

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська політехніка»

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ
МЕТОДИ В МОДЕЛЮВАННІ

INFORMATICS AND MATHEMATICAL
METHODS IN SIMULATION

Том 11, № 3

Volume 11, No. 3

Одеса – 2021
Odesa – 2021

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

Published 4 times a year

Заснований Одеським національним політехнічним університетом у 2011 році

Founded by Odessa National Polytechnic University in 2011

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

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

Головний редактор: *А.А. Кобозєва*

Editor-in-chief: *A. Kobozeva*

Заступник головного редактора:

Associate editor:

С.А. Положаєнко

S. Polozhaenko

Відповідальний редактор:

Executive editor:

О.А. Стопакевич

O. Stopakevych

Редакційна колегія:

Editorial Board:

І.І. Бобок, Д. Джухар, А.А. Кобозєва,

I. Bobok, J. Juhar, A. Kobozeva,

В.Ф. Ложечніков, В.В. Любченко,

V. Lozhechnikov, V. Liubchenko, V. Pavlenko,

В.Д. Павленко, В.В. Палагін,

V. Palahin, S. Polozhaenko, O. Rybalsky,

С.А. Положаєнко, О.В. Рибальський,

A. Sokolov, B. Speransky, O. Stopakevych,

А.В. Соколов, В.О. Сперанський,

O. Fomin

О.А. Стопакевич, О.О. Фомін

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

© Національного університет «Одеська політехніка», 2021

ЗМІСТ/CONTENTS

- | | | |
|---|-----|--|
| СТЕГANOГРАФІЧНИЙ МЕТОД
МНОЖИННОГО ДОСТУПУ НА
ОСНОВІ КОДОВОГО УПРАВЛІННЯ ТА
ЧАСТОТНИХ РОЗСТАНОВОК
А.В. Соколов | 147 | MULTIPLE ACCESS
STEGANOGRAPHIC METHOD BASED
ON CODE CONTROL AND FREQUENCY
ARRANGEMENTS
Sokolov A. |
| ЗАСТОСУВАННЯ ЗАСОБІВ МАСОВОЇ
ІНФОРМАЦІЇ У ІНФОРМАЦІЙНО-
ПСИХОЛОГІЧНІЙ ВІЙНІ
М.М. Браїловський, Т.П. Пірцхалава,
В.О. Хорошко, Ю.Є. Хохлачова | 162 | APPLICATION OF THE MEDIA IN THE
INFORMATION-PSYCHOLOGICAL
WAR
Brailovsky M., Pirtskhalava T.,
Khoroshko V., Khokhlachova Yu. |
| МЕТОДИКА ОЦІНКИ ЗАХИЩЕНОСТІ
ІНФОРМАЦІЙНИХ СИСТЕМ
С.В. Батечко, О.Ю. Лебедева, В.В. Зоріло | 173 | METHODOLOGY FOR ASSESSING THE
SAFETY OF INFORMATION SYSTEMS
Batechko S., Lebedeva O., Zorilo V. |
| ВИЯВЛЕННЯ ПОРУШЕНЬ ЦІЛІСНОСТІ
ЦИФРОВОГО ЗОБРАЖЕННЯ В
КОНТЕКСТІ ЦИФРОВОЇ
КРИМІНАЛІСТИКИ
Д.Ю. Берія, М.Є. Войтовецька,
Н.Г. Козаченко, В.В. Зоріло,
О.Ю. Лебедева | 181 | DETECTION OF VIOLATIONS OF
INTEGRITY OF DIGITAL
IMAGE IN THE CONTEXT OF DIGITAL
FORENSICS
Beriiia D., Voitovetska M., Kozachenko N.,
Zorilo V., Lebedeva O. |
| РОЗРОБКА МЕТОДУ ДЛЯ
ПІДВИЩЕННЯ СТІЙКОСТІ ДО
СТАТИСТИЧНОГО СТЕГANOАНАЛІЗУ З
ВИКОРИСТАННЯМ ГЕНЕРАТИВНО-
ЗМАГАЛЬНИХ МЕРЕЖ
Ю.І. Даракчі, Н.І. Кушніренко,
О.Є. Плачінда | 191 | DEVELOPMENT OF A METHOD TO
INCREASE RESISTANCE TO
STATISTICAL STEGANALYSIS USING
GENERATIVE
ADVERSARIAL NETWORK
Darakchi Yu., Kushnirenko N., Plachinda O. |
| СИСТЕМА МОДЕЛЮВАННЯ
КІБЕРАТАКИ ПІДМІНОЮ ОРС-
СЕРВЕРА ПРИ КОМП'ЮТЕРНОМУ
УПРАВЛІННІ ТЕХНОЛОГІЧНИМИ
УСТАНОВКАМИ
А.А. Зозуля, О.А. Стопакевич,
А.О. Стопакевич | 200 | SIMULATION SYSTEM OF
CYBERATTACK BY OPC SERVER
REPLACEMENT
IN COMPUTER CONTROL SYSTEMS OF
TECHNOLOGICAL PLANTS
Zozulya A., Stopakevich O., Stopakevich A. |

МОДИФІКАЦІЇ АЛГОРИТМУ
ВИЯВЛЕННЯ РУХУ КАМЕРИ
В.В. Кордюк, О.Ю. Лебедєва

209

MODIFICATIONS OF THE CAMERA
MOTION DETECTION ALGORITHM
Kordyuk V., Lebedieva O.

МЕТОД РОЗВ'ЯЗКУ ЗАДАЧІ ПРО
ВИБІР КОНТЕЙНЕРА, ЩО
ЗАБЕЗПЕЧУЄ
МАЛУ ЧУТЛИВІСТЬ
СТЕГАНОВІДОМЛЕННЯ ДО
ЗБУРНИХ ДІЙ
О.Ю. Надвоцький, А.А. Кобозєва

216

A COVER IMAGE SELECTION
METHOD PROVIDING STEGO-OBJECT
ROBUSTNESS TO VARIOUS IMAGE
PROCESSING ATTACKS
Nadvotskiy A., Kobozeva A.

РОЗРОБКА ЗАХИЩЕНОЇ
АВТОМАТИЗОВАНОЇ ВЕБ-СИСТЕМИ
ТЕСТУВАННЯ ЗНАНЬ
С.О. Перерва, К.О. Трифонова

227

DEVELOPMENT OF A SECURE
AUTOMATED WEB-BASED
KNOWLEDGE TESTING SYSTEM
Pererva S., Tryfonova K.

МОДЕЛЮВАННЯ ОРГАНІЗАЦІЙНИХ
ЗАХОДІВ ДЛЯ СТВОРЕННЯ
ПОЛІТИКИ БЕЗПЕКИ ОРГАНІЗАЦІЇ З
ВИКОРИСТАННЯМ БІЗНЕС-ПРОЦЕСІВ
В.В. Радущ, О.Ю. Лебедєва,
Н.І. Кушніренко, В.В. Зоріло

239

MODELING ORGANIZATIONAL
ACTIVITIES TO CREATE AN
ORGANIZATION'S SECURITY POLICY
USING BUSINESS PROCESSES
Radush V., Lebedieva O., Kushnirenko N.,
Zorilo V.

**MULTIPLE ACCESS STEGANOGRAPHIC METHOD BASED
ON CODE CONTROL AND FREQUENCY ARRANGEMENTS****A.V. Sokolov**National Odessa Polytechnic University
Ukraine, Odessa, 65044, Shevchenko Ave., 1, e-mail: radiosquid@gmail.com

The development, as well as the wider practical application of modern steganography, leads to the need to create steganographic methods with multiple access, which would be able to ensure the simultaneous transmission and division of information from several users in a steganographic channel. The currently known multiple-access steganographic methods are based on MC-CDMA technology and do not show how exactly the embedding and extraction of additional information should be performed. The purpose of this paper is to develop a multiple-access steganographic method based on code control and frequency arrangements. This purpose was achieved through the development of a steganographic method with code control and the use of frequency arrangements based on double-cyclic Reed-Solomon codes over Galois fields $GF(q)$, which provides separate embedding of information by each user at any time which is convenient for him using a personal frequency arrangement. It was proposed to construct the frequency arrangements on the basis of Reed-Solomon codes over the Galois fields $GF(5)$ and $GF(13)$. The characteristics of the developed method are researched, within which it is shown that the PSNR of the resulting steganographic message depends on the number of users simultaneously transmitting information through the steganographic channel. With the number of simultaneously operating users $N \leq 8$, the PSNR values remain at an acceptable level. During the operation of the proposed steganographic method, the occurrence of intra-system interference in the steganographic channel was detected with the number of users simultaneously transmitting information $N > q$, however, when using frequency arrangements based on the Reed-Solomon code over the $GF(13)$, their effect is insignificant with a practically justified number of divided channels. The developed steganographic method is a rational solution if it is necessary to organize a steganographic channel with multiple access and can provide flexible resource allocation: the operation of the required number of users with a given bandwidth and the required perception reliability.

Keywords: steganography, code control, multiple access, code division, frequency arrangement.

Introduction and statement of the problem

Steganography is one of the most important components of modern information security systems [1], which not only makes it impossible to read information without the presence of a secret key, but also allows to hide the very fact of secret information transference. The rapid development of the theory and practice of steganography, which is currently taking place, has led to the emergence of many effective steganographic methods with a high level of performance [2], resistance to common attacks (lossy compression, noise, blurring, scaling, etc.) [3...6], as well as providing a high level of reliability of steganographic message perception [7]. A property of these methods is the ability to transmit additional information in a steganographic message, intended for one specific user.

Nevertheless, in order to solve some practical tasks [8, 9], it becomes necessary to transmit in one steganographic message information intended for more than one user, i.e. organize in the steganographic channel a multiple access. One of the effective methods for solving this problem is the use of MC-CDMA technology using the Walsh-Hadamard transform, which was proposed in [8], and was further developed in [10]. The disadvantages of this technology include the fact that the number of users is strictly regulated and equal to $N = 2^k = 2, 4, 8, 16, \dots$. MC-CDMA

technology does not show exactly how the embedding and extraction of additional information should be performed, which is another significant disadvantage of the mentioned method of code division of channels.

As it is shown in this paper, the mentioned disadvantages of using MC-CDMA technology in steganographic methods can be eliminated by combining the advantages of the steganographic method with code control, as well as the frequency arrangement technology used to build asynchronous address communication systems based on time-frequency matrices (TFM signals) [11]. Such signals are used in terrestrial, satellite and other communication systems, in command radio control systems as well as in the air traffic control systems.

The purpose of this paper is to develop a multiple-access steganographic method based on code control and frequency arrangements.

Definitions and constructions

The proposed in this paper method uses the relationship established in [3] between the two-dimensional and one-dimensional Walsh-Hadamard transforms: up to a coefficient $1/N$, the two-dimensional Walsh-Hadamard transform $W = H'XH'^T$ can be represented in terms of the one-dimensional Walsh-Hadamard transform using the following relation $\tilde{W} = \tilde{X}H_{N^2}$, where H_N is the Walsh-Hadamard matrix of order $N = 2^k$, which is constructed according to Sylvester's construction

$$H_{2^k} = \begin{bmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{bmatrix}, \quad H_1 = 1, \quad (1)$$

while $H'_N = \frac{1}{\sqrt{N}}H_N$, and operator $\tilde{A}$ denotes writing the matrix A of order $N \times N$ as a row vector of length N^2 by sequential rows concatenation.

As the basis of the developed steganographic method with multiple access, it is proposed to use the steganographic method with the code control [3], the main idea of which is to use the linearity property of the Walsh-Hadamard transform

$$\begin{aligned} \tilde{M} &= \tilde{X} + \tilde{D}; \\ \tilde{M}H_{N^2} &= \tilde{X}H_{N^2} + \tilde{D}H_{N^2}, \end{aligned} \quad (2)$$

where X is a block of a matrix-container of size $\mu \times \mu$, D is a block of additional information of size $\mu \times \mu$, M is a block of a steganographic message of size $\mu \times \mu$. In this paper we consider the block size $\mu \times \mu = 8 \times 8$.

Using additional coding of the matrix D with codes having a given form of Walsh-Hadamard transform coefficients, it is possible to embed the additional information into a given Walsh-Hadamard transform coefficient of the container image X . Thus, by modifying the codewords that represent the bits of the steganographic message, it is possible to manipulate the properties of the steganographic method: the embedding of information into medium or low frequencies makes it possible to achieve resistance to attacks by compression, noise, and

blurring, while the embedding of information into higher frequency components allows a higher probability to guarantee the reliability of the steganographic message perception.

In [3], an explicit correspondence was established between the transformants of the Walsh-Hadamard transform, as well as transformants of the discrete cosine transform (DCT), which has

$$\frac{\mu}{2} \times \frac{\mu}{2} = 4 \times 4$$

the following form for the case of the size of transformations

DCT		Walsh-Hadamard Transform	DCT		Walsh-Hadamard Transform
(1,1)	$\leftrightarrow$	(1,1)	(3,1)	$\leftrightarrow$	(4,1)
(1,2)	$\leftrightarrow$	(1,3)	(3,2)	$\leftrightarrow$	(4,2)
(1,3)	$\leftrightarrow$	(1,4)	(3,3)	$\leftrightarrow$	(4,4)
(1,4)	$\leftrightarrow$	(1,2)	(3,4)	$\leftrightarrow$	(4,2)
(2,1)	$\leftrightarrow$	(3,1)	(4,1)	$\leftrightarrow$	(2,1)
(2,2)	$\leftrightarrow$	(3,3)	(4,2)	$\leftrightarrow$	(2,3)
(2,3)	$\leftrightarrow$	(3,4)	(4,3)	$\leftrightarrow$	(2,4)
(2,4)	$\leftrightarrow$	(3,2)	(4,4)	$\leftrightarrow$	(2,2)

For example, to ensure the reliability of perception, the embedding of information must be done so that just the most high-frequency Walsh-Hadamard transformants undergo modifications.

In Table 1, we present the codewords used in the steganographic method developed in this paper, which affect the transformants (1,2); (1,4); (2,1); (2,2); (2,3); (2,4); (3,2); (3,3); (3,4); (4,1); (4,2); (4,3); (4,4) (excluding the lowest-frequency transformants (1,1); (1,3); (3,1)).

Table 1

Codewords aimed at modifying the given Walsh-Hadamard transformant

$T_{4,(1,2)}^+$	$T_{4,(1,4)}^+$	$T_{4,(2,1)}^+$	$T_{4,(2,2)}^+$
$\begin{bmatrix} 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 \end{bmatrix}$	$\begin{bmatrix} 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 \end{bmatrix}$	$\begin{bmatrix} 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \end{bmatrix}$
$T_{4,(2,3)}^+$	$T_{4,(2,4)}^+$	$T_{4,(3,2)}^+$	$T_{4,(3,3)}^+$
$\begin{bmatrix} 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \end{bmatrix}$	$\begin{bmatrix} 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \\ -1 & 1 & -1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 \\ -1 & -1 & 1 & 1 \end{bmatrix}$
$T_{4,(3,4)}^+$	$T_{4,(4,1)}^+$	$T_{4,(4,2)}^+$	$T_{4,(4,3)}^+$
$\begin{bmatrix} 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \\ -1 & 1 & 1 & -1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \\ -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 \\ -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 \end{bmatrix}$
$T_{4,(4,4)}^+$	—	—	—
$\begin{bmatrix} 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \\ -1 & 1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$	—	—	—

Such a number of selected frequency components is chosen because of the fact that in this paper we consider the use of two frequency arrangement codes: the first code assumes the largest number of users operating in the system, using 13 frequency components, while the second code uses five frequency components and provides the best reliability of perception.

Note that the application of the codewords presented in Table 1 in accordance with (2) causes a targeted effect on the corresponding Walsh-Hadamard transformant, while the remaining transformants of the steganographic message remain unchanged.

Each codeword shown in Table 1 is the frequency component for the first frequency arrangement code f_{1i} and the second f_{2i} , respectively

$$\begin{array}{llll}
 T_{4,(1,2)}^+ & \leftrightarrow & f_{10} & \\
 T_{4,(1,4)}^+ & \leftrightarrow & f_{11} & \\
 T_{4,(2,1)}^+ & \leftrightarrow & f_{12} & \\
 T_{4,(2,2)}^+ & \leftrightarrow & f_{13} & \\
 T_{4,(2,3)}^+ & \leftrightarrow & f_{14} & T_{4,(2,2)} \leftrightarrow f_{20} \\
 T_{4,(2,4)}^+ & \leftrightarrow & f_{15} & T_{4,(2,3)} \leftrightarrow f_{21} \\
 T_{4,(3,2)}^+ & \leftrightarrow & f_{16} & T_{4,(2,4)} \leftrightarrow f_{22} \\
 T_{4,(3,3)}^+ & \leftrightarrow & f_{17} & T_{4,(3,2)} \leftrightarrow f_{23} \\
 T_{4,(3,4)}^+ & \leftrightarrow & f_{18} & T_{4,(4,2)} \leftrightarrow f_{24} \\
 T_{4,(4,1)}^+ & \leftrightarrow & f_{19} & \\
 T_{4,(4,2)}^+ & \leftrightarrow & f_{110} & \\
 T_{4,(4,3)}^+ & \leftrightarrow & f_{111} & \\
 T_{4,(4,4)}^+ & \leftrightarrow & f_{112} &
 \end{array} \quad (4)$$

These frequency components f_i of the size $\frac{\mu}{2} \times \frac{\mu}{2} = 4 \times 4$ are used in the developed method as elements to form codewords of size $\mu \times \mu$, which is unique for each user in accordance with the frequency arrangement rule

$$\begin{array}{|c|c|}
 \hline
 f_{i_1} & f_{i_2} \\
 \hline
 f_{i_3} & f_{i_4} \\
 \hline
 \end{array}, \quad (5)$$

where the vector of indices $[i_1, i_2, i_3, i_4]$ is unique for each user and is determined by the corresponding frequency arrangement.

In modern asynchronous address communication systems for constructing frequency arrangement codes with good correlation properties, non-binary cyclic Bose–Chaudhuri–Hocquenghem codes also known as Reed–Solomon codes (RS-codes) [11] have become widespread.

In this paper, considering an example of the block length $\mu \times \mu = 8 \times 8$, we present two options for generating the frequency arrangement code: the first one is constructed over the Galois field $GF(13)$, which allows you to ensure the maximum number of users operating in the system while maintaining acceptable perception reliability, and the second one is constructed

over the Galois field $GF(5)$, which allows you to provide the best reliability of perception with a smaller number of users operating in the system.

Let's form the first frequency arrangement code based on the RS-code over the Galois field $GF(13)$ with the following parameters: codeword length $N=12$, number of information digits $K=2$, primitive element $\theta=2$, code distance $d=12-2+1=11$. The generating polynomial of a given code is determined by the following relationship

$$g(z) = \prod_{i=1}^{d-1} (z - \theta^i) = \prod_{i=1}^{10} (z - 2^i) = (z-2)(z-4)(z-8)(z-3)(z-6)(z-12)(z-11)(z-9)(z-5)(z-10) = 11 + 7z + 12z^2 + 9z^3 + 3z^4 + 4z^5 + 6z^6 + 10z^7 + 5z^8 + 8z^9 + z^{10}. \quad (6)$$

On the basis of the generating polynomial (6), we construct a generating matrix, the first row of which consists of the coefficients of the generating polynomial, the remaining $K-1$ rows are defined as a non-cyclic shift to the right by 1 of the previous row, while all unfilled elements of the generating matrix are considered as equal to 0

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

The first row in the generating matrix G will be called as the basic codeword and will be denoted as C_1 . Based on the property of double cyclicity of RS-codes, we can construct all other codewords by cyclic shifts of the basic codeword in time and frequency. Further, each of the codewords of the RS-code is truncated, as a result of which we obtain its first four symbols that we will use as the frequency arrangement.

In this case, the total number of available frequency arrangements generated using the RS-code over the Galois field $GF(q)$ is

$$J = q(q-1) = 13 \cdot 12 = 156. \quad (8)$$

For brevity in Table 2 these frequency arrangements are presented with the radix equal to 13 ($10 \rightarrow A, 11 \rightarrow B, 12 \rightarrow C$).

Thus, using the method of additional coding of information with codewords (5) using frequency arrangements based on the RS-code, presented in Table 2 it is theoretically possible to provide the operation of 156 users in the steganographic channel.

For example, in this case, the first user in the system will transmit information using a frequency arrangement $[B7C9] \rightarrow [11 \ 7 \ 12 \ 9]$, on the basis of which, in accordance with (4), we form

codewords of the form (5) $[f_{111} \ f_{17} \ f_{112} \ f_{19}] = [T_{4,(4,3)}^+, T_{4,(3,3)}^+; T_{4,(4,4)}^+, T_{4,(4,1)}^+]$, where the symbol “;” means horizontal concatenation, and the symbol “,” means vertical concatenation.

Thus, the first user in the system encodes information using the following codewords (T_1^+ for transmitting bit “0” and T_1^- for transmitting bit “1”)

Table 2

Representation of the frequency arrangement code based on the RS-code over the Galois field $GF(13)$ in the form of cyclic shifts in time and frequency of the basic codeword C_1

B7C9	7C93	C934	9346	346A	46A5	6A58	A581	5810	810B	10B7	0B7C
C80A	80A4	0A45	A457	457B	57B6	7B69	B692	6921	921C	21C8	1C80
091B	91B5	1B56	B568	568C	68C7	8C7A	C7A3	7A32	A320	3209	2091
1A2C	A2C6	2C67	C679	6790	7908	908B	08B4	8B43	B431	431A	31A2
2B30	B307	3078	078A	78A1	8A19	A19C	19C5	9C54	C542	542B	42B3
3C41	C418	4189	189B	89B2	9B2A	B2A0	2A06	A065	0653	653C	53C4
4052	0529	529A	29AC	9AC3	AC3B	C3B1	3B17	B176	1764	7640	6405
5163	163A	63AB	3AB0	AB04	B04C	04C2	4C28	C287	2875	8751	7516
6274	274B	74BC	4BC1	BC15	C150	1503	5039	0398	3986	9862	8627
7385	385C	85C0	5C02	C026	0261	2614	614A	14A9	4A97	A973	9738
8496	4960	9601	6013	0137	1372	3725	725B	25BA	5BA8	BA84	A849
95A7	5A71	A712	7124	1248	2483	4836	836C	36CB	6CB9	CB95	B95A
A6B8	6B82	B823	8235	2359	3594	5947	9470	470C	70CA	0CA6	CA6B

$$T_1^+ = \left[\begin{array}{cccc|cccc} 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ \hline 1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 \\ -1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 \\ -1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 \end{array} \right], \quad T_1^- = \left[\begin{array}{cccc|cccc} -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 \\ \hline -1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 \\ -1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 \end{array} \right]. \quad (9)$$

Let us now proceed to the construction of the second frequency arrangement code, for which we construct a RS-code over the Galois field $GF(5)$ with the following parameters: codeword length $N=4$, number of information digits $K=2$, primitive element $\theta=3$, code distance $d=N-K+1=3$. We define the generating polynomial of the given code

$$\begin{aligned} g(z) &= \prod_{i=1}^{d-1} (z - \theta^i) = \prod_{i=1}^2 (z - 3^i) = \\ &= (z - 3)(z - 4) = 2 + 3z + z^2. \end{aligned} \quad (10)$$

Similarly, to the case of the first frequency arrangement code, based on the generating polynomial (10), we construct the generating matrix

$$G = \begin{bmatrix} 2 & 3 & 1 & 0 \\ 0 & 2 & 3 & 1 \end{bmatrix}, \quad (11)$$

on the basis of which we construct all the $J = 20$ codewords of the Reed-Solomon code (Table 3). Since each of these codewords has a length $N = 4$ that corresponds to construction (5), for this code the codewords do not need to be truncated and can be used unchanged.

Table 3Representation of the RS-code over the Galois field $GF(5)$

$C_1 = [2 \ 3 \ 1 \ 0]$	$C_6 = [3 \ 1 \ 0 \ 2]$	$C_{11} = [1 \ 0 \ 2 \ 3]$	$C_{16} = [0 \ 2 \ 3 \ 1]$
$C_2 = [3 \ 4 \ 2 \ 1]$	$C_7 = [4 \ 2 \ 1 \ 3]$	$C_{12} = [2 \ 1 \ 3 \ 4]$	$C_{17} = [1 \ 3 \ 4 \ 2]$
$C_3 = [4 \ 0 \ 3 \ 2]$	$C_8 = [0 \ 3 \ 2 \ 4]$	$C_{13} = [3 \ 2 \ 4 \ 0]$	$C_{18} = [2 \ 4 \ 0 \ 3]$
$C_4 = [0 \ 1 \ 4 \ 3]$	$C_9 = [1 \ 4 \ 3 \ 0]$	$C_{14} = [4 \ 3 \ 0 \ 1]$	$C_{19} = [3 \ 0 \ 1 \ 4]$
$C_5 = [1 \ 2 \ 0 \ 4]$	$C_{10} = [2 \ 0 \ 4 \ 1]$	$C_{15} = [0 \ 4 \ 1 \ 2]$	$C_{20} = [4 \ 1 \ 2 \ 0]$

A steganographic system with multiple access based on the presented Reed-Solomon code (Table 3) can theoretically ensure the operation of $J = 20$ users with help of five frequency components.

Algorithms for embedding and extraction of information

Based on the theoretical material presented, we will describe algorithms for embedding and extraction of information for the developed steganographic method with multiple access.

Information embedding algorithm

Step 1. An ensemble of codewords of size $\frac{\mu}{2} \times \frac{\mu}{2}$ is formed (Table 1), which are acting purposefully on the given transformants of the Walsh-Hadamard transform, as well as an ensemble of frequency arrangements based on the RS-code over the Galois field $GF(q)$ (Table 2 or Table 3). The choice of the base q depends on the number of users operating in the system, as well as on the number of modified Walsh-Hadamard transformants participating in the transmission of information.

Step 2. To each user A_z , $z = 1, 2, \dots, J$ registered in the steganographic system, a frequency arrangement is allocated for transmitting information over the steganographic channel. On the basis of given frequency arrangement, in accordance with construction (5) and Table 1, the user generates codewords T_z^+ and T_z^- of size $\mu \times \mu$.

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

$$M_k = X_k + D_k. \quad (12)$$

The undoubted advantage of the developed steganographic method is the fact that different users, using their frequency arrangements, can embed information independently of each other at any time convenient for them. The number of subscribers simultaneously operating in the system can also be easily scaled.

Let's consider a specific example of information embedding using the developed steganographic method.

Let an ensemble of codewords of size 4×4 to be formed, which consists of codewords $T_{4,(2,2)}, T_{4,(2,3)}, T_{4,(2,4)}, T_{4,(3,2)}, T_{4,(4,2)}$, as well as an ensemble of frequency arrangements (Table 2). Consider the operation of two users A_1 and A_2 with the following frequency arrangements: $C_1 = \begin{bmatrix} 2 & 3 & 1 & 0 \end{bmatrix}$ and $C_2 = \begin{bmatrix} 3 & 4 & 2 & 1 \end{bmatrix}$. Let these users perform embedding of information bits $d_{1,k} = 1, d_{2,k} = -1$ into the block of the container image

$$X_k = \begin{bmatrix} 213 & 214 & 215 & 216 & 215 & 214 & 214 & 214 \\ 214 & 215 & 215 & 216 & 215 & 214 & 216 & 214 \\ 214 & 214 & 215 & 215 & 214 & 213 & 214 & 214 \\ 215 & 215 & 216 & 217 & 214 & 214 & 214 & 214 \\ 214 & 214 & 215 & 215 & 214 & 217 & 216 & 216 \\ 214 & 214 & 215 & 215 & 216 & 216 & 214 & 216 \\ 215 & 216 & 215 & 216 & 215 & 215 & 214 & 216 \\ 214 & 216 & 215 & 214 & 215 & 215 & 216 & 215 \end{bmatrix}. \quad (13)$$

On the basis of a given frequency arrangement C_1 , as well as an ensemble of codewords of size 4×4 , the first user generates codewords of size 8×8 intended for transmitting an additional information bit $d_{1,k}$

$$T_1^+ = \left[\begin{array}{cccc|cccc} 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 \\ -1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 \\ -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 \\ \hline 1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 \\ -1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 \\ -1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 \end{array} \right], \quad T_1^- = \left[\begin{array}{cccc|cccc} -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 \\ -1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 \\ \hline -1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 \\ -1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 \end{array} \right], \quad (14)$$

while the second user generates his codewords based on the frequency arrangement C_2

$$T_2^+ = \left[\begin{array}{cccc|cccc} 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 \\ \hline 1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 \\ -1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 \\ -1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 \end{array} \right], \quad T_2^- = \left[\begin{array}{cccc|cccc} -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ \hline -1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 \\ -1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 \end{array} \right]. \quad (15)$$

Based on (12), the first user embeds a bit of information $d_{1,k} = 1$, while the second user embeds a bit of information $d_{2,k} = -1$, as a result of which we get a steganographic message

$$M_k = X_k + T_1^+ + T_2^- = \begin{bmatrix} 213 & 214 & 213 & 218 & 215 & 214 & 214 & 214 \\ 212 & 217 & 215 & 216 & 217 & 212 & 218 & 212 \\ 216 & 212 & 215 & 215 & 214 & 213 & 214 & 214 \\ 215 & 215 & 218 & 215 & 212 & 216 & 212 & 216 \\ 214 & 216 & 215 & 213 & 214 & 215 & 218 & 216 \\ 214 & 212 & 215 & 217 & 216 & 218 & 212 & 216 \\ 215 & 218 & 215 & 214 & 215 & 213 & 216 & 216 \\ 214 & 214 & 215 & 216 & 215 & 217 & 214 & 215 \end{bmatrix}. \quad (16)$$

We note here that the degree of perturbation of the container image when embedding information by the developed method depends on the following factors: the number of users simultaneously transmitting the additional information, and specific values of the additional information bits.

Remark. In view of the fact that most of the images used today are represented using the RGB model, where 1 byte is allocated for encoding of each color (each color component is represented by numbers in the range $[0, \dots, 255]$), in the case of the presence in the block of boundary values for this range (0 or 255), the mentioned block is not used in the process of steganographic transformation.

Let's move on to the information extraction algorithm.

Information Extraction Algorithm

Step 1. In accordance with the relationship between the two-dimensional and one-dimensional Walsh-Hadamard transforms, each user A_z of the steganographic system, in accordance with the frequency arrangement code issued to him, selects the rows of the Walsh-Hadamard matrix H_{N^2} of the order N^2 , which are denoted as $\{h_{z,1}\}, \{h_{z,2}\}, \{h_{z,3}\}, \{h_{z,4}\}$.

Step 2. The user finds the difference matrix of the steganographic message M and the container image X , splits the resulting difference matrix into blocks Δ_k of size $\mu \times \mu$.

Step 3. The user divides each of the blocks of the difference matrix Δ_k into 4 sub-blocks of size $\frac{\mu}{2} \times \frac{\mu}{2}$, in accordance with the construction (5). By sequentially concatenating the rows, each of the resulting four subblocks is represented as a vector $\{\delta_{z,i}\}, i = \{1, 2, 3, 4\}$ of length μ^2 .

Step 4. The user A_z calculates the vector P in accordance with the following formula

$$P_{z,k} = [p_1 \quad p_2 \quad p_3 \quad p_4],$$

$$p_i = \sum_{k=1}^{\mu^2} \delta_{j,k} h_{j,k}, i = \{1, 2, 3, 4\}. \quad (17)$$

Step 5. The user calculates the intended data bit embedded in the block Δ_k using the following formula

$$d_{z,k} = \text{sign} \left(\sum_{i=1}^4 p_i \right). \quad (18)$$

As an example, let us extract the information embedded by the first and second users in the steganographic message (16). To do this, in accordance with the selected frequency arrangement codes, we form a set of Walsh functions for the first user

$$\begin{aligned}
 \{h_{1,1}\} &= \{+1 \ -1 \ -1 \ +1 \ -1 \ +1 \ +1 \ -1 \ +1 \ -1 \ -1 \ +1 \ -1 \ +1 \ +1 \ -1\}; \\
 \{h_{1,2}\} &= \{+1 \ -1 \ +1 \ -1 \ +1 \ -1 \ +1 \ -1 \ -1 \ +1 \ -1 \ +1 \ -1 \ +1 \ -1 \ +1\}; \\
 \{h_{1,3}\} &= \{+1 \ +1 \ -1 \ -1 \ -1 \ -1 \ +1 \ +1 \ +1 \ +1 \ -1 \ -1 \ -1 \ -1 \ +1 \ +1\}; \\
 \{h_{1,4}\} &= \{+1 \ -1 \ +1 \ -1 \ -1 \ +1 \ -1 \ +1 \ +1 \ -1 \ +1 \ -1 \ -1 \ +1 \ -1 \ +1\},
 \end{aligned} \tag{19}$$

and also, for the second user

$$\begin{aligned}
 \{h_{2,1}\} &= \{+1 \ -1 \ +1 \ -1 \ +1 \ -1 \ +1 \ -1 \ -1 \ +1 \ -1 \ +1 \ -1 \ +1 \ -1 \ +1\}; \\
 \{h_{2,2}\} &= \{+1 \ -1 \ +1 \ -1 \ -1 \ +1 \ -1 \ +1 \ -1 \ +1 \ -1 \ +1 \ +1 \ -1 \ +1 \ -1\}; \\
 \{h_{2,3}\} &= \{+1 \ -1 \ -1 \ +1 \ -1 \ +1 \ +1 \ -1 \ +1 \ -1 \ -1 \ +1 \ -1 \ +1 \ +1 \ -1\}; \\
 \{h_{2,4}\} &= \{+1 \ +1 \ -1 \ -1 \ -1 \ -1 \ +1 \ +1 \ +1 \ +1 \ -1 \ -1 \ -1 \ -1 \ +1 \ +1\}.
 \end{aligned} \tag{20}$$

Further, both users calculate the matrix of the difference between the steganographic message and the container image, and divide it into blocks of size $\mu \times \mu$. In the case of our example, the considered block will have the form

$$\Delta_k = M_k - X_k = \begin{bmatrix} 0 & 0 & -2 & 2 & 0 & 0 & 0 & 0 \\ -2 & 2 & 0 & 0 & 2 & -2 & 2 & -2 \\ 2 & -2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & -2 & -2 & 2 & -2 & 2 \\ 0 & 2 & 0 & -2 & 0 & -2 & 2 & 0 \\ 0 & -2 & 0 & 2 & 0 & 2 & -2 & 0 \\ 0 & 2 & 0 & -2 & 0 & -2 & 2 & 0 \\ 0 & -2 & 0 & 2 & 0 & 2 & -2 & 0 \end{bmatrix}. \tag{21}$$

Based on the obtained matrix Δ_k , the first and second users select the corresponding vectors $\{\delta_{z,i}\}, i = \{1, 2, 3, 4\}$

$$\begin{aligned}
 \{\delta_{1,1}\} &= [0 \ 0 \ -2 \ 2 \ -2 \ 2 \ 0 \ 0 \ 2 \ -2 \ 0 \ 0 \ 0 \ 0 \ 2 \ -2]; \\
 \{\delta_{1,2}\} &= [0 \ 0 \ 0 \ 0 \ 2 \ -2 \ 2 \ -2 \ 0 \ 0 \ 0 \ 0 \ -2 \ 2 \ -2 \ 2]; \\
 \{\delta_{1,3}\} &= [0 \ 2 \ 0 \ -2 \ 0 \ -2 \ 0 \ 2 \ 0 \ 2 \ 0 \ -2 \ 0 \ -2 \ 0 \ 2]; \\
 \{\delta_{1,4}\} &= [0 \ -2 \ 2 \ 0 \ 0 \ 2 \ -2 \ 0 \ 0 \ -2 \ 2 \ 0 \ 0 \ 2 \ -2 \ 0].
 \end{aligned} \tag{22}$$

Further, using (17), as well as his own set of vectors $\{h_{1,i}\}$ (19), the first user calculates the vector $P_{1,k}$, as well as, in accordance with expression (18), the data bit intended for him

$$P_{1,k} = [16 \ 16 \ 16 \ 16] \rightarrow d_{1,k} = 1. \quad (23)$$

Similarly, the vector $P_{2,k}$, as well as the intended data bit, is calculated by the second user

$$P_{2,k} = [-16 \ -16 \ -16 \ -16] \rightarrow d_{2,k} = -1. \quad (24)$$

Characteristics of the developed multiple-access steganographic method

One of the most important properties of the developed steganographic method is the possibility of simultaneous operation of such a number of users, which is necessary at the given moment, with the total number J of registered users, each of which has its own frequency arrangement.

Nevertheless, with an increase in the number of simultaneously operating users in the system, the information load on the image-container increases, and, accordingly, its quality deteriorates. As a measure of the quality of a steganographic message, we will take the PSNR [1] indicator, which is determined in accordance with the following formula

$$PSNR = 20 \lg \left(\frac{255}{\sqrt{MSE}} \right), \quad (25)$$

Where

$$MSE = \frac{1}{nm} \sum_i \sum_j |X(i, j) - M(i, j)|^2. \quad (26)$$

In Fig. 1 a graph of the dependence of PSNR of steganographic messages on the number of simultaneously operating in the system users is shown.

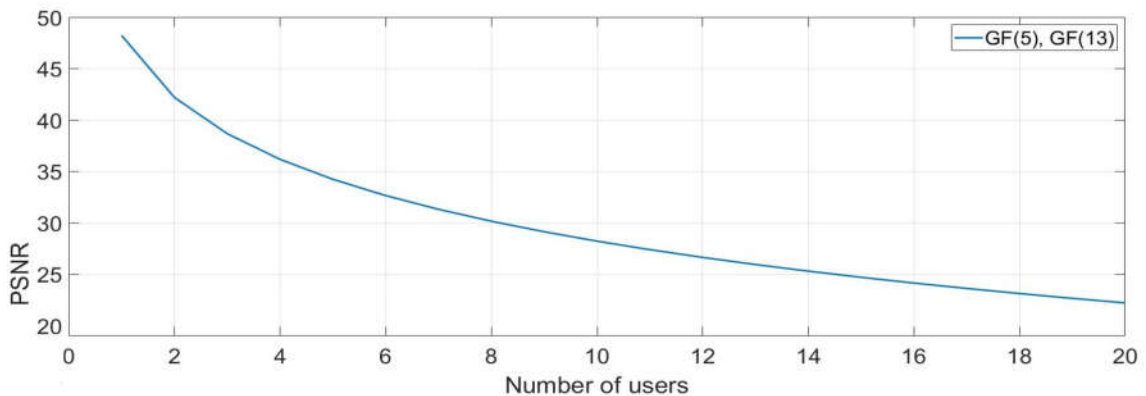


Fig. 1. Graph of dependence of PSNR of steganographic message on the number of simultaneously operating users

To obtain this data, an experiment was performed using 500 lossless TIFF images from the NRCS database [12], into each of which information coming from a different number of users was embedded, after which the PSNR of the received steganographic message was measured.

The analysis of data displayed on Fig. 1 shows that an increase in the number of simultaneously operating users leads to a drop in the PSNR of a steganographic message, and this process is the same both for the case of using the frequency arrangement code based on the RS-code over the Galois field $GF(5)$ and over the Galois field $GF(13)$. Note that with the number of simultaneously operating users $N \leq 8$, the PSNR values remain at an acceptable level. In the case of using frequency arrangements based on the RS-code over the Galois field $GF(5)$, information is embedded into the high-frequency components, therefore, even with a value $PSNR \approx 30 \text{ dB}$, the reliability of perception remains at a sufficient level, which can be clearly seen in Fig. 2.

Moreover, in Fig. 2 into the blue RGB component of an image of size 2592x3872 with a total number of shared channels $N = 20$ we embedded in total a $20 \cdot 324 \cdot 484 \text{ bits} = 3136320 \text{ bits} = 382.85 \text{ KB}$ of information.

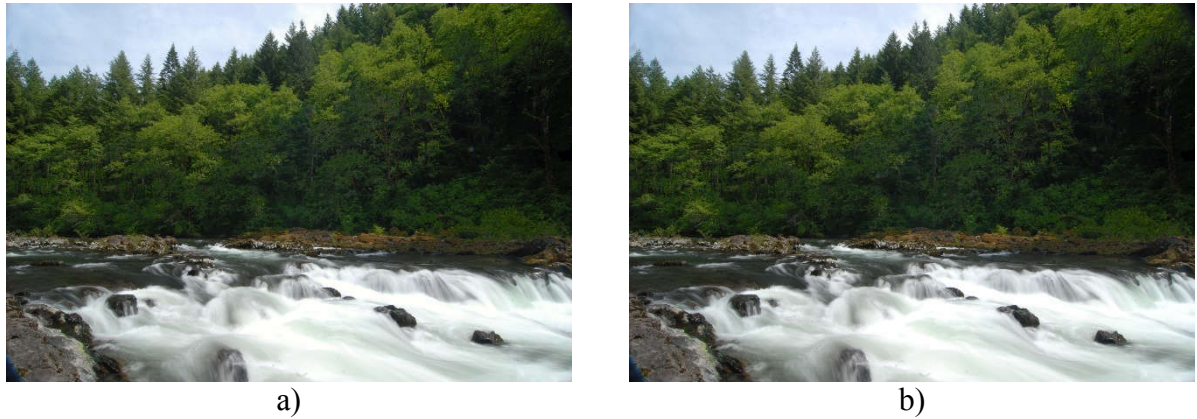


Fig. 2. An example of a steganographic message with embedded information from $N = 20$ users (a), as well as the original container (b)

Subjective ranking of the images shown in Fig. 2 does not reveal any artifacts or visual differences from the original container image in the steganographic message.

A property of asynchronous address communication systems, which is reflected in the developed steganographic method with multiple access, is the presence of intra-system interference: forming into a common stream, pulses of other channels can accidentally form a code combination of a given channel, leading to the appearance of a corresponding interference. Another type of intra-system noise is interference suppression and nonlinear pulse suppression.

The experiments performed show that intra-system interference appears when the number of users simultaneously operating in the system exceeds the value q . In Fig. 3 we show the dependence of the number of errors (in %) occurring in the communication channel (channel of each of the users) depending on the number of users operating in the system for frequency arrangement codes based on RS-codes over the Galois fields $GF(5)$ and $GF(13)$.

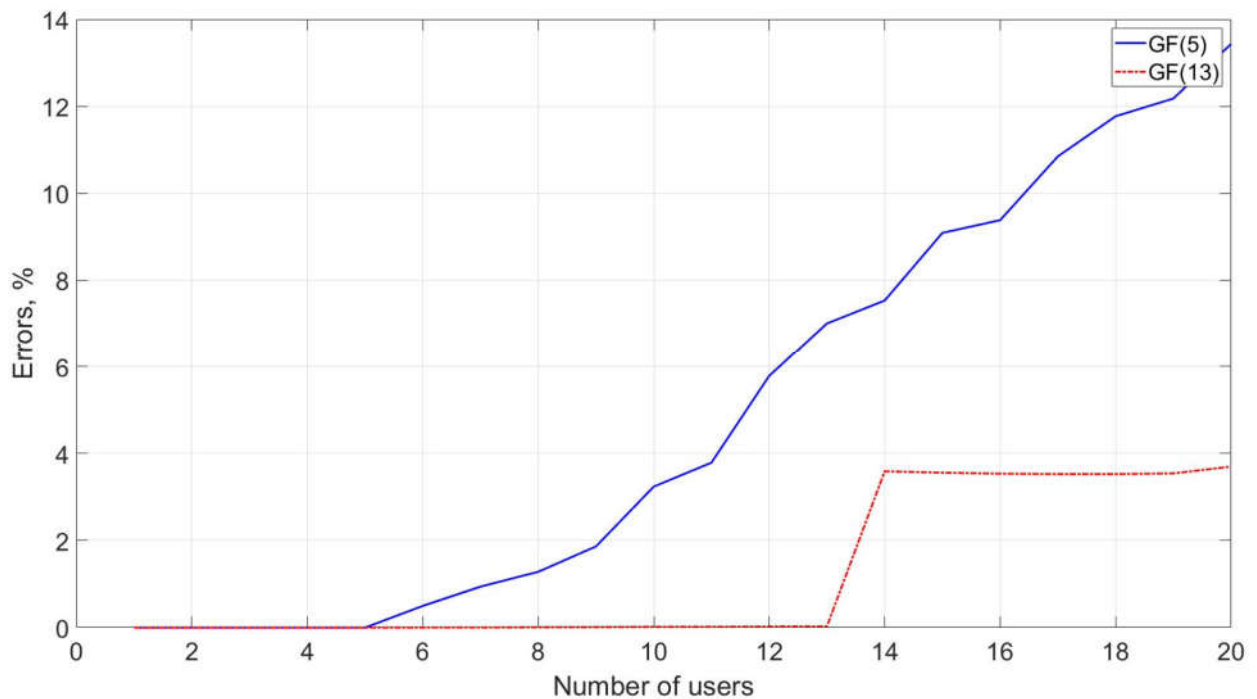


Fig. 3. Graphs of the dependence of the percentage of errors resulting from intra-system interference on the number of users

Analysis of the data presented in Fig. 3 shows that frequency arrangements based on the RS-code over the Galois field $GF(5)$ allow simultaneous operation of $N = 5$ users without the occurrence of intra-system interference, while frequency arrangements based on the RS-code over the Galois field $GF(13)$ allow simultaneous operation of $N = 13$ users without the occurrence of intra-system interference, however, even for values of the number of simultaneously operating users $N = 20$ for these frequency arrangements (Table 2), the level of intra-system interference remains acceptable, and the number of errors that occur does not exceed 3.7%.

Conclusions

Let us note the main results obtained in this paper:

1. In contrast to the well-known analogs that perform code division of channels regardless of the embedding of information into the container, in this paper we developed a fully-fledged steganographic method with multiple access based on code control and frequency arrangements. The developed steganographic method that provides the separate embedding (absence of the embedding) of information by each user at any time which is convenient for him using a personal frequency arrangement. It is proposed to use RS-codes over the Galois fields $GF(5)$ and $GF(13)$ as the frequency arrangement codes, which ensure the maximum reliability of perception and the largest number of simultaneously operating users.

2. The characteristics of the developed method are researched, within the framework of which it is shown that the PSNR of the resulting steganographic message depends on the number of users simultaneously transmitting information through the steganographic channel. With the number of simultaneously operating users $N \leq 8$, the PSNR values remain at an acceptable level. The existence of intra-system interference in the steganographic channel was detected with the number of simultaneously transmitting information users $N > q$. However, in the case of using frequency arrangements based on RS-codes over the Galois field $GF(13)$ with the number of users $N = 20$, the number of errors generated by intra-system interference does not exceed 3.7%.

3. The developed steganographic method is a rational solution if it is necessary to organize a steganographic channel with multiple access and can provide flexible resource allocation: the operation of the required number of users with a given bandwidth (by allocating several communication channels to individual users) and the necessary reliability of perception (by increasing or reducing the number of simultaneously operating users).

References

1. Kobozeva A.A., Horoshko V.A. Information security analysis. Kiev: GUIKT, 2009. 251 p. (Original text in Russian)
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. Kobozeva A.A., Sokolov A.V. Robust Steganographic Method with Code-Controlled Information Embedding. Problemele energeticii regionale. 2021. No. 4 (52). P. 115-130. (Original text in Russian)
4. Melnik M.A. Compression-resistant steganographic algorithm. Information security. 2012. №2(8). P. 99-106. (Original text in Russian)
5. Chang C.C., Lin C.C., Hu Y.S. An SVD oriented watermark embedding scheme with high qualities for the restored images. International Journal of Innovative Computing, Information & Control, 2007. Vol. 3, No. 3. P. 609-620.
6. Chanu Y.J., Singh Kh.M., Tuithung T. A Robust Steganographic Method based on Singular Value Decomposition. International Journal of Information & Computation Technology, 2014. Vol. 4, No. 7. P. 717-726.
7. Singh N. High PSNR based image steganography. Int J Adv Eng Res Sci (IJAERS). 2019. Vol. 6. No. 1. P. 109-115.
8. Sheidaieian 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.
9. Czvetkov K.Yu., Fedoseev V.E., Korovin V.M., Abazina E.S. Model of a covert channel code division multiple coder using Frank-Walsh, Frank-Chrestenson signaling sequences. Proceedings of the Radio Research Institute. 2015. No. 1. P. 2-11. (Original text in Russian).
10. Kobozeva A.A., Sokolov A.V. Efficient Coding of the Embedded Signal in Steganographic Systems with Multiple Access. Problemele energeticii regionale. 2021. No. 2 (50). P. 101-113. (Original text in Russian)
11. Mazurkov M.I. Broadband radio systems. Odessa: Science and Technology, 2010. 340 p. (Original text in Russian)
12. NRCS Photo Gallery // United States Department of Agriculture. URL: <https://www.nrcs.usda.gov/wps/portal/nrcs/main/national/newsroom/multimedia/>

**СТЕГАНОГРАФІЧНИЙ МЕТОД МНОЖИННОГО ДОСТУПУ НА
ОСНОВІ КОДОВОГО УПРАВЛІННЯ ТА ЧАСТОТНИХ РОЗСТАНОВОК**

А.В. Соколов

Національний Університет «Одеська політехніка»
Одеса, 65044, пр.Шевченка, 1, e-mail: radiosquid@gmail.com

Розвиток, а також ширше практичне застосування сучасної стеганографії призводить до необхідності створення стеганографічних методів з множинним доступом, які могли б забезпечити одночасну передачу і розділення у стеганографічному каналі інформації від декількох користувачів. Відомі на сьогоднішній день стеганографічні методи з множинним доступом засновані на технології MC-CDMA і не показують, як саме має відбуватися вбудовування та вилучення додаткової інформації. Метою цієї статті є розробка стеганографічного методу з множинним доступом на основі кодового управління та частотних розстановок. Поставлена мета була досягнута за рахунок розробки стеганографічного методу з кодовим управлінням та застосуванням частотних розстановок на основі двічі циклічних кодів Ріда-Соломона над полями Галуа $GF(q)$, що забезпечує роздільне вбудовування інформації кожним користувачем у будь-який зручний для нього час з використанням особистої частотної розстановки. При цьому частотні розстановки запропоновано будувати за допомогою РС-кодів над полями $GF(5)$ і $GF(13)$. Досліджено характеристики розробленого методу, в рамках чого показано, що PSNR результуючого стеганоповідомлення залежить від кількості користувачів, що одночасно передають інформацію через стеганографічний канал. При кількості одночасно працюючих абонентів $N \leq 8$, значення PSNR залишаються на допустимому рівні. Під час роботи запропонованого стеганографічного методу виявлено виникнення внутрішньосистемних перешкод у стеганографічному каналі при кількості абонентів $N > q$, що одночасно передають інформацію, однак при використанні частотних розстановок на основі РС-коду над полем $GF(13)$, їх вплив є несуттєвим при практично обґрунтованій кількості каналів, що розділяються. Розроблений стеганографічний метод є раціональним рішенням у разі необхідності організації стеганографічного каналу з множинним доступом і може забезпечити гнучкий розподіл ресурсів: роботу потрібної кількості абонентів із заданою пропускнуою здатністю та необхідною надійністю сприйняття.

Ключові слова: стеганографія, кодове управління, множинний доступ, кодове розподілення каналів, частотні розстановки.

ЗАСТОСУВАННЯ ЗАСОБІВ МАСОВОЇ ІНФОРМАЦІЇ У ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНІЙ ВІЙНІ**М.М. Браїловський¹, Т.П. Пірцхалава², В.О. Хорошко³, Ю.Є. Хохлачова³**¹Київський національний університет ім. Т.Шевченка,
01033, Україна, Київ, вул. Володимирська, 64/13,²Університет Грузії, 0171, Грузія, Тбілісі, вул. М. Костава 77а³Національний авіаційний університет, 03058, Україна, Київ, пр. Любомира Гузара, 1

У ході проведеного дослідження було сформовано рекомендації щодо протистояння інформаційній війні. Проведено аналіз факторів інформаційних впливів та протидія інформаційній зброї, в результаті якого зазначено ряд можливих дій для здійснення протидії російській інформаційній ескаляції в Україні з метою створення гідної і адекватної відповіді на інформаційні виклики сучасності. Запропоновано підхід, який дозволяє відстоювати власні інтереси та інтереси держави в умовах глобальних інформаційних впливів. Як показує досвід останніх збройних конфліктів одними з найважливіших механізмів війни є не тільки зміни у військовій справі, але й інформаційна революція, яка зараз переживає стадію формування. Прикладом масштабного використання інформаційної зброї є інформаційна війна, яка ведеться Росією проти України. Забезпечення інформаційної безпеки в сфері державного та муніципального управління ґрунтується на детальному аналізі структури та змісту управління, а також інформаційних процесів і використання при управлінні відповідних технологій. При цьому визначальними факторами при розробці засобів інформаційної зброї стають саме індивідуальні особливості людини та соціуму. Для того, щоб змодельовати поведінку людини (або суспільства), необхідно знати саме її (його) індивідуальні особливості та переваги. Зараз уже зрозуміло, що інформаційна боротьба стає тим фактором, що впливає на саму війну, її початок, хід і результат. Це підтверджується агресією Росії проти України. Тому, досить актуальною проблемою безпеки України є розробка концепції захисту системи інформаційно-аналітичного забезпечення завдань інформаційної боротьби. У ході проведеного дослідження було сформовано рекомендації щодо протистояння у інформаційній війні. А також проведено аналіз факторів інформаційних впливів та протидії інформаційній зброї, який дозволяє зазначити що потрібно, на нашу думку, для того, щоб протидіяти російській інформаційній ескаляції в Україні.

Ключові слова: інформаційна війна, інформаційний вплив, інформаційно-психологічний вплив, інформаційна зброя, протидія, засоби масової інформації.

Вступ

Сучасний світ перебуває в стані системної нестабільності, розбалансованості та хаосу. До викликів і загроз епохи «холодної війни» додалися якісно нові небезпеки і загрози, що мають і глобальний характер. Майже всі воєнні конфлікти кінця XX та початку XXI століття розвивалися та протікали не за класичними схемами воєнного мистецтва. Бойові дії на Сході України та аналіз ситуації, що передувала цим подіям, дозволило зробити висновок, що Україна зіткнулася з витонченою формою війни, коли перед захопленням територій відбувається інформаційна агресія – інформаційний вплив.

Аналіз ведення локальних війн і збройних конфліктів показує, що протистояння у військовій сфері дедалі частіше переміщується у вербальний простір – інформаційний [1-4]. Інформаційна війна реалізує асиметричні рішення та передбачає проведення спеціальних заходів. Деструктивний вплив на об'єкт досягається також шляхом проведення інформаційно-психологічних операцій (ІПО), які спрямовані проти людини,

групи, суспільства та держави і впливають на їхню моральну стійкість, емоції та мотиви прийняття рішень.

Сучасна війна (гібридна війна) дедалі більшою мірою стає війною на ураження та руйнування свідомості противника та консолідацію свідомості населення власної держави. На жаль Україна стала об'єктом добре організованої та спланованої інформаційної війни з боку Російської Федерації. Тому, саме зараз актуальним є питання виявлення та протидії інформаційно-психологічному впливу (ІПВ) на об'єкт (людину, групу, суспільство та державу).

Слід враховувати, що окупувавши український інформаційний простір Росія робить все, щоб спотворити інформацію про Євросоюз, про євроінтеграцію та НАТО, щоб зомбувати українців неправдивими історичними фактами щодо України та Росії. Фактично вона використовує український простір для розколу суспільства та реалізації планів Кремля стосовно України – політичної та культурної експансії. При цьому Кремлем використовуються такі методи, як [5,6]:

- нав'язування думок про нездатність нинішнього воєнно – політичного керівництва України керувати країною та приймати раціональні рішення, що приводить до невиправданих жертв серед сил операції об'єднаних сил (ООС);
- створення уявлення про те, що зараз для української еліти більш важливі бізнес інтереси ніж інтереси держави та події на Сході;
- поширення поглядів про те, що українські збройні сили на Сході України деморалізовані та не здатні вести бойові дії, а їх особистий склад не довіряє військовому керівництву;
- нав'язування думки про те, що Україна не може прожити без Росії, її економічного та промислового потенціалу;
- підтримка теми малайзійського Боїнга з обвинуваченням України в замовчуванні фактів, обстрілах силами ООС території падіння лайнера.

Цільовою аудиторією ІПВ Кремля стало внутрішнє населення Росії та російськомовних діаспор за кордоном, населення України (у тому числі аудиторія окупованих районів Донбасу та Криму), аудиторія західних країн, аудиторія держав близьких до Росії по політичним поглядам.

Тому дуже важливо враховувати наміри Росії та її інформаційний потенціал, який складається з дуже потужних засобів масової інформації (ЗМІ).

Крім цього слід пам'ятати, що історія відношень між Україною та Росією – це історія постійної боротьби, яка вже йде багато століть. Тільки для України це відстоювання своєї незалежності, а для Росії – зробити з нас рабів.

Основна частина

В епоху процесів глобалізації засоби масової інформації впевнено посіли чільне місце серед засобів комунікацій. Сама глобалізація як явище не була б можливою без діяльності сучасних електронних засобів комунікації та мас-медіа, які охоплюють усю планету.

ЗМІ відіграють чи не найголовнішу роль у сучасному політичному житті більшості держав. Вони виступають основним суб'єктом формування в суспільстві громадської думки про події та явища, що відбуваються в світі та в кожній країні. При цьому спостерігається зворотна закономірність: чим більш розвинутою є інформаційна мережа держави, тим менше залишається можливостей щодо використання інформації на користь якогось одного суб'єкта і навпаки – при менш розвинутій мережі існує більше можливостей для її монополізації та подачі інформації у спотвореному або неповному вигляді.

Зараз всі розуміють, що ми живемо у інформаційній сфері і нікуди з неї не вирвемось.

Можна сміливо говорити, що за такий невеликий проміжок часу процес перепрограмування суспільства пройшов дуже швидко.

Раніше були якісь складнощі, треба було якось донести інформацію до людини так як люди не завжди її розуміли. Сьогодні, підключившись до Internet, можна отримати будь-яку інформацію. Мережа допомагає перевести на будь-яку мову, будь-який текст, який у вас є.

Слід зазначити, що інформаційно-психологічна війна-це не дія сьогоднішнього дня. Багато прийомів інформаційної війни виникли тисячі років тому разом з появою інформаційних систем-історія навчання людства це і є свого роду постійні інформаційні війни.

Слід відзначити, що основними цілями інформаційно-психологічної війни (ІПсВ), в яку входять ІПО та ІПВ, є:

- забезпечення прийняття рішень і спонукання до виконання дій влади країни-жертви (об'єкта), які б задовольняли потреби країни-агресора;
- підрив легітимності політичної влади та міжнародного авторитету країни-жертви;
- дестабілізації у країні-жертви, провокування політичних протестів, соціальних конфліктів, підрив морально-психологічного стану населення країни-жертви;
- підрив обороноздатності країни-жертви та боєздатності її збройних сил;
- підтримка дій внутрішніх сил, направлених на знищення чи завдання шкоди своїй державі, у тому числі шляхом коруптування влади та політичної еліти;
- заміна соціально-культурної ідентичності всього населення або його частини у країні-жертви, зміна національних цінностей та засад державотворення.

При цьому, активними учасниками цих дій є воєнно-політична нерівність РФ, її збройні сили та спецслужби, а також проросійські сили українського суспільства та проросійські налаштовані політичні діячі деяких держав світу.

Для досягнення визначних цілей застосовуються повний спектр каналів комунікацій: засоби масової інформації (електронні та друковані), телебачення, Internet і соціальні мережі. При цьому застосовуються всі методи та засоби ІПВ та ІПО.

ІПВ володіє двома методами впливу [7,8]: справою і словом. Вплив словом не перебуває в переможному застосуванні зброї і в терористичних актах. Саме слово показує, що цей вид впливу- хворобливе явище. Хвилювати, збуджувати, впливати на нерви народу рівносильно даючи йому збуджуючи засоби від випадку до випадку. І тим не менш, ІПВ треба вважати одним з головних засобів гібридної війни: агітація нападу сприяє ослабленню супротивника, оборонна агітація підсилює дух країни, яка стала об'єктом нападу.

Ще треба врахувати, що джерела інформаційної небезпеки можуть бути природними (об'єктивними) і навмисними.

Розглядаючи теорію ІПВ в політичній сфері слід враховувати, що небезпека відбувається на стратегічному, оперативному та тактичному рівнях.

В основному на стратегічному рівні повинна діяти політична еліта, а інформаційні підрозділи політичного клану – на оперативному та тактичному рівнях.

Як вказують експерти, ІПсВ складається з дій, що вживаються з метою досягнення інформаційної переваги в забезпеченні національної, військової, стратегічної та політичної шляхів впливу на інформацію та інформаційні системи супротивника з одночасним зміцненням і захистом власної інформації та інформаційних систем та інфраструктури.

Подальший розвиток гібридної війни з появою кібер-простору отримала розвиток у вигляді кібер-війни та ІПсВ.

Вперше концептуальні питання та основи теорії мережево-центричної системи управління та організації бойових дій і кібер дій та фактичний розгляд військових дій та їх організації з позицій військової кібернетики були сформульовані Н.В. Очарковим (1977-1984 рр. начальник Генерального штабу ЗС СРСР) в кінці 70-х-на початку 80-х років XX сторіччя.

Послідовними, типовими складовими етапами гібридної війни були визначені в цій концепції як:

- інноваційна агресія (кібервійна, економічний тиск, інформаційно-психологічні атаки та ін.);
- застосування нерегулярних збройних формувань або приватних армій (сепаративний рух козаки, самооборони);
- офіційні військові дії або демонстрація сили (ідентифікована уніформа, зброя, офіційне визначення участі в конфлікті).

ПО РФ в Криму планувалися відповідно до концепції Очаркова та системної моделі противника на основі теорії Уордена. В основу цієї теорії покладено концепція центрів тяжіння. Об'єкт з критичною кібернетичною інфраструктурою (центр тяжіння за Уорденом) - це та точка де об'єкт або суб'єкт впливу є найбільш вразливим. Згідно з даною теорією, якщо розглядати об'єкт або суб'єкт впливу як систему з критичною кібернетичною інфраструктурою то його можна подати як систему, що складається з п'яти кілець (рис.1) [7,10].

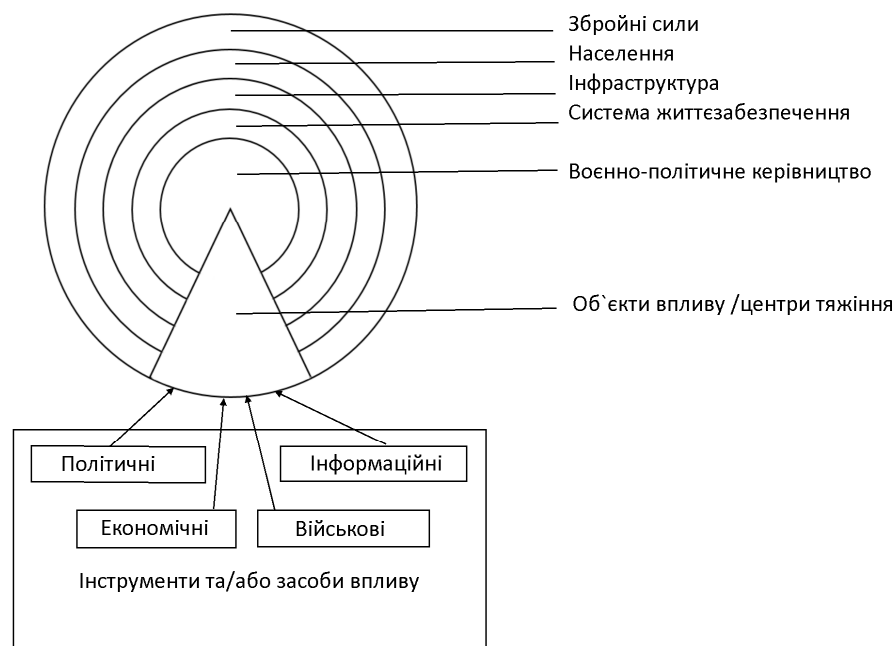


Рис. 1. Модель впливу побудована за теорією Уордена

У центрі моделі Уордена є воєнно-політичне керівництво та національні лідери, які становлять критично важливу складову в архітектурі системи національної безпеки та системи і захищені чотирма іншими кільцями. Так другим кільцем є система життєзабезпечення, виробництво, електричні та атомні станції, підприємства різного призначення, нафтові-постачальні заводи, банки, які під час війни є життєво важливими для забезпечення функціонування військово-промислового комплексу.

Державна інфраструктура-автомобільні шляхи, залізниця, лінії електропостачання-створюють третє кільце. Четвертим кільцем є народо-населення (соціум), а п'ятим, зовнішнім кільцем є збройні сили.

Ця модель реалізує схему «війна з середини-назовні» Слід враховувати, що модель Уордена добре працює в зонах конфлікту, коли збройні сили розглядаються місцевим населенням як зовнішній агресор.

На відміну від цієї моделі, Росія тривалий час мала на території Автономної Республіки Крим підтримку з боку місцевого населення та значні військові формування Чорноморського флоту, які не сприймалися ним у ролі агресора або ворога (рис.2) [7]

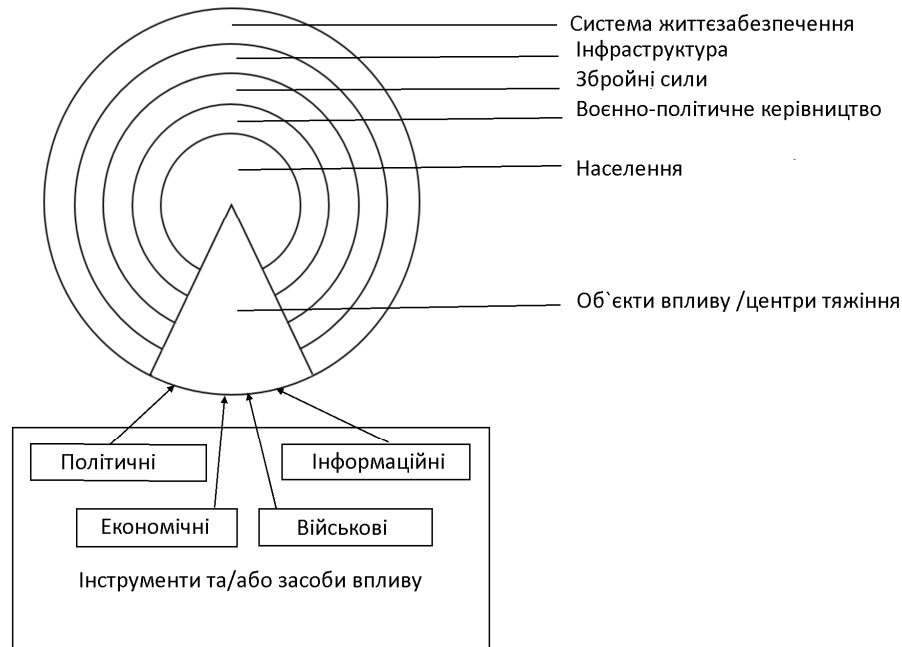


Рис. 2. Модель впливу, використання Росією в Криму

Росія здійснювала тривалий, плановий та спланований вплив на населення Республіки Крим з метою сприйняття військовослужбовців Російської Федерації як захисників населення та виправлення «історичної помилки» щодо поєднання Криму до України. З початком Революції Гідності почався потужний вплив на керівництво Криму та міста Севастополя, а поряд з ним масовий вплив на особистий склад Збройних Сил України. Слід враховувати, що ПВ на Збройні Сили України здійснювався постійно, так, наприклад, квартирне питання військовослужбовців Росії було вирішено, та матеріальне забезпечення росіян було на порядок вище ніж в українських військовослужбовців. Крім того, кожний другий мешканець Севастополя був пов'язаний з Російським Чорноморським флотом. У місті постійно проживало 24 тисячі військовослужбовців. Військові та Чорноморський флот для Севастополя –це підприємства, робота, заробітна плата, соціальна інфраструктура. Флот як би вріс у місто. Тому введення збройних сил Росії до Криму та Севастополя пройшло без протидії та мали ознаки підготовленої та спланованої за цілями, заходами та наслідками ІПО, спрямованого у першу чергу на росіян, а з іншого боку - на українську та західну спільноти. При цьому, в першу чергу було взяті під контроль основні об'єкти транспортної інфраструктури, системи життєзабезпечення та військові об'єкти Збройних Сил України.

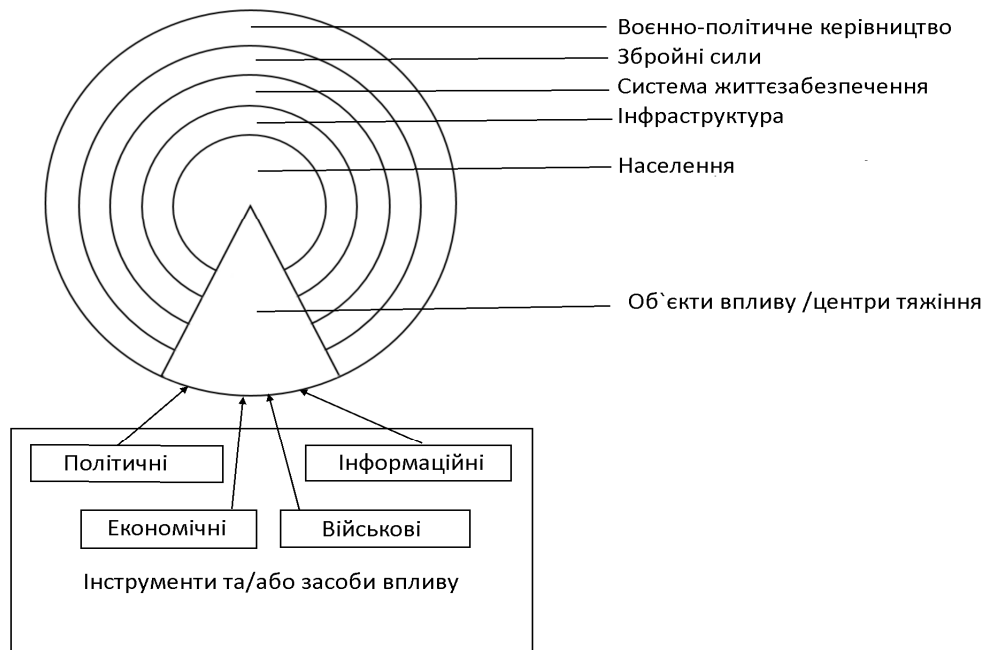


Рис. 3. Модель впливу використана Росією в Донбасі

Анексія Криму показала, що це була добре спланована та організована операція. Слід зазначити, що проросійські організації в Республіці Крим роками використовувались як 5-і колони Кремля в Криму. Вони фінансувались урядом Росії, а їх керівники були агентами впливу російських спецслужб і активно проводили анти українську діяльність.

Все це створило комфортні умови для російської інформаційно-пропагандистської діяльності. На території Криму ретранслювалися телевізійні канали та радіопередачі російських каналів кримськими телерадіоканалами та поширювалися серед жителів Криму українські версії російських газет.

Через ЗМІ Чорноморського флоту Росії російська сторона продовжувала активно впливати на інформаційний простір Республіки Крим. Під прикриттям відстоювання інтересів російськомовного населення регіону, флотськими ЗМІ організовувалася інформаційна компанія, спрямована на формування іміджу Росії, як єдиного надійного гаранта стабільності в регіоні. Для розповсюдження відповідних матеріалів широко використовувалися можливості органів інформаційного забезпечення флоту. За активної підтримки Чорноморського флоту Росії, адміністрацією м. Москви в Севастополі було створено найпотужнішу міську кабельну мережу.

У проросійських ЗМІ активно виступали численні російські діячі: політологи, філософи, релігійні проповідники, які спрямовували відповідні ідеологічні посилення.

Для розпалювання ідей автономізму, сепаратизму та російського шовінізму активно залучалася Руська православна церква та підконтрольна їй Українська православна церква Московського патріархату, а також різноманітні братства Української православної церкви Московського патріархату.

Росія протягом багатьох років вели підривну діяльність у Криму і проводила антиукраїнську пропаганду. Більш того, практично всі проросійські організації Криму співпрацювали із різноманітними спецслужбами Росії. Найбільше на соціально-політичну ситуацію у Криму впливало Головне розвідувальне управління Генерального штабу Міністерства оборони та розвідувальні підрозділи Чорноморського флоту, Служби зовнішньої розвідки Росії та Федеральна служби безпеки Росії.

Тактика гібридної війни, застосованої Росією у Криму була застосована й на Сході України з деякими змінами (рис.3) [5]. Так основний вплив був зосереджений на населенні Донбасу. Наступними об'єктами ПІВ були державна інфраструктура та система

життєзабезпечення. Четвертим та п'ятим кільцем впливу стали Збройні Сили та воєнно-політичне керівництво України.

Особливістю проведення ІПО Росією в Донбасі та в Україні був і є постійний пошук і використання актуальних інформаційних приводів, здатних сформувати необхідну громадську думку. При цьому, основний вплив здійснювався на сфері перегляду історії України та Росії та міжконфесійні відносини.

Для вирішення цих завдань Росія використовувала наступне [11,12] :

групи спеціальних журналістів (з 3-4 чоловік), які мають чіткі інструкції про те, як висвітлювати події на Сході України та безпосередньо працювати на російські інформаційні канали;

1) оперативних груп психологічних операцій, які чисельністю 2-4 чоловіки виконували на території окупованого Донбасу завдання:

- усна пропаганда, у тому числі і робота з місцевим населенням;
- поширення пропагандистської літератури та іншої інформації;
- створення з місцевих пропагандистських груп у анексованих населених пунктах, організація та координація їхніх дій;

- сприяння роботі російських ЗМІ, збору інформації та визначення найбільш гострих проблем у населення для використання цього, як інформаційного приводу;

- моніторинг поточного морально-психологічного стану місцевого населення;

2) загону психологічних операцій, дислокованого недалеко від Ростову-на-Дону разом з пунктом управління розвідцентра Головного розвідувального управління ГШ ЗС Росії.

Його завданнями є [3]:

- збір, обробка та аналіз інформації щодо поточного морально-психологічного стану населення України та підрозділів терористичних та військових формувань;

- керівництво підрозділами психологічних операцій, що виконують спеціальні завдання з ІПВ;

- розробка та здійснення ІПО на території України;

3) агентів диверсійної психологічної роботи в неокупованих областях України, які будуть виконувати наступні завдання:

- створювати диверсійно-пропагандистські групи в неокупованих областях України;

- навчати місцеві групи проведення підричних пропагандистських акцій;

- забезпечувати групи необхідним матеріально-технічним майном;

- безпосередньому проведенню мітингів, акцій протесту та поширенню пропагандистських матеріалів.

Інформаційна ситуація в Україні загострилася після трагедії з малайзійським Боїнгом. Саме в цей період український медіапростор зміг створити досить потужний інформаційний заслон російській пропаганді. Кремль намагався створити інформаційний шум з величезною кількістю версій навколо катастрофи лайнера для відволікання уваги аудиторії від реальних причин трагедії та пошуку найбільш вигідного для Росії правдоподібного варіанта. Однак в цьому інформаційному протистоянні Україна перемогла.

Активність російських спецслужб і пропагандистів в соціальних мережах, принаймні, в Україні, вже давно відомо. Найняті ними «тролі» почали активну роботу ще під час Євромайдана в 2014 році. Оприлюднені зараз документи є підтвердженням цього. Так, американське видання The Washington Post опублікувало секретний звіт Російського Головного розвідувального управління ГШ ЗС про масштабну інформаційну компанію з метою створення можливості для військового захоплення України. Що власне кажучи і трапилося 26 лютого 2014 року, коли почалася анексія Криму. У звіті ГРУ ГШ РФ містяться відомості про роботу однієї з команд управління протягом одного тижня. Так, після втечі Януковича, в лютому 2014-го року агенти російських спецслужб створили

безліч фейкових сторінок в «Facebook» і «В Контакте», на яких в різних варіантах тиражували ідеї розчарування про результати Революції Гідності або в новій українській владі, а також такі, що дискредитують її заяви.

Згідно з документами ГРУ в акаунті «баліція» та інших, створених співробітниками психологічної служби розвідувального управління, на той час, було більше 30-ти фейкових сторінок і груп у соціальних мережах. Прикидаючись звичайними громадянами України, оперативники писали тексти, налаштовуючи громадян України проти протестуючих на майдані.

Російські агенти в соціальних мережах лякали жителів Півдня та Сходу України, публікуючи фейкові загрози тим, хто не підтримував Євромайдан. А після того, як в лютому 2014 року російський спецназ захопив будівлю кримського парламенту, ГРУ створило в «Facebook» і «В Контакте» чотири групи, щоб спонукати кримчан підтримати відділення від України. Використовуючи наші акаунти в «Facebook», ми поширили коментарі, що інформують населення Кримського півострова про загрозу з боку нацистських організацій-цитуює The Washington Post доповідь російського ГРУ. При цьому, вони доповіли, що використовували платні оголошення в «Facebook», щоб підвищити популярність своїх акаунтів та коментарів. За їхніми даними, тільки 27 лютого 2014 року їх пости в фейкових повідомленнях переглянули майже 200 тисяч користувачів.

Враховуючи методи та засоби, які мають проводитись передусім підрозділами анті ПІВ України слід віднести:

- генерування контенту та контр інформаційних операцій, які працюватимуть на об'єднання українців;
- проведення якісної перевірки всієї інформації та ведення боротьби з фейками;
- проведення агітації та пропаганди, яка б висвітлювала би реальні наміри агресорів;
- роз'яснення цілей зовнішньої політики та дій зі встановлення миру на Сході України;
- інформування світової спільноти, впливових іноземних політичних, урядових, бізнесових та культурних кіл, а також іноземних ЗМІ про дії за встановлення миру на Сході України;
- дискредитації воєнно-політичного керівництва Росії.

У сучасній обстановці, дуже важливо вивчати та враховувати психічний стан, політичні настрої суспільства. Дослідження громадської думки дають можливість враховувати не тільки настрої, які мають на поверхні, але і приховані психологічні тенденції політичних процесів, а відповідно до цього і обирати такі заходи, які б були адекватними ситуації, що виникла. Пізнавати стан і динаміку громадської думки-це значить виконати основну вимогу, яка необхідна для правильного прийняття політичного рішення [13].

Зв'язки з громадськістю відіграють важливу роль в житті суспільства. Спочатку ЗМІ створені для інформування громадськості про ключові події в житті країни та владних структур, вони поступово стали виконувати ще одну не менш важливу функцію-вплив на свідомість своєї аудиторії з метою формування певного ставлення до фактів, явищ і дійсності, які повідомляються. Цей вплив здійснюється за допомогою методів пропаганди та агітації, що розробляються на протязі не однієї тисячі років. Для досягнення впливу ЗМІ на сучасну думку люди активно використовують їх для задоволення своїх потреб. Отже ЗМІ є дуже різнобічним і виражається в [14]:

- інформативності громадськості;
- вказівках суспільству, визначення поведінки суспільства.

Результати впливу ЗМІ можуть бути:

- зміни в поведінці суспільства;
- зміни в суспільстві (тому, що поведінка та вказівки не можуть бути ототожнені);
- зміни в знаннях суспільства, як наслідок простої інформативності його.

Слід зазначити, що ЗМІ мають дуже великий вплив на суспільство в цілому і на окрему людину.

Вплив ЗМІ може мати короткостроковий та довгостроковий характер. Реакція на конкретне повідомлення, новину, подію є швидкоплинною. Комплексний та постійний вплив різноманітних каналів інформації зазнає глибинні пласти громадської та людської свідомості.

Глобальні ЗМІ формують універсальну, глобальну систему цінностей. Для суспільства, що розвивається, побудова, підтримка та захист символічної системи є одним з основних завдань. Якщо руйнується символічна система, то суспільство різко змінює традиційні схеми поведінки, що може мати непередбачувані наслідки. Під загрозою можуть виявитися символи, які формують із суспільства націю та народ.

Деструктивний вплив на існуючу в суспільстві систему цінностей здійснюється насамперед завдяки інформації та ЗМІ як універсальних каналів її передачі можна констатувати, ЗМІ є не просто суб'єктами впливу на масову свідомість, але й інструментом, за допомогою якого здійснюється безпосереднє її формування. Формуючи в такий спосіб нові, часто відірвані від життя міфи та стереотипи, ЗМІ створюють свою реальність. При цьому, оскільки така реальність сприймається мільйонами та навіть мільярдами споживачів одночасно, саме вона стає такою, що заслуговує на довіру [14,15]

Отже, можемо відокремити три основні канали масової комунікації: телебачення та Internet, радіо та преса. Кожний із зазначених видів ЗМІ має свої особливості, що визначають успішність його впливу на аудиторію.

Насамперед ЗМІ не можна розглядати як однаково ефективні інструменти поширення інформації. Радіо, телебачення (Internet) та преса відповідають на три принципово різних питання і відповідно до цього кожен із них висвітлює свій аспект певної події. Радіо відповідає на запитання : «Що?», «Що сталося?». Телебачення та Internet дає відповідь на запитання «Як?», «Як сталося те про що вже повідомило радіо?» Преса з'ясовує: «Чому?», «Чому сталося саме те, про що говорило радіо та як це показало телебачення та Internet?» Таким є об'єктивний «розподіл праці» між основними комунікаційними каналами. І тільки системний підхід, спираючись на три взаємодоповнюючих відповіді може дати об'ємну картину того, що справді відбулося.

Висновки

Зараз інформаційна війна між Україною та Росією досягла свого апогею. Усе, що виходить у ЗМІ, у соціальних мережах, у російських інформаційних ресурсах, необхідно уважно вивчати, аналізувати та фільтрувати. Також інформацію необхідно постійно перевіряти. З огляду на те, що в епоху Internet повністю засекретити ті або інші дії просто неможливо. Інформаційна політика України має бути такою, щоб не було недооцінки можливостей інформаційно-психологічної зброї, заходів протидії впливам, які б задовольняли агресора.

Список літератури

1. Манойло А.В. Технологии несилового разрешения современных конфликтов. М.: Горячая линия-Телеком, 2008. 392с.
2. Панарин Н.Н. Технология информационной войны. М.: Мир безопасности, 2003. 320 с.
3. Поченцов Г.Г. Информационная война. М.: Рефл-Бук, 2000. 362 с.
4. Расторгуев С.П. Информационная война. Проблемы и модели. М.: Радио и связь, 1999. 416 с.
5. Зелинский С.А. Информационно-психологическое воздействие на массовое сознание. М: Алгоритм, 2000. 464 с.
6. Леонтьева А.С. Пропаганда, як інформаційно-психологічний складник політичних процесів. Львів: ЛНУ ім. І. Франка, 2004. 296 с.
7. Певцов Г.В., Залкін С.В., Сідченко С.О., Хударковський К.І. Інформаційно-психологічні операції Російської Федерації в Україні: моделі впливу та напрями протидії. Наука і оборона. 2015. №2. С. 28-32.
8. Бухарин С.Н. Методы и технологии информационных войн. М.: Академический проект, 2007. 382 с.
9. Баланюк Ю.В., Козловський В.В., Хорошко В.О., Хохлачова Ю.Є. Інформаційно-психологічні впливи у кіберпросторі. К.: Компринт. 2020. 109 с.
10. Гришук Р.В., Даник Ю.Г. Основы кібернетичної безпеки. Житомир: ЖНАЕУ, 2016. 636 с.
11. Бурячок В.Л. Гулак Г.М., Толубко В.Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. К.: СІК ГРУП УКРАЇНА, 2015. 449 с.
12. Білобородов О.О., Довгополий А.С. Технології інформаційно-психологічних війн та інформаційно-психологічна зброя. Озброєння та військова техніка. 2019. №4 (24). С.93-98.
13. Чалдин Р. Психология влияния. СПб: Питер, 2016. 336 с.
14. Прокоф'єв М.І., Скачек Л.М., Хорошко В.О. Інформаційна війна, як форма ведення інформаційного протиборства: частина 2. Правове нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2019. №1 (37). С. 7-24.
15. Artemov V., Brailovskyi N., Opirskyi I., Ivanchenko I., Khoroshko V. Information War in Ukraine. SPCSI. 2020. Vol.4, №4, P. 28-34.

APPLICATION OF THE MEDIA IN THE INFORMATION-PSYCHOLOGICAL WAR

M.M. Brailovsky¹, T.P. Pirtskhalava², V.O. Khoroshko³, Yu.Ye. Khokhlachova³.

¹Kyiv National University named after T. Shevchenko

01033, Ukraine, Kyiv, vul. Volodymirska, 64/13,

²University of Georgia, 0171, Georgia, Tbilisi, ul. M.Костава 77a

³National Aviation University, 03058, Ukraine, Kyiv, pr. Lubomira Guzara, 1

In the course of the study, recommendations were formed on countering information warfare. The analysis of the factors of informational influences and counteraction to informational weapons is carried out, as a result of which a number of possible actions are indicated to counter the Russian informational escalation in Ukraine in order to create a worthy and adequate response to the informational challenges of our time. An approach is proposed that allows to defend its own interests and the interests of the state in the context of global information influences. As the experience of recent armed conflicts shows, one of the most important mechanisms of war is not only changes in military affairs, but also the information revolution, which is now undergoing a stage of formation. An example of the large-scale use of information weapons is the information war waged by Russia against Ukraine. Ensuring information security in the field of state and municipal management is based on a detailed analysis of the structure and content of management, as well as information processes and the use of appropriate technologies in management. At the same time, the determining factors in the development of information weapons are the individual characteristics of a person and society. In order to model the behavior of a person (or society), it is necessary to know exactly his (his) individual characteristics and preferences. It is now clear that information warfare is becoming the factor that affects the war itself, its beginning, course and result. This is confirmed by Russia's aggression against Ukraine. Therefore, a rather urgent problem of the security of Ukraine is the development of the concept of protecting the system of information and analytical support of information warfare tasks. In the course of the study, recommendations were formed on countering information warfare. And also, an analysis of the factors of informational influences and counteraction to information weapons was carried out, which makes it possible to note what is needed, in our opinion, in order to counteract the Russian informational escalation in Ukraine.

Keywords: information war, information influence, information-psychological influence, information weapon, counteraction, mass media.

МЕТОДИКА ОЦІНКИ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ**С.В. Батечко, О.Ю. Лебедєва, В.В. Зоріло**Національний університет «Одеська політехніка»,
пр. Шевченко, 1, Одеса, 65044, Україна; e-mail: o.y.lebedieva@op.edu.ua,

У роботі розглядається сучасний стан розробок в області оцінки захищеності. Проблема забезпечення безпеки інформаційних технологій займає все більш значне місце у реалізації комп'ютерних систем у міру того, як зростає їхня роль в інформатизації суспільства. Забезпечення безпеки інформаційних технологій є комплексною проблемою, що вирішується у напрямках удосконалення правового регулювання застосування інформаційних технологій, удосконалення методів та засобів їх розробки, розвитку системи сертифікації, забезпечення відповідних організаційно-технічних умов експлуатації. У роботі розглядаються системні проблеми безпеки інформаційних систем, наводиться перелік загроз, які можуть спричинити один або кілька шкідливих впливів на системи. У роботі наводиться перелік стандартів та нормативних документів за допомогою яких можна оцінити якість інформаційної системи чи окремі показники. Наводяться актуальність роботи, її мета та задачі. Ключовим аспектом вирішення проблеми безпеки інформаційних технологій є вироблення системи вимог, критеріїв та показників рівня безпеки інформаційних технологій. У роботі детально описується структура стандарту ISO 15408, який був обраний за основу методики, що розробляється. Стандарт ISO 15408 складається з трьох частин. У роботі використовується друга частина стандарту, яка містить універсальний систематизований каталог функціональних вимог безпеки та передбачає можливість їх деталізації та розширення за певними правилами. Наводиться розроблена методика оцінки захищеності інформаційних систем. В роботі описані основні показники, за допомогою яких проводиться оцінка захищеності інформаційних систем у методикі, що розроблялась. Було розроблено програмний продукт, який реалізує описану методикі у роботі наводиться інтерфейс програми у вигляді основних вікон програми.

Ключові слова: інформаційна система, захист інформаційної системи, стандартизація, стандарт ISO 15408, оцінка захищеності інформаційних систем.

Вступ

На сьогоднішній день інформаційна безпека підприємства – один з провідних факторів його ефективного розвитку. Інформація має реальну вартісну вагу, яка чітко визначається прибутком, що отримується при її використанні, або шкодою, яку може бути завдано підприємству у разі використання її іншими особами.

Постійно зростає частка витрат організацій на забезпечення цілісності інформації та захисту її від можливих зовнішніх загроз. У зв'язку з цим гостро постає питання оцінки ефективності засобів захисту та оцінки захищеності всієї інформаційної системи в цілому. Зробивши таку оцінку, можна вибрати найбільш ефективну систему захисту як із функціонального, так і з економічного погляду у кожному конкретному випадку. Тому дана робота є актуальною в житті суспільства.

Метою роботи є розробка методики оцінки захищеності інформаційної системи шляхом використання стандарту ISO 15408.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

- Проаналізувати стан сучасних розробок в області оцінки захищеності;
- Провести аналіз сучасних стандартів безпеки;
- Розробити методикі оцінки захищеності інформаційної системи;

- Розробити програмний продукт, який реалізує розроблену методику оцінки захищеності інформаційної системи.

Основна частина

Проблема забезпечення безпеки інформаційних технологій займає все більш значне місце у реалізації комп'ютерних систем у міру того, як зростає їхня роль в інформатизації суспільства. Забезпечення безпеки інформаційних технологій є комплексною проблемою, що вирішується у напрямках удосконалення правового регулювання застосування інформаційних технологій, удосконалення методів та засобів їх розробки, розвитку системи сертифікації, забезпечення відповідних організаційно-технічних умов експлуатації.

Інформаційна система – інтегрований набір компонентів для збору, зберігання та обробки даних, а також для надання інформації, знань та цифрових продуктів. Бізнес-фірми та інші організації покладаються на інформаційні системи для здійснення та управління своїми операціями, взаємодії зі своїми клієнтами та постачальниками та конкуренції на ринку.

Уряди впроваджують інформаційні системи для економічного надання послуг громадянам. Цифрові товари, такі як електронні книги, відеопродукти та програмне забезпечення, та онлайн-послуги, такі як ігри та соціальні мережі, постачаються разом із інформаційними системами.

Інформаційні системи часто піддаються різним видам загроз, які можуть спричинити різні типи збитків, що може призвести до значних фінансових втрат. У різних дослідженнях називаються системні проблеми безпеки інформаційних систем:

- маніпулювання доступом у внутрішній інформаційний простір;
- крадіжка інформації з корпоративних мереж і баз даних;
- зміна інформації, фальсифікація документів в електронному вигляді;
- промислове стеження;
- крадіжка засобів з банківських рахунків;
- вірусні загрози.

Загроза безпеці може спричинити один або кілька шкідливих впливів на системи, на які вони поділяються. Їх є сім видів:

- 1) знищення інформації,
- 2) пошкодження інформації,
- 3) крадіжка або втрата інформації,
- 4) розкриття інформації,
- 5) відмова у використанні,
- 6) підвищення привілеїв,
- 7) незаконне використання.

Ключовим аспектом вирішення проблеми безпеки інформаційних технологій є вироблення системи вимог, критеріїв та показників рівня безпеки інформаційних технологій.

Стандартизація – це діяльність, що направлена на розробку та встановлення вимог, норм та правил, характеристик, що є обов'язковими до виконання або рекомендованими.

Самі стандарти – це нормативні документи, що розроблені на основі консенсусу, затвердженого признаним органом та направлені на досягнення оптимального ступеня упорядкованості у певній області. В стандарті встановлюють для загального та багатократного використання загальні принципи, правила і характеристики, що стосуються змісту різних видів діяльності або їх результатів.

Стандарти в галузі інформаційної безпеки покликані виробити чіткий набір критеріїв, за якими можна звести до мінімуму можливі загрози системі. При оцінці

безпеки інформаційних систем слід враховувати думку трьох груп фахівців: розробників інформаційних систем, замовників або користувачів інформаційних систем, спеціалістів – аналітиків з інформаційної безпеки.

Розглянемо, за допомогою яких стандартів та нормативних документів можна оцінити якість інформаційної системи чи окремі показники.

ISO/IEC 27001 – цей документ містить стандарти ISO щодо вимог щодо створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою в контексті організації. Стандарт ISO/IEC 27001 є першим загальновизнаним міжнародним стандартом системи управління інформаційною безпекою. Від багатьох інших стандартів у галузі захисту інформації його відрізняє те, що він може застосовуватись у будь-якій організації незалежно від роду її діяльності. Особливістю ISO 27001 є те, що він висуває вимоги не так до технічних засобів захисту, як до системи управління інформаційною безпекою.

ISO/IEC 27002 – Цей документ вводить кодекс практики для контролю інформаційної безпеки.

ISO/IEC 27017 – цей документ містить рекомендації, що підтримують впровадження засобів контролю інформаційної безпеки для споживачів і постачальників хмарних послуг. Вибір відповідних засобів контролю та застосування рекомендацій щодо впровадження базуються на оцінці ризиків та інших вимогах до використання хмарних сервісів.

Стандарт ISO/IEC 13355 – це посібник з управління безпекою інформаційних та телекомунікаційних технологій, встановлює концепцію та моделі, що лежать в основі базового розуміння безпеки, і розкриває загальні питання управління, які важливі для успішного планування, реалізації та підтримки безпеки. Метою цього стандарту є формування загальних понять та моделей управління безпекою.

Загальні критерії, також відомі як ISO/IEC 15408 – це набір критеріїв оцінки розроблено та узгоджено з національними організаціями стандартів безпеки Австралії, Канади, Франції, Німеччини, Японії, Нідерландів, Нової Зеландії, Іспанії, Великобританії та США. У стандарті детально розглянуті загальні підходи, методи та функції забезпечення захисту в організаціях. Функції системи інформаційної безпеки забезпечують виконання вимог конфіденційності, цілісності, достовірності та доступності інформації.

ISO/IEC 15408 складається з наступних частин під загальною назвою Інформаційні технології – Методи безпеки – Критерії оцінки ІТ-безпеки:

- Частина 1: Вступ і загальна модель;
- Частина 2: Функціональні вимоги безпеки;
- Частина 3: Вимоги до забезпечення безпеки.

Оцінка інформаційної безпеки ґрунтується на моделях системи безпеки, що складаються з перелічених у стандарті функцій. В ISO 15408 міститься ряд зумовлених моделей (так званих профілів), що описують стандартні модулі безпеки.

Особливості ISO 15408 в порівнянні з іншими стандартами безпеки:

- стандарт дозволяє визначити повний перелік вимог до засобів безпеки, а також критеріїв їхньої оцінки (показники захищеності інформації);
- стандарт визначає повний перелік об'єктів аналізу та вимог до них, не загострюючи уваги на методах створення, управління та оцінки системи безпеки;
- стандарт дозволяє оцінити повноту системи інформаційної безпеки з технічного погляду, не розглядаючи при цьому комплекс організаційних заходів із забезпечення захисту інформації.

Усі функції в стандарті ISO/IEC 15408 представлені у вигляді чотирьохрівневої ієрархічної структури: клас – сімейство – компонент – елемент. За аналогією представлені

вимоги якості. Подібна градація дозволяє описати будь-яку систему інформаційної безпеки та зіставити створену модель із поточним станом справ.

У стандарті ISO/IEC 15408–2 виділено 11 класів функцій: аудит, ідентифікація та аутентифікація, криптографічний захист, конфіденційність, передача даних, захист даних, управління безпекою, захист функцій безпеки системи, використання ресурсів, доступу до системи, надійність коштів [1].

Кожен функціональний клас має унікальну назву. Категоріальна інформація складається з короткої назви з трьох символів. Коротка назва класу використовується в специфікації коротких імен сімейства цього класу.

Назва сім'ї надає категоріальну та описову інформацію, необхідну для ідентифікації та категоризації функціональної сім'ї. Кожна функціональна сім'я має унікальну назву. Інформація про категорію складається з короткої назви з семи символів, причому перші три ідентичні короткій назві класу, за якими слідує символ підкреслення та коротка назва сімейства (XXX_YYY). Унікальна коротка форма назви надає основне посилання для компонентів [1].

Функціональні сімейства містять один або більше компонентів, будь-який з яких можна вибрати. Метою цього розділу є надання інформації користувачам при виборі відповідного функціонального компонента після того, як сімейство було визначено як необхідну або корисну частину їхніх вимог безпеки. Цей розділ опису функціонального сімейства описує доступні компоненти та їх обґрунтування. Точні відомості про компоненти містяться в кожному компоненті. Відносини між компонентами всередині функціонального сімейства можуть бути ієрархічними, а можуть і не бути такими. Компонент є ієрархічним щодо іншого, якщо він забезпечує більшу безпеку [1].

Для кожного компонента надається набір елементів. Кожен елемент визначається окремо і є самостійним. Функціональний елемент – це функціональна вимога безпеки, подальше розділення якої не дасть значущого результату оцінки [1]. Це найменша функціональна вимога безпеки, визначена та визнана в ISO/IEC 15408.

Залежності між функціональними компонентами виникають, коли компонент не є самодостатнім і покладається на функціональність або взаємодію з іншим компонентом для свого належного функціонування.

Список залежностей визначає мінімальні функціональні або впевнені компоненти, необхідні для задоволення вимоги безпеки, пов'язані з ідентифікованим компонентом. Компоненти, які є ієрархічними щодо ідентифікованого компонента, також можуть використовуватися для задоволення залежності. Залежності, зазначені в ISO/IEC 15408-2, є нормативними [1].

Розроблена методика оцінки захищеності інформаційних систем має наступні кроки:

1. Визначення класів, що беруть участь в оцінці;
2. Ранжирування класів та розрахунок вагових коефіцієнтів класів;
3. Ранжирування сімейств кожного класу та розрахунок вагових коефіцієнтів сімейств;
4. Відмітка про виконання дій зазначених в компонентах кожного сімейства серед класів, що беруть участь в оцінці;
5. Формування матриці вагової функції по відміткам про виконання;
6. Розрахунок залежностей для кожної компоненти сімейства, якщо така залежність присутня у стандарті;
7. Розрахунок узагальнених показників по кожному класу;
8. Розрахунок підсумкової оцінки;

9. Розрахунок залежностей, узагальнених показників та підсумкової оцінки для класів, що беруть участь в оцінці в ситуації що стоять всі позитивні відмітки про виконання дій зазначених в компонентах кожного сімейства;

10. Порівняння результатів, отриманих на кроках 8 та 9 та формування рекомендацій по підвищенню захищеності інформаційної системи, що оцінюється.

Розглянемо детальніше перелічені кроки.

Обчислення вагових коефіцієнтів C_i для кожного i -го класу безпеки відбувається за формулою:

$$C_i = 1 - \frac{R_i - 1}{M}$$

де R – ранг, а M – число функціональних класів.

Нормування коефіцієнтів, виконується наступним чином:

$$C_k = \frac{C_i}{\sum_{i=1}^M C_i}.$$

Ранжування сімейств класів та обчислення вагового коефіцієнту сімейству відбувається за наступними формулами:

$$F_i = 1 - \frac{R_i - 1}{M}.$$

$$F_k = \frac{F_i}{\sum_{i=1}^M F_i}.$$

Вводиться вагова функція яка має 3 різні поведінки: «-1» – якщо компонент не виконано, «0» – якщо він не використовується та «1» – якщо компонент виконано. Ці значення заносяться у вагову функцію на етапі анкетування, коли експерт проставляє виконання компонентів кожного сімейства.

В результаті анкетування компонентів кожного сімейства обчислюється оцінка по сімейству:

$$W_{kj} = \sum_{k=1}^n F_k^j w_k,$$

де F_k^j – ваговий коефіцієнт k -сімейству j -класу;

w_k – вагова функція k -сімейству.

Вагова функція сімейству складається з вагових функцій компонент цього сімейству з урахуванням залежностей для кожної компоненти сімейства.

Оцінка по кожному класу обчислюється за наступною формулою:

$$X_j = \sum_{k=1}^n C_j w_{kj},$$

де C_j – ваговий коефіцієнт важливості j -го класу;

w_{kj} – підсумковий показник по всім сімействам j -го класу

Підсумкова оцінка захищеності визначається за формулою:

$$Y = \sum_j X_j$$

Було розроблено програмний продукт, який реалізує описану методику оцінки захищеності інформаційних систем. Для ранжування класів та сімейств класів використовується вікно, яке представлено на рисунку 1.

Classes	Applied	Rank	Calculate the weight coefficient
FAU. Аудит безпеки	☒	1	0,182
FCO. Інформаційний обмін	☒	3	0,145
FCS. Криптографічна підтримка	☒	2	0,164
FDP. Захист інформації користувача	☒	6	0,091
FIA. Ідентифікація й автентифікація	☒	10	0,018
FMT. Керування безпекою	☒	4	0,127
FPR. Конфіденційність доступу до системи	☒	9	0,036
FPT. Захист функцій безпеки	☒	7	0,073
FRU. Контроль за використанням ресурсів	☒	5	0,109
FTA. Контроль доступу до системи	☒	8	0,055
FTP. Забезпечення прямої взаємодії	☐	1	0,000

Рис. 1. Вікно для ранжування класів та сімейств класів

Для встановлення вагових коефіцієнтів компонентів кожного сімейства використовується вікно, яке представлено на рисунку 2.

Class: FAU. Аудит безпеки. Вимоги до розпізнання, реєстрації, зберігання та аналізу інформації, що пов'язана з діями, що стосуються безпеки об'єкта оцінювання

Family: FAU_ARP. Визначає реакцію на виявлення подій, що вказують на можливе порушення безпеки

Components:

FAU_ARP — 1

Save results Done!

1

Зроблені дії (зі списку дій, що вживаються у відповідь на очікувані порушення безпеки) при виявленні можливого порушення безпеки

☒ + ☐ -

Рис. 2. Вікно для опитування

Після оцінки усіх класів можна отримати оцінку захищеності конкретної інформаційної системи згідно з результатами анкетування.

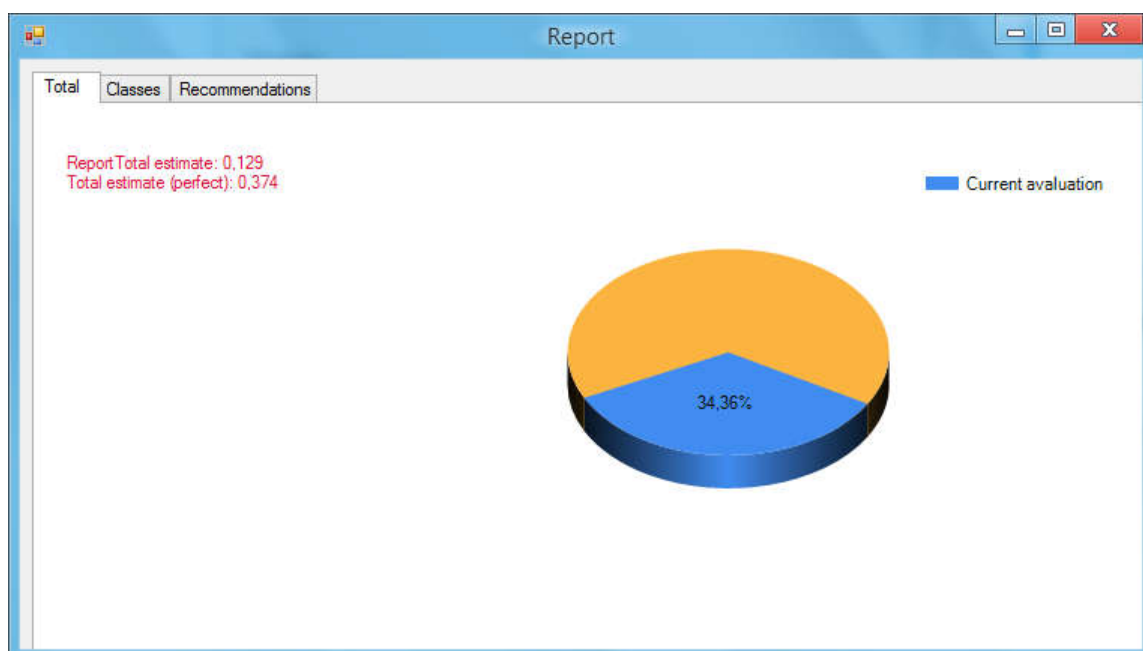


Рис. 3. Відображення результатів оцінювання

Висновки

Було проведено аналіз сучасного стану розробок в області оцінки захищеності. Для методики оцінки захищеності інформаційних систем були обрані функціональні вимоги стандарту ISO/IEC 15408. Було розроблено програмний продукт, який дозволяє оцінити захищеність інформаційної системи згідно з розробленою методикою.

Список літератури

1. ISO/IEC 15408-2:2008. Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components. URL: <https://www.iso.org/obp/ui/#iso:std:iso-iec:15408:-2:ed-3:v2:en>

METHODOLOGY FOR ASSESSING THE SAFETY OF INFORMATION SYSTEMS

S.V. Batechko, O.Yu. Lebedova, V.V. Zorilo

National Odessa Polytechnic University
Shevchenko Ave., 1, Odessa, 65044, Ukraine; e-mail: o.y.lebedieva@opu.ua,

The paper considers the current state of developments in the field of security assessment. The problem of information technology security is becoming increasingly important in the implementation of computer systems as their role in the informatization of society. Ensuring the security of information technology is a complex problem that is solved in the areas of improving the legal regulation of information technology, improving methods and means of their development, development of certification systems, ensuring appropriate organizational and technical conditions of operation. The paper considers systemic problems of information systems security, lists the threats that can cause one or more harmful effects on systems. The paper provides a list of standards and regulations that can be used to assess the quality of the information system or individual indicators. The urgency of the work, its purpose and objectives are given. A key aspect of solving the problem of information technology security is to develop a system of requirements, criteria and indicators of the level of information technology security. The paper describes in detail the structure of the ISO 15408 standard, which was chosen as the basis of the developed methodology. The ISO 15408 standard consists of three parts. The paper uses the second part of the standard, which contains a universal systematized catalog of functional safety requirements and provides for the possibility of detailing and expanding them according to certain rules. The developed method of assessing the security of information systems is given. The paper describes the main indicators used to assess the security of information systems in the developed methodology. A software product has been developed that implements the described technique and the program interface is presented in the form of the main program windows.

Keywords: information system, information system protection, standardization, ISO 15408 standard, information systems security assessment.

**ВИЯВЛЕННЯ ПОРУШЕНЬ ЦІЛІСНОСТІ ЦИФРОВОГО ЗОБРАЖЕННЯ В
КОНТЕКСТІ ЦИФРОВОЇ КРИМІНАЛІСТИКИ****Д.Ю. Берія, М.Є. Войтовецька, Н.Г. Козаченко, В.В. Зоріло, О.Ю. Лебедєва**Національний університет «Одеська політехніка», 1, пр.Шевченка, Одеса, 65044
vikazorilo@gmail.com, whiteswanhelen@gmail.com

Цифрова криміналістика – галузь знань, що активно розвивається наразі. Задачі, що стоять перед цифровою криміналістикою, часто перетинаються з математичними методами пошуку слідів порушень цілісності цифрових зображень. Фотомонтаж, застосування фільтрів та інші порушення цілісності цифрових зображень можливі завдяки графічним редакторам з численною кількістю інструментів, зокрема – фільтрами штучного підвищення різкості. Такі графічні редактори як Gimp або Adobe Photohsop дозволяють користувачам навіть без спеціальної підготовки виконувати різні маніпуляції з зображеннями і з іншими цифровими мультимедійними файлами. Проблемі виявлення порушень цілісності цифрових зображень у вигляді обробки фільтрами, зокрема, фільтрами підвищення різкості, у відкритому друці приділено мало уваги. Метою цієї роботи є підвищення ефективності виявлення обробки цифрового зображення шляхом модифікації методу виявлення підвищення різкості. Було помічено, що під впливом фільтру штучного підвищення різкості у матрицях цифрового зображення з'являється велика кількість пікселів із значенням 0. Даний ефект отримав назву «ефект чорного». У роботі проведено аналіз параметрів цифрового зображення та ефекту чорного, що дозволило виконати модифікацію методу виявлення штучного підвищення різкості цифрових зображень. У результаті виконання роботи модифіковано метод виявлення штучного підвищення різкості цифрових зображень. Оригінал методу було протестовано для цифрових зображень у форматі без втрат. Виконану модифікацію перевірено як для зображень, збережених після обробки фільтром у форматі без втрат, так і з втратами. При тестуванні методу кількість помилок першого роду склала 8%, другого роду – 10% для цифрових зображень, збережених після фальсифікації з втратами, та 4% і 7% відповідно для цифрових зображень, збережених після фальсифікації у форматі без втрат.

Ключові слова: різкість, матриця зображення, порушення цілісності, пошук фальсифікації

Вступ

Порушення цілісності цифрових зображень не представляє складнощів для сучасних користувачів. Спеціалізоване програмне забезпечення просте й інтуїтивно зрозуміле як серед платних за стосунків (Adobe Photoshop), так і серед безкоштовних (Gimp).

Загалом усі методи підробки цифрових зображень можна поділити на дві основні категорії – зміна сцени зображення (додавання або видалення об'єктів шляхом клонування або шляхом фотомонтажу з використанням декількох зображень) та пост обробка зображення після його фальсифікації (розмиття країв доданих об'єктів, маскування розмиття підвищенням різкості, зміна кольору тощо) [1-5]. Штучне підвищення різкості можна використовувати як з метою приховання фотомонтажу, так і з метою стеганографічної атаки на зображення. У будь-якому випадку виявлення даного фільтру у цифровому зображенні свідчить про порушення його цілісності. Тому дана тема є актуальною.

Метою цієї роботи є підвищення ефективності виявлення обробки цифрового зображення шляхом модифікації методу виявлення підвищення різкості.

Матеріали та методи

Як зазначено в [6], при застосуванні фільтру графічного редактора Gimp «Unsharp mask» у всіх трьох колірних компонентах цифрового зображення спостерігається значне збільшення пікселів зі значенням 0. Це легко можна пояснити з урахуванням контексту вирішуваної задачі. Коли ми щось хочемо візуально виділити, то використовуємо для цього підсилення контурів темнішими кольорами. Саме це і відбувається при використанні зазначеного фільтру. Бо у діапазоні значень матриць яскравості пікселів цифрового зображення від 0 до 255 0 – найтемніший колір (чорний), 255 – найсвітліший (білий).

Візуально цей ефект дуже легко побачити при аналізі гістограм матриць яскравості цифрового зображення (рис.1) – чітко видно пік гістограми саме в місці локації нульового значення. Це і є так званий «пік чорного».

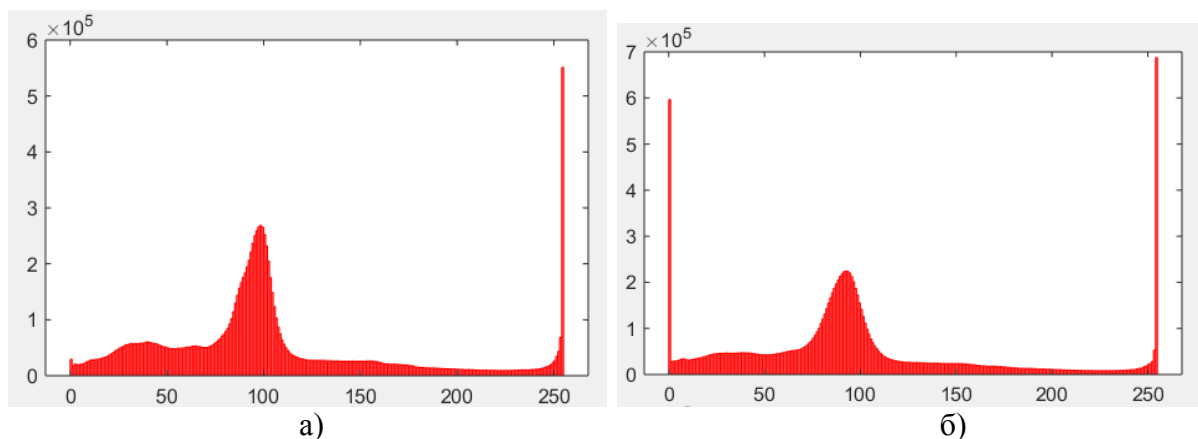


Рис. 1. Гістограма компоненти R: а) – до обробки; б) – після обробки

Проте для автоматизації в роботі [29] запропоновано алгоритм, кроки якого наведемо далі.

Нехай R , G і B матриці червоної, зеленої та синьої компонент цифрового зображення, (r_{ij}, g_{ij}, b_{ij}) тріада цифрових компонент пікселя з координатами (i, j) .

1. Для матриці R знайти r , що дорівнює кількості тріад виду $(0, g_{ij}, b_{ij})$, та знайти r' – кількість тріад виду $(1, g_{ij}, b_{ij})$.

Якщо $r=0$,

то вважати, що зображення необроблене фільтром «Unsharp Mask»,

інакше перейти до пункту 2.

2. Для матриці G знайти g , що дорівнює кількості тріад виду $(r_{ij}, 0, b_{ij})$, та знайти g' – кількість тріад виду $(r_{ij}, 1, b_{ij})$.

Якщо $g=0$,

то вважаємо, що зображення необроблене фільтром «Unsharp Mask»,

інакше перейти до пункту 3.

3. Для матриці B знайти b , що дорівнює кількості тріад виду $(r_{ij}, g_{ij}, 0)$, та знайти b' – кількість тріад виду $(r_{ij}, g_{ij}, 1)$.

Якщо $r=0$,

то вважати що зображення необробленим фільтром «Unsharp Mask»,

інакше переходимо до пункту 4.

4. Якщо $r < r'$ або $g < g'$ або $b < b'$,

то зображення вважати необробленим фільтром «Unsharp Mask»,

інакше перейти до пункту 5.

5. Знайти коефіцієнт різкості K за формулою (1), розрахувавши попередньо відсоткові значення різниці тріад r та r' для червоної компоненти rR по формулі (2), аналогічно відсоткові значення різниці тріад g та g' для зеленої компоненти rG за формулою (3) та відсоткові значення різниці тріад b та b' для синьої компоненти rB за формулою (4):

$$K = \frac{|rR - rG| + |rG - rB| + |rB - rR|}{3}, \quad (1)$$

де

$$rR = \frac{(r - r') * 100}{r}, \quad (2)$$

$$rG = \frac{(g - g') * 100}{g}, \quad (3)$$

$$rB = \frac{(b - b') * 100}{b}. \quad (4)$$

6. Якщо $K < 16$,

то будемо вважати, що зображення оброблене фільтром «Unsharp Mask», інакше зображення є оригінальним.

Помилки першого і другого роду при даному підході складають 10% і 18% відповідно.

Основна ідея – порівняння піку чорного з кількістю пікселів наступного за значенням кольору, тобто порівняння кількості нулів та одиниць. Якщо їх співвідношення у всіх трьох кольорних компонентах менше за порогове значення, зображення вважають обробленим. В іншому випадку вважають, що штучне підвищення різкості не виявлено.

Дослідження ефекту «піку чорного» для зображень, збережених у форматі без втрат після обробки фільтром. У відкритому друці не знайдено інших робіт стосовно виявлення штучного підвищення різкості, тож немає з чим порівнювати даний метод. Проведемо дослідження даного ефекту.

Результати та обговорення

Для обчислювального експерименту сформуємо базу з цифрових зображень у форматі з втратами та без втрат у кількості 600 штук: 300 з них було взято з бази NRCS [7] у форматі без втрат, та 300 цифрових зображень, отриманих сучасним смартфоном iPhone 12 у режимі стандартної зйомки у форматі з втратами. Усі цифрові зображення було оброблено у графічному редакторі Gimp за допомогою фільтру «Unsharp mask» при стандартних параметрах фільтру. Після обробки усі цифрові зображення було збережено у форматі без втрат (bmp).

Для усіх цифрових зображень за трьома кольорними компонентами було підраховано кількість пікселів зі значення 0 до та після застосування фільтру. Типові результати представлено у таблицях 1 – 3.

Таблиця 1

Вплив фільтру на кількість 0-пікселів червоної колірної компоненти

№ цифрового зображення	Кількість 0-пікселів до обробки (N)	Кількість 0-пікселів після обробки (M)	Відношення M/N
1	25312	63526	2,50971871
2	188507	572980	3,03956882
3	954	10607	11,1184486
4	47233	162785	3,44642517
5	35054	136325	3,88899983
6	22875	109866	4,80288525
7	10696	83406	7,79786836

Таблиця 2

Вплив фільтру на кількість 0-пікселів зеленої колірної компоненти

№ цифрового зображення	Кількість 0-пікселів до обробки (N)	Кількість 0-пікселів після обробки (M)	Відношення M/N
1	16394	45296	2,76296206
2	82359	309015	3,75204896
3	28	4555	162,678571
4	16561	78881	4,76305779
5	8378	58510	6,98376701
6	195	38140	195,589744
7	7988	17769	2,22446169

Таблиця 3

Вплив фільтру на кількість 0-пікселів синьої колірної компоненти

№ цифрового зображення	Кількість 0-пікселів до обробки (N)	Кількість 0-пікселів після обробки (M)	Відношення M/N
1	2918944	3034603	1,03962358
2	240576	602991	2,50644703
3	3822	31344	8,20094192
4	1860674	1780279	0,95679254
5	3318235	3281909	0,98905261
6	775796	4783538	6,16597404
7	6233357	6285168	1,00831189

Як можемо спостерігати, результати для червоної та зеленої компонент порівнянні між собою, в той час як показники синьої колірної компоненти значно відрізняються від інших двох. Отримані результати вказують на неможливість усереднення показників за трьома колірними компонентами та використання усіх трьох компонент одночасно для виявлення зазначеного фільтру. Проте використання червоної або зеленої матриць дійсно дозволяє чітко побачити пік чорного та дає можливість використовувати цей ефект надалі.

В той самий час збільшення піку чорного також відбувається, проте не є таким вираженим при повторному застосуванні зазначеного фільтру. Для усіх оброблених зображень було проведено повторне застосування фільтру за тими ж параметрами. Результат повторної обробки збережено у форматі без втрат. Типові результати представлено у таблицях 4-6.

Таблиця 4

Вплив повторного застосування фільтру на кількість 0-пікселів червоної колірної компоненти

№ цифрового зображення	Кількість 0-пікселів до обробки (N)	Кількість 0-пікселів після обробки (M)	Відношення M/N
1	63526	127776	2,01139691
2	572980	1070919	1,86903382
3	10607	44551	4,20015084
4	162785	331190	2,03452407
5	136325	289577	2,12416651
6	109866	247965	2,25697668
7	83406	176152	2,11198235

Таблиця 5

Вплив повторного застосування фільтру на кількість 0-пікселів зеленої колірної компоненти

№ цифрового зображення	Кількість 0-пікселів до обробки (N)	Кількість 0-пікселів після обробки (M)	Відношення M/N
1	45296	98576	2,1762628
2	309015	620728	2,00873097
3	4555	9618	2,1115258
4	78881	183349	2,32437469
5	58510	109870	1,87779867
6	38140	69391	1,81937598
7	17769	82912	4,66610389

Таблиця 6

Вплив повторного застосування фільтру на кількість 0-пікселів червоної колірної компоненти

№ цифрового зображення	Кількість 0-пікселів до обробки (N)	Кількість 0-пікселів після обробки (M)	Відношення M/N
1	3034603	3170059	1,0446371
2	602991	1095081	1,8160818
3	31344	92368	2,9469117
4	1780279	1625188	0,9128839
5	3281909	3164033	0,9640831
6	4783538	4702879	0,9831382
7	6285168	6241724	0,9930879

Як можемо бачити, дійсно при повторному застосуванні фільтру до цифрового зображення збільшення кількості пікселів зі значенням 0 у червоній колірній компоненті в більшості випадків відбувається менше, ніж у 2,25 рази в порівнянні з первинним підвищенням різкості.

Дане порогове значення визначено емпіричним шляхом. Приданому значенні кількість помилок першого роду складає 4%, помилок другого роду – 7%. Подібний результат отримано і для зеленої матриці, при використанні зазначеного порогового значення кількість помилок першого роду 5 %, помилки другого роду – 7%.

Використання синьої колірної компоненти дещо відрізняється від отриманих показників за іншими двома колірними компонентами. Проте використання тільки

червоної колірної компоненти вже дало кращі результати в порівнянні з методом, описаним в роботі [6].

Для зручності розташуємо відношення відповідних показників у одній таблиці для червоної колірної компоненти (табл.7).

Таблиця 7

Порівняння відношень після першої та повторної обробки

№ цифрового зображення	Відношення необробленого обробленого ЦЗ	М/N та	Відношення обробленого та повторно обробленого ЦЗ
1	2,50971871		2,01139691
2	3,03956882		1,86903382
3	11,1184486		4,20015084
4	3,44642517		2,03452407
5	3,88899983		2,12416651
6	4,80288525		2,25697668
7	7,79786836		2,11198235

Як показав обчислювальний експеримент, при пороговому значенні 2,25 досягається найменша кількість помилок першого і другого роду.

Дослідження ефекту «піку чорного» для зображень, збережених у форматі без втрат після обробки фільтром. Проведемо експеримент таким самим чином, як попередній, з різницею у тім, що збережемо фотографії після обробки у форматі з втратами (jpg). Типові результати представлено у таблицях 8 – 10.

Таблиця 8

Вплив фільтру на кількість 0-пікселів червоної колірної компоненти

№ цифрового зображення	Кількість 0-пікселів до обробки (N)	Кількість 0-пікселів після обробки (M)	Відношення M/N
1	25312	60163	2,37685683
2	188507	512670	2,71963375
3	954	8996	9,42976939
4	47233	142776	3,02280185
5	35054	117192	3,3431848
6	22875	91609	4,00476503
7	10696	66025	6,17286836

Таблиця 9

Вплив фільтру на кількість 0-пікселів зеленої колірної компоненти

№ цифрового зображення	Кількість 0-пікселів до обробки (N)	Кількість 0-пікселів після обробки (M)	Відношення M/N
1	16394	44243	2,69873124
2	82359	278508	3,38163407
3	28	3922	140,071429
4	16561	68570	4,14045046
5	8378	48409	5,77810933
6	195	28249	144,866667
7	7988	23088	2,8903355

Таблиця 10

Вплив фільтру на кількість 0-пікселів синьої колірної компоненти

№ цифрового зображення	Кількість 0-пікселів до обробки (N)	Кількість 0-пікселів після обробки (M)	Відношення M/N
1	2918944	2918944	0,74128829
2	240576	240576	2,36730181
3	3822	3822	6,93851387
4	1860674	1860674	0,65423712
5	3318235	3318235	0,688906
6	775796	4775796	0,70241317
7	6233357	6233357	0,70960351

Як можемо спостерігати, результати для червоної та зеленої компонент порівнянні між собою і статистика за даними колірними компонентами така, що можна виділити порошкове значення для виділення оброблених зображень серед необроблених.

Втім для синьої матриці даний ефект піку чорного не такий виражений. Про це свідчать результати експерименту. Тому використовувати синю колірну компоненту за даних обставин було б некоректно. Потрібні додаткові обстеження.

Для усіх оброблених зображень було проведено повторне застосування фільтру за тими ж параметрами. Результат повторної обробки збережено у форматі з втратами. Типові результати представлено у таблицях 11-13.

Таблиця 11

Вплив повторного застосування фільтру на кількість 0-пікселів червоної колірної компоненти

№ цифрового зображення	Кількість 0-пікселів до обробки (N)	Кількість 0-пікселів після обробки (M)	Відношення M/N
1	63526	120312	1,9997673
2	572980	914096	1,78301051
3	10607	36421	4,04857715
4	162785	273052	1,91245027
5	136325	231106	1,97202881
6	109866	159161	1,7373948
7	83406	137215	2,07822794

Як можемо бачити, дійсно при повторному застосуванні фільтра до цифрового зображення збільшення кількості 0-пікселів у червоній колірній компоненті в більшості випадків відбувається менше, ніж у 2 рази в порівнянні з первинним підвищенням різкості.

Дане порошкове значення визначено емпіричним шляхом. При даному значенні кількість помилок першого роду складає 6%, помилок другого роду – 13%.

Таблиця 12

Вплив повторного застосування фільтру на кількість 0-пікселів зеленої колірної компоненти

№ цифрового зображення	Кількість 0-пікселів до обробки (N)	Кількість 0-пікселів після обробки (M)	Відношення M/N
1	45296	87970	1,98833714
2	309015	512243	1,83923981
3	4555	7816	1,99286079
4	78881	139256	2,03085898
5	58510	90272	1,86477721
6	38140	53874	1,90711176
7	17769	37477	1,62322419

Таблиця 13

Вплив повторного застосування фільтру на кількість 0-пікселів червоної колірної компоненти

№ цифрового зображення	Кількість 0-пікселів до обробки (N)	Кількість 0-пікселів після обробки (M)	Відношення M/N
1	3034603	1893813	0,875234
2	602991	972887	1,7082698
3	31344	73833	2,7841548
4	1780279	839802	0,6898766
5	3281909	1749792	0,7654544
6	4783538	2659782	0,7928803
7	6285168	3569772	0,8070542

Для зручності розташуємо відношення відповідних показників у одній таблиці для червоної колірної компоненти (табл.14).

Як показав обчислювальний експеримент, при пороговому значенні 2 досягається найменша кількість помилок першого і другого роду.

Зменшення порогового значення та отриманих показників у порівнянні з аналогічним експериментом для зображень, збережених після фальсифікації без втрат, зумовлене тим, що формат з втратами вносить певні артефакти у цифрове зображення. Один з основних кроків стиснення – квантування частотних коефіцієнтів у блоках матриці.

Таблиця 14

Порівняння відношень після першої та повторної обробки

№ цифрового зображення	Відношення M/N необробленого та обробленого ЦЗ	Відношення M/N обробленого та повторно обробленого ЦЗ
1	2,37685683	1,9997673
2	2,71963375	1,78301051
3	9,42976939	4,04857715
4	3,02280185	1,91245027
5	3,3431848	1,97202881
6	4,00476503	1,7373948
7	6,17286836	2,07822794

Ефект повторної обробки вже було використано в методі виявлення розмиття цифрового зображення, заснованому на аналізі швидкості росту відповідних сингулярних чисел. Складність виявлення порогового значення для відокремлення розмитих цифрових зображень від нерозмитих була в тому, що для різних категорій зображень порогове значення також було різним. Застосування так званого експертного розмиття призвело до уникнення необхідності використовувати чи підлаштовувати порогове значення для різних категорій цифрових зображень.

Тобто, для виявлення штучного підвищення різкості потрібно створити копію підозрюваного зображення, застосувати до неї обробку фільтром. Для обох зображень знайти кількість 0-пікселів червоної компоненти та обчислити їх співвідношення. Якщо воно менше за порогове значення, то експертну обробку слід вважати вторинною, а підозрюване зображення першочергово обробленим, тобто не автентичним.

Інколи можлива ситуація, коли кількість 0-пікселів до обробки дорівнює нулю. Тобто матимемо ділення на нуль. Для уникнення помилки у роботі програми просто вирішити цю проблему, змінивши нуль на одиницю. Це не зменшить ефективності методу, оскільки після застосування штучного підвищення різкості кількість 0-пікселів завжди буде великою.

Отже, на основі проведених експериментів та отриманих результатів складемо алгоритм модифікованого методу виявлення штучного підвищення різкості цифрового зображення.

Нехай A – підозрюване цифрове зображення, R – матриця червоної колірної компоненти цифрового зображення.

1. Для матриці R знайти r , що дорівнює кількості нульових значень.
Якщо $r=0$,
то призначити $r=1$,
інакше перейти до пункту 2.
2. Створити копію підозрюваного зображення. Застосувати до копії обробку фільтром «Unsharp Mask» графічного редактора Gimp з використанням параметрів за замовчуванням.
3. Для копії зображення виділити матрицю R' .
4. Для матриці R' знайти r' , що дорівнює кількості нульових значень матриці R' .
5. Знайти «коефіцієнт чорного»:

$$KoeffBlack = r'/r$$

6. $KoeffBlack < 2,25$ (або 2),
то зображення вважати обробленим фільтром «Unsharp Mask»,
інакше виявлення штучного підвищення різкості не виявлено.

Висновки

Проведено два обчислювальні експерименти з використанням 600 цифрових зображень. Усі зображення було оброблено фільтром фоторедактору GIMP «Unsharp Mask» та збережено у форматі з втратами і без втрат.

Отримано порогове значення 2 для застосування експертної обробки при збереженні зображення у форматі з втратами та 2,25 – без втрат. Кількість помилок першого і другого роду при даному підході становила 6 і 13 відсотків відповідно для збережених з втратами зображень та 4 і 7 відсотки – для зображень без втрат.

На основі проведених експериментів та отриманих результатів було модифіковано метод виявлення штучного підвищення різкості.

Список літератури

1. Зоріло В.В. Методи підвищення ефективності виявлення порушення цілостності цифрового зображення. *Науково-технічний збірник «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні»*. 2013. №1 (25). С. 75-81.
2. Zorilo V.V., Mokritskiy V.A. «Detection of digital image blurring traces». *Інформатика і математичні методи в моделюванні*. 2012. №3, P.220-226.
3. Зоріло В.В., Лебедева Е.Ю., Матвеева А.И., Ефименко А.А., Мокрицкий В.А. Влияние повышения резкости на математические параметры цифрового изображения. *Сучасна спеціальна техніка*. 2017. № 2. с. 67-73.
4. Кобозева А.А. Основы общего подхода к решению проблемы обнаружения фальсификации цифрового сигнала. *Електромашинобудування та електрообладнання*. 2009. Вип.72. С.35-41.
5. Узун И.А. Стеганоанализ цифровых изображений, хранящихся в произвольных форматах. *Информатика и математические методы в моделировании*. 2013. Том 3, № 2. С.179-189.
6. Zorilo V.V., Pyvovar O.V., Safronov P.S. Histogram analysis for detection of sharpened digital images. *Informaics and Mathematical Methods in Simulation*. 2019. Том 9. № 3. P.279-283.
7. NRCS Photo Gallery. URL: <https://photogallery.sc.egov.usda.gov/res/sites/PhotoGallery/index.html>.

DETECTION OF VIOLATIONS OF INTEGRITY OF DIGITAL IMAGE IN THE CONTEXT OF DIGITAL FORENSICS

D.Yu. Beriia, M.Ye. Voitovetska, N.G. Kozachenko, V.V. Zorilo, O.Yu. Lebedeva

National Odessa Polytechnic University,
1, Shevchenko, Odessa, 65044, Ukraine
vikazorilo@gmail.com, whiteswanhelen@gmail.com

Digital forensics is a field of knowledge that is currently actively developing. The challenges facing digital forensics often intersect with mathematical methods for finding traces of violations of the integrity of digital images. Photomontage, application of filters and other violations of the integrity of digital images are possible thanks to graphic editors with a large number of tools, in particular - filters for artificial sharpening. Graphic editors such as Gimp or Adobe Photohsop will allow users to perform various image manipulations and other digital media files, even without special training. Little attention has been paid in open printing to the problem of detecting violations of the integrity of digital images in the form of filter processing, in particular, sharpening filters. The aim of this work is to improve the detection efficiency of digital image processing by modifying the method of detecting sharpening. It has been observed that a large number of pixels with a value of 0 appear in the digital image matrices under the influence of the artificial sharpening filter. This effect is called the "black effect". The paper analyzes the parameters of the digital image and the black effect, which allowed to modify the method of detecting artificial sharpening of digital images. As a result of the work, the method of detecting artificial sharpening of digital images was modified. The original method was tested for digital images in a lossless format. The performed modification was checked both for the images saved after processing by the filter in a lossless format, and with losses. When testing the method, the number of errors of the first kind was 8%, the second kind - 10% for digital images saved after falsification with loss, and 4% and 7% respectively for digital images saved after falsification in lossless format.

Keywords: sharpness, image matrix, integrity breakdown, falsification search.

**РОЗРОБКА МЕТОДУ ДЛЯ ПІДВИЩЕННЯ СТІЙКОСТІ ДО СТАТИСТИЧНОГО
СТЕГАНОАНАЛІЗУ З ВИКОРИСТАННЯМ ГЕНЕРАТИВНО-ЗМАГАЛЬНИХ
МЕРЕЖ****Ю.І. Даракчі, Н.І. Кушніренко, О.Є. Плачінда**Національний університет «Одеська Політехніка», просп. Шевченка, 1,
Одеса, 65044, Україна; e-mail: infsec2011@gmail.com

В сучасних умовах постійного розвитку обчислювальної техніки та мережевих технологій загострюється питання захисту інформації від несанкціонованого доступу. Одним із найефективніших інструментів для вирішення цього питання є стеганографія. Застосування стеганографічних методів дозволяє передавати вбудовану в контейнер додаткову інформацію не привертаючи увагу сторонніх спостерігачів. В якості контейнера доцільно використовувати розповсюджені формати, наприклад зображення JPEG, мільйони яких щодня циркулюють у мережі. Існує достатньо велика кількість стеганоалгоритмів для контейнерів формату JPEG, однак з кожним роком з'являються нові методи стеганоаналізу, які їм ефективно протидіють. Тому вдосконалення існуючих та розробка нових стеганоалгоритмів залишається актуальною задачею. Метою даної роботи є розробка методу вбудовування додаткової інформації в зображення з використанням генеративно-змагальних мереж для адаптивної модифікації контейнера з метою підвищення стійкості до статистичного стеганоаналізу. Попереднє підстроювання контейнера дозволить зберегти розподіл кількості пар коефіцієнтів дискретного косинусного перетворення з певними значеннями. В роботі проаналізовані сучасні методи стеганоаналізу та побудовано статистичний класифікатор для стеганографічного алгоритму F5, розроблено генеративно-змагальну мережу для попередньої модифікації зображення-контейнера, досліджена ефективність роботи розробленого статистичного класифікатора без модифікації контейнера та при її наявності, розроблено програмне забезпечення, яке реалізує стеганографічний метод з адаптивною модифікацією зображення-контейнера. Результати експериментів показали, що модифікований за допомогою генеративно-змагальної мережі контейнер є на 36% більш стійким до виявлення додаткової інформації за допомогою статистичного класифікатора.

Ключові слова: цифрове зображення, дискретне косинусне перетворення, вбудовування додаткової інформації, генеративно-змагальні мережі, стеганоаналітичний метод.

Вступ

В епоху бурхливого розвитку інформаційних технологій особливо актуальним залишається питання захисту інформації від несанкціонованого доступу. В останні десятиліття одним з найефективніших інструментів, який забезпечує вирішення цього питання, стала стеганографія. Стеганографічні системи дозволяють приховати факт присутності секретної інформації завдяки формуванню прихованого каналу передачі даних [1]. Повідомлення вбудовується у контейнер, який може передаватися адресату по відкритим каналам зв'язку без ризику виявлення злоумисниками. В якості стеганографічного контейнера доцільно використовувати файли розповсюджених і загальноживаних цифрових форматів, які не привернуть зайвої уваги, наприклад медіафайли, мільйони яких щодня циркулюють у мережі Інтернет. На сьогоднішній день переважна більшість цифрових зображень зберігається у форматі JPEG, тому його використання в якості стеганографічного контейнера не має викликати підозри з боку

сторонніх спостерігачів. В той же час, застосування статичних зображень в якості контейнера може забезпечити більшу ємність у порівнянні, наприклад, з текстовими форматами. Однак, існує велика кількість стеганоаналітичних алгоритмів, які дозволяють виявляти наявність прихованого повідомлення у зображеннях формату JPEG [2]. Зокрема це статистичні методи стеганоаналізу та методи на основі машинного навчання. Тому актуальним завданням є розробка нових стеганографічних методів, стійких до стеганоаналізу, чому і присвячена дана робота.

Аналіз досліджень та публікацій

Формат JPEG передбачає стиснення із втратами, одним з кроків алгоритму є дискретне косинусне перетворення (ДКП). Наявність втрат дозволяє зменшити помітність викривлень, викликаних вбудовуванням додаткової інформації у контейнер. Існує велика кількість стеганографічних алгоритмів, які призначені для приховування інформації у частотній області зображень. Деякі з них, наприклад, використовують різницю коефіцієнтів ДКП для кодування бітів стеганографічного повідомлення, наприклад алгоритм Коха-Жао [1]. Інші виконують модифікацію найменших значущих бітів коефіцієнтів ДКП, наприклад алгоритм F5 [2]. У свою чергу, постійно розробляються нові методи стеганоаналізу, спрямовані на контейнери JPEG формату. В [3] запропоновано швидкодіючий алгоритм для виявлення прихованого повідомлення при його вбудовуванні у найменші значущі біти коефіцієнтів ДКП контейнера на основі аналізу різниці розбалансу парних та непарних коефіцієнтів ДКП. Однак, при частковому заповненні контейнера, алгоритм не забезпечує надійного виявлення. В [4] запропоновано стеганографічний алгоритм для аналізу зображень JPEG на основі Rich-моделі, який забезпечує виявлення прихованого повідомлення навіть за умов часткового заповнення контейнера. Це можливо за рахунок зміни розподілу кількості пар коефіцієнтів ДКП з різними значеннями. Але якщо розподіл пар коефіцієнтів ДКП не змінюється при вбудовуванні повідомлення, надійне виявлення неможливе. У роботі [5] розглянуто можливість виявлення факту модифікації контейнера на основі аналізу окремих блоків із використанням сингулярних чисел. Даний алгоритм забезпечує надійне виявлення прихованого повідомлення у випадку часткового заповнення контейнера, але із збільшенням коефіцієнту заповнення контейнера ефективність виявлення може зменшуватись.

Останнім часом все більшого розвитку набувають методи стеганоаналізу засновані на машинному навчанні [6]. Даний підхід полягає у поєднанні побудови складних статистичних моделей для зображень з можливостями методів машинного навчання, які використовують статистичні показники розподілу для знаходження стійких закономірностей та класифікації. Наприклад, в [7] запропоновано метод стеганографічного аналізу з використанням машинного навчання, що є альтернативою використанню Rich-моделі. Він більш ефективно виявляє приховані повідомлення, хоча і має меншу швидкодію. За допомогою методів машинного навчання вдалося побудувати ефективні класифікатори для багатьох поширених стеганографічних алгоритмів: YASS [8], F5 [6] та інших.

Оскільки стеганоаналітичні методи спираються на аналіз статистичних змін значень коефіцієнтів ДКП, доцільним є дослідження можливості мінімізації цих змін. Одним із способів зменшити викривлення розподілу значень коефіцієнтів ДКП може бути приховування інформації шляхом додавання шумоподібного повідомлення, яке імітує шум фотографічного сенсора, як запропоновано в [9]. Разом з цим, таке рішення обмежує вибір контейнера фотографічними зображеннями. Актуальною задачею є розробка більш універсальних стеганографічних методів, які б забезпечили би попередню модифікацію контейнера таким чином, щоб після вбудовування

повідомлення розподіл значень коефіцієнтів ДКП був наближений до розподілу вихідного контейнера. У цьому відношенні дуже перспективно виглядає застосування генеративно-змагальних мереж (ГЗМ), які добре зарекомендували себе в галузях комп'ютерного зору та обробки природної мови (генерація текстів і зображень), а також все частіше знаходять застосування в задачах стеганографії [10].

Мета статті та постановка завдань

Метою даної роботи є розробка методу вбудовування додаткової інформації в зображення з використанням генеративно-змагальних мереж для адаптивної модифікації контейнера з метою підвищення стійкості до статистичного стеганоаналізу. Попереднє підстроювання контейнера дозволить зберегти розподіл кількості пар коефіцієнтів ДКП з певними значеннями.

Для досягнення мети в роботі розв'язуються наступні задачі:

- проаналізувати сучасні методи стеганоаналізу та побудувати статистичний класифікатор для стеганографічного алгоритму F5;
- побудувати генеративно-змагальну мережу для попередньої модифікації зображення-контейнера;
- дослідити ефективність роботи розробленого статистичного класифікатора без модифікації контейнера та при її наявності;
- розробити програмне забезпечення, яке реалізує стеганографічний метод з адаптивною модифікацією зображення-контейнера.

Основна частина

Для проведення експериментів в роботі обрано стеганографічний алгоритм F5, стеганоаналіз якого залишається актуальним напрямом завдяки наступним його особливостям [6]:

- забезпечує велику пропускну спроможність;
- висока ефективність (вбудовує більше бітів за одну зміну) завдяки матричному кодуванню;
- добре протидіє візуальним атакам;
- має високу стійкість до статистичних атак;
- використовує розповсюджений формат для контейнерів (JPEG);
- має відкритий код.

При вбудовуванні бітів стеганографічного повідомлення у коефіцієнти ДКП алгоритм F5 здійснює декремент значень цих коефіцієнтів. Хоча візуально такі зміни можуть бути непомітними завдяки псевдовипадковому вибору коефіцієнта ДКП для вбудовування, відносна кількість коефіцієнтів із певним значенням буде змінюватися. Кількість коефіцієнтів із значеннями 1, -1 буде зростати, а коефіцієнтів із більшими абсолютними значеннями зменшуватися. Тому можливим є виявлення факту вбудовування повідомлення за допомогою аналізу зміни статистики зображення.

Для експериментів в якості контейнерів було використано набір даних «Linnaeus 5 256X256» [11], зображення формату JPEG. Розмір кожного із зображень 256×256 пікселів. У якості повідомлення було використано псевдовипадкову бітову послідовність із рівномірним розподілом.

Нижче наведено кроки, необхідні для визначення розподілу значень пар коефіцієнтів ДКП та побудови класифікатора з використанням машинного навчання. На даному етапі наявні 8000 цифрових зображень, у які була вбудована додаткова інформація за алгоритмом F5 та така ж кількість зображень, які не підлягали стеганографічному перетворенню.

Масив розподілу значень пар коефіцієнтів ДКП формується за наступним алгоритмом:

- Із набору даних обирається монохромне цифрове зображення $I_{(n,m)}$, де n, m — його ширина та висота.
- Виконується ДКП пікселів зображення, у результаті якого отримуємо масив коефіцієнтів тієї ж розмірності. Його перший елемент (ДС коефіцієнт) пропорційний до середньої яскравості блоку і зазвичай набагато більше інших елементів. Інші 63 елементи (АС коефіцієнти) пропорційні інтенсивності колірних переходів у блоці.
- Після виконання квантування коефіцієнтів отримуємо цілі значення.
- Формується масив зсувів з 10 елементів типу (i', j') , де i', j' — координатний зсув для обрання парного коефіцієнта.
- Будується нульова матриця A , розмірність якої дорівнює подвоєному максимальному коефіцієнту ДКП після квантування (без урахування ДС коефіцієнтів).
- Для кожного коефіцієнта K з координатами i, j , який не є нульовим чи ДС коефіцієнтом, визначаємо парний коефіцієнт $K_{(i+i', j+j')}$. Далі будемо позначати пари як (p, q) .
- Виконується інкремент значень $A_{(p,q)}$ для кожної пари коефіцієнтів.
- Виконуємо нормалізацію відносно кількості блоків ДКП (використовуємо блоки 8×8):

$$A_n = A / \left(\frac{n}{8} + \frac{m}{8} \right),$$

- Повторюємо кроки 5-8 для кожного з 10 зсувів.
 - Об'єднуємо отримані матриці в одну, яка й буде характеризувати зображення.
- Перед тренуванням нейронної мережі дані розбиваються на тренувальну та тестову вибірки. Після завершення процесу навчання на основі тренувальній множині виконується перевірка результату на тестових даних, встановлюється порогове значення. Для оцінки ефективності запропонованого алгоритму на тренувальних та тестових даних використані ймовірності помилок першого та другого роду. Чим менше значення помилок, тим вище ефективність отриманої мережі. У якості вихідної гіпотези H_0 виступає припущення, що контейнер порожній, а H_1 , відповідно, що у контейнері є приховане повідомлення. Ймовірності вибору та вірності цих гіпотез наведено у табл. 1.

Таблиця 1

Гіпотеза, що була обрана мережею	Ефективність класифікатора	
	Правильна гіпотеза	
	H_0	H_1
H_0	0,949	0,051
H_1	0,051	0,949

З наведених результатів видно, що ймовірність успішного виявлення наявності додаткової інформації складає 96%, а детектування порожнього контейнера майже 95%. Відповідно помилок першого роду — 5% та другого 4%. Такі значення дозволяють мережі надійно виявляти факт вбудовування додаткової інформації.

Для протидії стеганоаналізу на основі класифікатора необхідно вирішити проблему зміни статистичних показників контейнера. Можливим шляхом у даному випадку може бути штучна модифікація зображення-контейнера за умови збереження візуальної подібності до його початкового стану. Для розв'язання такої задачі доцільним є використання генеративно-змагальних мереж, які знайшли широке застосування в галузі генерації зображень. Генеративно-змагальні мережі складаються з двох нейронних мереж: одна навчена генерувати дані, а інша – відрізняти підроблені дані від реальних даних. Хоча ідея структури для генерації даних не нова, мережі ГЗМ дають вражаючі результати по створенню штучних зображень та відео. Можливості ГЗМ у стеганографії можна розглядати з різних боків: змагальна гра, генератор або функція відображення. Вони узгоджуються із класифікацією основних стратегій у стеганографії, тобто модифікації, синтезу та селекції [10].

Модифікація зображення, заснована на ГЗМ, фокусується на змагальній грі між стеганографом і стеганоаналізатором. Даний підхід використовує генератор, навчений для побудови різних ключових елементів, що дозволяє створювати більш захищене від стеганоаналізу стегоповідомлення, яке може передавати по відкритому каналу зв'язку. Фактично генеративно-змагальна мережа складається з трьох мереж: генератор G, дискримінація D та стеганоаналізатор S (рис. 1).

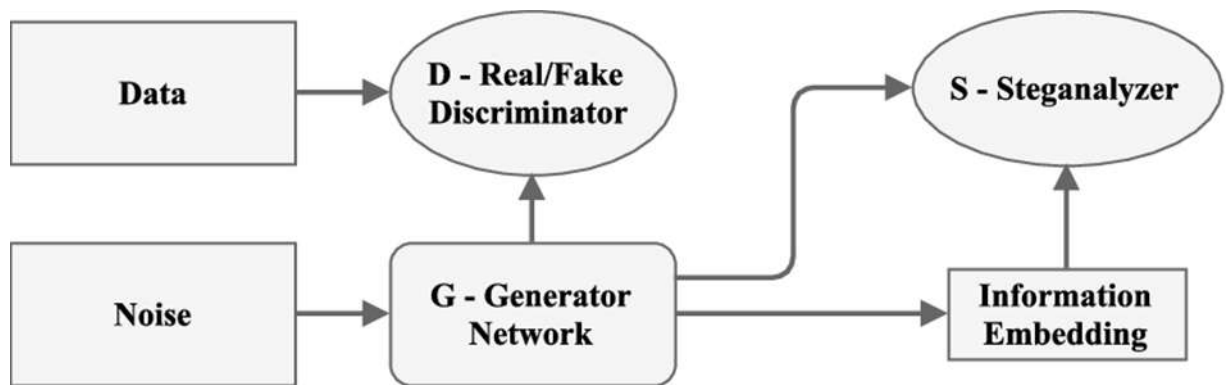


Рис. 1. Структурна схема ГЗМ для модифікації контейнера

На рис. 2 зображена запропонована схема навчання ГЗМ для модифікації контейнера з вбудовуванням на основі стеганографічного методу F5. Модифікація контейнера перед вбудовуванням прихованого повідомлення проводиться таким чином, щоб після нього за статистичними та візуальними характеристиками контейнер був максимально подібним до порожнього. На вхід генератора подаються порожній та заповнений контейнери. Мережа дискримінатора є стандартною згортковою мережею, яка може класифікувати зображення. Генератор є зворотною мережею згортки. Створені таким чином модифіковані контейнери після вбудовування секретного повідомлення будуть більш наближені до порожнього контейнера, але це можливо лише при заздалегідь відомому повідомленні.

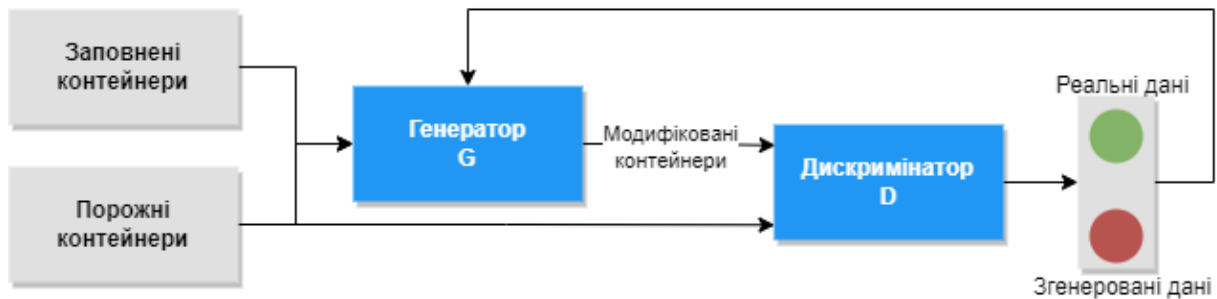


Рис. 2. Схема навчання запропонованої ГЗМ

На рис. 3 наведена спрощена схема роботи стеганографічної системи з застосуванням методу модифікації контейнера. Після вбудовування повідомлення в контейнер статистичний класифікатор (стеганоаналізатор) перевіряє контейнер з повідомленням. Якщо на виході він не виявляє факт вбудовування додаткової інформації, то вважаємо, що повідомлення вбудовано успішно та готово для подальшої передачі по відкритому каналу зв'язку. Якщо класифікатор виявляє повідомлення, то застосовуємо ГЗМ, якій передаємо оригінальний та заповнений контейнери для генерації модифікованого контейнера. Після чого здійснюємо повторне вбудовування, але вже у модифікований контейнер.

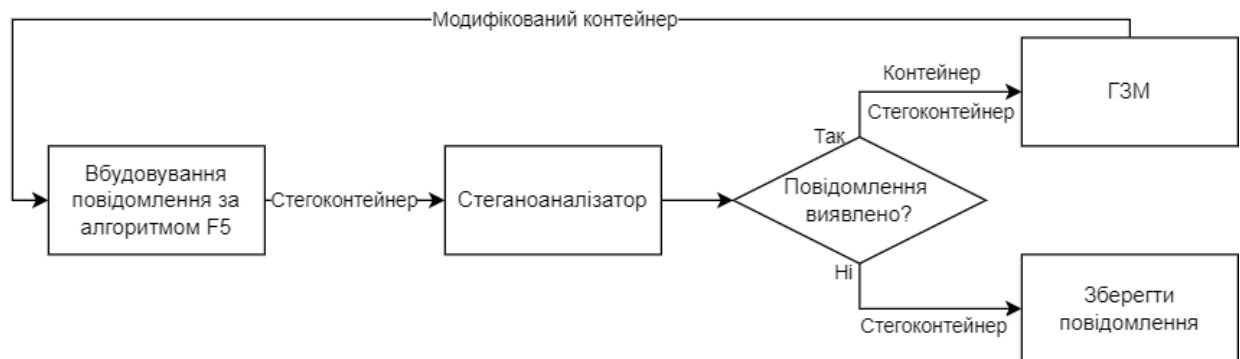


Рис. 3. Структурна схема запропонованої стеганографічної системи

Тренування ГЗМ виконується наступним чином:

1. Для тренування генератора використовується набір зображень «Linnaeus 5 256X256», який розбивається на 3 множини: тренувальну, тестову та валідаційну. На тестову вибірку відводиться 20% від тренувальної – 1600 зображень. На валідаційну – 20% від різниці між кількістю зображень тренувальної та тестовою вибірок, тобто 1280.

2. Будується генеративно-змагальна мережа.

3. Під час її тренування за допомогою алгоритму F5 проводиться вбудовування повідомлення у кожний контейнер. Отримані стеганоповідомлення разом із порожніми контейнерами подаються на вхід генеративної мережі.

4. Дискримінатор приймає як реальні, так і модифіковані зображення і повертає ймовірності від 0 до 1, причому 1 являє собою справжнє зображення (оригінальний контейнер) і 0 представляє фейкове (створене нейронною мережею).

Проведено дослідження роботи розробленого методу модифікації контейнера за умов застосування запропонованого в статті статистичного класифікатора. Для оцінки ефективності запропонованого методу використані ймовірності помилок першого та другого роду. Помилки першого роду демонструють, з якою ймовірністю класифікатор під час аналізу порожнього контейнера покаже, що він заповнений. Помилки другого

роду демонструють, з якою ймовірністю класифікатор покаже, що цей контейнер є порожнім. Чим ближче значення помилок до 0,5, що відповідає випадковому вгадуванню, тим менш дієвим буде стеганоаналіз, і тим більшою буде ефективність запропонованої ГЗМ.

Таблиця 2

Ефективність класифікатора за умови модифікації контейнера

Гіпотеза, що була обрана мережею	Правильна гіпотеза	
	H_0	H_1
H_0	0,599	0,401
H_1	0,401	0,599

З отриманих результатів видно, що ймовірність успішного виявлення значно зменшилась у порівнянні із вбудовуванням без попередньої модифікації (табл. 1). Ймовірність помилок першого та другого роду збільшилась на 36%. Такі значення більше не дозволяють класифікатору надійно виявляти факт вбудовування секретного повідомлення.

Висновки

У даній роботі було запропоновано метод, що базується на застосуванні генеративно-змагальних мереж та здатен значно підвищити стійкість до статистичного стеганоаналізу. Під час його розробки було проаналізовано сучасні методи стеганоаналізу та побудовано статистичний класифікатор для стеганографічного алгоритму F5 засобами машинного навчання.

Для аналізу контейнера та детектування наявності вкладеного повідомлення класифікатор розглядає характеристичну матрицю зображення, сформовану на основі аналізу розподілу пар АС коефіцієнтів ДКП. Для його тренування у якості секретного повідомлення було використано псевдовипадкову послідовність бітів з рівномірним розподілом для наближення його статистичних властивостей до повідомлення, яке пройшло процес шифрування.

Тренування генеративно-змагальної мережі та перевірка ефективності її роботи проводилися на окремих частинах набору даних «Linnaeus 5 256X256». Загальний розмір вибірки становить 8000 зображень формату JPEG.

Оцінка ефективності роботи генеративно-змагальної мережі проводилась, виходячи з максимізації ймовірностей помилок першого та другого роду класифікатора. У результаті проведеного моделювання ймовірність помилки під час виявлення вбудованого повідомлення до модифікації контейнера становить 4,5%. Після модифікації цей показник зростає до 40%. З отриманих результатів видно, що застосування генеративно-змагальної помітно зменшує ймовірність виявлення повідомлення, прихованого за алгоритмом F5.

Також було розроблено програмне забезпечення для реалізації стеганографічного метода з адаптивною модифікацією контейнера. Для тренування мереж було застосовано бібліотеку для машинного навчання від Google — TensorFlow, а також хмарний сервіс Google Colab для прискорення процесу навчання. Графічний інтерфейс було реалізовано за допомогою мови програмування Python та бібліотеки PySide6.

Список літератури

1. Конахович Г.Ф., Прогонов Д.О., Пузиренко О.Ю. Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних. К.: Alex Print Centre, 2018. 558 с.
2. Denemark T, Fridrich J. Steganography With Multiple JPEG Images of the Same Scene. *IEEE Transactions on Information Forensics and Security*. 2017. Vol. 12. Is. 10. P. 2308–2319.
3. Калашніков М.В. Яковенко О.О., Кушніренко Н.І., Чечельницький В.Я., Статистичне виявлення стеганографічних повідомлень у зображеннях формату JPEG. *Електротехнічні та комп'ютерні системи*. 2017. № 25(101). С.310–316.
4. Fridrich J., Kodovsky J. Rich Models for Steganalysis of Digital Images. *IEEE Transactions on Information Forensics and Security*, 2012. No 7(3), P. 868–882.
5. Kobozeva A.A., Bobok I.I. Method for detecting digital image integrity violations due to its block processing. *Radiotekhnika*. 2019. No 4 (199), P. 130–141.
6. Fridrich J., Sedighi V. Histogram Layer, Moving Convolutional Neural Networks Towards Feature Based Steganalysis. *Proc. IS&T, Electronic Imaging, Media Watermarking, Security, and Forensics 2017*. San Francisco, CA, 2017. URL: DOI:10.2352/ISSN.2470-1173.2017.7.MWSF-325
7. Chen M., Boroumand, M., Fridrich, J. Deep Learning Regressors for Quantitative Steganalysis. *Electronic Imaging*, 2018. No 7, 160-1–160-7.
8. Fridrich J., Kodovsky J., Pevný T. Modern Steganalysis Can Detect YASS. *Proc. SPIE, Electronic Imaging, Media Forensics and Security XII*. San Jose, CA, 2010. P. 02-01 - 02-11.
9. Denemark T., Bas P., Fridrich J. Natural Steganography in JPEG Compressed Images. *Electronic Imaging*. 2018. No 7. P. 316-1–316-10.
10. Zhang Y. Zhang W., Chen K., Liu J., Liu Y., Yu N. Adversarial Examples Against Deep Neural Network based Steganalysis. *Acm Workshop on Information Hiding & Multimedia Security*. Insbrik, Austria, 2018. P. 67-72.
11. Chaladze G. Linnaeus 5 dataset. URL: <http://chaladze.com/15/>

**DEVELOPMENT OF A METHOD TO INCREASE RESISTANCE TO
STATISTICAL STEGANALYSIS USING GENERATIVE
ADVERSARIAL NETWORK**

Yu.I. Darakchi, N.I. Kushnirenko, O.E. Plachinda

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

In the current conditions of constant development of computer technology and networking, the issue of protection of information from unauthorized access is becoming more acute. One of the most effective tools for solving this problem is steganography. The use of steganographic methods allows the transfer of additional information embedded into the container without attracting the attention of outside observers. As a container, it is advisable to use common formats, such as JPEG images, millions of which are circulating on the network every day. There are quite a few steganographic algorithms for JPEG containers, but every year developed new methods of steganalysis that effectively counteract them. Therefore, the improvement of existing and development of new steganographic algorithms remains an urgent task. The aim of this work is to develop a method of embedding additional information in the image using generative adversarial networks for adaptive modification of the container in order to increase resistance to statistical steganalysis. Pre-tuning the container will preserve the distribution of the number of pairs of discrete cosine transform coefficients with certain values. The modern methods of steganalysis are analyzed and the statistical classifier for steganographic algorithm F5 is constructed, the generative adversarial network for preliminary modification of the image-container is developed, efficiency of work of the developed statistical classifier without and with modification of the container is investigated. The results of the experiments showed that the container modified by the generative-competitive network is 36% more resistant to the detection of additional information using the statistical classifier.

Keywords: digital image, discrete cosine transform, additional information, generative adversarial network, steganalysis method.

СИСТЕМА МОДЕЛЮВАННЯ КІБЕРАТАКИ ПІДМІНОЮ OPC-СЕРВЕРА ПРИ КОМП'ЮТЕРНОМУ УПРАВЛІННІ ТЕХНОЛОГІЧНИМИ УСТАНОВКАМИ

А.А. Зозуля¹, О.А. Стопакевич¹, А.О. Стопакевич²

¹Національний університет «Одеська політехніка»

1, пр. Шевченка, Одеса, 65044, Україна; e-mail: stopakevich@op.edu.ua

²Державний університет інтелектуальних технологій та зв'язку

1, вул. Кузнечна, Одеса, 65023, Україна; e-mail: stopakevich@gmail.com

Відповідно до звіту компанії Positive Technologies за вересень 2021р. 91% промислових компаній світу мають вразливі до кібератак інформаційні системи. Промисловий сектор – це другий за кількістю кібератак сектор в США, й ведучий в розвинутих країнах. Шосте й сьоме місце в топ двадцятці серед найбільших виробничих атак займає Україна. Сектору промислової кібербезпеки в світі присвячено багато наукових публікацій, але, нажаль, в Україні цією сферою кібербезпеки займаються слабо. Для розвитку тематики підвищення рівня кібербезпеки промислових систем керування, ми зосередились на проблемах кіберзахисту нижньої ланки керування – операторської станції керування технологічною установкою. Попередньо нами досліджена проблема кіберзахисту промислової комп'ютерної мережі нижчого рівня Modbus RTU. Продовжуючи тему, в цій роботі дослідитимемо кібербезпеку важливого програмного забезпечення – OPC сервера. В дослідженні пропонується звернути увагу на вразливість, якої ще не досліджено. Ця вразливість зв'язана з тим, що маючи розгалужену мережу робочих станцій на підприємстві, зловмисник може підмінити OPC-сервер на будь якій робочій станції (зазвичай, найбільш важливій на виробництві) власним OPC-сервером і зробити таким чином, щоб з одного боку привести технологічний апарат обраної ділянки до зупинки чи аварії, а з другого боку, щоб оператор технологічної установки, спостерігаючи за SCADA-системою на екрані комп'ютера, нічого не помітив. Для виявлення кібератаки розроблено спеціальну діагностичну систему. Розроблено відповідне програмне забезпечення та, за його допомогою, всі рішення промодельовано в реальному часі з використанням компонентів реального промислового програмного забезпечення та моделі мережі Modbus. Розроблені рішення та програмне забезпечення можуть бути використані в промисловості.

Ключові слова: Кібератака, кіберзахист, OPC, OLE for Process Control, SCADA, система керування технологічною установкою.

Вступ

Відповідно до звіту компанії Positive Technologies [1] за вересень 2021 р. 91% промислових компаній світу мають вразливі до кібератак інформаційні системи. Промисловий сектор – це другий по кількості кібератак сектор в США, й ведучий в розвинутих країнах. Шосте й сьоме місце в топ 20 серед найбільших успішних виробничих атак займає Україна. Відповідно, сектору промислової кібербезпеки в світі присвячено багато наукових публікацій, наприклад [2-5], але, нажаль, в Україні цією сферою кібербезпеки займаються слабо.

Для розвитку наукової теми підвищення кібербезпеки промислових систем керування ми зосередились на проблемах кіберзахисту нижньої ланки керування – операторської станції керування технологічною установкою. В роботі [6] нами було досліджено кіберзахист промислової комп'ютерної мережі нижчого рівня Modbus RTU. Продовжуючи тему, в цій роботі дослідимо проблему кібербезпеки важливого програмного забезпечення – OPC сервера.

Головною метою технології OPC [7] є забезпечення можливості спільної роботи засобів автоматизації, що функціонують на різних апаратних платформах, у різних промислових мережах та вироблених різними фірмами. До поширення технології OPC

з'єднання SCADA системи з кожним засобом автоматизації проводилось індивідуально. Існували довгі списки "підтримуваного обладнання", дуже складною була технічна підтримка. При модифікації обладнання потрібно було вносити зміни до всіх драйверів, кожен з яких підтримував протокол обміну тільки з однією клієнтською програмою. Число таких драйверів доходило до сотень. Після появи OPC практично всі SCADA-пакети були перепроєктовані як OPC-клієнти, а кожен виробник апаратного забезпечення став постачати свої контролери, модулі вводу-виводу, інтелектуальні датчики та виконавчі пристрої зі стандартним OPC-сервером. Завдяки появі стандартизації інтерфейсу стало можливим підключення будь-якого фізичного пристрою до будь-якої SCADA, якщо вони відповідали стандарту OPC. Розробники отримали можливість проектувати лише один драйвер для всіх SCADA-пакетів, а користувачі отримали можливість вибору обладнання та програм без колишніх обмежень на їхню сумісність.

Приклад архітектури систем, що включають OPC-сервери та OPC-клієнти, показано на рис. 1. За наявності кількох операторських робочих станцій кожна з них може містити OPC-сервер та підключені до нього фізичні пристрої. У такій системі будь-який OPC-клієнт з будь-якого комп'ютера може звертатися до будь-якого OPC-сервера, у тому числі розташованого в іншій комп'ютерній мережі. Це досягається завдяки технології DCOM, яка використовує віддалений виклик процедур (RPC – Remote Procedure Call). Наприклад, технологічна установка 3 під керуванням SCADA-системи на рис. 1 може завдяки RPC звернутися й отримати дані зі SCADA-системи, яка керує установкою 1, що вказано штриховою лінією. Звернемо увагу, що комп'ютери та контролери у такій архітектурі можуть працювати з різними промисловими мережами. Обмін даними з ПЛК виконується точно так, як із комп'ютерами. OPC-сервер монополює COM-порт (RS485) комп'ютера (оскільки безперервно виконує оновлення даних), тому кількість портів має дорівнювати кількості OPC серверів.

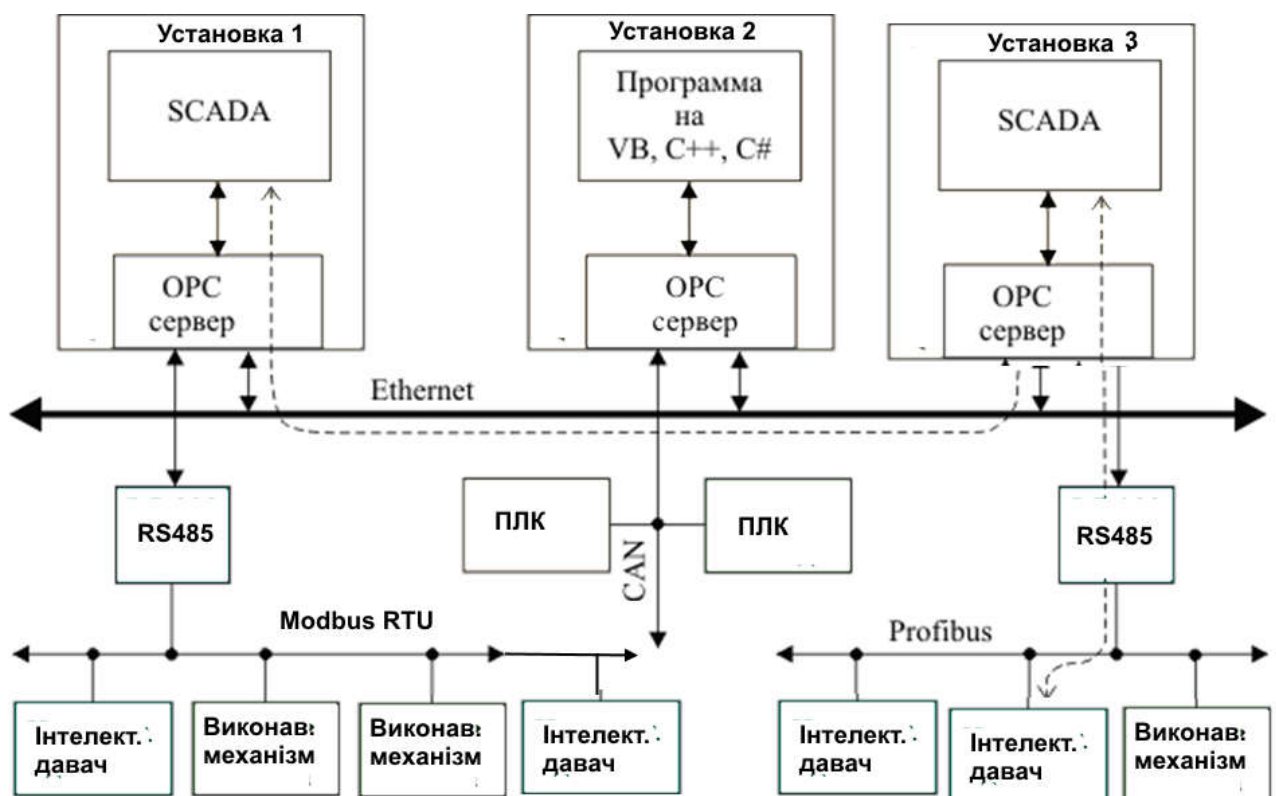


Рис. 1. Приклад використання OPC технології в системах автоматизації

Згідно аналітичному звіту [8] в програмному забезпеченні промислових систем керування знайдені вразливості, перелічені в табл.1.

В дослідженні пропонується звернути увагу на вразливість, яку ще не досліджено. Ця вразливість зв'язана з тим, що маючи розгалужену мережу робочих станцій на підприємстві, зломисник може підмінити OPC сервер на будь якій робочій станції (зазвичай, найбільш важливій на виробництві) власним OPC-сервером і зробити таким чином, щоб з одного боку привести технологічний апарат обраної ділянки до зупинки чи аварії, а з другого боку, щоб оператор технологічної установки спостерігаючи за SCADA-системою на екрані комп'ютера нічого не помітив.

Таблиця 1

Кількість основних вразливостей, які знайдені розробниками звіту [8] за рік в програмному забезпеченні промислових систем керування, та умовний рівень їх небезпеки

№	Найменування вразливості	Кількість вразливостей	Рівень небезпеки
1	Переповнення буфера	17	2
2	Міжсайтові скрипти	14	2
3	Вразливості обходу аутентифікації	14	2
4	Жорстко закодовані облікові дані	9	2
5	Неправильна перевірка введення	9	2
6	Вразливості при передачі конфіденційної інформації	8	1
7	Зберігання паролів	6	2
8	Необмежене завантаження файлу	5	2
9	Ін'єкція SQL	5	2

Основна частина

Для моделювання обрано технологічний процес ректифікації суміші ізопропіла з водою [9]. Структура комп'ютерної системи керування відповідає структурі установки 1 на рис. 1. В програмному забезпеченні моделюється система керування з ПІ-регуляторами, яка налаштована за принципами, описаними в роботі [10] і описується математичною моделлю, зображеною на рис.2.

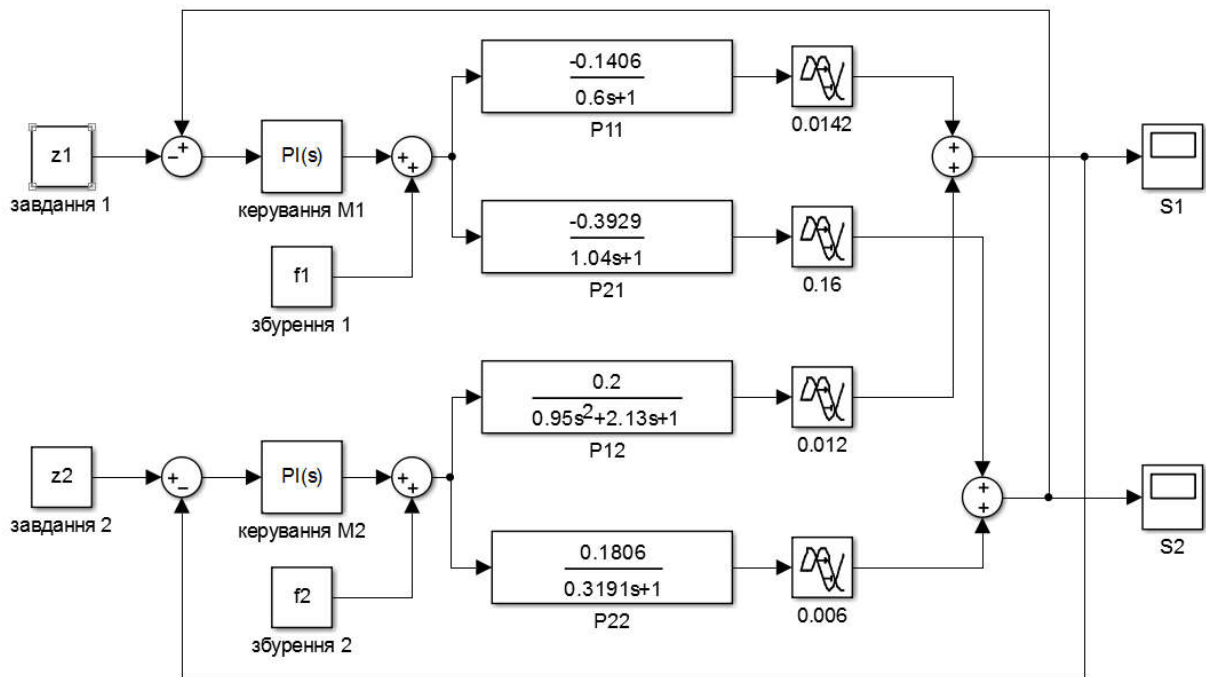


Рис. 2. Модель система керування ректифікаційною колоною (час в хвиликах)

Керовані змінні – температури зверху та знизу колони. Керуючі впливи – витрати пари і флегми (готового продукту, який повертається до колони для покращення розділення). S1 – це давач температури зверху, S2 – давач температури знизу, M1 – виконавчий механізм витрати флегми, M2 – виконавчий механізм витрати пари. Давачі і виконавчі механізми моделюються відповідно до технічної документації давачей типу TXTMINI-M12-485 і виконавчих механізмів TMB1-RTI Modbus Control Board for Electric Actuators. Бажаними показниками якості ходу технологічного процесу є підтримання температури зверху близької до 50 °С, температури знизу близької до 70°С. На технологічний процес діють збурення за живленням колони, тому використовується автоматичне керування.

Для початку моделювання системи кібербезпеки запустимо симулятор технологічного процесу. Симулятор написано мовою програмування Python. Технологічний процес і пристрої керування, які працюють за протоколом Modbus, моделюються в реальному часі. В якості емулятора нуль-модемного з'єднання використовується програма com0com.

Temperature Top :
50.0 Deg C

Temperature Btm :
70.0 Deg C

Reflux VLV :
50.0 %

Steam VLV :
50.0 %

	S1	S2		M1	M2
00	60001	60002	00	0	0
01	30001	30001	01	10	10
02	100	100	02	0	0
03	10	10	03	0	0
05	500	700	05	0	0
07	3	3	07	10	10
08	0	0	08	500	500
09	1	1	10	500	500
10	0	0	11	60	60
11	0	0	12	300	300
12	0	0	13	5	5
13	0	0	14	1000	1000
22	5	5	15	500	500

Column is operating in normal mode

Legend: Primary RW Primary R Secondary RW

Version: 0.10, Uptime: 0:00:03.022389

Port: COM4, Baud: 9600, Parity: None, XonXoff: False, StopBits:1

Рис. 3. Симулятор технологічного процесу для моделювання системи кібербезпеки

Основним робочим регістром давачей є регістр 5, який зберігає значення вимірювань як ціле число. Наприклад, 500 – це 50.1 °С. Для виконавчих механізмів найважливішими є три регістри. Регістр 0 вказує переміщення виконавчого механізму – значення 0 означає, що немає переміщення; 64 – переміщення за часовою стрілкою; 128 – переміщення проти часової стрілки. Регістр 8 зберігає поточне положення регулюючого органу, яке вимірюється давачем положення. Регістр 10 використовується для задавання нового положення. Значення в регістрах теж цілочислове.

Для реалізації зв'язку промислової мережі Modbus і комп'ютерної мережі використано популярний OPC-сервер фірми Insat (рис. 4). Сервер з'єднується з емулятором за допомогою нуль-модемного з'єднання. Кожен важливий параметр має свій відповідник –

тег, тобто структуровану змінну, значення якої прив'язано до певного регістру і масштабується сервером.

Теги					
Имя	Регион	Адрес	Значение	Качество	Время (UTC)
DC.Temperature Top.Measurement	SER...	--	50.099...	GOOD	2021-10-21 20:21:36.457
DC.Temperature Bottom.Measurement	SER...	--	70	GOOD	2021-10-21 20:21:36.457
DC.Reflux.MV	SER...	--	50	GOOD	2021-10-21 20:21:36.457
DC.Reflux.Moving	SER...	--	0	GOOD	2021-10-21 20:21:36.457
DC.Reflux.MVnow	SER...	--	50	GOOD	2021-10-21 20:21:36.457
DC.Steam.MV	SER...	--	50	GOOD	2021-10-21 20:21:36.457
DC.Steam.Moving	SER...	--	0	GOOD	2021-10-21 20:21:36.457
DC.Steam.MVnow	SER...	--	50	GOOD	2021-10-21 20:21:36.457

Сообщения		Запросы	Сообщения скриптов
Режим вывода: Запущен Фильтр: Все сообщения			
25-10-2021 20:21:36.457	Steam:	Запись в FromScript	значения ф
25-10-2021 20:21:36.457	MVnow:	Запись в DC.Reflux.MVnow	значения 50.000000
25-10-2021 20:21:36.457	Moving:	Запись в DC.Reflux.Moving	значения 0
25-10-2021 20:21:36.457	Reflux:	Ответ	Reflux:HOLDING_REGISTERS

Рис. 4. Копія головного вікна OPC-серверу

OPC-сервер є одним з вразливих елементів системи автоматизації, оскільки доступ до нього можуть мати всі комп'ютери мережі. Сам сервер має програмний інтерфейс за допомогою якого програмісти можуть змінювати його поведінку в реальному часі. Таким чином, можливо, наприклад, сфальсифікувати параметри. Захист від такої фальсифікації – актуальна задача.

Розглянемо як мету хакерської атаки зупинку технологічного процесу. Для цього хакеру необхідно відключити автоматичне керування і вивести витрату флегми та пари на 100% відкриття.

Запустимо комп'ютерне програмне забезпечення системи керування – SCADA-систему (рис. 5). Ця система реалізує процес керування і людино-машинний інтерфейс. Зв'язок з промисловою мережею в SCADA-системі реалізується за допомогою OPC-серверу. Вважаймо, що доступ до SCADA-системи хакер не має.

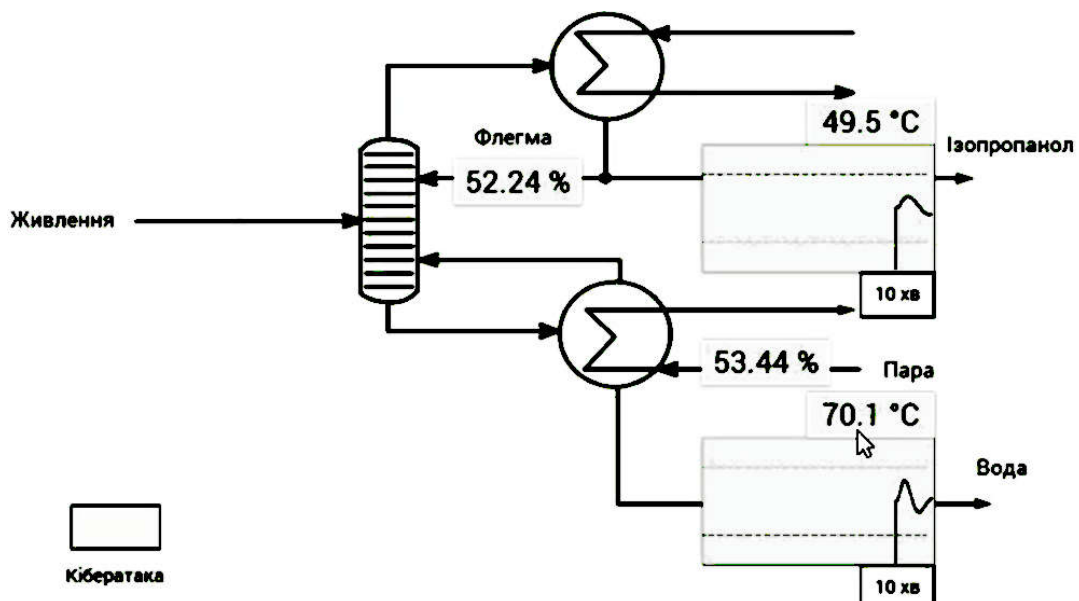


Рис. 5. Форма оператора-технолога в SCADA-системі

Дочекаємось часткової стабілізації параметрів технологічного процесу. Бачимо за трендами, що регулятори реалізують автоматичне керування.

Метою хакера є створити видимість того, що автоматичне керування продовжується і змінні більш-менш в регламентних межах. В той же час значення не мають бути постійними, бо для оператора технологічної установки це буде дуже помітним.

Хакер не має моделі технологічного процесу і не знає налаштувань регуляторів, тому для нього єдиним виходом щоб не видати себе є програмна імітація достатньо реалістичного продовження ходу технологічного процесу після зламу таким чином, щоб регулятори за заданий час не вийшли за регламентні межі. Це він реалізує шляхом заміни OPC-серверу на такий же, але перепрограмований під фальсифікацію показань давачей і положень виконавчих механізмів.

Проведемо підміну OPC-сервера, запустивши скрипт hack з командної консолі Windows (рис. 6).

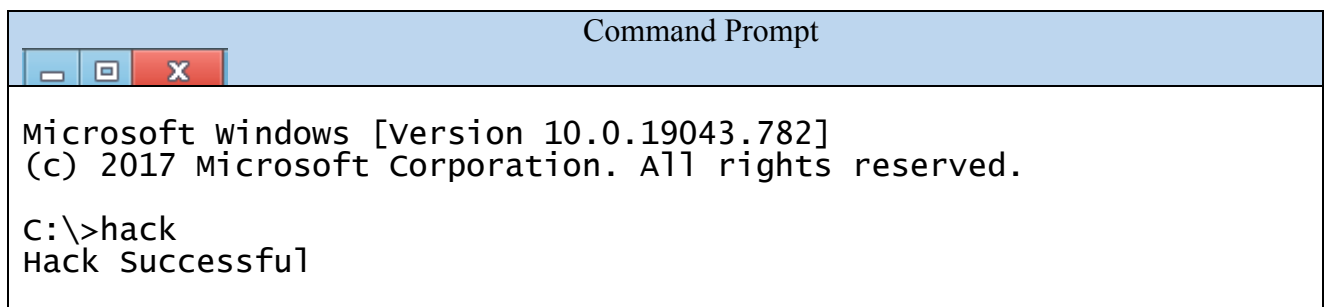


Рис. 6. Введення команди для зламу

Після цього станеться неконтрольоване збільшення положення виконавчих механізмів (бачимо що завдання на реальне положення виконавчих механізмів встановлені на 100% відсотків у вікні симулятора на рис. 7). Але на формі SCADA-системи цього помітно не буде (рис. 5).

	s1	s2		m1	m2
08	0	0	08	710	710
09	1	1	10	1000	1000

Рис. 7. Значення регістрів в симуляторі після зламу

В програмному забезпеченні SCADA-системи працює алгоритм виявлення зламу. Сутність цього алгоритму полягає в тому, що для кожного регулятора розраховується різниця між поточним й попереднім (секунду назад) значенням керуючого впливу. Якщо $u_i - u_{i-1} > 0$ і значення регістру 0 дорівнює 64, або $u_i - u_{i-1} < 0$ і значення регістру 0 дорівнює 128, або $u_{i-1} = 0$ і значення регістру 0 дорівнює 0, то процес керування йде вірно. При порушенні будь-якого з цих умов підраховується кількість таких порушень і якщо вона перевищує порогове значення (прийнято 10 підряд), то спрацьовує сигналізація в SCADA-системі (червоний прямокутник) й оператору передається повідомлення про хакерську атаку.

Бачимо, що OPC-сервер передає у промислову мережу значення керуючих впливів, яке дорівнює 100% (рис. 7). Відлік часу до порушення роботи колони почався. Програмне забезпечення, реалізоване в SCADA має виявити нестандартну поведінку. Критерієм нестандартної поведінки є відсутність руху регулюючого органу при підтвердженні зміни положення.

На формі SCADA-системи бачимо, що процес для оператора установки висвітлюється як нормальний (рис.8). Але розроблена система діагностики виявила злам і пропонує оператору технологічної установки зупинити OPC-сервер. Це він повинен зробити з допомогою спеціальної кнопки. Після її натискання оператором OPC-сервер буде зупинено разом зі SCADA-системою.

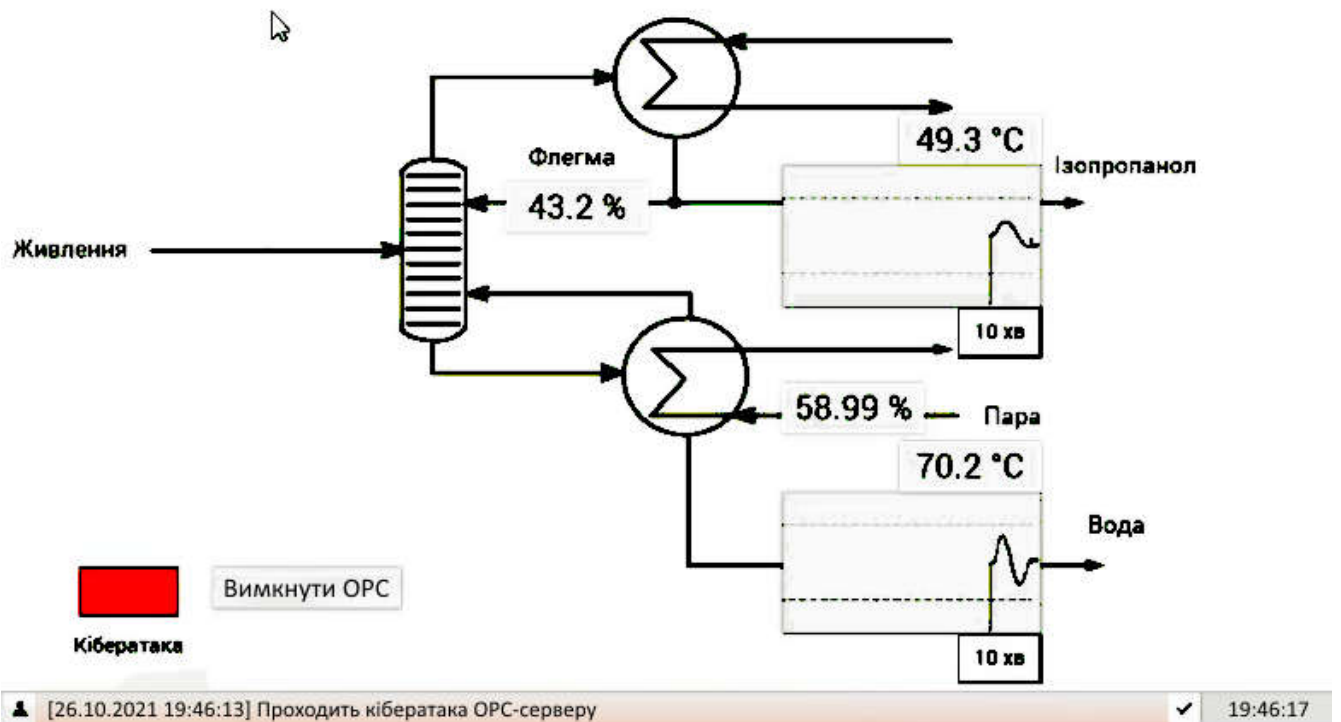


Рис. 8. Екран SCADA-системи після діагностування кібератаки

Після відімкнення SCADA-системи адміністратор мережі має повернути положення регулюючих органів за допомогою команд Modbus чи оператор технологічної установки має повернути положення регулюючих органів вручну за допомогою ручного дублера, який встановлений на кожному регулюючому органі. Далі системний адміністратор мережі повинен зрозуміти знаходження джерела зламу, усунути його та відновити роботу оригінального OPC-серверу. Після цього SCADA-систему треба запустити знову.

Висновки

Викрито можливість нової кібератаки на робочі станції керування технологічними установками промислових процесів. Сенс кібератаки полягає в тому, що по мережі, яка зв'язує технологічні станції, робиться підміна OPC-сервера, після чого технологічна установка зловмисником переводиться в аварійний стан таким чином, щоб оператор, спостерігаючи за технологічним процесом за допомогою SCADA-системи не міг помітити розбалансування процесу. Для виявлення кібератаки розроблено спеціальну діагностичну систему. Розроблено відповідне програмне забезпечення та, за його допомогою, всі рішення промодельовано в реальному часі з використанням компонентів реального промислового програмного забезпечення та моделі мережі Modbus. Розроблені рішення та програмне забезпечення можуть бути використані в промисловості.

Список літератури

1. Information security risks at industrial companies. Moscow: Positive Technologies, 2021. 7p.
2. Zegzhda D.P., Kalinin M.O., Levykin M.V. Actual Vulnerabilities of Industrial Automation Protocols of an Open Platform Communications Series. *Automatic Control and Computer Sciences*, 2019. Vol. 53, No. 8, pp. 972–979
3. Candell R., Anand D.M., Stouffer K. A Cybersecurity Testbed for Industrial Control Systems. *ISA Process Control & Safety Symposium*. Texas, Houston: ISA, 2014. 16p.
4. Adeyanjul I.A., Emake E.D., Olaniyan O.M., Omidiora E.O., Adefarati T., Uzedhe G.O., Okomba N.S. Digital Industrial Control Systems: Vulnerabilities and Security Technologies. *Current Applied Science and Technology*. Vol. 21. No. 1. P. 185–200.
5. Alves T., Das R., Morris T. Virtualization of Industrial Control System Testbeds for Cybersecurity. *ICSS '16*. Los Angeles, CA: ACM, 2016. P.1-19
6. Зозуля А.А., Стопакевич О.А. Вдосконалення протоколу Modbus RTU з метою підвищення кіберзахищеності комп'ютерно - інтегрованої АСУТП. 62 Міжнародна наук. конф. «Актуальні наукові дослідження в сучасному світі». Переяслав, 2020. Вип. 6 (62). Ч. 2. С. 49-53.
7. Энциклопедия АСУ ТП. OPC сервер. URL: https://www.bookasutp.ru/chapter9_2.aspx
8. Andreeva O., Gordeychik S., Gritsai G., Kochetova O., Potseluevskaya E., Sidorov S., Timorin A. Industrial control systems vulnerabilities statistics. Moscow: Kaspersky Lab, 2015. 18p.
9. Yadav E.S., Indiran T., Priya S.S., Fedele G. Parameter Estimation and an Extended Predictive-Based Tuning Method for a Lab-Scale Distillation Column. *ACS Omega*, 2019. Vol. 4, No. 25. P. 21230–21241.
10. Stopakevych, A., Stopakevych, O. Design of robust controllers for plants with large dead time. *Eastern-European Journal of Enterprise Technologies*, 2016. Vol. 1. No. 2. P. 48-56. <https://doi.org/10.15587/1729-4061.2016.59107>

**SIMULATION SYSTEM OF CYBERATTACK BY OPC SERVER REPLACEMENT
IN COMPUTER CONTROL SYSTEMS OF TECHNOLOGICAL PLANTS**

A.A. Zozulya, O.A. Stopakevich, A.O. Stopakevich

National Odessa Polytechnic University

1, Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: stopakevich@gmail.com

According to a September 2021 report by Positive Technologies, 91% of the world's industrial companies have information systems vulnerable to cyberattacks. The industrial sector is the second most attacked sector in the U.S., and the leading one in developed countries. Ukraine ranks sixth and seventh in the top 20 for the largest industrial attacks. Many scientific publications are devoted to industrial cybersecurity in the world, but, unfortunately, in Ukraine this area of cybersecurity is poorly studied. To develop the topic of increasing the level of cybersecurity of industrial control systems, we focused on the problems of cybersecurity of the lower level of control - the operator control station of the technological plant. Previously, we investigated the problem of cybersecurity of the industrial computer network of the lower level Modbus RTU. Continuing the topic, in this paper we investigate the cybersecurity of important software - the OPC server. This study proposes to pay attention to a vulnerability that has not yet been investigated. This vulnerability is related to the fact that having an extensive network of workstations in the enterprise, an attacker can substitute OPC server on any workstation (usually the most important one in production) with his own OPC server and do it in such a way that on the one hand to bring the technological unit of the selected site to stop or crash, but on the other hand to prevent the operator of technological unit, watching the SCADA-system on the computer screen, from noticing anything. A special diagnostic system has been developed to detect a cyber attack. Appropriate software has been developed and, with its help, all solutions have been simulated in real time using components of real industrial software and Modbus network model. The developed solutions and software can be used in industry.

Keywords: Cyber-attack, cyber defense, OPC, OLE for Process Control, SCADA, process control system.

МОДИФІКАЦІЇ АЛГОРИТМУ ВИЯВЛЕННЯ РУХУ КАМЕРИ**В.В. Кордюк, О.Ю. Лебедєва**Національний університет «Одеська політехніка»,
пр. Шевченко, 1, Одеса, 65044, Україна; e-mail: o.y.lebedieva@op.edu.ua,

Відеоаналіз – дуже необхідний інструмент у системах відеоспостереження з однією або великою кількістю камер. Серед найбільш перспективних функцій при цьому є відстеження переміщень об'єктів – трекінг. У роботі розглядається сучасний стан розробок в області трекінгу. Існує кілька типів трекінгу. Pixel tracking – це відстеження руху конкретної точки (пікселя) або групи точок на вихідній відеопослідовності. В результаті цього процесу виходить траєкторія руху пікселя, відповідного руху якогось об'єкта в кадрі. Matchmoving – це складний процес, який дозволяє за наявної відеопослідовності створити тривимірну сцену з цифровою камерою, яка в точності повторює рух реальної знімальної камери. Motion capture – це технологія, призначена для визначення позиції і орієнтації реального об'єкта в віртуальному середовищі, визначення позиції і орієнтації реального об'єкта в просторі здійснюється за допомогою спеціальних датчиків та маркерів. Кожен з означених типів трекінгу може використовуватися як сам по собі, так і бути частиною більш складних процесів. У роботі розроблено модифікацію алгоритму виявлення руху камери, який працює в області pixel tracking. Наводиться опис основних підходів до оцінки руху, а саме рекурсивні растрові алгоритми, алгоритми частотної області, алгоритми оптичного потоку та методи відповідності блоків. Наводяться актуальність роботи, її мета та задачі. В роботі описується спосіб розташування блоків в кадрі відеопослідовності, які використовуються для обчислення руху камери. В якості оцінки подоби блоків використовуються метрики подоби, а саме коефіцієнт кореляції. В роботі описуються кроки розробленої модифікації алгоритму виявлення руху камери. Наводяться результати роботи модифікації алгоритму виявлення руху камери. Результат роботи це показник візуальної якості трекінгу у вигляді 2d-зображення вектору руху камери.

Ключові слова: цифрова відеопослідовність, цифрове зображення, трекінг, метрики подоби, виявлення руху камери.

Вступ

Питання безпеки будинку, офісу, підприємства дуже актуальне у сучасному світі. У зв'язку з цим виникає життєва важлива потреба в охоронних підприємствах, службах безпеки та охоронцях. Але технічний прогрес не стоїть на місці, і на допомогу охоронцям надходить відеоспостереження. Системи відеоспостереження стають невід'ємною частиною охоронних комплексів. Завдяки таким системам охорона може своєчасно відреагувати на дії зловмисників та припинити їх. За останнє десятиліття відеоспостереження набуло широкого поширення і сьогодні залишилося мало об'єктів, не обладнаних системами відеоспостереження.

Від швидкого прогресу в технології автономних систем та засобів для відеоспостереження до більш повсякденних функцій допомоги оператору в сучасних системах безпеки, відеоспостереження майбутнього все більше покладається на досягнення в області комп'ютерного зору для більшої безпеки та зручності.

Досягнення в області комп'ютерного зору відіграють вирішальну роль у вирішенні проблем в системах безпеки все більш ефективними способами. Привабливість комп'ютерного зору для цих цілей передусім пов'язана з економічною ефективністю цих

технологій, а також із широким спектром застосувань, які може підтримувати комп'ютерний зір. Тому дана робота є актуальною.

Метою роботи є розробка модифікації алгоритму виявлення руху відеокамери шляхом аналізу чотирьох блоків у кожному кадрі відео.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

- Проаналізувати стан сучасних розробок в області трекінгу;
- Проаналізувати та виявити слабкі місця розробленого алгоритму виявлення руху відеокамери;
- Розробити основні кроки модифікації алгоритму виявлення руху відеокамери;
- Розробити програмний продукт для розробленої модифікації алгоритму виявлення руху відеокамери; провести експерименти, спрямовані на порівняння показника візуальної якості трекінгу.

Під показником візуальної якості трекінгу будемо розуміти 2D-зображення вектору руху камери.

Основна частина

Відеоаналітика – технологія, що використовує методи комп'ютерного зору для автоматизованого отримання різних даних на підставі аналізу послідовності зображень, що надходять із відеокамер у режимі реального часу або з архівних записів. Відеоаналітика є програмним забезпеченням (ПЗ) для роботи з відеоконтентом. В основі програмного забезпечення лежить комплекс алгоритмів машинного зору, що дозволяють вести відеомоніторинг та проводити аналіз даних без прямої участі людини. Алгоритми відеоаналітики можуть бути інтегровані в різні бізнес-системи, які найчастіше використовуються у відеоспостереженні та інших сферах безпеки.

Відстеження відео – це процес виявлення об'єкта, що рухається, з часом за допомогою камери. Він має безліч застосувань, у тому числі: взаємодія людини з комп'ютером, безпека та спостереження, відеозв'язок і стиснення, доповнена реальність, управління трафіком, отримання медичних зображень і т. д. Відстеження відео може зайняти багато часу через велику кількість даних, що містяться у відео. Ще більше ускладнює ситуацію можлива необхідність використання методів розпізнавання об'єктів для відстеження, що є складним завданням.

Мета відстеження відео – пов'язати цільові об'єкти у послідовних відеокадрах. Асоціація може бути особливо складною, коли об'єкти швидко рухаються щодо частоти кадрів. Ще одна ситуація, що ускладнює проблему, - це коли об'єкт, що відстежується, з часом змінює орієнтацію. Для цих ситуацій системи відеоспостереження зазвичай використовують модель руху, яка описує, як зображення мети може змінитися при різних можливих рухах об'єкта.

Трекінгом називається визначення розташування об'єкта, що рухається в часі за допомогою камери. Алгоритм аналізує кадри відео і видає положення цільових об'єктів, що рухаються, відносно кадру.

Існує кілька типів трекінгу [1]:

- Pixel Tracking;
- Matchmoving;
- Motion Capture.

Кожен з типів трекінгу може використовуватися як сам по собі, так і бути частиною більш складних процесів.

Pixel Tracking – це відстеження руху конкретної точки (пікселя) на вихідному відео ряді. В результаті цього процесу виходить траєкторія руху пікселя, відповідного руху

якогось об'єкта в кадрі. Причому, в залежності від завдання можна відстежувати як одну точку, так і цілу групу точок.

Matchmoving (з англ. повторення руху) – це складний процес, який дозволяє за наявним відео-ряду створити тривимірну сцену з цифровою камерою, яка в точності повторює рух реальної знімальної камери.

Motion Capture (з англ. захоплення руху) – це технологія, призначена для визначення позиції і орієнтації реального об'єкта (наприклад, руки, голови або спеціального пристрою) в віртуальному середовищі. Визначення позиції і орієнтації реального об'єкта в просторі здійснюється за допомогою спеціальних датчиків та маркерів.

У різних публікаціях запропоновано такі підходи до оцінки руху: рекурсивні растрові алгоритми, алгоритми частотної області, алгоритми оптичного потоку та методи відповідності блоків.

Рекурсивні растрові алгоритми використовують ітеративне вдосконалення оцінки руху для окремих елементів растрових зображень, які виконуються градієнтними методами, для передбачення рекурсивного усунення кожного елемента растру від його сусідніх елементів. Ці алгоритми мають більшу обчислювальну складність і менше піддаються налаштуванню, тому їх важко використовувати в апаратних засобах.

Частотні методи оцінки руху застосовуються для глобальної оцінки руху кадру (Global Motion). Найбільш відомим із цих методів є фазовий метод кореляції на основі перетворення Фур'є. Існуючі алгоритми визначення глобального руху кадру використовуються як для стиснення, так і для обробки відеоматеріалів, наприклад, задачах побудови панорамного зображення або стабілізації відео з тремтіння кадру.

Алгоритми визначення глобального руху кадру можна розділити на три групи [2]:

- Алгоритми, які використовують особливі точки (Feature Points), наприклад, алгоритм 2D Ridge Motion;
- Алгоритми, які використовують вектори руху (Motion Vector);
- Алгоритм глобального пошуку.

Алгоритми з кожної групи мають характерні сильні і слабкі сторони. Так, застосування апарату особливих точок потребує значних тимчасових витрат на вибір спеціальних точок (Feature Points Selection) та на їх відстеження (Feature Points Tracking). Перевагою цих алгоритмів є висока надійність визначення зсувів.

Використання векторів руху (Motion Estimation) дає нижчу надійність визначення зсувів, ніж особливі точки. Але алгоритми визначення векторів руху мають велику перевагу – високу швидкість.

Під алгоритмами глобального пошуку розуміються алгоритми, що визначають глобальний рух по всьому кадру без застосування проміжних перетворень.

Алгоритми відповідності блоків оцінюють рух на підставі прямокутних блоків та обчислюють один вектор руху для кожного блоку. Ці алгоритми є найбільш підходящими для такої апаратної реалізації через їх продуману модифікацію і простоту.

Цифрове відео є впорядкованим набором зображень, або кадрами. Саме тому стосовно нього часто використовують термін відеопослідовність. При послідовному виведенні цих кадрів на екран створюється імітація «живого» зображення. Для здобуття злитого, плавного руху без ривків, використовується особливість людського зору. Людський зір володіє інертністю, тобто око продовжує бачити предмет ще деякий час після того, як предмет перемістився або зник з поля зору в інше місце. Таким чином, якщо змінювати кадри на екрані з достатньою швидкістю, людина бачитиме наступний кадр в той час, як попередній ще не потухнув остаточно.

Вважатимемо, що маємо відео, яку зняла цифрова відеокамера. Цифрове відео при обробці представлено набором кадрів. Кадрами є статичні зображення. Вважатимемо, що можна отримати будь-який кадр з відео. Отриманий кадр це зображення в моделі RGB.

Кожний кадр перетворюється до моделі YUV і в подальшому огляді ми будемо використовувати для аналізу тільки складову Y.

Нехай є відеопослідовність, що складається з безлічі кадрів $F = F_1 \cup F_2 \dots \cup F_n$, де n – кількість кадрів, F_i – i -ий кадр. Кожний кадр має розмір $M \times N$. Розглянемо два сусідніх кадру F_i та F_{i+1} . Кадр F_i розіб'ємо на чотири не пересічні блоки $P^i = \{P_1^i, P_2^i, P_3^i, P_4^i\}$, які розташуються по периметру кадру (рис. 1).

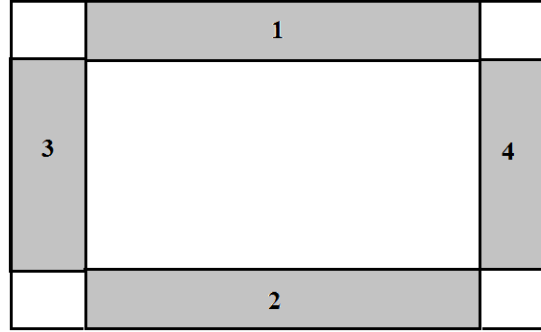


Рис. 1. Блоки периметру, що аналізуються

Тоді модифікація алгоритму виявлення руху відеокамери має наступні кроки:

1. Маємо відео V , яке складається з кадрів $F_1, F_2, \dots, F_t$. Нехай F_i – це i – кадр, цифрове зображення розміром $n \times m$.

2. Для кожної пари кадрів F_i та F_{i+1} :

2.1 Кадр F_i розіб'ємо на чотири блоки $P^i = \{P_1^i, P_2^i, P_3^i, P_4^i\}$, які розташуються по периметру кадру. Нехай $(x_1, y_1), (x_2, y_2), \dots, (x_4, y_4)$ – координати лівої верхньої вершини блоків P^i . Нехай f – зміщення для пошуку.

2.2 Розбити кадр F_{i+1} на множину пересічних блоків $S^{i+1} = \{s_1^{i+1}, \dots, s_q^{i+1}\}$, для кожного з чотирьох блоків, починаючи з координати $(x_i - f, y_i - f)$ до координати $(x_i + f, y_i + f)$, де (x_i, y_i) – координати лівої верхньої вершини блоку P_j^i .

2.3 Для кожної пари блоків P_j^i та s_k^{i+1} обчислити коефіцієнт метрики між двома блоками. Нехай mk_w – значення коефіцієнту метрики подібності для пари блоків P_j^i та s_k^{i+1} . Нехай після розглядання всієї множини пересічних блоків маємо послідовність значень коефіцієнту метрики подібності $MK = \{mk_1, mk_2, \dots, mk_q\}$.

2.4 Серед значень $MK = \{mk_1, mk_2, \dots, mk_q\}$ знайдемо екстремум та координати лівої верхньої вершини блоку s_k^{i+1} , якому відповідає екстремум. Нехай ці координати є (x_r, y_r) , позначимо їх, як вектор руху як вектор руху блоку P_j^i , $\overline{v_j} = (-x_r, -y_r)$, $\overline{v_z} = (-x_r, -y_r)$.

2.5 Аналізуємо отримані вектори для кожного блоку $P^i = \{P_1^i, P_2^i, P_3^i, P_4^i\}$ на i -кадрі. Результатом аналізу є вектор руху $\overline{v_z}$ між двома кадрами F_i та F_{i+1} .

3. Після проходження усіх кадрів маємо вектор руху камери для відео: $\overline{v} = \{\overline{v}_1, \overline{v}_2, \dots, \overline{v}_t\}$.

Для оцінки подоби блоків використовується метрика кореляція Пірсона. Кореляція обчислюється за формулою

$$Correlation = \frac{\sum_{ij} \left(Y_{ij} - \frac{1}{MN} \sum_{ij} Y_{ij} \right) \left(Y'_{ij} - \frac{1}{MN} \sum_{ij} Y'_{ij} \right)}{\sqrt{\sum_{ij} \left(Y_{ij} - \frac{1}{MN} \sum_{ij} Y_{ij} \right)^2 \cdot \sum_{ij} \left(Y'_{ij} - \frac{1}{MN} \sum_{ij} Y'_{ij} \right)^2}}$$

де Y_{ij} значення яскравості пікселя к-го кадру, що перебуває на перетині і строки та j стовпця;

Y'_{ij} - значення яскравості пікселя к-1 -го кадру, що перебуває на перетині і строки та j стовпця.

Коефіцієнт кореляції може приймати значення від мінус одного до плюс одного. При цьому негативний коефіцієнт кореляції дозволяє прийняти гіпотезу про наявність лінійного негативного зв'язку.

Зазвичай, кореляція цифрових зображень ґрунтується на максимізації коефіцієнта кореляції, який визначається інтенсивністю масиву розглянутих пікселів на двох і більше відповідних зображеннях.

Для проведення експериментів, спрямованих на оцінку ефективності розробленого алгоритму та порівняння показника візуальної якості трекінгу використовувалось 50 відеопослідовностей.

Під показником візуальної якості трекінгу розуміємо 2D-зображення вектору руху камери.

Для перевірки розробленої модифікації алгоритму виявлення руху відеокамери, здійсненої шляхом використання в алгоритмі коефіцієнта кореляції.

Експеримент проводився над відео з різним розташуванням камери: всередині або поза об'єктом руху. Приклади результатів з використанням коефіцієнту кореляції зображені на рис. 2.



Рис. 2а. Результати трекінгу

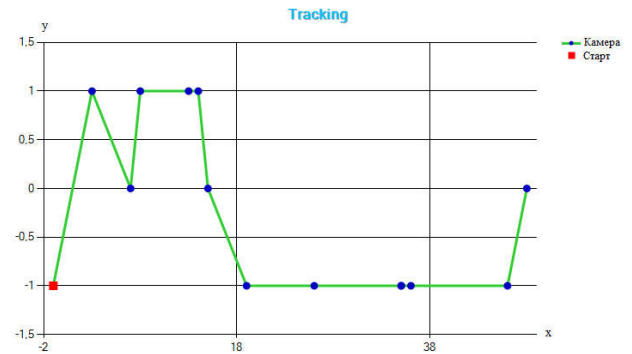
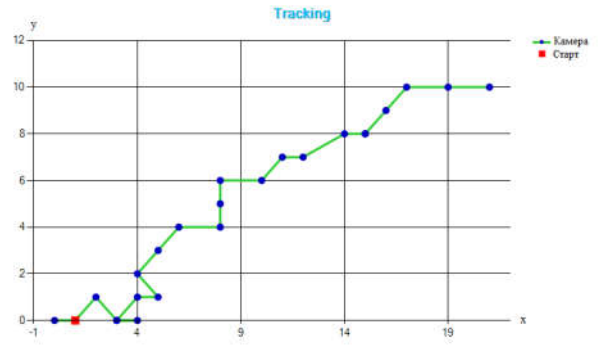


Рис. 26. Результати трекінгу

Висновки

Проведено аналіз стану сучасних розробок в області трекінгу. Розглядалися підходи до оцінки руху. Розроблено модифікацію алгоритму виявлення руху відеокамери шляхом аналізу чотирьох блоків у кожному кадрі відео. У розробленій модифікації алгоритму виявлення руху відеокамери розглядались чотири блоку, що в сукупності складають периметр кадру, крім кутових блоків, що дозволяє обчислити рух камери, коли вона розташована в середині або на об'єкті, що рухається.

Список літератури

1. Трекінг. URL: http://maskedbrothers.ru/articles/tracking_basic
2. Буряченко В.В. Стабилизация видео для статичной сцены на базе модифицированного метода соответствия блоков. *Вестник Сибирского государственного аэрокосмического университета им. академика М.Ф. Решетнева*. – 2012. – С. 10-15.

MODIFICATIONS OF THE CAMERA MOTION DETECTION ALGORITHM

V.V. Kordyuk, O.Yu. Lebedieva

National Odessa Polytechnic University

1, Shevchenko Ave., Odessa, 65044, Ukraine, e-mail: o.y.lebedieva@op.edu.ua,

Video analysis is a very important tool in video surveillance systems with one or more cameras. Among the most promising features are tracking the movement of objects - tracking. The current state of development in the field of tracking is considered in the work. There are several types of tracking. Pixel Tracking is the tracking of the movement of a specific point (pixel) or group of points on the original video sequence. The result of this process is the trajectory of the pixel, corresponding to the movement of an object in the frame. Matchmoving is a complex process that allows you to create a three-dimensional scene with a digital camera based on the available video sequence, which exactly repeats the movement of a real camera. Motion Capture is a technology designed to determine the position and orientation of a real object in a virtual environment, determining the position and orientation of a real object in space is carried out using special sensors and markers. Each of these types of tracking can be used on its own or as part of more complex processes. The paper develops a modification of the camera motion detection algorithm, which works in the field of Pixel Tracking. The description of the main approaches to motion estimation is given, namely recursive raster algorithms, frequency domain algorithms, optical flow algorithms and block matching methods. The urgency of the work, its purpose and objectives are given. The paper describes a method of arranging blocks in a video sequence frame, which are used to calculate the movement of the camera. Similarity metrics are used to estimate the similarity of the blocks, namely the correlation coefficient. The paper describes the steps of the developed modification of the camera motion detection algorithm. The results of the modification of the camera motion detection algorithm are presented. The result of this work is an indicator of the visual quality of tracking in the form of a 2D image of the camera motion vector.

Keywords: digital video sequence, digital image, tracking, similarity metrics, camera motion detection.

**МЕТОД РОЗВ'ЯЗКУ ЗАДАЧІ ПРО ВИБІР КОНТЕЙНЕРА, ЩО ЗАБЕЗПЕЧУЄ
МАЛУ ЧУТЛИВІСТЬ СТЕГАНОВІДОМЛЕННЯ ДО ЗБУРНИХ ДІЙ****О.Ю. Надвоцький, А.А. Кобозєва**Національний університет «Одеська політехніка»
1, пр.Шевченка, Одеса, 65044, e-mail: alla_kobozeva@ukr.net

З розвитком інформаційних технологій зростають вимоги до стеганографічних систем. Сьогодні стеганосистема повинна протистояти стеганоаналітичним атакам, що використовують найсучасніші математичні базиси, атакам проти вбудованого повідомлення, які просто і якісно реалізуються в будь-якому сучасному програмному середовищі, забезпечувати значну пропускну спроможність при організації прихованого каналу зв'язку, тощо. Для забезпечення цих вимог потрібно використовувати всі можливі засоби. Одним із способів, що сприяє забезпеченню певної вимоги, є вибір контейнера, в якості якого в роботі розглядається цифрове зображення. Вибір контейнера відбувається з метою забезпечення кращих характеристик стеганоповідомлення в певному сенсі. Метою роботи є забезпечення можливості вибору цифрового зображення-контейнера, що породжує стеганоповідомлення, нечутливе до збурних дій. В роботі отримані наступні результати: теоретично обгрунтовано та практично підтверджено доцільність використання збурень власних векторів матриці контейнера як показників захищеності вбудованої в контейнер додаткової інформації; запропонована кількісна оцінка збурення власного вектору матриці цифрового зображення в результаті стеганоперетворення, яка дає змогу для відокремлення чутливого власного вектора від нечутливого, адекватно відображає збурення вектора незалежно від величини кута повороту; запропонована умова вибору захищених від збурної дії власних векторів, що враховує індивідуальні характеристики контейнера; запропонована формула для розрахунку обсягу захищеної додаткової інформації; розроблений метод вибору контейнера, що забезпечує малу чутливість стеганоповідомлення до збурних дій з наявної множини потенційних контейнерів.

Ключові слова: стеганосистема, стеганоповідомлення, вибір контейнера, цифрове зображення, атака проти вбудованого повідомлення, чутливість стеганоповідомлення до збурних дій, власне значення, власний вектор.

Вступ

Стеганографія сьогодні є одним з найпотужніших засобів захисту інформації, яка передбачає приховування самого факту наявності секретної інформації [1,2]. З розвитком інформаційних технологій зростають вимоги до стеганографічних систем. Сьогодні стеганосистема повинна протистояти стеганоаналітичним атакам, що використовують найсучасніші математичні базиси, атакам проти вбудованого повідомлення, які просто і якісно реалізуються в будь-якому сучасному програмному середовищі, забезпечувати значну пропускну спроможність при організації прихованого каналу зв'язку, надійність сприйняття формованого стеганоповідомлення, малу обчислювальну складність використовуваних стеганоалгоритмів для роботи в режимі реального часу тощо.

Переважає кількість сучасних стеганоалгоритмів розраховані на застосування випадкового контейнера, що взагалі вважається їх позитивною характеристикою, але, враховуючи значні труднощі для забезпечення згаданих вище вимог до стеганосистеми, не можна нехтувати таким додатковим джерелом, як вибір контейнера, в якості якого в роботі розглядається цифрове зображення (ЦЗ). В відкритих джерелах питання вибору контейнеру є маловивченим, одною з причин чого є обов'язково присутня значна обчислювальна складність такої задачі, оскільки передбачає, як правило, прямий перебір всіх можливих варіантів (ЦЗ-контейнерів) [3]. Але очевидно, що тут можливий деякий компроміс між

забезпеченням певної вимоги до стеганосистеми (стеганоповідомлення) та обчислювальною складністю (кількістю потенційно можливих контейнерів), досягнення якого буде залежити від ступеня критичності кожної з цих складових в конкретних умовах функціонування стеганосистеми. Таким чином, задача вибору контейнеру з метою забезпечення кращих характеристик стеганоповідомлення в певному сенсі є важливою та актуальною задачею сучасної стеганографії. Взагалі така задача може розв'язуватися з урахуванням різних критеріїв. Так вибір контейнера є актуальним в умовах організації прихованого каналу зв'язку при забезпеченні стійкості стеганосистеми до стеганоаналізу, зокрема при використанні LSB-методу [4], де оригінальне зображення принципово можна підібрати так, щоб воно вже містило в собі необхідну додаткову інформацію з урахуванням стеганошляху та секретного ключа, що зробить будь-який стеганоаналітичний метод неспроможним тут виявити факт обміну даними [3]. Задача вибору контейнера (локалізації частини контейнера, яка використовується для стеганоперетворення) може ставити за мету забезпечення, по можливості, найменшого спотворення в результаті стеганоперетворення обраним алгоритмом [5] та ін.

Як вже зазначалося вище, одною з основних вимог до стеганосистеми є вимога стійкості до атак проти вбудованого повідомлення, тобто атак, що збурюють матрицю стеганоповідомлення. Рівень розвитку графічних редакторів на сьогодні є настільки високим, що змінення ЦЗ з їх допомогою стає легким, простим, непомітним, що призводить до значного полегшення проведення атак проти вбудованого повідомлення [3], серед яких накладання різноманітних шумів, фільтрація, розмиття, стиск з втратами, геометричні атаки. В таких умовах навіть використання стійких до збурних дій стеганоалгоритмів часто не забезпечує бажану ефективність декодування додаткової інформації (ДІ), підвищення якої можливо шляхом вибору контейнера (зі скінченної множини потенційно можливих), який би забезпечував найменшу чутливість стеганоповідомлення до збурних дій. В [6] розглядалося питання розв'язку задачі вибору контейнера з наявної множини ЦЗ для забезпечення, по можливості, малої чутливості формованого стеганоповідомлення до атак проти вбудованого повідомлення, запропонований відповідний метод. Значною перевагою згаданого методу є відсутність обмежень на область його застосування як в сенсі використовуваних стеганографічних алгоритмів, так і в сенсі конкретики атак проти вбудованого повідомлення, що є результатом використання в якості математичного базису загального підходу до аналізу стану й технології функціонування інформаційних систем, заснованого на теорії збурень та матричному аналізі [7], тому саме цій роботі приділена основна увага в даній статті. В [6] було введено поняття додаткової інформації, захищеної від збурення (ЗІ), формальним представленням якого є матриця E з розмірами, відповідними розмірам зображення, що піддається збурній дії. Обсяг ЗІ обчислювався з урахуванням збурень захищених власних векторів (ВВ) і абсолютних відокремленостей відповідних власних значень (ВЗ) матриці ЦЗ [7], в якості кількісного показника збурення захищеного ВВ з урахуванням його нормованості розглядався синус кута його повороту в результаті стеганоперетворення (не враховуючи можливість того, що кут повороту ВВ на практиці може бути не обов'язково гострим), а захищені власні вектори визначалися з урахуванням абсолютної відокремленості відповідного власного значення, при цьому ця абсолютна відокремленість виступала ще як ваговий коефіцієнт при розрахунках обсягу ЗІ, тобто враховувалася двічі, доцільність чого не була достатньо обгрунтована. Вищенаведене залишає актуальною задачу вибору ЦЗ-контейнера, що забезпечує для відповідного стеганоповідомлення нечутливість до збурних дій, яка розглядається в даній роботі, удосконалення процесу цього вибору.

Мета статті й постановка досліджень

Метою роботи є забезпечення можливості вибору цифрового зображення-контейнера, що породжує стеганоповідомлення, нечутливе до збурних дій, шляхом розробки

відповідного методу на основі загального підходу до аналізу стану й технології функціонування інформаційних систем [7].

Для досягнення поставленої мети в роботі розв'язуються наступні *задачі*:

1. Обґрунтувати вибір формальних параметрів цифрового зображення, їх кількісні характеристики, збурення яких можуть використовуватися як показники захищеності вбудованої в контейнер ДІ;
2. Обґрунтувати спосіб кількісної оцінки збурення ВВ в результаті стеганоперетворення;
3. Визначити поняття ВВ, захищеного від збурної дії;
4. Отримати кількісну оцінку для обсягу додаткової інформації, захищеної від збурної дії;
5. Розробити метод вибору контейнера, що забезпечує малу чутливість стеганоповідомлення до збурних дій.

Основна частина

Нехай формальним представлення ЦЗ-контейнера є одна $n \times n$ -матриця F . По аналогії з [6] будемо вважати, що в процесі стеганоперетворення було проведено перетворення матриці контейнера, що забезпечує її симетричність, тобто: $F = F^T$. Симетричність матриці забезпечує наявність для неї нормального спектрального розкладання [6]:

$$F = U \Lambda U^T, \quad (1)$$

де $\Lambda = \text{diag}(\lambda_1, \lambda_2, \dots, \lambda_n)$ - діагональна матриця власних значень F , U - ортогональна матриця, тобто $U^T U = I$, де I - одинична $n \times n$ -матриця, стовпці $u_1, u_2, \dots, u_n$ матриці U - ортонормовані лексикографічно додатні ВВ F .

Відповідно до загального підходу до аналізу стану й технології функціонування інформаційних систем [7] будь-яке перетворення симетричної матриці F , зокрема стеганоперетворення (незалежно від конкретного стеганоалгоритму), може бути формально представлено у вигляді сукупності збурень власних значень та/або власних векторів матриці, які однозначно визначаються її нормальним спектральним розкладанням. Таким чином, сукупність таких збурень може розглядатися як формальне представлення додаткової інформації, вбудованої в контейнер з матрицею F , результатом «розподілу» ДІ по ВЗ і ВВ в області нормального спектрального розкладання. В [6] для оцінки обсягу ДІ, захищеної від збурної дії E , враховувалися як характеристики ВВ, так і ВЗ, зокрема, їх абсолютних відокремленостей, що для ВЗ λ_i визначається відповідно до формули:

$$\text{gap}_{abs}(i, F) = \min_{i \neq j} \|\lambda_j\| - \|\lambda_i\|.$$

Однак ВЗ симетричної матриці F є нечутливими [8] до збурних дій згідно з формулою:

$$\max_{1 \leq j \leq n} \|\lambda_j(F) - \lambda_j(F + E)\| \leq \|E\|_2 \quad (2)$$

де E - $n \times n$ -матриця збурення, $\|\cdot\|_2$ - спектральна матрична норма [8], $\lambda_j(F)$, $\lambda_j(F + E)$ - ВЗ матриць F , $F + E$ відповідно, а тому їх абсолютна відокремленість майже не змінюється при вбудові ДІ, оскільки збурна дія, що є формальним представленням стеганоперетворення, є незначною, бо інакше таке стеганоперетворення не гарантувало б забезпечення надійності сприйняття стеганоповідомлення. Отже, збурення ВЗ, їх абсолютних відокремленостей практично «не несуть в собі» вбудованої інформації. Збурення ВЗ не залежать від розподілу ДІ по (збуренням) ВВ матриці контейнера. Крім того, оскільки ВЗ є нечутливими до збурних дій, то вони принципово не можуть характеризувати чутливість до збурних дій формованого

стеганоповідомлення, яке може бути як чутливим, так і нечутливим, чого не можна сказати про ВВ, враховуючи, що чутливість ВВ u_i , який відповідає ВЗ λ_i , в межах матриці F визначається відповідно до співвідношень [8]:

$$\frac{1}{2} \sin \theta_i \leq \frac{\|E\|_2}{\text{gap}_{abs}(i, F)}, \quad \frac{1}{2} \sin \theta_i \leq \frac{\|E\|_2}{\text{gap}_{abs}(i, F + E)}, \quad (3)$$

де θ_i — кут між u_i і $\bar{u}_i$, $\bar{u}_i$ — нормований збурений ВВ u_i . Врахування абсолютної відокремленості ВЗ як вагового коефіцієнта при розрахунку обсягу захищеної інформації в [6] є не тільки недоцільним, але й шкідливим. Дійсно, $\|E\|_2$ — це верхня межа збурень ВЗ в результаті стеганоперетворення відповідно з (2), але конкретні збурення, що зазнаються різними ВЗ в результаті вбудови ДІ є різними, на практиці залежать не від обсягу ДІ, а від величини модуля ВЗ (найбільше збурюються найбільші за модулем ВЗ), відмінності в збуреннях не залежать від особистостей стеганоперетворення, не характеризують процес вбудови ДІ.

Такий теоретичний висновок знайшов своє практичне підтвердження: експериментально встановлено, що на величину обсягу захищеної інформації впливає величина відхилення саме власних векторів, а не абсолютної відокремленості відповідних ВЗ (в ході експерименту відбувалося поступове зниження вкладу абсолютної відокремленості власного значення, тобто вектору ваги під час побудови вектору розподілу додаткової інформації по власним векторам стеганоповідомлення).

Таким чином, для обчислення обсягу ЗІ доцільним є врахування збурень лише ВВ матриці ЦЗ-контейнера. Але кількісна оцінка такого збурення може робитися різними способами. В [6] показником збурення ВВ u_i виступає $\sin \theta_i$ (див.(3)), але така оцінка не є адекватною з урахуванням можливості на практиці значного збурення ВВ, аж до розгорнутого результуючого кута повороту. Взагалі на практиці можлива ситуація, коли два різні ВВ u_1 і u_2 після свого збурення можуть мати одне й те саме значення функції синуса для відповідних кутів повороту, при цьому один з цих векторів u_1 є нечутливим до збурних дій, а інший u_2 навпаки (рис.1).

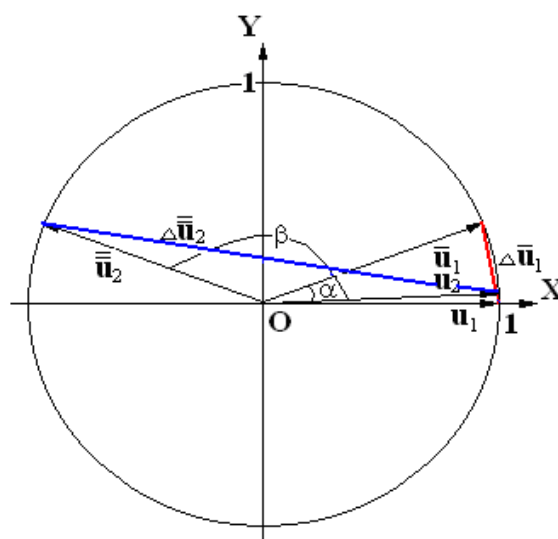


Рис. 1. Відмінність між збуреннями ВВ u_1 і u_2 при $\sin \alpha = \sin \beta$

Така ситуація є неприйнятною, оскільки для адекватної кількісної оцінки обсягу додаткової інформації, захищеної від збурної дії E , кількісна оцінка збурення ВВ повинна

відображати його чутливість/нечутливість до збурних дій. Для цього в роботі запропоновано використання в якості кількісної оцінки збурення ВВ евклідової норми вектору різниці між оригінальним і збуреним ВВ (рис.1): більшому збуренню вектора (більшому куту між поданим і збуреним векторами) відповідає більше значення норми вектора різниці і навпаки, що витікає з відомих властивостей довжин сторін довільного трикутника.

В [6] вводиться поняття захищеного ВВ від збурної дії E , що передбачає необхідність визначення ВЗ з достатньою абсолютною відокремленістю по відношенню до збурення E , а оцінка для цього збурення обирається у відповідності з наступним:

1. Для $j=1,2,\dots,k$, де k — кількість наявних контейнерів:

1.1. Побудувати $\bar{F}_j = E(F_j)$, де F_j — матриця j -го контейнера, $\bar{F}_j$ — матриця j -го контейнера після накладання деякого очікуваного збурення $E(F)$;

1.2. Знайти $E_j = F_j - \bar{F}_j$.

2. Знайти середнє значення показника збурення $\|E\| = \frac{1}{k} \sum_{j=1}^k \|E_j\|_2$.

Але кожне із зображень є унікальним за характеристиками матриці. Використання у якості кількісної оцінки збурної дії E , за якою обираються захищені власні вектори, усередненого значення норм $\|E_j\|_2$ з серії проведених попередньо експериментів приводе до «прив'язки» $\|E\|$ до характеристик тих зображень, на яких було виконано розрахунок. Це вводить додаткові умови щодо того, які саме зображення необхідно використовувати для обчислення розрахункового значення збурення, а також не враховує особливості безпосередньо тих контейнерів, що розглядаються, замінюючи критично важливу характеристику лише усередненим значенням. Обчислюючи середнє значення $\|E\|$ для певної кількості зображень, немає ніякої гарантії в тому, що $\|E\|$ однакового добре може бути застосовано для будь-яких інших зображень, а також для кожного конкретного зображення навіть з цієї ж множини.

З урахуванням цього в роботі пропонується метрика, яка нижче позначається $Capacity(j)$, що не розраховується попередньо для певної вибірки зображень, а враховує особливості безпосередньо такого контейнера F_j , об'єм захищеної інформації якого досліджується. Для її отримання після вбудовування додаткової інформації стеганоповідомленню необхідно надати очікуване збурення, та для результуючої матриці знайти ортонормовані лексикографічно додатні власні вектори (за допомогою нормального спектрального розкладання). Умовою виділення елементів відповідних векторів розподілу додаткової інформації по власним векторам стеганоповідомлення є умова того, чи норма вектору різниці між початковим власним вектором контейнера і власним вектором після накладання збурення на стеганоповідомлення менша, ніж деяке K , що є параметром розробленого методу і визначається експериментально (див.(4)). В результаті обчислювального експерименту встановлено, що найбільш стабільні та очікувані результати відповідно до кількості захищеної інформації та кількості відновленої інформації при декодуванні дає $K=0.005$ (рис.2).

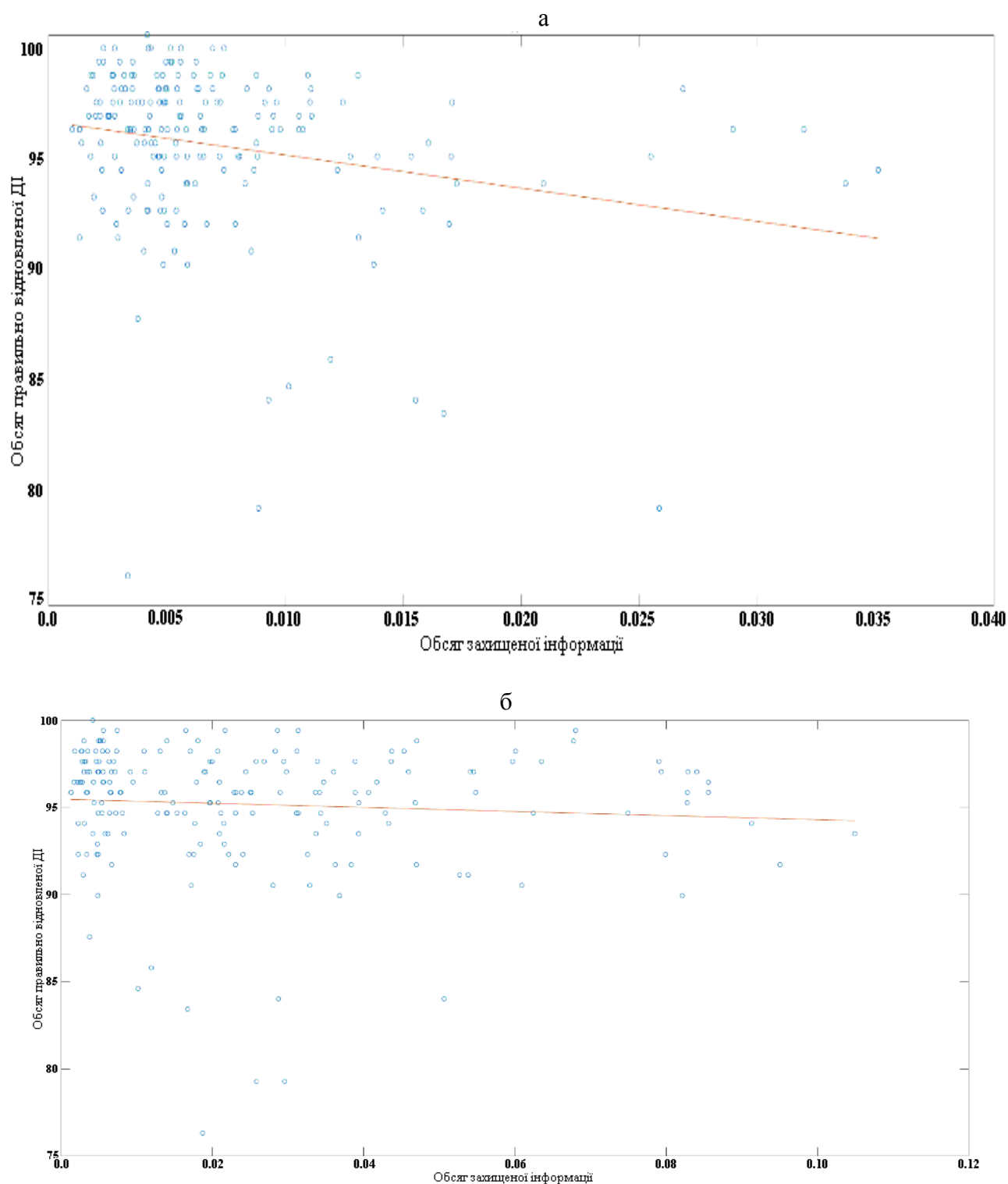


Рис. 2а. Співвідношення між обсягом захищеної інформації та відновленої при декодуванні додаткової інформації (%) при різних значеннях K : а – $K = 0.01$; б – $K = 0.001$

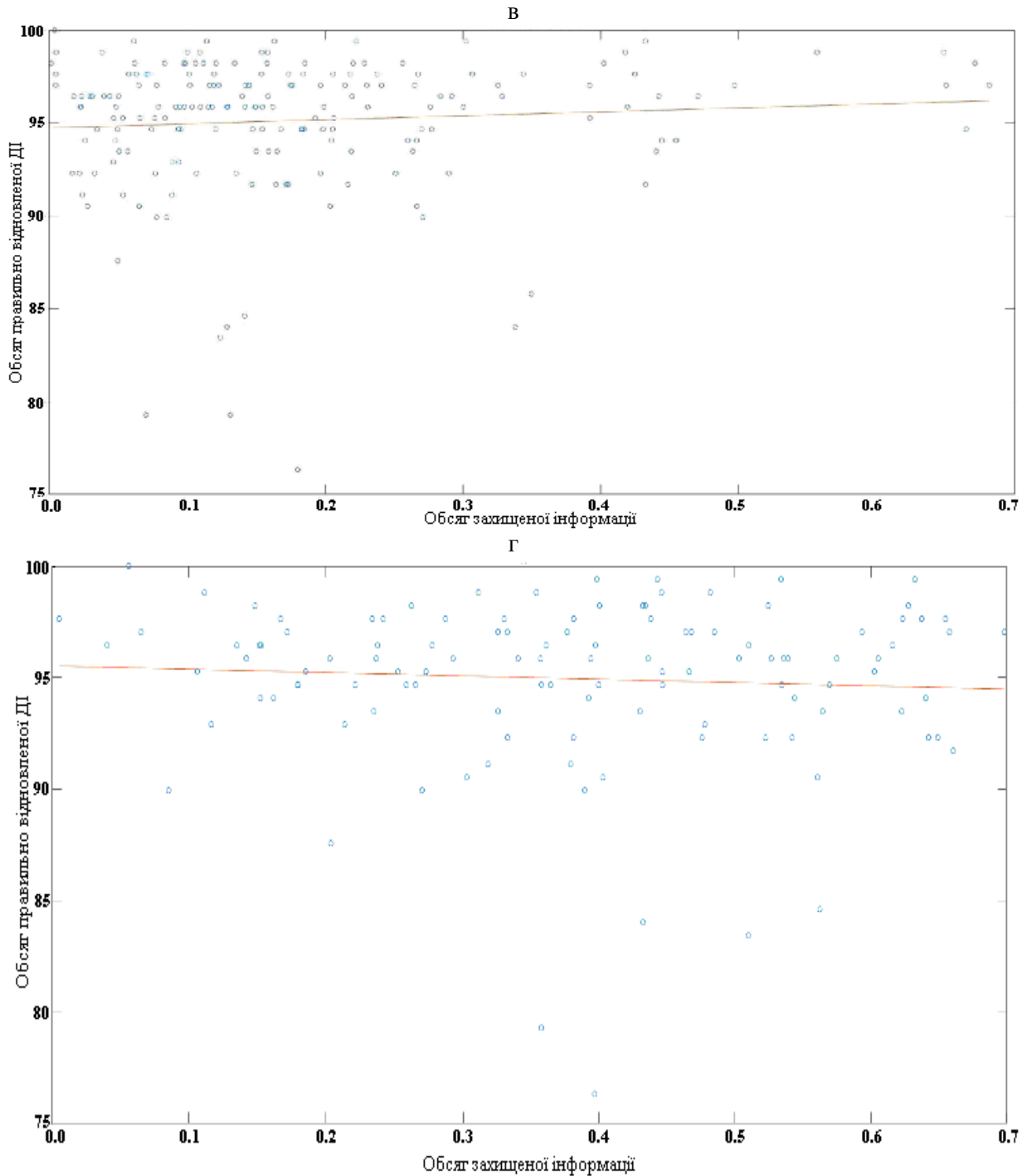


Рис. 26. Співвідношення між обсягом захищеної інформації та відновленої при декодуванні додаткової інформації (%) при різних значеннях K : в – $K = 0.002$; г – $K = 0.005$

При проведенні всіх обчислювальних експериментів для визначеності використовувався стеганометод Коха і Жао з параметром $P=30$ [9] (вбудова ДІ проводилася шляхом зміни значень (4,5) - і (5,4) - коефіцієнтів дискретного косинусного перетворення 8×8 -блоків матриці контейнера), що ніяк не обмежує спільності міркувань, враховуючи універсальність використовуваного загального підходу до аналізу стану й технології функціонування інформаційних систем. Цей вибір був зроблений з урахуванням: наявності стійкості методу Коха і Жао до атак проти вбудованого повідомлення, його загальної поширеності, відсутності обмежень на область застосування, наявності гнучких параметрів

вбудовування інформації для управління ступенем внесення змін до контейнеру в результаті стеганоперетворення.

Критеріями вибору збурних дій для моделювання в роботі процесу атак проти вбудованого повідомлення були: наявність можливості для атакуючої сторони забезпечення надійності сприйняття збуреного стеганоповідомлення, оскільки інакше неавторизоване втручання буде одразу виявленим, в чому порушник очевидно є незацікавленим; поширеність конкретних атак на практиці.

Однією із найбільш поширених атак проти вбудованого повідомлення є атака стиском. Враховуючи величезні обсяги інформації, що передається по каналах зв'язку, ця інформація зберігається, як правило, у форматах з втратами, тому атака стиском не привертає уваги, але вносить зміни у зображення при будь-якому коефіцієнті стиску. Як атака стиском в роботі використовується збереження ЦЗ в форматі Jpeg.

Серед атак проти вбудованого повідомлення поширеними залишаються атаки накладанням різноманітних шумів. Це пов'язано з тим, що сам результат вбудови ДІ в стеганографії часто трактується як накладання шуму, зокрема, при застосуванні LSB-методу. Ці атаки є такими, що важко виявляються, особливо, коли параметри шуму обрані так, що величина збурної дії є незначною, але очевидно призводять до змін в стеганоповідомленні. При моделюванні атак проти вбудованого повідомлення в роботі використовувалися: гаусівський шум з нульовим математичним очікуванням; мультиплікативний шум з різними значеннями дисперсії.

З урахуванням вищенаведеного основні кроки методу вибору контейнера, що забезпечує нечутливе стеганоповідомлення, наступні:

Крок 1. Нехай $F_1, F_2, \dots, F_k$ - матриці наявних потенційних ЦЗ-контейнерів.

Для $j = 1, 2, \dots, k$, де k — кількість контейнерів, робити:

- 1.1. Побудувати стеганоповідомлення з матрицею $F_j^{(s)}$, що відповідає контейнеру F_j ;
- 1.2. Піддати стеганоповідомлення $F_j^{(s)}$ очікуваній збурній дії $E(F)$. Результат – ЦЗ з матрицею $\overline{F}_j^{(s)}$;
- 1.3. Побудувати нормальні спектральні розкладання (1) для $F_j, F_j^{(s)}, \overline{F}_j^{(s)}$:

$$F_j = U_j \Lambda_j U_j^T; F_j^{(s)} = U_j^{(s)} \Lambda_j^{(s)} (U_j^{(s)})^T; \overline{F}_j^{(s)} = \overline{U}_j^{(s)} \overline{\Lambda}_j^{(s)} (\overline{U}_j^{(s)})^T;$$

- 1.4. Побудувати вектор $Deviation_j$:

$$1.4.1. \overline{Deviation}_j(i) = \|U_j(i) - U_j^{(s)}(i)\|,$$

де $U_j(i), U_j^{(s)}(i)$ - i -ий стовпець матриці $U_j, U_j^{(s)}$ відповідно; $i=1, 2, \dots, n$, де n — кількість власних векторів F_j ;

$$1.4.2. Deviation_j(i) = \frac{\overline{Deviation}_j(i)}{\|\overline{Deviation}_j\|}, i=1, 2, \dots, n.$$

- 1.5. Побудувати вектор $Distribution_j$ розподілу додаткової інформації по власних векторах стеганоповідомлення:

$$1.5.1. \overline{Distribution}_j(i) = Deviation_j(i);$$

$$1.5.2. \text{Distribution}_j(i) = \frac{\overline{\text{Distribution}_j(i)}}{\sum_{i=1}^n \overline{\text{Distribution}_j(i)}} \cdot 100\%, \quad i = 1, 2, \dots, n,$$

де n — кількість власних векторів F_j ;

1.6. Визначення об'єму захищеної від збурної дії $E(F)$ інформації в стеганоповідомленні:

$$\text{Capacity}(j) = \begin{cases} \sum_{i=1}^n \text{Distribution}_j(i), & \text{якщо } \|U_j(i) - \bar{U}_j^{(s)}(i)\| < K, \\ 0, & \text{інакше} \end{cases} \quad (4)$$

де K — параметр.

Крок 2. Визначення контейнера з найбільшим обсягом захищеної від збурної дії $E(F)$ інформації:

$$m = \arg \max_j \text{Capacity}(j).$$

F_m — шуканий контейнер.

Зауваження 1. Кожний пункт кроку 1 запропонованого методу використовує лише конкретний контейнер, який розглядається, без суміжних зв'язків з іншими контейнерами, а тому може виконуватися одночасно для кількох контейнерів, використовуючи технології розпаралелювання або навіть кластеризації.

Зауваження 2. Запропонований метод не може однозначно передбачити показник (відсоток) відновлення додаткової інформації після накладання на стеганоповідомлення збурень, що наочно підтверджує рис.2(г): беручи у якості зрізу невеликі значення обсягу захищеної інформації, наприклад, 0.07, легко переконатися у тому, що для різних зображень можливе як абсолютне (100%) відновлення ДІ, так і взагалі неефективне декодування — близько 75%. Аналізуючи ситуацію при збільшенні обсягу захищеної інформації, стає очевидним, що чим більшим є обсяг захищеної інформації, тим більш стабільним є результат ефективного відновлення додаткової інформації із стеганоповідомлення після атаки проти вбудованого повідомлення. При значному обсязі захищеної ДІ отримане стеганоповідомлення є нечутливим до збурних дій.

Висновки

В роботі розв'язано важливу науково-практичну задачу забезпечення можливості вибору цифрового зображення-контейнера, що породжує стеганоповідомлення, нечутливе до збурних дій.

Отримані наступні результати:

1. Теоретично обґрунтовано та практично підтверджено неінформативність та шкідливість урахування при розрахунку обсягу захищеної в стеганоповідомленні додаткової інформації абсолютних відокремленостей власних значень матриці цифрового зображення, як це робиться в [6], що привело до усунення власних значень з множини параметрів, збурення яких враховується при кількісній оцінці захищеності стеганоповідомлення;
2. Запропонована кількісна оцінка збурення власного вектору матриці цифрового зображення в результаті стеганоперетворення, яка, на відміну від [6], дає змогу для відокремлення чутливого власного вектора від нечутливого, адекватно відображає

збурення вектора незалежно від величини кута повороту, що дало можливість для удосконалення формули для розрахунку обсягу захищеної додаткової інформації;

3. Запропонована умова вибору захищених власних векторів, що враховує індивідуальні характеристики контейнера, замість попереднього обчислення над певною наперед визначеною, а отже небездоганною вибіркою зображень, що дозволяє враховувати особливості кожного ЦЗ-контейнера;
4. Розроблений метод вибору контейнера, що забезпечує малу чутливість стеганоповідомлення до збурних дій з наявної множини потенційних ЦЗ-контейнерів.

Список літератури

1. Goel M. Review on Steganography Techniques. *Journal of Emerging Technologies and Innovative Research*. 2019. V.6(2). P.148-153.
2. Subramanian N., Elharrouss O., Al-Maadeed S., Bouridane A. Image Steganography: A Review of the Recent Advances. *IEEE Access*. 2021. V.9. P.23409-23423.
3. Аграновский А.В. Стеганография, цифровые водяные знаки и стеганоанализ. М.: Вузовская книга, 2009. 220 с.
4. Amarendra K., Mandhala V.N., Gupta B.C., Sudheshna G.G., Anusha V.V. Image Steganography Using LSB. *International Journal of Scientific & Technology Research*. 2019. V.8 (12). P. 906-909.
5. Кушниренко Н.И., Кирмичиева А.С., Яковенко А.А., Калашников Н.В., Лозан А.Э. Метод встраивания информации в цифровые изображения jpeg, минимизирующий психовизуальные искажения для малых объемов встроенной информации. *Інформатика та математичні методи в моделюванні*. 2018. Т.8, № 4. С. 313-323.
6. Кобозева А.А., Нариманова Е.В. Оценка чувствительности стегосообщений к возмущающим воздействиям. *Системні дослідження та інформаційні технології*. 2008. No 3. С. 52-65.
7. Кобозева А.А., Хорошко В.А. Анализ информационной безопасности: монография. К.: ГУИКТ, 2009. 251 с.
8. Деммель Д. Вычислительная линейная алгебра: теория и приложения. М.: Мир, 2001. 430 с.
9. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография: теория и практика. Киев: МК-Пресс, 2006. 288 с.

**A COVER IMAGE SELECTION METHOD PROVIDING STEGO-OBJECT
ROBUSTNESS TO VARIOUS IMAGE PROCESSING ATTACKS**

A.Yu. Nadvotskiy, A.A. Kobozeva

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

With the development of information technology, the requirements for steganography systems are growing. Today, the steganography system must resist steganalysis attacks using the latest mathematical bases, attacks and countermeasures, which can be easily and efficiently implemented in any modern software environment, providing significant bandwidth when organizing a secret communication channel, and so on. All possible means must be used to meet these requirements. One of the ways to meet a certain requirement is to choose the cover as which the digital image is considered in the study. The cover deciding is to be done in order to provide the best characteristics of stego-object in a sense. The aim of the study is to provide the possibility to choose a cover image, which results in the stego-object that is robust to various image processing attacks. The following results are obtained in the study: the expediency of using perturbations of eigenvectors of the cover image matrix as indicators of security of secret message embedded into the cover is theoretically substantiated and practically confirmed; the quantitative estimation of the perturbation of the eigenvector matrix of the digital image as a result of embedding is proposed, which allows separating the sensitive eigenvector from the insensitive one, adequately reflects the perturbation of the eigenvector regardless of the angle of rotation; the proposed condition for the selection of eigenvectors protected from influence, taking into account the individual characteristics of the cover image; the formula for calculating the amount of protected additional information is proposed; a cover image selection method from the available set of potential containers is developed, which provides stego-object robustness to various image processing attacks.

Keywords: steganography system, stego-object, container selection, digital image, attacks against the embedded secret message, stego-object robustness, eigenvalue, eigenvector.

РОЗРОБКА ЗАХИЩЕНОЇ АВТОМАТИЗОВАНОЇ ВЕБ-СИСТЕМИ ТЕСТУВАННЯ ЗНАНЬ

С.О. Перерва, К.О. Трифонова

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

Сучасна освіта націлена на надання можливості отримання якісних знань та умінь. Багато чисельні дослідження останніх років демонструють значний вклад інформаційних технологій в підвищення якості отримуваних знань та умінь в будь-яких сферах освіти. Для оцінки якості отримуваних знань на протязі учбового процесу необхідно виконувати проведення контролю у різних формах. Значні педагогічні дослідження доводять ефективність проведення тестового контролю для отримання оцінки якості знань та умінь. Інформаційні технології можуть допомогти підвищити незалежність перевірки та встановлення оцінки від особи викладача, тобто підвищити об'єктивність, завдяки застосуванню форми проведення тестування у автоматизованому форматі. У відповідності до сучасних реалій, розробка, реалізація та подальше використання автоматизованого програмного забезпечення для тестування знань, відбувається у мережі Інтернет. У зв'язку з цим, фактором, який повинен бути визначений найважливішим, є інформаційна безпека. Отже, метою даної роботи є розробка та реалізація автоматизованої веб-системи тестування знань з підвищеним рівнем інформаційної безпеки. Один з найпопулярніших відкритих проектів з дослідження безпеки веб-додатків Open Web Application Security Project, щорічно публікує топ десять найпоширеніших загроз. В роботі представлено розробку механізму захисту програмного забезпечення, рівень інформаційної безпеки якої, забезпечує захист інформації від найбільш критичних ризиків, встановлених у відповідності до OWASP Top-10 2021. Розроблений програмний продукт може бути рекомендований для застосування в вищих та загальноосвітніх навчальних закладах, для підвищення якості знань та об'єктивності, завдяки застосуванню форми проведення тестування у автоматизованому форматі, з підвищеним рівнем інформаційної безпеки.

Ключові слова: захист інформації, веб-застосування, дистанційне навчання, якість освіти, тестування знань

Вступ

Сучасна освіта націлена на надання можливості отримання якісних знань та умінь [1-7].

Використання інформаційних технологій при оцінюванні почалося в 1920-х роках, коли Сідні Л. Пресс розробив машини для автоматичного тестування. Більше того, водночас у школах почали використовувати стандартизоване оцінювання та технологію автоматичного підрахунку балів, що допомогло зробити масштабне тестування зручним та економічно ефективним. Величезні зміни в багатьох секторах, особливо в освіті, відбулися, коли в 1990-х роках було введено всесвітню мережу. З того часу багато компаній запровадили власну систему електронного оцінювання. В Англії, Уельсі та Північній Ірландії принципи та вказівки щодо електронного оцінювання були запроваджені JISC (Об'єднаний комітет інформаційної системи) для роз'яснення різних кваліфікаційних регуляторів у Сполученому Королівстві. У 2009 році IMS Global Learning Consortium розробив специфікацію інтероперабельності IMS Question and Test. У 2009 році Cisco, Intel та Microsoft випустили Transforming Education: Assessing and Teaching 21st Century Skills [3].

На даний час, електронне оцінювання надає нові привабливі можливості та методики оцінювання різних аспектів і рівнів набутих знань, умінь і компетенцій. Це допомагає подолати деякі недоліки, які притаманні традиційним підходам до оцінювання [4].

Електронне оцінювання має ряд переваг [4]:

- використання різних методик оцінювання, які відповідають заздалегідь поставленим цілям навчання та використовуються педагогічні підходи;
- оцінка великої кількості тестів виконується швидко і легко завдяки високому ступеню процесу автоматизації;
- негайний персоналізований зворотній зв'язок, для подальшого корегування навчання;
- об'єктивність за рахунок автоматизації оціночної діяльності або оцінювання на основі заздалегідь встановлених критеріїв і шаблонів;
- впровадження в будь-який час і в будь-якому місці, що гарантує більшу гнучкість;
- можливість повторного використання діяльності або їх компонентів у різних комбінаціях і контекстах;
- широкий вибір типів запитань в електронних тестах;
- можливість оцінити групу у цілому, враховуючи індивідуальний внесок.

Розрізняють наступні види електронного оцінювання [4]:

- за поставленими навчальними цілями та періодом, в який воно проводиться, оцінювання може бути: діагностичним (допомагає поставити чіткі, точні та адекватні навчальні цілі, що відповідають рівню готовності до роботи з новим змістом); формуюча (допомагає контролювати успішність та вносити зміни в навчальний процес, щоб адаптуватися до потреб та покращити навчання); підсумковий (підтримує оцінку знань і навичок наприкінці навчання за встановленими критеріями або стандартами, щоб визначити, чи були досягнуті поставлені цілі навчання [5]);
- відбувається оцінювання одночасно чи ні: синхронно (одночасно оцінюються); асинхронно (оцінювання в зручний час);
- за кількістю оцінюваних та суб'єктів-оцінювачів: групові (оцінюються вироби, які є результатом спільної роботи групи та їх уміння працювати в команді); індивідуальний (оцінюються індивідуальні знання та вміння); рівноправний (допомагає розвивати критичне мислення, мотивувати та відстоювати власну думку на основі фактів і доказів) [6].

Отже, багато чисельні дослідження останніх років демонструють значний вклад інформаційних та комунікаційних технологій в підвищення якості отримуваних знань та умінь в будь-яких сферах освіти, та доводять необхідно виконувати проведення тестового контролю для отримання оцінки якості знань та умінь на протязі учбового процесу. У відповідності до сучасних реалій, розробка, реалізація та подальше використання автоматизованого програмного забезпечення для тестування знань, відбувається у мережі Інтернет. У зв'язку з цим, фактором, який повинен бути визначений найважливішим, є інформаційна безпека. Компанії з розробки програмного забезпечення найчастіше не дотримуються вимог інформаційної безпеки, концентруючись на інших цілях. Компанія Positive Technologies постійно виконує дослідження з інформаційної безпеки веб-додатків, які свідчать, що значна частина програмного веб-забезпечення містить вразливості різного ступеня ризиків. OWASP – відкритий проект з дослідження безпеки веб-додатків, щорічно публікує топ десять найпоширеніших загроз. Все це стимулює проведення подальших досліджень в поданій галузі та робить тему даної роботи надзвичайно актуальною.

Мета і задачі дослідження

Метою роботи є підвищення рівня інформаційної безпеки розробленої та

реалізованої автоматизованої веб-системи тестування знань.

Для досягнення поставленої мети необхідно розв'язати наступні *задачі*:

- а) виконати аналіз педагогічного напрямку дослідження форми проведення та оцінки якості знань у форматі автоматизованого тестування;
- б) виконати аналіз найбільш критичних ризиків та існуючих механізмів захисту веб-додатків;
- в) розробити механізм захисту програмного забезпечення, рівень інформаційної безпеки якої, забезпечує захист інформації від найбільш критичних ризиків, встановлених у відповідності до OWASP Топ-10 2021;
- г) реалізувати програмний продукт, автоматизовану веб-систему тестування знань, з підвищеним рівнем інформаційної безпеки, у відповідності до запропонованого механізму захисту програмного забезпечення.

Основна частина

На сьогодні інформаційні технології стають все більш поширеними в суспільстві. Вони використовуються в найрізноманітніших галузях: у соціальних мережах, електронній пошті, новинних та урядових порталах, електронній комерції, форумах, блогах та інших веб-сайтах. Разом з розвитком ІТ все більшого значення набуває інформаційна безпека (ІБ). Якщо розглядати історичну перспективу розвитку інформаційних технологій, то виявляється, що з 1996 року, коли була прийнята Конституція нашої держави, і до моменту написання цієї роботи кількість людей, які відчувають себе захищеними в інформаційному полі, постійно падає. Справа не лише в лавиноподібному зростанні використання ІТ, а, швидше за все, у порушеннях, які держава робить в інформаційній сфері. Зростання вимог до забезпечення інформаційних технологій визначається, насамперед, розвитком ІТ. Потенційні порушники мають нові можливості для деструктивних дій у всіх сферах нашого життя. Найефективніші з цих дій відбуваються у кіберпросторі. Виходячи з вищесказаного, можна зробити висновок про необхідність захисту веб-додатків.

Залежно від того, де використовується веб-додаток, в ньому може оброблятися інформація різних рівнів доступу та значень. Наприклад, програми можуть використовувати інформацію про банківські картки, персональні дані користувачів, паролі та інші ідентифікаційні дані. Жоден користувач не застрахований від того, що його дані можуть бути скопійовані або піддані ряду випадкових і зловмисних впливів у процесі їх обробки, передачі та зберігання [8].

Веб-додатки реалізують архітектуру «клієнт-сервер». У цій концепції клієнт – це браузер користувача, а сервер – веб-сервер. В основі концепції «клієнт-сервер» відбувається обмін інформацією через мережу, клієнт починає взаємодіяти, а дані зберігаються переважно на сервері.

В основному веб-додатки мають розподілену структуру. Основні переваги цієї конструкції:

- хороша масштабованість – можливість збільшення функціональності без зміни структури;
- наявність можливості керувати навантаженням програми – направлення потоків запитів користувача на менш навантажені сервери.

Типова архітектура цих програм може бути представлена у трьох рівнях: клієнтська частина (веб-браузер), веб-сервер та база даних.

Кожен день будь-який веб-сайт може піддаватися кібератакам. Як правило, більшість атак є цільовими. Це означає, що зловмисник не обмежується однією спробою отримати необхідні дані несанкціонованим способом, оскільки він не знає, які саме уразливості є в коді. Усі спроби зламати сайт зводяться до серії подій, які відбуваються протягом певного періоду часу. За статистикою за 2018 рік, найбільша

кількість атак на одне веб-додаток припадає на сайти фінансових організацій, транспортних компаній та обслуговуючих компаній. Вибір методу атаки залежить від особливостей веб-додатка. Припустимо, якщо в додатку не передбачена можливість введення даних користувача, то зловмисник не буде проводити атаки, спрямовані на зміну логіки програми за допомогою введення будь-яких даних користувачем. Найпопулярніші атаки включають: введення коду SQL, вихід за межі каталогу та між-сайтові сценарії.

Щоб виявити вразливості в коді та зрозуміти, як система реагуватиме на атаку – програму потрібно протестувати. Процес тестування максимально схожий на процес злому, який проводить зловмисник. Мета таких дій – визначити, наскільки вразливим є веб-додаток.

Для критичної інфраструктури спеціалізовані фішери використовують передові методи, які поєднують соціальну інженерію, орієнтуючись як на відсутність спеціалізованих активних заходів безпеки системи, так і на недостатню обізнаність або пильність співробітників [9].

Найбільш популярний методології тестування [8]:

- посібник з методології тестування безпеки з відкритим кодом; - Спеціальна публікація Національного інституту стандартів і технологій (NIST) 800-115;
- керівництво з тестування OWASP;
- стандарт виконання тестування на проникнення;
- структура оцінки безпеки інформаційних систем.

Для перевірки безпеки веб-додатків доцільніше використовувати методологію OWASP. Ця методологія заснована на методі чорного ящика – інформація про тестований додаток обмежена або відсутня взагалі. Безпека програмного забезпечення охоплює дуже широку область тем. Щоб мати безпечне програмне забезпечення, потрібно враховувати багато речей.

Найважливіші вразливості OWASP

Розуміння поширених вразливостей у веб-додатках допомагає краще підготуватися до захисту даних від таких атак. Завдяки знанням, отриманим від досліджень, користувачі та розробники можуть бути краще підготовлені для боротьби з найпоширенішими атаками та формувати рішення для запобігання майбутнім атакам на їхні веб-додатки. Вразливості існують у багатьох формах у сучасних веб-додатках, які можна легко пом'якшити, вкладаючи час та дослідження [10].

Нижче перелічено найважливіші вразливості 2021 року.

Атаки SQL Injection відбуваються, коли введені дані користувача не очищені належним чином і мають найбільший вплив на Інтернет. Коли зловмисники знаходять ін'єкцію SQL, у більшості випадків вони можуть отримати дані з бази даних, а в деяких випадках призводять до віддаленого виконання коду в цільовій системі. Атаки ін'єкцій SQL бувають у багатьох формах, таких як атаки на основі помилок, атаки на основі об'єднань, сліпі атаки та атаки поза діапазоном [10].

Порушена аутентифікація – це термін, який використовується для позначення кількох уразливостей, які дозволяють зловмисникам використовувати та видавати себе за користувачів веб-додатків. Існують різні методи, за допомогою яких зловмисники можуть отримати облікові дані користувача або зловити сеанси користувача, щоб мати можливість видавати себе за цих користувачів, наприклад, слабкі облікові дані користувача, які можна вгадати, неправильно збережені облікові дані, такі як паролі, які не були хешовані, які можуть бути вилучені з інших типів атак, таких як ін'єкції SQL, ідентифікатори сеансів, які відкриваються в URL-адресах, атаки фіксації сеансів, фіксовані ідентифікатори сеансів і особливо паролі, ідентифікатори сеансів та інші облікові дані, які надсилаються через незашифровані з'єднання, такі як HTTP [10].

Конфіденційні дані – це веб-програми, які не захищають таку інформацію, як паролі, фінансову інформацію або дані про стан здоров'я, що може призвести до того, що кіберзлочинці зловживають цією інформацією для отримання несанкціонованого доступу до облікових записів користувачів, вчиняють шахрайські дії, такі як онлайн-покупки за допомогою вкраденого платежу. інформації або здійснювати шантаж отриманими конфіденційними даними. Розкриття конфіденційних даних може призвести до фінансових втрат, завдати шкоди репутації корпорацій, які розкрили свою інформацію чи активи, і спонукає підприємства оплачувати витрати на розслідування порушень даних. Захист від таких атак залежить від законодавчої бази країни та галузі, оскільки їх ігнорування може призвести до фінансово руйнівних результатів.

Атаки введення зовнішніх об'єктів XML, також відомі як ін'єкції XXE, відбуваються, коли зловмисники зловживають аналізаторами розширеної мови розмітки (XML) на веб-серверах, надсилаючи на веб-сервери спеціально створені шкідливі XML-документи, які обробляються і можуть призвести до відмови в обслуговуванні, віддаленого виконання коду або підробка запитів на стороні сервера.

Порушений контроль доступу складається з кількох можливих векторів атак, таких як обхід перевірок контролю доступу, редагування облікових записів інших користувачів, підвищення привілеїв, неправильні налаштування CORS, які дозволяють несанкціонований доступ до обмежених API, маніпулювання метаданими за допомогою маркерів контролю доступу, таких як веб-токени JSON (JWT) або доступ неавторизовані веб-сторінки як непривілейований користувач, що може призвести до контролю зловмисників бізнес-функцій або можливості отримання зловмисниками всіх даних. Рекомендується використовувати списки контролю доступу та забороняти доступ до функцій, використовуючи код на стороні сервера, де зловмисники не можуть отримати доступ до метаданих або контролювати їх.

Неправильна конфігурація безпеки відноситься до веб-програм, які були неправильно налаштовані таким чином, що залишають їх підданими загрозам безпеки. Вони можуть включати неправильні конфігурації брандмауера, відкриті порти адміністрування, які піддають програму віддаленим атакам, або застарілі програми, які намагаються спілкуватися з програмами, які більше не існують. Забезпечення того, що конфігурації проходять належний процес забезпечення якості та ретельно перевіряються, тестуються та перевіряються, зменшує поверхню атаки від такого типу вразливості.

Міжсайтові сценарії, також відомі як XSS, мають багато форм, які призводять до різних результатів залежно від типу виконаного XSS, але зазвичай відбувається, коли зловмисники вводять у веб-додаток шкідливі сценарії, які потім розкривають конфіденційну інформацію, внутрішні служби або розкривають файли cookie привілейованих користувачів.

Небезпечні атаки десеріалізації відбуваються, коли програми намагаються перетворити шкідливі дані, які контролює зловмисник, у внутрішні структури даних, які контролюються програмою. Впроваджуючи спеціально створені корисні навантаження, зловмисники можуть взяти під контроль змінні, функції та внутрішні стани програми. Це часто призводить до вразливостей віддаленого виконання коду, а також до впливу операційної системи веб-додатка.

Використання компонентів з відомими вразливими місцями означає використання певного програмного або апаратного забезпечення з відомими вразливими місцями, незалежно від того, чи вони були припинені або закінчилися терміном служби. Зловмисники, швидше за все, використовують поширені або відомі експлойти для отримання доступу до систем, а не виявляють нові вразливості. Захист від цієї вразливості вимагає відстеження залежностей програми, належної документації, видалення невикористаних залежностей, видалення мертвого коду та

включення залежностей у політику оновлення програми, процедури та життєвий цикл обслуговування.

Недостатнє ведення журналів і моніторинг означає відсутність належних механізмів ведення журналів, які допомагають у моніторингу та виявленні інцидентів безпеки. Це дозволяє зловмисникам вести свою діяльність непомітно, що значно ускладнює завдання виявлення інцидентів та реагування на атаки. Журнали використовуються не лише для відстеження діяльності зловмисників або виявлення помилок та інших аномальних дій, які можуть мати місце в програмі. Крім того, багато нормативних вимог залежать від належних механізмів ведення моніторингу.

Методи самозахисту веб-додатку під час виконання

Додатки соціальних мереж стали важливим джерелом Інтернет-послуг і трафіку. Як правило, він заснований на динамічних сторінкових програмах, таких як обмін інформацією, інтерактивний зворотний зв'язок і запити на послуги, що надаються веб-програмами. Більшість хмарних платформ та інтерфейсів керування мережевими пристроями також використовують веб-інтерфейси. Упорядковуючи додаткові оператори сценаріїв у введених користувачами, за відсутності надійних методів фільтрації, міжсайтові сценарії можуть викликати ефект вставки зайвого коду на сторінки веб-програм і порушення логіки вихідної сторінки, спричиняючи зловмисних дій клієнта.

Зазвичай уразливості міжсайтових сценаріїв можна уникнути за допомогою безпечних методів програмування, таких як фільтрація даних користувача. Оскільки веб-додатки побудовані на мові сценаріїв високого рівня, розробники більше стурбовані дизайном інтерфейсу з Web 2.0, а технології інтерфейсу стають більш складними. В результаті ускладнюються перетікання змінних. Якщо це відсутність загального дизайну та розробки безпеки, а також немає ефективного фільтрації та обмежень, оскільки вразливості, засновані на архітектурі такого типу додатків, неминуче існуватимуть міжсайтові вразливості, які стануть актуальною проблемою безпеки мережі в умовах широкого застосування. Уразливості міжсайтових сценаріїв широко існують у веб-додатках у звіті про загрози безпеки OWASP десяти найбільших (OWASP top 10), ін'єкція команд і міжсайтове скриптування залишаються важливими загрозами [8]. Його можна виявити як на стороні сервера, так і на стороні клієнта. Метод виявлення на стороні сервера в основному полягає в тому, щоб переглянути введений користувачем вміст, відфільтрувати ненадійний вміст і зробити так, щоб шкідливий код сценарію не міг досягти браузера користувача. З точки зору виявлення на стороні сервера, репрезентативними методами є вбудовані політики з підтримкою браузера (BEEP). Щоб запобігти введенню зловмисного коду сценарію у веб-програми, BEEP реалізує білий список довірених сценаріїв. Таким чином, створюється лише код надійного сценарію веб-розробником може виконуватися на клієнті, а решта відфільтровується. Однак BEEP має серйозні недоліки при роботі з динамічно генерованими сценаріями. Особливо коли поточна структура веб-моделі дозволяє процедурний дизайн, проблема стає більш очевидною, і були складніші атаки XSS, спеціально спрямовані на BEEP.

Метод визначення політики безпеки вмісту (Content Security Policy - CSP) довіряє виконанню браузера. Вважається, що причиною проблеми XSS є недоліки у веб-додатку. З цієї причини CSP додає багато атрибутів до основної частини кожної сторінки, створеної на стороні сервера. Під час створення сторінки надійність сценаріїв, зображень або іншого вмісту на сторінці визначається цими атрибутами. Таким чином, він забезпечує функцію автоматичного захисту від несправності. Оскільки ця політика поширюється на всю сторінку, ненадійний вміст обмежується цією політикою. Однак, оскільки CSP накладає суворі обмеження на створені сторінки, це спричинить серйозні проблеми з продуктивністю перед великомасштабними веб-

додатками, а також не може добре адаптуватися до веб-архітектури дизайну процедурної моделі [11].

WAF (брандмауер веб-додатків) проникає у веб-протокол для фільтрації та використовує технологію брандмауера для обмеження з'єднань. WAF зазвичай розгортається на передньому кінці кластера веб-серверів для захисту веб-сайтів і використовує режим зворотного проксі для виконання двонаправленої фільтрації пакетів запитів HTTP. Якщо брандмауер розуміє протокол і семантику параметрів програми, це призведе до більш точного виявлення вразливостей. Однак із збільшенням складності додатків і швидкою появою нових типів програм і технологій (таких як JSON, REST тощо), здатність WAF забезпечувати точне виявлення вразливостей без штучної настройки ще не реалізована. Сьогодні мало хто вважає, що WAF розгорнуто в режимі безумовного блокування для будь-якої програми, що доводить притаманну неточність технології WAF. Деякі вдосконалені методи використовують машинне навчання для вивчення правил підпису, а також стикаються з труднощами отримання набору даних і робочого навантаження на тегування вручну [11]. Комбінація методів виявлення на стороні сервера і клієнта в основному полягає в тому, що клієнтський браузер повинен проаналізувати повернутий HTML-документ способом, визначеним сервером, щоб шкідливий код не міг бути виконаний, навіть якщо він досягне клієнта. Створення наскрізного довіреного шляху між користувачем веб-програми та веб-сервером. Типовими прикладами є цілісність структури документів (DSI) [11].

Технологія RASP (Runtime application self-protection) є вдосконаленням WAF. Вона вводить код захисту в прикладну програму, інтегрується з прикладною програмою, а також відстежує та блокує атаки в режимі реального часу, так що програма має власні можливості захисту. Захищеному додатку не потрібно вносити жодних змін у кодування, лише за допомогою простої конфігурації. Цей метод підходить для рішень динамічного захисту від виправлень для певних вразливостей. Вона поки не може самостійно та комплексно вирішити певний тип загрози безпеки [11].

Техніка виявлення атак з використанням мови структурованих запитів

Більшість методів виявлення атак – це методи, які використовуються веб-розробниками для виявлення атак, як правило, під час виконання коду JavaScript на стороні клієнта. Сьогодні існує багато методів, і більшість з них відрізняються один від одного у виявленні та запобіганні SQLIA за допомогою спеціальних інструментів і механізмів кодування для виявлення або запобігання зловмисних атак SQL на цільову базу даних на сервері. Перш ніж представити техніку виявлення, важливо показати дуже поширені типи вразливостей безпеки [12].

Тип I - перевірка введених даних – це спроба перевірити або відстежити будь-які підозрілі вхідні дані на предмет можливої зловмисної поведінки. Неправильна перевірка поля даних може призвести до багаторазового виконання шкідливого коду без належної та точної перевірки початкового наміру. Таким чином, зловмисник, використовуючи SQL, може захотіти скористатися неправильною перевіркою, щоб він міг виконати шкідливий код, а потім здійснити атаку на цільову базу даних.

Тип II - відсутність поділу між типами даних, які приймаються як вхідні.

Тип III - будь-яка затримка процесів до етапу виконання, оскільки наявні змінні вимірюються, незважаючи на те, що вихідний код використовує вираз для здійснення атаки.

Деякі статті в літературі навіть посилаються на збережені процедури як на засіб проти SQLIA. Оскільки збережені процедури знаходяться на передньому плані бази даних, запропоновані ними методи не можна застосовувати для захисту самих збережених процедур. Наприклад, деякі дослідження запропонували нову техніку захисту від атак, спрямованих на збережені процедури. Ця техніка поєднує статичний

аналіз коду програми з перевіркою під час виконання, щоб виключити такі атаки. Інші дослідники розробили метод, який виявляє та запобігає атакам SQL-ін'єкції, перевіряючи, чи введені користувачем зміни в результатах запиту. Вони запропонували метод виявлення атак ін'єкції SQL за допомогою токенизації запитів, який реалізується методом Query Parser, який використовує метод Black Box Testing, для тестування веб-додатків на наявність вразливостей ін'єкції SQL. Ця техніка використовує веб-сканер для визначення всіх точок у веб-додатку, які можна використовувати для введення SQLIA. Інші дослідники використовували техніку під назвою динамічний аналіз, де це дуже корисно для проведення аналізу часу виконання або динамічного SQL-запиту, він генерується за допомогою даних, що вводяться користувачем, спочатку шляхом реалізації веб-додатка. Техніка виявлення також у постгенерованій категорії може виконувати запит перед відправкою запиту до цільової бази даних на стороні сервера. Існує ще одна запропонована методика під назвою SQL-IDS, це підхід на основі специфікації для виявлення шкідливих вторгнень. Деякі дослідники SQLIA пропонують використовувати нову методологію, засновану на специфікації, а також на характеристиках експлуатації та виявлення шкідливих ін'єкцій SQL, щоб уникнути вразливостей. Виявлено, що виявлення, засноване на певному запиті, дозволяє системі виконувати аналіз, зосереджений на незначних обчисленнях без будь-якої необхідності створення хибно-негативних або хибно-позитивних результатів. У центрі уваги дослідження методів виявлення I типу, запропонована методика виявлення, яка називається Combined Detect, заснована на JavaScript, і два рішення, де перевірка в залежності від введених даних як спроба довести або відфільтрувати будь-який підозрілий вхід містить специфікацію зловмисної поведінки. Більшість методів показали, що прийнята методика виявлення недостатньої перевірки введення дозволить виконувати шкідливий код без належної перевірки його наміру. Тому будь-яка методика виявлення повинна перешкоджати зловмисникові скористатися перевагами недостатньої перевірки введення, які загрожують цільовій базі даних і допомагають зловмиснику використовувати шкідливий код SQL для легкого проведення атак.

В даному розділі виконано огляд теоретичних основ захисту веб-додатків.

Безпеці веб-додатків необхідно приділяти дуже багато уваги. Безпека веб-додатків залежить від якості програмного коду, від кваліфікації системного адміністратора та від компетенцій усіх користувачів, які мають доступ до чутливої інформації.

Вразливості OWASP є дуже шкідливими і в цьому списку зосереджені найнебезпечніші вразливості, які можуть коштувати купу грошей, або підірив ділової репутації, чи довести аж до втрати бізнесу.

Методи самозахисту веб-додатку під час виконання мають деякі складнощі з виявленням вразливостей без штучного налаштування, але з використанням машинного навчання можуть бути корисними у нагоді.

Техніки виявлення атак з використанням мови структурованих запитів є необхідними, однак фільтрація даних здається дуже ефективною та найпростішою технікою. Незважаючи на те, що виявлено, що методи виявлення SQLIA, які використовують перевірку введення, схильні до великої кількості хибно-позитивних результатів, і все ж немає 100% гарантії, що немає помилкових негативів.

Практична реалізація захищеної автоматизованої веб-системи тестування знань

Для розробки захищеної автоматизованої веб-системи тестування знань було використано мови програмування JavaScript та PHP, фреймворки Nuxt та Laravel. Для розробки використовувалось інтегроване середовище PhpStorm.

Архітектура програмного продукту

Структура програмного продукту є модульною. Функціональна структура додатку включає в себе наступні модулі:

- модуль автентифікації та реєстрації;
- модуль відновлення паролю;
- модуль публікацій;
- модуль тестувань знань;
- модуль груп;
- модуль користувачів;
- модуль управління особистою інформацією.

Модуль автентифікації та реєстрації дозволяє ідентифікувати користувачів по їх електронній адресі. Без цього модулю користувач не може бути ідентифікований, а це значить, що він не може використовувати функціонал додатку. Цей модуль, використовуючи API віддаленого серверу, відправляє запит на перевірку або створення нового облікового запису.

В успішному випадку сервер віддає токен, тобто деякий унікальний ключ. Унікальний ключ складається з 512 бітів інформації, тобто 64 символи по одному байту, що на практиці унеможливорює підбір цього ключа зломисником. За допомогою унікального ключа користувач може здійснювати керування обліковим записом та отримувати інформацію з сервера, де необхідна автентифікація за токеном.

Модуль відновлення паролю дозволяє відновлювати пароль, якщо виникає така ситуація, коли користувач не пам'ятає пароль від облікового запису. На вказану електронну адресу посилається лист з токеном для відновлення паролю. Використовуючи цей токен, користувач може змінити пароль, але на протязі деякого часу, так як токен обмежений за часом.

Модуль публікацій дозволяє створювати публікації, переглядати та видаляти їх. Модуль є повністю незалежним від інших, тому з легкістю може переноситись на інші веб-додатки.

Модуль тестувань знань дозволяє створювати тестування з різними питаннями та відповідями, які можуть підтримувати математичні формули. Модуль підтримує перемішування питань та відповідей в питаннях. Є можливість завдання обмеження за часом, щоб проходження тестування було доступно лише в деяких проміжках часу. Також він дозволяє проходити тестування, переглядати вже пройдені тестування та бачити результати тестувань.

Модуль груп дозволяє створювати та видаляти групи, можливість додавати користувачів до груп. При використанні модуля груп надається можливість чітко визначати область видимості для тестувань знань, тобто надавати доступ до тестування лише для вказаних груп.

Модуль користувачів надає можливість перегляди усіх користувачів в системі, обмежувати або надавати доступ до системи користувачу, переглядати дії користувача. Є можливість змінювати профіль користувача, а саме змінювати ім'я, групу, роль, пароль. Використовуючи фільтр, надається можливість знаходити лише певних користувачів, які задовольняють умовам фільтру.

Модуль управління власною інформацією надає можливість лише змінювати пароль та ім'я в системі для усіх ролей в системі.

Технологія реалізації програмного продукту

Під час реалізації веб-додатку було виявлено чимало проблем як з клієнтської частиною, так із серверною.

Першою проблемою, що було виявлено в ході розробки, стало те, що додаток використовує фреймворк Nuxt, який в свою чергу використовує NodeJS збоку серверу. Майже всі додатки, що спершу роблять відображення контенту зі сторони серверу,

можуть мати проблеми з витіком пам'яті. Тобто це процес, при якому відбувається постійне зменшення доступної програмі оперативної пам'яті, причому програма не має інформації про більшу частину зайнятої пам'яті. При витіку пам'яті додаток рано чи пізно переходить до аварійного завершення, що означає, що користувачі можуть бачити помилку 502 з боку серверу та не можуть користуватися веб-додатком. Проблема була вирішена використанням PM2, що є менеджером виробничих процесів для додатків Node.js з вбудованим балансувальником навантаження. Це дозволяє підтримувати додатки назавжди, перезавантажувати їх без простоїв і полегшувати звичайні задачі системного адміністратора. Менеджер слідкує за станом веб-додатку, тому при або аварійному завершенні, або при витіку пам'яті за деяку межу, або при раптовому перезавантаженню серверу, веб-додаток буде перезавантажений.

Другою проблемою виявилось те, що коли користувач намагається відновити пароль та просить сервер, щоб він відправив листа до заданої електронної пошти, то ця операція відбувається синхронно, що є проблемою з точки зору великого відгуку від серверу. Вирішенням цієї проблеми було використано менеджер фонових завдань. Створювати завдання у чергу, які можуть опрацьовуватися у фоновому режимі. Переміщаючи трудомісткі завдання в чергу і виконуючи їх у фоні, програма може швидше обробляти веб-запити та швидше відповідати клієнту. Але в даному випадку, фонові завдання повинні оброблятися зі сторони автоматичного програмного забезпечення без відвідання будь-якої сторінки для їх запуску.

Автоматична обробка фонових завдань передбачає, що програма, яка оброблює завдання, також може потерпіти невдачу та аварійно завершитись. Отож для вирішення цієї проблеми було використано supervisor - клієнт-серверну систему, яка дозволяє контролювати низку процесів у операційних системах, подібних до UNIX.

Третьою проблемою є дуже повільна віддача статичного контенту веб-додатком, адже Nuxt призначен в першу чергу для візуалізації з JavaScript коду на HTML представлення. Отож Nuxt дуже погано підходить в якості веб-серверу, тому було вирішено використовувати в якості прошарки NGINX, що є HTTP-сервером і може виконувати завдання зворотного проксі-серверу. Таким чином, коли користувач вперше потрапляє на сторінку, nginx оброблює запит та делегує завдання візуалізації через проксі-сервер до Nuxt. Натомість вся статика, яка буде проходити на сервер, буде оброблятися саме веб-сервером NGINX, що підвищує продуктивність серверу та економить ресурси серверу.

У відповідності до перелічених проблем узагальнена схема запитів до серверу зображена на рисунку 1.

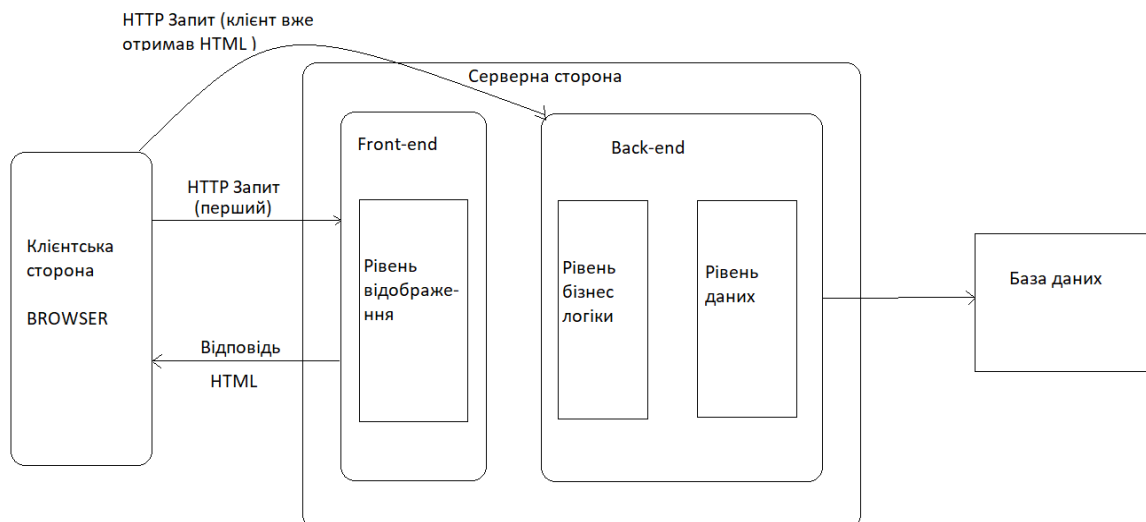


Рис. 1. Схема запитів до серверу з використанням візуалізації на стороні серверу

Висновки

В роботі виконана розробка та реалізація автоматизованої веб-системи тестування знань, рівень інформаційної безпеки якої, забезпечує захист інформації від найбільш критичних ризиків, встановлених у відповідності до OWASP Топ-10 2021. Розроблений програмний продукт може бути рекомендований для застосування в вищих та загальноосвітніх навчальних закладах, для підвищення якості знань та об'єктивності, завдяки застосуванню форми проведення тестування у автоматизованому форматі, з підвищеним рівнем інформаційної безпеки.

Список літератури

1. Mimirinis M. Qualitative differences in academics' conceptions of e-assessment. *Sci-hub*. URL: <https://www.tandfonline.com/doi/abs/10.1080/02602938.2018.1493087>
2. Li X. An examination of a gamified E-quiz system in fostering students' reading habit, interest and ability. URL: <https://doi/10.1002/pra2.2018.14505501032>
3. Alruwais N., Wills G., Wald M. Advantages and Challenges of Using e-Assessment. *International Journal of Information and Education Technology*. 2018. Vol. 8, No. 1. P. 34-37.
4. Kiryakova G. E-assessment-beyond the traditional assessment in digital environment. *International Conference on Technics, Technologies and Education 2020 (ICTTE 2020)*, 4-6 November 2020 Yambol, Bulgaria. P. 1-8.
5. Yin H. Taking e-Assessment Quizzes - A Case Study with an SVD Based Recommender System. *Sci-hub*. URL: <https://doi/10.1007/978-3-030-03493-1>
6. Mouri K. An automatic quiz generation system utilizing digital textbook logs. *Sci-hub*. URL: <https://www.tandfonline.com/doi/abs/10.1080/10494820.2019.1620291>
7. Petrova T., Ivanova M., Naydenova I. Evaluation of e-assessment: the students' perspective. *The 16th International Scientific Conference eLearning and Software for Education Bucharest*, 23-24 April 2020, Bucharest. P. 199-206.
8. Pevnev V., Popovichenko O., Tsokota Ya. Web application protection technologies. *Сучасні інформаційні системи*. 2020. Т.4, № 1. С. 119-123.
9. Demertzis K. Cognitive Web Application Firewall to Critical Infrastructures Protection from Phishing Attacks. *Journal of Computations & Modelling*. 2012. V.9. P. 1-26.
10. Bach-Nutman M. Understanding The Top 10 OWASP Vulnerabilities. *Ar Xiv*. URL: <https://arxiv.org/ftp/arxiv/papers/2012/2012.09960.pdf>
11. Zhongxu Y., Zhufeng L., Yan C. A Web Application Runtime Application Self-protection Scheme against Script Injection Attacks. *4th International Conference, ICCCS 2018*, 8-10 June 2018, Haikou, China. P. 566-577.
12. Rua M.T., Musab A.M., Farooq B.A. The impact of sql injection attacks on the security of databases. *6th International Conference on Computing and Informatics, ICOCI 2017*, 25-27 April, 2017, Korea. P. 323-331.

DEVELOPMENT OF A SECURE AUTOMATED WEB-BASED KNOWLEDGE TESTING SYSTEM

S.O. Pererva, K.O. Tryfonova

National Odessa Polytechnic University

1, Shevchenko, Odessa, 65044, Ukraine; e-mail: katikkatik@gmail.com

Modern education is aimed at providing an opportunity to acquire quality knowledge and skills. Many studies in recent years demonstrate the significant contribution of information technology to improving the quality of acquired knowledge and skills in all areas of education. To assess the quality of the knowledge gained during the educational process, it is necessary to carry out control in various forms. Significant pedagogical research proves the effectiveness of test control to obtain an assessment of knowledge and skills. Information technology can help increase the independence of testing and assessment from the personality of the teacher, that is, increase objectivity through the use of an automated test form. In accordance with modern realities, the development, implementation and subsequent use of automated software for testing knowledge takes place on the Internet. In this regard, information security is a factor that must be identified as the most important. Therefore, the purpose of this work is to develop and implement an automated web-based knowledge testing system with an increased level of information security. One of the most popular open source web application security research projects, the Open Web Application Security Project, publishes the top ten most common threats annually. The paper presents the development of a software protection mechanism, the level of information security of which ensures the protection of information from the most critical risks established in accordance with the OWASP Top 10 2021. The developed software product can be recommended for use in higher and general educational institutions, to improve the quality of knowledge and objectivity through the use of a test form in an automated format with an increased level of information security.

Keywords: information protection, web applications, distance learning, the quality of education, knowledge testing

МОДЕЛЮВАННЯ ОРГАНІЗАЦІЙНИХ ЗАХОДІВ ДЛЯ СТВОРЕННЯ ПОЛІТИКИ БЕЗПЕКИ ОРГАНІЗАЦІЇ З ВИКОРИСТАННЯМ БІЗНЕС-ПРОЦЕСІВ**В.В. Радущ, О.Ю. Лебедєва, Н.І. Кушніренко, В.В. Зоріло**Національний університет «Одеська політехніка», пр. Шевченко, 1, Одеса, 65044,
Україна; e-mail: o.y.lebedieva@opu.ua, kushnirenko@op.edu.ua, v.v.zorilo@op.edu.ua

Фундаментальним поняттям захисту інформації є політика безпеки, або політика захисту. Важливість цього поняття важко переоцінити – існують ситуації, коли правильно сформульована політика є чи не єдиним механізмом захисту від несанкціонованого доступу. Під поняттям політика безпеки інформації розуміється організована сукупність документованих керівних рішень, спрямованих на захист інформації й асоційованих з нею ресурсів системи. Політика безпеки викладає систему поглядів, основних принципів, практичних рекомендацій і вимог, що закладаються в основу реалізованого в системі комплексу заходів із захисту інформації. Формування політик безпеки є дуже складним аналітичним процесом, який важко формалізувати. У роботі наводяться організаційних заходів для створення політики безпеки підприємства. Для опису цих заходів використовуються нотації бізнес-процесів. Моделювання бізнес-процесу це процес відображення суб'єктивного бачення потоку робіт у вигляді формальної моделі, що складається з взаємопов'язаних операцій. В даний час найбільший розвиток і застосування при описі бізнес-процесів отримують графічні підходи та методи. Найбільш широко використовувана методологія опису бізнес-процесів це стандарт IDEF0. Нотація IDEF0 призначена для високорівневого опису бізнесу-процесу у функціональному аспекті. Було розроблено декомпозицію діаграм A-0 та A0. IDEF0 не використовують для побудови процесів нижнього рівня, які деталізують докладне виконання робіт персоналом для підвищення розуміння функціонування розробленого процесу було прийнято рішення показати взаємодію між механізмами, які використовувались у нотація IDEF0. Для опису взаємодії між механізмами була обрана нотація BPMN, яка орієнтована на детальний опис потоків робіт, і якнайкраще підходить для моделювання процесів на нижньому рівні.

Ключові слова: захист інформації, політика безпеки, організаційні заходи для створення політики безпеки, бізнес-процес, нотації бізнес-процесу, IDEF0, BPMN.

Вступ

Сучасне суспільство характеризується бурхливим розвитком інформаційних технологій, які займають дедалі міцніше місце на підприємствах різного профілю, допомагаючи вирішувати нагальні завдання управління та функціонування підприємств. В умовах безперервно змінюваних та вдосконалюваних загроз, реалізація яких може призвести до зриву функціонування підприємства на перше місце виходять завдання забезпечення інформаційної безпеки.

У міру того, як процес інформатизації більшості сфер діяльності в Україні, промисловості, соціальній сфері, бізнесу тощо розвивається бурхливими темпами. Постає питання про комплексний підхід до захисту інформації. Політика інформаційної безпеки спрямована на вирішення цієї проблеми. Коректне розроблена та актуальна політика безпеки відображає думку керівництва з питання інформаційної безпеки, пов'язує до купи всі методи захисту інформації, регламентує роботу співробітників. Політики інформаційної безпеки є основою подальшої розробки документів із забезпечення безпеки процедур, регламентів, посадових інструкцій тощо.

Актуальність розробки політик інформаційної безпеки для компаній пояснюється необхідністю створення механізму управління та планування інформаційної безпеки.

Також політики інформаційної безпеки дозволяють удосконалювати такі напрями діяльності компанії, як залучення інвестицій, підтримка безперервності бізнесу, мінімізація ризиків, підвищення рівня довіри до компанії тощо. Удосконалення напрямів діяльності організації залежить від грамотності упорядкування політики інформаційної безпеки. Тому тема даної роботи є актуальною.

Метою роботи є розробка бізнес-процесу організаційних заходів для створення політики безпеки підприємства шляхом використання різних нотацій опису бізнес-процесів.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

- Провести аналіз організаційних заходів для створення політики безпеки підприємства;
- Проаналізувати та обрати нотації моделювання бізнес-процесів для опису організаційних заходів для створення політики безпеки підприємства;
- Розробити бізнес-процес з використанням обраних нотацій.

Основна частина

Забезпечення інформаційної безпеки – це комплексна проблема, розв'язання якої на практиці вимагає ефективного сполучення нормативно-правових заходів (законодавчий рівень), організаційних заходів, інженерно-технічних методів і засобів, блокування та нейтралізації технічних каналів витоку інформації (адміністративний і процедурний рівень), методів і засобів криптографічного та технічного і захисту (програмно-технічний рівень)[1].

Основу заходів адміністративного рівня, тобто заходів, що реалізуються керівництвом організації, становить політика безпеки.

Під політикою безпеки розуміється сукупність документованих управлінських рішень, спрямованих на захист інформації й асоційованих з нею ресурсів. Політика безпеки визначає стратегію організації в галузі інформаційної безпеки, а також ресурси, які керівництво вважає за можливе виділити для реалізації її завдань. На підставі політики безпеки будується програма безпеки, яка реалізується на процедурному й програмно-технічному рівнях.

Політикою інформаційної безпеки (ІБ) називається комплекс заходів, правил та принципів, якими у своїй повсякденній практиці керуються співробітники підприємства/організації з метою захисту інформаційних ресурсів.

За час, що минув із виникнення самого поняття ІБ, напрацьовано чимало подібних політик – у кожній компанії керівництво саме вирішує, яким чином та яку саме інформацію захищати.

Політика безпеки є обов'язковою складовою певних місцевих або міжнародних стандартів (ISO/IEC 17799, ISO/IEC 27001 тощо). Необхідна відповідність конкретним вимогам, які зазвичай висувають зовнішні аудитори, що вивчають діяльність організації. Відсутність безпекової політики породжує негативні відгуки, а подібні оцінки негативно впливають на такі показники організації, як рейтинг, рівень надійності, інвестиційна привабливість тощо.

Узгодження політики безпеки з керівництвом підприємства, це спосіб донести до керівників цілі та завдання безпеки компанії. Затверджена безпекова політика, по суті, є формалізованою думкою керівництва компанії з питань забезпечення захисту інформації, на яку можна посилалися при обговоренні поточних питань, пов'язаних з безпекою.

Ще одне призначення політики інформаційної безпеки підприємства – доведення до рядових працівників основних принципів та правил захисту інформації, прийнятих у компанії. Зазвичай прості користувачі не будуть вдумливо читати насичені технічними термінами документи, наприклад, інструкції з роботи з електронною поштою або регламент антивірусного захисту. Політика безпеки, будучи верхньорівневим документом,

повинна у простій та зрозумілій формі доносити до кожного працівника позицію компанії щодо питань, пов'язаних з інформаційною безпекою.

Методологія моделювання, включає послідовність дій, які необхідно виконати для побудови моделі (процедуру моделювання), і нотацію (мова). Мова моделювання має свій синтаксис (умовні позначення різних елементів та правила їх поєднання) та семантику (правила тлумачення моделей та їх елементів).

Бізнес-процес являє собою систему послідовних, цілеспрямованих і регламентованих видів діяльності, в якій за допомогою керуючого впливу і за допомогою ресурсів входи процесу перетворюються в виходи, результати процесу, що представляють цінність для споживачів.

Ключовими властивостями бізнес-процесу є те, що це кінцева і взаємопов'язана сукупність дій, що визначається відносинами, мотивами, обмеженнями і ресурсами всередині кінцевої множини суб'єктів і об'єктів, які об'єднуються в систему заради спільних інтересів з метою отримання конкретного результату.

Моделлю бізнес-процесу називається його формалізований (графічний, табличний, текстовий, символічний) опис, що відображає реально існуючу або передбачувану діяльність підприємства[2].

Модель, як правило, містить такі відомості про бізнес-процес:

- 1) набір складових процесів кроків – бізнес-функцій;
- 2) порядок виконання бізнес-функцій;
- 3) механізми контролю та управління в рамках бізнес-процесу;
- 4) виконавців кожної бізнес-функції;
- 5) вхідні документи/інформацію, що використовуються кожною бізнес-функцією;
- 6) вихідні документи/інформацію, що генеруються кожною бізнес-функцією;
- 7) ресурси, необхідні для виконання кожної бізнес-функції;
- 8) документацію/умови, що регламентують виконання кожної бізнес-функції;
- 9) параметри, що характеризують виконання бізнес-функцій та процесу в цілому.

Метою моделювання є систематизація знань про компанію та її бізнес-процеси в наочній графічній формі з тим, щоб в подальшому дані процеси можна було аналізувати і вдосконалювати. Моделювання бізнес-процесів дозволяє проаналізувати не тільки, як працює підприємство в цілому, як воно взаємодіє із зовнішніми організаціями, замовниками та постачальниками, але і як організована діяльність на кожному окремо взятому робочому місці.

Текстовий спосіб опису бізнес-процесу це такий спосіб, що являє собою простий текстовий послідовний опис процесів.

Табличний спосіб опису бізнес-процесу є більш формалізованим і передбачає розбиття бізнес-процесу по осередках структурованої таблиці, в якій кожен стовпець і рядок мають деякий певне значення.

В даний час найбільший розвиток і застосування при описі бізнес-процесів отримують графічні підходи та методи. Вони мають найбільшу результативність при вирішенні задач по опису, аналізу та раціоналізації діяльності підприємства.

Нотація – це набір знаків і правил, які використовуються для графічного опису, моделювання бізнес-процесів. Нотація визначає як ми позначаємо на схемі процеси, операції, події та тощо, і за якими правилами з'єднуємо їх між собою.

Найбільш широко використовується методологія опису бізнес-процесів – стандарт IDEF0. Моделі у нотації IDEF0 призначені для високорівневого опису бізнесу компанії у функціональному аспекті. За допомогою наочної графічної мови IDEF0 система, що вивчається, постає перед розробниками та аналітиками у вигляді набору взаємопов'язаних функцій (функціональних блоків – у термінах IDEF0). Як правило, моделювання засобами IDEF0 є першим етапом вивчення будь-якої системи.

Розглянемо основні елементи нотації IDEF0, такі як результат, власник, виконавець, вхід, управління та механізми процесу.

В нашій роботі головний процес, що описується – це створення політики безпеки.

Результат бізнес-процесу – те, заради чого здійснюється бізнес-процес, тобто діяльність завжди розглядається разом з метою цієї діяльності – отримання на виході деякого результату, що задовольняє заданим вимогам. Результати бізнес-процесу часто згадуються як виходи бізнес-процесу. В нашій роботі результатом опису організаційних заходів для створення політики безпеки підприємства є документ з описаною політикою безпеки.

Власник бізнес-процесу – посадова особа, яка несе відповідальність за отримання результату процесу і володіє повноваженнями для розпорядження ресурсами, необхідними для виконання процесу. В нашій роботі власником бізнес-процесу є начальник відділу ІБ.

Виконавці бізнес-процесу – команда фахівців з різних функціональних областей (крос-функціональна команда), що виконують дії процесу. В нашій роботі виконавці – це спеціаліст з відділу ІБ та експертна група.

Входи бізнес-процесу – ресурси (матеріальні, інформаційні), необхідні для виконання і отримання результату процесу, які споживаються або перетворюються при виконанні процесу. В нашій роботі входи це відомості про організацію, для якої створюється політика безпеки.

Під відомостями про організацію будемо розуміти: структуру організації, модель ієрархії засобів обчислювальної техніки, ресурси інформаційної системи, що підлягають захисту, технологію обробки інформації.

Управління процесу – як правило інформація, яка визначає правила перетворення входів в вихід. В нашій роботі під управлінням процесу будемо розуміти стандарти, які використовуються для створення політики безпеки.

Механізм процесу – то, що перетворює вхід у вихід. Механізмами, як правило, є співробітники (в роботі це начальник відділу ІБ, спеціаліст з відділу ІБ, експертна група, керівники відділів) організації та техніка, на якій вони працюють (в роботі це програмне забезпечення для створення документу з політика безпеки).

Для опису процесу в нотації IDEF0 використовується такий принцип, як декомпозиція. Використання декомпозиції дозволяє розділити кожен блок, який розуміється як єдине ціле, на свої складові, що описуються на більш детальній діаграмі. Процес декомпозиції проводиться до досягнення необхідного рівня подробиці опису. Кожний рівень опису оформлюється як контекстна діаграма.

Перша діаграма в ієрархії діаграм IDEF0 завжди зображує функціонування системи в цілому. Такі діаграми позначаються А-0 (А мінус нуль). На рисунку 1 зображена діаграма А-0.

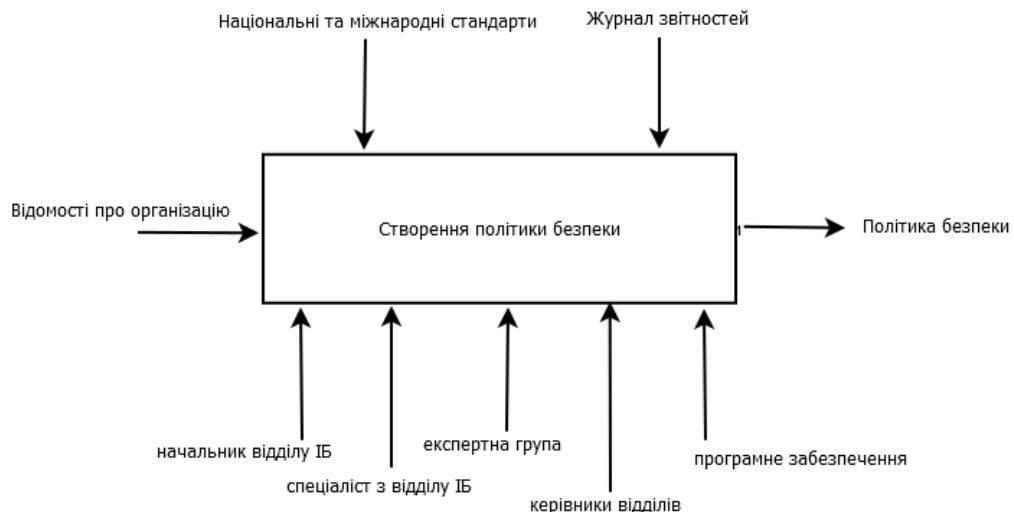


Рис. 1. Діаграма А-0

Процес «Створення політики безпеки» можна поділити на такі підпроцеси:

- Аудит інформаційної безпеки;
- Оцінювання ризиків;
- Опис правил інформаційного обміну з урахуванням ризиків і інцидентів, що виникали раніше.

Аудит інформаційної безпеки підприємства – процес отримання об'єктивних якісних та кількісних оцінок про поточний стан інформаційної безпеки організації відповідно до певних критеріїв, стандартів та показників.

Аудит ІБ передбачає реалізацію наступних етапів:

- проведення аудиту об'єкту інформаційної діяльності.
- створення моделі загроз.

Результатом аудиту будуть ризики, пов'язані з вразливостями в ІБ.

Другий процес при створенні політики безпеки це оцінка ризиків. Спочатку встановлюється зв'язок між ресурсами, втратами, загрозами і вразливими місцями, виділеними на процесі «Аудит ІБ».

Оцінка ризиків на цьому кроці здійснюється шляхом:

- з'ясування наслідків для ресурсів в разі реалізації ризиків в плані конфіденційності, цілісності та доступності;
- оцінки імовірності реалізації ризиків;
- встановлення рівня ризиків.

Ціль оцінки ризиків полягає у визначенні характеристик ризиків для інформаційної системи і її ресурсів. На основі таких даних можуть бути обрані необхідні засоби керування ІБ. Діаграма другого рівня (A0) зображена на рисунку 2.

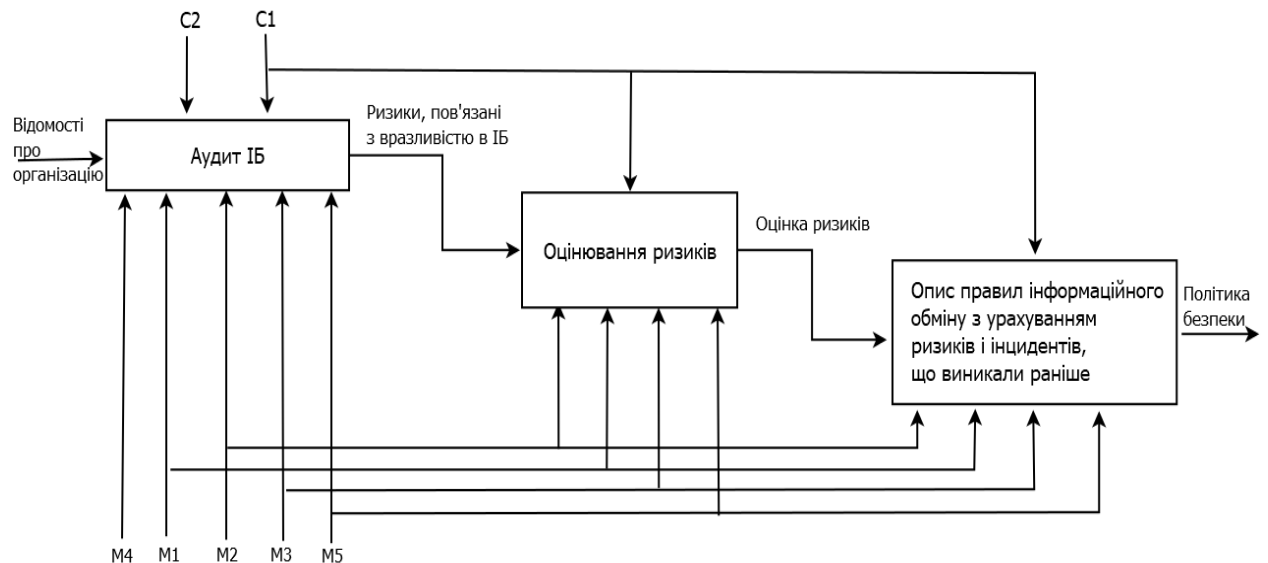


Рис. 2. Діаграма A0

За всіх переваг IDEF0 її не використовують для побудови процесів нижнього рівня, то що вона не деталізує докладне виконання робіт персоналом. По-перше, нотація IDEF0 не здатна відобразити тимчасову послідовність виконання робіт, а по-друге, не містить блоків умовного переходу, тому всі процеси описуватимуть роботи лише лінійно і недостатньо деталізовано.

При описі процесу «Створення політики безпеки» в нотації IDEF0 були запропоновані такі механізми, як начальник відділу ІБ, спеціаліст з відділу ІБ, експертна група, керівники відділів. Для підвищення розуміння функціонування процесу «Створення політики безпеки» бажано показати взаємодію між цими механізмами. Для цієї задачі підійде нотація BPMN.

BPMN (Business Process Management Notation) – це мова моделювання бізнес-процесів, яка є проміжною ланкою між формалізацією/візуалізацією та втіленням бізнес-процесу. Нотація є описом графічних елементів, що використовуються для побудови схеми протікання бізнес-процесу.

Розроблений процес «Створення політики безпеки» в нотації BPMN зображено на рисунку 3.

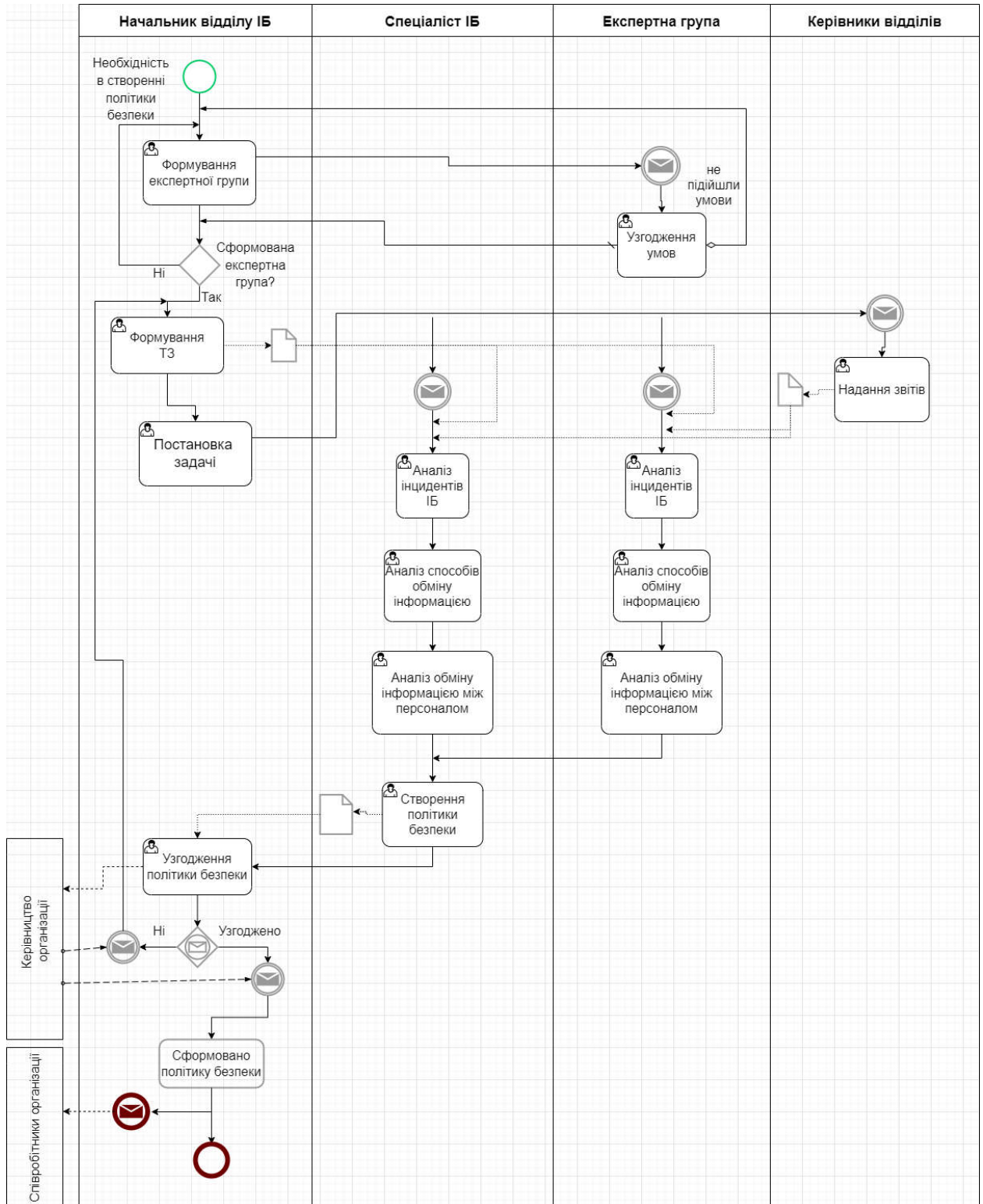


Рис. 3. Розроблений процес в нотації BPMN

Для відображення взаємодії між учасниками бізнес-процесу в нотації BPMN використовуються елементи Пул та Доріжка. Елемент Доріжка часто використовують як внутрішні ролі (зони відповідальності), що є розподілом обов'язків серед учасників процесу. Для процесу «Створення політики безпеки» в якості доріжок виступають начальник відділу ІБ, спеціаліст з відділу ІБ, експертна група, керівники відділів.

Доріжка фактично є зоною відповідальності учасника: будь-який елемент, вміщений у доріжку, виконується виконавцем, прописаним у заголовку доріжки.

Під дією або завданням у нотації BPMN розуміється одиниця роботи, що виконується під час виконання бізнес-процесу.

Подія є одним із головних елементів BPMN і служить для опису того, що має статися (на відміну від завдання, коли щось має бути зроблено). Залежно від стану події на схемі процесу діляться на: початкова подія (що ініціює бізнес-процес), проміжна подія, кінцева подія (що закінчує бізнес-процес).

Потік – це послідовність дій, що позначається стрілкою. Елемент потік показує яку дію після якої потрібно зробити.

Під артефактами в BPMN розуміють об'єкти, які безпосередньо не впливають на виконання бізнес-процесу. Це може бути документи, дані, інформація.

Висновки

Було проведено аналіз організаційних заходів для створення політики безпеки підприємства. Були розглянуті сучасні нотації моделювання бізнес-процесів. Для опису організаційних заходів для створення політики безпеки підприємства обрано нотації IDEF0 та BPMN. Було розроблено процес «Створення політики безпеки» з використанням обраних нотацій.

Список літератури

1. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підручник. К.: Видавництво НА СБ України, 2020. 256 с.
2. Гадецька З.М., Холопова М.О. Моделювання бізнес-процесів діяльності підприємства. *Ефективна економіка*. 2016. № 5. URL: <http://www.economy.nayka.com.ua/?op=1&z=4950>

**MODELING ORGANIZATIONAL ACTIVITIES TO CREATE AN
ORGANIZATION'S SECURITY POLICY USING BUSINESS PROCESSES**

V.V. Radush, O.Yu. Lebedieva, N.I. Kushnirenko, V.V. Zorilo

National Odessa Polytechnic University

The fundamental concept of information security is security policy. The importance of this concept is difficult to overestimate - there are situations where a well-formulated policy is almost the only mechanism to protect against unauthorized access. The concept of information security policy means an organized set of documented management decisions aimed at protecting information and associated system resources. The security policy sets out a system of views, basic principles, practical recommendations and requirements that underlie the set of information protection measures implemented in the system. Security policy-making is a very complex analytical process that is difficult to formalize. The paper presents organizational measures to create a security policy of the enterprise. Business process notations are used to describe these activities. Business process modeling is the process of reflecting a subjective vision of the workflow in the form of a formal model consisting of interrelated operations. Currently, the greatest development and application in the description of business processes are graphical approaches and methods. The most widely used business process description methodology is the IDEF0 standard. IDEF0 notation is intended for a high-level description of the business process in functional terms. Decomposition of diagrams A-0 and A0 was developed. IDEF0 is not used to build lower-level processes that detail the detailed work performed by staff. To increase the understanding of the functioning of the developed process, it was decided to show the interaction between the mechanisms used in the IDEF0 notation. To describe the interaction between the mechanisms, the BPMN notation was chosen, which focuses on a detailed description of workflows and is best suited for modeling lower-level processes.

Keywords: information protection, security policy, organizational measures for creating security policy, business process, business process notation, IDEF0, BPMN.

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

Том 11, номер 3, 2021. Одеса – 105 с., іл.

ИНФОРМАТИКА И МАТЕМАТИЧЕСКИЕ МЕТОДЫ В МОДЕЛИРОВАНИИ

Том 11, номер 3, 2021. Одесса – 105 с., ил.

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Volume 11, No. 3, 2021. Odesa – 105 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 № 5 від 16.11.2021)

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

Автори опублікованих матеріалів несуть повну відповідальність за підбір, точність наведених фактів, цитат, економіко-статистичних даних, власних імен та інших відомостей. Редколегія залишає за собою право скорочувати та редагувати подані матеріали

© Національний університет «Одеська політехніка», 2021