ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

UDC 004.056.55 **doi: 10.32620/reks.2023.4.13**

Volodymyr KORCHYNSKYI[1], Valerii HORDIICHUK[2], Vitalii KILDISHEV[1], Sergii STAIKUTSA[1], Olexandr RIABUKHA[1], Khaled ALFAIOMI[1]

[1] ***State University of Intellectual Technologies and Communication, Odesa, Ukraine***
[2] ***National Defence University of Ukraine, Kyiv, Ukraine***

METHOD OF INFORMATION PROTECTION BASED ON THE INTEGRATION OF PROBABILISTIC ENCRYPTION AND NOISE IMMUNE CODING

*The **subject matter** of this article is the processes of increasing information security in communication systems to solve applied problems that are critical in the transmission of confidential data. The **goal** is to develop a multi-stage method for protecting information from unauthorized access, based on probabilistic encryption integration, error-correcting code, and error decorrelation. The **tasks** to be solved are as follows: to develop a probabilistic encryption algorithm that considers the entropy of the characters' appearance in a message; to implement iterative coding with variable parameters of the information bits matrix; and to implement error decorrelation based on the generated matrix by interleaving information and check bits according to a given algorithm. **Methodology**: theory of signal communication and signal processing, theory of cryptography, theory of noise-resistant codes, probability theory, statistical analysis. The following **results** were obtained: a multi-stage method for protecting information from unauthorized access was proposed, in which at each step of data conversion, information secrecy is increased; probabilistic encryption was implemented, which considers the entropy of a discrete source of information when forming a space of random combinations; based on an iterative code with specified matrix parameters, an additional increase in the space of random combinations was implemented; error decorrelation reduces the multiplicity of errors in codewords and ensures mixing of bits according to a predetermined law. **Conclusions.** The scientific novelty of the results obtained is as follows: 1) an improved method of information protection from unauthorized access is proposed, based on probabilistic encryption integration, interference-resistant coding, and error decorrelation; 2) increasing information concealment is realized by eliminating the main shortcomings of probabilistic encryption, which did not take into account the entropy of the symbols of the open message; 3) it is proposed to form the space of random combinations taking into account the average probability of the appearance of a symbol in open texts, which will allow the output of a probabilistic cipher to form a stream of random combinations, which, according to its statistical properties, is close to the uniform distribution law; 4) further development of information protection methods based on interference-resistant coding and error decorrelation with encryption functions is received; 5) a further development of the statistical encryption method is the use of all redundant elements for both probabilistic encryption and interference-resistant coding.*

Keywords: *information protection; encryption; noise immunity; coding; random combination; decorrelation; ciphertext; statistics; probability; entropy.*

Introduction

Motivation. Increasing the information protection [1] of modern telecommunication systems requires effective and simple methods of interference immunity. Interference immunity allows the evaluation of confidential communication systems that operate under the conditions of electronic countering. The main indicators of interference immunity are noise immunity and secrecy. *Noise immunity* characterizes the ability of a communication system to provide a given transmission fidelity in the presence of random interference. *Secrecy* characterizes the ability of a communication system to transmit covertly confidential data over a communication channel in the conditions of radio electronic warfare.

Depending on the level of the OSI model, is carried out the information protection from unauthorized access (UAA), the following types of secrecy are distinguished: informational [2], structural [3], and energy [4]. To ensure information secrecy (cryptographic strength) [5], as a rule, cryptographic protocols are used [6]. Structural secrecy [7] is aimed at complicating the recognition of the structure of signal-code constructions and is implemented at the second level of the OSI model. Energy secrecy [8, 9] characterizes the ability of a communication system to mask the transmitted signal under the level of interference to complicate its interception by means of enemy electronic intelligence. This type of secrecy is implemented at the first level of the OSI model through various methods of spreading the spectrum of the original narrowband signal.

State of the art. As a rule, when data are transmitted over communication channels, it is necessary to solve two different problems: to protect data from channel interference or equipment malfunctions and to ensure the protection of information from UAA. The first problem solving is based on the theory of noise-resistant coding, but it does not address issues of information protection from UAA. The solution to the second problem is based on the theory of cryptography, which led to the creation of many different encryption systems. The works of K. Shannon [10] on coding and encryption served as the starting point for the development of these two areas independently of each other. Later, there has been a tendency to combine the processes of noise-resistant coding and encryption. A number of studies appear, in particular, in which researchers propose a comprehensive approach to information protection.

In 1984, S. Goldwasser and S. Mykali [11] first proposed the principle of probabilistic encryption for a cryptosystem with an open key. The disadvantage of such a cryptosystem is its vulnerability to plaintext attacks. It follows that a cryptanalyst can encrypt any message using the public key, and then compare it with the intercepted ciphertext.

At the same time, it is necessary to consider the fact that, as a rule, the tasks related to ensuring noise immunity and secrecy were considered by researchers separately and independently of each other. As a result, in communication systems in which it is necessary to ensure the minimum processing rate of the message in the transmitter and receiver, this requirement is not met. To minimize processing time, it is justified to use simple methods of data conversion, based on which integrated methods of protection against UAA and random noise can be implemented.

In modern conditions, issues of probabilistic encryption and noise immune coding are widely studied. There are several ways to develop this scientific direction.

The first way is to increase structural secrecy by complicating the algorithm of probabilistic encryption, as in previous studies [12, 13]. However, by itself, the complication of the signal structure leads to a deterioration of noise immunity, which is unacceptable in the conditions of radio-electronic warfare. In the work of African colleagues [14], a simple algorithm of probabilistic encryption is used, but it cannot be realistically applied in the conditions of a complex radio-electronic environment.

Note that the enemy is also working on this issue. In 2015, G. Maltsev proposed a combination of random coding (encryption), which is implemented together with noise-resistant coding and pseudo-random ensemble change [15]. It is possible to assume that with this method of protecting information from random interference and UAA, the current quality of the channel will affect the length of the ciphergram code combinations. For this reason, to ensure the necessary reliability of information transmission, the redundancy of the correcting code must be chosen considering the worst quality of the channel. The disadvantage of such a system is the high redundancy of ciphergram combinations, which is necessary to ensure the required reliability of transmission and protection of information from UAA.

The second way is the improvement of energy secrecy and noise immunity by various methods (as a variant by spectral characteristics changing), for example, as in works [3, 4, 16]. This, in turn, leads to additional complexities in the determination of signals at reception and, again, to additional computing power and energy costs.

Therefore, numerous works have appeared that consider the issue of increasing informational (cryptographic), structural, and energy secrecy in the complex, in particular by combining coding and encryption. This is the third way of development within the framework of the specified subject of research. Such methods have been considered, in particular, in works [7, 17]. However, again, the complexity of signals and measures to ensure energy secrecy require additional energy expenditure, which is extremely noticeable in certain cases – for example, in UAVs or embedded autonomous radio transmitters, ultra-low power radio stations, in general – all that have limited energy autonomy. Therefore, it is necessary to find a balance in accordance with the requirements for a specific communication system.

Thus, the issue of applying "lightweight" signal processing algorithms according to the requirements set for the information exchange system, which are not without significant computational complexity, and therefore significant energy consumption, has become relevant.

Among the recent works on the development of such lightweight signal processing methods, we consider that [18] is one of the best, which is based on the application of the block-matrix method of coding and encryption. The method is simple, suitable for transmitting information in real time (not a significant delay), developed specifically for use in UAVs, and it is sufficiently noise immune and secrecy. In turn, we offer an even simpler scheme in case it is necessary to extend the autonomy of the device with the given interference protection and secrecy.

Objectives and approach. Therefore, for performing the set requirements, it is advisable to use an approach in which confidential information is protected using various methods of data transformation that complement each other. In this work, to solve this problem, it is proposed to use probabilistic encryption, in which, in order to increase information secrecy, we should consider the entropy of the appearance of characters in the message.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

The feature of probabilistic encryption [13] is the possibility of forming different combinations of ciphertext for the same open text. The results of the research showed that the uneven distribution of the probability of the appearance of symbols in the open text is the reason for their correlation with random combinations of the ciphertext at the output of the probabilistic encoder. This means that this method of protecting information from UAA can be vulnerable to frequency analysis. To solve this problem, we propose the use of an algorithm for the redistribution of random combinations, in which the probability of their appearance at the output of the probabilistic encoder tends to the uniform law. Statistical analysis of the distribution of characters in texts of various lengths and subject matter was performed. Boundary values of the deviation of the probability of the occurrence of symbols in texts from the average value are determined. Based on these research results, the principles of forming the space of random code combinations for a probabilistic encoder are proposed. To increase the information secrecy and noise immunity of ciphertexts, we propose the use of probabilistic encryption together with an iterative code and error decorrelation.

The object of this research is to integrate probabilistic encryption and error-correcting coding with error decorrelation. Known methods of probabilistic encryption, as a rule, do not consider the entropy of a discrete source of information and do not provide control over the correctness of information transmission. To solve this problem, when forming the space of random code combinations, it is proposed to consider the average probability of appearing symbol in the open text. The increase in the space of random combinations is proposed to be combined with the control of the fidelity of information transmission based on iterative coding. Error decorrelation allows the implementation of additional mixing of bits in ciphertexts according to a given law, based on which it also decreases the multiplicity of errors in random combinations.

The subject of this research is methods for improving information secrecy and noise immunity based on the integration of probabilistic encryption and noise immune coding with error decorrelation. Known methods of probabilistic encryption are characterized by low information secrecy and are considered independent of noise immune coding. The problem of combining the considered methods of converting open information to ensure the noise immunity of transmitted data over a communication channel is solved.

The purpose of this study is to develop a method for integrated information protection based on probabilistic encryption and noise immune coding with error decorrelation.

1. Current Research Analysis

The noted shortcomings of the considered methods of statistical encryption made it possible to conclude about the expediency of using a multi-stage data transformation scheme. At the same time, at each stage, the tasks of increasing noise immunity and information secrecy must be solved without significantly increasing the redundancy of random code combinations.

Therefore, the authors propose a three-stage data transformation scheme. The first degree of information protection is realized using probabilistic encryption, in which the entropy of a discrete source of information is considered when forming the space of random combinations. In the second stage, iterative coding with parity control is used which solves the problem of data integrity control and increases the space of random combinations by forming a matrix with variable parameters. Such an interference-resistant coding algorithm will also increase the indicator of information secrecy. In the third stage, decorrelation of errors is implemented to reduce the frequency of error grouping in code combinations. This conversion makes it possible to increase the noise immunity of the channel and does not make high demands on the correcting ability of the code. The increase in information secrecy at this stage is performed on the basis of a given algorithm for reading bits of code combinations of the iterative code matrix. Thus, each stage of data transformation increases the information secrecy of the ciphertext. In the second and third stages, the tasks of increasing noise immunity are also solved.

It is known [8] that the use of uncertainty in the operation of information encryption systems significantly increases their cryptographic strength. In cryptographic protection systems, which are implemented based on probabilistic encryption, this is achieved by using generators of random sequences and many combinations. These combinations are randomly selected from some probability space L for representing symbol combinations in open text [8, 13]:

$$E_k : M \times L \to C, \tag{1}$$

where E_k is the encryption function;

k is the secret key;

M is the space of open texts;

L is the probabilistic space of codewords for representing text symbols;

C is the ciphertext space.

The advantage of such a cryptographic algorithm is that when the same open message is repeatedly encrypted, different ciphertexts can be obtained. However, this encryption method has redundancy of closed text combinations, the size of which depends on the cryptographic strength, which is a certain disadvantage. It

should also be noted that in some studies [13], the algorithm of probabilistic encryption is similar to random coding.

Figure 1 shows one of the possible schemes of probabilistic encryption based on the electronic codebook (ECB), where is implemented the mode of simple replacement.

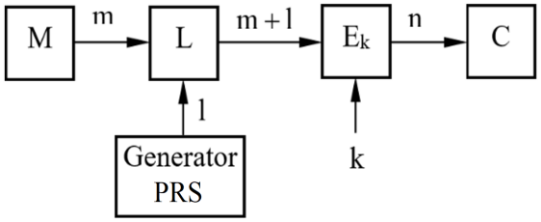

Fig. 1. Scheme of probabilistic encryption (random coding) in mode ECB (electronic codebook)

Code combinations with length m from the output space of the open texts M_i come to the concatenation block L. With the help of the pseudo random sequence (PRS) generator, combinations of length l are formed, which also come to block L, where the concatenation of sequences m occurs. From the output of block L, the extended code combination m + l is input to encryption block E_k. At the output of the block E_k, will be obtained encrypted combination with bitness n, which is more combination m open text. The feature of this method of encrypting code combinations is that with the same key, different ciphertexts for the same message will be obtained.

The following advantages of probabilistic encryption can be noted:

1) the possibility of increasing the lifetime of session keys;

2) increasing speed due to the reduction of in rounds;

3) increasing redundancy improves cryptographic strength.

Thus, in the case of interception of encrypted messages, the adversary's cryptographer remains able to calculate the encryption function. However, the disadvantage of such an encryption system is that the ciphertext will be a more open message and there is also the possibility of using frequency analysis for the decryption task.

2. Materials and Methods

2.1. Features of Integrating the Encryption Function with Noise-Resistant Coding

In the studies [7, 17] noted the feasibility of having a single data transformation process that would allow combining the functions of encryption and noise immunity coding. In cryptographic protocols, certain data conversion algorithms are used that allow the conversion of open text into closed text. The cryptographic strength of the algorithm depends on the length of the key. You can pay attention to the fact that both in noise immunity coding and encryption, data transformation is carried out. However, in the theory of coding and cryptography, two opposite problems are solved. This explains the presence of two different blocks of encryption and noise immunity coding in telecommunication systems. For the task of information protection from UAA, the noise immunity code cannot be applied because the formed allowed combination is divided, i.e., the location of information and check bits is known in advance. Noise immunity coding [7, 17] is implemented by adding a combination of check elements to the information part, which are formed according to a certain algorithm. The noise immunity code is characterized by its corrective ability, which determines the frequency of detection and correction errors.

In the study [17], we proposed various options for using noise immunity coding to protect transmitted information from random interference and UAA. As a rule, this is ensured by such a decoding procedure, in which non-separated allowed code combinations are formed. For example, for the McEliece cryptosystem, based on the corrective code are determined the minimum values of the parameters n=1024, t=50 and k=524, at which the sufficient cryptographic strength of the cipher is ensured. At the same time, the performance of such an encryption system is two to three orders of magnitude higher than that of a cryptosystem with RSA open key. However, the main disadvantage of the McEliece cryptosystem is the high redundancy of encryption.

In studies [3, 7], various options for integrating plausible encryption (random coding) with various noise immunity coding were proposed. In some articles [7, 13], random coding is understood as probabilistic encryption because they have similar principles for generating ciphertexts based on random combinations.

Integration of probabilistic encryption with noise immune code [8] provides: protection against random interference; message secrecy; integrity control of transmitted information (imitation protection). It can identify the main features of such integration [8]:

1) ensuring the required noise immunity of the transmission system, considering the probability of errors and the features of their distribution in the discrete channel;

2) on the transmitting side, a direct stochastic transformation of the code block of the message is performed, in which the functions of encryption and noise immunity coding are combined, and the statistical characteristics of the channel are also taken into account;

3) on the receiving side, the reverse transformation of the code block is performed, in which the integrity of

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

the received block is analyzed, if necessary, the integrity of the code block is corrected, and it is converted into open data of the confidential message.

Note that the implementation of this method of information protection from both random interference and UAA is ensured by the ensemble of random code combinations. The required level of cryptographic protection and transmission reliability is ensured by the number of code combinations used, which is designed to transmit the characters of an open message. At the same time, can be noted the certain disadvantages of stochastic coding:

- the entropy of a discrete source of information is not taken into account when choosing an ensemble of random code combinations, which increases the vulnerability of this method of protecting information from UAA;

- the cryptographic strength of the method directly depends on the redundancy of the method, which occurs due to the operation of replacing the combination of the open text symbol with a random combination from the given ensemble.

To eliminate these shortcomings, we propose increasing the cryptographic strength of the method by redistributing a sample of random code combinations, considering the probability of occurrence of symbols from the output of the message source. This will allow the output of the probabilistic converter to receive a stream of random code combinations with a uniform distribution law. To reduce the redundancy of random code combinations, we propose to integrate noise immunity coding in such a way that some of the excess bits are simultaneously used for detection or correction and to increase the size of the ensemble of random code combinations.

2.2. Method for Forming a Space of Random Combinations in Probabilistic Encryption

Consider the possibility of increasing the cryptographic strength of probabilistic encryption and reducing redundancy, provided that when forming the space of random encrypted combinations E_i, the entropy of a discrete source of information is considered. Entropy for the case when the symbols at the output of the information source do not obey the uniform distribution law is determined as follows [8]:

$$H_{NUN}(M) = -\sum_{j=1}^{L} p_j(m_j) \times \log_2 p_j(m_j), \quad (2)$$

where $p_j(m_j)$ is the probability of appearing symbol m_j in the message.

For the Russian alphabet, the entropy, considering the probability of the appearance of symbols in the text, is $H_{NUN}(M) = 4.42$. However, for the equiprobable law of the occurrence of symbols in the message, entropy $H_{UN}(M) = 5$.

The first condition for increasing the cryptographic strength of probabilistic encryption is possible on the condition that the combinations used in the space E_i for encryption, appear in the ciphertext with the equiprobable distribution law, i.e.

$$H_{NUN}(C) \to H_{UN}(C), \quad (3)$$

where $H_{NUN}(C)$ is the entropy of the space of combinations of ciphertexts with an uneven distribution law;

$H_{UN}(C)$ is the entropy of the space of ciphertext combinations with a uniform distribution law.

The second condition for increasing cryptographic strength is a magnification of the bitness of encryption combinations due to l, i.e.

$$n = m + l \to \infty. \quad (4)$$

where n is the total length of the combination;

m is the number of information bits;

l is the number of additional bits for forming random combinations.

It is obvious that condition (4) is purely theoretical because in practice, the combinations of the ciphertext should be limited.

One of the methods of cryptanalysis is the frequency analysis, based on which it is possible to assume that the existence of non-trivial statistical distribution of individual symbols and their sequences in both open and encrypted text. This means that during encryption and decryption, the regularities replacing symbols of open text with combinations ciphertext will be preserved. Important characteristics of the text are the repetition of letters (the number of different letters in each language is limited), pairs of letters, i.e., m (m -gram), compatibility of letters with each other, alternation of vowels and consonants, and some other features. Characteristically, these characteristics are quite stable.

Frequency analysis predicts that a text with a large amount of information will have a certain probability of appearing in a given letter alphabet. In addition, each language is characterized by the frequency of occurrence of repeated letters, the number of which is, as a rule, limited. For example, pairs of letters (m -grams), compatibility of letters with each other, alternation of vowels and consonants, and other features. At the same time, it is assumed that these characteristics are quite stable.

Table 1

Statistical indicators of the appearance symbols in texts of different lengths

№	Symbol	Average probability $p_j(c_j)$ appearance of symbols in the text	Deviation of the probability of the characters appearance in texts with different lengths from the average probability					
			$N_1 = 1424$		$N_2 = 3382$		$N_3 = 22336$	
			1424	$\Delta(c_j)_1$, %	3382	$\Delta(c_j)_2$, %	22336	$\Delta(c_j)_3$, %
1	о	0.10983	0.0955	13.05	0.095	13.50	0.0927	15.60
2	е	0.08483	0.0590	30.45	0.0618	27.15	0.0743	12.41
3	а	0.07998	0.0723	9.60	0.0671	16.10	0.0642	19.73
4	и	0.07367	0.0674	8.51	0.078	-5.88	0.0600	18.56
5	н	0.06700	0.0632	5.67	0.0529	21.04	0.0561	16.27
6	т	0.06318	0,0625	1.08	0.0574	9.15	0.0536	15.16
7	с	0.05473	0.0442	19.24	0.0426	22.16	0.0409	25.27
8	р	0.04746	0.0358	24.57	0.0464	2.23	0.0385	18.88
9	в	0.04533	0.0435	4.04	0.0331	26.98	0.0431	4.92
10	л	0.04343	0.0358	17.57	0.0302	30.46	0.0331	23.79
11	к	0.03486	0.0239	31.44	0.0237	32.01	0.0242	30.58
12	м	0.03203	0.0253	21.01	0.0378	-18.01	0.0272	15.08
13	д	0.02977	0.0225	24.42	0.0216	27.44	0.0237	20.39
14	п	0.02804	0.0225	19.76	0.0287	-2.35	0.0239	14.76
15	у	0.02615	0.0190	27.34	0.0180	31.17	0.0216	17.40
16	я	0.02001	0.0267	-33.43	0.0163	18,54	0.0160	20.04
17	ы	0.01898	0.0154	18.86	0.0186	2.00	0.0190	-0.11
18	ь	0.01735	0.0091	47.55	0.0139	19.88	0.0169	2.59
19	г	0.01687	0.0126	25.31	0.0121	28.28	0.0148	12.27
20	з	0.01641	0.0154	6.15	0.0136	17.12	0.0137	16.51
21	б	0.01592	0.0091	42.84	0.0133	16.46	0.0098	38.44
22	ч	0.0145	0.0147	-1.38	0.0103	28.97	0.0133	8.28
23	й	0.01208	0.0105	13.08	0.0109	9.77	0.0105	13.08
24	х	0.00966	0.0084	13.04	0.0121	-25.26	0.0107	-10.77
25	ж	0.0094	0.0084	10.64	0.0062	34.04	0.0093	1.06
26	ш	0.00718	0.0084	-16.99	0.0053	26.18	0.0075	-4.46
27	ю	0.00639	0.0049	23.32	0.0053	17.06	0.0048	24.88
28	ц	0.00486	0.0014	71.19	0.005	-2.88	0.0028	42.39
29	щ	0.00361	0.0035	3.05	0.0047	-30.19	0.0018	50.14
30	э	0.00331	0.003	9.37	0.0024	27.49	0.0026	21.45
31	ф	0.00267	0.00205	23.22	0.0035	-31.09	0.00207	22.47
32	ъ	0.00037	0.00033	10.81	0.00031	16.22	0.00031	16.22
33	ё	0.00013	0.00014	-7.69	0.00011	15.38	0.00014	-7.69

Let us analyze how different the probability of appearing symbols in russian-language texts with different numbers of symbols: $N_1 = 1424$, $N_2 = 3382$ and $N_3 = 22336$. Table 1 represents the results of the research, from which we can see that the deviation of the probability of the appearance of symbols in the text from the average probability $p_j(c_j)$ depends on its size and subject matter.

For example, the letter "e" for the texts of size N_1 and N_2 has deviation respectively $\Delta = 30.45\%$ and $\Delta = 27.15\%$, respectively, which is almost twice as much for text with a larger volume of symbols N_3 ($\Delta = 12.41$). That is, the statistical regularity approximation of the distribution probability appearance of the symbol «е» to the average value $p(e) = 0.08483$ when increasing N_i is preserved. However, it should be noted that there may be some anomalous deviations in the probability occurrence of the symbol from $p_j(c_j)$, which are not related to the increase in the amount of text. For example, for the letter «т» for the values N_1, N_2 and N_3, we obtain the corresponding values $p(т)_1 = 0.0625$, $p(т)_2 = 0.0574$ and $p(т)_3 = 0.0536$ with the deviation from the average probability $p_j(т_j) = 0.06318$, respectively, $\Delta(т)_1 = 1.08\%$, $\Delta(т)_2 = 9.15\%$ and $\Delta(т)_3 = 15.16\%$. The best indicator for the letter «т» is for text with a smaller amount.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Table 2

Variants of the distribution of combinations of encryption symbols, considering their redundancy and the probability of their appearance in open text

№	Symbol	Average probability of symbols appearing in the text $p_j(c_j)$	Distribution of the number of random combinations considering the probability of the appearance of symbols $p_j(c_j)$ in texts with different lengths and the total number of random code combinations N_l					
			l = 1		l = 2		l = 3	
			$N_{l=1} = 512$, $\gamma_{pe} = 0.889$		$N_{l=2} = 1024$, $\gamma_{pe} = 0.8$		$N_{l=2} = 2048$, $\gamma_{pe} = 0.727$	
1	2	3	4	5	6	7	8	10
1	о	0.10983	56		112		225	
2	е	0.08483	43	$N_{gr1} = 297$	87	$N_{gr1} = 595$	174	$N_{gr1} = 297$
3	а	0.07998	41	$N_{1-8} = 37$	82	$N_{1-8} = 74$	164	$N_{1-8} = 149$
4	и	0.07367	38		75		151	
5	н	0.06700	34		69		137	
6	т	0.06318	32		65		129	
7	с	0.05473	28		56		112	
8	р	0.04746	24		49		97	
9	в	0.04533	23		46		93	
10	л	0.04343	22	$N_{gr2} = 133$	44	$N_{gr2} = 266$	89	$N_{gr2} = 133$
11	к	0.03486	18	$N_{9-16} = 17$	36	$N_{9-16} = 33$	71	$N_{9-16} = 66$
12	м	0.03203	16		33		66	
13	д	0.02977	15		30		61	
14	п	0.02804	14		29		57	
15	у	0.02615	13		27		54	
16	я	0.02001	10		20		41	
17	ы	0.01898	10		19		39	
18	ь	0.01735	9	$N_{gr3} = 62$	18	$N_{gr3} = 125$	36	$N_{gr3} = 62$
19	г	0.01687	9	$N_{17-24} = 8$	17	$N_{17-24} = 16$	35	$N_{17-24} = 31$
20	з	0.01641	8		17		34	
21	б	0.01592	8		16		33	
22	ч	0.0145	7		15		30	
23	й	0.01208	6		12		25	
24	х	0.00966	5		10		20	
25	ж	0.0094	5		10		19	
26	ш	0.00718	4	$N_{gr4} = 19$	7	$N_{gr4} = 39$	15	$N_{gr4} = 19$
27	ю	0.00639	3	$N_{25-33} = 2$	7	$N_{25-33} = 5$	13	$N_{25-33} = 10$
28	ц	0.00486	2		5		10	
29	щ	0.00361	2		4		7	
30	э	0.00331	2		3		7	
31	ф	0.00267	1		3		5	
32	ъ	0.00037	0.19		0.38		0.76	
33	ё	0.00013	0.07		0.13		0.27	

Table 2 lists the variants for the symbol encryption combination distribution. Taking into account their redundancy l = 1, 2, 3 and the probability of the symbol appearance in the open text, provided that the number of alphabet symbols in the of open text $M_i = 33$. It is obvious that an increase in redundant elements l reduces the code rate of probabilistic encryption:

$$\gamma_{pe} = \frac{m}{n}, \qquad (5)$$

however, the cryptographic strength of the encryption increases. Therefore, when l = 1, we get the total encryption combinations $N_{l=1} = 512$. In columns 5, 7, and 9 of Table 2 we can see the distribution of encryption combinations considering the average probability of occurrence of symbols $p_j(c_j)$. Therefore, as we can see the distribution of encryption combinations considering the average probability of the occurrence of symbols $p_j(c_j)$. Therefore, as shown in Table 2, it is possible to increase the cryptographic strength of probabilistic encryption by increasing the space of random combinations, which reduces the relative speed γ_{pe}.

2.3. Method for integrating statistical encryption with error-correcting coding and error decorrelation

Consider the method of integrating probabilistic encryption and noise immunity coding. For efficient use of channel bandwidth, it is necessary to coordinate with the source of information at the input.

According to Shannon's main coding theorem [10], the probability of an erroneous element tends to zero when transmitting data over a noisy channel under the condition $n \to \infty$. This means that the code rate

$$\gamma_c = \frac{m}{n} = \frac{m}{m+r} \to 1, \quad (6)$$

a number of check elements r increases insignificantly compared with the number of information bits m. Such dynamics γ_c, m and r is presented for the cyclic code with a minimum code distance $d_0 = 4$ (see in Table 1). At the same time, the corrective ability of the code does not worsen.

As noted earlier, the main disadvantage of probabilistic encryption is redundancy. At the same time, it is obvious that with an increase in encryption redundancy, the cryptographic strength rises, and the code rate decreases.

Similar dynamics are typical for noise immunity coding. The more is code redundancy, the higher is the noise immunity. Consider the following integration option when probabilistic encryption is performed first, followed by noise immunity coding. In this case, the code block length is given by:

$$n = m + l + r, \quad (7)$$

In this case, the total code rate when using probabilistic encryption and noise immunity coding together is determined in view m, l and r as follows:

$$\gamma_{pec} = \frac{m}{m+l+r}. \quad (8)$$

The coefficient γ_{pec} can be increased by using the large number of bits in code block n. According to (6), it is advisable to choose long length code blocks n. It should be noted that in real data transmission (DT) systems with feedback (FB), the maximum packet length is limited because this can lead to an increase in the number of retransmissions. The effective speed of DT system with FB is estimated using the coefficients γ_c and γ_{req} [11]:

$$R_e = \gamma_c \cdot \gamma_{req} = \frac{1 - P_{del}(n)}{1 + (M-1) \cdot P_{del}(n)}, \quad (9)$$

where M is the number of repeated code words;

γ_{req} – coefficient that considers the probability of packet requests;

$P_{del}(n)$ is the probability of deleting the package.

Thus, with an increase in the packet length, the probability of its distortion increases, i.e., $\gamma_c \to \infty$, $\gamma_{req} \to 0$ and $R_e \to 0$. On Figure 2 shows the dependences R_e, γ_c and γ_{req} on the packet length.

It can be seen from the diagram that the condition

$$\gamma_c = \gamma_{req} \quad (10)$$

determines the optimal packet length n_{opt}, at which is provided the maximum value of the effective rate $R_e = R_{max}$.

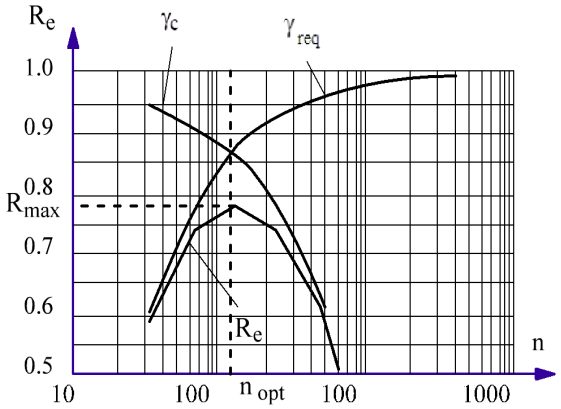

Fig. 2. Dependencies R_e, γ_c and γ_{req} from the length of the package

Consider the integration of probabilistic encryption and noise immunity coding using an example of iterative code (Figure 3) with a parity check bit in rows and columns.

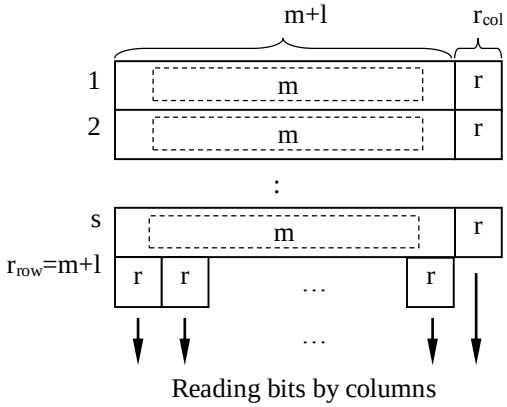

Fig. 3. Integration of probabilistic encryption and iterative coding with error decorrelation

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

The encryption and encoding options are as follows:

$m = 8$ – number of information bits;

s – the number of code combinations in the matrix;

$q = m \times s$ – length of the information part of the iterative code;

$n = s \times (m + l) + r_{tot}$ – total number of bits in the iterative code;

$r = 1$ – check bit for each row and column;

$r_{tot} = r_{row} + r_{col}$ – total number of check bits;

r_{row} – number of check bits for rows;

r_{col} – number of check bits for columns.

Thus, adding just one check bit increases the length of the random sequence, which increases the information secrecy of probabilistic encryption and ensures the detection of odd multiplicity errors in each row and column. With iterative coding, the minimum code distance $d_0 = 4$, which guarantees the correcting of single errors $t_{cor} = 1$ the detection of errors of higher multiplicity $t_{det} = 3$.

For the channel with grouping errors, it is possible to increase the efficiency of the iterative code by interleaving bits. The output sequence of the encoder is formed as a result of bit-by-bit reading of the columns of the matrix. This method of transmission allows the implementation of decorrelation of errors, which reduces the multiplicity of their occurrence in the code block. Bit interleaving also increases both the noise immunity of the transmission system and the cryptographic strength of probabilistic encryption.

3. Results

The results of the research showed the possibility of increasing the information secrecy of probabilistic encryption, given that when forming an ensemble of random combinations, we will consider the entropy of the discrete message source. It was proposed to consider the probability of its occurrence in the message $p_j(c_j)$ while choosing the number of random combinations for each symbol. For symbols c_j with a higher probability of occurrence, combinations that are more random should be used. The number of random combinations is determined by the following formula:

$$N(c_j) = p_j(c_j) \cdot N_l, \qquad (11)$$

where $N_l = 2^{m+l}$ is the total number of statistical encryption combinations.

In Table 2 in the columns 4, 6, 8 present the calculated values of the random code combinations $N(c_j)$ for each symbol, taking into account the average probability $p_j(c_j)$. Thus, it is necessary to consider $p_j(c_j)$ for each symbol of the alphabet to form ensembles of random combinations. A simplified version of the distribution of combinations is also possible, in which the symbols of the alphabet are divided into certain groups, considering the magnitude of the values. In Table 2 shows four such groups. For $l = 1$ total $N_{l=1} = 512$ random combinations are used with their distribution into groups: $N_{gr1} = 297$; $N_{gr2} = 133$; $N_{gr3} = 62$; $N_{gr4} = 19$. Within each group, for each symbol c_j, the same number of random combinations is selected: $N_{1\text{-}8} = 37$; $N_{9\text{-}16} = 17$; $N_{17\text{-}24} = 8$; $N_{25\text{-}33} = 2$. A similar division into groups was made for $l = 2$ and $l = 3$. It is advisable to carry out such a distribution of random combinations only when small text sizes are used for encryption. Statistical evaluation of the probabilities of the occurrence of symbols for texts with sizes $N_1 = 1424$, $N_2 = 3382$ и $N_3 = 22336$ showed a significant spread of values $\Delta(c_j)_i$ from zero. For text of small size $N_1 = 1424$, the spread is quite large $\Delta(c_j)_1 = -33.55 \ldots 71.19\%$. With an increase in the size of texts, the range of values $\Delta(c_j)_2 = -31.09 \ldots 34.04\%$ and $\Delta(c_j)_3 = -10.77 \ldots 38.46\%$ decreases by 1.6 ... 2.12 times. Thus, the statistical regularity of the obtained results indicates that the symbol appearance probabilities tend to average with increasing text size.

The integration of probabilistic encryption and noise immunity coding should be based on the more efficient use of redundant elements that could be used to increase cryptographic strength and detect and/or correct errors. In this case, the redundancy of probabilistic encryption can be considered justified if part of the additional symbols $r_{tot} = r_{row} + r_{col}$ are aimed at increasing cryptographic strength and solving the problem of ensuring noise immunity. We should also pay attention to the expediency of using as many random combinations 2^{m+l} as possible to implement the problem of noise immunity coding. When iterative coding is used, the increase in cryptographic strength is carried out by increasing the ensemble of used combinations by adding the checked bit for each row and column of the matrix. For the given iterative code, the value is $d_0 = 4$, so the code can correct a single error $t_{cor} = 1$ and detect errors of higher multiplicity $t_{det} = 3$. Given that the corrective ability of the code is not very high, the use of error decorrelation will reduce the grouping of errors in the channel. The choice of the optimal length of the encrypted packet according to the condition makes it possible to match the transmission parameters with the statistical features of the distribution of errors in the discrete channel.

The data reading algorithm can be different and in fact represents another encryption scheme based on mixing the elements of the rows and columns matrix of the iterative code.

4. Discussion

The advantage of probabilistic encryption is the use of random processes in the algorithm of open text transformation. It allows the formation of different ciphertexts during repeated probabilistic encryption of the same message. One of the disadvantages of this method is the

availability of a large random combination redundancy, on which information secrecy depends. Another disadvantage is the non-uniformity of the generated random combinations at the output of the probabilistic encoder. This enables an adversary cryptanalyst to successfully apply frequency analysis to decrypt intercepted ciphertexts.

The combined use of probabilistic encryption and noise-immunity coding with error decorrelation ensures information protection from UAA and random noise. The information secrecy of probabilistic encryption depends on the number of used random combinations; however, at the same time, the size of the ciphertext increases. The disadvantage of this method of information protection is the uneven nature of the appearance of random code combinations from the output of the probabilistic encoder. Therefore, in the scheme of a probabilistic encoder, it is proposed to consider the entropy of a discrete message source, i.e., the number of random combinations should be chosen in view of the average probability appearance of a symbol in the texts of the alphabet used. This ensures the formation of stream random code combinations from the output of the probabilistic encoder, which tends to a uniform distribution law. When intercepting such an encrypted message, the work of the enemy cryptographer becomes much more difficult. It is also possible for the simple version to form ensembles of random code combinations by combining symbols into groups, in which the probabilities of their occurrence do not differ significantly. However, this method is advisable when open texts are small.

It is possible to increase the information secrecy by expanding the space of random combinations, which is possible due to additional bits, which will also be the test part of the noise immune code. Thus, the integration of check elements of the noise immune code in combination with probabilistic encryption will increase information secrecy and combine noise immunity and transformation processes into one task.

The ideal option for this task is when all redundant elements are used for both probabilistic encryption and noise immune coding. In this case, it is necessary to form for each symbol of the alphabet its own ensemble of allowed random combinations. It should also be noted that one of the problems of probabilistic encryption is the generation of an ensemble of random combinations, which must be periodically changed.

The proposed method for protecting information from interference and unauthorized access is quite simple from an implementation point of view because it does not contain complex data conversion methods and can be easily implemented in software. Wherein it is possible to obtain arbitrarily high information secrecy, given that $n = m + l \to \infty$. However, in practice, transmitting data with large lengths of code combinations increases the likelihood of errors. This means that it is also necessary to increase the redundancy of the correction code to ensure the required reliability of the ciphergram transmission. Consequently, the effective transmission rate of the communication system R_e will decrease significantly, as shown in Figure 2. Therefore, the number of additional bits to the information combination k = 8 should not exceed three bits.

Conclusions

The actual task to improve methods of increasing information secrecy and noise immunity is implemented based on the integration of probabilistic encryption and noise immunity coding with error decorrelation.

The scientific novelty lies in the fact that for the first time, a method of information protection from unauthorized access was proposed using three stages of data conversion; each solves the problem of information secrecy and noise immunity increasing.

Information secrecy (the first step in information protection from unauthorized access) is implemented based on probabilistic encryption, which considers the entropy of the appearance of characters in the message. At this stage of the study, an analysis of the probabilistic encryption effectiveness in terms of counteracting frequency analysis is presented.

In the second stage, it was proposed to use iterative noise immune coding with parity check bits over the rows and columns of the matrix. This noise immune code guarantees the correcting of a single error and the detection of errors of the highest multiplicity. The use of the iterative code with variable parameters allows setting the required matrix size and the rule for reading data when implementing the error decorrelation procedure. At this stage, the space of random combinations increases because of the presence of additional check bits, the location of which depends on the parameters of the matrix and the data reading algorithm.

In the third stage, interleaving and reading bits according to the given algorithm from the matrix of the iterative code implement the error decorrelation. This allows reducing the frequency of occurrence errors in code combinations and increasing the reliability of data transmission without increasing the corrective ability of the noise immune code. Error decorrelation is equivalent to the procedure of mixing the bits of the message, which, as a rule, is characteristic of encryption. Thus, in the third stage, an increase in the noise immunity of transmission and information secrecy is provided.

Future research development. The practical significance of the obtained results lies in the fact that the algorithm for information protection has been developed from both random noise and unauthorized access. Simultaneously, the problems of integrating methods for

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

increasing noise immunity and secrecy of transmission into a single process are solved. The results of the experiment make it possible to recommend the proposed method of information protection for the development of real noise-immune communication systems. The prospect of further research is the study of the proposed set of indicators for constructing no- noise immunity communication systems that increase noise immunity and information and secrecy.

Contributions of authors: Contributions of authors: review and analysis of references, formulation of the purpose and tasks of research, formulation of conclusions – **Olexandr Riabukha**; development of conceptual provisions and methodology of research – **Volodymyr Korchynskyi, Valerii Hordiichuk, Khaled Alfaiomi**; development of mathematical models and analysis of research results – **Sergii Staikutsa, Vitalii Kildishev**.

All the authors have read and agreed to the published version of this manuscript.

References

1. Serkov, A. A., Kasilov, O. V., Lazurenko, B. O., Pevnev, V. Y., & Trubchaninova, K. A. Strategy of building a wireless mobile communication system in the conditions of electronic counteraction. *Radioelectronic and computer systems*, 2023, no. 2(106), pp. 160-170. DOI: 10.32620/reks.2023.2.13.

2. Avramenko, V., & Demianenko, V. Serial encryption using the functions of real variable. *Radioelectronic and computer system*, 2021, no. 2(98), pp. 39-50. DOI: 10.32620/reks.2021.2.04.

3. Hordiichuk, V., Korchynskyi, V., Kildishev, V., & Zakharchenko, M. Timer Signals Transmission Security Increase Based on Spectrum Spreading Methods. *IEEE 2nd Ukrainian Microwave Week (UkrMW)*, 2022, pp. 1-4. DOI: 10.1109/UkrMW58013.2022.10036952.

4. Vasyuta, K. V., Zbezhkhovska, U. R., Slobodyaniuk, V. V., Zakharchenko, I. V., Kashchyshyn, O. L., Dubynskyi, M. S., Ryabukha, Yu. M., & Koval, O. M. Metod pidvyshchennya skrytnosti system peredachi informatsiyi na osnovi moduliatsiyi z ortohonal'nym chastotnym rozdilennyam i mul'typleksuvannyam khaotychnykh pidnesuchykh [The method of increasing the stealthiness of information transmission systems based on modulating with orthogonal frequency division and multiplexing of chaotic subcarriers]. *Radioelektronni i komp'uterni sistemi – Radioelectronic and computer systems*, 2021, no. 4, pp. 79-93. DOI: 10.32620/reks. 2021.3.07. (In Ukrainian).

5. Grozov, V., Guirik, A., Budko, M., & Budko M., Cryptographic Strength Study of the Pseudorandom Sequences Generator Based on the Blender Algorithm *14th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, 2022, pp. 191-195. DOI: 10.1109/ICUMT57764. 2022.9943350.

6. Mohammad Khalid Imam, R. Cryptographic Algorithms and Protocols. *Chapter 2 in A Step Towards Society 5.0. Research, Innovations, and Developments in Cloud-Based Computing Technologies* Boca Raton: CRC Press, 2021, pp. 32-42. DOI: 10.1201/9781003138037-2.

7. Zakharchenko, M., Korchynskii, V., Kildishev, V. Integrated methods of information security in telecommunication systems. *International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo'2017),* proceeding, 2017, pp. 78-81. DOI: 10.1109/UkrMiCo.2017.8095428.

8. *Information technology. Security techniques. Code of practice for information security controls.:* ISO/IEC 27002:2013. [Effective from 2013-09-25]. Geneva, ISO, 2013. 80 p. Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en (accessed November 10, 2023).

9. Korchinskyi, V., Hadzhyiev, M., Pozdniakov, P., Kildishev, V., & Hordiichuk, V. Development of the procedure for forming nonstationary signal structures based on multicomponent LFM signals. *Eastern-European Journal of Enterprise Technologies*, 2018, vol. 6, no. 9 (96), pp. 29-37. DOI: 10.15587/1729-4061.2018.151816.

10. Shannon, C. E. Communication theory of secrecy systems. *The Bell System Technical Journal*, 1949, vol. 28, no. 4, pp. 656-715. Doi: 10.1002/j.1538-7305.1949.tb00928.x.

11. Goldwasser, S., Micali, S. Probabilistic Encryption. *Journal of Computer and System Sciences*, 1984, no.28, pp.270-299, DOI: 10.1016/0022-0000(84)90070-9

12. Yong Zhang, Ruiyou Li, Yuwen Shi & Fan Luo The Probabilistic Image Encryption Algorithm Based on Galois Field GF(257), *IETE Journal of Research*, Published online: 22 Nov 2023. DOI: 10.1080/ 03772063.2023.2284956

13. Munoz, F. D., & Watson, J. P. A scalable solution framework for stochastic transmission and generation planning problems. *Computational Management Science*, 2015, no. 12, pp. 491-518, DOI: 12.10.1007/ s10287-015-0229-y.

14. George Asante, James Ben Hayfron-Acquah, Michael Asante, Joshua Caleb Dagadu. A Symmetric, Probabilistic, NonCircuit Based Fully Homomorphic Encryption Scheme, *International Journal of Computer Networks and Applications*, 2022, no. 9(2), pp. 160-168, DOI: 10.22247/ijcna/2022/212332.

15. Maltsev, G. N. Pomehoustojchivost i skrytnost peredachi informacii po radiokanalam na osnove kombinirovannogo sluchajnogo kodirovanija [Noise immunity and secrecy of transmitting information over radio channels based on combined random coding].

Informacionno upravliajushchie sistemy – Information control systems, 2015, no. 2 (75), pp. 82-89. (In Russian).

16. Dhall, S.; Pal, S.K.; Sharma, K. A chaos-based probabilistic block cipher for image encryption. Journal of King Saud University - Computer and Information Sciences, 2022, no. 34 (1), pp. 1533-1543. DOI: 10.1016/j.jksuci.2018.09.015.

17. Korchynskyi, V. V., Kildishev, V. I., Holev, D. V., & Berdnikov, O. M. Increasing the secrecy of transmission information based on combined random coding. *Radio Electronics, Computer Science, Control*, 2019, no. 3, pp. 108-116. DOI: 10.15588/1607-3274-2019-3-12.

18. Shafique, A., Mehmood, A., Elhadef, M., Hesham khan, K. A lightweight noise-tolerant encryption scheme for secure communication: An unmanned aerial vehicle application, PLoS ONE, 2022, no. 17(9), Published online: 19 Sep, 2022. DOI: 10.1371/journal.pone.0273661.

Received 17.07.2023, Accepted 20.11.2023

МЕТОД ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ ІНТЕГРУВАННЯ ІМОВІРНІСНОГО ШИФРУВАННЯ ТА ЗАВАДОСТІЙКОГО КОДУВАННЯ

Володимир Корчинський, Валерій Гордійчук, Віталій Кільдішев, Сергій Стайкуца, Олександр Рябуха, Аль-Файюмі Халед

Предметом дослідження статті є процеси підвищення безпеки передавання інформації в системах зв’язку. Об’єкт дослідження – способи обробки інформації, що об’єднують методи підвищення її захисту в системах зв’язку: забезпечення інформаційної прихованості (захист від виявлення), криптозахисту (захист від дешифрування та розкриття вмісту повідомлення), завадостійкості (стійкість до випадкових завад). Безпосередньою метою роботи є розробка методу комплексного захисту інформації від несанкціонованого доступу на основі інтеграції ймовірнісного шифрування, завадостійкого кодування та декореляції даних. Під час дослідження були використані: основи теорії зв'язку та обробки інформації, теорія завадостійких кодів, теорія ймовірностей, ентропійна оцінка інформації, статистичний аналіз, частотний аналіз, математичне моделювання та ін. Запропонований метод захисту інформації від несанкціонованого доступу на основі інтеграції ймовірнісного шифрування, завадостійкого кодування та декореляції помилок дозволить підвищити скритність інформації шляхом усунення основних недоліків імовірнісного шифрування, яке не враховує ентропію символів у відкритому повідомленні. Збільшення простору випадкових комбінацій пропонується здійснити на основі контролю вірності передачі інформації ітераційним кодом. Декореляція даних в пакетах повідомлень шляхом змішування бітів за заздалегідь визначеним законом дозволить в подальшому виявляти або виявляти та виправляти (залежить від кратності помилок в пакеті) більше помилок при застосуванні завадостійкого кодування та додатково зменшить ймовірність розкриття вмісту повідомлення. Висновок. Завдання підвищення захисту інформації вирішується на трьох етапах радіоелектронної боротьби: виявлення та визначення, дешифрування та розкриття, глушіння. Наукова новизна отриманого результату полягає в запропонованому методі, який поєднує в одному процесі підвищення завадостійкості та інформаційної прихованості прихованості за допомогою перерахованих вище методів.

Ключові слова: захист інформації; шифрування; завадостійкість; кодування; випадкова послідовність; декореляція; шифротекст; статистика; ймовірність; ентропія.

Корчинський Володимир Вікторович – д-р техн. наук, проф., зав. каф. кібербезпеки та технічного захисту інформації, Державний університет інтелектуальних технологій і зв’язку, Одеса, Україна.

Гордійчук Валерій Валентинович – канд. техн. наук, старш. досл., начальник науково-дослідного відділу Центру воєнно-стратегічних досліджень, Національний університет оборони України, Київ, Україна.

Кільдішев Віталій Йосипович – канд. техн. наук, доц. каф. кібербезпеки та технічного захисту інформації, Державний університет інтелектуальних технологій і зв’язку, Одеса, Україна.

Стайкуца Сергій Володимирович – канд. філос. наук, доц. каф. кібербезпеки та технічного захисту інформації, Державний університет інтелектуальних технологій і зв’язку, Одеса, Україна.

Рябуха Олександр Миколайович – канд. техн. наук, старш. викл. каф. кібербезпеки та технічного захисту інформації Державний університет інтелектуальних технологій і зв’язку, Одеса, Україна.

Аль-Файюмі Халед – асп. каф. кібербезпеки та технічного захисту інформації Державного університету інтелектуальних технологій і зв’язку, Одеса, Україна.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Volodymyr Korchynskyi – D. Sc. (Technical Sciences), Full Professor, Professor at Cybersecurity and Technical Information Protection Department, State University of Intelligent Technologies and Telecommunications, Odesa, Ukraine,
e-mail: vladkorchin@ukr.net, ORCID: 0000-0003-3972-0585, Scopus Author ID: 35762706900.

Valerii Hordiichuk – Candidate of Technical Sciences, Senior Research Fellow, Head of the Research Department, Centre for Military and Strategic Studies, National Defence University of Ukraine, Kyiv, Ukraine, e-mail: gordiychukvalval@gmail.com, ORCID: 0000-0003-3665-4201, Scopus Author ID: 57195354143.

Vitalii Kildishev – Candidate of Technical Sciences, Associate Professor, Associate Professor at Cybersecurity and Technical Information Protection Department, State University of Intelligent Technologies and Telecommunications, Odesa, Ukraine,
e-mail: kildishev@ukr.net, ORCID: 0000-0002-7121-4060, Scopus Author ID: 57200279601.

Oleksandr Riabukha – Candidate of Technical Sciences, Senior Lecturer at Cybersecurity and Technical Information Protection Department, State University of Intelligent Technologies and Telecommunications, Odesa, Ukraine, e-mail: ryabukha@gmail.com, ORCID: 0000-0001-7402-0395, Scopus Author ID: 57553362000.

Sergii Staikutsa – Candidate of Philosophical Sciences, Associate Professor, Associate Professor at Cybersecurity and Technical Information Protection Department, State University of Intelligent Technologies and Telecommunications, Odesa, Ukraine,
e-mail: s.staikuca@gmail.com, ORCID: 0009-0002-1710-5792.

Khaled Alfaiomi – PhD student of Cybersecurity and Technical Information Protection Department, State University of Intelligent Technologies and Telecommunications, Odesa, Ukraine,
e-mail: khaled@alfaiomi.com, ORCID: 0000-0003-4624-2569.