Information Technology of Information Security Audit of Objects of Critical Infrastructure

Igor Kozubtsov[a], Nataliya Lishchyna[b], Lesia Kozubtsova[a], Igor Trush[c], and Andrii Yashchuk[b]

[a] *Military Institute of Telecommunications and Informatization named after Heroes of Kruty, 45/1 Moscow str., 01011, Kyiv, Ukraine*
[b] *Lutsk National Technical University, 75 Lvivska str., 43000, Lutsk, Ukraine*
[c] *Legistation Institute of the Verkhovna Rada of Ukraine, 4 Nestorivsky prov., 04053, Kyiv, Ukraine*

Abstract

Context. The scientific and practical task to substantiate the mathematical apparatus on the basis of which the information technology of information security audit of critical infrastructure is developed, which provides verification of compliance of critical infrastructure with the general requirements approved by the Cabinet of Ministers of Ukraine dated 2019-06-19, No.518. A security audit is one of the most effective measures to increase the level of information security of the critical infrastructure. Objective. The purpose of the work is to create information security audit of critical information infrastructure on the basis of separate partial solutions of information technology. Method. On the basis of the general requirements defined by the Resolution of the Cabinet of Ministers of Ukraine dated 2019-06-19, No.18 "On approval of the General requirements for cyber protection of critical infrastructure objects" a set of indicators and evaluation criteria was proposed. The structure of future information technology was offered. In accordance with the structure of information technology, the stages of the methodology of information security audit of critical infrastructure were built. The technique contains a simple mathematical apparatus that simplifies calculations even in Microsoft Excel spreadsheets. In this paper, in contrast to the known methods and techniques, it is proposed to take into account the weight of the importance of information security requirements. As a result, the method has become sensitive to the most critical requirements for cybersecurity of critical infrastructure. Results. Information technology of information security audit of critical information infrastructure objects has been developed. Conclusions. The experiments in Microsoft Excel spreadsheets confirm the efficiency of the proposed method. It is advisable to recommend the development of software that would in practice automate the process of information security audit of critical information infrastructure. The scientific novelty of the obtained result is that for the first time the information technology of information security audit of critical infrastructure facilities was developed, which provides verification of compliance of critical infrastructure facilities with the general requirements approved by the Cabinet of Ministers of Ukraine dated 19 June 2019, No.518. The practical significance of the work lies in the possibility of developing information technology software. Prospects for further research in this area. The presented study does not cover all aspects of this problem. Theoretical and practical results obtained in the process of scientific research are the basis for further study in such areas as the development of information technology software.

Keywords

Information technology, audit, information security, critical infrastructure facility.

Emerging Technology Trends on the Smart Industry and the Internet of Things, January 19, 2022, Kyiv, Ukraine
EMAIL: kozubtsov@gmail.com (I. Kozubtsov); lischyna@gmail.com (N. Lishchyna); l.kozubtsova@gmail.com (L. Kozubtsova); trysh_iv@ukr.net (I. Trush); xxxxandyxxxx@gmail.com (A. Yashchuk)
ORCID: 0000-0002-7309-4365 (I. Kozubtsov); 0000-0002-5200-536X (N. Lishchyna); 0000-0002-7866-8575 (L. Kozubtsova); 0000-0002-5340-3212 (I. Trush); 0000-0003-4872-7949 (A. Yashchuk)

1. Introduction

Cybersecurity is a state of protection of critical objects of national infrastructure and its individual components, which ensures their sustainable functioning and development, timely detection, prevention and neutralization of cyber threats in the interests of man, society and state.

According to current practice, cybersecurity of objects of critical infrastructure (OCI) is not a constant value over time. The cybersecurity of the OCI is a function of a number of random parameters, namely the availability of a cybersecurity system, staffing, and the frequency of new cyber threats. There is a constant cyber confrontation between the security system and the stakeholder "Threat Agents" [1].

Security audit of the information security is a systematic process of obtaining objective qualitative and quantitative assessments of the current state of information system security, a comprehensive assessment of the level of information security of the client, taking into account three main factors: personnel, processes and technologies.

Independent information security audit at critical infrastructure facilities (hereinafter - independent audit) is a systematic, independent and documented process of assessing the state of information security at critical infrastructure facilities, based on legal requirements, national standards and recommendations of international information security standards.

A regular information security audit is needed in order to assess the real state of security of OCI resources and its ability to withstand external and internal threats to information security, which are constantly changing and adapting.

2. Problem Statement

In order to ensure compliance with the Law of Ukraine "On Basic Principles of Cyber Security of Ukraine", it is recommended to conduct a scheduled and unscheduled independent audit of information security of OCI on the effectiveness of cybersecurity. In accordance with the second part of Article 6 of the Law of Ukraine "On Basic Principles of Cyber Security of Ukraine", the Cabinet of Ministers of Ukraine resolves: paragraph 7. If the critical information infrastructure does not process state information resources or information with limited access, the protection requirement of which is established by law, the provisions of these General Requirements are taken into account during the creation (modernization) of the information security system of the critical infrastructure object. Compliance with the General Requirements is verified during an independent information security audit of the critical infrastructure.

Thus, the owner and/or manager of a critical infrastructure facility is obliged to organize and conduct an independent information security audit at the critical infrastructure facility in accordance with the requirements of the legislation in the field of information protection and cybersecurity.

According to the provisions of the National Security Strategy of Ukraine, the Concept of Development of the Security and Defense Sector of Ukraine [2, 33], the Law of Ukraine "On Basic Principles of Cyber Security of Ukraine" [3];

Cybersecurity Strategies of Ukraine [4];

Decision of the National Security and Defense Council of Ukraine dated 2017-07-10 "On the status of implementation of the decision of the National Security and Defense Council of Ukraine dated 2016-12-29", "On threats to cybersecurity and urgent measures to neutralize them" [5].

Therefore, solving the scientific problem of the demand to conduct an audit of OCI in compliance with the general requirements of the Cabinet of Ministers of Ukraine dated 2019-06-19, No.518 "On approval of the General requirements for cyber protection of critical infrastructure" [6] is currently considered relevant.

3. Review of the Literature

This work is also aimed at implementing urgent public policy measures to neutralize object of critical information infrastructure (OCII) threats [5], which could lead to negative consequences, as predicted

in the description “Future Security Environment 2030” [7].

In general, research and publications on the problem of information security audit are devoted to a relatively large number of works, among which, in our opinion, the following deserve attention.

In [8] the peculiarities of building the methodology of information security audit in modern conditions are presented.

In [9] the method of information security audit is described.

In [10] the methods of information security audit of information systems that process personal data in non-state military pension funds are revealed.

In [11], the authors proposed a method for assessing the stability of the OCII, which operates in cyberspace.

In [12] the problem of developing a methodology for assessing the cyber security of the communication system of the organization was solved.

In [13] the authors developed a method of auditing information objects for information security requirements. The methodology is based on a combination of techniques that use quantitative and qualitative criteria as parameters for assessing security.

The monograph [14] describes the procedure for conducting security audits of information systems.

The monograph [15] considers the audit of critical infrastructure security by special information influences.

The monograph [16] describes the types of internal control, security and integrity procedures that management should incorporate into its automated systems. This book provides auditors with the guidance they need to keep their systems safe from both internal and external threats.

The monograph [17] outlines a systematic process of creating a virtual environment for the practice of penetration testing. The author gives examples of creating a network architecture that allows you to test almost any environment.

There is no doubt that the implementation of the requirements presented in the documents [6] requires a method of independent information security audit, which takes into account the main aspects of OCI information security, and in these works there is no mathematical apparatus of calculation. In addition, the practical result of solving the scientific problem should be information technology audit of information security of critical information infrastructure.

The purpose of the article is to develop information technology of audit of information security of objects of critical information infrastructure on the basis of separate partial decisions.

4. Materials and Methods

According to the State standard of Ukraine DSTU 2392-94 [18] “information system” is a communication system that provides collection, retrieval, processing and transmission of information.

The Law of Ukraine “On Information Protection in Information and Telecommunication Systems” defines an information (automated) system as an organizational and technical system in which information processing technology is implemented using technical and software tools [19].

According to ISO / IEC 2382: 2015 [20] “information system – a system designed for storage, retrieval and processing of information, as well as relevant organizational resources (human, technical, financial, etc.) that ensure the dissemination of information”.

Information technology is a set of methods, tools, techniques that provide search, collection, storage, processing, presentation, transmission of information between people.

Information technology is a process that can be implemented by means of computer technology, which will ensure compliance with the requirements for the search, presentation, conversion and transmission of information, ie processes that implement human information activities. Schematically, the components of information technology are presented in Figure 1.

The main components of the proposed information technology are hardware (personal computer, multimedia, etc.), software and organizational and methodological support.

Information technology provides the implementation of the following interconnected processes in the form of algorithm stages:

- Stage 1 search, collection and storage of information
- Stage 2 information processing

- Stage 3 displaying information

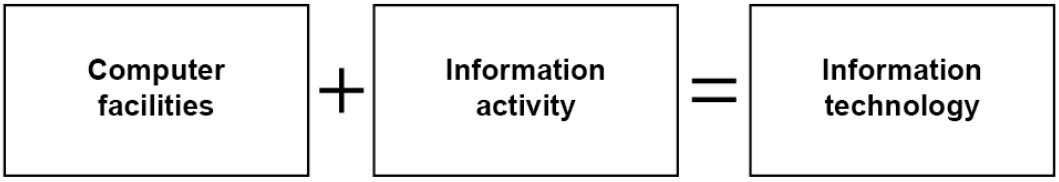

Figure 1: Components of classical information technology

Each stage of the information technology process is important for the correctness of the functional operation of the designed information system. According to the results of the application of information technology, it is necessary to find numerical values: $K_{IS}N$ and $K_{IS(OCII)}$.

Nomenclature

W_{Kj} – components (K_j) as part of the object of inspection of OCII;

W_{Vi}. – weighting significance of information security requirement;

$V1 \ldots VN$ – general information security requirements;

$K_{IS}N$ – пан indicator of the effectiveness of cybersecurity on the component of the object of verification of OCII;

$K_{IS(OCII)}$ – an indicator of the effectiveness of cybersecurity at the object of inspection of OCII;

m – the number of components (K_j) of the object of inspection of OCII;

VN – the number of general information security requirements;

VN_1 – the number of general requirements VN that take the value "1";

VN_0 – the number of general requirements VN that take the value "0" for the component of the test object of OCII.

Stage 1 Search, collection and storage of information.

Choice of evaluation indicators. The indicators assessed by the independent audit committee for compliance with the objects of inspection are defined in the requirements [3], namely:

$K_{IS}1$ – fulfillment of the requirement for mandatory formation of a general information security policy at the OCI (V1);

$K_{IS}2$ – fulfillment of the requirement for mandatory implementation of user and administrator access control to OCII OCI (V2) security objects;

$K_{IS}3$ – compliance with the requirement for mandatory identification and authentication of OCII OCI users and administrators (V3);

$K_{IS}4$ – compliance with the requirement for mandatory registration of events by OCII OCI components and their periodic audit (V4);

$K_{IS}5$ – compliance with the requirement for mandatory network protection of components and information resources OCII OCI (V5);

$K_{IS}6$ – compliance with the requirement for mandatory availability and resilience of components and information resources OCII OCI (V6);

$K_{IS}7$ – fulfillment of the requirement to determine the conditions for the use of removable (external) devices and media on OCII OCI (V7);

$K_{IS}8$ – compliance with the requirement to determine the conditions of use of software and hardware OCII OCI (V8);

$K_{IS}9$ – compliance with the requirement to specify the conditions for the placement of OCII OCI components (V9).

Collection of source data. The stage of collecting audit data is quite complex and extremely important. Competent conclusions about the current position of information security at the OCII OCI can be made by the auditor only if all the necessary input data are available for analysis. Obtaining information about the organization, operation and current state of the OCII OCI is carried out using:

- providing questionnaires to be filled out by the customer's employees;
- interviewing the customer's employees who have the necessary information;
- analysis of existing organizational and technical documentation used on OCII OCI.

Audit (passive) information security OCII is carried out as of time t_0, when the destructive information

impact is absent: *DII* = 0.

The information security audit of OCI is performed by questioning the persons responsible for the operation and information security.

Questionnaire questions are developed on the basis of current general requirements for cybersecurity of critical infrastructure [6].

Stage 2 Information processing.

Evaluation criteria must be specified before processing. The criterion for evaluating the results of an independent information security audit of OII is the effectiveness of the implementation of measures at the inspection sites, which should perform the target function under the conditions of destructive information impacts $K_{IS(OCII)}$, see table.1.

Table 1

Information security criteria

Criteria	Level
$0,9 \le K_{IS(OCII)}(t) < 1,0$	Highest
$0,7 \le K_{IS(OCII)}(t) < 0,9$	High
$0,5 \le K_{IS(OCII)}(t) < 0,7$	Medium
$0,3 \le K_{IS(OCII)}(t) < 0,5$	Low
$0 \le K_{IS(OCII)}(t) < 0,3$	Lowest

Calculation of the effectiveness of information security on the component of the object of verification $K_{IS}N$.

1) the requirements V1… VN are distributed for each component of the object of inspection (*Kj*) OCII;

2) the implementation of the requirements (V1… VN) on each component of the object of verification (*Kj*) OCII OCI is checked;

3) the audit committee carries out the audit as on each component of the object of audit (*Kj*) OCII OCI implemented measures defined in the requirements (V1… VN)

The value of information security efficiency on each component of the object of verification (*Kj*) OCII OCI takes the value of $K_{IS}N$ [0; 1] under the following conditions, if:

partial requirements are implemented on each component of the OCII test object (*Kj*), then (V1) = "1", otherwise (V1) = "0" requirements are not implemented.

Quantity (VN) for different components of the test object (*Kj*) OCII OCI has a different number.

The results of the calculations are listed in table 2

Table 2

Matrix of indicators (VN) for different components of the test object (K_j) OCII OCI

The component of the tool	The value of the partial requirement (VN)					*VN*
	1	2	3	…….	*N*	
Component of the test object No.1	0	1	1	…….	0	VN_1+VN_0
Component of the test object No.2	1	1	1		1	VN_1+VN_0
Component of the test object No.3	1	0	0		0	VN_1+VN_0
……	…..	……	….	……	……	VN_1+VN_0
Component of the test object No.*N*	1	0	1	…….	0	VN_1+VN_0

The value of $K_{IS}N$ is calculated by formula (1):

$$K_{IS}N = \frac{\sum_{i=1}^{N} VN_1}{\sum_{i=1}^{k}(VN_0 + VN_1)} = \frac{\sum_{i=1}^{N} VN_1}{VN}, \quad (1)$$

where *VN* – the number of general information security requirements; VN_1 – the number of general requirements *VN* that take the value "1"; VN_0 – the number of general requirements *VN* that take the value "0" for the component of the test object of OCII.

The results of the calculations are listed in table 3.

Table 3
Calculation results

No.	Components	K_j	
		$K_{IS}N$	W_{Vi}.
1	Component of the test object No.1		
2	Component of the test object No.2		
..	……	….	…
K	Component of the test object No.*N*		

Calculation of the overall effectiveness of information security at the object of verification $K_{IS(OCII)}$ at time t_0.

The quantitative indicator for assessing the information security of a complex system is $K_{IS(OCII)}$ – the probability that in a complex system, all components will be protected from cyber interference and will operate normally.

The Information Security Performance Indicator $K_{IS(OCII)}$ is generally calculated according to formula (2) as a weighted and standardized assessment of the cyber security performance of all components of a complex system.

$$K_{IS(OCII)} = \frac{\sum_{i=1}^{m}(K_{IS}N \times W_{Vi})}{m}. \quad (2)$$

where *m* – the number of components (K_j) of the object of inspection of OCII;

Step 3 Displaying information.

The results of the independent OCI information security audit are recorded in the protocols, which record the results of tests for compliance with current legislation of Ukraine and draw a conclusion on the effectiveness of information security at the OCI. The generalized results of the protocols are formalized by the act of compliance with information security on the OCI and the effectiveness of cybersecurity.

5. Experiments

The general scheme of the experimental setup, which implements the information technology of information security audit of critical information infrastructure objects according to the ideology in Fig. 1 includes:

- computer (laptop);
- Microsoft Excel software, version higher than 2000;
- programmed calculation file.

The initial data are:

- the list of general requirements for cyber protection of critical infrastructure is formed on the basis of the Resolution of the Cabinet of Ministers dated 2019-06-19, No.518 “On approval of the General requirements for cyber protection of critical infrastructure” [6];
- weighting factors of information security requirements (WVi);
- *m* is the number of components (K_j) in the OCII OCI object.

As a result of the verification of compliance with the requirements, the following values are calculated:

- number of general information security requirements (VN);
- the number of VN1, which takes the value “1”;
- the number of requirements VN0, which takes the value “0”.

Conditions and procedure for conducting an independent information security audit. The algorithm of information activities of the audit committee is presented in Table 4 (abbreviations:

ROCII OCI is responsible for the object of critical information infrastructure of an object of critical infrastructure;

SAOCII OCI is a system administrator of the object of critical information infrastructure of an object of critical infrastructure;

CIISAC is a chairman of the Independent Information Security Audit Commission;

MC1-CN are members of the independent information security audit commission;

P1-P9 are audit protocols;

V1-V9 are general requirements for cybersecurity of critical infrastructure.

6. Results

The paper presents a structured methodology for information security audit with a description of each of the stages.

The result of an independent OCI information security audit is considered positive if the objects of the inspection comply with the requirements of the Law of Ukraine "On Basic Principles of Cyber Security of Ukraine" and ensure effective use of the information security system within certain standards. Based on the results of the evaluation, a general conclusion is made on the effectiveness of the information security measures implemented at the inspection facilities of OCI.

Table 4

Algorithm of information activity of the audit commission

No.	Name of works	Algorithm of actions of the audit commission	
		Responsible	The result of actions
1	Organizational	ROCII OCI	orders the establishment of a general independent audit committee composed of representatives of the independent organization and the owner OCII
2	The beginning of the audit committee	CIISAC	informs MC1-CN about the features. Instructs MC1-CN to begin an audit of the audit facility of OCII
3	Testing No.1	CIISAC MC1-CN SAOCII OCI	questionnaire (testing) of the verification object of OCII for compliance with the requirements of V1. As a result, the audit report (P1) is drawn up
4	Testing No.2	CIISAC MC1-CN SAOCII OCI	questionnaire (testing) of the verification object of OCII for compliance with the requirements of V2. As a result, the audit report (P2) is drawn up
5	Testing No.3	CIISAC MC1-CN SAOCII OCI	questionnaire (testing) of the verification object of OCII for compliance with the requirements of V3. As a result, the audit report (P3) is drawn up
6	Testing No.4	CIISAC MC1-CN SAOCII OCI	questionnaire (testing) of the verification object of OCII for compliance with the requirements of V4. As a result, the audit report (P4) is drawn up
7	Testing No.5	CIISAC MC1-CN SAOCII OCI	questionnaire (testing) of the verification object of OCII for compliance with the requirements of V5. As a result, the audit report (P5) is drawn up
8	Testing No.6	CIISAC MC1-CN SAOCII OCI	questionnaire (testing) of the verification object of OCII for compliance with the requirements of V6. As a result, the audit report (P6) is drawn up
9	Testing No.7	CIISAC MC1-CN SAOCII OCI	questionnaire (testing) of the verification object of OCII for compliance with the requirements of V7. As a result, the audit report (P7) is drawn up
10	Testing No.8	CIISAC MC1-CN SAOCII OCI	questionnaire (testing) of the verification object of OCII for compliance with the requirements of V8. As a result, the audit report (P8) is drawn up
11	Testing No.9	CIISAC MC1-CN SAOCII OCI	questionnaire (testing) of the verification object of OCII for compliance with the requirements of V9. As a result, the audit report (P9) is drawn up

12	Calculating	MC1-CN SAOCII OCI	calculation of the coefficient of efficiency of information security on OCII. The result is a numerical value of the total efficiency factor of information security on the OCII
13	Drawing up an act	CIISAC MC1-CN SAOCII OCI	draft act of compliance of information security on OCII and efficiency of information security
14	Signing the act	CIISAC ROCII OCI	signing of the audit report by all parties

To increase the information security of OCII OCI, it is recommended to use information technology audit of information security of critical infrastructure objects according to the PDCA scheme (Plan, Do, Chek, Act). The influence of the frequency of the audit on the level of compliance is shown in (Fig. 2).

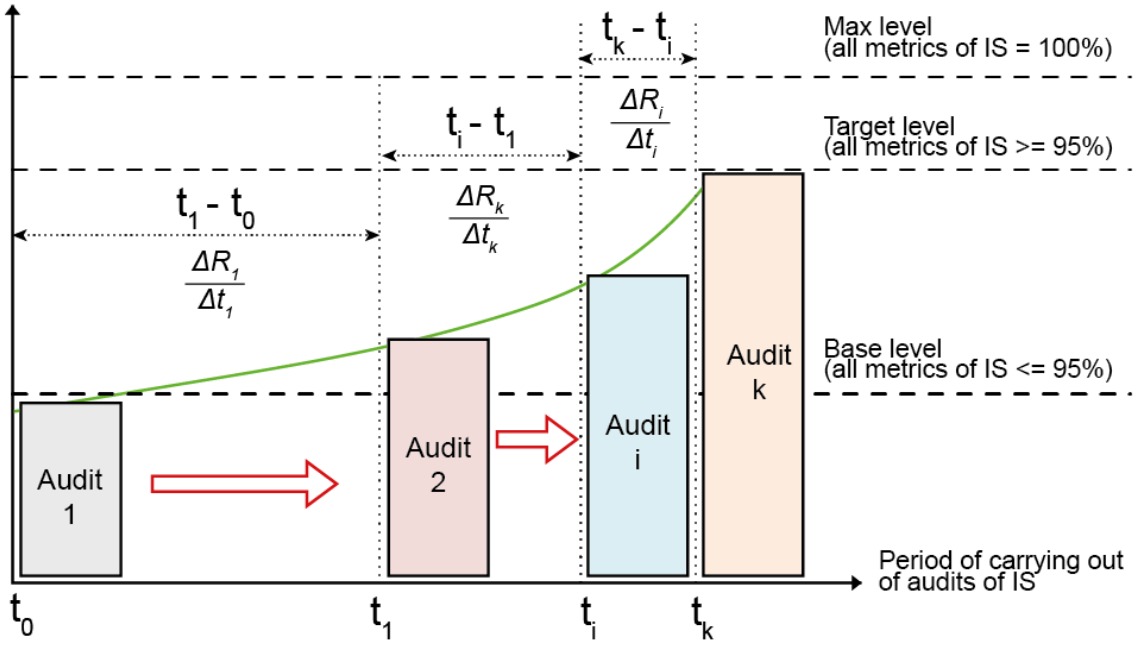

Figure 2: Influence of audit frequency on the level of compliance

Important factors for successful evaluation of audit results are:

- awareness and motivation of the management (owner) of the OCII OCI;
- confidentiality;
- trust.

7. Discussion

A debatable issue in the development of information technology audit of information security of critical information infrastructure, which provides verification of compliance of critical information infrastructure with the general requirements approved by the Cabinet of Ministers of Ukraine dated 2019-06-19, No.518, is the choice of weighting of information security requirements W_{Vi}.

It should be noted that in the review of the scientific literature on the problem of developing methods of information security audit [8 – 13] in similar decisions, when the generalized indicator is calculated, it is not taken into account the weight of the importance of information security requirements. In contrast to these works, in the actual work for the first time it is proposed to take into account the weighting significance of the information security requirement W_{Vi}.

In this version of information technology, it is proposed to assign a weighting factor by expert method, which requires prior approval of this value before the audit.

8. Conclusions

Therefore, security audit is one of the most effective measures to increase the level of information security of critical infrastructure.

The scientific and practical problem of substantiation of the mathematical apparatus is solved in the work and on its basis the information technology of audit of information security of objects of critical infrastructure is created. This information technology allows to check the compliance of critical infrastructure facilities with the general requirements approved by the Resolution of the Cabinet of Ministers of Ukraine dated 2019-06-19, No.518.

The scientific novelty of the result is that for the first time the information technology of information security audit of critical infrastructure facilities was developed, which provides verification of compliance of critical infrastructure facilities with the general requirements approved by the Cabinet of Ministers dated 2019-06-19, No.518.

The practical significance of the work lies in the possibility on the basis of the proposed mathematical apparatus to develop special information technology software.

Prospects for further research in this area. The presented study does not cover all aspects of this problem. Theoretical and practical results obtained in the process of scientific research are the basis for its further study in such areas as the development of information technology software.

9. Acknowledgements

The study was conducted by the authors on their own initiative. Funding was provided at their own expense.

10.References

[1] V.I. Slipchenko, Wars of the sixth generation weapons and military art of the future, Moscow, Veche, 2002.

[2] A. G. Petrenko, Action Plan for the implementation of defense reform in 2016-2020 (roadmap for defense reform), Kiev, DVPSP and MS of the Ministry of defense of Ukraine, 2016.

[3] Law of Ukraine "On basic principles of ensuring cybersecurity of Ukraine". URL: https://zakon.rada.gov.ua/laws/show/2163-19.

[4] On the decision of the national security and Defense Council of Ukraine of January 27, 2016 "On the cybersecurity strategy of Ukraine", approved by Presidential Decree No. 96/2016 of 15.03.16. URL: https://zakon5.rada.gov.ua/laws/show/96/2016.

[5] Decision of the national security and Defense Council of Ukraine of 10.07.17 "On the status of implementation of the decision of the national security and Defense Council of Ukraine of December 29, 2016" "On threats to state cybersecurity and urgent measures to neutralize them", put into effect by Presidential Decree No.254/2017 of 13.02.17. URL: https://zakon.rada.gov.ua/laws/show/n0006525-17.

[6] Resolution of the Cabinet of Ministers of Ukraine No. 518 of 19.06.19 "On approval of general requirements for cyber protection of critical infrastructure facilities". URL: https://zakon.rada.gov.ua/laws/show/518-2019-п.

[7] I. M. Kozubtsov, L. M. Kozubtsova, Forecast of possible consequences of the onset of "collapse of special purpose information systems", Actual problems of information security management of the state: sat. abstracts of scientific documents, Nauk. - prakt. conf. (Kiev, March 26, 2021), Kiev, on the SBU, 2021, pp. 50-53.

[8] M.A. Egorov, Methods of information security audit in modern conditions, Bulletin of Science and Education, 2019, 11(65), 2, pp. 34-37.

[9] A. A. Zamula, K. I. Ivanov, V. I. Chernysh, B.V. Volobuev, Methodology of information security audit, Radio Engineering, 2012, 168, pp. 83-86.

[10] E. V. Ermakova, Methodology of information security audit of personal data information systems in non-state pension funds, International Scientific Journal “Young Scientist”, 2016, 3(107). pp. 92-95.
[11] R. I. Zakharchenko, I. D. Korolev, Methodology for assessing the stability of the functioning of objects of critical information infrastructure functioning in cyberspace, Vol. 10. High-tech technologies in space research of the Earth, 2018, 2, pp. 52-61.
[12] I. M. Kozubtsov, L. M. Kozubtsova, V. V. Kutsaev, T. P. Tereshchenko, Metodika otseniya cybernetic Zahi-schist sistemy Svyaznoy organizatsii [methodology for evaluating the cybernetic security of the organization's communication system], 2018, 1 (31), pp. 43-46.
[13] A. P. Nyrkov, S. A. Rudakova, Methodology of audit of informatization objects according to information security requirements, Bulletin of the Admiral S. O. Makarov State University of the Sea and River Fleet, 2012, 3 (15), pp. 146-149.
[14] N. Skobtsov, Information systems security audit. St. Petersburg, Petersburg, 2018.
[15] S. I. Makarenko, Security audit of critical infrastructure by special information impacts. Monograph, St. Petersburg, Science-intensive technologies, 2018.
[16] R. Moeller, IT Audit, Control, and Security. Hoboken, John Wile & Sons Inc., 2010.
[17] K. Cardwell, Building Virtual Pentesting Labs for Advanced Penetration Testing, Packt Publishing, 2014.
[18] DSTU 2392-94 “Information and documentation. Basic concepts”, Kiev, UkrNDISSI, 1994.
[19] Law of Ukraine “On information protection in information and telecommunications systems” of 05.07.1994, No. 80/94-BP, Verkhovna Rada of Ukraine. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр.
[20] GOST 33707-2016 (ISO/IEC 2382:2015) Information Technologies (ICS).