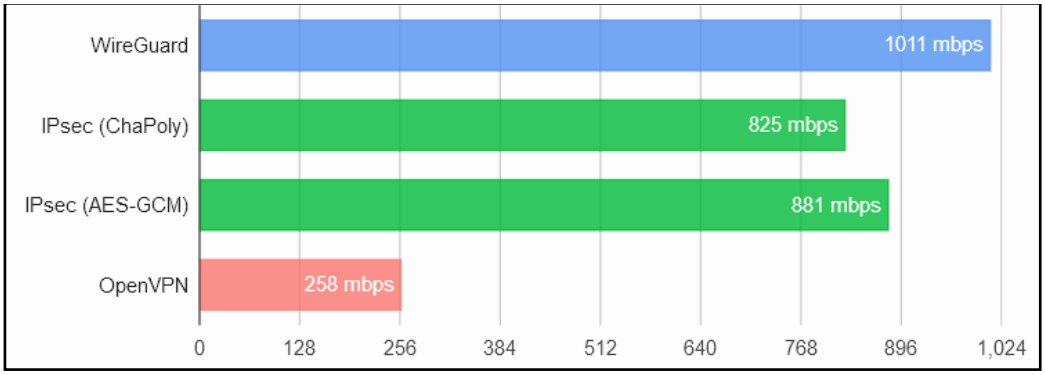


Рис.1. Порівняння швидкості роботи VPN протоколів

Основа Wireguard вміщується в 7000 рядків коду, що у порівнянні з IPsec (400000 рядків) і OpenVPN (70000 рядків), що позитивно сприяє продуктивності роботи, аудитам безпеки і зниженню «засміченості» протоколу. В Wireguard передбачений механізм "kill-switch", який полягає у припиненні пересилання трафіку через незахищену у разі переривання тунелю.

До недоліків можна віднести відсутність можливості вибору криптографічних алгоритмів, потребу встановлювати клієнтське програмне забезпечення. Також "зліпок" його заголовків легко ідентифікується, що може призвести до неможливості доступу до деяких сайтів, що блокують VPN-трафік.

У якості постачальника хмарних послуг було обрано Amazon Web Services. Виходячи зі статистики на 1 квартал 2022 року, 62% світового ринку хмарних послуг займають AWS, Microsoft Azure і Google Cloud Platform [9]. AWS в свою чергу має 33% усієї долі ринку. Тому даний провайдер є більш пріоритетною ціллю для організування до нього безпечного з'єднання.

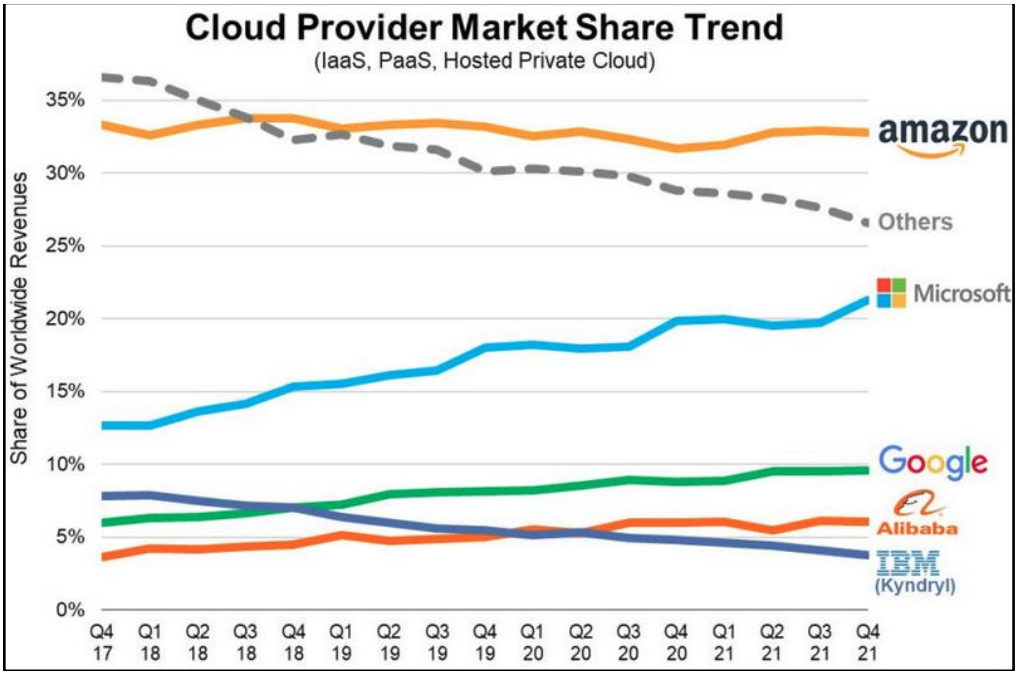


Рис.2. Світовий ринок постачальників хмарних послуг

AWS поділяється на різні сервіси: кожен може бути налаштований різними способами залежно від потреб користувача. Наразі кількість сервісів перевищує 200 одиниць. VPC (Virtual Private Cloud) – сервіс, в якому можливо створити ізольовану віртуальну приватну мережу, підмережі, резервувати IP-адреси, створювати таблиці маршрутизації трафіку ззовні та з середини мережі [10]. Підмережі бувають приватними і публічними. До приватних підмереж немає доступу з зовнішнього інтернету, до них можна отримати доступ лише з середини. Ресурси в публічних мережах доступні з будь-яких джерел. Важливо зазначити, що за замовчуванням увесь трафік в межах однієї мережі повністю дозволений, тобто між двома приватними або між публічною і приватною підмережами завжди є зв'язок без потреби додавання правил.

EC2 (Elastic Cloud Compute) - середа для створення віртуальних серверів у хмарі [10]. Вона надає можливість дуже гнучко налаштовувати і створювати обчислювальні машини. Користувач може обрати кількість процесорів, оперативну пам'ять, диск, різного роду адаптери, операційну систему і навіть задати перелік команд для виконання при створенні серверу. Опціонально можлива генерація SSH-ключа для подальшого отримання доступу до серверу для конфігурації, а також вибір віртуальної мережі та підмережі. Безпека портів серверу контролюється групами безпеки (Security groups), де можна обрати протокол, порт, список адрес, з яких доступне з'єднання до обчислювальної машини. Можливе додавання до декількох груп безпеки одночасно.

В основі спілкування AWS лежать API-виклики, за допомогою яких сервіси обмінюються інформацією один з одним. API можуть використовувати користувачі для створення і конфігурування ресурсів через командну строку, минуючи необхідність робити усе через графічний інтерфейс на веб-сторінці. Такий підхід допоможе автоматизувати і повторно

використовувати створені команди, що зменшить рівень впливання людського фактору і час на операції.

Через те, що для доступу до ресурсів AWS трафік в будь-якому випадку потрібно передавати через відкриту мережу Інтернет, необхідно вирішити проблему безпечного під'єднання до VPC. Тому для цього вирішено створити з'єднання, використовуючи протоколи тунелювання, і організувати автоматичне створення і налаштування VPN-серверу в публічній підмережі.

Корпоративний працівник, якому потрібно отримати доступ до внутрішньої приватної підмережі, повинен мати змогу зробити це без зайвих зусиль. Трафік при цьому проходить шлях від роутера користувача до його Інтернет-провайдера, далі через Інтернет, в кінці потрапляючи до мережі AWS. Після входження до мережі, згідно з правилами таблиць маршрутизації може пройти далі до VPN-серверу в публічній підмережі, при цьому обов'язковими умовами для серверу є його розташування в саме публічній підмережі, а також присвоєна йому автоматично публічна IP-адреса. Перед входом на мережевий інтерфейс VPN-серверу, спрацьовують правила груп безпеки, які перевіряють чи дозволено даному клієнту мати доступ до порту. Налаштований VPN-сервер перебуває точкою для спілкування з внутрішньою підмережею, тунель закінчується на його стороні і далі трафік може бути проксований по мережі до адресату. В приватній підмережі можуть розташовуватись як і інші сервери, так і повноцінні сервіси, такі як внутрішні веб-сторінки і FTP-хости.

Таким чином, проаналізувавши хід трафіку від користувача до приватної мережі, можна побудувати схему з'єднання з усіма необхідними пунктами. Спираючись на модель мережі на рис.3, з'являється можливість для втілення плану такої схеми в реальних умовах.

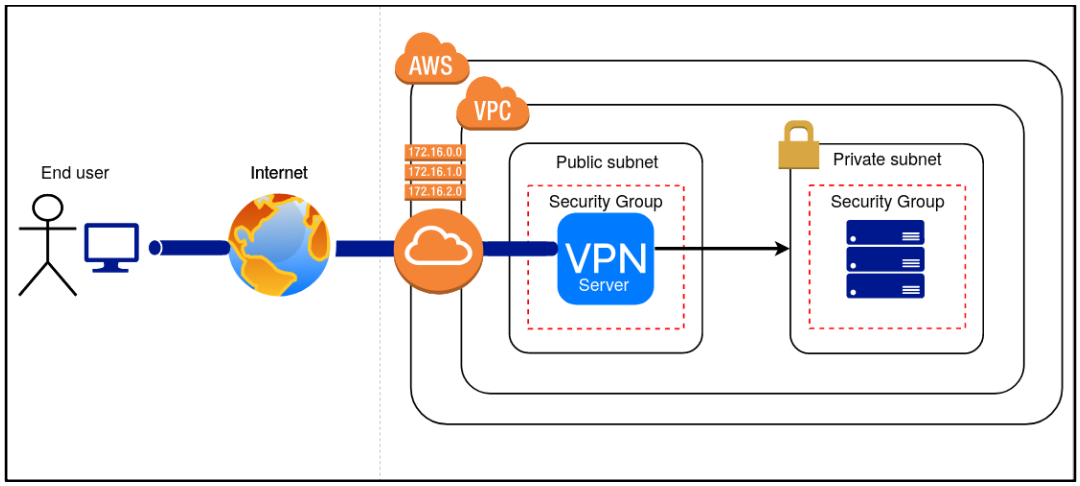


Рис.3. Схема топології мережі та з'єднання

Основною проблемою в даному випадку являється складність і витрати часу для адміністратору мережі ручного створення серверу і усіх необхідних компонентів для його роботи, а також налаштування самих VPN-протоколів на ньому. Тому було вирішено створити програмний продукт з інтерфейсом, в якому можливо, використовуючи програмний доступ до акаунту, швидко і зручно повністю розгорнути готовий VPN-сервер з можливістю створення конфігурацій для клієнта у виді логіну і паролю, або файлу налаштувань. Завдяки тому, що в коді програми вже буде готовий шаблон для серверу, досягається безпомилкове створення. Необхідні змінні параметри будуть зв'язані з інтерфейсом програми, де їх можливо редагувати. Перелік команд для конфігурації клієнта і сервера будуть занесені до окремих файлів –

скриптів, які викликаються за потребою. Також такий підхід дозволяє розбити програмний продукт на модулі, що сприяє тому, що ці скрипти можна власноруч запустити на будь-якому сервері не в мережі AWS. Тому результатом виконання даної роботи буде програмний продукт, що автоматизовано розгортає VPN-сервер в мережі AWS з ціллю підвищення безпеки, зниження витрат часу і запобігання людського фактору при створенні усього комплексу ресурсів.

Для реалізації програмного продукту була обрана мова програмування Python через її потужність і модульність. В основі задуманого програмного продукту лежить модуль під назвою “boto3”. Даний модуль був створений розробниками AWS, він включає в себе набір інструментів для розробки програм, які використовують і взаємодіють з програмним інтерфейсом AWS. Завдяки ньому можливо робити виклики, постачаючи в них повну конфігурацію сервісу або об’єкту, або ж дізнаватися інформацію з вже існуючих компонентів. Майже усе, що користувач може зробити через інтерфейс на сайті, можливо описати за допомогою коду. Передумовами для користування ним є вилучені з акаунту користувача дані для програмного доступу з відповідними правами на маніпуляції з ресурсами, AWS_ACCESS_KEY_ID та AWS_SECRET_ACCESS_KEY.

Іншим важливим компонентом для створення графічного інтерфейсу послугував модуль “tkinter”, один із популярних, простих, але дуже потужних компонентів. Він дозволяє створювати віконні додатки з різними елементами, такими як кнопки, текстові поля, надписи, повзунки, списки тощо. Для зв’язання програмної логіки з інтерфейсом, в tkinter існує концепт подій – простіше кажучи, функції, які будуть викликатися при маніпуляціях з об’єктами. Такі події закріплюються за об’єктами, обираються умови спрацювання.

Boto3 і tkinter лежать в основі розробки програмного забезпечення даної роботи. Вони вирішать проблеми з взаємодією користувача з програмою, а програми з ресурсами AWS.

В результаті роботи була створена програма, що працює за наступною логікою:

– Введення та валідація даних для доступу в AWS і їх мережу;
– Перевірка на наявність та отримання ідентифікаторів публічних підмереж;
– Вибір протоколу тунелювання через елемент RadioButton, зміна портів за необхідністю;
– Створення серверу із заданою конфігурацією;
– Після попереднього кроку, уведення та перевірка даних для користувача, з подальшим створенням конфігурації клієнту;
– Отримання виводу програми з готовими налаштуваннями для клієнту.

Інтерфейс готового програмного продукту зображений на рис.4., а результат її відпрацювання (вивід готових даних для створення тунелю) – на рис.5.

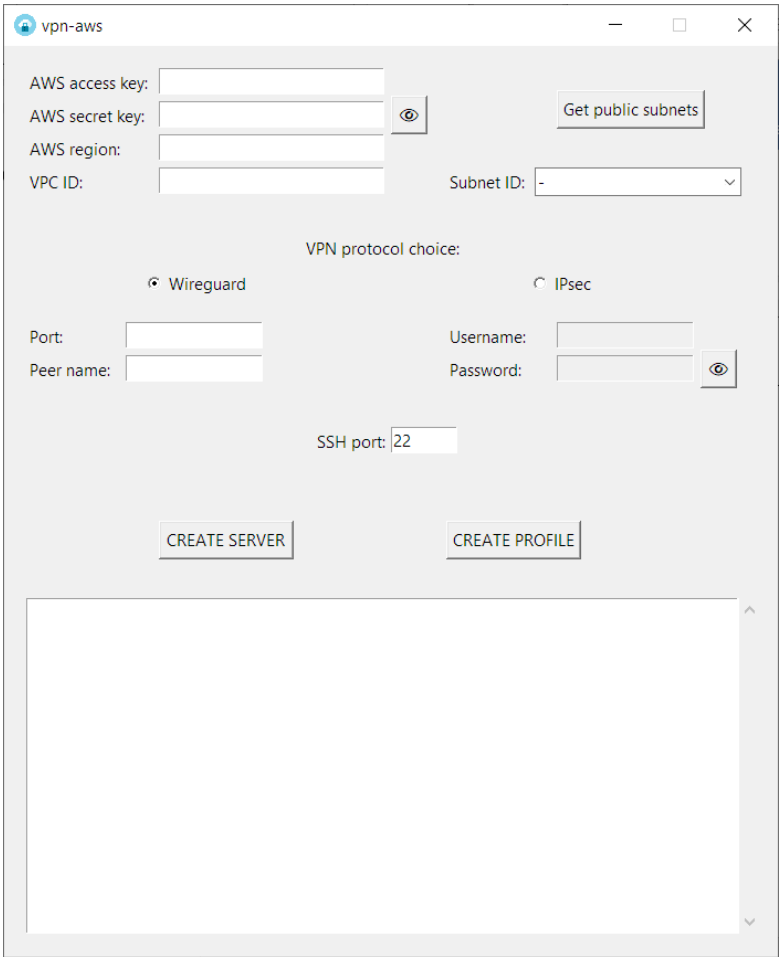


Рис.4. Інтерфейс програми

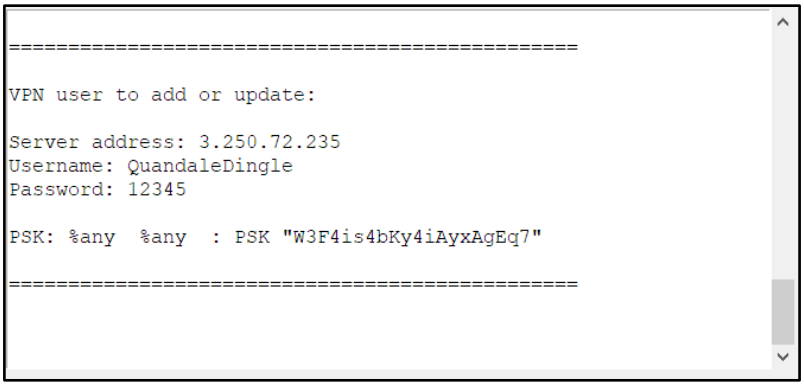


Рис.5 Приклад готової конфігурації для клієнта

Висновки

В роботі було розглянуто сучасні підходи до об’єднання сегментів мереж, їх сильні і слабкі сторони. Було виявлено найдоречніший і актуальний метод створення з’єднання через мережу Інтернет. Приведені основні загрози інформації при її передаванні. Приведений опис технології VPN, що вирішує проблему із передаванням трафіку у відкритому виді, використовуючи шифрування і інкапсуляцію.

Детально порівняно різні протоколи тунелювання для побудови VPN-з’єднання, їх сильні і слабкі сторони, при яких умовах доречніше використовувати. Було описано і

охарактеризовано постачальника хмарних послуг AWS, розібрані основні концепти і сервіси, що послугували базою для розробки. Також побудована схема топології мережі, яка описує структуру з'єднання і потоку трафіку. Повною мірою викладена проблема, і які аспекти з неї вирішить програмний продукт.

Розроблене програмне рішення, яке зменшило витрати часу при створенні усіх необхідних компонентів для організації з'єднання, а також мінімізувало помилку людського фактору, за рахунок чого підвищено безпеку клієнту і серверу. Запропонований програмний продукт має зручний інтерфейс, за допомогою якого користувач може налаштувати VPN-сервер і створити конфігурації для клієнтів, які можуть одразу бути використані для безпечного під'єднання до приватної мережі.

Для подальшого покращення програми рекомендується додати підтримку для більшої кількості хмарних постачальників і VPN-протоколів.

Список літератури

1. Організація комп'ютерних мереж. URL: https://ela.kpi.ua/bitstream/123456789/22890/1/Organizacia_komputernyh_merezh_Konspekt_lekciy.pdf

2. Тип атаки «Людина по середині». URL: https://csrc.nist.gov/glossary/term/man_in_the_middle_attack

3. OWASP Session hijacking threat. URL: https://owasp.org/www-community/attacks/Session_hijacking_attack

4. Fisli R. Secure Corporate Communications over VPN-Based WANs. Master's Thesis in Computer Science at the School of Computer Science and engineering, Royal Institute of Technology, Sweden. 2005. P.61-83

5. Khan M.T., DeBlasio J., Voelker G.M., Snoeren A.C., Kanich C., Vallina-Rodriguez N. An Empirical Analysis of the Commercial VPN Ecosystem. IMC, 2018. P.170-186

6. Donenfeld J. Next Generation Kernel Network Tunnel. WireGuard, 2018. URL: http://www.wireguard.com/papers/wireguard.pdf

7. Впровадження Wireguard до ядра Linux. URL: https://lists.zx2c4.com/pipermail/wireguard/2020-March/005220.html

8. Оцінка і порівняння роботи основних VPN-протоколів. URL: https://www.wireguard.com/performance/

9. Розподіл ринку в розрізі хмарних постачальників на 2022. URL: https://www.channele2e.com/news/cloud-market-share-amazon-aws-microsoft-azure-google/

10. Огляд найпопулярніших сервісів Amazon Web Services. URL: https://www.clickittech.com/aws/aws-services-list/

AUTOMATION OF CONFIGURATING SECURE CONNECTION TO CORPORATE NETWORKS

P. Patalashko, N. Kushnirenko

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

With the rapid development of information technology, there is a increasing need to protect information and securely transmit it over the global network. The purpose of work is the problem of information security, its systematization, identification of sources of information threats, indicators, criteria and standards. The problem of information security at the stage of transportation via the Internet has a high priority for research and the development of various solutions. Virtual private network (VPN) technology was created because of the need to connect computer networks or their segments to each other using a secure communication channel over a network with less trust. From point №1 to point №2, the data must be transmitted in such a way that it cannot be accessed by third parties and only the intended reciever has the ability to obtain and use it. Quite a real and practical problem, the relevance of which grows with each year of development of information technology, which is aimed at the technology of virtual private networks. Another important reason for using VPN technology is the rapid growth of cloud services. The problem of secure access of employees and connection of two or more networks to each other via the Internet must be solved, without increasing the level of threat due to the inevitable intersection of information through open network. The proposed software product can be recommended for use in practice with the real needs of companies that use Amazon Web Services, for automated organization of secure connection to internal networks. Also, this development can serve as a basis for the implementation of similar solutions that will satisfy the conditions of each user individually, as the code base will be same for any provider.
Keywords: virtual private networks, data transmission, organization of secure connection, tunneling protocols, cloud services, AWS.

DOI 10.15276/imms.v12.no1-2.84
УДК 681.51

Informatics and Mathematical Methods in Simulation
Vol. 12 (2022), No. 1-2, pp. 84-93

СИНТЕЗ СУБОПТИМАЛЬНОЇ СИСТЕМИ АВТОМАТИЧНОГО КЕРУВАННЯ МІНІМАЛЬНОЇ СКЛАДНОСТІ ВАКУУМНОЮ РЕКТИФІКАЦІЙНОЮ КОЛОНОЮ СПИРТОВОГО ВИРОБНИЦТВА

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

Розроблено новий метод синтезу багатовимірних систем автоматичного керування мінімальної складності з наближеним до інтегрально квадратичного критерієм оптимальності ISE, який доцільно застосовувати для синтезу систем керування ректифікаційними колонами. Метод включає розв'язок наступних задач: розробка нової форми запису багатовимірної системи в просторі станів; розробка процедури синтезу оптимального багатовимірного регулятора, який має властивість інтегрованості й зручну матричну розріджену структуру; розробка нового методу синтезу регулятора блочної структури, якість керування якого є наближеною до оптимального багатовимірного регулятора. Найбільш істотним результатом роботи є розробка ітеративного алгоритму синтезу, який базується на застосуванні процедури оптимізації за критерієм ISE. Процедура оптимізації не є ресурсовитратною, оскільки базується на застосуванні матричного рівняння Ляпунова. Розроблений метод має обмеження для всіх передаточних функцій повної матриці передаточних функцій об'єкта. Передаточні функції мають бути: стійкими; мінімально реалізованими, тобто ніякий член розкладу поліному чисельника не може бути скорочений з членом розкладу поліному знаменника, а всі моделі каналів за кожним рядком і кожним стовпцем матриці не повинні мати спільного множника в вигляді правильної передаточної функції. З застосуванням розробленого методу був проведений синтез нової системи автоматичного керування вакуумною бражною колоною спиртового виробництва брагоректифікаційної установки потужністю 6000 дал спирту на добу. Імітаційне моделювання перехідних процесів показало, що синтезована система керування дуже якісно подолала максимальне збурення – відхилення всіх виходів значно менші від допустимих.

Ключові слова: система керування, субоптимальна, блокова структура, ISE, критерій якості, оптимізація, Ляпунов, спирт, вакуумна, брагоректифікаційна установка

Вступ

Системи автоматичного керування (САК) ректифікаційними колонами (РК) як багатовимірними (MIMO) об'єктами керування можна розділити на два основних типи: децентралізовані й централізовані.

Докладно переваги й недоліки підходів до синтезу децентралізованих систем керування РК проаналізовані в роботах [1-6]. Децентралізовані САК мають мінімальну структуру, яка складається з переважно однотипних блоків з легко змінюваними параметрами. Кількість таких блоків дорівнює кількості керованих змінних. Структура децентралізованих систем в першу чергу визначається вибором каналів керування (конфігурації), який проводиться за критерієм працездатності й досягається мінімізацією перехресних впливів [3]. Може виявитись що вибору каналів керування не достатньо, наприклад в будь-якій конфігурації з можливих присутні істотні чи домінантні перехресні впливи, що призводить до нестійкості чи малого запасу стійкості. Тоді настройки регуляторів в конфігурації змінюються для збільшення запасу стійкості САК [2]. Визначимо ключову перевагу й недолік децентралізованих САК з точку зору цього дослідження. Перевагою є те, що структура децентралізованої САК спрощує впровадження й експлуатацію систем, оскільки емпірично можна виявити непрацюючий

блок й змінити його настройки. Недоліком є те, що в цілому структура обирається виходячи з ідеї працездатності і нейтралізації перехресних впливів, тому в межах такої структури і підходу взагалі майже не можливо ставити за мету синтез САК з максимальною якістю перехідних процесів (оптимальну САК).

Якщо брати класичні централізовані оптимальні регулятори, такі як регулятори стану (чи лінійно-квадратичні регулятори) з спостерігачем [7-13], то задача синтезу таких регуляторів ставиться з врахуванням всіх перехресних впливів, а не їх нейтралізації. Тому в межах такого підходу можна ставити задачу синтезу оптимальної САК. Такі регулятори мають протилежні переваги й недоліки: регулятори, які фактично представляють собою декілька матриць, заповнених числами різного порядку складні для діагностування та не є параметризованими, тобто емпірично підібрати певні числах в матрицях регуляторів таких об'єктів як РК майже не можливо, але, з іншого боку, вони є теоретично оптимальними. Також, відмітимо, для задач керування РК при синтезі таких регуляторів не можливо обійтись без спостерігача, а його застосування вимагає додаткової уваги [7, 8]

Мета роботи

Мета синтезу САК полягає у формуванні MIMO регулятора простої блочно-каскадної структури, який наближається за якістю керування до оптимального MIMO регулятора стану. При цьому, регулятор формується поблоковим синтезом, а величина покращення критерію якості при додаванні кожного блоку є відомою розробнику. Таким чином кількість необхідних блоків можна визначити в процедурі синтезу, таким чином . сформувавши регулятор мінімальної складності. Отриманий регулятор має бути зручним для впровадження в системах автоматизації, оскільки відомий порядок включення блоків та є критерії перевірки доцільності їх додавання до структури САК.

Задачі роботи

Для синтезу оптимального регулятора стану, який можливо перетворити в блочно-каскадний, треба вирішити три задачі: 1 – розробити нову форму запису багатовимірної системи в просторі станів (канонічну форму); 2 – розробити процедуру синтезу оптимального багатовимірного регулятора, який має властивість інтегрованості й зручну матричну розріджену структуру; 3 – розробити новий алгоритм синтезу регулятора блочно-каскадної структури (БКС), якість керування якого є наближеною до оптимального багатовимірного регулятора.

Розробка нової форми запису багатовимірної системи в просторів станів

Відомо, що формально перетворення з простору станів в матриці передавальних функцій (МПФ) може бути проведено за простою формулою $P(s) = C \cdot (s \cdot I - A)^{-1} \cdot B$. Зворотне перетворення – задача складніша і кількість варіантів адекватного перетворення MIMO системи майже нескінченне. Для спрощення алгоритмічної реалізації вводять структурні обмеження. Системи в просторі станів, які записані в обмеженій структурі, називають канонічними формами [14-16].

Для того, щоб чітко відокремити канали керування один від одного нам необхідно, щоб: 1) вихід кожної підсистеми знаходився на першому стані цієї підсистеми; 2) було б точно зрозуміло, які стани належать підсистемі; 3) в матриці розрахованого для системи регулятора стану повинно бути відомо, які коефіцієнти регулятора стану зв'язані виключно зі станами кожної окремої підсистеми. Відомі канонічні форми таку мету не ставили, таким чином розроблена форма є новою. Назвемо нову канонічну форму формою з зовнішніми зв'язками CFOL (Canonical Form with Outer Links). При цьому будемо розглядати лише квадратні моделі, де число входів *m* дорівнює числу виходів.

Маючи МПФ *W(s)*, з елементами $W_{i,j}(s)$, відповідні системи в просторі станів позначимо $S(A,B,C)$ та $S_{i,j} = S\left(A_{i,j}, B_{i,j}, C_{i,j}\right)$. Система є в CFOL, якщо

$$A=\bigoplus_{i=1}^{m}A_i;\ A_i=\bigoplus_{j=1}^{m}A_{i,j};\ B=\bigoplus_{i=1}^{m}B_i;\ C_j=\bigoplus_{i=1}^{m}C_{i,j};$$

$$B_i=\begin{bmatrix}B_{i,1}\\B_{i,2}\\\cdots\\B_{i,L}\end{bmatrix};\quad C=[C_1,C_2,\ldots,C_m];\ A\in\mathfrak{R}^{n,n};\ B\in\mathfrak{R}^{n\times m};\ A_{i,j}\in\mathfrak{R}^{n_{i,j}\times n_{i,j}};\ A_i\in\mathfrak{R}^{n_i\times n_i};\ C\in\mathfrak{R}^{m\times n};\ C_i\in\mathfrak{R}^{n_i};\ C_{i,j}\in\mathfrak{R}^{n_{i,j}}.\tag{1}$$

Зручно позначити $S=\bigoplus_{i=1}^{m}S_i;\ S_i=\bigoplus_{j=1}^{m}S_{i,j}$, де знак $\bigoplus_{j=1}^{m}$ означає розстановку елементів по діагоналі.

Для нашого використання система у вигляді CFOL має відповідати додатковим умовам: 1) МПФ є стійкою; 2) усі $W_{i,j}(s)$ є мінімально реалізованими, тобто ніякий член розкладу поліному чисельника не може бути скорочений з членом розкладу поліному знаменника; 3) всі $W_{i,j}(s)$ за рядками та стовпцями МПФ не мають спільного множника в вигляді передаточної функції. Приведені обмеження для опису моделей РК не є суттєвими. У випадку невиконання третьої умови можливо незначно змінити корені поліному знаменників $W_{i,j}(s)$, що не має дуже впливати на якість роботи системи керування, при умові що процедура її синтезу враховує факт значної неточності будь-якої експериментальної моделі РК. Для того, щоб перетворити стійку $W_{i,j}(s)$ в систему $S_{i,j}$ можна використати пакет Matlab.

Розробка нової процедури синтезу оптимального багатовимірного регулятора.

Регулятор стану K може бути синтезованим для системи S, заданій в CFOL, як у цілому (див. формулу 1), так і бути сформованим з регуляторів станів $K_{i,j}$ для систем $S_{i,j}$. В обох випадках результат має бути ідентичним.

Можливість такого формування можна математично обґрунтувати наступним чином.

Нехай задані $R=\bigoplus_{i=1}^{m}R_i;\ Q=\bigoplus_{i=1}^{m}Q_i;\ \mathrm{R}_i\in\mathfrak{R}_+;\ \mathrm{Q}_i\in\mathfrak{R}_+^{n}.$

Тоді

$K=\bigoplus^{m}K_i;\ K_i=lqr(A_i,B_i,Q_i,R_i)$. Враховуючи, що $(A\oplus B)^T=A^T\oplus B^T$, підставимо в рівняння, яке визначає розв'язок, вихідні матриці. Тоді

$$\left[\bigoplus_{i=1}^{m}\bigoplus_{j=1}^{L}A^T{}_{i,j}\right]\cdot P+P\left[\bigoplus_{i=1}^{m}\bigoplus_{j=1}^{L}A_{i,j}\right]+\bigoplus_{i=1}^{m}Q-P\cdot\left[\bigoplus_{i=1}^{m}B_i\right]\cdot\left[\bigoplus_{i=1}^{m}R\right]^{-1}\cdot\left[\bigoplus_{i=1}^{m}B_i\right]^T\cdot P=0$$

Але $\left[\bigoplus_{i=1}^{m}B_i\right]\cdot\left[\bigoplus_{i=1}^{m}R_i\right]^{-1}\cdot\left[\bigoplus_{i=1}^{m}B_i\right]^T=\bigoplus_{i=1}^{m}B_i\cdot R_i^{-1}\cdot B_i;\quad\left[\bigoplus_{i=1}^{m}R_i\right]^{-1}=\bigoplus_{i=1}^{m}R_i^{-1}.$

Прийнявши $P=\bigoplus_{i=1}^{m}P_i$ отримаємо m незалежних рівнянь Ріккаті відносно P_i

$$A_i^T\cdot P_i+P_i\cdot A_i+Q_i-P_i\cdot B_i\cdot R_i^{-1}\cdot B_i^T\cdot P_i=0.$$

Тоді $K=R^{-1}\cdot B^T\cdot P=\bigoplus_{i=1}^{m}R_i^{-1}\cdot B_i^T\cdot P_i=\bigoplus_{i=1}^{m}K_i$ чи $K_i=R_i^{-1}\cdot B_i^T\cdot P_i.$

Перевіримо задану властивість за допомогою Matlab.

Перетворимо МПФ об'єкта в простір станів

$$\mathrm{P}=\begin{bmatrix} \dfrac{1}{5\cdot s+1} & \dfrac{1.2}{6\cdot s+1} \\ \dfrac{1}{8\cdot s+1} & \dfrac{0.8}{9\cdot s+1} \end{bmatrix} \Rightarrow \begin{array}{l} S_{1,1}(A_{1,1},B_{1,1},C_{1,1})=ss(-0.2,0.2,1,0); \\ S_{2,1}(A_{2,1},B_{2,1},C_{2,1})=ss(-0.125,0.125,1,0); \\ S_{1,2}(A_{1,2},B_{1,2},C_{1,2})=ss(-0.1667,0.2,1,0); \\ S_{2,2}(A_{2,2},B_{2,2},C_{2,2})=ss(-0.1111,0.0889,1,0). \end{array} \quad (2)$$

$$A=\begin{bmatrix} -0.2000 & 0 & 0 & 0 \\ 0 & -0.1250 & 0 & 0 \\ 0 & 0 & -0.1667 & 0 \\ 0 & 0 & 0 & -0.1111 \end{bmatrix},\ B=\begin{bmatrix} 0.2000 & 0 \\ 0.1250 & 0 \\ 0 & 0.2000 \\ 0 & 0.0889 \end{bmatrix},C=\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \quad (3)$$

Задавшись ваговими матрицями $Q=diag([5,1,1,10])$, $R=I$ синтезуємо ЛКР в Matlab за допомогою функції lqr для моделі (3) і в результаті отримаємо матрицю

$$K=\begin{bmatrix} 1.3937e{+}00 & 2.5206e{-}01 & -1.4749e{-}17 & 3.5165e{-}17 \\ 1.4203e{-}16 & -4.0134e{-}16 & 3.2811e{-}01 & 1.9744e{+}00 \end{bmatrix}.$$

Якщо ж розрахувати регулятор стану для кожної підсистеми (2) і об'єднати їх в єдину систему за приведеними вище правилами, то отримаємо більш точну і зручну матрицю

$$K=\begin{bmatrix} 1.3937 & 0.2521 & 0 & 0 \\ 0 & 0 & 0.3281 & 1.9744 \end{bmatrix} \quad (4)$$

яка підтверджує математичне обґрунтування. Підкреслимо, що матриця Q в приведеному вище математичному обґрунтуванні передбачається лише діагональною. Необхідність встановлення вагових коефіцієнтів саме на стани передбачає застосування моделей, одиниці виміру яких однакові чи коректне масштабовані.

Розробка нового алгоритму синтезу регулятора блоково-каскадної структури.

Алгоритм базується на застосуванні процедури оптимізації за критерієм $J=x^T\cdot Q\cdot x+u^T\cdot R\cdot u$ і не є розрахунково витратним, оскільки базується на застосуванні матричного рівняння Ляпунова виду

$$P=LP(A_{inp},Q_{inp})\rightarrow solve(A_{inp}{}^T\cdot P_{inp}+P_{inp}\cdot A_{inp}+Q_{inp}=0). \quad (5)$$

Введемо операцію розрахунку критерію

$Jcnt(A_{inp},Q_{inp}):x_o{}^T\cdot LP(A_{inp},Q_{inp})\cdot x_0$, де x_0 – початкові умови.

Умови коректності виконання операції: 1) САК є стійкою; 2) $P=LP(A_{inp},Q_{inp})$ є додатне вирзначеною матрицею; 3) результат розрахунку критерію більше 0.

Початкові умови звичайно отримуються як $B\cdot f_{\max}$, де $f_{\max}$ – вектор максимуму величин збурюючих впливів.

Для системи (3) максимум критерію J_p (для об'єкта без підключеного оптимального регулятора стану) дорівнює $J_p=Jcnt\left(A,Q\right)=0.2595$, а мінімум критерію J_c (для об'єкта з підключеним оптимальним регулятором стану) дорівнює $J_c=Jcnt\left(A-B\cdot K,Q+K^T\cdot K\right)=0.1378$.

Процедура синтезу передбачає формування двох MIMO регуляторів C_o і C_f. C_f який початково є нульовими і має містити тільки регулятор виходу з блоків. Для розглянутого прикладу (3) C_o складається за (4)

$$\{Co_{11},Co_{21},Co_{12},Co_{22}\}=\{K_{11},K_{21},K_{12},K_{22}\}=\{1.3937,\ 0.2521,\ 0.3281,\ 1.9744\}.$$

Ітеративна процедура синтезу описується алгоритмом:

1. Знайти таку підсистему регулятора C_o, яка призводить до максимального зменшення критерію якості. Зафіксувати у відповідний підсистемі номер входу u_i і виходу y_i об'єкта.

2. Додати до C_f в якості регуляторів виходу $u_i - y_i$ блок

$$\Xi_N = \frac{a_0 \cdot s + a_1}{b_0 \cdot s + 1} \tag{6}$$

де a_0, a_1, b_0 – це параметри, які визначаються процедурою оптимізації з виконанням умов коректності виконання операції розрахунку критерію якості, N – номер блоку. Блок додається при умові, що він наближає J_f (для об'єкта з регулятором C_f) до величини J_c. Після додавання блоку Ξ_N до C_f він додається також у відповідну підсистему регулятора C_o, тобто виконується $Co_{i,j} = Co_{i,j} - \Xi_N$. Формула розрахунку критерію для регулятора C_f дорівнює $J_f = Jcnt\left(A - B \cdot K, Q + C_u\right)$, де C_u має враховувати не тільки K, а й додані блоки $\Xi_{1..N}$ в формі простору станів. Якщо умова наближення не виконується чи його величина занадто мала, то виконання ітеративного циклу завершується. Зони нечутливості вхідних параметрів блоку краще задавати такими, щоб найбільш важливими був коефіцієнт a_1. У термінах прямих показників якості особливість такої оптимізації наступна: перший знайдений блок по каналу керування має амплітуду відхилень таку ж як у оптимального регулятора стану, наступні – зменшують час керування.

Опис об'єкту керування для дослідження ефективності розробленого методу

Як об'єкт керування розглянемо бражну колону (БК) вакуумної брагоректифікаційної установки (БРУВАК) потужністю 6000 дал спирту на добу з використанням розробленого методу. Особливістю установки є те, що в ній тільки БК працює під розрідженням, а її обігрів проводиться переважно вторинною парою, яка поступає з дефлегматора-випаровувача РК (річ йде про додатковий до звичайного дефлегматора апарат, який у типовій БРУ відсутній). Це так звана вакуумна установка першого типу [17]. Відомо, що такі установки зменшують використання пари на 32-35% у порівнянні з типовою БРУ [17, 18]. Крім того, перегонка бражки слабким вакуумом ~76 кПа (560-570 мм рт. ст.) при низькій температурі (біля 65°С) дозволяє отримати дистилят з вмістом ефірів, альдегідів й кислот у 5-8 разів меншим, ніж при звичайній перегонці [17, 18]. Проте у БК є і недоліки: 1) більш складне обслуговування й менша надійність вакуумних насосів; 2) більший вплив температурного режиму на ступінь сепарації від вуглекислоти; 3) підвищені вимоги до точності підтримання тиску як знизу, так й зверху вакуумного апарату. Саме до третьої проблеми, яка відноситься до задачі керування, будемо шукати розв'язок.

Повна експериментальна МПФ БК приведена в табл. 1.

Таблиця 1.

Експериментальна МПФ БК БРУВАК

№	u_1	u_2
y_1	$\frac{-7}{110 \cdot s + 1}$	$\frac{25}{40 \cdot s + 1}$
y_2	$\frac{-12}{200 \cdot s + 1}$	$\frac{20}{100 \cdot s + 1}$
y_3	$\frac{-0.15}{(110 \cdot s + 1)^2} e^{-160s}$	$\frac{0.005}{(150 \cdot s + 1)^2} e^{-80s}$

У таблиці 1 керуючі впливи: u_1 – витрата бражки (%х.в.м.), u_2 – витрата пари (%х.в.м.). Керовані змінні: y_1 – розрідження знизу (мм. вод. ст.), y_2 – розрідження зверху (мм.

вод. ст.) ,

y_3 – температура зверху (°С). Максимальні збурення, приведені до входу:

$\Delta u_{\max} = [10,10]$. Допустимі відхилення керованих змінних: $\Delta y_{\max} = [2,200,200]$.

Синтез нової системи керування БК БРУВАК

Оскільки МПФ є неквадратною, тому один з виходів для задачі оптимального керування не може бути безпосередньо задіяний; 2) динаміка каналів тиску є значно швидшою, ніж інших каналів; 3) для керування усіма параметрами об'єкта з врахуванням важливості якісного підтримання необхідного тиску необхідно застосування САК каскадної структури; 4) технологічно обґрунтованою є каскадна схема стабілізації температури зверху, впливаючи на один з тисків. Тоді для синтезу оптимального регулятор будемо використовувати МПФ

$$P = \begin{bmatrix} \dfrac{-7}{110\cdot s+1} & \dfrac{25}{40\cdot s+1} \\ \dfrac{-12}{200\cdot s+1} & \dfrac{20}{100\cdot s+1} \end{bmatrix}. \qquad (7)$$

яка переводиться у форму CFOL

$$A = \begin{bmatrix} \text{-0.00(90)} & 0 & 0 & 0 \\ 0 & \text{-0.0250} & 0 & 0 \\ 0 & 0 & \text{-0.0050} & 0 \\ 0 & 0 & 0 & \text{-0.0100} \end{bmatrix}, B = \begin{bmatrix} \text{-0.0(63)} & 0 \\ 0.6250 & 0 \\ 0 & \text{-0.0600} \\ 0 & 0.2000 \end{bmatrix}, C = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}.$$

Для визначення вагових коефіцієнтів використаємо правило Брайсона, яке найбільш адекватне для мінімальнофазових об'єктів. Ідея правила в тому, що кожен *i* діагональний елемент матриці Q дорівнює $1/Ym_i^2$, де Ym_i^2 – максимальне допустиме відхилення відповідного виходу. Аналогічно визначається діагональні елементи матриці *R*. Потім емпірично залишається визначити загальний множник матриці *Q*. Тоді

$Q = ky \cdot diag([1/200^2, 1/200^2, 1/200^2, 1/200^2]), R = 1/10^2$, де *ky*=1000.

Оптимальний ЛКР має наступний вигляд

$$K = \begin{bmatrix} \text{-0.29264181} & 1.52049751 & 0 & 0 \\ 0 & 0 & \text{-0.63398538} & 1.41419545 \end{bmatrix} \qquad (8)$$

Використовуючи алгоритм синтезу регулятора блокової структури нами були знайдено 4 блоки регулятора наступного виду

$\Xi_1[u_1 - y_2] = \text{-0.059371888306747}$

$\Xi_2[u_2 - y_1] = 0.155238499856077$

$$\Xi_3[u_2 - y_1] = \frac{a_0 \cdot s + a_1}{b_0 \cdot s + 1}$$

$a_0 = 1.243045604992952 \cdot 10^{-4}$

$a_1 = \text{-0.313709800335321}$

$a_2 = 0.429145965506400$

$$\Xi_4[u_1 - y_2] = \frac{1.05 \cdot s + 2.5}{s + 1}$$

Імітаційне моделювання перехідних процесів при імпульсному збуренні показані на рис. 1.

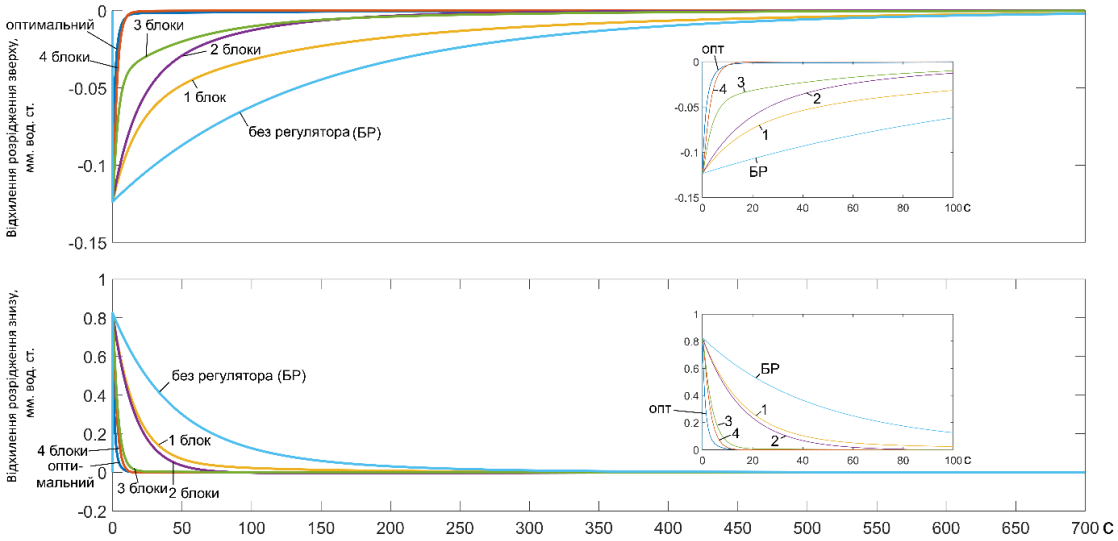


Рис.1. Результати моделювання перехідних процесів за тиском в БК при збуренні одиничним імпульсом по обом входам

Результати моделювання, показані на рис. 1 було проведено для наступних випадків:

1) без регулятора;
2) субоптимальний регулятор з одним блоком;
3) субоптимальний регулятор з двома блоками;
4) субоптимальний регулятор з трьома блоками;
5) субоптимальний регулятор з чотирма блоками;
6) з оптимальним регулятором стану.

Представлені графіки показують, що дійсно додавання кожного блоку збільшує якість керування:

САК з одним блоком має ~42 відсотки критерію об’єкту без регулятора;

САК з двома блоками має ~37% відсотки критерію об’єкту без регулятора;

САК з трьома блоками має ~10% відсотки критерію об’єкту без регулятора;

САК з чотирма блоками має ~7.5% відсотки критерію об’єкту без регулятора.

Додавання 5-го блоку вже не має сенсу, оскільки рівень покращення наближається до меж розрахункових помилок та помилок каналів вимірювання. Вихідний оптимальний регулятор має ~5%. критерію.

Останній крок – додаймо каскадний ПІ-регулятор для керування температурою зверху колони виду

$$C(s) = -27.0133570327766 - \frac{0.167792240312229}{s}.$$

Структурна схема математичної моделі САК БК БРУВАК показана на рис. 2.

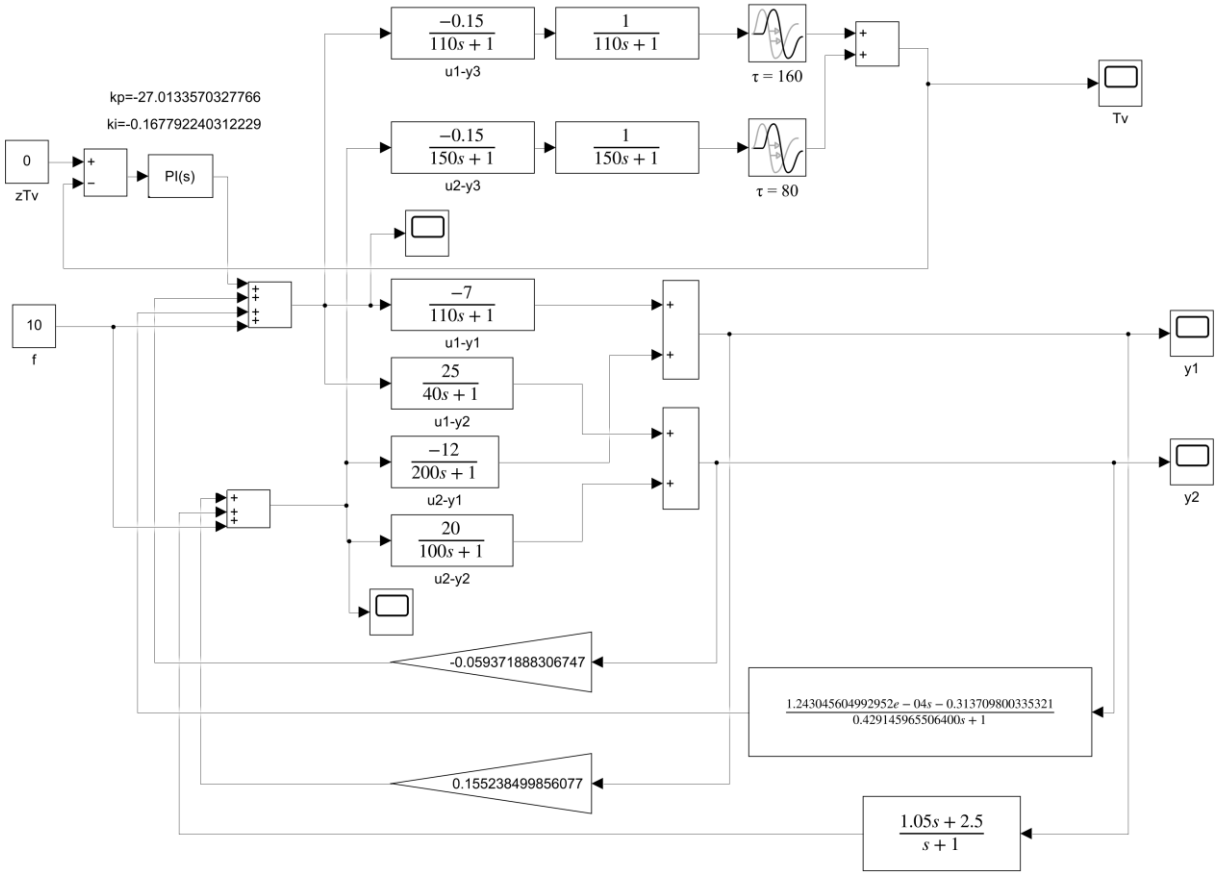


Рис.2. Структурна схема імітаційної моделі САК БК

Перехідні процеси по керуванням і вимірюванням при подачі максимального збурення стрибком 10% х.в.м. по обом входам показані на рис. 3.

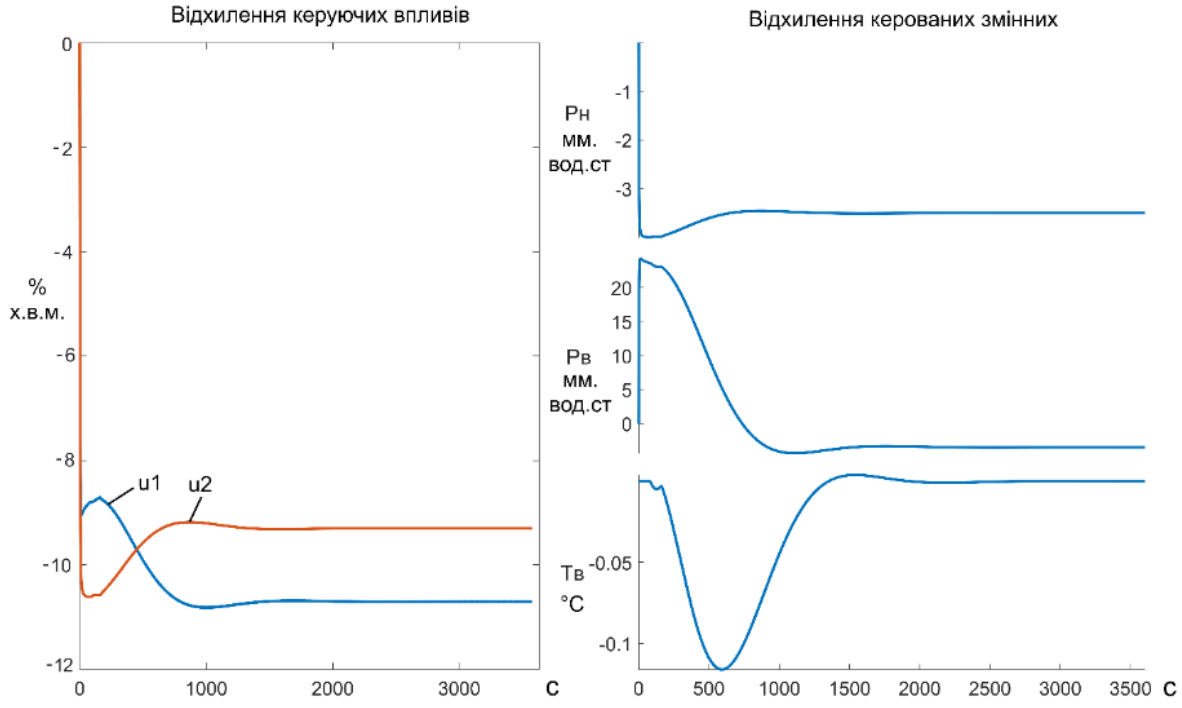


Рис.3. Перехідні процеси в САК БК

Перехідні процеси показують дуже незначне відхилення температури при максимальному відхиленню тиску зверху у 10% від максимально допустимої величини.

Висновки

1. Розроблено новий алгоритм синтезу багатовимірних субоптимальних регуляторів, які складаються з блоків та додавання кожного з яких вносить відоме покращення в сенсі інтегрального квадратичного критерію, що дуже спрощує впровадження й відлагодження САК.

2. Розроблена нова система керування промисловою вакуумною бражною колоною виробництва спирту з використанням запропонованого методу. Імітаційне моделювання перехідних процесів показує, що загалом САК дуже якісно подолала максимальне збурення – відхилення всіх виходів значно менші від допустимих.

Список літератури

1. Stopakevych A. Analysis of the major approaches to the design of multivariable decentralized control systems for distillation columns. *Eurasian scientific discussions :* proceedings of the 6th International scientific and practical conference. Barcelona, Spain: Barca Academy Publishing, 2022. P. 80-84.

2. Stopakevych A., Stopakevych O. Design of Robust Decentralized Control Systems for Distillation Columns. *Problemele Energeticii Regionale*. 2022. №2 (54). P. 38-52. https://doi.org/10.52254/1857-0070.2022.2-54.04

3. Стопакевич А.О., Стопакевич О.А. Аналітичний огляд методів розв'язування задачі синтезу децентралізованих систем керування ректифікаційними колонами *Інформатика та математичні методи в моделюванні*. 2021. Т. 11. №. 4. С. 343–356. https://doi.org/10.15276/imms.v11.no4.343

4. Sedigh A. K., Moaveni B. Control Configuration Selection for Multivariable Plants. Berlin/Heidelberg : Springer-Verlag, 2009. ISBN : 978-3642031922

5. Thone M., Potters M., Baldi S. Control configurations in distillation columns: A comparative study. *European Control Conference* : Proceedings 2016 European Control Conference. IEEE: Denmark, Aalborg. 2016. P. 37-42. https://doi.org./10.1109/ECC.2016.7810260

6 Zhu Z.-X. Variable Pairing Selection Based on Individual and Overall Interaction Measures. *Industrial & Engineering Chemistry Research*. 1996. V. 35, No 11. P. 4091–4099. https://doi.org/10.1021/ie960143n

7. Стопакевич А.О., Стопакевич О.А. Синтез та дослідження астатичних оптимальних цифрових систем керування ректифікаційною колоною. *Інформатика та математичні методи в моделюванні*. 2021. Т. 11. №. 1-2. С. 91-103. https://doi.org/10.15276/imms.v11.no1-2.91

8. Стопакевич А. А., Стопакевич А. А. Разработка робастной системы управления колонной атмосферной перегонки нефти. *Восточно-Европейский журнал передовых технологий*. 2016. Т.5, № 77. С. 49–57 . https://doi.org/10.15587/1729-4061.2015.50964

9. Stopakevych A., Stopakevych O. Development of Resilient Control Systems for Technological Plants *Problemele energeticii regionale*. 2021. №2 (50). P.114-126. https://doi.org/10.52254/1857-0070.2021.2-50.10

10. Rojas-Moreno A. Control of MIMO Time-Delay Processes Having Disturbances with Time Delays. BTSym 2021 : proceedings of the 7th Brazilian Technology Symposium. São Paulo, Brazil : Springer. P. 443-451. https://doi.org/10.1007/978-3-031-08545-1_42

11. Rojas-Moreno A. PI LQR control of MIMO time-delay processes subject to output disturbances. *International Conference on Electronics, Electrical Engineering and Computing (IEEE INTERCON)* : proceeding of XXVII conference. Lima, Peru: IEEE. 2020. P. 1–4. https://doi.org/10.1109/INTERCON50315.2020.9220212

12. Maldonado J. L. B., Valarezo J. M., Peralta D.T. Multivariable Control of a Binary Distillation Column. *International Journal of Engineering and Applied Sciences*. 2015. Vol. 2. No. 12. P.18-23. https://doi.org/10.31873/IJEAS.2.12.05

13. Kiss A. A. Advanced Distillation Technologies. Chichester, U.K.: John Wiley & Sons, 2013. ISBN: 9781119993612

14. Albertos, P., Sala A. Multivariable Control Systems: An Engineering Approach. Springer-Verlag, 2004. ISBN: 978-1-85233-738-4

15. Skogestad S., Postlethwaite I. Multivariable feedback control. Analysis and design. John Wiley & Sons, 2005. ISBN: 978-0470011683

16. Стопакевич А.А. Системный анализ и теория сложных систем. Одесса: Астропринт, 2013. 350 с. ISBN 978-966-190-760-6.

17. Цыганков П. С., Цыганков С. П. Руководство по ректификации спирта. Москва : Пищепромиздат, 2001. ISBN: 5-89703-035-9.

18. Шиян П.Л., Сосницький В.В., Олійнічук С.Т. Інноваційні технології спиртової промисловості. Теорія і практика. Київ: Асканія, 2009. ISBN: 978-966-2203-01-1.

DESIGN OF A MINIMAL COMPLEXITY SUBOPTIMAL CONTROL SYSTEM FOR THE VACUUM DISTILLATION COLUMN OF AN ALCOHOL PRODUCTION PLANT

Andrii Stopakevych, Oleksii Stopakevych

National University of Intellectual Technologies and Communications,
1, Kuznechna street, Odessa, 65029, Ukraine, stopakevich@gmail.com
National Odessa Polytechnic University,
1, Shevchenko Ave., Odessa, 65044, Ukraine, stopakevich@op.edu.ua

It is developed a new design method for multivariable control systems with the following properties: a system has minimum complexity and its performance index is close to the integral of square error ISE. The intended scope of the new method is to solve distillation column control problems. The desired aim is achieved by solving the following problems: to develop a new form of notation of multivariable systems in the state space; to develop a procedure for the design of the optimal multivariable controller, which has the property of integrity and convenient matrix sparse structure; to develop a new method for the design of the controller with the block structure, the performance index of which is close to the optimal multivariable controller. The most significant result of the work is the development of a new iterative design algorithm, which is based on the application of the optimization procedure on the base of the ISE performance index. The optimization procedure is not resource-demanding since it is based on the Lyapunov matrix equation usage. The developed method has the following restrictions for the transfer function matrix of the plant model: all channel models must be stable; all channel models must be minimally realized; all channel models by rows and columns of the matrix have no common right multiplier in the form of the transfer function. A new automatic control system for the vacuum distillation column has been synthesized. The distillation is part of the distillation unit with the capacity of 60000 liters of alcohol per day. Simulation of transients shows that the developed control system very qualitatively overcame the maximum disturbance because the deviation of all outputs is significantly less than the permissible.

Keywords. Control system, suboptimal, block structure, ISE, performance index, optimization, Lyapunov, alcohol, vacuum distillation column.

DOI 10.15276/imms.v12.no1-2.94
УДК 681.51

Informatics and Mathematical Methods in Simulation
Vol. 12 (2022), No. 1-2, pp. 94-103

УДОСКОНАЛЕННЯ СИСТЕМ РЕГУЛЮВАННЯ ВОДОГРІЙНИХ КОТЛІВ

А.М. Тігарєв[1], Т.Г. Тігарєва[2]

[1]Державний університет інтелектуальних технологій та зв'язку, 65029, Україна, Одеса, вул. Ковальська, 1; e-mail: amtigar@ukr.net
[2] Одеська державна академія будівництва та архітектури, 65029, Україна, Одеса, вул. Дідріхсона, 4; e-mail: tatianatigareva@gmail.com

Розглядається варіант удосконалення автоматичних систем керування режимом спалювання природного газу в якості палива для водогрійних котлів. Метою удосконалення є оптимізація співвідношення газ-повітря для підтримання заданої температури в приміщеннях, що опалюються, в залежності від температури довкілля. У більшості використовуваних зараз водогрійних котлів підтримка співвідношення газ/повітря здійснюється відповідно до режимних карт без урахування економічного та екологічного спалювання газу, а також без автоматичного урахування температури навколишнього середовища. Прагнення до зменшення зайвих витрат палива викликає необхідність створення таких систем автоматичного керування, які б дозволяли підтримувати необхідну температуру теплоносія на виході котла при різних температурах довкілля. Основним принципом підвищення ефективності є максимально можливе використання наявної (нижчої) теплоти згоряння $Q_н^P$. Основними складовими втрат теплоти при цьому є втрати з газами, що відходять q_2, і втрати від так званого хімічного недопалу q_3. Обидва ці показники тісно пов'язані з коефіцієнтом надлишку повітря α у факелі палаючого палива, від якого залежить і кількість шкідливих викидів в атмосферу. В роботі проаналізовано кілька видів систем регулювання співвідношення «паливо-повітря», відзначено їхні переваги та недоліки. Зроблено висновок, що найбільшого позитивного ефекту можна досягнути тільки при використанні систем безперервного автоматичного контролю й регулювання співвідношення «паливо-повітря». Запропоновано структуру системи керування, що стежить за температурою довкілля та відповідно до неї змінює температуру на виході котла. При цьому для забезпечення здатності системи працювати в значному діапазоні температур довкілля та підтримання економічного спалювання палива пропонується застосування адаптивних ПІД регуляторів на підставі табличної зміни їх налаштувань. Для забезпечення екологічного спалювання палива застосовано режим «відскоку». Проведене моделювання для однієї температури показало можливість практичного використання подобної системи в системах опалення приміщень за допомогою котлів малої потужності.

Ключові слова: водогрійний котел, регулювання температури, співвідношення газ-повітря, регулятор, режим відскоку, моделювання, концентрація CO.

Вступ

Безперервний ріст цін на усі види палива змушує до пошуку шляхів підвищення ефективності його спалювання. При цьому важливо, щоб вироблення теплової енергії у будь-який момент часу мало відповідати заданому навантаженню. Найбільше поширення для отримання теплової енергії одержало використання природного газу. Тому подальший розгляд проблеми ефективності використання палива буде присвячений лише котельним агрегатам, які працюють на газі. При спалюванні газу в атмосферу здійснюється викид шкідливих речовин, отже, крім економічної, виникає також екологічна потреба оптимального спалювання газу. Незважаючи на статус «малої» енергетики, комунальні та промислові котли займають значне місце у споживанні палива. Оптимізація режиму горіння в топках енергетичних котлів залишається актуальною. Це стосується і водогрійних котлів. Враховуючи сучасні тенденції побудови котелень малої та середньої потужності для опалення окремих багатоквартирних будинків, підприємств малої потужності та об'єктів житлово-комунального господарства (ЖКГ), удосконалення систем керування для них є актуальним. На

більшості водогрійних котлів у комунальній теплоенергетиці оптимізація спалювання газоподібного палива до сьогоднішнього дня знаходиться на рівні підтримки співвідношення газ/повітря відповідно до режимних карт без урахування економічного та екологічного спалювання газу. Також, у них не передбачено завдання автоматичного регулювання теплового навантаження опалювальних котлів відповідно до коливань температури навколишнього середовища. Тенденція до зменшення витрат палива при використанні водогрійних котлів викликає необхідність створення систем автоматичного керування, які необхідні для подальшого використання в енергоекономічних та екологічних системах з метою підтримання температури теплоносія на виході котлів при різних температурах довкілля.

Мета роботи

Метою роботи є розробка варіанта вдосконалення такої автоматичної системи, яка стежить за температурою довкілля і дозволяє забезпечити необхідну температуру води, яка подається в систему опалення, тобто на виході котла. Тому далі буде розглядатися не загальна система регулювання котельним агрегатом, а виключно режим підтримання температури води на виході котла з підтриманням режиму енергоекономичного спалювання палива.

Матеріали та методи

У більшості випадків при промисловому спалюванні палива основним принципом підвищення ефективності є максимально можливе використання наявної (нижчої) теплоти згоряння $Q_н^Р$. Основними складовими втрат теплоти при цьому є втрати з газами, що відходять q_2, і втрати від так званого хімічного недопалу q_3. Обидва ці показники тісно пов'язані з коефіцієнтом надлишку повітря α у факелі палаючого палива. Від цього ж коефіцієнта залежить і кількість шкідливих викидів в атмосферу [1, рис.1].

У більшості пристроїв спалювання газового палива, що застосовуються в даний час, оптимізація режиму горіння забезпечується шляхом підтримки співвідношення витрат газу і повітря (тиску перед пальним пристроєм) відповідно до режимної карти. Такий спосіб є недостатньо ефективним, він не дозволяє вести облік зміни температури та вологості повітря, теплотворної здатності та температури газу та низки інших зовнішніх факторів. У зв'язку з цим при складанні режимних карток допускають наявність значного надлишку повітря, щоб ні за яких умов не допустити виникнення хімічного недопалу газу. В результаті в деяких режимах кількість повітря перевищує оптимальне в 1,5-2 рази, що збільшує витрату електроенергії на дуття і призводить до необхідності нагрівання надмірної кількості повітря, що подається, тобто до додаткової витрати пального [2].

Аналіз процесу горіння газоподібного та рідкого палива показує, що при нестачі кисню проявляється різке підвищення концентрації оксиду вуглецю (CO). Відповідно, система регулювання процесу горіння, яка заснована на вимірюванні концентрації CO, матиме більш високу чутливість до відхилення режиму горіння від оптимального. Регулювання при цьому може зводиться до підтримки режиму горіння газу на межі хімічного недопалу, що дозволяє враховувати зміни більшості інших чинників, які впливають на якість спалювання палива [3].

Розроблені автоматичні системи оптимізації співвідношення «паливо-повітря», які побудовані з використанням стаціонарних газоаналізаторів, ведуть процес регулювання за величиною вмісту кисню у газах, що відходять. На деяких типах котлів ці системи регулювання обов'язково передбачені проектною документацією. Однак зазначені системи, як правило, не працюють у режимі регулювання, а газоаналізатор використовується у моніторинговому режимі, що обумовлено низкою причин [4]:

– концентрація кисню в димових газах залежить не тільки від інтенсивності дуття, але і від інших умов експлуатації (неконтрольоване підсмоктування повітря, зміна характеристик пальників у процесі експлуатації, неідентичність пальників у багатогорілкових котлах, зміна теплотворної здатності палива, коливання вологості

повітря), що, свою чергу, знижує ефективність роботи системи з регулюванням за величиною вмісту кисню;

– обмежене поширення контролерів, які мають стійкі (надійні) алгоритми роботи з газоаналізаторами (багато з розроблених алгоритмів регулювання не враховують перехідні процеси в топці при зміні потужності).

Більш досконалі автоматичні системи оптимізації співвідношення газ/повітря, побудовані з використанням стаціонарних газоаналізаторів, які ведуть процес регулювання з корекцією по концентрації кисню O_2, діоксиду вуглецю CO_2 або продуктів недопалу CO, H_2 і ін. у газах, що відходять з котла [5, 6]. Однак у цих роботах не розглядається, як проводиться процес регулювання й не розглядаються питання вибору необхідних режимів роботи котла для різних температурних режимів. Безумовно, при реалізації таких режимів буде спостерігатись зниження коефіцієнта корисної дії (ККД) котельного агрегату, тому що всі котли розраховуються для роботі в номінальному режимі з максимальним ККД. Тому виникає потреба вибору пріоритетів: або зниження витрати газу при роботі з урахуванням температури довкілля і зменшення шкідливих викидів в атмосферу, або досягнення максимального ККД. На нашу думку, на теперішній час перший пріоритет є більш вагомим.

На практиці застосовується кілька видів систем регулювання співвідношення «паливо-повітря» [7, 8]. Найпоширеніші з них:

1. Система регулювання процесом горіння, у якій підтримується співвідношення «паливо-повітря» відповідно до заздалегідь підготовленої режимної карти [8]. Недоліком цієї системи є труднощі складання режимної карти і її неефективність за певних умов (зношування технологічного устаткування, зміна складу палива і т. і., що призводить до виникнення статичної помилки регулювання).

2. Система регулювання процесом горіння, у якій відбувається екстремальне керування зі зворотним зв'язком по тому або іншому показнику якості роботи котельної установки [9]. Недоліком цієї системи є недостатня швидкодія й низька перешкодозахищеність.

3. Система регулювання процесом горіння за складом димових газів. Відомі наступні методи керування [4, 8]: за концентрацією залишкового кисню (O_2) у продуктах згоряння; за концентрацією продуктів хімічного недопалу ($CO_{екв}=CO+H_2+CH_4$); з використанням спільної інформації про концентрацію O_2 і продуктів неповного згоряння (CO). Ці методи засновані на сучасних датчиках – газоаналізаторах, які розроблені в останні роки [2, 3, 10].

Наступним логічним етапом енергоекологічної оптимізації спалювання палива є впровадження технологічних рішень, що спрямовані на організацію горіння з низьким або гранично низьким коефіцієнтом надлишку повітря. Позитивного ефекту можна досягнути тільки при використанні систем безперервного автоматичного контролю й регулювання співвідношення «паливо-повітря». Це – найбільш маловитратний і ефективний спосіб економії палива з одночасним зменшенням утворення шкідливих речовин у топці [1, 2, 3]. При цьому необхідно підтримувати подачу повітря таким чином, щоб значення коефіцієнта знаходилось в досить вузькій області, нижню границю якої визначає поява слідів оксиду вуглецю (на рівні 100-300 ppm), а верхню – зростання втрат теплоти з газами, що відходять, й підвищення інтенсивності утворення оксидів азоту, що супроводжує зростання концентрації вільного кисню.

З технічної літератури відомі наступні підходи до керування [8, 11]:

– для котлів з постійним навантаженням кращим є регулювання за співвідношенням «паливо-повітря» з вибором співвідношення концентрації CO, CO_2, O_2 – системи стабілізації співвідношення витрат «паливо-повітря» з корекцією за складом газів, що відходять; система екстремального регулювання горінням палива в котельному агрегаті;

– для котлів зі змінним навантаженням доцільна робота на межі хімічного недопалу, тобто з циклічним зниженням витрати повітря до появи різкого зростання концентрації CO, із наступним мінімальним збільшенням витрати повітря, щоб уникнути хімічного недопалу, якій має назву «режим відскоку» [4].

Контролери із вбудованим алгоритмом регулювання по оксиду вуглецю почали випускати різні виробники. Зокрема, у лінійці контролерів «СПЕКОН СК-n» (виробництво НВФ «Теплоком») реалізовано алгоритм використання газоаналізатора для корекції співвідношення «паливо-повітря» з урахуванням наявності в газах, що відходять, не тільки CO, але й O_2, а також з урахуванням впливу перехідних процесів у топці при зміні потужності [4]. При виході тиску повітря за припустимі межі коригувальний сигнал від газоаналізатора не враховується при регулюванні.

Основна частина

Протягом опалювального сезону температура довкілля може коливатися від плюс 10°C до мінус 25°C. При цьому параметри котла як об'єкта керування теж змінюються. Теплотехнічні розрахунки показують, що при таких умовах температура води на виході котла має змінюватися від 48°C до 150°C. Графік залежності температури на виході котла при заданій температурі 18°C в приміщеннях, які опалюються, від температури довкілля приведені в [8, рис. 2.9]. Система регулювання температури на виході котла має стежити за температурою довкілля, тобто бути такою, що слідкує. Існуючі типові регулятори при постійних налаштуваннях не в змозі працювати в такому широкому діапазоні. Отже, регулятор має бути адаптивним, тобто змінювати свої параметри в процесі роботи. Розробка такого регулятора представляє значні труднощі, і супроводження їх також буде складним. Оскільки в технічних системах на сьогоднішній день найбільш поширені регуляторі ПІД сімейства і використовуються вони в 90-95% контурів регулювання [12-14], перевагу слід віддати їм. Відомо, що регулятори ПІД-сімейства добре працюють у діапазоні ± 10...20% від заданого значення [12]. Найбільш простим методом адаптації ПІД-регулятора до змінних властивостей об'єкта керування є табличне керування коефіцієнтами регулятора. Воно може бути використано не тільки для адаптивного керування, але й для керування нелінійними об'єктами, нестаціонарними процесами, при необхідності змінювати параметри залежно від деяких умов [12, 15, 16].

Для розробки такої системи керування необхідно визначити для неї певні вимоги:

– час запізнення зміни температури на виході котла при зміні температури довкілля на ±5°C не має перевищувати ≈1…1,5 годин;
– відхилення температури від номінального значення на виході котла не має перевищувати ±2,5°C.

Базуючись на графіку [8, рис. 2.9], пропонується модель системи регулювання температури води на виході водогрійного котла, яка забезпечує підтримку необхідної температури залежно від коливань температури довкілля.

Структурна схема системи регулювання, що стежить, в загальному вигляді матиме наступний вигляд (рис. 1).

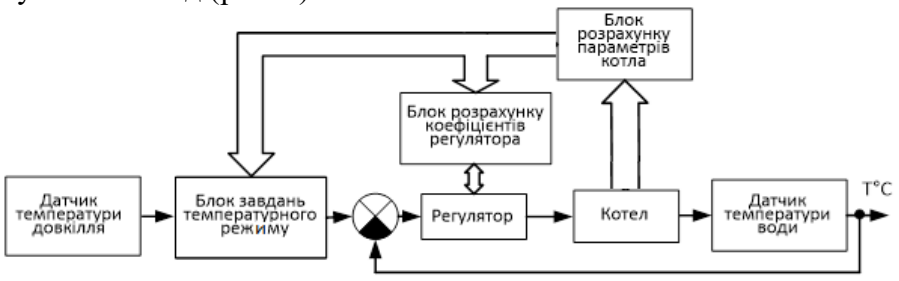


Рис. 1. Структурна схема системи регулювання температури води на виході котла

Інформація від датчика температури довкілля надходить у блок формування графіка температурного режиму. Оскільки температура довкілля не змінюється миттєво, слід вибрати крок графіка змін завдання температури води на виході котла: наприклад,

змінювати завдання кожні дві години для добового режиму. Таким чином, отримаємо таблицю з 12 значень температури, що задається.

Крім того, враховуючи, що параметри котла також змінюються для різних режимів, для кожного значення температури необхідна ще наявність банку даних про параметри котла, які можуть змінюватися в часі. Тобто, необхідно сформувати загальний банк даних із двох груп параметрів (за температурою та параметрами котла) для налаштування ПІД регуляторів.

Оскільки реалізація цих завдань не становить складності, основний вплив приділимо побудові моделі системи регулювання температури для одного заданого значення, що дорівнює 55°С. Так як при роботі котла для оптимального горіння газу в топці необхідно підтримувати невеликий надлишок повітря (тобто співвідношення повітря-газ – α = 1,05 ... 1,1), застосуємо регулятор співвідношень для подачі газу та повітря в топку котла [12, 17]. Оскільки в якості окиснювача для виконання хіміко-фізичного процесу горіння застосовується повітря, у складі якого кисень, необхідний для підтримки горіння, становить усього п'яту частину, а точніше, 20,93% – саме таке процентне співвідношення прийнято використовувати для всіляких технічних розрахунків. Тобто повітря знадобиться в 9,52 рази більше, ніж кисню. Ця кількість повітря, яка необхідна для ефективного горіння газу, є теоретичною витратою. Але, коли особлива точність не потрібна, те отримане значення 9,52 просто множити на так званий коефіцієнт надлишку повітря. Значення цього коефіцієнта звичайно лежить у межах α = 1,04 – 1,2 [1–7, 11, 18]. В результаті повітря треба подавати в 9,996≈10 разів більше.

В зв'язку з розповсюдженням котлів серії ДКВР, які можуть працювати в водогрійному режимі, оберемо для подальшого моделювання котел типу ДКВР-10-13-255ГМ з вентилятором ВДН 10, якій має потужність двигуна 11 кВт. Для регулювання витрати повітря застосуємо частотний перетворювач з стандартним керуючим токовим сигналом 4…20 мА. Модель котла, як об'єкта керування, складається з каналу подачі газу й повітря в пальник, самого пальнику, топки котла й барабана котла. У канал подачі газу входять: двигун вентиля подачі газу і вентиль газу у вигляді ланок першого порядку й блоку обмеження (Saturation), що враховує межу відкриття вентилю на 100% ходу регулювального органу. Канал подачі повітря складається з блоку Gain, що забезпечує співвідношення витрат газу й повітря у вигляді підсилювача, а також частотного перетворювача (блок Gain1) для двигуна вентилятора, який подає повітря в топку, з електродвигуном у вигляді ланки першого порядку. Пальник (Bumer) представлений у вигляді суматора, на виході якого сформована газоповітряна суміш, що згоряє в топке, а топка й котел представлені у вигляді ланок першого порядку [19, 20].

Вузол T_{voda}-F_{gaz} реалізовано з застосуванням блоку одномірної таблиці Look-Up Table на підставі експериментальних даних для аналогічних котлів. Регулятор співвідношення газ – повітря реалізовано за типовою схемою, у якій стабілізація витрати газу виконується верхнім регулятором (PID Controller1), а стабілізація витрати повітря нижнім регулятором (PID Controller2) [12, 17]. Для підвищення якості регулювання регулятор співвідношення охоплений загальним зворотним зв'язком з виходу котла. Таким чином, уся система регулювання являє собою каскадну систему та має наступний вигляд (рис. 2).

Налаштування регулятора виконано за допомогою вбудованого в MATLAB тюнера таким чином, щоб перехідний процес був аперіодичним без перерегулювання. Оскільки більшість застосованих пристроїв має значний час для досягнення номінальних режимів, приймемо хвилину в якості кроку моделювання.

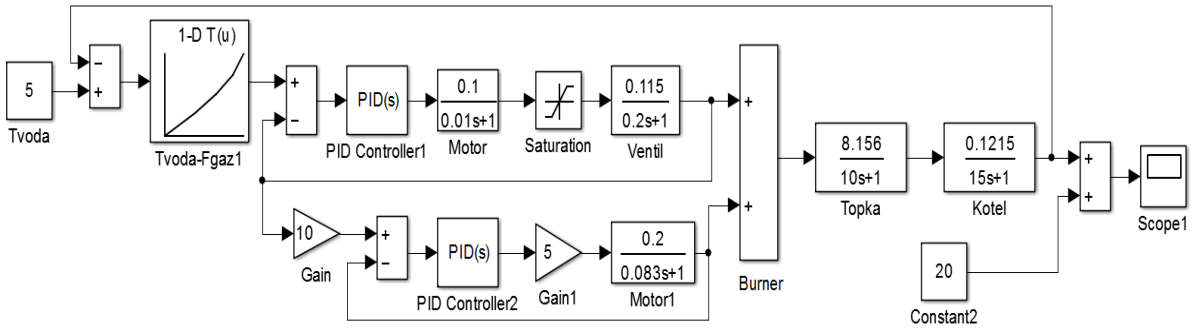


Рис. 2. Модель системи регулювання температури води на виході котла

Результат моделювання зі збуренням показують, що система досягає задане значення за час близько в 1,5 години, що є цілком припустимим для систем опалення в ЖКГ [8]. Таким чином перехідний процес, який було отримано при моделюванні каскадної системи з регулятором співвідношення газ-повітря показує, що вона забезпечує економічний режим опалення. Виконавши аналогічне моделювання для різних значень температур довкілля та отриманих значень параметрів регулятора можливо створити банк даних для впровадження запропонованої системи регулювання.

Для розгляду можливості реалізації поліпшення екологічності спалювання газу застосуємо запропонований в [2] алгоритм циклу «зниження-відскок-підтримка». Цей алгоритм в словесному вигляді розглянуто далі. Він передбачає завдання швидкості зниження витрати повітря, величину різкого зниження (стрибку) витрати повітря з появою хімічного недопалу, а також час нечутливості, протягом якого підтримується стала витрата повітря, після чого знову починається її зниження. Такий підхід дозволяє вести процес оптимальним чином на всіх режимах, при практично будь-яких змінах умов експлуатації й з будь-якими регуляторами й виконавчими механізмами.

Згідно з словесним алгоритмом блок схема циклу «зниження-відскок-підтримка» буде мати наступний вигляд (рис. 3).

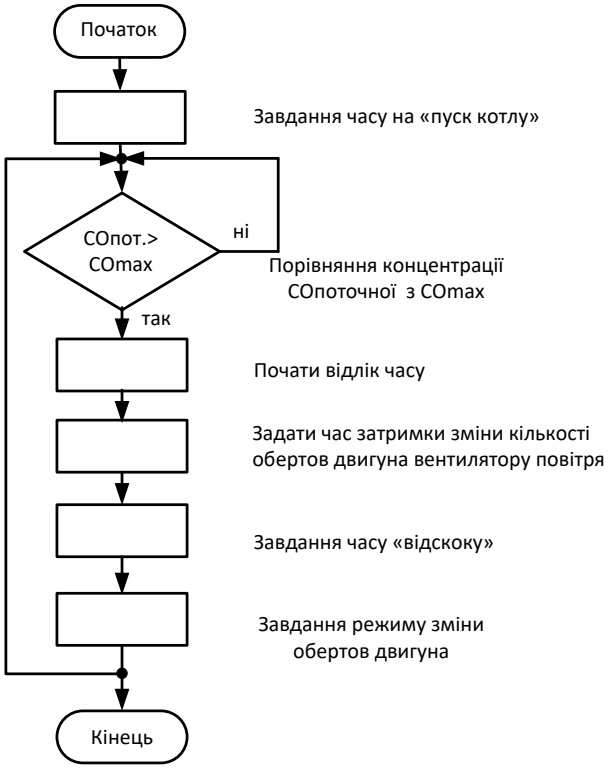


Рис. 3. Блок схема алгоритму «зниження-відскок-підтримка»

Реалізацію цього алгоритму виконано в програмному пакеті MATLAB-Simulink з застосуванням стандартних блоків.

Пояснімо вибір числових значень основних параметрів блоків алгоритму «зниження-відскок-підтримка», так як вони дозволяють застосувати дану модель для різних типів котлів та режимів. Значення концентрації CO обумовлено нормативними документами для котельних агрегатів. Однак, звичайно ці значення є значно завищеними, і тому пропонується використовувати дані нижче чим ті, які наведені в [3, 4, 6], тобто для прикладу приймемо Q_{COmax}=500 ppm, а значення Q_{COmin}=30 ppm. Затримку на підпал та вихід котлу на сталий режим приймемо рівною 100 хв.

Параметри, які характеризують пристрої котла, мають бути постійними. А більшість параметрів, які представляють режимні параметри, можуть бути змінені при імітаційному моделюванні. Наприклад, при зміні режимів котельного агрегату, для визначення кількості ступенів часу відскоку і кількості ступенів режимів потужності двигуна вентилятору, для подання повітря на горілку котлу.

Кількість ступенів часу відскоку приймемо для прикладу рівною 3. Слід враховувати, що кількість блоків, які визначають кількість ступенів сигналу для зміни потужності вентилятору повітря, має буди на один більше. Це пов'язано з тим, що спочатку двигун в період часу, яка дорівнює 1 хв., при перевищенні концентрації CO продовжує працювати в номінальному режимі, потім підвищує потужність до значення, яке близьке до максимального. Далі потужність двигуна зменшується. Конкретний вибір кількості ступенів зниження обумовлено, з одного боку, потужністю двигуна, а з другого плавністю зниження його потужності для зменшення зносу. Наприкінці потужність двигуна стає номінальною.

Як показано в [1, рис. 1], коливання концентрації кисню O_2 незначно змінюються при роботі котлу, а коливання окису вуглецю мають різке виражений характер, тому пропонується досліджувати тільки вплив максимальної концентрації CO на температуру на виході котла. Загальний вигляд моделі для дослідження впливу режиму відскоку на температуру на виході котла при збуренні по завданню має наступний вигляд (рис. 4).

Проведене моделювання системи керування температурою на виході котла в режимі екологічного спалювання палива показало короткочасний сплеск температури, якій не впливає на якість регулювання. Результати моделювання показані на рис. 5.

Для зручності моделювання з урахуванням збурень модель для виконання циклу «зниження-відскок-підтримка» представлена в вигляді підсистеми Subsystem1, а модель збурень в каналі подання повітря в вигляді підсистеми Subsystem.

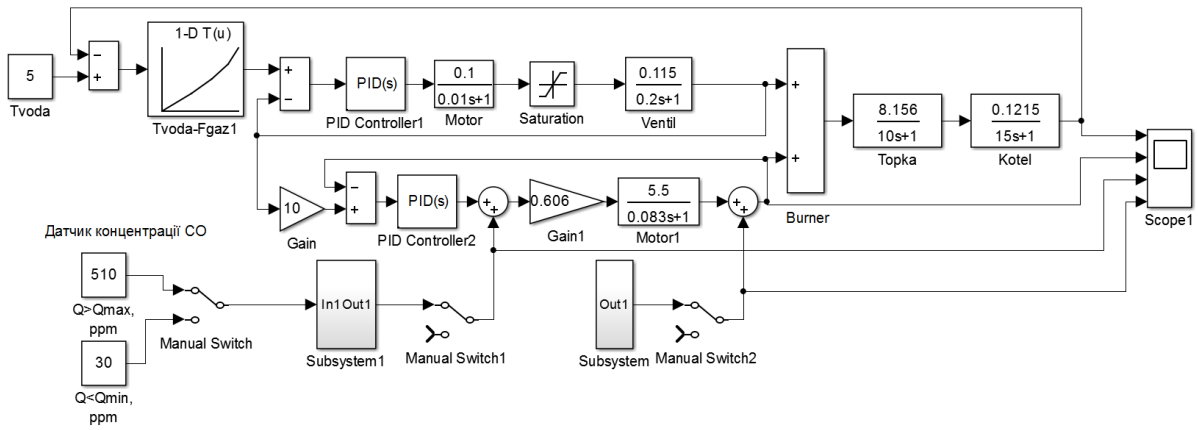


Рис. 4. Модель системи регулювання температури на виході котла з урахуванням режиму «відскоку» та збурень в каналі подання повітря

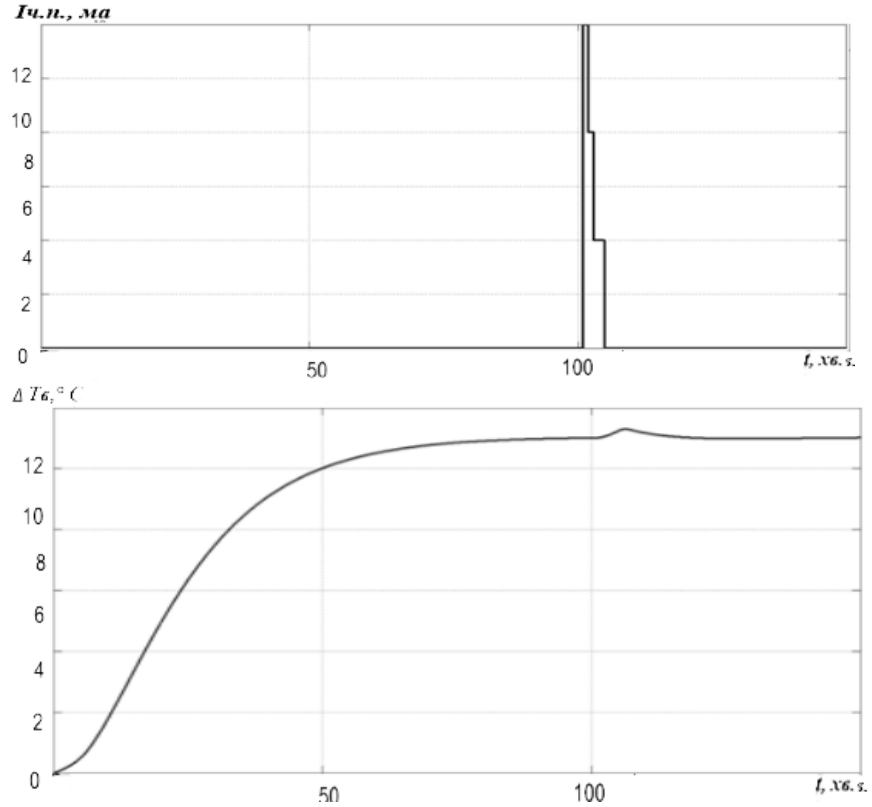


Рис. 5. Вплив «відскоку» зміною струму на вході частотного перетворювача для вентилятору повітря на перехідний процес по зміні завдання по температурі

Аналіз перехідного процесу, що отримано в результаті моделювання, показують, що запропонована модель відповідає вимогам, які пред'являються до підтримання температурного режиму на виході котла.

Висновки

В роботі запропонована структура системи керування, що стежить за температурою довкілля та відповідно до неї змінює температуру на виході котла. При цьому для можливості забезпечення здатності системи працювати в значному діапазоні температур довкілля та підтримання економічного спалювання палива пропонується застосування адаптивних ПІД регуляторів на підставі табличної зміни їх налаштувань. Для забезпечення енергоекологічного спалювання палива застосовано режим «відскоку». Проведено моделювання для однієї температури показало можливість використання подобної системи в системах опалення приміщень за допомогою котлів малої потужності.

Список літератури

1. Новиков О.Н., Окатьев А.Н., Шкаровский А.Л. Автоматическое управление качеством сжигания топлива – ключ к энергосбережению и энергоэкологической безопасности предприятия. *Инженерные системы*. 2011. №1. С. 38-43.

2. Тележко Г.М., Ягов Г.В. Современные методы обеспечения ресурсоэнергосбережения в теплоэнергетике и теплоснабжении. *Энергетика Татарстана*. 2009. № 1. С. 27-32.

3. Шкаровский А.Л., Новиков О.Н. Новикова А.В., Полушкин В.И. Разработка нового семейства интеллектуальных систем управления качеством сжигания топлива *Современные наукоемкие технологии*, 2016. № 12-3, С. 556-561.

4. Тележко Г.М., Хойна Е.В., Ягов Г.В. Новый подход к оптимизации режимов горения топлива. *Энергонадзор-Информ*. 2008. №1. С. 26-28.

5. Росляков П.В., Плешан К.А. Использование сжигания топлива с контролируемым химическим недопалом. *Новое в российской электроэнергетике*. 2010. Т.1. №1 (23). С. 12-30.

6. Воликов А.Н., Новиков О.Н., Окатьев А.Н. Энергоэкологическая эффективность сжигания газового и жидкого топлива в котлах малой и средней мощности. *Современные проблемы науки и образования*. 2012. № 4. С 88-98.

7 Воликов А.Н. Сжигание газового и жидкого топлива в котлах малой мощности. Ленинград : Недра, 1989. 159 с.

8. Бузников Е.Ф., Роддатис К.Ф., Берзиньш Э.Я. Производственные и отопительные котельные. М.: Энергоатомиздат, 1984. 248 с.

9 Авдеева, О. В. Система экстремального регулирования горением топлива в котельной установке. *Вестник Пензенского государственного университета*. 2015. Т.1. № 3 (11). С. 167–174.

10. Анализаторы дымовых газов комбинированные (интеллектуальный анализатор качества горения) URL: https://www.testo.ru/ru-RU/produkty/analizator-dymovyh-gazov.

11. Новиков О.Н., Артамонов Д.Г., Шкаровский А.Л., Кочергин М.А., Окатьев А.Н. Энергоэкологическая оптимизация сжигания топлива в котлах и печах регулированием соотношения «топливо – воздух». *Промышленная энергетика*. 2000. Т. 1. № 2 (79). С. 46-48.

12. Astrom K.J., Hagglund T. Advanced PID control. The Instrumentation, Systems, and Automation Society, 2006. 460 p.

13. Ротач В.Я. Теория автоматического управления. М.: МЭИ, 2008.

14. Александров А.Г. Оптимальные и адаптивные системы. М.: Высшая школа, 1989.

15. Шубладзе А.М., Гуляев С.В., Шубладзе А.А. Адаптивные автоматически настраивающиеся ПИД-регуляторы. *Промышленные АСУ и контроллеры*. 2003. № 6.

16. Шубладзе А.М., Кузнецов С.И. Автоматически настраивающиеся промышленные ПИ и ПИД-регуляторы. *Автоматизация в промышленности*. 2007.№ 2.

17. Денисенко В.В. ПИД-регуляторы: вопросы реализации. *СТА*. 2007. №4. С. 86 – 97.

18. Андросов А.С., Бегишев Е.П., Салеев И.Р. Теория горения и взрыва. М.: Академия ГПС МЧС России, 2015. 248с.

19. Документация MATLAB URL: https://docs.exponenta.ru .

20. Дьяконов В. П. Simulink 5/6/7: Самоучитель. Москва : ДМК Пресс, 2008.

21. Ощепков А.Ю. Системи автоматичного управління: теорія, застосування, моделювання в MATLAB URL: http://e.lanbook.com/books/element.php?pl1_id=5848

22. Бочаров Г.В., Тигарєв А.М. Моделирование начальной стадии температурного цикла нагрева конвейерной печи. *Збірник матеріалів VI Міжнародної науково-практичної конференції Економіка та управління в умовах побудови інформаційного суспільства.* 2017. Ч. II. С. 46-49.

IMPROVEMENT OF HEATING BOILERS REGULATION SYSTEMS

A.M.Tigarev1, T.G. Tigareva2

1 State University of Intellectual Technologies and Communications, 65029, Ukraine, Odesa, st. Kovalska, 1; e-mail: amtigar@ukr.net
2 Odesa State Academy of Civil Engineering and Architecture, 65029, Ukraine, Odesa, st. Didrichson, 4; e-mail: tatianatigareva@gmail.com

The article considers the option of improving the automatic control systems for natural gas combustion as a fuel for boilers. The aim of the improvement is to optimize the gas-air ratio to maintain the set temperature in the heated rooms, depending on the ambient temperature. In most of the currently used hot water boilers, the gas / air ratio is maintained in accordance with the regime maps without taking into account the economic and environmental combustion of gas, without automatically taking into account the ambient temperature. The desire to reduce excess fuel consumption necessitates the creation of automatic control systems that would maintain the required temperature of the coolant at the boiler outlet at different ambient temperatures. The main principle of increasing efficiency is the maximum possible use of available (lower) heat of combustion QnP. The main components of losses of warmth at the same time are losses with q2 flue gases and losses from so incomplete combustion of q3 fuel. The amount of harmful emissions into the atmosphere depends of both of these indicators that are closely related to the coefficient of excess air α in the burning fuel flare. The paper analyzes several types of fuel-air ratio control systems, notes their advantages and disadvantages. It is con-cluded that the greatest positive effect can be achieved only with the use of systems of continuous automatic control and regulation of the fuel-air ratio. The article proposes the structure of the control system that moni-tors the ambient temperature and changes the temperature at the boiler outlet accordingly. At the same time, in order to be able to operate the system in a significant range of ambient temperatures and maintain economical fuel combustion, the use of adaptive PID controllers is proposed on the basis of tabular changes in their set-tings. To ensure environmentally friendly fuel combustion, a "rebound" mode is used. The simulation of tem-perature change in the control system showed the possibility of its practical for house heating systems with low-power boilers.
Keywords: boiler, temperature regulation, gas-air ratio, regulator, rebound mode, modeling, CO concentra-tion

DOI 10.15276/imms.v12.no1-2.104
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 12 (2022), No. 1-2, pp. 104-113

СТЕГАНОАНАЛІТИЧНИЙ АЛГОРИТМ, ЗАСНОВАНИЙ НА ДОСЛІДЖЕННІ СИНГУЛЯРНОГО РОЗКЛАДУ БЛОКІВ МАТРИЦІ ЦИФРОВОГО ЗОБРАЖЕННЯ

К.О. Трифонова, С.М. Сокальський

Національний університет «Одеська політехніка»,
1, пр. Шевченка, Одеса, 65044, Україна; e-mail: katikkatik@gmail.com

Одною з найпоширеніших технологій для забезпечення захисту будь-яких цифрових даних при передачі по відкритих каналах зв'язку, на поданий час, вважаються стеганографічні методи. Застосування розв'язку задачі захисту цифрових даних за допомогою стеганографічних методів, використовується не лише державними службами, але й терористичними організаціями. У зв'язку з цим, необхідність дослідження, розробки та постійного підвищення ефективності стеганоаналітичних методів, стає надзвичайно актуальним. В роботі запропоновано стеганоаналітичний алгоритм, заснований на дослідженні сингулярного розкладу блоків матриці цифрового зображення. Головною метою поданої роботи є підвищення ефективності стеганоаналізу цифрового зображення, у відсутності контейнеру, шляхом розробки нового стеганоаналітичного алгоритму, заснованого на дослідженні сингулярного розкладу блоків матриці цифрового зображення. В результаті детального дослідження стеганографічного алгоритму, що використовує сингулярний розклад блоків матриці цифрового зображення, встановлені статистичні характеристики сингулярних чисел блоків матриці зображення. На основі визначених характеристик, в роботі представлені основні кроки стеганоаналітичного алгоритму. В якості критерію для оцінки ефективності розробленого стеганоаналітичного алгоритму, використана ймовірність детектування додаткової інформації. Розглянуто помилки першого та другого роду. Для порівняння результатів роботи, розробленого стеганоаналітичного алгоритму з існуючими алгоритмами у відкритому доступі, обрані наступні застосування: XSteg; StegSpy. Для автоматизованого розв'язку стеганоаналітичної задачі для цифрового зображення реалізовано програмний продукт «StegoAnalysis».

Ключові слова: захист інформації, стеганоаналіз, цифрове зображення, сингулярні числа, сингулярні вектори.

Вступ

Задача реалізації захисту особистих та секретних даних від незаконного доступу, займає провідну позицію, як для кожної особистості окремо, так і для держави в цілому. Найбільш поширеною технологію для забезпечення захисту даних при передачі даних по відкритих каналах зв'язку є стеганографічні методи [1-5].

Для розв'язку задач захисту даних, стеганографія знаходить своє застосування не лише секретними службами, але й терористичними організаціями. У зв'язку з цим, задача розробки стеганоаналітичних методів, стає важливішою рік від року.

Методи виявлення секретного повідомлення в контейнері активно розроблюються [6]. В залежності від встановленого критерію, визначають різні способи класифікації існуючих стеганоаналітичних методів для цифрових зображень, представлених на рисунку 1 [7].

В залежності від наявної інформації у стеганоаналітика виділяють наступні групи стеганоаналітичних методів.

Спрямований. В поданому випадку передбачається, що доступна вся інформація про стеганографічний алгоритм. Невідомою виявляється інформація про стеганографічний ключ.

Універсальний. В поданому випадку жодної інформації про алгоритм вбудовування секретного повідомлення немає. Аналітик виконує роботу з дослідження та виявлення не характерних особливостей цифрових зображень.

В залежності від атаки розрізняють наступні групи стеганоаналітичних методів.

Статичний. Головним завданням поданих методів є розрізнення заповнених та порожніх контейнерів, встановлення методу занурення додаткової інформації.

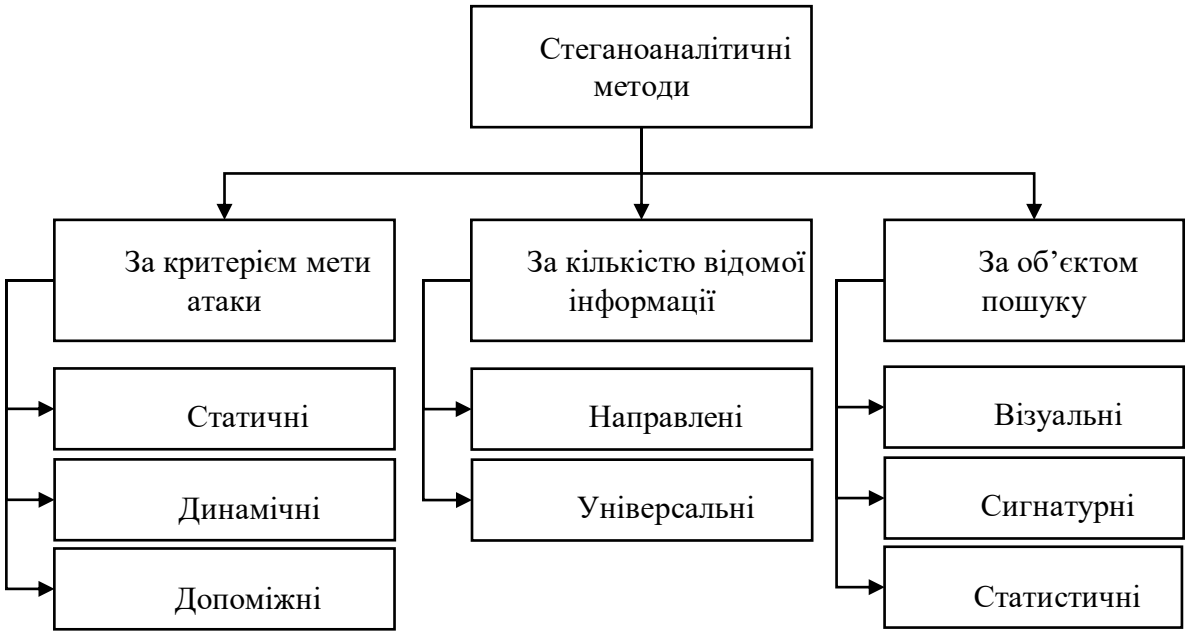


Рис. 1. Класифікація стеганоаналітичних методів

Динамічний. Головним завданням методів даної групи є визначення розміру вбудованого секретного повідомлення, його місце розташування, певні параметри алгоритму вбудовування, а також, в деяких випадках, навіть декодування приховуваного повідомлення.

Допоміжний. Головним завданням для даних методів є побудова різноманітних атак з метою активізації роботи стеганоканалу.

Стеганоаналітичні методи в залежності від предмета пошуку підрозділяють на наступні групи.

Візуальні. Методи, що відносяться до поданої групи, засновані на можливості людського зору встановлювати особливості цифрового зображення. При поданому аналізі відбувається дослідження графічного представлення контейнеру. Автоматизація такого типу методів, поки що є надзвичайно складним завданням, оскільки базується на розвитку методів комп'ютерного бачення та методів, що встановлюють характеристики справжності цифрових зображень.

Сигнатурні. Методи, що відносяться до поданої групи, засновані на дослідженні характерних особливостей формату зберігання цифрових зображень. Тобто пошук секретного повідомлення виконується в службових полях та полях даних. Методи сигнатурного допомагають виявити інформацію, яка була внесена у кінець файлу цифрового зображення Приховування інформації в такому випадку забезпечується тим, що стандартні програми перегляду зображень доходячи до маркеру кінця зображення припиняють свою роботу, і інформація, що находиться після цього маркеру залишається прихованою.

Статистичні. Методи, що відносяться до поданої групи, є найбільш поширеними. Подані методи засновані на дослідженні різноманітних статистичних характеристик натуральних, справжніх цифрових зображень.

Найбільш поширені методи, інформація про які наявна у відкритому доступі, відносяться до трьох груп: візуальні, сигнатурні, статистичні. Методи з кожної групи мають як свої переваги, так і не позбавлені значних недоліків, все це вимагає виконання нових досліджень, для розробки нових алгоритмів стеганографічного аналізу.

Мета і задачі дослідження

Метою роботи є підвищення ефективності стеганоаналізу цифрового зображення, у відсутності контейнеру, шляхом розробки нового стеганоаналітичного алгоритму, заснованого на дослідженні сингулярного розкладу блоків матриці цифрового зображення.

Для досягнення поставленої мети необхідно розв'язати наступні задачі:

1. виконати аналіз предметної області – дослідити реалізацію методів стеганоаналізу цифрових зображень;
2. виконати дослідження стеганоалгоритму, що використовує сингулярний розклад блоків матриці контейнера;
3. розробити стеганоаналітичний алгоритм, заснований на дослідженні сингулярного розкладу блоків матриці цифрового зображення;
4. реалізувати програмний продукт для виконання стеганоаналізу цифрового зображення.

Основна частина

Основні кроки алгоритму вбудовування секретного повідомлення стеганографічного алгоритму, заснованого на дослідженні сингулярного розкладу блоків матриці цифрового зображення, наведені в [8].

Ефективність цього стеганоалгоритму оцінюється за трьома критеріями: візуальна оцінка якості; ступінь забезпечення надійності сприйняття сформованого стеганоповідомлення; ступінь забезпечення надійності сприйняття стеганоповідомлення після атаки стисненням з різними ступенями стиснення.

Перш за все була проведена візуальна оцінка якості зображення після стеганоперетворення. В результаті експерименту було отримано набір стеганоповідомлень, для яких експертом не було виявлено жодних артефактів. На рисунку 2 наведено приклад цифрового зображення та зображення отриманого в результаті стеганоперетворення.

а) порожній контейнер б) заповнений контейнер

Рис. 2. Демонстрація результату стеганоперетворення

Наступним кроком оцінки стеганоалгоритму була оцінка надійності сприйняття стеганоповідомлення після атак стисненням. Важливо відмітити, що ці атаки були проведені за допомогою невеликих коефіцієнтів стиснення, оскільки важливо, щоб стеганоповідомлення зберігало надійність сприйняття після атак, інакше організатори прихованого каналу зв'язку можуть виявити факт використання атак стисненням. Тому атаки були використані із різним коефіцієнтом стиснення Q в діапазоні 80-100.

Експеримент проводився наступним чином. В обране цифрове зображення за допомогою стеганоперетворення вбудовувалась додаткова інформація, після чого воно зберігалось у форматі без втрат та у форматі з втратами з різними коефіцієнтами стиснення. Надійність сприйняття оцінена чисельно за допомогою пікового співвідношення сигнал-шум PSNR. Прийнято вважати, що надійність сприйняття не порушена, якщо PSNR > 37 Db. В ході експерименту встановлено, що для отриманих стеганоповідомлень подана нерівність не була порушена.

Стеганоаналітичний алгоритм, заснований на дослідженні сингулярного розкладу блоків матриці цифрового зображення

Стеганоаналітичні алгоритми можна класифікувати по різним критеріям. Наприклад, залежно від кількості наданої інформації для стеганоаналіза, методи розділяють на універсальні та направлені. Для направлених методів потрібно надати інформацію про стеганографічний алгоритм, за допомогою якого виконувалось стеганоперетворення. А при моделюванні універсального метода інформація про стеганографічний алгоритм може використовуватись лише в режимі «чорного ящика». При використанні такого класу методів стеганоаналітик старається найти деякі ознаки, які характерні для пустого контейнера, які одночасно задовольняли вимоги репрезентативності та контекстної незалежності, та змінювались би при стеганоперетворенні. Універсальні методи менш точні ніж направлені, але мають більш широкий спектр використання. Стеганоаналітичний алгоритм, заснований на дослідженні сингулярного розкладу блоків матриці цифрового зображення, відноситься до групи направлених алгоритмів. Основною метою поданого стеганоаналітичного алгоритму є встановлення факту наявності секретного повідомлення в контейнері цифрового зображення, що було піддано стеганоперетворенню на основі сингулярного розкладу блоків матриці цифрового зображення.

Розглянемо цифрове зображення F. Для кольорового цифрового зображення необхідно виконувати дослідження для кожної кольорової складової окремо. Матриця F розбивається стандартним чином на непересічні блоки f, розміром 8×8. Для кожного блоку виконується побудова сингулярного розкладу.

У відповідності до алгоритму стеганоперетворення вбудовування додаткової інформації в кожний блок виконується у відповідності до наступних формул:

$$\overline{\sigma}_1 = roundn(\sigma_1, K) + 1/4 \cdot \sigma_2, \quad (1)$$

для випадку вбудовування одиниці та

$$\overline{\sigma}_1 = roundn(\sigma_1, K) + 3/4 \cdot \sigma_2, \quad (2)$$

для випадку вбудовування нуля.

Позначимо співвідношення між першим та другим сингулярним числом блоку f матриці цифрового зображення F:

$$T = \frac{\overline{\overline{\sigma}}_1 - roundn(\overline{\overline{\sigma}}_1, K)}{\overline{\overline{\sigma}}_2}. \quad (3)$$

На основі поданої відомої інформації, зрозуміло, що після виконання стеганоперетворення, для заповненого контейнеру цифрового зображення, співвідношення між першим та другим сингулярними числами повинно відповідати наступним формулам:

$$\frac{\overline{\overline{\sigma}}_1 - roundn(\overline{\overline{\sigma}}_1, K)}{\overline{\overline{\sigma}}_2} \approx 1/4, \quad (4)$$

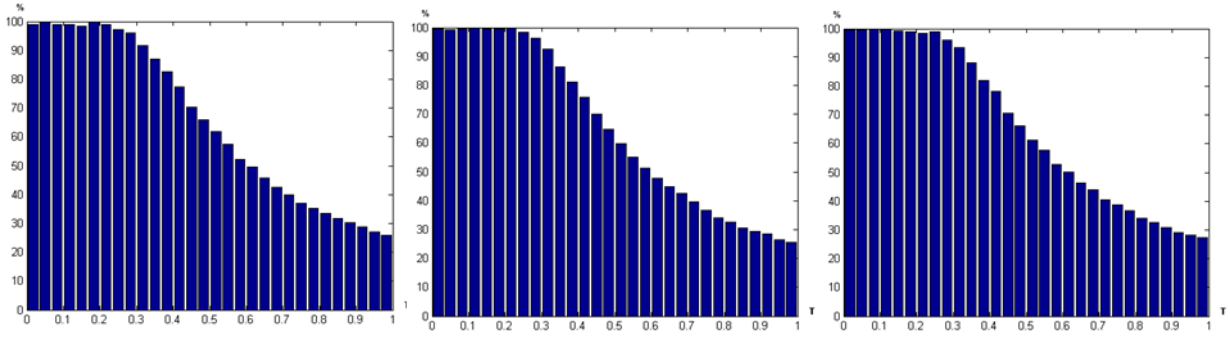
$$\frac{\overline{\overline{\sigma}}_1 - roundn(\overline{\overline{\sigma}}_1, K)}{\overline{\overline{\sigma}}_2} \approx 3/4. \quad (5)$$

Для підтвердження теоретичних висновків проведено обчислювальний

експеримент.

В експерименті задіяне 500 цифрових зображень різного розміру, що збережені в форматі без втрат та з втратами. Дослідження були виконані окремо для кожної кольорової складової: червоної, зеленої та синьої. Попередньо кожне цифрове зображення стандартним чином було розбито на блоки 8x8, для кожного блоку був побудований сингулярний розклад, та визначена величина T у відповідності до (3).

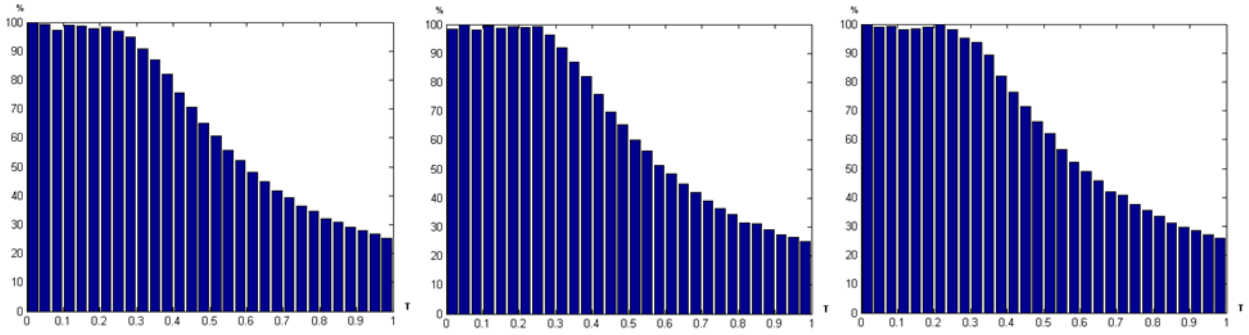
На основі отриманих даних побудовані для кожної кольорової складової усіх цифрових зображень збережених без втрат відповідні гістограми (рис. 3).



а) R б) G в) B

Рис.3. Гістограми значень T для порожніх контейнерів збережених без втрат

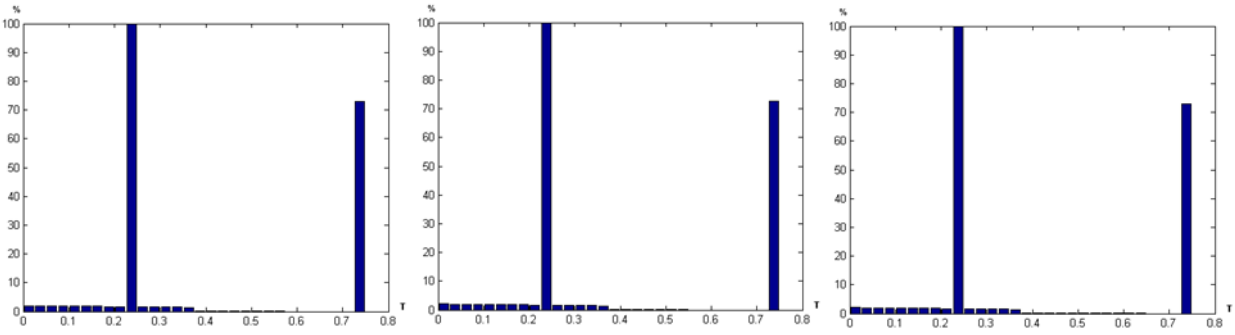
На основі отриманих даних побудовані для кожної кольорової складової усіх цифрових зображень збережених з втратами відповідні гістограми (рис. 4).



а) R б) G в) B

Рис.4. Гістограми значень T для порожніх контейнерів збережених з втратами

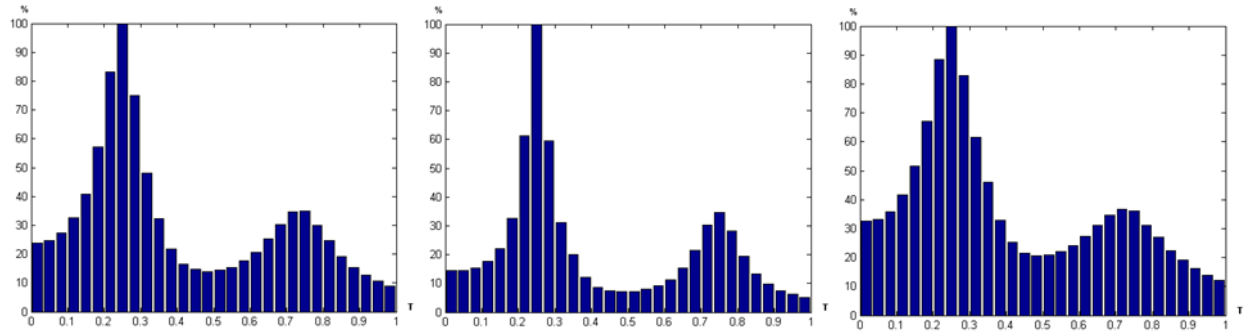
На основі отриманих даних побудовані для кожної кольорової складової усіх стеганоповідомлень збережених без втрат відповідні гістограми (рис. 5).



а) R б) G в) B

Рис.5. Гістограми значень T для заповнених контейнерів збережених без втрат

На основі отриманих даних побудовані для кожної кольорової складової усіх стеганоповідомлень збережених з втратами відповідні гістограми (рис. 6).



а) R б) G в) B

Рис.6. Гістограми значень T для заповнених контейнерів збережених з втратами

Основні кроки запропонованого стеганоаналітичного алгоритму наступні.

а) виконати розбиття матриці F стандартним чином на блоки f $8x8$;

б) виконати для кожного блоку f матриці F:

1) побудувати набір сингулярних чисел, в результаті $f = U\Sigma V^T$;

2) визначити величину $T(f) = \dfrac{\overline{\overline{\sigma_1}} - roundn(\overline{\overline{\sigma_1}}, K)}{\overline{\overline{\sigma_2}}}$;

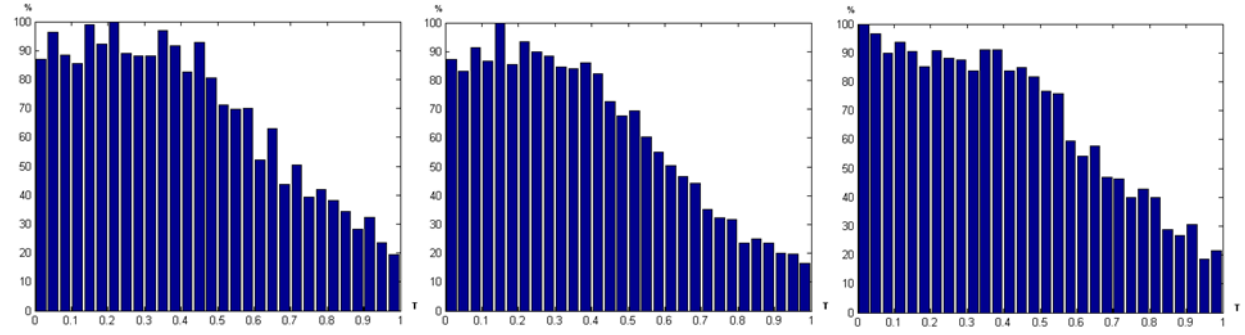
в) побудувати гістограму значень $T(f)$;

г) якщо $T(0{,}25) \geq T(0{,}5) \geq T(0{,}75)$, то F порожній контейнер,

якщо $T(0{,}25) > T(0{,}5) < T(0{,}75)$, то F заповнений контейнер.

Для демонстрації роботи, запропонованого стеганоаналітичного алгоритму, заснованого на дослідженні сингулярного розкладу блоків матриці цифрового зображення, розглянемо два цифрових зображення з рисунку 2.

Для цифрового зображення (рис. 2а) гістограми значень T представлені на рис. 7.



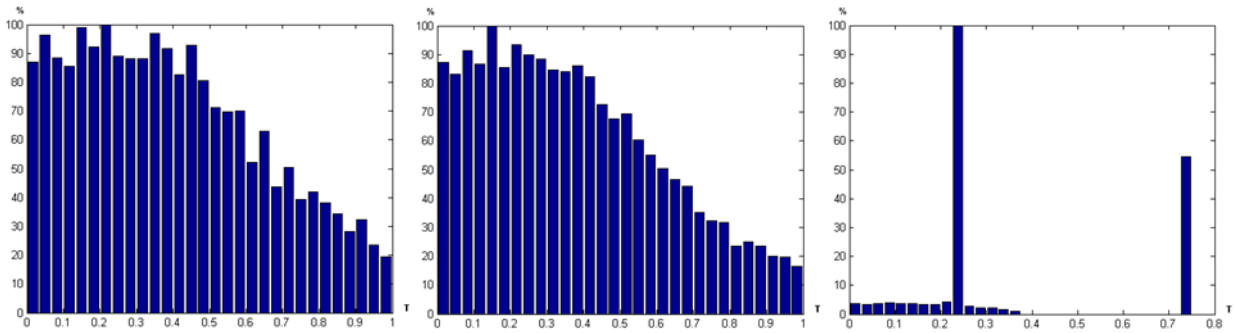
а) R б) G в) B

Рис.7. Гістограми значень T для порожнього контейнера збереженого без втрат

Для цифрового зображення (рис. 2б) гістограми значень T представлені на рис. 8.

Ефективність розробленого стеганоаналітичного алгоритму

В якості критерію для оцінки ефективності розробленого стеганоаналітичного алгоритму, заснованого на дослідженні сингулярного розкладу блоків матриці цифрового зображення, буде використана ймовірність детектування додаткової інформації. Розглянемо помилки першого та другого роду.



а) R б) G в) B

Рис.8. Гістограми значень T для заповненого контейнера збереженого без втрат

Помилка першого роду – випадок, коли стеганоаналітичний алгоритм визначає порожній контейнер як заповнений контейнер.

Помилка другого роду – випадок, коли стеганоаналітичний алгоритм визначає, що заповнений контейнер є порожнім.

Проведено обчислювальний експеримент. В експерименті задіяне 500 цифрових зображень різного розміру, що збережені в форматі без втрат та з втратами. В тестовому наборі були як порожні контейнери так і контейнери, що містили секретну інформацію. Кожний заповнений контейнер містив додаткову інформацію, вбудовану за допомогою стеганографічного алгоритму, заснованого на дослідженні сингулярного розкладу блоків матриці, в одну з кольорових складових. Для забезпечення надійності сприйняття порожнього або заповненого контейнеру, формат збереження з втратами обирався з невеликим ступенем стиснення. Вбудовування додаткової інформації, в матрицю обраної відповідної кольорової складової, відбувалось на 100%.

В результаті виконання експерименту встановлено, що помилки першого роду становили 1% та помилки другого роду 2%. Подані випадки представляють собою цифрові зображення невеликого розміру.

Для порівняння результатів роботи розробленого стеганоаналітичного алгоритму з існуючими алгоритмами у відкритому доступі, обрані наступні (рис. 9):

- C1 – стеганоаналітична програма XSteg [9];
- C2 – стеганоаналітична програма StegSpy [10];
- C3 – стеганоаналітична програма, заснований на дослідженні сингулярного розкладу блоків матриці цифрового зображення.

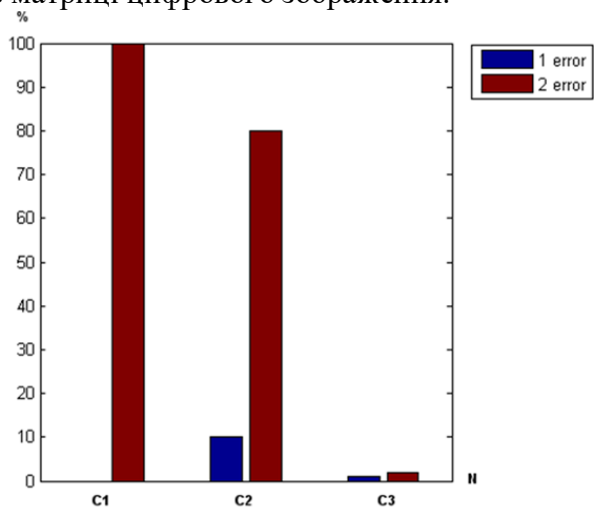


Рис. 9. Ефективність стеганоаналітичних методів

Для автоматизованого розв’язку стеганоаналітичної задачі для цифрового зображення реалізовано програмний продукт «StegoAnalysis», який складається з компонентів наступних програм [11-15]. Діаграма послідовності програмного продукту

«StegoAnalysis» зображена на рисунку 10.

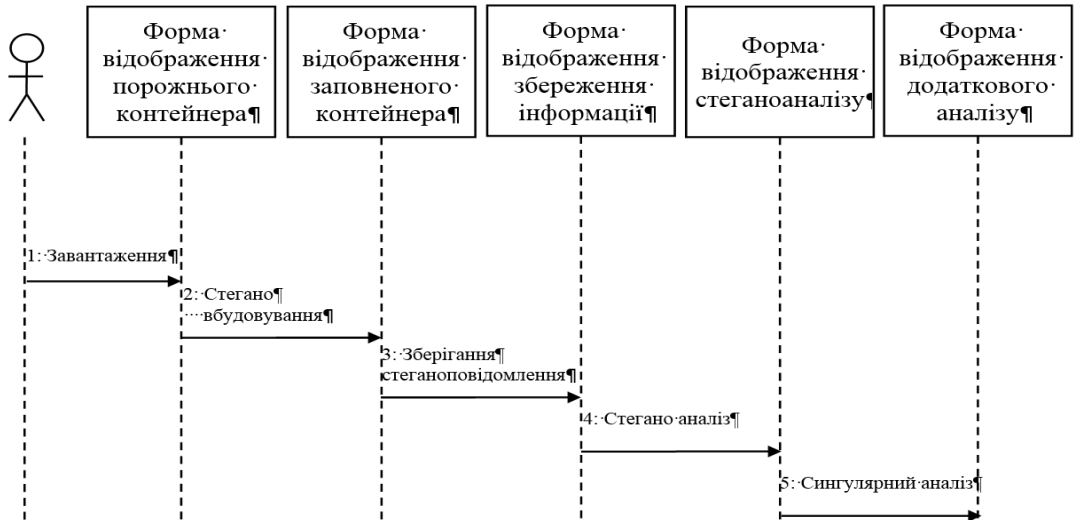


Рис. 10. Діаграма послідовності програмного продукту «StegoAnalysis»

Структура програмного продукту є модульною. Функціональна структура застосування включає в себе наступні модулі.

Модуль завантаження цифрового зображення: виконує завантаження контейнеру у різних форматах, як з втратами так і без.

Модуль стеганографічного перетворення: для виконання дослідження, реалізує стеганографічний алгоритм, заснований на дослідженні сингулярного розкладу блоків матриці цифрового зображення.

Модуль збереження стеганоповідомлення: реалізує можливість збереження заповненого контейнера у різних форматах, як з втратами так і без.

Модуль збереження секретного повідомлення: реалізує збереження генерованого секретного повідомлення.

Модуль стеганографічного аналізу: для виконання дослідження, реалізує стеганоаналітичний алгоритм, заснований на дослідженні сингулярного розкладу блоків матриці цифрового зображення.

Модуль сингулярного аналізу: додатково реалізує сингулярне дослідження для кожного блоку матриці цифрового зображення.

Інтерфейс програмного продукту представлено на рис.11.

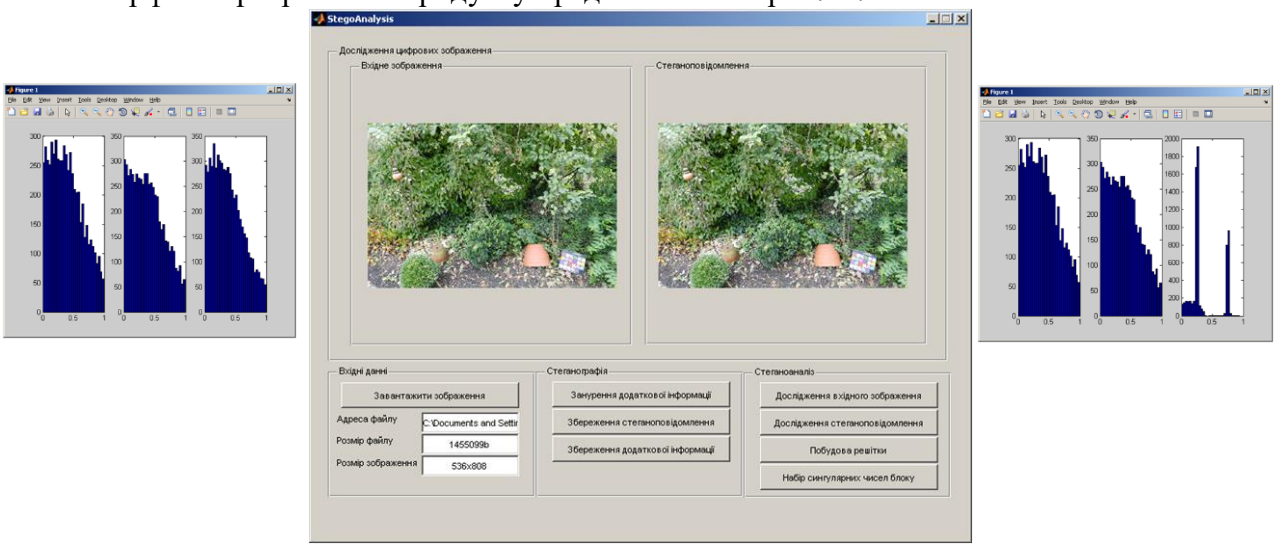


Рис. 11. Гістограми співвідношення першого та другого сингулярних чисел для кожної кольорової складової цифрового зображення

Висновки

В роботі представлені теоретичні основи стеганоаналітичного алгоритму, заснованому на дослідженні сингулярного розкладу блоків матриці цифрового зображення.

Детально виконано дослідження стеганоалгоритму, що використовує сингулярний розклад блоків матриці контейнера. Виявлено співвідношення між першим та другим сингулярними числами, що встановлюється в результаті вбудовування додаткової інформації. Проведено обчислювальний експеримент, що підтверджує теоретичні міркування.

На основі виявлених особливостей, розроблено стеганоаналітичний алгоритм, заснований на дослідженні сингулярного розкладу блоків матриці цифрового зображення.

Для оцінки ефективності розробленого стеганоаналітичного алгоритму підраховані помилки першого та другого роду.

Для автоматизованого розв'язку стеганоаналітичної задачі реалізовано програмний продукт «StegoAnalysis» для виконання стеганоаналізу цифрового зображення.

Список літератури

1. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. К.: МК-Пресс, 2006. 288 с.
2. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации. К.: Юниор, 2003. 504 с.
3. Хорошко В.О., Яремчук Ю.Є., Карпінець В.В. Комп'ютерна стеганографія: навчальний посібник. Вінниця: ВНТУ, 2017. 155 с.
4. Аграновский А.В., Грибунин В.Г. Стеганография, цифровые водяные знаки и стегоанализ. М.: Вузовская книга, 2009. 220 с.
5. Грибунин В.Г., Туринцев И.В. Цифровая стеганография. М.: Солон-Пресс, 2009. 272 с.
6. Сокальський С.М., Трифонова К.О. Стеганоаналіз цифрових зображень. Актуальные научные исследования в современном мире. Сборник научных трудов. 2021. №5(73), Ч.2. С. 75–78.
7. Кошкина Н.В. Обзор и классификация методов стеганоанализа. Control Systems and Computers. Фундаментальные и прикладные проблемы Computer Science. 2015. № 3. С.3–12.
8. Козіна М.О., Папковська О.Б. Стеганоалгоритм, що використовує сингулярне розкладання матриці контейнера. Сучасний захист інформації. 2018. № 2(34). С.47–52.
9. XSteg. URL: https://launchpad.net/ubuntu/hoary/i386/xsteg/0.5-6
10. StegSpy. URL: http://www.spy-hunter.com/stegspy
11. Matlab. URL: https://www.mathworks.com/help/matlab/
12. Image Processing Toolbox. URL: https://www.mathworks.com/products/image.html
13. Документация IPT. URL: https://docs.exponenta.ru/images/index.html
14. IPT. URL: https://exponenta.ru/image-processing-toolbox
15. Matlab GUI. URL: https://www.mathworks.com/discovery/matlab-gui.html

STEGANOANALYTICAL ALGORITHM BASED ON THE STUDY OF THE SINGULAR DECOMPOSITION OF DIGITAL IMAGE MATRIX BLOCKS

K.O. Tryfonova, S.M. Sokalsky

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

Steganography methods are considered to be one of the most common technologies for the protection of any digital data when transmitted over open communication channels at a given time. The solution of the problem of digital data protection using steganography methods is used not only by government services, but also by terrorist organizations. Therefore, the need for research, development and continuous improvement of steganoanalytical methods is becoming extremely important. The steganoanalytical algorithm based on the study of the singular decomposition of digital image matrix blocks is proposed in the paper. The main purpose of this paper is to increase the efficiency of digital image steganoanalysis, in the absence of a container, by developing a new steganoanalytical algorithm based on the study of the singular decomposition of digital image matrix blocks. As a result of a detailed study of the steganography algorithm using the singular decomposition of digital image matrix blocks, the statistical characteristics of the singular values of image matrix blocks are established. Based on the defined characteristics, the paper presents the main steps of the steganoanalytical algorithm. As a criterion for assessing the effectiveness of the developed steganoanalytical algorithm, the probability of detecting additional information was used. Errors of the first and second type are considered. To compare the results of the developed steganoanalytical algorithm with existing algorithms in open access, the following applications are selected: XSteg; StegSpy. The software product "StegoAnalysis" has been implemented for the automated solution of the steganoanalytical problem for digital image.

Keywords: information security, steganoanalysis, digital image, singular values, singular vectors

DOI 10.15276/imms.v12.no1-2.114
УДК 004.681.3

Informatics and Mathematical Methods in Simulation
Vol. 12 (2022), No. 1-2, pp. 114-123

ОЦІНКА СТАНІВ ФУНКЦІОНУВАННЯ СИСТЕМИ КІБЕРНЕТИЧНОГО ЗАХИСТУ ДЕРЖАВИ

В.О.Хорошко, Ю.Є. Хохлачова

Національний авіаційний університет,
1, просп. Любомира Гузера, Київ, 03058, Україна, e-mail: professor_va@ukr.net

Розглядаються математичні методи дослідження процесу функціонування системи кібербезпеки держави, накопичення та обробки інформації. З урахуванням того, що в умовах війни Росії проти України задачі кіберзахисту інформаційних систем держави набули не аби якої значення, а полем інформаційної війни стали комп'ютерні мережі. Також показано, що для практичного використання одержаних теоретичних аналітичних результатів немає принципових труднощів. Незважаючи на те, що вони не дуже оглядові та мало відчутні на простий чисельний дотик, бо містять неелементарні функції, при наявності сучасних електронних обчислювальних машин та найрізноманітнішого програмного забезпечення, чисельно-графічні трактування одержаних формул і розв'язки, які в них входять, не є непереборною перепоною для одержання наглядного розв'язку та практичного використання в розрахунку та обґрунтуванні ефективності функціонування системи кібербезпеки держави.

Ключові слова: кібербезпека, кібербезпека держави, системи кібербезпеки держави, оцінка станів функціонування системи, математичні методи функціонування системи, ефективність функціонування системи.

Вступ

Події кінця XX – початку XXI сторіччя проходить на фоні трансформації суспільства від постіндустріального до інформаційного. В світі відбувається стрімкий розвиток інформаційних технологій та їх проникнення у всі сфери діяльності людини: соціальну, економічну, політичну, військову тощо. До основних рис процесу інформаційного суспільства на сучасному етапі відносяться глобалізація та інтенсифікація інформаційних процесів, зміна сучасної картини світу.

Завдяки революції в області інформатизації і комунікації відбуваються значні зміни у сфері кібербезпеки та захисту інформаційних ресурсів держави. Поширився континуум вимірів, в яких може вестися інформаційна війна – сьогодні можна констатувати, що вона ведеться не тільки в традиційних вимірах «простір-час», але і в «інформаційному вимірі» [1].

У сучасних умовах інформаційна інфраструктура держави набуває статусу критичної (життєво важливої для існування) з усіма від цього похідними: вона стає об'єктом першого удару і потребує для свого захисту збалансованої державної політики в інформаційному просторі. Це наглядно показує Росія своїми діями у війні проти України. Тому, до критичної інформаційної інфраструктури належать, в першу чергу, економіка, транспорт, енергетика, фінансова система, системи управління у державі, що забезпечують безпеку та оборону держави тощо. Інформаційна система, система управління, канали зв'язку, системи навігації, розвідка, банківські системи та інші елементи інформаційного середовища потребують захисту від відповідних впливів та атак.

Аналіз подій, що розгортаються в інформаційному просторі, дозволяє відзначати необхідні тенденції [1,2]:

- по-перше, глобальна інформатизація та створення високоінтелектуальних систем управління призводить до глобалізації об'єктів інформаційного впливу, розвитку відповідно до цього форм і способів ведення інформаційного протиборства.
- по-друге, використання світової мережі Internet та електронних засобів масової інформації для маніпулювання свідомістю як світової громадськості, так і населення окремої країни, зміщення та перенос, для цього, центру тяжіння у масовому інформуванні в бік електронних засобів;
- по-третє, перенос тероризму у площину інформатизації;
- по-четверте, наявність конфліктів у інформаційному просторі, при цьому вже зараз це підтверджує Росія.

Таким чином, в умовах сьогодення, коли суспільство практично повністю залежить від застосування інформаційних технологій, полем інформаційної війни стали комп'ютерні мережі, а метою й завданнями – стають задачі кіберзахисту інформаційних систем держави. Слід враховувати, що в умовах війни Росії проти України ці питання набувають не аби якої значення.

Мета роботи

Розглядаються математичні методи дослідження процесу функціонування системи кібербезпеки держави (СКБД), накопичення та обробки інформації.

Основна частина

Дослідження процесу функціонування СКБД щодо накопичення та обробки інформації вимагає застосування різноманітного математичного апарату для вдосконалення структури та форми управління процесом функціонування цієї системи. При цьому слід враховувати, що СКБД має у своєму складі підсистеми, які виконують задачі відповідно до регіону та ситуації. Таке управління передбачає використання досить адекватних математичних методів та моделей для аналізу та оптимізації різноманітних ситуаційних та технологічних процесів. Для побудови високо ймовірного прогнозу оптимального управління подальшим процесом функціонування системи в літературі відомі частково розроблені математичні моделі подібного призначення та проведені на їх основі дослідження для найпоширеніших задач прогнозу процесу функціонування системи. [3]. Проте інколи виникають такі специфічні умови в технологічних процесах, що відомі математичні моделі стають недостатньо адекватними. Розглянемо реальну задачу в термінах теорії масового обслуговування (ТМО) специфіка якої полягає в тому, що система накопичення та обробки інформації починає функціонування та діє лише при наявності накопиченої в ній визначеної кількості необхідної інформації, необхідного забезпечення, або в термінах ТМО – необхідної кількості вимог. Наприклад, створення кінцевої інформації системою або підсистемою може починатися лише в тому випадку, коли накопичена певна первинна кількість даних у вигляді певної бази, певного математичного та програмного забезпечення, що може бути обумовлено використанням певної технології. Надалі обсяг кінцевої інформації, необхідної для прийняття рішень, накопиченої та обробленої утворює достатній запас для подальшого зв'язку зі споживачами до того моменту, коли буде повністю задоволена потреба в цій інформації. Такий спосіб функціонування є найбільш раціональним, оскільки вимагає можливість неповного завантаження СКБД та зниження ефективності використання її ресурсів.

Таким чином маємо наступну інтерпретацію: вимога - квант - набір інформації та можливих програмних комплектуючих, обслужена вимога – готовий накопичений інформаційно оброблений та готовий до вживання продукт. Нагадаємо, що мова йде про обробку та накопичення інформації, її формалізацію та формалізацію лише в сенсі кількості інформації з позицій теорії інформації, без розгляду прикладного сенсу та захисту, що вкладається в цю кількість. Отже, в систему ТМО надходить деяка кількість первинної інформації. Моделюючи течію надходження вважаємо, що найадекватнішна модель його буде коли ймовірність того, що на малий проміжок часу $\Delta(\Delta \to 0)$ надійде певна кількість m вихідної інформації, дорівнює $\lambda_m \Delta + g(\Delta)$. З даного вихідного припущення випливає, що є стаціонарна неординарна пуасонівська течія. Природно для неї ввести узагальнене позначення параметра $\lambda = \sum_{i=1}^{\infty} \lambda_i$ та припустити виконання умови

$$\sum_{i=1}^{\infty} h_i < \infty, \qquad (1)$$

що є логічним продовженням вихідних даних.

Технологічний цикл (перший канал обслуговування) починається лише тоді, коли накопичена достатня кількість первинної інформації (кількість вимог в черзі), величину якої позначимо r_0.

Наступний технологічний цикл (другий цикл обслуговування) викликається, коли для цього також забезпечено кількість первинної інформації (кількість вимог) r_0, а в системі масового обслуговування їх є не менше $2r_0$. Таким чином n-ий канал включається і може обслуговувати лише після того, коли в системі буде не менше $r_0 n$ вимог; при цьому для простоти дослідження та математичної формалізації обмежень на кількість каналів в системі накладати не будемо, що не є суттєвими обмеженням застосовності результатів, адже реальне співвідношення вхідних параметрів завжди забезпечує досить обмежене граничне значення n. Вважаємо, що час обслуговування однієї вимоги кожним каналом не залежить від обслуговування на інших каналах, від течії вимог і розподілений за показниковим законом. Значення параметра обслуговування знову ж для простоти аналітичних виразів та обчислень покладемо рівним одиниці, що це звужує загальності вихідної задачі, адже параметри усталеного процесу ТМО залежить не від конкретних значень окремих параметрів елементів ТМО, а від їх співвідношення. Тому будь-який параметр можна взяти за одиницю виміру, поклавши його значення рівним одиниці і нормуючи при цьому значення інших параметрів. Таким чином припущення параметра експоненціального обслуговування, рівного одиниці, не має принципового значення.

В цих умовах та припущеннях нас цікавить розподіл кількості зайнятих каналів в режимі роботи системи, що встановлюється. Іншими словами, нас цікавить ймовірність зайнятості каналів технологічного циклу в установленому режимі функціонування, тобто коли накопичено достатню кількість первинної інформації та після цього пройшло відносно багато часу.

Введемо наступні позначення. Нехай p_r, r = 0,1,2,3,… - ймовірність того, що в довільно обраний момент часу в установленому режимі роботи системи обслуговуванням зайнято r каналів; p_k, k=0,1,2,3,… - ймовірність того, що в установленому режимі в довільний момент часу в системі знаходяться k вимог. Як бачимо з введеної формалізації вихідної задачі прогноз, а також управління процесу функціонування СКБД накопичення та обробки інформації визначається саме ймовірностями p_r. Очевидно, що за ймовірностями p_k легко визначити ймовірність p_r. Тому знаходим ймовірність p_k [4]. Ще раз відмітимо, що сформульована задача не втрачає загальності за припущення, що параметр обслуговування рівний одиниці, адже стаціонарний розподіл p_k визначається не

конкретними значеннями параметрами потоку та обслуговування, а їх співвідношенням. Якщо в реальній системі параметр обслуговування m то пронормувавши відповідно параметр потоку, можна користуватися результатами, що отримані нижче.

Подовжимо формалізацію та позначимо [x] – ціла частина величини *x*; *β(t)* – число вимог, що знаходяться в системі в момент часу *t*. Неважко побачити, що введений до розгляду процес *β(t)* являє собою однорідний ланцюг Маркова, і визначається ймовірностями переходу за малий час $\Delta(\Delta\to 0)$ у вигляді

$$p\{[\beta(t)^* = k] \to^{\Delta} \{\beta(t+\Delta) = k\}\} = 1 - \left(\lambda + \left[\frac{\lambda}{r_0}\right]\right)\Delta + g(\Delta),$$
$$p\{[\beta(t) = k] \to^{\Delta} \{\beta(t+\Delta) = k+m\}\} = \lambda_m\Delta + g(\Delta), m \geq 1, \quad (2)$$
$$p\{[\beta(t) = k] \to^{\Delta} \{\beta(t+\Delta) = k-1\}\} = \left[\frac{k}{r_0}\right]\Delta + g(\Delta).$$

З початкових умов про роботу системи випливає, що стани ланцюга *β(t)* діляться на два класи. Стани $\{0,1,2,\ldots,r_0\text{-}2\}$ утворюють клас незворотніх станів (інформаційно-програмне накопичення), тому що процес *β(t)* попадаючи у множину станів $\{r_0\text{-}1,\ r_0,\ r_0+1,\ldots\}$, вже ніколи не повернеться до множини станів $\{0,1,2,\ldots,r_0\text{-}2\}$, оскільки обсяг інформаційних запасів щодо нормального функціонування системи не може зменшитися більш ніж до r_0-1 рівня в силу технологічного … функціонування системи. Математично це видно із співвідношення (2). Інші стани $\{r_0\text{-}1,\ r_0,\ r_0+1,\ldots\}$ утворюють замкнений клас сполучених станів, тому що як вихід з (2), від'ємні стрибки процесу *β(t)* можуть бути лише одиничними, що відповідає реальній ситуації, коли закінчення обслуговування відбувається по одному, тобто одинарно. Зі сказаного можна зробити висновок, що коли

$$p\{\beta(t)=k\}=p_k(t)$$

То, незалежно від розподілу β(t) ,границі

$$\lim_{t\to\infty} p_k(t) = p_k, \qquad k = 0,1,2,\ldots, \qquad (3)$$

За введених умов шукані ймовірності завжди існують, тобто ланцюг *β(t)* є ергодичним. Факт ергодичності ланцюга *β(t)* встановлюється теоремою.

Теорема. Якщо *β(0)* є $\{r_0\text{-}1,\ r_0,\ r_0+1\}$, то ланцюг Маркова *β(t)* має стаціонарний розподіл і значить, всі його стани $\{r_0\text{-}1,\ r_0,\ r_0+1,\ldots\}$ утворюють ергодичний клас.

Доведення. Розглянемо рівняння для визначення стаціонарних імовірностей $\{P_k\}$. Як слідує з співвідношення (2) вони мають такий вигляд

$$\lambda p_{r0-1} = p_{r0};$$
$$\left(\lambda + \left[\frac{k}{r_0}\right]\right)p_k = \left[\frac{k+1}{r_0}\right]p_{k+1} + \sum_{j=r-1}^{k-1} p_j\lambda_{k-j}, k \geq r_0. \qquad (4)$$

Припустимо $p_k=q_{k+1-r0}$, $k\geq r_0\text{-}1$. Тоді (4) набуває вигляду

$$hq_0 = q_1;$$
$$\left(\lambda + \left[\frac{m+r_0-1}{r_0}\right]\right)q_m = \left[\frac{m+r_0}{r_0}\right]q_{m+1} + \sum_{t=0}^{m-1} q_1\lambda_{m-t}, m \geq 1. \qquad (5)$$

Для зручності обчислень аналітичних перетворень та подальших викладок введемо твірні функції послідовностей λ_m і q_m, тобто

$$L(z) = \sum_{m=1}^{\infty} \lambda_m z^m, \theta(z) = \sum_{m=0}^{\infty} q_m z^m \ (|z| \leq 1). \qquad (6)$$

Згідно одержаних визначень (5) маємо

$$\frac{\lambda - L(z)}{1-z}\theta(z) = \sum_{m=0}^{\infty}\left[\frac{m+r_0}{r_0}\right]q_{m+1}z^m,$$

або в позначення правої частини

$$\theta'_{1/r_0}(z) = \frac{h - L(z)}{1-z}\theta(z), \qquad (7)$$

де для компактності виразу приймемо позначення

$$\theta'_{1/r_0}(z) = \sum_{m=0}^{\infty}\left[\frac{m+r_0}{r_0}\right]q_{m+1}z^m.$$

Перетворимо вираз, позначений $\theta'_{1/r0}(z)$ наступним чином: зважаючи на те, що ціла частина $\left[\frac{m+r_0}{r_0}\right]$ для будь-якого $m=nr_0+k$ є незмінною для всіх $k \in [0,r_0-1]$, перейдемо від сумування за індексом до індексу, а саме

$$\begin{aligned}\theta'_1(z) &= \sum_{m=0}^{\infty}\left[\frac{m+r_0}{r_0}\right]q_{m+1}z^m = \sum_{k=0}^{r_0-1}\sum_{n=0}^{\infty}\left[\frac{nr_0+k+r_0}{r_0}\right]q_{nr_0+k+1}\,z^{nr_0+k}\\ &= \sum_{k=0}^{r_0-1}\sum_{n=0}^{\infty}(n+1)q_{nr_0+k+1}z^{nr_0+k}\\ &= \frac{1}{r_0}\left\{\theta^1(z) + \sum_{k=0}^{r_0-1}(r_0-k+1)\sum_{n=0}^{\infty}q_{nr_0+k+1}z^{nr_0+k}\right\}\\ &= \frac{1}{r_0}\theta'(z) + \frac{1}{r_0 z}\sum_{k=1}^{r_0}(r_0-k)\sum_{n=0}^{\infty}q_{nr_0+k}z^{nr_0+k}.\end{aligned}$$

Тепер позначимо через $\sqrt[r_0]{1} = \varepsilon_0, \varepsilon_1, \varepsilon_2, \dots, \varepsilon_{r_0-1}$ корені r_0-го ступеня з одиниці, тобто

$$\varepsilon_k = \cos\frac{2\pi k}{r_0} + i\sin\frac{2\pi k}{r_0} \qquad (8)$$

($k=0,1,2,\dots,r_0-1$).

Оскільки сума k–их ступенів їх

$$\varepsilon_0^k + \varepsilon_1^k + \varepsilon_2^k + \cdots + \varepsilon_{r_0-1}^k = \begin{cases} r_0, \text{якщо } k \text{ без залишку ділиться на } r_0, \\ 0, \text{якщо } k \text{ не ділиться на } r_0, \end{cases}$$

то можна записати

$$\sum_{j=0}^{r_0-1}\varepsilon_j^{-k}\,\theta(\varepsilon_j z) = \sum_{j=0}^{r_0-1}\varepsilon_j^{-k}\sum_{m=0}^{\infty}q_m\,\varepsilon_j^m z^m = \sum_{m=0}^{\infty}q_m z^m\sum_{j=0}^{r_0-1}\varepsilon_j^{m-k} = r_0\sum_{n=0}^{\infty}q_{nr_0+k}z^{nr_0+k} \qquad (9)$$

Використовуючи співвідношення (6) – о(9) отримаємо

$$\frac{\lambda - L(z)}{1-z}\theta(z) = \frac{1}{r_0}\theta(z) + \frac{1}{zr_0^2}\sum_{k=1}^{r_0-1}(r_0-k)\sum_{j=0}^{r_0-1}\varepsilon_j^{-k}\,\theta(\varepsilon_j r),$$

або спростивши рівність і розв'язуючи її відносно похідної, маємо

$$\theta'(z) = r_0\frac{\lambda - L(z)}{1-z}\theta(z) - \frac{1}{zr_0}\sum_{t=1}^{r_0-1}t\sum_{j=0}^{r_0-1}\varepsilon_j^t\,\theta(\delta_j z) \qquad (10)$$

Оскільки для j є {1,2,…,r_0-1} має місце рівність

$$\sum_{j=1}^{r_0-1} r\varepsilon_j^t = \frac{\varepsilon_j}{(\varepsilon_j-1)^2}\left[(r_0-1)\varepsilon_j^{r_0} - r_0\delta_j^{r_0-1} + 1\right],$$

що виходить з тотожності

$$\sum nx^n = \frac{x}{(1-x)^2}[(N-1)x^N - Nx^{N-1} + 1](x \neq 1)$$

і рівності $\varepsilon_j^{r_0} = 1$,то маємо

$$\sum_{t=1}^{r_0-1} t\varepsilon_j^t = \frac{r_0}{\varepsilon_j - 1}(j = 1,2,\dots,r_0-1), \qquad (11)$$

що разом з (10) дозволяє записати

$$\theta'(z) = \left(r_0\frac{\lambda - L(z)}{1-z} - \frac{r_0-1}{2z}\right)\theta(z) + \frac{1}{z}\sum_{j=1}^{r_0-1}\frac{\theta(\varepsilon_j z)}{1-\varepsilon_j}. \qquad (12)$$

Відмітимо, що в частинному випадку при $r_0 = 1$ (коли не існує обсягу інформації для нормальної роботи системи, точніше технологічний процес не вимагає необхідних запасів інформаційних та програмних ресурсів) співвідношення (12) набуває вигляду

$$\theta'(z) = \frac{\lambda - L(z)}{1-z}\theta(z), \qquad (13)$$

що разом з умовою $\theta(1) = 1$ дає знайомий результат

$$\theta(z) = exp\left\{-\int_z^1 \frac{\lambda - L(u)}{1-u}du\right\}, \qquad (14)$$

який досить добре відомий в літературі для системи масового обслуговування з необхідною кількістю каналів. [5] Якщо L(z)=λz (тобто потік ординарний), то

$$\theta(z) = e^{h(z-1)}$$

І шуканий розподіл в цьому окремому випадку добре відомий тобто

$$p_k = q_k = e^{-\lambda}\frac{\lambda^k}{k!}(k \geq 0).$$

Маємо частковий побічний результат з ТМО, який одержаний раніше іншими авторами. [6] Нас цікавить загальний розв'язок поставленої задачі. А тому продовжимо займатися розв'язуванням отриманого диференційно-функціонального рівняння (10). Введемо позначення

$$\theta_j(z) = \theta\left(E_j z\right)\ (j = 0,1,2,\dots,r_0-1).$$

Підставляючи в (10) замість z значення ε_jz, отримаємо

$$\theta'_e(z) = \left(\varepsilon_e r_0\frac{\lambda - L(\varepsilon_e z)}{1-\varepsilon_e z} - \frac{r_0-1}{2z}\right)\theta_e(z) + \frac{1}{2}\sum_{j=0}^{r_0-1}\left(1-\varepsilon_j\right)^{-1}\theta_{j+k}(mod\ r_0)(z), \qquad (15)$$

(l=0,1,2,…,r_0-1).

Вводячи вектор-стовпчик (для зручності записаний рядком)

$$\bar{\theta}(z) = \{\theta_0(z), \theta_1(z), \dots, \theta_{r_0-1}(z)\}.$$

І матрицю

$$P(z) = \left\| \begin{matrix} P_{0,0}(z) & \dots & P_{0,r_0-1}(z) \\ \dots & \dots & \dots \\ P_{r_0-1,0}(z) & \dots & P_{r_0-1,r_0-1}(z) \end{matrix} \right\|,$$

де сегменти

$$P_{ee}(z) = \varepsilon_e z_0 \frac{\varepsilon - L(\varepsilon_e z)}{1 - \varepsilon_e z} - \frac{r_0 - 1}{2z},$$
$$P_{ee}(z) = z^{-1}(1 - \varepsilon_{k-1})^{-1},\ (k \neq l).$$

І корені з від'ємним індексом визначені $\varepsilon_{-k} = \varepsilon_k^{-1}$, можемо переписати систему лінійних диференціальних рівнянь (15) у матричному вигляді

$$\frac{d}{dz}\bar{\theta}(z) = p(z)\bar{\theta}(z). \quad (16)$$

Оскільки як при всіх l має місце $\theta_e(0) = q_0$, то систему (16) потрібно розв'язувати разом з початковою умовою

$$\bar{\theta}(0) = q_0\bar{e}, \quad (17)$$

де

$$\bar{e} = \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}.$$

Розв'язок системи (16), (17) (див. [7]) можливо подати у вигляді

$$\theta(z) = q_0\Omega_0^z(P)\bar{e}, \qquad (18)$$

де матриця $\Omega_0^z(P)$- матрицант, що відповідає матриці P(z) на проміжку (0,z). Згідно [7], $\Omega_0^z(P)$можна обчислювати за будь-яким із наступних правил:

$$\Omega_0^z(P) = \sum_{k=0}^{\infty}\left[\int_0^2 p(u)du\right],$$

$$\Omega_0^z(P) = \lim_{n\to\infty}\left[e^{\frac{z}{n}P(z)}e^{\frac{z}{n}P(\frac{(n-1)z}{n})}\dots e^{\frac{z}{n}P(\frac{z}{n})}\right],$$

$$\Omega_0^z(P) = \int_0^z [E + P(u)]du = \lim_{n\to\infty}\left[E + P(z)\frac{z}{n}\right]\left[E + P\left(\frac{(n-1)z}{n}\right)\frac{z}{n}\right]\dots\left[E + P\left(\frac{z}{n}\right)\frac{z}{n}\right],$$

де E – одинична матриця.

З приводу представлення (18) відмітимо наступне: цей вираз має невизначеність в нулі, тому вираз треба розуміти в сенсі правої границі. В дійсності $\Omega_0^z(P)$ не існує, так як елементи матриці P(z) в околі нуля не тільки не обмежені, а і до того ж не інтегровані через наявність в них доданку виду $\frac{c}{z}$. Однак границя $\lim_{\varepsilon\to+0}\Omega_E^z(p)\bar{e}$ існує оскільки:

а) при множинні матриці на е отримуємо вектор-стовпчик, елементи якого є сумою рядків матриці:

б) в матриці P(z) суми рядків вже не містять «недобрих» додатків типу e/z, тому що

$$\sum_{\substack{k=0 \\ k\neq 1}}^{r_0-1}\frac{1}{1 - \varepsilon_k - 1} - \frac{r_0 - 1}{2} = 0. \quad (19)$$

Дійсно, згідно з рішенням (11)

$$r_0 \sum_{\substack{k=0 \\ k\neq 1}}^{r_0-1} \frac{1}{1-\varepsilon_k-1} = r_0 \sum_{k=0}^{r_0-1} \frac{1}{1-\varepsilon_k} = -\sum_{t=1}^{r_0-1} t \sum_{k=1}^{r_0-1} \varepsilon'_k = -\sum_{t=1}^{r_0-1} t \sum_{k=1}^{r_0-1} \varepsilon_t^{tk}$$

$$= -\sum_{t=1}^{r_0-1} t \sum_{k=1}^{r_0-1} (\varepsilon_t)^k = -\sum_{t=1}^{r_0-1} t \frac{\varepsilon_t^{r_0}-\varepsilon_t}{\varepsilon_t-1} = \sum_{t=1}^{r_0-1} t \frac{r_0(r_0-1)}{2},$$

що рівносильно рівності (19).

Зі сказаного маємо, що (18) потрібно розуміти як

$$\theta(z) = q_0 \lim_{\varepsilon\to+0} \Omega_\varepsilon^z(p)\bar{e}.$$

Нехай матриця

$$\Omega_\varepsilon^z(p) = \left\| \bar{\omega}_{lk}^{(\varepsilon)}(z) \right\|, (l,k = 0,1,2,\dots,r_0-1),$$

має елементи, що задовольняють співвідношення.

$$\lim_{\varepsilon\to+0} \sum \bar{\omega}_{lk}^{(\varepsilon)}(z) = \overline{\omega_l}(z),$$

Тоді будемо мати:

$$\emptyset(z) = \theta_0(z) = q_0\bar{\omega}_0(z),$$

або, використовуючи умову нормування $\emptyset(1) = 1$, остаточно отримаємо

$$\emptyset(z) = \frac{\bar{\omega}_0(z)}{\bar{\omega}_0(1)}. \quad (20)$$

Тобто, стаціонарний розподіл ланцюга Маркова β_k існує. Його твірна функція, що повністю визначає шуканий розподіл співпадає з правою частиною отриманої рівності (20).

Цим доведено, що всі стани $\{r_0\text{-}1, r_0, r_0+1, \dots\}$ утворюють один ергодичний клас, тобто теорема повністю доведена.

Якщо розглядати окремий випадок – потік вимог ординарний ($L(z)=\lambda z$), то стаціонарний розподіл може бути знайдений в явному вигляді, тому що β_k в такому припущені є частковим випадком процесу розмноження і загибелі. Дійсно, в окремому частинному випадку, що розглядається

$$p_k\left(\lambda + \left[\frac{k}{r_0}\right]\right) = \lambda p_{k-1} + \left[\frac{k+1}{r_0}\right] p_{k+1}, (k \geq r_o - 1),$$

або

$$\lambda p_k - \left[\frac{k+1}{r_0}\right] p_{k+1} = \lambda p_{k-1} - \left[\frac{k}{r_0}\right] p_k, (k \geq r_o - 1). \quad (21)$$

Оскільки $\lambda p_{r0} - 1 = p_{r0}$, то з виразу (21) маємо

$$p_k = \frac{\lambda}{\left[\frac{k}{r_0}\right]} p_{k-1}, (k \geq r_0),$$

або, отримуючи вираз через значення p_{r_0-1}, маємо

$$p_k = \frac{\lambda^{k+1-r_0}}{\left[\frac{k}{r_0}\right]\left[\frac{k-1}{r_0}\right]\dots\left[\frac{r_0}{r_0}\right]} p_{r_0-1}, (k \geq r_0). \quad (22)$$

Використовуючи умову нормування $\sum_{k=r_0-1}^{\infty} p_k = 1$, останню рівність остаточно можна переписати у вигляді

$$p_k = \left(\sum_{l=r_0}^{\infty} \frac{\lambda^l}{\prod_{j=r_0}^{l-1} \left[\frac{j}{r_0}\right]} \right)^{-1} \frac{\lambda^{k+1}}{\prod_{j=r_0}^{k} \left[\frac{j}{r_0}\right]}, (k \geq r_0 - 1). \quad (23)$$

Зупинимось детальніше на ще одному окремому під випадку даного випадку, тобто розглянемо $r_0 = 2$. Неважко показати, що при цьому підвипадку величини p_k є коефіцієнтами розкладу в степеневі ряди бесселевих функцій чисто уявного аргументу. Дійсно з (22) при $r_0 = 2$ отримаємо

$$p_{2k} = c \frac{\lambda^{2k+1}}{\left[\frac{2}{2}\right]\left[\frac{3}{2}\right] \cdots \left[\frac{2k-1}{2}\right]\left[\frac{2k}{2}\right]} = c \frac{\lambda^{2k+1}}{k!\,(k-1)!},$$

$$p_{2k} = c \frac{\lambda^{2k}}{\left[\frac{2}{2}\right]\left[\frac{3}{2}\right] \cdots \left[\frac{2k-1}{2}\right]\left[\frac{2k}{2}\right]} = c \frac{\lambda^{2k}}{(k-1)!\,(k-1)!}.$$

Тоді в силу цих співвідношень можна записати рівності:

$$\sum_{k=1}^{\infty} p_{2k}\, z^{2k} = \lambda c \sum_{k=1}^{\infty} \frac{(\lambda z)^{2k}}{k!\,(k-1)!} = \lambda^2 cz \frac{(\frac{1}{2} 2\lambda z)^{1+2r}}{r!\,(r+1)!} = \lambda^2 cz I_1(2\lambda z);$$

$$\sum_{k=1}^{\infty} p_{2k-1} z^{2k-1} = \lambda c \sum_{k=1}^{\infty} \frac{(\lambda z)^{2k-1}}{(k-1)!\,(k-1)!} = \lambda^2 cz \sum_{r=0}^{\infty} \frac{(\frac{1}{2} 2\lambda z)^{2r}}{r!\,r!} = \lambda^2 cz I_0(2\lambda z),$$

а з цих рівностей виходить:

$$p(z) = \sum_{k=1}^{\infty} p_k z^k = z \frac{I_0(2\lambda z) + I_1(2\lambda z)}{I_0(2\lambda) + I_1(2\lambda)}, \quad (24)$$

з цього рівняння маємо

$$p_1 = \frac{1}{I_0(2\lambda) + I_1(2\lambda)}\ . \quad (25)$$

Одержані аналітичні результати дозволяють визначити стаціонарні імовірності станів процесів функціонування системи, які розглядаються.

Потрібно відмітити, що розрахункову формулу (23) в явному вигляді можна поширити (також узагальнити) для під випадку неординарного потоку з геометричним розподілом вимог у групі. Отримані аналітичні формули (20), (23)-(25) дозволяють знаходити стаціонарні ймовірності станів процесу функціонування СКБД, яка розглядалась та підсистеми, які є в її складі, при специфічних припущеннях, характерною серед яких є деякий початковий обсяг первинної інформації, що дорівнює r_0-1.

Висновки

Слід зауважити, що для практичного використання одержаних теоретичних аналітичних результатів немає принципових труднощів. Незважаючи на те, що вони не дуже оглядові та мало відчутні на простий чисельний дотик, бо містять неелементарні функції, при наявності сучасних ЕОМ та найрізноманітнішого програмного забезпечення, чисельно-графічні трактування одержаних формул і розв'язки, які в них входять, не є непереборною перепоною для одержання наглядного розв'язку та практичного використання в розрахунку та обґрунтуванні ефективності функціонування СКБД.

Список літератури

1. Козюра В.Д., Хорошко В.О., Шелест М.Є., Ткач Ю.М., Балюнов О.О. Захист інформації в комп'ютерних системах. Ніжин: Орхідея, 2020. 236с.
2. Браіловський М.М.,Зибін С.В, Пискун І.В., Хорошко В.О., Хохлачова Ю.Є. Технології захисту інформації. К: Компринт, 2021. 296с.
3. Опірський І.Р. Загальні проблеми прогнозування НСД в інформаційних системах держави. *Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні*. 2015. Вип. 2(30). С. 31-34.
4. Вентцель Е.С. Теория вероятностей. М., Наука 1969. 464с.
5. Анисимов В.В., Закусило О.К., Донченко В.С. Элементы теории массового обслуживания и ассиметричного анализа систем. К: Вища школа, 1998. 249с.
6. Хинчин А.Я. Работы по математической теории массового обслуживания. М: ФМЛ, 1993. 242с.
7. Гантмахер Ф.Ф. Теория матриц. М: Наука, 1997. 659с.

ASSESSMENT OF THE STATES OF FUNCTIONING OF THE STATE CYBERNETIC PROTECTION SYSTEM

V.O. Khoroshko, Yu.Ye. Khokhlachova

National Aviation University,
1, pr. Lubomir Guzar, Kyiv, 03058, Ukraine, e-mail: professor_va@ukr.net

In this work, mathematical methods of researching the process of functioning of the state cyber security system, accumulation and processing of information are considered. Taking into account the fact that in the conditions of Russia's war against Ukraine, the tasks of cyber protection of the state's information systems have gained considerable importance, and computer networks have become the field of information warfare. It is also shown that there are no fundamental difficulties for the practical use of the obtained theoretical analytical results. Despite the fact that they are not very comprehensive and not very perceptible to a simple numerical touch, because they contain non-elementary functions, in the presence of modern electronic computers and a wide variety of software, numerical and graphic interpretations of the obtained formulas and the solutions included in them are not is an insurmountable obstacle for obtaining a visual solution and practical use in calculating and justifying the effectiveness of the state's cyber security system.

Keywords: cyber security, state cyber security, state cyber security systems, assessment of system functioning states, mathematical methods of system functioning, efficiency of system functioning.

DOI 10.15276/imms.v12.no1-2.124
УДК 517.518.84

Informatics and Mathematical Methods in Simulation
Vol. 12 (2022), No. 1-2, pp. 124-131

ЗМЕНШЕННЯ ФЕНОМЕНУ ГІББСА ДВОВИМІРНИМИ АПРОКСИМАЦІЯМИ

І. В. Шапка, Т.С. Науменко

Український державний хіміко-технологічний університет
прос. Гагаріна, 8, Дніпро, 49005, Україна, e-mail: irinaschapka@ukr.net

В роботі запропоновано та обґрунтовано доцільність застосування феномену Гіббса. Це явище виникає на краю розриву функції, для якої проводиться аналіз. Розглядається створення способу побудови таких багатовимірних апроксимацій наближень та визначення множини коефіцієнтів ряду, необхідного для побудови наближення заданої структури. Визначено умови збіжності апроксимант наближуваних багатовимірних функцій, побудованих за розробленою методикою. Показано, що в розрахунках двовимірних апроксимацій застосування феномена Гіббса дає можливість значно знизити якість обробки зображень для більшості популярних графічних стандартів, оскільки вони використовують кінцеву суму гармонік. Стиснення зображення відіграє дуже важливу роль у багатьох технологічних програмах, наприклад, документи та медичні зображення, телевізійні відеоконференції тощо. Методи стиснення зображень часто поділяють на дві категорії: без втрат та з втратами. Методи без втрат зазвичай вибираються для програм, де важливо зберегти дуже дрібні деталі зображення. До них можна віднести медичні та космічні дослідження, дистанційне зондування. З іншого боку, методи з втратами застосовуються в ситуаціях, коли потрібен значний ступінь стиснення. Це стосується, наприклад, цифрової фотографії, де, як правило, втрата деяких деталей зображення не є критичною. Вибираючи алгоритм стиснення, важливо розібратись з його позитивними і негативними сторонами. Вибираючи алгоритми з втратою частини даних, необхідно чітко розуміти за яких умов зображення буде втрачати якість сприйняття людиною.Це пов'язано з тим, що нечіткість відбувається на границях контрасної різкої зміни і призводить до появи помилкових оптичних тіней та до неякісного аналізу при обробці результатів рентгенологічних і сонарних досліджень. Розроблено було двовимірний метод апроксимацій типу Паде, який зменшує явище Гіббса для гармонійного двовимірного ряду Фур'є. Такий підхід дозволяє розробити схему застосування методу, алгоритм обробки зображень і його ефективність. Завдяки цьому виникає можливість оптимізувати підрахунки та побудувати алгоритм перетворень.
Ключові слова: апроксимація Паде, феномен Гіббса, двовимірні ряди Фур’є, дискретне косинусне та синусне перетворення.

Вступ

Пошук оптимального рішення для конкретних задач вимагає обґрунтованого вибору найбільш доцільних методів. Говорячи про феномен Гіббса - це особлива поведінка одновимірного ряду Фур'є при розкладанні розривної періодичної функції та скорочуванні доданків за умови використання кінцевої кількісті членів [1,3-4,11]. Сам ряд для нескінченної кількості членів у точці розриву дає півсуму значень функції праворуч і ліворуч від розриву, а в усіх інших точках рівномірно і абсолютно наближає цю функцію до максимуму. У випадку викривлення відбувається викривлення поблизу точок розриву, які неможливо усунути шляхом збільшення кінцевої кількості доданків ряду.

Не можливо не відмітити, що для двовимірної апроксимації також існує феномен Гіббса, який значно підвищує якість обробки зображень для більшості популярних графічних стандартів, оскільки вони використовують кінцеву суму гармонік [2-4]. Доказом цьому можуть бути праці, присвячені викривленням, що відбуваються на кордонах різкої зміни контрасту і призводить до появи помилкових оптичних тіней [2,7-8]. Це позначається на якості аналізу при обробці результатів рентгенологічних і сонарних досліджень. Феномен Гіббса є тип артефакту магнітно-резонансної томографії,

який призводить до ряду ліній на магнітно-резонансному зображенні, паралельних різких і інтенсивних змін об'єкта, таким як спинномозкова рідина і інтерфейс череп-мозок [4]. Це свідчить тому, що тематика зменшення феномену Гіббса є актуальною.

Теорія наближення функцій математичної фізики є найбільш швидко розвиваючою сферою математики [1,6]. Традиційно апроксимація розглядається з використанням поліномів [1,6,9,10] і тригонометричних функцій [5]. Найбільш вдалою розробкою таких наближень є наближення дробово-раціональними функціями [1,6,9]. Інтерес до теорії дробово-раціональних наближень неухильно зростає в зв'язку з їх широким застосуванням в різних дослідженнях в галузі теоретичної фізики, прикладної механіки, геофізики і ін. [2,7] через можливість узагальненого підсумовування з використанням рядів і розширенням функцій, які повинні бути апроксимовані в області мероморфності.

В останній час великий інтерес приділяється розширенню класичної теорії наближення дробово-раціональними функціями на різні типи базисних функцій і різні методи побудови наближень типу Паде [1,9]. Вибір відповідного методу побудови апроксимації дозволяє у більшості випадках досягти істотного поліпшення корисних властивостей апроксимант для деяких виокремлених класів функцій [1,9].

Ми пропонуємо використовувати двовимірний метод наближення типу Паде, що дасть можливість зменшити явище Гіббса для гармонійного двовимірного ряду Фур'є.

Основна частина

Приведемо метод побудови наближень Паде-типу для гармонійного двовимірного ряду Фур'є.

Згідно з розрахунками [11], ми розглядаємо сепарабельний метричний простір Гільберта $L_2[(a_2,b_2)\times(a_2,b_2)]$ двовимірних комплексних функцій $f(x_1,x_2)$ комплексних змінних x_1 і x_2 з квадратною мірою на прямокутнику $(a_2,b_2)\times(a_2,b_2)$, який інтегрується на цьому прямокутнику. Межі прямокутника можуть бути кінцевими або нескінченними. В якості основи простору ми можемо вибрати скінчену множину функцій $B_1=\{e_{1k},k=\overline{1,\infty}\}$ і $B_2=\{e_{2j},j=\overline{1,\infty}\}$, які пов’язані між собою

$$B=\{e_{1k}e_{1j},k=\overline{\overline{1,\infty}},j=\overline{\overline{1,\infty}}\} \qquad (1)$$

Основні функції можуть бути представлені у вигляді тригонометричних функцій

$$e_{nk}=(e^{ix_n})^k=e^{ikx_n},n=1,2 \qquad (2)$$

Довільну функцію розглянутого простору можна розкласти по базису як двовимірний узагальнений степеневий ряд виду

$$f=\sum_{k,p=1}^{\infty} a_{kp}(e_{11})^k(e_{21})^p \qquad (3)$$

де f – розклад в степеневий ряд, a_{kp} – коефіцієнти степеневого ряду, e_{nk} – експоненціальна функція.

В [10] ми запропонували визначення функціоналу типу Паде в наступному вигляді.

Визначення. Припустимо, що дано двовимірний степеневий ряд $S=\sum_{k,p=1}^{\infty} a_{kp}(x_1)^k(x_2)^p$ (S – розклад в степеневий ряд) комплексних змінних x_1 і x_2 і пов'язаної з ними апроксимації Паде $P[m_1,n_1/m_2,n_2](x_1,x_2)$ правильному розумінні. Функціонал Паде-типу $GP_{GS}[m_1,n_1/m_2,n_2](f_1,f_2)$ пов'язаний з даними узагальненим

степеневим рядом $GS=\sum_{k,p=1}^{\infty} a_{kp}(f_1)^k(f_2)^p$ для комплексних функцій цих змінних визначається як

$$GP_{GS}[m_1,n_1/m_2,n_2](f_1,f_2)=P[m_1,n_1/m_2,n_2](x_1,x_2)|_{x_1=f_1,x_2=f_2} \quad (4)$$

Процес побудови здійснюється у такій послідовності:

1. Обираються типи базисів для окремих змінних B_1,B_2 та основа простору B.

2. Апроксимація функції f представляється у вигляді (3).

3. Для степеневого ряду двох комплексних змінних x_1 і x_2 з коефіцієнтами, що збігаються, апроксимація Паде $P[m_1,n_1/m_2,n_2](x_1,x_2)$ побудована в правильному розумінні.

4. Робиться підстановка базисних функцій в функціонал Паде-типу.

Запропонована схема дозволяє визначити набір коефіцієнтів ряду, необхідний і достатній для побудови апроксимант Паде-типу із заданою структурою чисельника і знаменника.

В теорії наближення функцій дробово-раціональними апроксимаціями прийнято розглядати збіжність в сенсі теорем типу Монтессуса де Болора [9], які визначають ефективне аналітичне продовження мероморфної функція за радіусом збіжності. Тригонометрична функція є періодичною і в складній формі завжди належить одиничному колу.

Крім того, розглядаються кусково-гладкі інтегровані функції, що саме по собі мається на увазі відсутність особливих точок типу полюсів або по суті особливих точок. Доказ збіжності Паде-типу до значення самої функції в цьому випадку тривіально, оскільки базисні функції не мають особливих точок (за винятком степеневих функцій у нескінченності). Єдине обмеження - це випадок, коли особливі точки змінної, яка згодом замінюється тригонометричною функцією, лежать всередині одиничного кола.

Автори робіт по наближенням Фур'є-Паде в основному розглядають максимальне торкання тригонометричного полінома гладкої функції з постійно спадаючими коефіцієнтами і апроксимації Фур'є-Паде [11]. У цьому випадку продовження тригонометричних функцій не належить до одиничного кола. Крім того, вони розглядають голоморфні функції [5] без особливих точок.

В іншому випадку ми аналізуємо збіжність першого типу. Функції e_{nk} не мають особливих точок (за винятком степеневих функцій). Єдиний випадок, який потрібно дослідити, - це випадок, коли по суті особливі точки в змінній, яка згодом замінюється тригонометричною функцією, лежать всередині одиничного кола [5]. Оскільки в цьому випадку одновимірний ряд, що складається з коефіцієнтів a_{kp} розбігається відносно індексу цієї змінної, визначення цього випадку не складне.

При оцінці коефіцієнтів збіжності двовимірного апроксиматора до функції, що апроксимується за коефіцієнтами використовується значення швидкості зменшення коефіцієнтів вихідного ряду [3,6,12]. У разі побудови апроксимацій Паде $P[m_1,n_1/m_2,n_2](x_1,x_2)$ за схемою [1,6] використовуємо набори коефіцієнтів двовимірних рядів, які правильно перераховуються для монотонно зростаючого мінімуму розглянутих показників m_1, n_1, m_2 і n_2. На обмеженому прямокутнику $(a_2,b_2)\times(a_2,b_2)$, основні функції обох типів є функціями обмеженої варіації, тому швидкість спадання коефіцієнтів розкладення можна визначити методом [1].

Розглянемо етапи обробки зображення двовимірних сигналів.

Вхідне зображення розкладається на спектральні компоненти за допомогою дискретного косинусного або синусного перетворення [5].

Далі обираємо розмір області на цілочисельній решітці (рис. 1), з розміром якої безпосередньо пов’язана кількість рівнянь, які необхідно згенерувати. Для створення

алгоритму автоматичного генерування системи рівнянь необхідно використовувати відповідну формулу. Для цього розглянемо узагальнену апроксимацію Паде відносно рядів з двома змінними, запропоноване Чисхолмом [13].

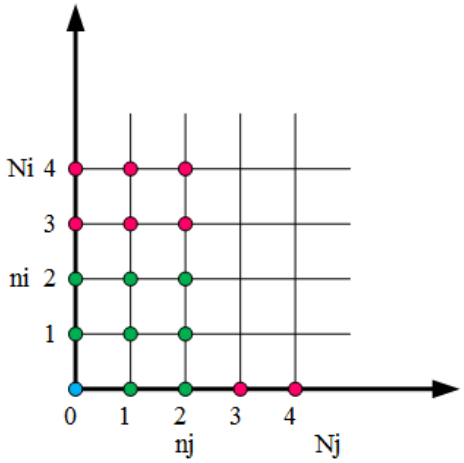


Рис. 1. Цілочисельна решітка для області *ni*, *nj* = 3

Якщо *f(x,y)*– функція двох змінних з фронтальним розкладанням в степеневий ряд виду

$$f(x,y)=\sum_{\alpha,\beta=0}^{\infty} a_{\alpha\beta}x^{\alpha}y^{\beta} \qquad (5)$$

то *N* - наближення Чисхолма записується у вигляді

$$f_{N,N}(x,y)=\frac{P_N(x,y)}{Q_N(x,y)}=\frac{\sum_{\mu}^{N}\sum_{\nu}^{N} c_{\mu\nu}x^{\mu}y^{\nu}}{\sum_{\sigma}^{N}\sum_{\tau}^{N} b_{\sigma\tau}x^{\sigma}y^{\tau}} \qquad (6)$$

Коефіцієнти $c_{\mu\nu}$ та $b_{\sigma\tau}$ ($c_{\mu\nu}$, $b_{\sigma\tau}$ – коефіцієнти ряду Чисхолма) визначаються з рівнянь

$$\sum_{\sigma=0}^{\gamma}\sum_{r=0}^{\delta} b_{\sigma r}a_{\gamma-\sigma,\delta-r}=c_{\gamma\delta},, \quad (\gamma,\delta=0,1,2,\ldots,2m;1\le\gamma+\delta\le 2m) \qquad (7)$$

$$\sum_{\sigma=0}^{\gamma}\sum_{r=0}^{\delta}\left(b_{\sigma r}a_{\gamma-\sigma,\delta-r}+b_{r\sigma}a_{\delta-r,\gamma-\sigma}\right)=0, \quad (\gamma=1,2,\ldots,m;\gamma+\delta=2m+1) \qquad (8)$$

де a_{00}=1 [13] З рівняння була виведена формула:

$$\sum_{i=0}^{ni+1}\sum_{j=0}^{nj+1}\left(q_{i,j}a_{Ni-i,Nj-j}+q_{i,j}a_{Nj-j,Ni-i}\right)=0 \qquad (9)$$

Розв’язок даної системи рівнянь являє собою матрицю коефіцієнтів *q*.

Зробимо розрахунок коефіцієнтів p за знайденими коефіцієнтами q відповідно до виразу ($p_{g,d}$ – коефіцієнти апроксимації Паде):

$$p_{g,d}=\sum_{s=0}^{g}\sum_{r=0}^{d}\left(g_{s,r}\cdot a_{g-s,d-r}\right). \qquad (10)$$

Коефіцієнти p та q зберігаються до файлу.

Для відновлення зображення виконується реконструкція зображення: дві матриці коефіцієнтів p і q підставляються до формули:

$$SF(x,y)=0.5Re\left[\frac{\sum_{ii}^{ni}\sum_{jj}^{nj}\left[p_{ii,jj}(e^{ii\cdot 1ix}\cdot e^{jj\cdot 1jy})\right]}{\sum_{ii}^{ni}\sum_{jj}^{nj}\left[q_{ii,jj}(e^{ii\cdot 1ix}\cdot e^{jj\cdot 1jy})\right]}+\frac{\sum_{ii}^{ni}\sum_{jj}^{nj}\left[p_{ii,jj}(e^{ii\cdot 1ix}\cdot e^{-jj\cdot 1jy})\right]}{\sum_{ii}^{ni}\sum_{jj}^{nj}\left[c_{ii,jj}(e^{ii\cdot 1ix}\cdot e^{-jj\cdot 1jy})\right]}\right] \qquad (11)$$

Наш аналіз дає можливість зробити деякі висновки щодо практичного використання наближення Паде-типу та про його переваги.

Перш за все, ми можемо бачити низький рівень шуму для наближення Паде-типу в порівнянні з рядами Фур'є для синуса (рис. 2 (а) проти рис. 2 (б)) і косинуса (рис. 2 (в) проти рис. 2 (г)) випадків.

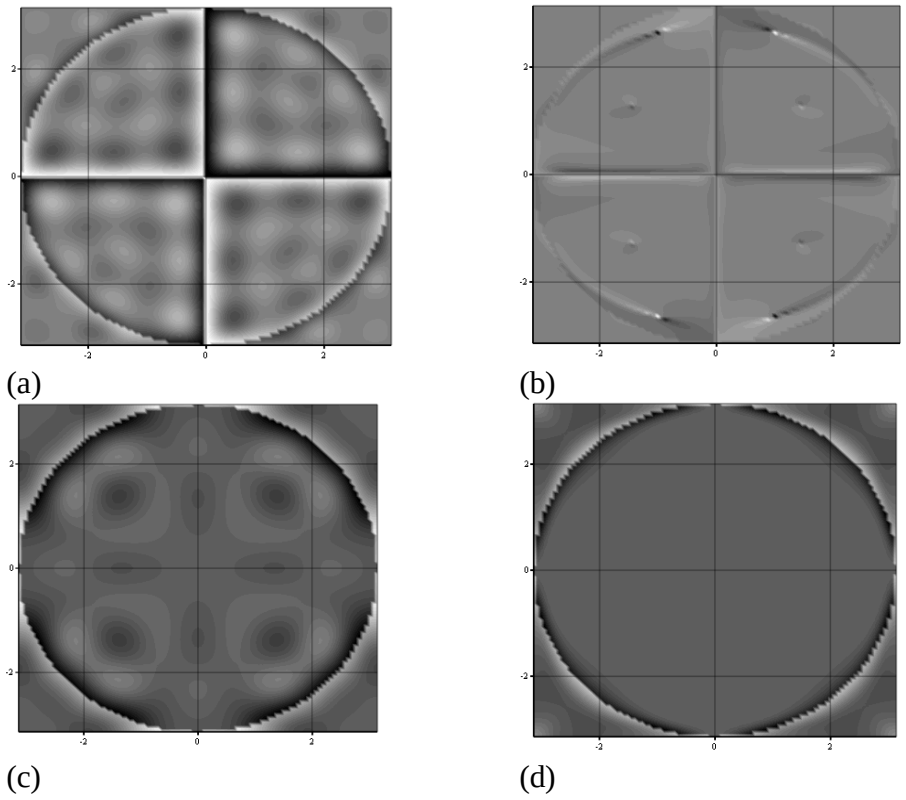


Рис. 2. Викривлення між шаблонними функціями і їх аппроксимацією для (a) синусоїдальних рядів Фур'є, (б) апроксимації Паде-типу для синусоїдальних рядів, (c) косинусних рядів Фур'є, (d) апроксимації Паде-типу для косинусних рядів.

По-друге, використання апроксимації Паде-типу призводить до різкого зменшення числа параметрів апроксимант без втрати точності (навіть з її ростом). Дійсно, коли ми використовуємо ряд Фур'є з рівним числом N гармонік в обох напрямках, ми отримуємо наступне число параметрів n_F:

$$n_F=N^2 \qquad (12)$$

Використання апроксимант Паде-типу з рівними порядками чисельника і знаменника $N/2$ дає нам наступну кількість параметрів n_P:

$$n_p=2\left(\frac{N}{2}\right)^2-1=\frac{N^2}{2}-1 \qquad (13)$$

Таким чином, ми отримуємо зменшення кількості параметрів більш ніж удвічі:

$$\frac{n_F}{n_p}>2 \qquad (14)$$

Це дуже важливо для зберігання зображень при цифровій обробці сигналів і може дати нам теоретичну основу для створення нового ефективного формату зображення, такого як добре відомий формат JPEG (JPEG - Joint Photographic Experts Group).

Висновки

Запропоновано схему використання методу двовимірних аппроксимаций Паде-типу, що дає можливість зменшити феномен Гіббса для гармонійного двовимірного ряду Фур'є. Розглянуто застосування методу і його ефективність. Показана працездатність методики і можливість її застосування для підвищення точності розрахунків. Дослідження дає нам можливість зробити висновки про переваги практичного використання апроксимації Паде-типу для обробки зображень.

Список літератури

1. Timan A. F. Theory of approximation of functions of a real variable. New York: MacMillan, 1963. 631 p.

2. Mitra S. K. Digital Signal Processing. New York: McGraw-Hill, 2001. 866 p.

3. Olevska Yu. B., Olevskyi V. I., Shapka I. V. and Naumenko T. S. Application of two-dimensional Padé-type approximants for reducing the Gibbs phenomenon. *AIP Conference Proceedings*. 2019. URL: https://doi.org/10.1063/1.5130816

4. Veraart J., Fieremans E., Jelescu I. O. Gibbs ringing in diffusion MRI. *Magnetic Resonance in Medicine*. 2016. Vol.76, P.301-314. URL: https://doi:10.1002/mrm.25866

5. Andrianov I., Olevskyi V. and Olevska Yu. Analytic approximation of periodic Ateb functions via elementary functions in nonlinear dynamics. *8th International Conference for Promoting the Application of Mathematics in Technical and Natural Sciences*. 2016. P. 040001-1–040001-7. URL: https://doi.org: 10.1063/1.4964964

6. Bazilevich Y.N. The Best Reduction of Matrices to Block-Triangular Form for Hierarchical Decomposition Problems. *Cybern Syst Anal*. 2017. URL: https://doi.org/10.1007/s10559-017-9947-1

7. Mossakovskii V. I., Mil'tsyn A. M., Olevskii V. I. Automating the analysis of results of a holographic experiment. *Strength of Materials*. 1994. No.26(5). P.385-391. URL:https://doi.org/10.1007/BF02207425

8. Drobakhin O. O. and Olevskyi O. V. Verification of applicability in space domain of the inverse filtering with evolution control for reconstruction of images obtained by radar scanning. *AIP Conference Proceedings*. 2018. URL:https://doi.org/10.1063/1.5007392

9. Baker J. and Graves-Morris P. Padé approximants. N. Y: Cambridge University Press, 1996, 746 p.

10. Andrianov I. V., Olevskyi V. I., Shapka I. V. Naumenko T. S. Technique of Padé-type multidimensional approximations application for solving some problems in mathematical physics. *AIP Conference Proceedings*. 2018. URL: https://doi.org/10.1063/1.5064886

11. Sablonniere P. Padé-Type Approximants for Multivariate Series of Functions. Lecture Notes in Mathematics, 1071. New York: Springer, 1984. pp. 238–251.

12. Olevskyi V. I. Asymptotic method of modeling of thin walled shells based on 2D Padé approximations. *6th International Conference for Promoting the Application of Mathematics in Technical and Natural Sciences*. 2014. P. 110-126. URL: https://doi.org/10.1063/1.4902265

13. Chisholm S.R. Rational approximations determined from a double power series. Mathematics of Computing, 1973. No 27 (124) P.841–848. URL: https://doi.org/10.1090/S0025-5718-1973-0382928-6

REDUCTION OF THE GIBBS PHENOMENON BY TWO-DIMENSIONAL APPROXIMATIONS

I. V. Shapka, T.S. Naumenko

Ukrainian State Chemical and Technological University
avg. Gagarina, 8, Dnipro, 49005, Ukraine, e-mail: irinaschapka@ukr.net

In this work, we propose and substantiate the expediency of using the Gibbs phenomenon. This phenomenon occurs at the edge of the function gap, for the analysis of which. The creation of a method of constructing such multidimensional approximations to the approximation and determination of the set of coefficients of the series necessary to construct an approximation of the given structure is considered. The conditions of convergence of approximants of approximate multidimensional functions constructed according to the developed method are determined. It is shown that in the calculations of two-dimensional approximations, the use of the Gibbs phenomenon makes it possible to significantly reduce the quality of image processing for most popular graphic standards, since they use a finite sum of harmonics. Image compression plays a very important role in many technological applications, such as document and medical imaging, television video conferencing, etc. Image compression methods are often divided into two categories: lossless and lossy. Lossless methods are usually chosen for applications where it is important to preserve very fine image details. These include medical and space research, remote sensing. On the other hand, lossy methods are used in situations where a significant degree of compression is required. This applies, for example, to digital photography, where, as a rule, the loss of some image details is not critical. Image compression methods are often divided into two categories: lossless and lossy. Lossless methods are usually chosen for applications where it is important to preserve very fine image details. These include medical and space research, remote sensing. On the other hand, lossy methods are used in situations where a significant degree of compression is required. This applies, for example, to digital photography, where, as a rule, the loss of some image details is not critical. When choosing a compression algorithm, it is important to understand its positive and negative sides. When choosing algorithms with the loss of part of the data, it is necessary to clearly understand under what conditions the image will lose the quality of human perception. This is due to the fact that blurring occurs at the borders of a sharp change in contrast and leads to the appearance of false optical shadows and poor-quality analysis when processing the results of radiological and sonar research. A two-dimensional Padé-type approximation method was developed, which reduces the Gibbs phenomenon for a harmonic two-dimensional Fourier series. This approach makes it possible to develop a method application scheme, an image processing algorithm and its effectiveness. Thanks to this, it becomes possible to optimize calculations and build a transformation algorithm.

Keywords: Padé approximation, Gibbs phenomenon, two-dimensional Fourier series, discrete cosine and sine transform.

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

Том 12, номер 1-2, 2022. Одеса – 132 с., іл.

ИНФОРМАТИКА И МАТЕМАТИЧЕСКИЕ МЕТОДЫ В МОДЕЛИРОВАНИИ

Том 12, номер 1-2, 2022. Одесса – 132 с., ил.

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Volume 12, No. 1-2, 2022. Odesa – 132 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 № 13 від 24.06.2022)

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