

Management of Security Risks of Information Resources in Information and Telecommunication Systems Using Expert Procedures

Petro Snitsarenko ¹, Yuriy Sarychev ¹, Andrii Fesenko ², Viktor Zubkov ¹ and Yuriy Pishchanskyi ¹

¹ National Defence University of Ukraine named after Ivan Cherniakhovskiy, Povitroflotskyi Av., 28, Kyiv, 03186, Ukraine

² Taras Shevchenko National University of Kyiv, Volodymyrska St., 60/13, Kyiv, 02000, Ukraine

Abstract

The article considers the problem of the security of electronic information resources in information and telecommunication systems as a component of cyber security. The main aspects, essence and characteristics of security risks of electronic information resources are highlighted. The option of creating a system for managing such risks is proposed. The solution is based on the cybernetic model of system functioning and the use of expert procedures.

Keywords

Management of security risks of electronic information resources, information and telecommunication systems, expert procedures.

1. Introduction

The factors influencing the external and internal security environment, the existing state of ensuring information sovereignty and information security of Ukraine require the state, with the active support of society, to implement a comprehensive set of measures to respond to information threats, particularly in cyberspace as an integral component of the national information space. At the same time, the simplest understanding of cyberspace is that it is an environment of information resources in electronic form (that is, electronic information resources - EIR), which is artificially formed as a result of functioning on the basis of uniform principles and general rules of information and telecommunication systems (ITS). Depending on the scale of the ITS network and the way it is organized, cyberspace can be considered global, local, and virtual.

Today, regardless of its scale, consumers make certain demands regarding their main properties: reliability, availability, completeness (sufficiency), integrity, confidentiality. Violation of such requirements can pose a threat to cyber security, in general, information security of the consumer and the state, which actually leads to significant damage in various spheres of life. Therefore, it is a problem of EIR security in ITS as a component of cyber security provision, which becomes extremely relevant in the general system of its provision. At the same time, EIR security means the state of their security in ITS, when in relation to them, the ability to commit unauthorized actions is made impossible or reduced [1].

One of the restraining factors in complying with the specified requirements and ensuring EIR security, and therefore cyber security in general, is the presence of accompanying EIR security risks, which require their identification, assessment and neutralization or reduction to an acceptable level.

2. Literature review and problem statement

The analysis of publications shows that most researchers understand risk as a quantitative measure of security or a scale that can be used to quantify the losses associated with the realization of threats that have various sources of origin. With the help of such a scale, it is possible to compare all types of threats (risks) with


Information Technology and Implementation (IT&I-2022), November 30 - December 02, 2022, Kyiv, Ukraine

EMAIL: snits1954@gmail.com (P. Snitsarenko), y.sarych@gmail.com (Y. Sarychev), aafesenko88@gmail.com (A. Fesenko), vpzubkov@ukrnet, (V. Zubkov), feliksrazumkov@gmail.com (Y. Pishchanskyi)

ORCID: 0000-0002-6525-7064 (P. Snitsarenko); 0000-0003-1380-4959 (Y. Sarychev), 0000-0001-5154-5324 (A. Fesenko); 0000-0003-1616-2795 (V. Zubkov); 0000-0003-4392-3318 (Y. Pishchanskyi)



© 2022 Copyright for this paper by its authors.
Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

 CEUR Workshop Proceedings (CEUR-WS.org)

each other and accordingly determine the level of security - the degree of protection [2-6]. In general, risk is understood as the predicted amount of loss that may arise as a result of decision-making in conditions of uncertainty and the realization of a threat [7, 8]. Risk management is considered as a rational measure to reduce the amount of such damage.

Researchers, analyzing modern threats to information security, including information security in cyberspace, that is, the security of EIR, identified the following causes of global risks: negative consequences of technological progress; increasing vulnerability in the use of information infrastructure and networks; cyber-attacks or malicious software; massive cases of fraud using disinformation, data theft, etc. [9]. At the same time, such a threat is understood as intentions, actions (inaction) or phenomena and factors, the manifestation of which can harm the available information (information resources).

The problems of the emergence of threats and risks in various fields, including in the field of information security (including cyber security), are also developed in the works of domestic information security researchers (V.P. Horbulin, A.B. Kachynskyi, A.I. Semenchenko, G. P. Sytnyk, O. M. Zagorka, P. M. Snitsarenko and others). They emphasize the need and relevance of a systematic approach to information protection, risk reduction to ensure the validity and consistency of measures planned for this purpose, and ensure their implementation as effectively as possible. At the same time, scientists have not yet developed a unified approach to EIR security risks management, in particular in the military sphere. Therefore, the search for the most rational solutions continues.

3. Formulation of the problem

Currently, the methodology of risk management is based on the choice of a mathematical model of risk assessment, which depends on each specific threat. As a result, there is a significant number of both the models themselves and approaches to modeling risk assessments [7]. Currently, additive-multiplicative models are used to formalize risk. They link the probability of occurrence of events (threats) and their corresponding undesirable consequences, which is discussed, in particular, in works [7, 8]. These models are complex, bulky, require appropriate personnel training, and are inconvenient for operational use. Due to the presence of many unpredictable, random, subjective circumstances, significant deviations from the expected result occur.

The purpose of the publication is the formation of a methodical approach to the management of EIR security risks in information systems as an integral component of the process of ensuring state cyber security.

4. The main section

In modern conditions, almost all areas of the state's vital activity can be under threat of EIR security risks (examples are repeated cyber-attacks on the information systems of state and private institutions of Ukraine), which directly affects the level of EIR security and causes the corresponding risk.

It can be argued that the risk of EIR security should be considered the predicted amount of information loss that may occur as a result of threats to EIR security due to unauthorized actions (access, changes, removal, destruction). Taking into account EIR security risks (in other words, managing such risks) will ensure the improvement of the procedure for supporting the management decision-making process, will allow to improve the quality of the implementation of practical measures.

In work [8] it is stated that any EIR security risk can be caused by a combination of the following negative factors: the presence and nature of the EIR security threat source, the uncertainty of the occurrence of a dangerous event, the uncertainty of the impact mechanism, the possibility and level of damage. The entire set of EIR security risks can be conditionally divided based on the characteristics of their certain factors. Factors associated with EIR security risk are various influences on the main characteristics of information [10] - these are reliability, sufficiency (completeness), integrity, availability, confidentiality. The risk of violation of *the reliability* is characterized by its ability to correspond to true (error-free) data.

Sufficiency (completeness) is the minimal, but sufficient composition of the information product for making a decision. The risk of EIR sufficiency violation is related to the amount of information sufficient for the user (consumer) to understand and make an informed decision.

Integrity is the ability of EIR to maintain its accuracy and completeness under the conditions of use. The risk of violation of the integrity of information is characterized by the possibility of failure of equipment or software, the imperfection of algorithms and the degree of reliability of the means of user access to the information system.

Availability is the subject's ability to access data upon request at any time (the ability to use EIR when necessary). The risk of violating the availability of information depends both on hardware malfunctions and software failures, and on successfully implemented network attacks on the information system from the outside. This type of risk depends on the reliability of the hardware and software components of the information system, as well as on the level of competence of the personnel managing their work.

Confidentiality is the level of EIR protection against unauthorized access. The risk of breach of confidentiality depends on the level of user authentication algorithms, the probability of undocumented situations when working with the information system, the imperfection of the organizational structure, non-compliance with the guiding documents on information protection and the human factor.

The sources of influence on information characteristics are the EIR security risk environment and the state of information systems [10]. According to the environment of occurrence, such risks are divided into external and internal. The external risks of EIR security risk include risks caused by the political situation around the country, relations between states, the economic situation on the market, the social condition of citizens, etc. The level of such risks is determined by several components that affect its overall value.

The internal risks of EIR security risk include risks that depend on the direct activity of the structural unit (organization) and its personnel. Among them, organizational risks are decisive - these are risks associated with the activities of personnel who operate and maintain information systems, problems of the internal control system, vaguely defined work rules, i.e. risks associated with the internal organization of the work of a structural unit (organization). According to the state of information systems (ITS), which should be understood as the level of performance of their components, EIR security risks are divided into hardware and software. Hardware risks arise when information system equipment fails (personal computers, servers, measuring devices (sensors), network switches, routers, etc.), and they also depend on the methods of its operation. Software risks are directly related to violations in the operation of the software (operating systems) of the information system, the actions of malicious software, as well as the actions of network attacks.

All types of risks, as a rule, can be the object of management, the best - adaptive management. So, we are talking about a certain cybernetic system of EIR security risk management, which should include a management body, an executive body, and a monitoring body (Figure 1). The object of management in such a system is precisely the level of EIR security risk. According to the main provisions of management theory [11], this methodical approach allows for the most effective (adaptive) management of EIR security risks as a component of cyber security.

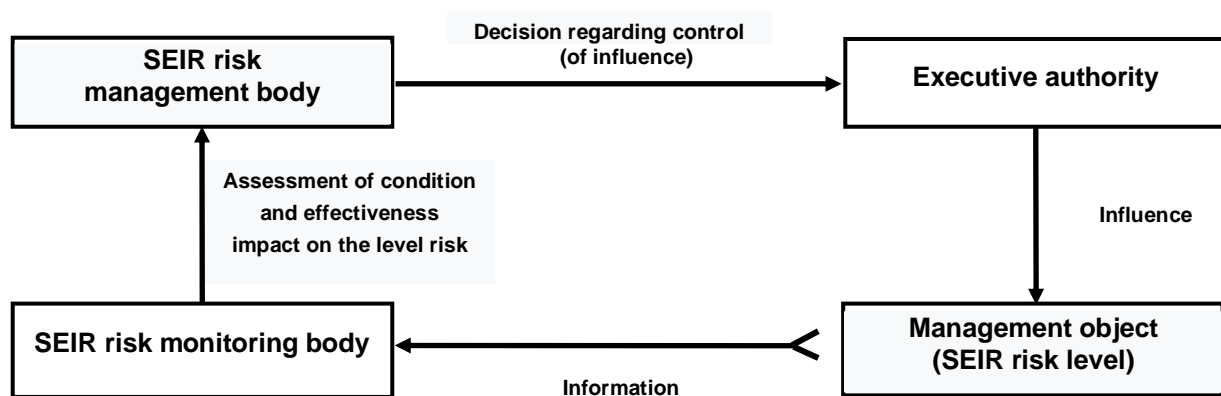


Figure 1: Cybernetic model of EIR security risk management system functioning

To manage the security risk of EIR, according to management theory [5, 11], means:

- monitor (identify, assess sources of risk);
- carry out risk analysis and assessment;
- predict scenarios of the development of dangerous events;
- make decisions based on the results of risk analysis;
- implement measures to prevent, localize, neutralize or reduce the level of risks to an acceptable level;
- eliminate the consequences of dangerous events.

The variant of the structural diagram of the implementation of such a cybernetic process related to the management of EIR security risks consists of 4 stages (Figure 2).

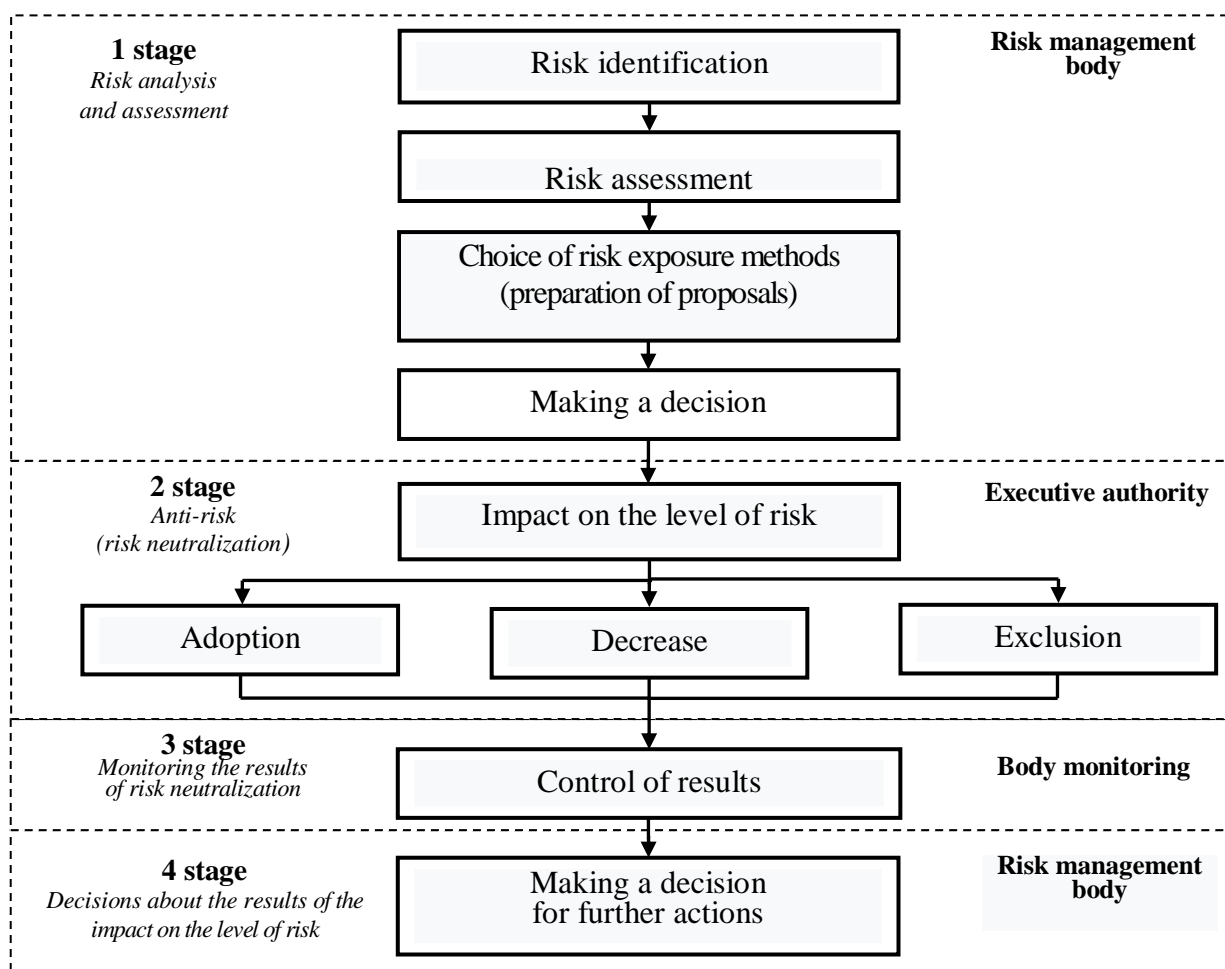


Figure 2: Structural diagram of the EIR security risk management process (option)

The sequence of implementation of the EIR security risk management process is the following.

The 1st stage of the EIR security management process is the most complex formation of a logical sequence of individual partial functions, when the management body, based on the detection, analysis and assessment of the predicted amount of information loss that may occur as a result of the implementation of EIR threats, draws a conclusion on the need for countermeasures, selects methods and measures to influence EIR security risk (preparation of proposals) and makes a decision regarding the need to organize countermeasures. Let's reveal the essence of the elements of this stage.

Identification of sources of EIR security threats and possible EIR security risks. When identifying and identifying the sources of threats to EIR security (who or what is the cause), the object of influence (on which the EIR security threat can act) and the initial analysis of the EIR security risk, it is necessary to assess the possibility of realizing such a threat. At the same time, you should take into account:

- the frequency of occurrence of the EIR security threat (how often it may occur according to statistical, research and other data, if any);
- the motivation, capabilities and informational resources needed by the potential infringer and which may be at his disposal;
- the degree of attractiveness and vulnerability of information assets from the point of view of a potential violator and a source of intentional EIR security threat;
- uncontrollable phenomena (natural disaster, epidemic) that can affect the state and quality of information resources.

The analysis and consideration of these factors is carried out using an expert method by specialists who have knowledge of the tasks, principles and conditions of specific ITS operation.

Upon completion of this process, the experts draw up a register of sources of threats to the security of the EIR, which is used in the risk management system to determine further countermeasures, and the possibility of their implementation is assessed. At the same time, a list of possible internal vulnerabilities (regarding leakage, disclosure, distortion or loss of information) is also taken into account, in particular:

- unprotected connections of the information system to the Internet, local networks;

- insufficiently qualified staff;
- imperfect organization of access (proper access control) of users to equipment and information resources;
- lack of backup copies of data (information) or software;
- failure of elements of the information system, etc.

The EIR security risk assessment is carried out by the risk management body in order to choose justified methods of neutralizing relevant threats (negative impact) and ensuring EIR security in the interests of the functioning of a certain management system, which is based on the use of EIR of the relevant ITS. The determination of the level (value) of the assessment should be carried out taking into account the experience of the staff, the requirements of regulatory documents, the history of previous cases of EIR security violations, the experience of other structural units (organizations), etc. The assessment is carried out for all types of EIR security risks and is documented in the form of a table for each partial characteristic of information.

For the risk assessment method, according to the State Standard [12], it is advisable to choose the matrix of consequences due to its advantages (it is relatively easy to use and allows you to quickly rank risks according to different levels of importance). To build the matrix itself, it is necessary to form quantitative ranking scales. By analogy with [13], quality scales are proposed for assessing the level of the possibility of EIR security threats (Table 1) and the levels of their impact, subject to implementation, on individual properties (characteristics) of information (Table 2 – 6). Such assessments of levels on a 5-point scale are preliminarily determined by experts, based on information about the threat factor, causes, mechanisms and measures to prevent (reduce) the risk of EIR security.

Table 1

Ranking scale for assessing the possibility of EIR security threats

The level (rank) of the possibility of threats to the security of the EIR	Content
1	Very low (extremely unlikely)
2	Low (unlikely, no more than once a month)
3	Medium (possible up to 1 time a week)
4	High (quite possible, up to 1 time per day)
5	Extremely high (very possible, more than 1 time per day)

Table 2

Ranking scale of the consequences of the implementation of EIR security threats (impact) on the reliability of information

Level of exposure	Content of the effects of exposure
1 (minimal)	The level of information reliability is high, the management process is satisfactory
2 (insignificant)	The level of information reliability is sufficient, but may have an insignificant negative impact on the result of the management process
3 (medium)	The level of reliability of the information is medium, which can have a noticeable negative impact on the result of the management process
4 (significant)	The level of information reliability is low, which can have a significant negative impact on the result of the management process
5 (maximum)	The level of reliability of the information is very low, which leads to the stopping of the management process

The received data of the assessment of the qualitative values of the levels of the possibility of EIR security threats and their impact on individual properties of information (ranking scales: Tables 1 - 6) are the basis for forming a matrix of consequences (estimates of the levels of EIR security risks) for each of its properties. Based on [12], using the above 5-rank scale, a numerical risk assessment matrix is formed by multiplying the numerical values of the corresponding rows and columns (ranks), which gives a conditional numerical value of the level of risk of EIR security for each property of information in the range of numbers from 1 to 25, that is, from the lowest level of risk to the highest. Due to the quantitative values of the matrix, it is possible to qualitatively assess the level of risk of EIR security, in particular, based on the application of the generalized Harrington desirability function [14, 15]. Harrington's desirability scale is a universal verbal-numerical scale (Table 7), which is used mainly in cases where assessments are subjective in nature.

Table 3

Ranking scale of the consequences of the implementation of EIR security threats (impact) for completeness of information

Level of exposure	Content of the effects of exposure
1 (minimal)	The level of completeness of information is high, the management process is satisfactory
2 (insignificant)	The level of completeness of information is sufficient, but to a small extent it can negatively affect the result of the management process
3 (medium)	The level of completeness of information is average, which to a certain extent can negatively affect the result of the management process
4 (significant)	The level of completeness of information is low, which can significantly affect the result of the management process
5 (maximum)	The level of completeness of information is very low, which does not satisfy the performance of the management process and leads to its stop

Table 4

Ranking scale of the consequences of the implementation of EIR security threats (impact) on the integrity of information

Level of exposure	Content of the effects of exposure
1 (minimal)	The level of information integrity is high, the management process is satisfactory
2 (insignificant)	The level of integrity of information is sufficient, but to a small extent it can negatively affect the result of the management process
3 (medium)	The level of integrity of information is average, which to a certain extent can negatively affect the result of the management process
4 (significant)	The level of information integrity is low, which can significantly affect the outcome of the management process
5 (maximum)	The level of information integrity is very low, which does not satisfy the performance of the management process and leads to its stop

Table 5

Ranking scale of the consequences of the implementation of EIR security threats (impact) on the confidentiality of information

Level of exposure	Content of the effects of exposure
1 (minimal)	The level of information confidentiality is high, it does not lead to the disclosure of the content of documents with limited access and the negative consequences of the management process
2 (insignificant)	The level of confidentiality of information is sufficient, but may lead to partial disclosure of the content of documents with limited access and a slight violation of the management process
3 (medium)	The level of confidentiality of information is medium, which may lead to indirect disclosure of the content of documents with limited access and a noticeable violation of the management process
4 (significant)	The level of confidentiality of information is low, which can lead to a significant disclosure of the content of documents with limited access and a violation of the management process as a whole
5 (maximum)	The level of confidentiality of information is very low, which leads to the disclosure of the content of documents with limited access in general and the disruption of the management process

Using the Harrington scale (Table 7), 5 qualitative levels of EIR security risk are approximately determined according to the following numerical scale (Table 8):

- “very low” level – 1 - 4 (1/25 = 0,04; 4/25 = 0,16);
- “low” level – 5 - 9 (5/25 = 0,2; 9/25 = 0,36);
- “average” level – 10 - 16 (10/25 = 0,4; 16/25 = 0,64);
- “high” level – 20 (20/25 = 0,80);
- “critical” level – 25 (25/25 = 1).

Thus, this matrix (Table 8) forms a set of values of qualitative assessments of the level of risk of EIR security, valid for application to any of the characteristics (properties) of EIR, and it makes it possible to quickly assess the "weight" of risks in relation to each property with relative quality information to make an appropriate decision. It should be noted that the presence of an unacceptable level of EIR security risk (for

example, "high" or "critical"), based on at least one property of the information, requires an appropriate response.

Table 6

Ranking scale of the consequences of the implementation of EIR security threats (impact) on the availability of information

Level of exposure	Content of the effects of exposure
1 (minimal)	The level of information availability is high, the management process is satisfactory
2 (insignificant)	The level of information availability is sufficient, but to a small extent it can negatively affect the result of the management process
3 (medium)	The level of information availability is average, which can significantly negatively affect the result of the management process
4 (significant)	The level of information availability is low, which can significantly affect the outcome of the management process
5 (maximum)	The level of information availability is very low, which does not satisfy the performance of the management process and leads to its halt

Table 7

Verbal-numerical scale of Harrington

Description of gradations of probability	Numerical value of probability
1. Very low	0 – 0,19
2. Low	0,20 – 0,36
3. Average	0,37 – 0,63
4. High	0,64 – 0,80
5. Very high	0,80 – 1,0

Therefore, for a response decision, it is sufficient to limit the calculation of the matrix for each property of information separately and not to complicate the evaluation process to an integral one (for all properties collectively). The result of the EIR security risk assessment is a register of such risks for each possible case of violation of the reliability, completeness, integrity, confidentiality, availability of information in the current management system. This register is used as a basis for forming conclusions when choosing a set of measures to ensure EIR security during the implementation stages of the management process related to countering EIR security risks.

The choice of methods (measures) of influence on the risk of EIR security is carried out by the management body in accordance with the conclusion on the level of EIR security risk to ensure the stable functioning of the entire information system and increase its reliability.

If, on the basis of the analysis and assessment of the safety risk of the EIR, a decision is made about the need to reduce its level, then proposals are prepared to take a set of measures to bring the level of such risk to the required value ("low" in practice). The specified proposals are developed by specialists of the expert group. The development of this set of measures requires studying the possibility of reducing the level of EIR security risk, provided that all available methods are adopted. At the same time, the impact on the reduction of the EIR security risk is carried out through various areas: the physical environment; hardware (software); elements of information infrastructure (means of ensuring communication); service personnel (process administration). In order to determine measures of influence on the level of the safety risk of the EIR, it is necessary to consider the vulnerabilities of the system (information assets) that require protection, and the types of threats that can be realized in the presence of these vulnerabilities, as well as the economic component (cost, expenditure of material resources, etc.) of one or the other of the event.

The directions for reducing the level of EIR security risks include:

- risk avoidance;
- reducing the level of threats;
- decrease in the degree of mechanical vulnerability of ITS elements;
- reducing the possible impact of irresistible events (natural disaster, defiant aggression, etc.).

Table 8
Matrix of qualitative assessment of EIR security risk levels

The level of possibility of SEIR threat	Very tall (5)	5 <i>Low</i>	10 <i>Average</i>	15 <i>Average</i>	20 <i>High</i>	25 <i>Critical</i>
	High (4)	4 <i>Very low</i>	8 <i>Low</i>	12 <i>Average</i>	16 <i>Average</i>	20 <i>High</i>
	Average (3)	3 <i>Very low</i>	6 <i>Low</i>	9 <i>Low</i>	12 <i>Average</i>	15 <i>Average</i>
	Low (2)	2 <i>Very low</i>	4 <i>Very low</i>	6 <i>Low</i>	8 <i>Low</i>	10 <i>Average</i>
	Very low (1)	1 <i>Very low</i>	2 <i>Very low</i>	3 <i>Very low</i>	4 <i>Very low</i>	5 <i>Low</i>
		Minimum (1)	Insignificant (2)	Average (3)	Significant (4)	Maximum (5)
The level of influence on the characteristics (properties) of EIR						

Measures by direction can be organizational and technical. Organizational measures provide for the presence of controlled methods of development and implementation of application programs, procedures for processing incidents in the event of a breach in IT, control over the work of personnel, their training, implementation of instructions on countering EIR security risks, and the use of safe methods of keeping documentation. Technical measures provide comprehensive protection of elements of the information system: hardware, software and means of providing the communication system (communication).

Decision-making on the need to organize countermeasures for each EIR security risk is made by the management body according to the binary principle:

- a). the assessed risk is insignificant (the value of the risk index falls within the range of the level of acceptable risks), it can be neglected and measures to reduce it should not be developed;
- b). the assessed risk is significant (unacceptable) and it is necessary to determine and implement measures to reduce it and further control its level.

The 2nd stage of the management process is carried out by the executive body and is aimed at the implementation of measures to counter the EIR security risk (influence on the EIR security risk level), the essence of which is to neutralize (reduce) the estimated level of the EIR security risk by applying a predefined (at the 1st stage) set of measures.

The main directions of influence on the risk level of the EIR security are the following:

- acceptance of the assessed risk (preparation of financial, material and other resources in case of dangerous situations);
- reduction of the assessed risk (implementation of measures to prevent dangerous situations, development of systems for their localization);
- exclusion of the assessed risk (use of safer technologies, improvement of security programs, duplication (reservation) of elements of the information system, etc.).

The 3rd stage of the management process (control of the results of neutralization of the EIR security risk) is performed by the monitoring body, which constantly monitors the effectiveness of the impact on the EIR security risk level. The essence of the implementation of the 3rd stage is to assess the results of reducing (neutralizing) the risk of EIR security and providing objective information about this state to the risk management body.

Stage 4 – the management body, on the basis of the data received from the monitoring body regarding the results of reducing (neutralizing) the level of EIR security risk, makes a decision on the results of the impact on the level of EIR security risk and draws a conclusion on the need for further management actions.

Thus, the proposed 4-stage scheme makes it possible to implement an adaptive EIR security risk management system based on a qualitative assessment of their level in order to choose reasonable countermeasures in a certain ITS, which ensures the sequence of systemic neutralization measures.

5. Conclusions

1. Destabilizing external and internal factors can cause EIR security risks in ITS based on the main characteristics of EIR (reliability, completeness, integrity, confidentiality, availability). The management of such risks is an important component of ensuring the cyber security of a certain management system supported by ITS, in general, the cyber security of the state.

2. The proposed methodological approach, based on the cybernetic management principle, allows creating a system of adaptive risk management of EIR security - an important element of ensuring cyber security. Such a system should include a management body, an executive body, a monitoring body and a management object - the level of EIR security risk. The system is based on the algorithm for forming a set of values (matrix) of qualitative levels of EIR security risk (according to the main characteristics of EIR) with the aim of choosing reasonable solutions for countering such risks.

3. The implementation of the proposed EIR security risk management process will provide improved decision-making support for risk neutralization (reduction) in any information systems (ITS), which will allow to increase the level of cyber security of the organization (institution), department and the state in general.

4. Further research should be focused on defining the list and essence of a set of measures to implement countermeasures against of EIR security risk according to the cybernetic principle of management.

6. References

- [1] Military standard BCT 01.004.004 – 2014 (01). Information security of the state in the military sphere. Terms and definitions. [Effective from 2014-02-02]. – Kyiv, Ukraine: MOU, 2014. (In Ukrainian).
- [2] Cybersecurity threats: the way forward [Electronic resource]. – Access mode: <https://intelligence.house.gov/hearing/cybersecurity-threats-way-forward>.
- [3] Sharp W.G. Cyberspace and the Use of Force. Falls Church. - V.A.: Aegis Research, 2009. – 234 p.
- [4] Lewis A.J. Securing Cyberspace for the 44th Presidency; Centre for Strategic and International Studies, 2008. [Electronic resource]. – Access mode: https://csis.org/files/media/isis/pubs/081208_securingcyberspace_44.pdf.
- [5] Bertil Almer. (2014). Modern General Risk Theory [Electronic resource]. – Access mode: <https://www.cambridge.org/core/journals/astin-bulletin-journal-of-the-iaa/article/modern-general-risk-theory/9BBF4F686467AD8C2C2CAF73F450299C>.
- [6] Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization, 2018. Official site [Electronic resource]. – Access mode: <https://www.nato.int/lisbon2018/strategic-concept-2018-eng.pdf>.
- [7] The Global Risks Report 2018 13th Edition. [Electronic resource]. – Access mode: http://www3.weforum.org/docs/WEF_GRR18Report.pdf.
- [8] Horbulin V.P., Kaczynskii A.B. Strategic planning: solving national security problems. Monograph. – Kyiv, NISR, 2010. - 288 p. (In Ukrainian).
- [9] Liepman J.M. The Third Domain; Homeland security digital library, 2018. [Electronic resource]. – Access mode: <https://www.hsdl.org/?view&doc=89385&coll=public>.
- [10] Cyberspace Presents Complex Global Challenges [Electronic resource]. – Access mode: <http://www.securityconference.de/Program425+M58b8d057766.0.html?&L=1>.
- [11] Viner N. Cybernetics: or control and communication in the animal and the machine. – 2nd revised ed. – Paris: Hermann & Cie, Camb. Mass. (MIT Press), 1961.
- [12] ISO.IEC 31010: 2009 – Risk management – Risk assessment techniques. [Electronic resource]. – Access mode: <https://www.en-standard.eu/une-en-31010-2011-risk-management-risk-assessment-techniques>.
- [13] Nefiodova L.Y. Application of principles of project management in defense management: Lecture // Project Office of Reforms of the Ministry of Defense of Ukraine. – Kyiv, MDU, 2019 (In Ukrainian).
- [14] Harrington E.C. The desirable function // Industrial Quality Control. – 1965. – Vol. 21. – № 10. – PP. 494-498.
- [15] Boschian-Campaner V. Maintenance task scheduling, reaching a twofold objective // American Journal of Operations Research. – 2015. – Vol. 5. – № 3. – PP. 124–131.