УДК 004.056.55: 003.26
https://doi.org/10.47533/2020.1606-146X.171

A. S. ABDIRAMAN*, A. M. NURUSHEVA, L. S. ALDASHEVA

L.N. Gumilyov Eurasian national university, Nur-Sultan, Kazakhstan
e-mail: a.s.abdiraman@gmail.com, nurusheva.assel@mail.ru
Astana IT university
e-mail: laura.aldasheva@astanait.edu.kz

ANALYSIS OF METHODS FOR INFORMATION SECURITY LEVEL ASSESSMENT OF INFORMATION AND COMMUNICATION INFRASTRUCTURE OBJECTS

In the world of automated digital technologies, one of the main tasks of the enterprise is to find an effective way to prevent the implementation of information security risks. In case to achieve these goals, various evaluation methods are currently used. Basically, any research begins with a literary review of the research topic development. Consequently, this article is a literary review of current methods, tools, and standards for assessing information security of systems, formed through scientific materials from the Scopus and Web of Science databases. Also, this paper examines the analysis of existing methods for assessing the level of information security in the objects of information and communication infrastructure. Based on literature review provides an analysis of information security level assessment methods. This article performs the results of research to an analysis of information security level of information systems within the framework of the project with grant funding from the Ministry of Education and Science of the Republic of Kazakhstan, grant number AP13067916.

Key words: *cyber security, assessment methods, information and communication infrastructure objects, CIOICI, impact, risk.*

Introduction. Currently, there are no organizations that would not face certain threats in information security, for example, malware, Internet fraud, phishing, impersonating another person, DoS, and also, the associated risks to their information systems [1-3]. Along with the large number of considerable risks to which each organization is bare now are active risks of information technology arising as of inadequately established domestic processes, people, and systems or from damaging outdoor events, such as computer attacks on resources [4-6].

The main aim in ensuring information security is to defend the business itself, the capability to defend its connected IT assets, guaranteeing privacy, integrity, and accessibility of

* E-mail корреспондирующего автора: a.s.abdiraman@gmail.com

information and information systems, as well as ensuring the confidentiality of the organization's resources [7].

Analysis of information security level assessment methods. In this regard, this article provides a systematic literature review of methods, techniques, and tools related to the prevention of threats to information security. A literature review on the use of various methods for assessing the level of information security of information and communication infrastructure (ICI) objects was compiled through the manual [8], which provides aspects of conducting a systematic review of the literature of a specific research area proposed by the authors B.Kitchenham and S.Charters.

A systematic literature review is a form of secondary research that uses a well-defined methodology to identify, analyze and interpret all available evidence related to a specific research issue A systematic literature analysis is a form of consequential research that uses a definite methodology to associate, analyze and clarify all available confirmation allied to certain research arise [8]. This method of conducting a literary review makes it possible to save time resources and narrow the list of analyzed literature by filtering through keywords.

The sources in the systematic literature review are the scientific Internet resources "Scopus" and "Web of Science". First of all, it is necessary to determine the keywords to search for relevant literature in the scientific platforms "Scopus" and "Web of Science".

The following words were selected as keywords for the search:

– assessment methods;

– information security;

– objects of information and communication infrastructure.

Considering the above keywords, statistics of published documents were compiled in the context of web sources. In Figure 1, you can see the publication trends corresponding to the search keywords of the study area. This graph shows certain popularity of the topic of assessing the level of information security, which determines the relevance of the study.

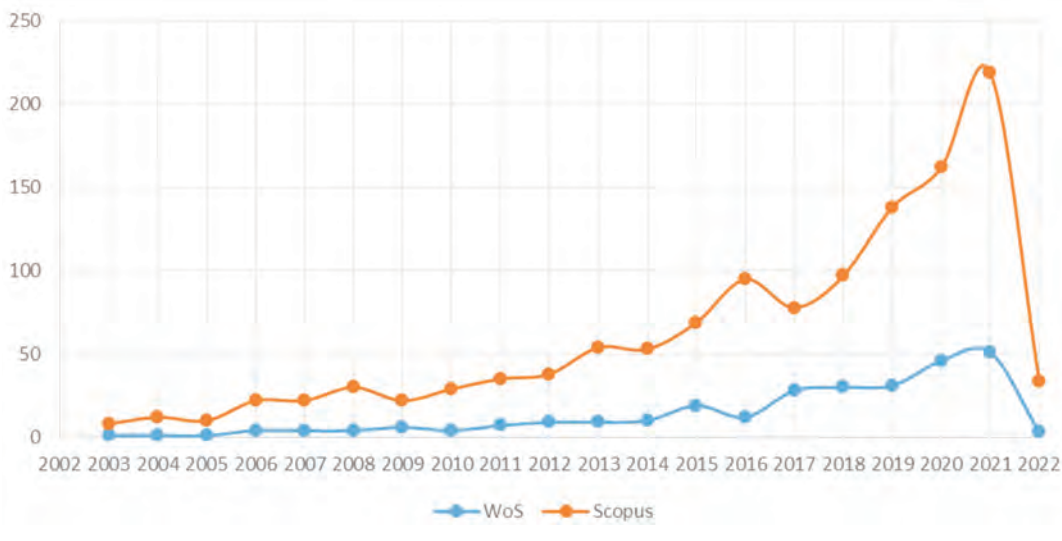

Figure 1 – Statistics of the number of publications by year of publication

Also, the largest number of publications on the topic under study was in the period from 2018 to 2021. During this period, "articles" were mainly published by type of publications. As can be seen from the graph, there is a decline in 2022. It is worth noting that publications for 2022 are still being accepted and under consideration, so the number is reduced.

Based on the statistics presented in Figure 1, the articles were analyzed by the number of citations by search, by keywords. As you know, the relevance of an article is determined by the number of its citations. This analysis was carried out on the Internet resource Web of science. According to the search results, by keywords, as well as by the type of document "article", the total number of publications was 280. It is worth noting that most of the articles during the study period were not cited. In this regard, a table has been compiled for the most cited publications (see Table 1). In addition, according to a similar method of selection, the Internet resource Scopus has issued 1227 articles.

The above number of articles considers the expanded research area; therefore, the following categories are selected to limit the research area:

– computer science information systems;

– telecommunications;

– methods of the theory of computer science.

The last 5 years in the period from 2018 to 2022 were chosen as the study period. Also, according to the type of publications, only articles for the last five years were selected.

After setting the above restrictions, the total number of publications was 39 in Web of Science, and 140 in Scopus.

Based on the analysis of publications through the Web of Science Internet resource, using the method described in the manual [8], a literary review was conducted on the most-cited statistics databases Web of Science and Scopus in accordance with the field of research.

In the article [9], the authors developed a methodology for assessing information security in a special-purpose information and telecommunications system. During the study, the authors used the main provisions of the theory of communication, the theory of queuing, artificial intelligence, as well as general scientific methods of analysis and synthesis. The difference between the proposed method and the known ones, which determines its novelty, lies in the possibility of detection and qualitative interpretation of cyber threats; modeling scenarios of acute situations caused as a result of the execution of cyber threats; assessment of risks having characteristics of several classes and ranking of information and telecommunication system assets by their level of criticalness; assessment of the number of critically vulnerable assets of the information and telecommunication system; substantiation of the constitution and likelihood of cyber threats that can cause extreme situations in the information and telecommunication system; risk assessment of their implementation in the information and telecommunication system. The practical significance of the proposed method lies in the fact that its application makes it possible to automatize the mechanism of analyzing cyber threats and assessing the risks of information security of an information and telecommunications system.

In [10], an innovative ontology and approach based on the graph method for assessing the information security of a network are proposed. The ontology is designed to represent

knowledge about information security, such as knowledge about assets, vulnerabilities, attacks, relationships, and inference rules to identify possible attacks. Subsequently, an effective system structure and an algorithm for generating an attack graph were developed to detect logical attack paths in corporate networks. However, the disadvantage of this method is the complexity of calculating the proposed algorithm for generating an attack graph. Moreover, the research in the article [11] shows that there is no standard method for representing attack graphs or attack trees and that additional research is needed to standardize this representation. Nevertheless, the studies carried out in [11] are useful for assessing the level of information security of ICI facilities. Since to conduct an assessment, we need data that describes the nature of cyberattacks, exploits, and vulnerabilities.

The object of research in [12] is the critically important objects of ICI (CIOICI), which are important in the field of national security, economy, and public security of each country. In this study, the impact of cyberattacks on CIOICI is assessed using a hierarchical flow model approach. Using this method, a CIOICI model is constructed that considers the cyber-physical interaction within the station, the dependence between stations, and the topological structure of the physical network. Further, based on the CIOICI model, an impact assessment is proposed to quantify the losses caused by the spread of the impact within the CIOICI network. However, the detailed relationship between the devices and the target has not been investigated, as has the analysis of the spread of the attack on the network.

The paper [13] presents a method of searching for aggregation operators to create a classification of attacks on a certain system. To implement this method, a set of data collected during decision-making exercises was used. Using the collected data, information security experts performed tasks to assess security based on a realistic system. The results showed that using the proposed method, it is possible to rank attacks on the system by ratings of security components, ranking security components by ratings of specific complexity factors, and, finally, ranking attacks on the system by ratings of specific factors. In the course of this work, important conclusions were obtained that made it possible to create tools to support expert security assessment. Such tools can reduce the time and effort required by experts to conduct assessments and allow system developers to make approximate safety assessments before they seek expert advice. These advances will address the growing concern about the capabilities of limited expert resources due to the increasing complexity and increasing number of information systems being attacked by an ever-changing set of attacks.

There are 3 types of assessment of the level of information security of ICI: assessment by reference, risk-based assessment, and assessment by economic indicators. For the study in this article, the most appropriate type of assessment of the level of information security is risk-oriented.

Results. Table 1 presents the above-described models and risk assessment methods proposed by various authors [9-13] for the study period.

Table 1 – Risk assessment models and methods [9-13]

Reference	Proposed method/model of information security level assessment	Disadvantage
[9]	a method for automating the process of analyzing cyber threats and assessing the risks of information security of an information and telecommunications system	works only with identified information security threats available in the knowledge base
[10]	graph method for network information security assessment	the complexity of calculating the proposed algorithm for generating an attack graph
[11]	Multicriterial decision method	Requires the creation of criteria for making a certain decision
[12]	hierarchical flow model method	the spread of the attack in the CIOI-CI network has not been analyzed
[13]	a method of searching for aggregation operators to create a classification of attacks on a specific system	requires constant updating of the database of information security threats

It is worth noting that a risk-based assessment of the level of information security is carried out on the example of a certain system. Also, during the analysis of the literature, the objects of research used to assess the level and risks of information security were identified. Table 2 presents various research objects used for research in [14-19].

Table 2 – Systems for assessing the level and risks of information security [14-19]

References	The object of the study
[14]	monitoring and data collection system
[15]	critical digital assets of nuclear power plants
[16]	Cyber-physical security systems
[17]	e-government websites
[18]	Internet of Things devices
[19]	Financial organizations

Along with the positive consequences, meeting the requires of community in the subject of information and communication technologies development entails an increase in the vulnerability of critical ICI facilities to cyber attacks. Given the ever-changing landscape of cyber threats, it is important that the country constantly ensures the cybersecurity of its information and communication technology infrastructure. Recently, cyberspace security has received much-needed emphasis from the government and international agencies. To ensure confidence, actions initiated by the country to counter cyber threats should be constantly evaluated for their implementation and effectiveness.

It is in the work [19] that the research is aimed at offering a new look at the comparative analysis and ensuring information security throughout the country. The article presents

a study and analysis of the methods and practices adopted by countries to assess the situation in the field of information security and create guarantees regarding the implemented information security measures. This paper examines the methods of assessing and ensuring information security used by 37 countries in order to understand the global scenario and identify various methods adopted to assess the state of information security.

In Kazakhstan, there is a methodology for assessing information security risks, including the order of ranking financial organizations by the degree of exposure to information security risks and rules for assessing the level of protection from information security threats.

The methodology for assessing information security risks described in [20] is intended for financial organizations that are not residents of the Republic of Kazakhstan. According to [20], the information security service of a financial institution in the Republic of Kazakhstan identifies the source of information security threats and vulnerabilities of critical information assets, assesses the amount of damage caused by information security threats. However, this methodology does not provide points regarding responding to information security threats in case of its occurrence/detection. It is worth noting that the untimely prevention of information security threats can lead to the penetration of intruders into the ICI of financial organizations, followed by causing enormous damage to the capital of individuals/legal entities.

At the moment, many financial organizations of the Republic of Kazakhstan are subject to phishing attacks, which clearly shows not a strong level of protection from information security threats. In accordance with [20], financial organizations, at the request of the authorized body, must assess the level of protection from information security threats. Nevertheless, practice shows that setting a certain regulatory period for conducting this assessment is more effective than on request. Also, the rules [20] do not specify further actions of the authorized body after the assessment in case of revealing a weak level of protection from threats to the information security of a financial organization.

In order to increase the effectiveness of the fight against cybercrime, developed countries have begun appropriate work to increase the security of their own information and telecommunications networks for general and special purposes. Current global trends in the spread of cybercrime and the activation of various attacks/threats to information security indicate the increasing importance of combating it and timely work to assess the level of security of the logistics from threats to information security. The current situation with cybercrime requires constant improvement of methods of combating cybercrime, the development of information systems, and methods aimed at ensuring information security in the country.

Conclusion. In this article, a systematic literature review of existing methods for assessing the level of information security of various systems was carried out, as well as an analysis of measures to ensure information security on the scale of financial organizations of the Republic of Kazakhstan. As can be seen from Table 2, methods for assessing the level and risks of information security have been most widely used in the field of finance, nuclear energy, cyber-physical security systems, e-government, and the Internet of things. The authors also formed a conclusion about the high relevance of research related to the assessment of the security of ICI from information security threats.

In addition, the results of the analysis showed the absence of a single standardized method for assessing the level of information security and security in various areas of communication. In this regard, further research to assess the level of information security will be conducted on the example of satellite communication systems.

As a result of the review, the following tasks were set for further research:

обзор review of existing methods for assessing the information security of objects of informatization of satellite communication systems;

determine the levels of the protected information;

to establish recommendations focused on improving measures to guarantee the information security of ICI facilities on the example of satellite communication systems;

research of increasing the level of information security of ICI facilities based on the developed evaluation method on the example of satellite communication systems.

REFERENCES

1 A.Boranbayev, S.Boranbayev, A.Nurusheva, K.Yersakhanov. (2018). The Modern State and the Further Development Prospects of Information Security in the Republic of Kazakhstan. 15th International Conference of Information Technology, Information Technology.

2 A. Boranbayev, S. Boranbayev, K. Yersakhanov, A. Nurusheva, and R.Taberkhan (2018). Methods of Ensuring the Reliability and Fault Tolerance of Information Systems. 15th International Conference of Information Technology, Information Technology.

3 Turskis, Z., Goranin, N., Nurusheva, A., Boranbayev S. (2019). Information Security Risk Assessment in Critical Infrastructure: A Hybrid MCDM Approach. Informatica.

4 Turskis, Z., Goranin, N., Nurusheva, A., Boranbayev S. A. (2019). Fuzzy WASPAS-Based Approach to Determine Critical Information Infrastructures of EU Sustainable Development. Sustainability.

5 Boranbayev A., Boranbayev S., Nurusheva A. (2018). Development of a software system to ensure the reliability and fault tolerance in information systems based on expert estimates. Advances in Intelligent Systems and Computing.

6 Boranbayev, A., Boranbayev, S., Nurusheva A., Yersakhanov K. (2018). Development of a Software System to Ensure the Reliability and Fault Tolerance in Information Systems. Journal of Engineering and Applied Sciences.

7 Boranbayev, S., Goranin, N., Nurusheva, A. (2018). The methods and technologies of reliability and security of information systems and information and communication infrastructures. Journal of Theoretical and Applied Information Technology.

8 Kitchenham, B., Charters, S. (2017). Guidelines for performing Systematic Literature Reviews in Software Engineering. EBSE Technical Report.

9 Zuiev P., Salnikova O., Mazulevskyi O., Shyshatskyi A., Shevchenko D., Shulhin A. (2020) Methods of cyber security assessment in the information and telecommunications system. International journal of advanced trends in computer science and engineering.

10 Wu S., Zhang Y., Cao W. (2017). Network security assessment using a semantic reasoning and graph based approach. Computers and Electrical Engineering.

11 Harjinder Singh Lallie, Kurt Debattista, Jay Bal A. (2020). Review of attack graph and attack tree visual syntax in cybersecurity. Computer science review.

12 Qianxiang Zhu, Yuanqing Qin, Chunjie Zhou, Li Fei (2019). Hierarchical flow model-based impact assessment of cyberattacks for critical infrastructures. IEEE systems journal.

13 Simon Miller, Christian Wagner, Uwe Aickelin, Jonathan M. Garibaldi (2016). Modelling cyber-security experts' decision-making processes using aggregation operators. Computers & Security.

14 Cherdantseva Y., 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.

15 Son J., Choi J., Yoon H. (2019). New Complementary Points of Cyber Security Schemes for Critical Digital Assets at Nuclear Power Plants. IEEE Access.

16 Ashibani Y., Mahmoud Q.H. (2017) Cyber physical systems security: Analysis, challenges, and solutions. Computers & Security.

17 Zhao JJ., Zhao SY. (2010) Opportunities and threats: A security assessment of state e-government websites. Government information quarterly.

18 Zolanvari M., Teixeira MA., Gupta L., Khan KM., Jain R. (2019). Machine learning-based network vulnerability analysis of industrial internet of things. IEEE internet of things journal.

19 Methodology for assessing information security risks, including the order of ranking financial organizations by the degree of exposure to information security risks // Resolution of the Board of the Agency of the Republic of Kazakhstan for Regulation and Development of the Financial Market dated November 23, 2020 No. 111

20 Rules for assessing the level of protection from information security threats // Resolution of the Board of the Agency of the Republic of Kazakhstan for Regulation and Development of the Financial Market dated November 23, 2020 No. 110

Ә. С. ӘБДІРАМАН, А. М. НУРУШЕВА, Л. С. АЛДАШЕВА

Л.Н.Гумилев атындағы Еуразия ұлттық университеті, Astana IT университеті
Нұр-Сұлтан қаласы, Қазақстан

АҚПАРАТТЫҚ-КОММУНИКАЦИЯЛЫҚ ИНФРАҚҰРЫЛЫМ ОБЪЕКТІЛЕРІНІҢ АҚПАРАТТЫҚ ҚАУІПСІЗДІК ДЕҢГЕЙІН БАҒАЛАУ ӘДІСТЕРІН ТАЛДАУ

Автоматтандырылған цифрлық технологиялар әлемінде кәсіпорынның басты міндеттерінің бірі ақпараттық қауіпсіздік шабуылдарын іске асырудың алдын алудың тиімді әдісін іздеу болып табылады. Осы мақсаттарға қол жеткізу барысында қазіргі уақытта бағалаудың әртүрлі әдістері қолданылады. Негізінде, кез-келген зерттеу зерттеу тақырыбының дамуына әдеби шолудан басталады. Сондықтанда, бұл мақала Scopus және Web of Science мәліметтер базасынан ғылыми материалдар негізінде құрылған жүйелердің ақпараттық қауіпсіздігін бағалаудың заманауи әдістеріне, құралдары мен стандарттарына әдеби шолу болып табылады. Сондай-ақ, ақпараттық-коммуникациялық инфрақұрылым объектілеріндегі ақпараттық қауіпсіздік деңгейін бағалаудың қолданыстағы әдістерін талдау қарастырылады. Әдебиеттерді шолу негізінде ақпараттық қауіпсіздік деңгейін бағалау әдістерін талдау ұсынылған. Бұл мақала ҚР Білім және ғылым министрлігінің 2022-2024 жылдарға арналған ғылыми және (немесе) ғылыми-техникалық жобалар бойынша жас ғалымдарды гранттық қаржыландыру шеңберінде AP13067916 гранттық жобасы шеңберінде ақпараттық жүйелердің ақпараттық қауіпсіздік деңгейін талдау бойынша зерттеу нәтижелері ретінде ұсынылған.

Түйін сөздер: *киберқауіпсіздік, бағалау әдістері, ақпараттық-коммуникациялық инфрақұрылым объектілері, КМАКИ, әсер ету, тәуекел.*

А. С. АБДИРАМАН, А. М. НУРУШЕВА, Л. С. АЛДАШЕВА

Евразийский национальный университет имени Л.Н.Гумилев, Astana IT университет
город Нур-Султан, Казахстан

АНАЛИЗ МЕТОДОВ ОЦЕНКИ УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ

В мире автоматизированных цифровых технологий одной из главных задач предприятия является поиск эффективного способа предотвращения реализации рисков информационной безопасности. В случае достижения этих целей в настоящее время используются различные методы оценки. По сути, любое исследование начинается с литературного обзора развития темы исследования. Следовательно, данная статья представляет собой литературный обзор современных методов, инструментов и стандартов оценки информационной безопасности систем, сформированных на основе научных материалов из баз данных Scopus и Web of Science. Также рассматривается анализ существующих методов оценки уровня информационной безопасности в объектах информационно-коммуникационной инфраструктуры. На основе обзора литературы представлен анализ методов оценки уровня информационной безопасности. Представлены результаты исследования по анализу уровня информационной безопасности информационных систем в рамках грантового финансирования молодых ученых по научным и (или) научно-техническим проектам на 2022-2024 годы Министерства образования и науки РК, номер гранта AP13067916.

Ключевые слова: *кибербезопасность, методы оценки, объекты информационно-коммуникационной инфраструктуры, КВОИКИ, воздействие, риск.*