Olexander BELEJ[1], Tavakkul RASHIDOV[2]

Opiekun naukowy: Olexander BELEJ

MODEL SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

Streszczenie: Badania systemów bezpieczeństwa informacji są możliwe używając metod modelowania procesów oraz działania tychże systemów. Jako model matematyczny opisujący dynamiczne zachowanie się system bezpieczeństwa informacji - zaproponowano metodę dyskretną do reprezentowania procesu bezpieczeństwa informacji. Taki sposób modelowania odpowiada rodzajowi rozważanych obiektów oraz istotnie ułatwia ich opis matematyczny. Wykazano, że najważniejszym czynnikiem (etapem), który ma wpływ na jakość podejmowanych decyzji – gdy zarządza się bezpieczeństwem informacji w jakieś organizacji – jest ocena rzeczywistego (bieżącego) stanu systemu bezpieczeństwa informacji. Zaprezentowany system mapowania pozwala na wykrywanie wzajemnych zależności oraz wzajemnych wpływów różnych czynników, które wpływają na system bezpieczeństwa informacji oraz stanowią metodologiczną bazę dla rozwoju specjalnych metod. Proces doskonalenia formalnego schematu (rozważanych systemów) pozwala na strukturalne oraz precyzyjne formułowanie zakresów i celów zadań przy ocenianiu stanu systemu bezpieczeństwa informacji.

Słowa kluczowe: bezpieczeństwo informacji, model, formalizacja, zarządzanie, system informacji, ocena stanu systemu

BUILDING A MODEL OF INFORMATION SECURITY MANAGEMENT SYSTEM

Summary: Investigation of the information security system is possible using the methods of modeling the processes of their operation. As a mathematical scheme for describing the dynamics of the information security system, a discrete method for representing information security processes is proposed, which corresponds to their content and greatly facilitates their mathematical description. It is shown that the most important stage that influences the quality of the decision taken while managing the organization's information security is the assessment of the actual state of the information security system. The presented mapping system allows revealing the interdependence and mutual influence of various factors that have an impact on the organization's information security system and serves as a methodological basis for the development of specific methods. The process of developing a formal scheme allows you

[1] Economic Dr, Lviv Polytechnic National University, Department of Computer-Aided Design, associate professor, Ukraine, Lviv, 5 Mytropolyt Andrei str., Building 4, Room 324, tiger_oles@i.ua, Oleksandr.I.Belei@lpnu.ua

[2] State university "The University of Banking", Lviv's educational institute, department of the "economic & information technology", student, kiber2@ukr.net

to structure and clearly formulate the essence of the task of assessing the state of the information security system.

Keywords: information security, model, formalization, management, information system, state assessment

1. Formulation of the problem

Information security is achieved by implementing an appropriate set of information security management measures to protect information from a wide range of threats to ensure confidentiality, integrity and accessibility of information in organizations [8, 10]. To ensure compliance with the requirements for confidentiality, integrity and accessibility of information, an information security management system and an appropriate information security management system (ISMS) should be established.

Specific features in solving the problems of creating an information security system (ISS) are:

- Incompleteness and uncertainty of the initial information about the characteristic threats to information security
- Multicriteria of the task of creating and evaluating the state of ISS, connected with the need to take into account a large number of particular indicators (requirements) of the information security system
- Availability of both quantitative and qualitative indicators, which must be taken into account when solving problems of development and implementation of ISS
- Impossibility of using classical optimization methods.

Consequently, the information security system is the bearer of the properties of a complex system. Determination of optimal (rational) options for its construction and ensuring the effectiveness of measures to neutralize threats to information security can be carried out with a thorough and in-depth knowledge of its functioning, which necessitates the use of mathematical modeling methods. The practical task of ensuring information security is to develop a model for representing the information security system, which would solve the tasks of creating, using and evaluating the effectiveness of ISS for both projected and existing systems.

2. Analysis of recent research and publications

The accumulation of large amounts of information leads to an increase in the likelihood of leakage of information of limited access, and hence to the need to take measures to ensure the security of information. Unfortunately, improved means and methods of unauthorized access to information, it`s distortion, destruction or substitution are developed by hackers. Therefore, problems how to ensure the safety of information processed, security issues in data transmission channels as well as in multiservice networks are added [1, 2]. In this regard, there is a need for continuous improvement of ways and means to ensure information security [3, 4, 5, 6]. In the specified organizations the objects of protection are [7]:

- Information processed and contained in information systems

- Technical means (including computer facilities, computer storage media, communication and data transmission systems and means, technical means for processing alphanumeric, graphic, video and voice information)
- System-wide, applied, special software
- Information technology, as well as information security.

3. Problem definition

As a mathematical scheme for describing the dynamics of the information security system, we adopt a discrete method of representing the processes of ensuring information security. Under the process of ensuring information security, we mean a set of sequential actions aimed at achieving the required protection of information and the information structure of the organization from current threats of information security. The representation of ISS functioning as a finite discrete process corresponds to its content and greatly facilitates its mathematical description.

In general, the elements of the internal state of the information security system are the management bodies *R*, organizational and administrative documents *D*, as well as information security means *Z*. Information security means include technologies, physical, technical, software, cryptographic, legal, organizational means, as well as means for collecting, forming, processing, transmitting or receiving information on the state of information security of an organization and measures to improve it.

Under the internal state of the elements of the information security system, we mean the vectors S^R, S^D, S^Z, defined on the range of possible values of the parameters for the description of the elements *R, D* and *Z*, respectively. Then the matrix of the internal state of the elements of the ISS will be determined by the vector $S = (S^R, S^D, S^Z)$.

In turn, the state of the information security system depends on [8]:

- A number of threats to information security relevant for the organization $W = \{W^A, W^T\}$, where W^A, W^T - the anthropogenic and man-caused threats to information security
- The set of requirements for the information security system $P = \{P^R, P^D, P^Z\}$, where P^R, P^D, P^Z are the sets of requirements for the state of the elements *R, D and Z* of the system *S*, respectively
- The set of control actions on the elements of the information security system $U = \{U^l\}$, where U^l is the value of the control parameter that determines the functioning of the ISS element - *l-th*.

Variables *S, W, P* form the multidimensional space of the state of the information security system. The point $G = (S, W, P)$ in this space is called the state of the information security system. Then the process of functioning ISS can be represented through a change in the time of its state: $G = (S, W, P)$.

To describe the dynamics of the state of the information security system, we adopt a discrete method of representing the processes of ensuring information security. Such a representation of the functioning of ISS, as a rule, corresponds to its content and especially the periodicity of the control (audit), and also makes it possible to simplify its mathematical description. Description of the processes of ISS functioning by

a discrete mathematical scheme is a time sequence of states of the system, determined by the position of the point *G* in the multidimensional space of parameters of its state. Taking into account the above, the expression describing the motion of point *G* in time has the following form:

$$\begin{aligned} &G(0), F_1:\{G(0)\} \rightarrow G(1), F_2:\{G(1)\} \rightarrow G(2),.., \\ &F_n:\{G(n-1)\} \rightarrow G(n),.., F_N:\{G(N-1)\} \rightarrow G(N) \end{aligned} \quad (1)$$

To simplify the further analysis, we assume that the operators of the transformation *Fn* do not depend on time, but depend on the *n*-th step number of the process of functioning of the system.

Assume that $F: \{G(n)\}, \forall n \in 1..N$ is the ISS process, where n is the step number of the process, and *N* is the number of steps that determine the considered duration of the system's operation. A change in the SOIB status is a control function $G(n) = G_U(U(n))$. At any *n-th* step of the process, the behavior of the information security system is determined by the control vector $U = (U_1)$.

The change in the state of ISS is determined by the change in the model of threats to information security, the functioning of its elements and their interaction in the process of this functioning in accordance with the control impacts that are generated by the ISMS. During operation, the elements of the information security system change their internal state; therefore, for a discrete description of the process of changing the state of the ISS *G (n)*, it is necessary to determine the sequence of changes in state components at each *n*-th step of the process of its functioning.

In view of the content of the processes of ISS operation, the sequence of state changes *G(n)* can be represented as follows: At *(n + 1)* step, the information security threats *W(n + 1)* change, which causes a change in the requirements for the information security system *P(n + 1)*? With the appearance of new requirements, an assessment is made of the conformity of the ISS state to the requirements and the control actions *U(n + 1)* are developed to change the internal state of the information security system $S = (S^R, S^D, S^Z)$ systems in order to neutralize new information security threats. Thus, the internal state vector *S(n + 1)* is formed at the *(n + 1)*-th step of the process of its functioning.

We represent the process $F: \{G(n)\} \rightarrow G(n+1)$ of the state and control of the system at the *(n + 1)*-th step by the following system of operators:

$$\begin{aligned} &M_1:\{W(n), P(n), U(n), S(n)\} \rightarrow W(n+1); \\ &M_2:\{W(n+1), P(n), U(n), S(n)\} \rightarrow P(n+1); \\ &M_3:\{W(n+1), P(n+1), U(n), S(n)\} \rightarrow U(n+1); \\ &M_4:\{W(n+1), P(n+1), U(n+1), S(n)\} \rightarrow S(n+1). \end{aligned} \quad (2)$$

The transformation operator *F* is a sequence of operators *M1, M2, M3, M4.*

The next step in the formalization of information security processes is the description of the control actions $U = (U_1)$, generated by the information security management system.

The activity of the information security service in the general case is the following sequence of actions:

- Collection of information on the state of the information security system
- Assessment of the state of the information security system
- Development of a plan for the organization's activities to improve ISS
- Development of control actions.

To implement the activities of the information security service, the actual state of the system *G* needs to be translated into its information image G^f:

$$M_5 :\{G\} \rightarrow G^f \tag{3}$$

where $G^f = \{W^f, P^f, S^f\}$.

Therefore, there must be some mapping operator M_6, designed to generate an information image about the actual state of the G^I information security system at the time $n = 0$:

$$M_6 :\{G^f, Q\} \rightarrow G^I \tag{4}$$

where Q is the set of quality indicators of the system, $Q = \{Q^R, Q^D, Q^Z\}$, Q^R, Q^D, Q^Z are the sets of quality indicators for the elements *R, D and Z* of the system S, respectively.

The set G^I represents the state of the information security system, from which a decision is made to change the system $S = (S^R, S^D, S^Z)$. The M_6 operator is of great importance in the activity of the information security service, since the completeness of the mapping of the state of ISS G_p^f depends on the quality of its implementation:

$$M_6 :\{G_p^f, Q\} \rightarrow G^I \equiv G \tag{5}$$

The most important stage that influences the quality of the decision is the evaluation of the actual state of the ISS [9, 10]. The assessment of the state of the O^S system includes: parameters of the elements of the information security system *S*; list of actual threats to information security *W* and possible damage $Y = \{Y_i\}$ from their implementation; the state of information infrastructure S^I. $S^I = \{S_1^I\}$, where S_1^I - parameters of information systems that process information in the organization; requirements for ISS, $P = \{P^R, P^D, P^Z\}$. An assessment of the state of the information security system can be represented by an operator of the form:

$$M_7 :\{W, Y, S^I, P, Q, S\} \rightarrow O^S \tag{6}$$

Then the process of obtaining the information image and evaluating the state of the system is determined by the sequence of the following operators:

$$\begin{aligned} &M_6 :\{G^f, Q\} \rightarrow G^I \\ &M_6 :\{G^f, Q\} \rightarrow G^I \\ &M_7 :\{W, Y, S^I, P, Q, S\} \rightarrow O^S \end{aligned} \tag{7}$$

To create an information image and assess the state of the information security system in organizations, an information security audit is carried out aimed at identifying inconsistencies in the system with the requirements, developing solutions for

eliminating existing contradictions, and developing a plan for implementing decisions.

The considered properties of ISMS and the assumptions made allow us to proceed to the formalization of management in the information security system. The process of functioning of the information security management system at the step *(n + 1)* can be represented by the following mapping:

$$F:\{G(n), U(n)\} \rightarrow G(n+1) \tag{8}$$

where $G(n) = (W(n), P(n), U(n), S(n))$ is the state vector of the information security system at the *n*-th step of its operation.

Management ISS is a purposeful activity. Objectives *C* (ensuring the integrity, accessibility and confidentiality of information), which are set for a certain period of operation of the information security system *n**, that is, *C(n*)*. The goal is considered achieved if $G(n) \rightarrow C(n^*)$. Control actions contain constraints that determine the parameters of the *G*(n)* system for the period when the tasks are performed (for example, restrictions on the allocation of material and financial resources), as well as restrictions on the management of *U*(n)* (the sequence of the solution, the tasks assigned, the expenditure of material and financial resources over time). In view of the above, the control effect can be represented by a mapping of the form:

$$U = \{C(n^*), G^*(n), U^*(n)\} \tag{9}$$

The decision-making process can be presented as the formation of a general action plan for M_8, the sequence of procedures in time and space, as a result of which the goal *C*, assigned to the information security system (neutralization of information security threats), is achieved, and the state of the elements of the ISS is aligned with requirements in the field of information security $S^B = \{S_b^r, S_b^d, S_b^z\}$:

$$\begin{aligned}
&M_1 :\{W(n), P(n), U(n), S(n)\} \rightarrow W(n+1),\\
&M_2 :\{W(n+1), P(n), U(n), S(n)\} \rightarrow P(n+1),\\
&M_3 :\{W(n+1), P(n+1), U(n), S(n)\} \rightarrow U(n+1),\\
&M_4 :\{W(n+1), P(n+1), U(n+1), S(n)\} \rightarrow S(n+1),\\
&G(n+1) = \{W(n+1), P(n+1), S(n+1)\},\\
&M_5 :\{G(n+1), U(n)\} \rightarrow G^f(n+1),\\
&M_6 :\{G^f(n+1), U(n)\} \rightarrow G^I(n+1),\\
&M_7 :\{W(n+1), Y(n+1), S^I(n+1), P(n+1), S(n+1), O^S(n)\} \rightarrow O^S(n+1),\\
&M_8 :\{G^I(n+1), O^S(n+1), U(n), C(n), S^T(n)\} \rightarrow C(n+1),\\
&M_9 :\{G^I(n+1), O^S(n+1), U(n), C(n+1), S^T(n)\} \rightarrow U(n+1),\\
&M_{10} :\{C(n+1), O^S(n+1), U(n+1), S^T(n)\} \rightarrow S^T(n+1)
\end{aligned} \tag{10}$$

where M_{10} is the operator of alignment of ISS elements in accordance with the requirements of regulatory legal acts and regulatory documents in the field of information security.

As can be seen from the above operators, the control actions are aimed at bringing ISS into compliance with the requirements for it $S^{T}(n+1)$. The most important stage determining the effectiveness of the solution is the assessment of the compliance of the M_7 information security system with the requirements.

Let us formulate the formulation of the problem of the realization of the operator for the formation of control actions, taking into account the provisions set forth in [12]. Let the information security risks *W(n+1)* change at the step *(n + 1)* of the ISS operation, which leads to a change in the requirements $P = \{P^{R}, P^{D}, P^{Z}\}$. As a result of estimating the state of M7, deviations of the individual indicators of the state of the elements of the ISS are recorded: $S = \{S^{R}, S^{D}, S^{Z}\}$, from the required values: $P = \{P^{R}, P^{D}, P^{Z}\}$. The reasons for the deviation as a result of changes in information security threats *W(n+1)* are known, and the means to achieve the required values are not determined in advance. Such a state in the management of information security is further understood as the standard situation in ensuring information security. The state estimation is carried out taking into account the system of ISS quality indicators: $Q = \{Q^{R}, Q^{D}, Q^{Z}\}$, $Q = QR \cup QD \cup QZ$, $Q = \{qi\}$, where q_i is the unit quality index from the set Q, where $i = \overline{1, N}$, N is the number of unit indices.

The values of require q_i:

- Evaluate the current situation $S = \{S^{R}, S^{D}, S^{Z}\}$ (S_{Cr} - critical, S_{NS} - not-satisfactory, S_N - normal)
- Find the root causes of g_x, which caused the occurrence of S
- To offer alternative solutions $\{r_i\}$
- Choose and justify the optimal (rational) solution R_j.

The goal of the solution is to return ISS to the state of normal functioning, i.e., meeting the requirements: $S^{t} = \{S_t^{r}, S_t^{d}, S_t^{z}\}$. In this case, two cases may arise.

The first case, when as a result of changing threats to information security, the W system is in a critical situation. Depending on the existing restrictions on G^* and U^*, it can be transferred immediately to the state of normal functioning of S_N or first to the state of unsatisfactory functioning of S_{NS}, and then to the state S_N:

$$\psi(Q): S_{cr} \rightarrow S_n \cup S_{ns} \rightarrow S_n, S_n \equiv S^{T} \tag{11}$$

The second case, when as a result of changing threats to information security, the W system is in a state of unsatisfactory functioning of the S_{ns}. Then, regardless of the existing constraints, the system must be transferred to state S_N:

$$\psi(Q): S_{ns} \rightarrow S_n, S_n \equiv S^{T} \tag{12}$$

The control formula can be simplified by the following expression:

$$\psi(Q) \subset I(Q), O^{S}(S), L(g_x), M(R_j) \tag{13}$$

where *I(Q)* is the measurement of the vector Q; $O^{S}(S)$ - assessment of the situation; $L(g_x)$ - search for indicators of primary causes that gave deviation from the required values; $M(R_j)$ is the search for the class of solutions R_j. This operation is repeated successively to refine the class R_j and exit to the operation R_o.

The results of solving the problem can be represented in the form of a diagram, shown in Fig. 1, which gives an example of assessing the state of protection of PD - personal data, CS - commercial secrets, SIIA - service information and an integrated assessment of the information security state of the organization.
Thus, the proposed method of formal description of information security systems contributes to the creation of clear organizational mechanisms for managing information security of the organization. The considered formal models allow revealing the interdependence and mutual influence of various factors affecting the system of providing information security of the organization, and serve as a methodological basis for the development of specific methods. The process of developing a formal scheme allows for structuring and clearly formulating the essence of the task of assessing the state of the information security system. The practical implementation of the proposed model will increase the efficiency of the information security system at the stages of its creation, functioning and further development.

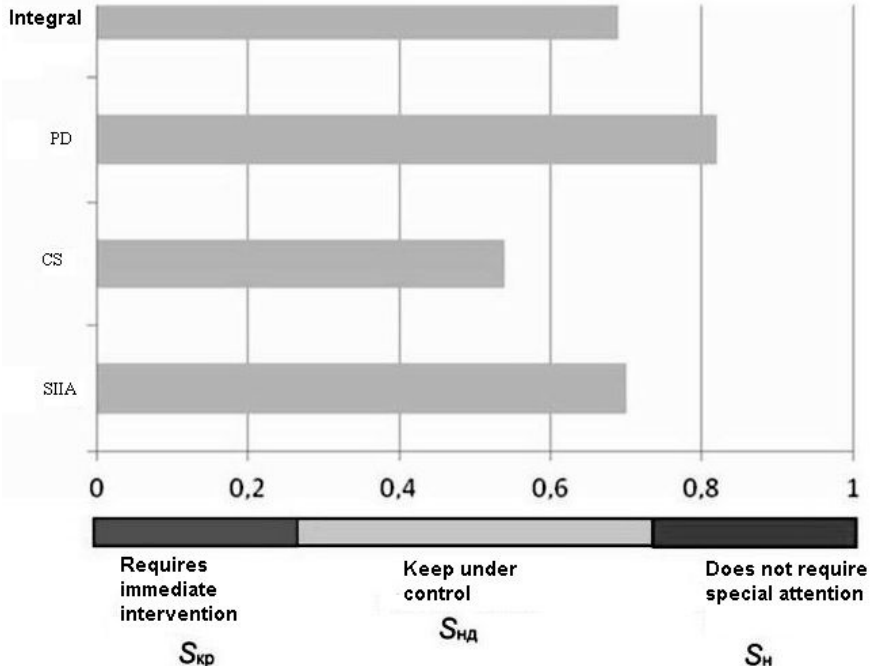

Figure 1. Diagram of assessing the state of protection of personal data, trade secrets and official information

But for any system of information security are important methods and means of protecting information. Next, we will consider the basic principles of the functioning of the hybrid cryptographic system.

4. Statement of the main material

For encryption of open text a special algorithm is used, the secrecy of the transformation of information is achieved through the use of a unique algorithm

or key that provides each time original encryption of information. However, with the development of cryptography, the basic principle of modern encryption systems was the Kerckhoff rule, according to which the popularity of the opponent of the algorithm of transformation should not reduce the reliability of the encryption system, and its crypto stability is determined only by the secrecy and quality of the used cryptographic keys. Thus, without the knowledge of the secret key decryption should be practically impossible, even under a known encryption algorithm [11].

Symmetric cryptosystems can be implemented on a variety of secret key encryption algorithms that can be split into block and threaded ones. As a rule, modern symmetric cryptosystems are represented by such well-known standard as DES and Rijndael (USA), which is a block cipher.

In practice, hybrid cryptosystems are effectively used, combining elements of symmetric and asymmetric cryptosystems and, accordingly, inherent in their properties: for symmetric methods of encryption - high speed and short cryptographic keys, for asymmetric - the possibility of an open and secure distribution of encryption keys [12].

In the hybrid cryptosystem, public key encryption is used to encrypt, transmit and further decrypt only the secret key of symmetric encryption, which is directly used to encrypt transmitted messages . Thus, the asymmetric cryptosystem harmoniously complements the symmetric cryptosystem, providing a simple and secure transmission of secret key encryption. The basic algorithm for the functioning of the hybrid cryptosystem is shown in Fig. 2.

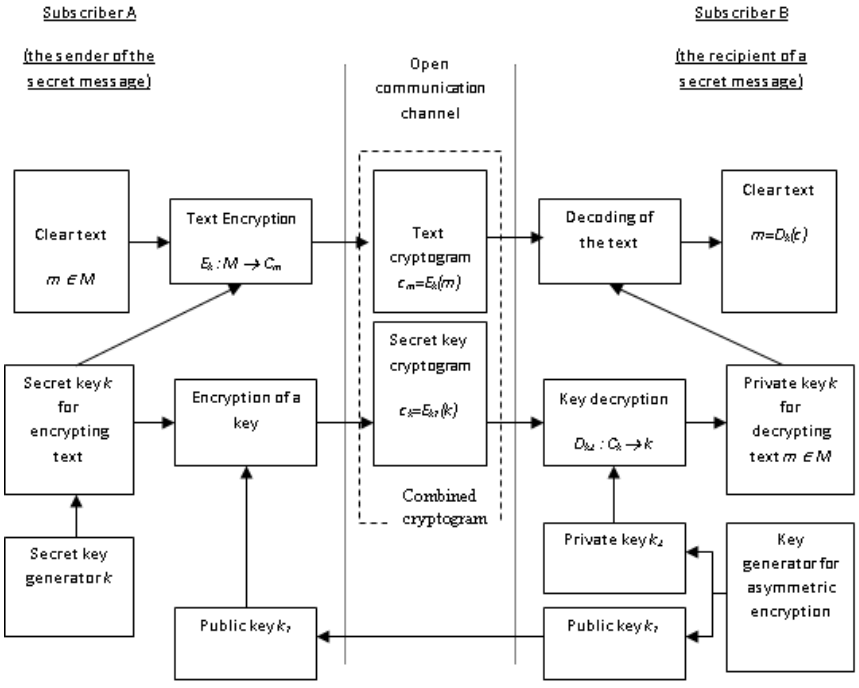

Figure 2. Basic algorithm for the functioning of the hybrid-cryptographic information security system

The secret communication protocol (transmission of a secret message) between subscriber *A* (sender) and subscriber *B* (receiver) may be as follows:

1. Subscriber *B* generates open (k_1) and closed (k_2) keys for asymmetric encryption, and transmits the public key k_1 to an open (accessible, unprotected) communication channel of subscriber *A*.
2. Subscriber *A* generates a session-secret cryptographic key for symmetric encryption and encrypts for it the secret message (open text) *m* to be transmitted.
3. Subscriber *A* encrypts the session secret cryptographic key on the public key k_1.
4. Subscriber *A* transmits an open communication channel to the user's address in an encrypted message (encrypted message) cryptogram with a cryptogram of the secret cryptographic key k used to encrypt this message.
5. Subscriber *B* decrypts the closed secret key k_2 session secret cryptographic key, which decrypts the cryptogram of the message *m*.

To increase cryptographic stability in the hybrid cryptographic system, each secret link session (encryption of a new message) generates its own secret key for symmetric encryption called sessional.

The choice of the size of cryptographic keys for symmetric and asymmetric encryption is carried out in such a way that their potential cryptantability to the attack by the method of full overview of possible options was comparable.

If the open and closed asymmetric encryption keys are used repeatedly (for a long time), then their cryptographic stability should be substantially higher than that of the session secret key of symmetric encryption, since when they are disclosed (discredited), the opponent will have the opportunity to decrypt the secret keys transmitted to the session and, accordingly, , encrypted messages on them.

In table 1 shows the lengths of the keys of symmetric cryptosystems that have difficulty disclosing by the method of full-fledging, which can be compared with the difficulty of factorizing the corresponding modules of asymmetric cryptosystems.

Table 1. The lengths of the keys of symmetric cryptosystems

Key length symmetric cryptosystem, bit	Module of an asymmetric cryptosystem, bit
56	384
64	512
80	768
112	1792
128	2304
192	5184
256	9216

Most hybrid systems work this way. For a symmetric algorithm (3DES, IDEA, AES, or any other), an occasional session key is generated. This key usually has a size from 128 to 512 bits (depending on the algorithm). Then a symmetric algorithm is used to encrypt the message. In the case of block encryption, you must use an encryption mode, which will allow you to encrypt messages with lengths that exceed the length of the block. Regarding the most accidental key, it should be encrypted using the

public key of the recipient of the message, and it is at this stage that an open-source cryptosystem is used (RSA or Diffie-Hellman algorithm). Because the session key is short, its encryption takes a bit of time. Encrypting a message set using an asymmetric algorithm is a computationally more complex task, so it is preferable to use symmetric encryption here. Then it's enough to send a message encrypted by a symmetric algorithm, as well as a corresponding key in an encrypted form. The recipient first decrypts the key using his secret key, and then, with the help of the received key, receives all messages.

5. Conclusions

The proposed model allows estimating or overestimating the level of the current state of information security of an enterprise, developing recommendations for providing (enhancing) information security of an enterprise, reducing potential losses of an enterprise or organization by increasing the sustainability of the corporate network, developing the concept and policy of enterprise security, and proposing plans for the protection of confidential information of the enterprise, transmitted through open communication channels, protection of information of the enterprise from intentional destruction, unauthorized access to it, its copying or use.

REFERENCES

1. MIKHAILOV S., Yu. LOSKUTOV A.: Foundations of Synergetics II. Chaos and Noise, 2nd revised and enlarged edition, Springer Series in Synergetics. Berlin — Heidelberg : Springer, 1996.
2. PETROV A. A., KARPINSKI M., PETROV O. S.: Development of methodological basis of management of information protection in the segment of corporate information systems, SGEM 2018: 18th International Multidisciplinary Scientific Geoconference : Informatics. Informatics, go informatics and remote sensing. Issue 2.1 : conference proceedings, 18(2018)2.1, STEF92 Technology, 317-324, ISSN: 1314-2704; ISBN: 978-619-7408-39-3.
   DOI: 10.5593/sgem2018/2.10000019097.
3. SCHNEIER B.: Applied Cryptography: Protocols, Algorithms and Source Code in C. John Wiley & Sons, Inc., 1994.
4. BABENKO L.K., ISHCHUKOVA E.A., MARO E.A.: Research about Strength of GOST 28147-89 Encryption Algorithm // Proceedings of the 5th international conference on Security of information and networks (SIN 2012), ACM, New York, NY, USA, 80-84.
5. COURTOIS N., KLIMOV A., PATARIN J., SHAMIR A.: Efficient algorithms for solving overdefined systems of multivariate polynomial equations, EUROCRYPT, 2000, 392–407.
6. COURTOIS N.: How Fast can be Algebraic Attacks on Block Ciphers, Nicolas T. Courtois Cryptology ePrint Archive, Report 2006/168, 2006.
7. COURTOIS N., Security Evaluation of GOST 28147-89 In View Of International Standardisation, http://eprint.iacr.org/2011/211.

8. KLEIMAN E.: The XL and XSL attacks on Baby Rijndael. http://orion.math.iastate.edu/dept/thesisarchive/MS/EKleimanMSSS05.pdf
9. RIVEST R.L., SHAMIR A., ADLEMAN L.: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. CACM, 21(1978)2, 120-126.
10. SAARINEN M.J.: A chosen key attack against the secret S-boxes of GOST. http://citeseer.ist.psu.edu – August 12, 1998.
11. BETH Th., FRISCH M., SIMMONS G.J. (eds.): Public-Key Cryptography: State of the Art and Future Directions. E.I.S.S. Workshop - Oberwolfach, Germany, July 1991 - Final Report. Lecture Notes in Computer Science, V.578.
12. DIFFIE W., HELLMAN M.: New Directions in Cryptography. IEEE Trans. Inform. Theory, IT-22, 6(1976), 644-654.