https://doi.org/10.33271/nvngu/2024-5/136

S. Onyshchenko,
orcid.org/0000-0002-6173-4361,
Ye. Zhyvylo,
orcid.org/0000-0003-4077-7853,
A. Hlushko*,
orcid.org/0000-0002-4086-1513,
S. Bilko,
orcid.org/0000-0003-0259-4482

National University "Yuri Kondratyuk Poltava Polytechnic", Poltava, Ukraine
* Corresponding author e-mail: glushk.alina@gmail.com

CYBER RISK MANAGEMENT TECHNOLOGY TO STRENGTHEN THE INFORMATION SECURITY OF THE NATIONAL ECONOMY

Purpose. Developing a technology for managing cyber risks based on their improved classification by the level of impact on the occurrence of an extreme situation.

Methodology. To achieve the goal, general scientific and special methods of cognition were used in the study: dialectical and systemic approaches, analysis and synthesis, logical generalization and grouping, structural-logical method, iterative approach, modeling, method of formal representations of uncertainty.

Findings. A cyber risk management technology has been developed, consisting of four main stages: analysis of cyber threats (context establishment; security audit; formation of scenario concepts); scenario modeling (threat decomposition; scenario formation; setting criteria; setting probability estimates of concepts (variables); building a network architecture; formation of a private threat model; scenario analysis); risk assessment; object classification. The proposed approach to cybersecurity risk management provides vulnerability detection and risk assessment (risk potential) and simplifies the development of management solutions to prevent events affecting cybersecurity.

Originality. The proposed technology differs from the existing ones by focusing on identifying those vulnerabilities and cyber threats that, according to their improved classification by the level of impact on the occurrence of an extreme situation, can lead to serious disruptions in the functioning of critical information infrastructure of the national economy.

Practical value. The practical significance of the study lies in the fact that the proposed cyber risk management technology is one of the tools for preventing the realization of risks in cyberspace and the basis for strengthening the information security of economic entities in particular and the national economy as a whole.

Keywords: *cybersecurity, critical information infrastructure, artificial intelligence, economic entity, digitalization*

Introduction. Global processes of information technology development have become a key factor in the formation of the digital economy and a determinant of global economic growth [1]. The total digitalization of public life, on the one hand, has helped to maximize benefits for the state, business, and citizens by increasing the efficiency and effectiveness of operations and information exchange. However, on the other hand, it has also led to an increase in financial risks and reputational damages due to cybercrime.

The increase in the intensity of cyber incidents in the information space at the national and global levels, related, among other things, to the development of artificial intelligence systems, has actualized the problem of cyberspace protection [2]. Unauthorized interference with information systems, their destabilization, theft of confidential information and other cyber threats require economic entities to implement effective security systems [3].

In recent years, powerful cyberattacks, in particular against Ukraine's critical information infrastructure, have been carried out in a complex, flexible, repeatable and measurable, multi-stage, pre-planned manner. These deliberate actions are aimed at blocking the operation of the main services of the technological network, which leads to interruptions in the provision of services to users, and sometimes to a complete disruption of the sustainable functioning of the entire information and communication system.

In this regard, the need to develop new methods of cyber risk management and mechanisms for their implementation, which will minimize cybersecurity risks for economic entities in Ukraine, is becoming increasingly important.

Literature review. The need to strengthen the information security of the national economy is objectively determined by the realities of today. Protection of information and communication systems and networks is one of the priority tasks for every economic entity of the national economy. An effective information security management system should be based not only on technological means of protection, but also predict systematic threat monitoring and vulnerability assessment, staff training, etc. This will ensure data security and stable operation of information and communication systems [4].

The United States is one of the world's leaders in the implementation of information technology. This requires the implementation of an effective information security policy and improvement of measures to counter information threats. The study of the US government's information security management policy allowed the author of [5] to argue that the dominant concept of information security is aimed at managing uncertainty through risk management. Interdependencies and the associated difficulties of breaking ties create a kind of uncertain governance – a regime of insecurity. It is emphasized that the digitalization of business processes can reduce costs, but at the same time requires increased security in computer networks. Since this article discusses only the theoretical foundations and policies of information security, the issue of preventing risks in cyberspace remains unresolved.

As in [5, 6] analyzes legislative initiatives of cybersecurity policy. The article conducts a retrospective analysis of the legal support for enhancing the resilience of cybersecurity of the United Nations (UN) and the European Union (EU). The author identifies five factors that explain the slow development of the global cybersecurity governance system, which underlies the complex relationship between cybersecurity and international law. These include the high speed of digitalization; fragmented jurisdiction and the legal problem of attribution; the regulatory role of the State or the private sector in cyberspace; the insufficiency of existing international law; and the phenomenon of "cybermania". The study concludes that there is a need to expand public-private partnerships in order to create

effective information security systems, but there is no specification of measures in this direction.

In work [7], enhancing the protection of information for economic entities is seen through the development of an information security culture (ISC) among employees. The research model developed ensures employee compliance with information security policies by promoting factors such as a supportive organizational culture, end-user engagement, and compliance leadership. The study results are not entirely accurate, as the model's effectiveness is confirmed solely by a conducted field survey.

The study [8] presents a model of effective cybersecurity management based on the following key components: cybersecurity strategy, standardized processes, compliance, senior management oversight, and resources. However, the model does not take into account such an important tool as security testing. The intrusion detection system as the basis for protecting the information resources of economic entities is detailed in [9]. An overview of existing intrusion detection systems is structured and presented. The study focuses on protecting information from DdoS attacks. Other types of cyber threats and hazards were not considered by the authors.

Unsolved aspects of the problem. Noting the practical value of the results of works [5–9], there are still many unresolved issues related to an integrated approach to cyber risk management in terms of strengthening information security in the digital economy. The introduction of risk management technology will allow economic entities to make timely adjustments and increase data security from risks and threats. This necessitates further research.

Purpose. The aim of the work is to strengthen the information security of the national economy by improving the technology of cyber risk management based on their improved classification by the level of impact on the occurrence of an extreme situation.

To achieve this goal, the following tasks were set:

1. To propose an improved classification of risks by their impact on the occurrence of an extreme situation.

2. To create a technology for managing cyber risks based on their improved classification.

Description of the research methodology for determining the cyber risk management technology. The results of the analysis of scientific studies [10, 11] suggest that the risk management process is an ongoing process that should take the form of an orderly sequence of events, actions and decisions that strengthen the cybersecurity of national economic entities, including critical infrastructure. Identifying potential risks is a key challenge for cybersecurity. For an effective risk analysis, it is crucial to identify critical information infrastructure, threats, vulnerabilities and understand the nature of cyberattacks, as well as to establish the risk as accurately as possible by determining its causes, scope, limitations and type of potential threats that may affect the achievement of goals and objectives of the impact.

The relationship between various attackers, threats, vulnerabilities, and their impact on information with subsequent consequences is shown in Fig. 1.

Currently, the catalog of cyber threats [12] includes at least the following: malware, Internet attacks, web application attacks, phishing, denial of service, spam, botnets, data and information leakage, insider threats, physical manipulation, damage/theft/loss of information and personal data, crypto theft, extortion, cyber espionage, backdoors, exploit kits. The risk management process related to the security of a critical information infrastructure facility may be iterative. The specificity of the iterative process is manifested in increasing the level of detail at each subsequent stage of the risk assessment or stopping the process. Upon completion of each stage, there are critical decision points (continuation of the process, its completion or return to the previous stage). This approach ensures an optimal balance between reducing the time and effort required to implement control measures and improving the accuracy of the risk assessment results.

The rapid development of information technologies and the spread of digitalization processes in all sectors of the national economy significantly increase cybersecurity risks for critical information infrastructure. This requires entities to implement preventive measures in cyberspace, an integral part of which is cybersecurity risk assessment.

Taking into account the number and types of risks in cyberspace, it is advisable to determine the level of cybersecurity risk acceptance by an economic entity, i.e. tolerance, when assessing and managing them. Risk tolerance allows determining the level of risk that an entity is willing to accept. A description of risk tolerance depending on its level is given in Table 1. Determining and managing risk tolerance are key aspects of ensuring business stability and efficiency. Adapting this approach to the specific context of an economic entity helps to optimize decision-making processes and minimize possible negative consequences.

Thus, risk assessment consists of identifying risks and determining the level of identified risks. The main stages of risk assessment are risk identification, quantitative risk assessment (which are elements of risk analysis) and qualitative risk assessment (Fig. 2).

The task of risk identification includes the following components:

a) asset identification (identifying and describing all assets that make up the system that are relevant to the risk). When identifying assets, it is important to determine which one is the

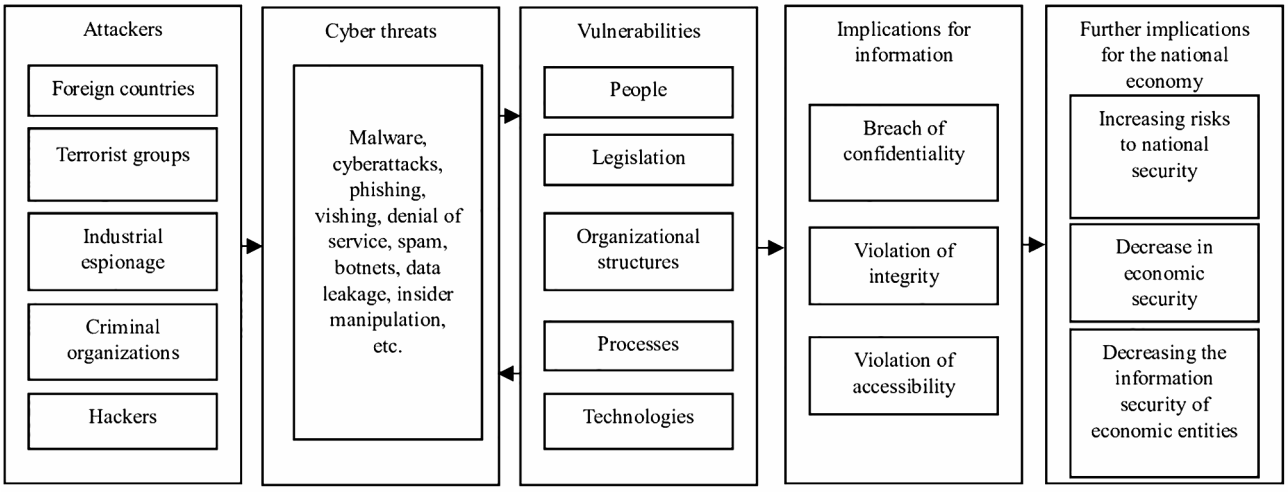

Fig. 1. Impact of cyber threats and vulnerabilities on cybersecurity

Table 1

Consideration of risk tolerance in the aspect of cyber risk management

Risk level	Description of risk tolerance
Very high	The level of risk cannot be accepted because its acceptance would result in consequences so severe that the related activity would have to be stopped immediately. Alternatively, mitigation strategies should be implemented immediately
High	The risk level cannot be accepted. Strategies to reduce the risk level should be developed and implemented within the next month
Above average	The level of risk cannot be accepted. Strategies to reduce the risk level should be developed and implemented within the next six months
Average	The level of risk can be accepted in the absence of strategies that can be easily and economically implemented. This risk must be continuously monitored to ensure that any changes are identified and addressed
Low	The level of risk can be accepted in the absence of strategies that can be easily and economically implemented. This risk should be monitored periodically to ensure that any changes are detected and addressed

primary asset, as well as the resources that attackers can take control of to reach the primary asset. For example, in a distributed control system power plant, a programmable logic controller (PLC), that controls the turbine is likely to be considered a major asset, as it directly affects the production of electricity. At the same time, the attacker's goal is likely to be to manipulate the PLC logic, namely to stop electricity production;

b) identification of threats based on resource inventory and network architecture schemes to detect threats [12, 13] that can exploit sensitive areas for each asset separately;

c) risk scenario building – the task of creating scenarios that provide a realistic and comparable view of risk based on the business context, system environment and associated threats. The risk scenario should consist of the following key elements: assets, threats, vulnerabilities (these elements can be identified through audits and/or penetration tests, and they can be associated with various physical spaces, the environment through the use of certain technologies, which are the direct result of threats).

Quantitative risk assessment involves determining the probability of occurrence and the level of impact (possible level of damage) of each risk scenario created at the previous stage. Traditionally, the frequency of targeted or accidental events has been used as a metric for measuring risk probability. However, due to the dynamic nature of cybersecurity threats, such a metric may be inappropriate. The absence of disruptions in the normal functioning of an economic entity's information system in the past does not guarantee protection against cyber threats in the future. Assessing the likelihood of cybersecurity risks should take into account the threats and vulnerabilities of the system. A number of factors should be taken into account:

- detection is the focus of attackers' efforts to find vulnerabilities in the network's assets (control system). This factor depends on the availability of information about the system's vulnerability and the impact of vulnerable assets on the system's functioning;

- exploitability is the development of a strategy, tactics, and a basic algorithm to implement the shortest paths to vulnerability of system assets. This factor depends on access rights, complexity of tools, and technical skills required to execute the attack;

- reproducibility is the build-up of preventive offensive actions against system (network) assets. This factor depends on the complexity of building the system architecture, its organizational and technical model of cyber defense, mechanisms for timely identification of threats and tools for detecting cyberattacks.

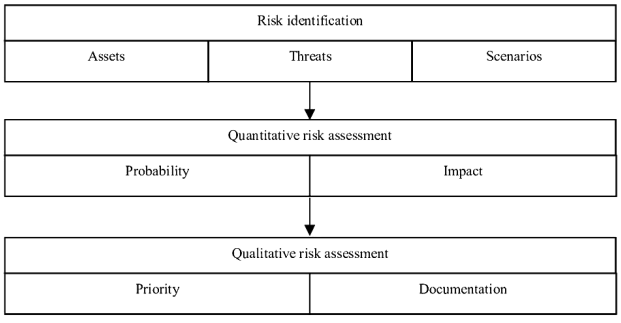

Fig. 2. Risk assessment process

The manifestation of a risk scenario could compromise the confidentiality, integrity, and/or availability of assets (e. g., information, equipment, operations). Any compromise of assets will lead to negative effects at the following levels: the state (the impact can be seen as damage to state security and the economy); the economic entity (the impact can be seen as disruption of business operations, damage to reputation and loss of finances); the individual (the impact can be seen as loss of life and injury).

A qualitative risk assessment consists in identifying and understanding the significance of the risk level and includes the following tasks:

- identification and prioritization of risks (building a risk matrix);

- documenting risks (entering risks into a register indicating the identified scenario, date, measure, residual risk, etc.).

At the same time, the complexity of cyber-physical relations in the functioning of critical information infrastructure facilities lies in unconscious system dependencies. Accurate risk assessment requires the development of models that provide a basis for dependency analysis and quantitative risk assessment. The relationship between the characteristics of critical information infrastructure facilitates the process of risk analysis and mitigation.

Therefore, this approach to cybersecurity risk assessment can be applied in the information and analytical system "Security Management System" [14], which provides vulnerability detection and risk assessment (risk potential) and simplifies the development of management decisions to prevent events affecting cybersecurity.

Summary of the main material and scientific results. In accordance with the provisions of the above-mentioned methods and the factors outlined above, the identification of real and potential cyber threats is carried out by establishing, on the basis of empirical experience, the correspondence between such sources and their characteristics. As a result, a set $\{ak\}$, $k = 1, 2, ...$, is formed, the elements of which are signs of threat sources, and the indices are their numbers.

For critical information infrastructure facilities, the sources of threats of computer attacks are:

$k = 1$ – foreign special services;

$k = 2$ – criminal organizations;

$k = 3$ – competitors;

$k = 4$ – facility personnel;

$k = 5$ – equipment manufacturers, enterprises that repair and maintain computers and peripheral equipment of critical information infrastructure facilities;

$a1$ – interest of foreign special services in the information resources of the object;

$a2$ – interest of criminal organizations in the information resources of the object;

$a3$ – the interest of representatives of the financial, economic and industrial environment (infrastructure) who have a competitive interest and use the information resources of the joint facility;

$a4$ – independent technical support and maintenance of the IT infrastructure by the officials of the facility;

$a5$ – the use of uncertified (unlicensed) software during maintenance and repair and restoration work at the facility.

In the context of the growing risk of phishing attacks, botnets, malware, ransomware, etc., the peculiarity of this approach is to identify vulnerabilities of information resources of critical information infrastructure. In order to reduce the risk of possible computer attacks, it is necessary to use calculation methods that allow establishing the fact of a potential threat.

When determining the vulnerabilities of an object's information resources to the threats of computer attacks, an expert analysis of the object's information environment is carried out. As a result, a set {bl}, $l = 1, 2, ..., L$ is formed, the elements of which determine the vulnerabilities. In this case, the indices correspond to the numbers of vulnerabilities from their list.

In the case of assessing the threat level of a computer attack on the information resources of an object, the following are vulnerable to such threats:

$b1$ – drivers of information input tools;

$b2$ – drivers of information display tools;

$b3$ – drivers of information processing tools;

$b4$ – BIOS chip drivers;

$b5$ – software of servers with open physical access;

$b6$ – software of the facility's communication equipment;

$b7$ – TCP/IP protocol stack;

$b8$ – gateway to the Internet;

$b9$ – application layer interconnection protocols;

$b10$ – undocumented points of interconnection;

$b11$ – open shared network resources;

$b12$ – uncertified software components;

$b13$ – e-mail;

$b14$ – Web browser;

$b15$ – facility equipment cables in areas where they are physically accessible.

In order to quantify the vulnerability that may lead to a computer attack on the information resources of critical information infrastructure, the probability of the existence of appropriate favorable conditions is determined. This probability is assessed by experts in the field of cybersecurity. The results of the assessment are represented by linguistic values: "yes", "probable", "possible", "improbable" and "no", which characterize the possibility of the k^{th} source of the computer attack threat exploiting the l^{th} vulnerability. Each of the five linguistic values is assigned a probability pkl of exploitation of the l^{th} vulnerability by the k^{th} source. Based on this probability, the probability P_l of exploitation of the l^{th} vulnerability ($l = 1, 2, ..., 15$) by possible five threat sources is determined

$$P_l = 1 - (\gamma l_1(1 - pl_1) \cdot \gamma l_2(1 - pl_2) \cdot \gamma l_3(1 - pl_3) \times \times \gamma l_4(1 - pl_4) \cdot \gamma l_5(1 - pl_5)), \quad (1)$$

where γl_k is a matching coefficient equal to 1 if the l^{th} vulnerability matches the k^{th} source and 0 if it does not.

This allows us to form a set $\{um\}$, $m = 1, 2, ..., M$, of computer attack threats [12]:

$u1$ – downloading malicious software with functions of an alternative operating system with extended powers;

$u2$ – unauthorized copying of information;

$u3$ – unauthorized modification of information;

$u4$ – introduction of a false trusted object;

$u5$ – substitution of system software;

$u6$ – redirection of network traffic;

$u7$ – manipulation of data remotely;

$u8$ – hacking into an electronic mailbox;

$u9$ – blocking an electronic mailbox;

$u10$ – substitution of Web browsers;

$u11$ – use of errors in application software algorithms;

$u12$ – blocking the user's host;

$u13$ – blocking the router;

$u14$ – bypassing the firewall.

A quantitative characteristic of the level of the m^{th} threat of a computer attack, where $m = 1, 2, ..., 14$, on the information resources of critical information infrastructure is the probability

$$P_m^{(y)} = 1 - \prod (1 - \alpha lm \cdot P_i),$$

where P_i is corresponds to expression (1); αlm is the coefficient of relevance of vulnerabilities of the object's information for the initialization of computer attack threats, equal to 1 if the l^{th} vulnerability is relevant for the initialization of the m^{th} threat and 0 if not relevant.

The values of the coefficient of relevance of information vulnerabilities of critical information infrastructure objects for the initialization of computer attack threats are given in Table 2.

Taking into account the threats of computer attacks, the values of the coefficient of destruction of threats of computer attacks on information resources of critical information infrastructure are given in Table 3.

From the above, it follows that the advantage of existing methods for assessing current information security threats is the simplicity of assessment procedures. The disadvantages that fundamentally limit their use for an adequate assessment of measures to ensure the cyber resilience of critical information infrastructure include the inability to take into account the dynamics of countering such threats and the low statistical reliability that is typical of expert assessments.

The technology implements the algorithm for applying the above methods to analyze cyber threats and assess cybersecurity risks, which consists of four main stages:

Stage I. Analysis of cyber threats (establishing the context; security audit; formation of scenario concepts).

Stage II. Scenario modeling (threat decomposition; scenario formation; setting criteria; setting probability estimates for concepts (variables); building a network architecture; forming a private threat model; scenario analysis).

Stage III. Risk assessment.

Stage IV. Object classification.

The proposed technology is designed for the following user groups:

- security engineer, i.e., an expert in the field of information security, or in the absence of such, the administrator of a local area network;

- energy knowledge engineer (expert): depending on the level of detail of the study, he/she can be either an expert in the field of energy security or an operator/energy engineer at the facility; in the field of security: security engineer;

- an analyst, who may be a knowledge engineer.

The interrelation of technology stages, methods and blocks of the information system is presented in Table 4.

Although the algorithm for applying these methods to analyze cyber threats and assess cybersecurity risks involves different levels, stages and components, it should be a single document and consist of hierarchical stages (levels).

The cyber risk management system is functionally presented in Fig. 3.

At the "Analysis of cyber threats" stage, the context is established, i.e., a description of the main characteristics of the object in question, its identification, and a description of the assets of the information technology system.

However, the security audit of an economic entity (enterprise, organization) at the initial stages consists in identifying critical components and identifying existing vulnerabilities [14].

Table 2

Values of the coefficient of relevance of information vulnerabilities of critical information infrastructure objects for initializing computer attack threats

Threats of of computer attacks	Vulnerability of information resources of critical information infrastructure to threats of computer attacks														
	$b1$	$b2$	$b3$	$b4$	$b5$	$b6$	$b7$	$b8$	$b9$	$b10$	$b11$	$b12$	$b13$	$b14$	$b15$
$u1$	1	0	0	0	1	1	0	0	0	0	0	1	1	1	1
$u2$	0	0	0	0	1	0	0	1	1	1	1	1	1	1	1
$u3$	1	1	1	0	1	0	0	1	1	1	1	1	1	1	1
$u4$	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1
$u5$	1	1	1	0	0	0	0	0	0	0	0	0	1	1	1
$u6$	1	1	1	0	1	1	1	1	1	1	0	0	1	1	1
$u7$	1	1	1	0	0	0	1	0	0	0	0	0	1	0	0
$u8$	1	1	1	0	0	1	0	0	1	0	0	0	1	1	0
$u9$	1	1	1	0	0	1	0	0	1	0	0	0	1	1	0
$u10$	1	1	1	0	0	1	0	0	1	0	0	0	1	0	1
$u11$	1	1	0	0	0	0	0	0	0	0	1	0	1	0	0
$u12$	1	0	0	0	0	1	0	1	0	0	0	1	0	0	0
$u13$	1	0	0	0	0	1	0	1	0	1	1	1	0	0	0
$u14$	1	1	1	0	0	0	0	0	0	0	0	0	1	0	0

Table 3

Information security assessment scale

Destruction	Threats of computer attacks													
	$u1$	$u2$	$u3$	$u4$	$u5$	$u6$	$u7$	$u8$	$u9$	$u10$	$u11$	$u12$	$u13$	$u14$
NK	1	1	0	1	0	0	1	1	0	1	1	0	0	1
NM	1	0	1	1	1	1	1	0	0	1	1	0	0	1
DB	1	0	0	1	0	0	1	0	1	1	1	1	1	1

Table 4

Interrelation of cyber risk management technology stages, methods and blocks

Stages	User groups	Methodologies	Tools and techniques
Analysis of cyber threats	Security engineer	Methodology for analyzing cyber threats to critical infrastructure	Expert system
Scenario modeling	Security engineer, knowledge engineer (expert in the field of industry security)	Methodology for creating scenarios of extreme situations in the energy sector	Block of Bayesian trust networks
Risk assessment	Knowledge engineer (expert), analyst	Methodology for assessing the risks of cybersecurity breaches in energy infrastructure	Risk assessment unit
Ranking of objects	Analyst		

Thus, the analysis of cyber threats in an intelligent system is carried out using technological and software tools that are part of the product expert system. Lists of critical assets and identified vulnerabilities are formed in accordance with existing/identified cyber threats, as well as typical attack vectors, which are a sequence of potential threats and vulnerabilities to target assets. Based on the result, concepts and connections between them are formed for further scenario building. Formally, the initial data of the first stage of the cyber threat analysis and risk assessment technology are represented by the formula

$$P = \{V, T, A, R_V\}.$$

The "Scenario Modeling" stage is proposed to be built according to "scenario planning" [15] using Bayesian network tools, which consists in calculating the value of trust in the proposed scenarios based on existing trust options in the network.

Scenarios are evaluated by an integral indicator of each IP address, DNS name, IP address range, subnet, and even a text file (by scanning).

Such calculations are considered as a pessimistic scenario – a set of events and interrelationships between them that lead to maximum losses and damages as a result of their occurrence and development [16].

Previously, the Bayesian network model was used to model the risks of critical situations in the implementation of strategic threats [15], but cybersecurity threats were not considered. In addition, this technique was used to model economic risks [17], as well as information technology risks [18].

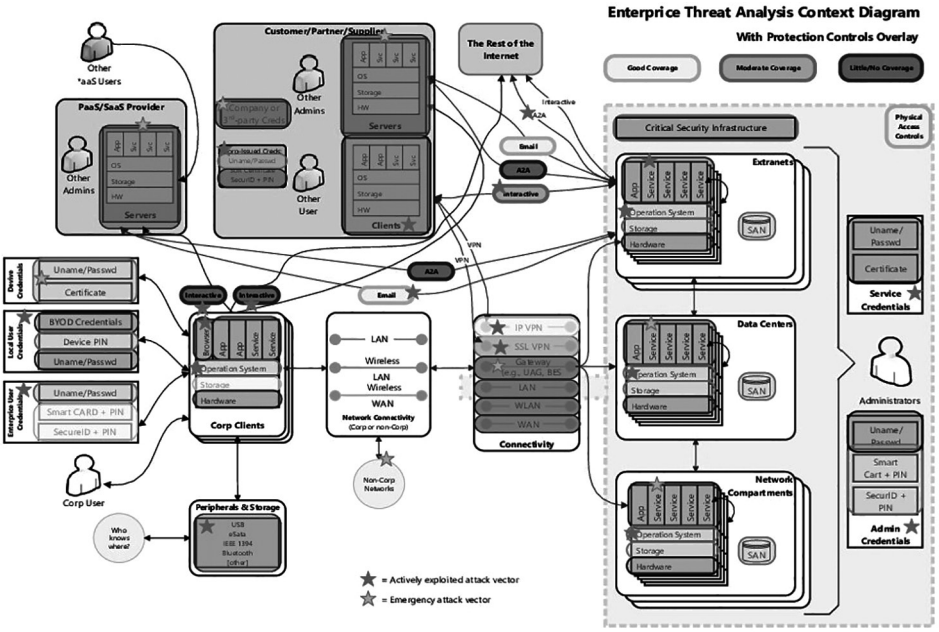

Fig. 3. Functional cyber risk management system

In connection with the inclusion of cyber threats among the strategic threats to the national economy and national security in general [19], the following structure of a typical scenario of a threshold situation caused by the implementation of cyber threats is proposed, which is represented by the formula

$$S = (X^f, X^v, X^t, X^c),$$

where S is the structure of the scenario of an extreme situation at an economic entity caused by the implementation of cyber threats; X^f – variables, according to the factors that influence the occurrence of an extreme situation; X^v – variables to indicate the vulnerabilities of electronic communication network assets; X^t – variables to indicate threats; X^c – variables, consequences associated with the probable occurrence of an extreme situation at an economic entity.

Next, scenarios of extreme situations are built under certain conditions of the state of electronic communication networks, and probable threats are identified, taking into account information on the spread of attack vectors. An extreme situation can be rightly considered as a critical state arising from the action of external or internal factors, which leads to significant disruptions in the functioning of objects or systems and poses a threat to the vital activity of the population, national security or economic stability of the state, requiring urgent measures to achieve the desired state. Based on the scenario analysis, strategic management decisions are made to achieve the desired states and situations [15].

At the "Risk Assessment" stage, risk is considered as a combination of the consequences of an event (incident) and the associated possibility of occurrence in accordance with the international standard ISO/IEC 27005:2011 "Information technology. Methods of protection. Information security risk management".

The risks of a sequence of threats leading to an extreme situation are assessed using both qualitative and quantitative indicators. The description of such risks is based on qualitative information obtained from experts (information security and cybersecurity specialists, engineering staff), which is necessary to identify and describe each of the six types of scenario concepts described above. Quantitative information related to the peculiarities of the system's functioning is used further when filling in the values in the concepts.

The risk level is measured for all significant scenarios, which are assigned values of probability and risk consequences [17]. The presence of vulnerabilities in the risk assessment allows determining the list of critical assets of the economic entity in order to further justify the financial costs of security. Risk assessment is carried out taking into account the established assessment criteria.

The "Object classification" stage of the cyber risk management technology consists in classifying objects according to the established criteria and risk levels for each of them. Critical objects are key objects (or their aggregates) of the relevant infrastructures, the impact on which can provoke the most negative effect in the economy, a key resource or lead to the destruction of the entire infrastructure [20].

Within the framework of the proposed technology, objects are classified according to the magnitude of the risks of an extreme situation covering a certain territory and a group of objects in their relationship with other critical information infrastructure objects, information about which is included in the scenario as concepts of consequences, external threats or factors. The criterion for the significance of classification is proposed

$$KS = \{C, R, O\},$$

where KS is the significance criterion; C – risk assessment criterion; R – integral indicator of the object's risks; O – object represented by a set of basic characteristics.

The result of this stage is a hierarchically compiled list of objects.

Thus, the proposed technology, in comparison with traditional approaches to cybersecurity, is aimed at identifying vulnerabilities and cyber threats, the realization of which can cause disruption of the functioning of an important facility to such an extent that the incident can be regarded as an extreme situation in the economy, a threat to life or a destructive situation in the national economy.

Conclusions. It is substantiated that information security in modern conditions is the basis for strengthening the security of the national economy and national security of the country as a whole. Building an effective information security management system for an economic entity should be based on a systematic approach that includes technologies, processes and tools to counteract risks in cyberspace. Given the ever-increasing challenges to Ukraine's economic security in the information space and business losses due to cyber incidents, the need to improve cyber risk management technology has been proven.

An improved classification of risks based on their impact on the occurrence of an extreme situation is proposed.

A cyber risk management technology has been developed, which, compared to traditional approaches, is aimed at identifying vulnerabilities and cyber threats, the realization of which can lead to serious disruptions in the functioning of critical information infrastructure, which can be regarded as an extreme situation in the national economy. This, in turn, will make it possible to develop effective tools to prevent the realization of cyber risks. The validity of the proposed technology at the development stage is confirmed by expert assessments of information security and cybersecurity specialists, which will be supported by its further testing.

Emphasizing the significance of the study, it should be noted that threats in cyberspace are constantly evolving and modifying. Therefore, the prospects for further research are to study new types of cyber threats and their behavior in order to develop innovative models for predicting and preventing cyberattacks based on the use of artificial intelligence technologies.

References.

1. Onyshchenko, S., Yanko, A., Hlushko, A., Maslii, O., & Cherviak, A. (2023). Cybersecurity And Improvement Of The Information Security System. *Journal of the Balkan Tribological Association*, *29*(5), 818-835.

2. Shefer, O., Laktionov, O., Pents, V., Hlushko, A., & Kuchuk, N. (2024). Practical principles of integrating artificial intelligence into the technology of regional security predicting. *Advanced Information Systems*, *8*(1), 86-93. https://doi.org/10.20998/2522-9052.2024.1.11.

3. Krasnobayev, V., Yanko, A., & Hlushko, A. (2023). Information Security of the National Economy Based on an Effective Data Control Method. *Journal of International Commerce, Economics and Policy*, 2350021. https://doi.org/10.1142/S1793993323500217.

4. Onyshchenko, S., Yanko, A., & Hlushko, A. (2023). Improving the efficiency of diagnosing errors in computer devices for processing economic data functioning in the class of residuals. *Eastern-European Journal of Enterprise Technologies*, *5*(4(125)), 63-73. https://doi.org/10.15587/1729-4061.2023.289185.

5. Slayton, R. (2021). Governing Uncertainty or Uncertain Governance? Information Security and the Challenge of Cutting Ties. *Science, Technology, & Human Values*, *46*(1), 81-111. https://doi.org/10.1177/0162243919901159.

6. Wouters, J., & Verhelst, A. (2020). Filling Global Governance Gaps in Cybersecurity: International and European Legal Perspectives. *International Organisations Research Journal*. https://doi.org/10.17323/1996-7845-2020-02-07.

7. Amankwa, E., Loock, M., & Kritzinger, E. (2018). Establishing information security policy compliance culture in organizations. *Information & Computer Security*, *26*(4), 420-436. https://doi.org/10.1108/ICS-09-2017-0063.

8. Yusif, S., & Hafeez-Baig, A. (2021). A Conceptual Model for Cybersecurity Governance. *Journal of Applied Security Research*, *16*(4), 490-513. https://doi.org/10.1080/19361610.2021.1918995.

9. Hidouri, A., Hajlaoui, N., Touati, H., Hadded, M., & Muhlethaler, P. (2022). A Survey on Security Attacks and Intrusion Detection Mechanisms in Named Data Networking. *Computers*, *11*, 186. https://doi.org/10.3390/computers11120186.

10. Onyshchenko, S., Yanko, A., Hlushko, A., Maslii, O., & Skryl, V. (2023). The Mechanism of Information Security of the National Economy in Cyberspace. *Proceedings of the 4th International Conference on Building Innovations. ICBI 2022. Lecture Notes in Civil Engineering, 299,* 791-803. Cham: Springer. https://doi.org/10.1007/978-3-031-17385-1_67.

11. Laktionov, A. (2019). Application of index estimates for improving accuracy during selection of machine operators. *Eastern-European Journal of Enterprise Technologies*, *3*(1(99)), 18-26. https://doi.org/10.15587/1729-4061.2019.165884.

12. Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research*, *253*(1), 1-13. https://doi.org/10.1016/j.ejor.2015.12.023.

13. *Cyber insurance: a new risk management tool* (n.d.). Retrieved from http://forbes.net.ua/ua/opinions/1426423-kiber-strahuvannya-novij-instrument-rizik-menedzhmentu.

14. Jain, P., Pasman, H.J., Waldram, S., Pistikopoulos, E.N., & Mannan, M.S. (2018). Process Resilience Analysis Framework (PRAF): A systems approach for improved risk and safety management. *Journal of Loss Prevention in the Process Industries*, *53*, 61-73. https://doi.org/10.1016/j.jlp.2017.08.006.

15. Cherdantseva, Yu., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security*, *56*, 1-27. https://doi.org/10.1016/j.cose.2015.09.009.

16. Eling, M., & Wirfs, J. (2019). What are the actual costs of cyber risk events? *European Journal of Operational Research*, *272*(3), 1109-1119. https://doi.org/10.1016/j.ejor.2018.07.021.

17. Young, D., Lopez Jr., J., Rice, M., Ramsey, B., & McTasney, R. (2016). A framework for incorporating insurance in critical infrastructure cyber risk strategies. *International Journal of Critical Infrastructure Protection*, *14*, 43-57. https://doi.org/10.1016/j.ijcip.2016.04.001.

18. Alali, M., Almogren, A., Hassan, M.M., Rassan, I.A.L., & Md Bhuiyan, Z. A. (2018). Improving risk assessment model of cyber security using fuzzy logic inference system. *Computers & Security*, *74*, 323-339. https://doi.org/10.1016/j.cose.2017.09.011.

19. Onyshchenko, S., Zhyvylo, Y., Cherviak, A., & Bilko, S. (2023). Determination of the peculiarities peculiarities of using information security systems in financial institutions in order to increase the financial security level. *Eastern-European Journal of Enterprise Technologies*, *5*(13(125)), 65-76. https://doi.org/10.15587/1729-4061.2023.288175.

20. *Global Cyber Insurance Market* (2019–2025). Retrieved from https://www.researchandmarkets.com/reports/4871728/global-cyber-insurancemarket-2019-2025.

Технологія управління кіберризиками для зміцнення інформаційної безпеки національної економіки

С. В. Онищенко, Є. О. Живило, А. Д. Глушко, С. С. Білько*

Національний університет «Полтавська політехніка імені Юрія Кондратюка», м. Полтава, Україна

* Автор-кореспондент e-mail: glushk.alina@gmail.com

Мета. Розроблення технології управління кіберризиками на основі удосконаленої їх класифікації за рівнем впливу на виникнення екстремальної ситуації.

Методика. Для досягнення поставленої мети в досліджені використані загальнонаукові та спеціальні методи пізнання: діалектичний і системний підходи, аналіз і синтез, логічне узагальнення та групування, структурно-логічний метод, ітераційний підхід, моделювання, метод формалізованого опису невизначеності.

Результати. Розроблена технологія управління кіберризиками, що складається з чотирьох основних етапів: аналіз кіберзагроз (встановлення контексту; аудит безпеки; формування концептів сценарію); моделювання сценаріїв (декомпозиція загроз; формування сценарію; установка критеріїв; установка оцінок імовірностей значень концептів (змінних); побудова архітектури мережі; формування приватної моделі загроз; аналіз сценаріїв); оцінювання ризиків; класифікація об'єктів. Запропонований підхід до управління ризиками кібербезпеки забезпечує виявлення вразливостей та оцінку ризиків (потенціал ризику) і спрощує розробку управлінських рішень для запобігання подіям, що впливають на кібербезпеку.

Наукова новизна. Запропонована технологія відрізняється від існуючих спрямованістю на виявлення тих вразливостей і кіберзагроз, які, у відповідності до удосконаленої їх класифікації за рівнем впливу на виникнення екстремальної ситуації, можуть призвести до серйозних порушень функціонування об'єктів критичної інформаційної інфраструктури національної економіки.

Практична значимість. Полягає в тому, що запропонована технологія управління кіберризиками є одним із інструментом для запобігання реалізації ризиків у кіберпросторі та базисом зміцнення інформаційної безпеки економічних суб'єктів, зокрема і національної економіки в цілому.

Ключові слова: *кібербезпека, критична інформаційна інфраструктура, штучний інтелект, економічний суб'єкт, цифровізація*

The manuscript was submitted 10.05.24.