ORGANIZATIONAL AND ANALYTICAL SUPPORT FOR CONDUCTING EXTERNAL AUDITS OF DATA PROTECTION SYSTEMS IN INSTITUTIONS

MYKOLA MASESOV[1], OLEG DIEGTIAR[1], DMYTRO MINOCHKIN[2], ANDRII KHAPSALIS[1], DMYTRO NOVYTSKYI[1], SERGII KRAMARENKO[3]

[1]Scientific Center of Communication and Information Technologies, Kruty Heroes Military Institute of Telecommunications and Information Technologies, Kyiv, Ukraine.

[2]Department of Telecommunication, Institute of Telecommunication Systems of National Technical University of Ukraine "Igor Sikorsky Kyiv Politechnic Institute", Kyiv, Ukraine.

[3]Interdisciplinary Research Institution Digitalization and AI, Kyiv, Ukraine.

E-mail: [1]mykola.masesov@viti.edu.ua

ABSTRACT

The main goal of information security is to protect information and related infrastructure from damage that may arise as a result of loss, alteration, or unauthorized distortion of information, whether due to criminal attempts or accidental actions. In such cases, the goal is to minimize the damage that may be caused by such circumstances. From time to time, it is also advisable to conduct an independent assessment of the information security in place at the organization. Such audits work at the level of actual protection and response to risks that are constantly changing. An audit is, in essence, an indispensable source of further recommendations for the design and modernization of protection systems to ensure compliance with standards. This article outlines the main stages of the methodology for developing an analysis of the effectiveness of information security measures in organizations, although some of the proposed indicators require serious refinement, which opens up new opportunities for further scientific research.

Keywords: *Independent Information Security Audit, Information Security Auditor, Information Security Assessment, Cybersecurity Assessment*

1. INTRODUCTION

If the computer is not properly protected and exchanges data with other devices, for example, when browsing the Internet, the likelihood of infection by malicious software (i.e., viruses, Trojans, spyware, adware, etc.) becomes almost inevitable. This, in turn, can lead to a significant decrease in performance or complete loss of control over the computer. In particular, hackers can use an infected computer to scan hard drives for confidential information such as bank details, record keystrokes to steal passwords, launch targeted DDoS attacks, DDoS attacks on selected targets, or encrypt data and then demand a ransom for its disclosure.

An organization's information system is a set of hardware and software designed to process, store, input, and output information resources. Information processing machines include computers, network equipment, printers, servers, and all types of technical equipment and hardware. Information is transferred within the system via a local or global network. A local area network (LAN) of a particular organization is a system subordinate to a central information processing center that serves to perform the tasks of the institution. Such networks are based on a closed architecture with significantly restricted external access. Restrictions on access to data in such a network are implemented through user administration tools. Information security in local networks is ensured by appointing responsible persons, access control systems, virtual private networks (VPN), etc. The main requirements for the design of local networks are availability, redundancy, and fast system response to user requests.

The reliability of computer systems, as well as the programs and networks that support them, particularly with regard to information security, is a concern not only for individual specialists, but also for researchers in the field of telecommunications and digital information technology. When administering network systems or protecting IT systems and information components of systems, their infrastructure emphasizes that existing systems and modern means of information protection, the quality of their design, and interaction with the user also require considerable effort. That is why the development of new automated information protection tools, protected from accidental or unauthorized prior intervention, is necessary given the current state of progress in this sensitive period of time.

Information security (IS) is, first and foremost, the state of information that ensures the confidentiality, integrity, and availability of the data it contains. The definition of the term IS is based on the system and, on the one hand, on all attempts to access (unauthorized interference, viewing, modification) information resources. The term IS covers actions aimed at preventing the cancellation or inaccessibility of management objects and cargoes that form information resources.

A problematic area of research is the insufficient effectiveness of existing mechanisms for auditing and verifying data protection systems in institutions, particularly in the field of critical infrastructure. Despite the existence of general requirements and standards (NIST, ISO/IEC 27001), they often leave institutions with a wide scope for interpretation, which complicates the unified assessment of risks and creates the risk of a formal approach to audits. Accordingly, the research questions are:

– Which organizational and analytical indicators most adequately reflect the actual state of an institution's information security?

– How can qualitative and quantitative methods be combined for independent auditing?

– Which indicators should be used to assess the effectiveness of technical, organizational, and personnel measures?

For effective functioning, it is advisable to create a system of addressing and zoning programs, which should include various forms of information, structurally combined by computer means and information technologies. In emerging situations, one of the main tasks of reification is to prevent potential losses of information resources that may be affected by external parties [1].

In the context of information security, the concept of threat refers to a set of factors or conditions that could disrupt the stable functioning of an information system. A threat, in general terms, is a potential action, event, or phenomenon that could harm the interests of a user, organization, or society.

Every object related to information security is necessarily subject to certain threats. Such threats can arise both during the interaction of different system components and as a result of external influences. Their nature can be accidental or intentional, but it is the deliberate actions of malicious actors that pose the greatest danger in terms of possible consequences [2].

System vulnerability is a state in which an information system is unable to effectively counteract the impact of certain threats or a combination of threats. In other words, it refers to the presence of weak points in the digital infrastructure through which its functioning can be deliberately disrupted or damaged. Such weak links can arise from errors in the code, miscalculations during architectural design, unreliable credentials, and the introduction of malicious software, such as viruses, scripts, or SQL injections.

In addition, any computer system, like any of its information security objects, can be exposed to various threats due to existing vulnerabilities. To minimize the risks associated with breaches of confidentiality and data unavailability, it is advisable to conduct regular information security audits.

When developing a comprehensive system of adequate protection, the system has the right to justify the introduction of both more secure methods and the inclusion of certain requirements from the basic list. For organizations to exist in Ukraine, independent information security assessments must be conducted. In accordance with the law, the information security project set out in Section 3 of Article 6 of Resolution No. 518 of the Cabinet of Ministers of Ukraine dated June 19, 2019, defines general requirements for the cybersecurity of critical infrastructure, and the authors propose that such assessments be conducted primarily in critical infrastructure and for all others as determined by the relevant regulatory authorities.

2019, defines the general requirements for cybersecurity of critical infrastructure, and the authors suggest that such assessments should be carried out primarily in critical infrastructure, and for all others – as determined by the management of each individual stabilization [3].

When conducting an IISA in an institution, it is important to assess in detail the usefulness and effectiveness of compensatory measures aimed at eliminating or mitigating threats and risks. Such an audit, conducted on a regular basis, is self-evidently important as it allows for a timely assessment of the actual state of cybersecurity of an institution exposed to various external and internal risks. A dynamic approach to information security in an institution requires active measures to protect confidential information, as the requirements for maintaining an adequate level of information security stem from objective factors. With this in mind, the authoring team has developed a methodology for independent auditing of cybersecurity systems in an organization, which allows assessing the effectiveness of cybersecurity implemented in the institution.

2. DEFINITION OF RESEARCH PROBLEM

In the spectrum of modern information technologies, the issue of information security has been relevant in the past. There are conceptual works on information security (IS) auditing in organizations, including its typology and key stages of implementation [4].

However, there are not many systematic studies on the comprehensive analysis of information resource security for its measurement based on objective data obtained from audits. The relevance of implementing independent information security auditing (ISA) is motivated by the legislative framework of Ukraine and draft documents that are currently being agreed upon.

Among these documents, the following should be highlighted:

1. Resolution of the Cabinet of Ministers of Ukraine No. 518 of June 19, 2019, “On Approval of General Requirements for Cyber Protection of Critical Infrastructure Objects” [3].
2. Resolution of the Executive Board of the National Bank of Ukraine No. 4 of January 16, 2021, “On Approval of the Regulations on Control over Banks' Compliance with the Requirements of Legislation in the Field of Information Security, Cyber Security, and Electronic Trust Services” [5].
3. Draft Resolution of the Cabinet of Ministers of Ukraine “On Certain Issues of Independent Audit of Information Security of Critical Infrastructure” dated July 1, 2021 [6].

As a rule, modern standards in the field of information security are rather general and conceptual in nature, which allows their initiators to independently choose methods, technical solutions, and means that are best suited to the identification, analysis, and management of risks. Standards in this area allow for both qualitative and quantitative risk assessments, but there is almost always a lack of specific questions and well-founded recommendations for choosing a framework, which Grundler offers as “mathematical” or methodological documents [7].

Vulnerabilities and their weaknesses can be assessed using an analysis method that is modified into three classes:

1. Qualitative classifications include vulnerability criticality levels: low, medium, or high. These were recently defined in the NIPC system, the SANS cybersecurity framework, and their Microsoft certification [8], [9].
2. Statistical – quantitative assessment criteria within classifications: PCI/DSS or NIST cybersecurity framework, US-CERT water assessment [10].
3. Model – combined – aggregation of data obtained for more in-depth analysis based on information accepted by technical management over time: CVSS (Common Vulnerability Scoring System), m/circle [11].

Each ranking system emphasizes different characteristics of vulnerabilities. For example, CVSS, as an open standard, allows formalizing threats to a computer system on a scale from 0 to 10, where 10 points are assigned based on three key indicators. However, this model has limitations: it does not take context into account, and vulnerabilities are assessed using a simplified direct damage accounting system [12].

The US-CERT system assesses, in particular, the threat to the Internet infrastructure and the conditions of its use in relation to vulnerabilities. US-CERT operates on a broader scale from 0 to 180 points. The SANS Institute conducts a series of tests, regardless of whether standard settings are used on both the client and server sides. Microsoft is also keeping pace by developing its own model that focuses on the number of negative consequences that could result from the potential exploitation of a vulnerability [13].

The purpose of this article is to describe the main stages of the IISA methodology in an institution based on the definition of information security indicators, as well as to formulate general recommendations for the head of an institution on conducting an IISA [14].

Therefore, the relevance of this scientific research is determined not only by the growth of cybercrime, but also by the requirements of Ukrainian regulatory and legal acts [3, 5]. However, as emphasized in [4], there is a real lack of systematic research on the integration of organizational and mathematical approaches to auditing in today's reality. A similar opinion is found in [7], which states that quantitative models need further adaptation for use in different institutional environments. Thus, we recognize the urgent need to develop methodological principles that would combine the independence of the expert approach, the objectivity of quantitative criteria, and the universality of application.

3. DESCRIPTION OF THE METHOD AND BASIC MATHEMATICAL EQUATIONS

Conducting an independent information security audit of an institution requires a structured, impartial, and formal set of processes aimed at assessing the compliance of the security level in the organization's information environment with internal organizational rules and conditions stipulated in contractual obligations between the organizational unit and the auditors. Such assessment frameworks are based on national legislation and derive from internationally recognized standards for information security.

Each such audit must be conducted by a natural or legal person who has no relevant conflicts of interest with the subject of the audit (independent information security auditors – IISA), be non-partisan, and have duly documented authority that meets the applicable legal requirements for the certification or recertification of cybersecurity professionals.

During an independent audit of an information security system, it is important to adhere to certain rules and regulations, which are set out below:

1. To monitor information threats, auditors are independent and impartial, independent in their activities, as this prevents conflicts of interest. Thus, the independence, impartiality of the IISA, and objectivity of the IISA's conclusions are fundamental to the system for identifying architecturally integrated monitors.
2. The audit should cover the most important aspects of information security within the controlled pyramid of the institution, paying close attention to known national regulatory systems and international recommendations in order to create a true data trajectory for the institution.
3. The audit results should reflect the identified risks, the aggregate of negligence, threats, and abuses in the allocation of resources in the audited information systems.
4. Professional conduct of the auditor means strict adherence to the code of ethics, namely responsibility, honesty, objectivity, fulfillment of ethical duties, and preservation of impartiality.

Particular attention is paid to confidentiality, as the auditor is fully responsible for not disclosing any information obtained during the audit of licensing processes without appropriate authorization.

The main objectives of IISA II independent security audits are as follows:

1. To assess the level of cyber protection of information processed and/or transmitted within the institution from organizational and technical measures within its management framework established by its management.
2. To analyze existing statistics on cybersecurity incidents and attacks by malicious users.
3. To assess the relevance and effectiveness of protective measures taken to neutralize threats and reduce potential risks.
4. To identify areas of potential danger due to external or internal modifications.
5. To identify gaps in security systems with the possibility of eliminating them.
6. Assessment of the qualifications and level of awareness of the employee responsible for information security.
7. Reporting on the results of the IISA [15].

Responsibility for conducting the IISA lies with the head of the institution, who is fully responsible for organizing this process. Audit processes can be divided into those performed according to plan or on demand. When calculating the staffing structure of the audit team for specific audits, the following aspects should be taken into account:

1. The level of professional training required of the auditor to achieve the IISA objectives.
2. The methods to be used during the IISA.
3. The auditor's ability to communicate effectively with the institution's employees.

The institution's management shall establish a team of auditors, which may include individual specialists, a group of auditors, or a dedicated information security department, taking into account the criteria identified. In order to prevent conflicts of interest, the same information security auditor is not allowed to conduct a second (qualitative) audit twice in a row. To formally record the relationship between them and information security, a cooperation agreement on IISA is concluded and a non-disclosure agreement is signed.

The following steps are taken in the following order:

1. Recording the fact/date and place of the audit.
2. Providing personal data of the person appointed as a result of the competition for the position of “information technology security auditor”.
3. Information about the position in accordance with the system of its distribution, the service of the manager over the participants of critical infrastructure.
4. Results in clearly defined subject areas, objectives, tasks, and audit categories.
5. List of national and international standards and documents used during the selection process, with an explanation of their relevance to the organization's field of activity.
6. System to be implemented during the audit.
7. Within the confidentiality specified in the results, regarding the investigation of information leaks.
8. Summary of the results of actions taken as part of the audit assignment.
9. Recommendations for adjusting and upgrading the cyber security system within the established parameters [16].

The Independent Information Security Assessment (IISA) includes the following components:

1. Expert Independent Information Security Audit (EISA) form.
2. Active External Independent Information Security Audit (AEISA).
3. Active Internal Independent Information Security Audit (AIIISA).

The independent expert audit (EIISA) procedure is conducted directly at the audit site. It includes interviews with employees involved in administrative information security systems, as well as verification of organizational and technical measures aimed at the cyber security of the institution.

The main stages of EISA implementation in an organization are as follows:

1. Familiarization with relevant EISA documents.
2. Creation of an EISA Independent Audit Plan section.
3. Collection and processing of data within the framework of EISA.
4. Systematization and analysis of the data obtained, as well as preparation of documents based on the audit results [17].

The stage of collecting and evaluating information for an independent information security audit (EIISA) includes:

1. Agreeing on key objectives and scope of work, methodological approach to conducting the audit.
2. Obtaining documents necessary for planning the audit.
3. Agreeing with the organization's management on procedures for accessing confidential information.
4. Appointment of a responsible person to accompany the audit process on behalf of the institution.

The second stage of document preparation involves formulating a specific section of the EISA audit plan for the virtual information system (IISA). This stage is planned based on the results of the analysis of the collected documentation, as well as the conclusions of the IISA, if one was conducted. At the stage of preparation for the EISA, the auditor knows:

1. Sources of internal directives that define the regulatory policy for the protection of processed, stored, and transmitted information in the organization.
2. The main tasks planned for the audit, the results of which are the objectives and deadlines for its implementation.
3. The structure, both organizational and service-related, associated with the functions of the protection system.
4. The institution's computer network, with an emphasis on the interaction of structural and functional elements where security mechanisms are located.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

5. The amount of resources that need to be spent to successfully complete the EISA.

During the third stage of an independent information security audit (EIISA), the auditor takes the following steps to gather the necessary information:

1. Conducts surveys of employees and observes their work, assessing compliance with regulatory requirements. In particular, the following is checked: the existence and implementation of a general information security policy; control of user and administrator access rights; identification and authentication procedures; event log maintenance and analysis; security audit and periodic review; network and information system security; stability of IT infrastructure operation and availability; use of external data storage devices; operating conditions for system software; physical security requirements for equipment placement; and basic technical means.
2. Assesses the parameters of the institution's computer infrastructure at meetings with responsible persons.
3. Uses previous audit results and analyzes logs at the system, application, and firmware levels.
4. Reviews the information, organizational, and technical documentation that actually governs information security processes.
5. Uses the configuration of IT components used in the institution.
6. Analyzes how information processing is structured in relation to existing computer systems [18].

In the final, fourth stage of the EEISA, according to the schedule, the information security audit specialist analyzes the data collected through surveys. Based on this information, a corresponding section with the EEISA results is created and attached to the Independent Verification Report. An Active External Information Security Audit (AEIISA) is conducted outside the organization using penetration testing to determine the level at which the IT infrastructure can protect its networks, software, devices, and users from external cyber threats. During an AEIISA, the behavior of a hypothetical attacker attempting to gain access to the system from the Internet is countered.

Some of the key phases that make up AEIISA are:

1. Planning AEIISA, including a preliminary review of relevant documentation.
2. Identifying the documentation to which the audit approach refers differently depending on the AEIISA.
3. Impersonating another person without the involvement of third parties, either manually or using tools, to investigate intrusion vulnerabilities.
4. Analysis of test results and preparation of a final report on the AEIISA conducted within the organization [19].

For each institution, the information security system is adaptable to implement an effective requirements support system:

Step 1

A penetration test (internal or external) shows how much the perimeter of protection can be adjusted to disable the target. Highly qualified cyber system penetration testers and senior analysts point out that there are indeed numerous gaps (real vulnerabilities) in the system that has been put into operation. Clear examples of fragmented manifestations over time lead to a reduction in the opponent's strategic threshold to defend only when absolutely necessary. Using specialized tools, such as vulnerability scanners, each technical element j of the installation is checked sequentially. If an element is found to be resistant to a specific type of attack v, the test result is marked as *Ptsv* (+). The entire procedure is carried out in stages for each object within the set J.

Based on the collected data, let's calculate the Ptsj indicator – the level of information security protection for a specific asset j, using formula (1). To do this, calculate the proportion of positive tests *Ptsv* (+), adjusted by the weighting coefficient *KWtsv*, and in the general test population V, where the corresponding value is taken into account to maintain the vulnerability database, for example, from mitre. org (CVS – Common Vulnerabilities and Exposures, CWE – Common Weakness Enumeration) or other specialized cybersecurity resources.

Within the framework of this study, it was decided to recommend the use of a predicted weight *KWtsv* for each test, which reflects the potential level of losses in the event of the realization of the corresponding cyber threat. Such a ranking allows for a significant improvement in the effectiveness of managing identified information security system deficiencies. However, the justification of a clear system for balancing the criteria for the importance of each test depending on its criticality in the field of information security requires special research.

$$P_{tsj} = \frac{\sum_{v=1}^{V} \left(P_{tsv(+)} \times K_{Wtsv}\right)}{\sum_{v=1}^{V} \left(P_{tsv} \times K_{Wtsv}\right)}, \tag{1}$$

where *Ptsv* (+) denotes the number of successfully passed tests, indicating the reliability of protection; Ptsv is the total number of penetration tests performed; *KWtsv* is the significance coefficient of each individual test; $v = 1, \ldots, V$ is the number of vulnerabilities detected for each tested component; $j = 1, \ldots, J$ is the number of tested objects of the institution.

Step 2

The determination of the overall index of the effectiveness of information resources protection of the entire set of technical means of the institution *(P1)* is carried out by calculating according to formula (2), which takes into account all the individual weight components of each element *KWzj* [20].

As in the first stage, this study proposes to allocate *a KWzj* index for each technical component – a weighted coefficient indicating the likely degree of damage that such a vulnerability can cause if it is exploited by an attacker through a hostile information system as a result of penetration testing. At the same time, the approach to determining the values of the *KWzj* coefficients, taking into account the importance of a particular technical means for an information system, is the subject of a separate study that is beyond the scope of this publication [21].

$$P_1 = \frac{\sum_{j=1}^{J} \left(P_{tsj} \times K_{Wj}\right)}{\sum_{j=1}^{J} \left(K_{Wj}\right)}, \tag{2}$$

where *Ptsj* is an indicator of the effectiveness of protection of each individual element of the system based on the results of penetration testing, *where* $j = 1, \ldots, J$ is the total number of objects tested in the institution. Thus, the value of P1 is its indicator of the integrated assessment of the level of cybersecurity of the computer infrastructure obtained as a result of the implementation of cyberattack modeling in the field of threats and forms of security (Figure 1) [22].

Step 3

It is necessary to carry out a professional assessment of the effectiveness of each of the organizational measures (denoted as $P_{(EF)\ -OZg}$) and to estimate its weight $K_{(W)\ (-)\ (OZg)}$ with the help of expert assessment g. In this case, evaluation is a determination of the quality or quantity of a certain event or process, which is performed by experts based on their knowledge and experience and presented in a conclusion, descriptive commentary and ranked assessment [23].

Evaluating the effectiveness of certain organizational activities using $P_{(EF)\ (-)\ (OZg)}$, in relation to assigning values to the weighting coefficients $K_{(W)\ (-)\ (OZg)}$, is a rather complex task. For this reason, the main purpose of this publication is to propose an approach that allows for a systematic assessment of an organization's cyber defense level based on evidence obtained during an information security audit. This allows an organization located in different geographical locations to make a comparative assessment of the state of security over time and among different facilities, which will help in formulating a strategy for further improving data security.

In this case, as in the previous one, the estimate of $P_{(EF)\ (-)\ (OZg)}$is the application of the expert assessment of the degree of effectiveness of the organizational measure to the significance indicator $K_{(W)\ (-)\ (OZg)}$that was analyzed. From the analysis of these procedures, it is assumed that these coefficients should take into account equally the worst-case scenarios that could arise if the information system were to be exposed to threats caused by organizational weaknesses in the structure of a particular information system.

Step 4

It is necessary to calculate *P2*, which reflects the effectiveness of the implemented organizational information security measures, by performing the previously mentioned calculations $P_{EF\text{-}OZg}$ with $K_{(W)\ (-)\ (OZg)}$.

Journal of Theoretical and Applied Information Technology
31st December 2025. Vol.103. No.24

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$P_2 = \frac{\sum_{g=1}^{G} \left(P_{EF-OZg} \times K_{W-OZg}\right)}{\sum_{g=1}^{G} \left(K_{W-OZg}\right)}, \quad (3)$$

In this case, g = 1, ..., G is the number of a particular organization, and G is the number of organizations that have been audited. Thus, $P_2$is defined as the level of information protection of a part of the institution, the state of which is regulated by the decisions of the head, both in terms of bringing this part to the required level and leaving the information-transparent organizational structure. To determine the importance of *the* P_2assessment criterion, a linear algorithm for assessing information security threats is used (Figure 2) [22].

Step 5

As part of its policy, the company develops a set of organizational and technical measures aimed at information security. It is well known that information security covers a set of threats that are difficult to combat with technical means. This applies, first of all, to internal threats generated by employees of the organization. On average, they account for about 80% of all costs associated with unresolved losses. Thus, in these situations, the main hope is placed on security management mechanisms. To effectively manage information security in an organization, a comprehensive structure of documents is created, namely financial and economic protection, which is fundamentally based on documents related to all areas of the enterprise, not just security concepts (there is a structure, regulations, job descriptions). For this purpose, we will consider alerts distributed according to awareness patterns - O_{OSm}, calculated by formula (4).

$$O_{OSm} = \frac{\sum_{m=1}^{M} \left(T_m + N_m + A_m\right)}{3}, \quad (4)$$

where $T_{(m)}$ isthe score obtained during testing of employee m of the institution from 0 to $B_{\max}$, $N_m$is the score obtained as a result of training of employee *m of the* institution from 0 to $B_{(\max)}$, $A_m$is the score obtained as a result of certification of employee m of the institution from 0 to $B_{\max}$, $B_{\max}$is the maximum score specified in the evaluation scale, m = 1, ..., M is the number of employees of the institution under review, M is the total number of employees of the institution.

The main scientific achievement of the research was the development of an organizational and analytical methodology for independent information security auditing (IISA), which synthesizes expert assessments with mathematically verified criteria. In contrast to existing methodologies, which are predominantly descriptive or regulatory in nature, the developed methodology combines three audit levels – expert, active external, and active internal – into a comprehensive analytical structure. This provides a comprehensive assessment that covers both technical parameters (including penetration testing results) and organizational aspects and staff competence.

The practical value of the study is determined by the possibility of implementing the developed methodology in organizations across a wide range of activities, from government institutions to private corporations. For cybersecurity managers and specialists, the implementation of IISA provides a number of strategic advantages:

1) ensuring objective, corporate bias-free diagnosis of information system security, which enhances the validity of the results;

2) identifying specific vulnerabilities in technological and management procedures, which contributes to the preventive elimination of risks;

3) forming comparative indices (P1, P2) suitable for tracking trends in the security situation in dynamics;

4) incorporation of audit findings into strategic planning, which ensures the synchronization of cyber security with the overall risk management concept.

Thanks to these characteristics, the methodology becomes an effective mechanism not only for verifying compliance with regulatory requirements, but also for optimizing the functional performance of entities that handle confidential data. In particular, financial institutions, state registration systems, telecommunications operators, and medical organizations can achieve an additional level of protection against internal and external cyber threats.

CONCLUSIONS

Thus, IISA is mandatory for all institutions. The strict implementation of these stages of IISA will determine the effectiveness of the institution's cybersecurity. The IISA is one of the most effective tools for obtaining an independent and objective assessment of the current level of protection of institutions against information security threats. In addition, the IISA results provide a basis for forming a strategy for the development of the cybersecurity system of institutions. It is worth noting that IISA should be implemented on a regular basis.

The results obtained show that the proposed methodology for independent information security auditing (IISA) provides a systematic assessment of both technical protection parameters and organizational measures and staff awareness levels. It can be used in institutions of various profiles, which confirms its versatility and practical significance. At the same time, in our opinion, the study has certain limitations. First, the proposed weighting coefficients require additional validation based on empirical data from various sectors of the economy. Second, an excessive focus on formalized indicators may create the risk of ignoring contextual factors, such as the specifics of internal communications or the security culture within an organization. Third, the lack of unified international approaches to independent auditing makes it challenging to compare results across countries.

The peculiarity of the proposed system of indicators for assessing the information security of an institution is that it covers economic indicators, technical and program parameters of the information security system and evaluates organizational measures and staff knowledge of the institution's information security policy. In addition, such a system for assessing information security indicators can be applied in any institution, regardless of its size, scope and line of business, which makes it universal. At the same time, it should be noted that this article reveals the main stages of applying the IISA methodology in an institution in terms of information security efficiency, and some indicators and proposed coefficients require additional study and research, which is a promising area for further research.

The study showed that consistent use of IISA can increase the security of institutions' information resources and ensure the creation of a unified performance indicator that can be used for inter-organizational comparisons. The result achieved is a scientifically based methodology containing a set of formulas, parameters, and coefficients for quantifying the level of protection. At the same time, there are still some unresolved issues that need further work. These include improving the mechanisms for calibrating weighting coefficients for different economic sectors, adapting the model to the specifics of small businesses with limited resources, and harmonizing IISA results with international certification standards.

REFERENCES:

[1] M. Artemchuk, I. Tsaruk, A. Avramenko, Y. Melnyk, and O. Kazmiruk, "Ensuring information security with firewalls at the border of the Internet", *Actual Problems of Cybersecurity*, State University Telecommunications (Ukraine), 2020, pp. 17–20.

[2] Y. Korpan, "Information security threat classification in computer systems during remote data processing", *Inf. Prot. Methods Comput. Syst. Netw.*, Vol. 17, No. 2, 2015, pp. 39–46.

[3] Cabinet of Ministers of Ukraine, *On approval of the General cyber security requirements for critical infrastructures: Resolution No. 518*, 2019. https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text

[4] Y. Roy, A. Petrenko, V. Ivanov, et al., "Information security audit – the basis of effective company protection", *Cybersecurity Educ. Sci. Technol.*, Vol. 1, No. 1, 2018, pp. 86–93. https://doi.org/10.28925/2663-4023.2018.1.8693

[5] National Bank of Ukraine, *On Approval of the Regulation on control over compliance by banks with the applicable legal requirements on information security, cyber security and electronic trust services*, 2021. https://zakon.rada.gov.ua/laws/show/v0004500-21#Text

[6] Draft Resolution of the Cabinet of Ministers of Ukraine, *Certain issues of independent information security audit at critical infrastructures*, 2021. http://www.drs.gov.ua/wp-content/uploads/2021/07/dokument-6273_0_19-21.pdf

[7] V. Kononova, S. Tarasenko, and A. Chabanenko, "Evaluation of information resources protection", Lviv Polytechnic National University (Ukraine), 2021, pp. 99–105. http://ena.lp.edu.ua

[8] V. Makedon, V. Myachin, T. Aloshyna, I. Cherniavska, and N. Karavan, "Improving the readiness of enterprises to develop sustainable innovation strategies through fuzzy logic models", *Economic Studies (Ikonomicheski Izsledvania),* vol. 34, no. 5, 2025, pp. 165–179. https://archive.econ-studies.iki.bas.bg/2025/2025_05/2025_05_09.pdf

[9] P. Goldstain, "What is a Cybersecurity Audit and Why is it Important?", 2021. https://fedtechmagazine.com/article/2021/06/what-cybersecurity-audit-and-why-it-important-perfcon

[10] National Institute of Standards and Technology (NIST), *NIST Special Publication 800-61 Rev. 2: Computer Security Incident Handling Guide*, 2020. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

[11] K. Donegan, "Computer Security Incident Response Teams", 2021. https://whatis.techtarget.com/definition/Computer-Security-Incident-Response-Team-CSIRT

[12] National Institute of Standards and Technology, *Managing information security risk: organization, mission, and information system view*, 2011. https://www.nist.gov/publications/managing-information-security-risk-organization-mission-and-information-system-view

[13] National Institute of Standards and Technology (NIST), "Security and privacy controls for information systems and organizations", *NIST Special Publication 800-53 Rev. 5*, U.S. Department of Commerce (USA), 2020. https://doi.org/10.6028/NIST.SP.800-53r5

[14] Army Cybersecurity, *Army Regulation 25–2*, 2019. https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN37506-AR_25-2-003-WEB-4.pdf

[15] O.I. Romanov, N.N. Nesterenko, and N.A. Fesokha, "Analysis of modern virtualization technologies for building information and telecommunications systems", *Coll. Sci. Pap. VITI*, No. 1, 2019, pp. 82–90.

[16] UK Ministry of Defence, *Digital & Information Technology Functional Strategy (V.1.01)*, 2019. https://www.gov.uk/government/publications/digital-and-information-technologies-strategy

[17] UK Ministry of Defence, *MOD Architecture Framework (MODAF) (v.1.2)*, 2010. https://www.gov.uk/guidance/mod-architecture-framework

[87] UK Ministry of Defence, *National Security Through Technology: Technology, Equipment, and Support for UK Defence and Security*, London: Ministry of Defence (UK), 2012.

[19] UK Ministry of Defence, *Communications and Information Systems Support to Joint Operations (Joint Doctrine Publication 6-00, 3rd Edition)*, 2008. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/33709/20111221JDP600_Ed3_inc_Chg1.pdf

[20] A. Zhilin, A. Divityskyi, and A. Kozachok, "Problems of protecting information resources when using cloud technologies", *Inf. Technol. Secur.*, Vol. 7, No. 2, 2019, pp. 171–182. https://doi.org/10.20535/2411-1031.2019.7.2.190565

[21] V. Makedon, V. Myachin, O. Plakhotnik, N. Fisunenko, and O. Mykhailenko, "Construction of a model for evaluating the efficiency of technology transfer process based on a fuzzy logic approach", *Eastern-European Journal of Enterprise Technologies*, no. 2(13(128)), 2024, pp. 47–57. https://doi.org/10.15587/1729-4061.2024.300796

[22] State Service for Special Communications and Information Protection of Ukraine, *Recommendations for the creation of CISPs in ITS used to provide Internet access services*, 2017. https://cip.gov.ua/ua/news/poradi-rekomendaciyi-shodo-stvorennya-kszi-v-its-yaki-vikoristovuyutsya-dlya-nadannya-poslug-dostupu-do-merezhi-internet

[23] Y.I. Neroznak, V.M. Ostapchuk, O.V. Draglyuk, M.M. Radchenko, and M.M. Korotkov, "Analysis of the possibilities of cloud technologies in the information infrastructure of the defense forces", *Bull. VITI*, No. 1, 2021, pp. 53–68.

Journal of Theoretical and Applied Information Technology
31st December 2025. Vol.103. No.24

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

FIGURES

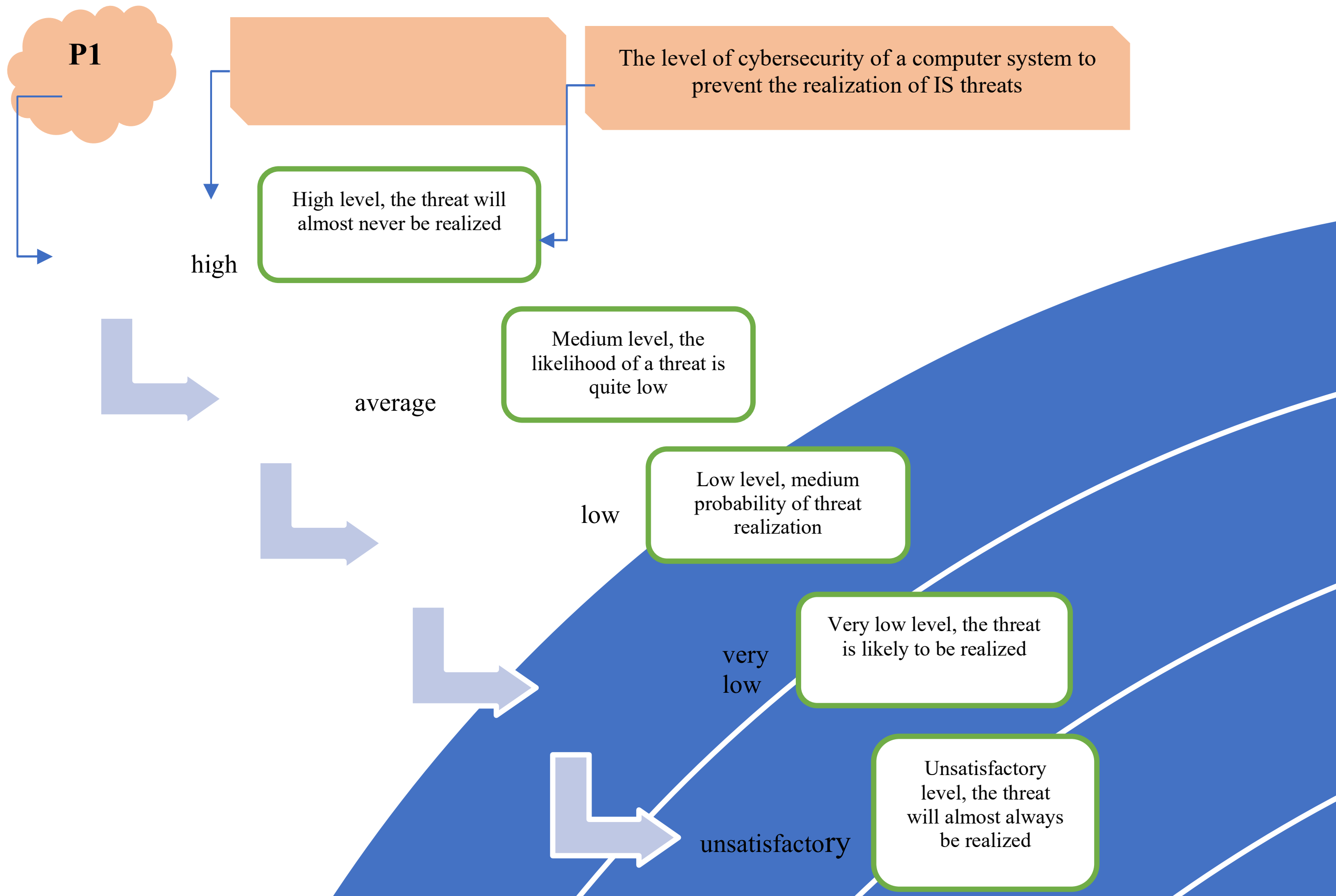

Figure 1. Overall Information Security Effectiveness of All Technical Means of the Institution Based on the Weighting of Each Element
Source: State Service for Special Communications and Information Protection of Ukraine [20]

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

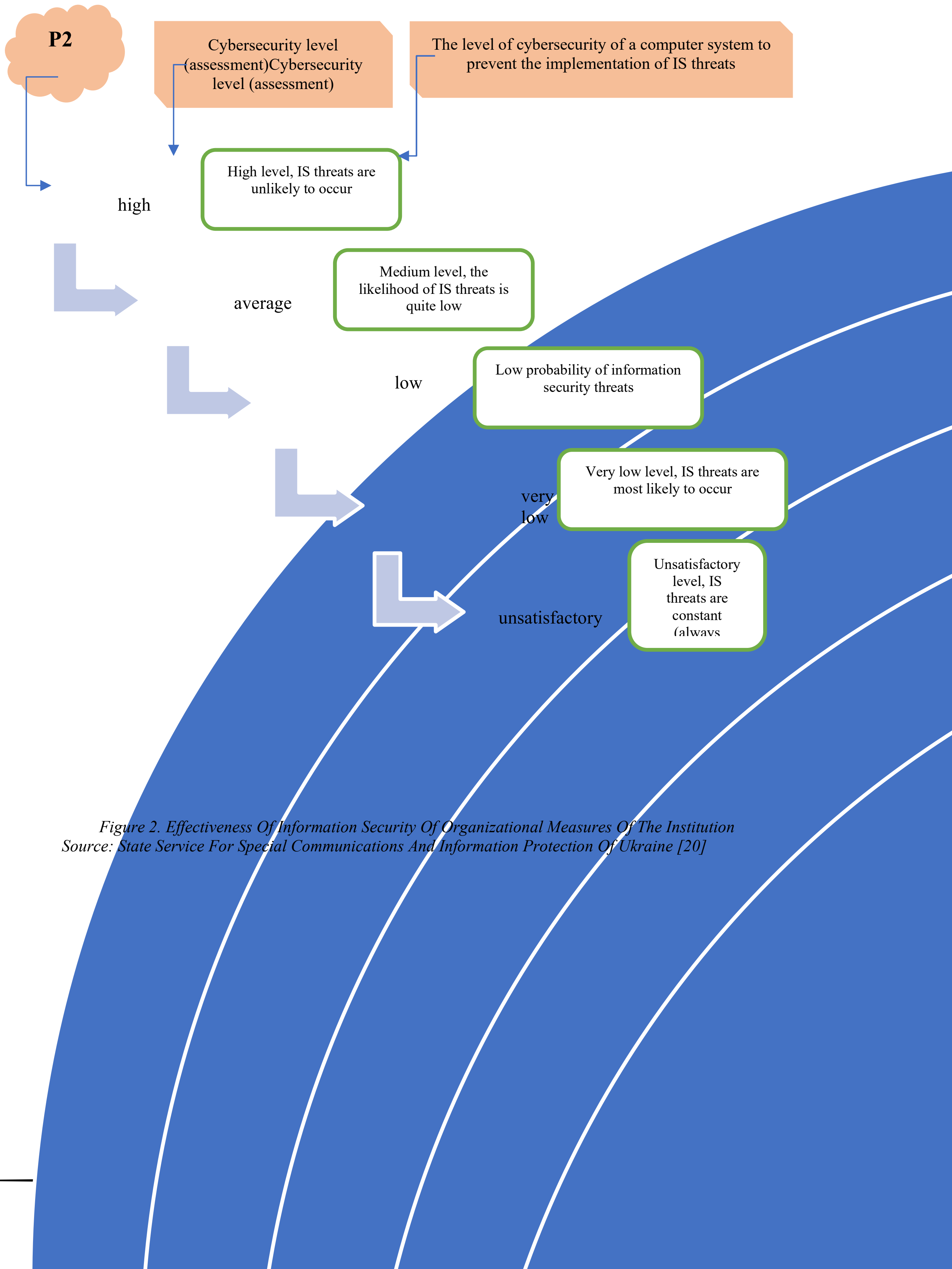

Figure 2. Effectiveness Of Information Security Of Organizational Measures Of The Institution
Source: State Service For Special Communications And Information Protection Of Ukraine [20]