Journal of Information Systems Engineering and Management
2025, 10(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Methodology for Conducting an Independent Information Security Audit of the Institution

Mykola Masesov[1,*], Oleg Diegtiar[2], Dmytro Minochkin[3], Andrii Khapsalis[4], Dmytro Novytskyi[4], Sergii Kramarenko[5]

[1]*Candidate of Technical Sciences, Senior Researcher, Chief of Scientific Center of Communication and Information Technologies, Kruty Heroes Military Institute of Telecommunications and Information Technologies, Kyiv, Ukraine*
[2]*Doctor of Sciences in Public Administration, Professor, Leading Researcher, Scientific Center of Communication and Information Technologies, Kruty Heroes Military Institute of Telecommunications and Information Technologies, Kyiv, Ukraine*
[3]*Associate Professor of the Department of Telecommunication, Institute of Telecommunication Systems of National Technical University of Ukraine "Igor Sikorsky Kyiv Politechnic Institute", Kyiv, Ukraine*
[4]*Scientific Researcher, Scientific Center of Communication and Information Technologies, Kruty Heroes Military Institute of Telecommunications and Information Technologies, Kyiv, Ukraine*
[5]*Candidate of Economic Science, Leading Researcher, Interdisciplinary Research Institution Digitalization and AI, Kyiv, Ukraine*
** Corresponding Author: mykola.masesov@viti.edu.ua*

ARTICLE INFO

Received: 10 Oct 2024

Revised: 14 Dec 2024

Accepted: 20 Dec 2024

ABSTRACT

Introduction: Any computer without special protection exchanging data with other computers, especially when using the Internet, is bound to be infected with malware and, as a result, its performance will be reduced or impossible and/or taken under control.

Objectives: The purpose of this article is to define information security is to protect data information and sup-porting infrastructure from accidental or intentional interference which can cause the loss of information or its unauthorized modification and in case of force majeure - to minimize the damage caused by such actions.

Methods: General scientific methods were used in the course of the study, including the structural-logical method, analysis and synthesis.

Results: Noted the need for regular independent information security audit in the institution to assess the real state of cybersecurity in the institution, the ability to withstand constantly changing and adapting the external and internal threats to information security, as well as for timely recommendations for bringing and improving the protection of systems in line with certain requirements.

Conclusions: Thus, it is worth noting this article reveals the main stages of the methodology in the institution on the information security effectiveness, and some of the indicators, offered coefficients require additional study and research, which is a promising direction to further research.

Keywords: independent information security audit, information security auditor, information security assessment, cyber security assessment.

INTRODUCTION

Any computer without special protection exchanging data with other computers, especially when using the Internet, is bound to be infected with malware (malware is short for malicious and software) and, as a result, its performance will be reduced or impossible and/or taken under control (for example: performing scans of hard drives for bank card data, recording keystrokes to steal passwords, using a computer to launch a DDoS attack against the hacker's enemies or encrypt data in order to obtain a ransom to restore access, etc.).

The institution's computer system is an information-technical complex whose purpose is to process, store, input and output information. The computer system includes computers, printers, servers, networks, etc. with software. Via a computer network, information is exchanged through a local or global data-transmission system.

A local area network (LAN) of an institution is a multiservice data transmission network that operates under the unified management and is dedicated to serving the own production needs of the institution, organization or enterprise (hereinafter referred to as the institution). This type network is a closed structure with a sufficiently high degree of protection external access to which is strictly restricted or completely prohibited and access to information within it is filtered with the administrative and technical methods. To provide data protection in local area networks, various organizational and technical methods can be used (assigning responsible scientists, applying access control lists, using VPN, etc.). Creating local area networks, the priority requirements are failure resistance, security and network speed.

The creation of secure computer systems is the purpose of network engineers and programmers, as well as a subject of theoretical research in the field of telecommunications and informatization. Computer system vulnerabilities pose a significant challenge to users because of the complexity and laboriousness of most processes and methods for protecting digital equipment, information and computer systems themselves from unintended or unauthorized access.

Information security (hereinafter – IS) – a state of data security processing and storage systems, which ensures the information confidentiality, availability and integrity or a set of measures aimed at protecting information from unauthorized access, usage, disclosure, disruption, modification, cognizance, checking recording or destruction.

The purpose of ensuring information security is to protect information data and the supporting infrastructure from accidental or intentional interference, causing data loss or unauthorized modification, and in the case of force majeure, reducing the damage caused to a minimum [1].

Information security threat is a set of conditions and factors creating the risk of breaking information security. Threat (in general) means a potentially possible event, action (impact), process or occurrence that could damage one’s interests.

Associated with any object of information security is the existence of a threat, which means a set of conditions and factors appearing in the interaction of this object with others, or its composing components with each other, and capable of negatively affecting it. Threats can be both accidental and intentional. The most dangerous, in terms of the consequences of exposure, intentional threats [2].

Vulnerability (system vulnerability) it is the system incapability to resist the implementation of a particular threat or set of threats. That is, these are certain flaws in a computer system that can intentionally compromise its integrity and cause it to malfunction. Vulnerability can result from programming errors, flaws in system design, insecure passwords, viruses and other malicious programs, scripting and SQL-injections.

Thus, a computer system information security can be compromised due to IS threats realized through vulnerabilities exist in the computer system. To prevent information security breaches an information security audit performed in a timely manner is necessary.

In the process of developing organizational and technical measures to ensure institution information security, the head of the institution grounds the application of compensatory measures or the exclusion of certain requirements from the list of basic ones. To ensure the continuous and effective institution operation in the information field, in view of the current regulatory basis of Ukraine, the authors of the article propose, based on paragraph 3 of Article 6 of the Resolution of the Cabinet of Ministers of Ukraine from June 19, 2019 № 518 “On approval of the General requirements for cyber protection of critical infrastructures“ to conduct an independent information security audit (hereinafter – IISA) not only at critical infrastructure facilities, but also in institutions by initiative of their managers [3]. An IISA of the institution must assess the sufficiency and relevance of the compensatory measures used to block (neutralize) threats and mitigate risks.

The importance of a regular IISA is the need to periodically assess the real state of the institution’s security in relation to the ability to withstand external and internal threats to information security, being constantly changed and adapted. The problems of ensuring the proper level of the institution information security requires a systematic approach to the analysis of the state of information protection, which would be based on the real indicators obtained during the IISA, so the group of authors proposed a methodology for an independent information security audit of the institution regarding the effectiveness of cybersecurity.

DEFINITION OF RESEARCH PROBLEM

Information security assessment has been engaged in since the very appearance of information technology. The scientific work that reviews the concept of information security audit in an organization, its types and main stages is noteworthy [4]. However, few publications and studies consider a systematic approach to the analysis of the state of information protection in the institution, which would be based on real indicators obtained during an IS audit.

The IISA need is noted in the following statutory legal acts of Ukraine and their drafts, which are at the stage of agreement:

- Resolution of the Cabinet of Ministers of Ukraine from June 19, 2019 № 518 “On approval of the General requirements for cyber protection of critical infrastructure facilities” ;

- Resolution No. 4 of the Executive Board of the National Bank of Ukraine of January 16, 2021 “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” [5];

- Draft Resolution of the Cabinet of Ministers of Ukraine of July 01, 2021 “Some issues of independent information security audit at critical infrastructures” [6].

The existent standards are frankly conceptual in nature, allowing information security experts to implement any methods, tools and technologies to assess, develop and manage risks. Different standards admit the use of quantitative and qualitative methods of information security risk assessment, but there is no justification and recommendations on the choice of mathematical and methodological apparatus [7; 8; 9].

There are three basic groups of vulnerability assessment methods (standards):

1. Qualitative ranking methodology is based on the use of several qualitative categories of vulnerabilities (e.g., low, medium, or high). Examples: US National Infrastructure Protection Center (NIPC) vulnerability classification scheme, SANS Institute’s Critical Vulnerability Analysis Scale, Microsoft Security Bulletin Severity Rating System [10; 11].

2. Quantitative ranking methodology is based on the use of a quantitative vulnerability assessment scale. Examples: Payment-Card Industry Data Security Standard (PCI DSS) vulnerability assessment system; United States computer emergency readiness team (US-CERT) vulnerability assessment system [12; 13].

3. Applying complex vulnerability assessment characteristics. Examples: Common Vulnerability Scoring System (CVSS), vulnerability assessment system nCircle [14; 15].

For the sake of understanding, note that vulnerability assessment systems also differ in what is measured. For example, the Common Vulnerability Scoring System (CVSS) is an open standard used to calculate quantitative assessments of computer system security vulnerabilities, usually in order to understand the priority of fixing, three metrics (vulnerability characteristics, time elements, effect of action) give a score from 0 to 10, but the drawbacks are: vulnerabilities are assessed independently of each other; only direct damage to the target host is considered in vulnerability assessment [16; 17]. Coordination Centre US-CERT gives a numerical score from 0 to 180, but takes into account factors such as the presence of risk to the Internet infrastructure and prerequisites for exploiting a vulnerability. The SANS vulnerability analysis scale takes into account whether a vulnerability is detected in default configurations or in client or server systems. Microsoft’s own scoring system tries to reflect the complexity of exploitation and the overall impact of the vulnerability, etc [18; 19].

Purpose of the article: to describe the main stages of the IISA methodology in the institution based on the determination of information security indicators, to formulate general guidelines for the head of the institution to conduct the IISA [20].

DESCRIPTION OF THE METHOD AND BASIC MATHEMATICAL EQUATIONS

An independent information security audit of the institution is a systematic, independent and documentary process of obtaining an assessment of the institution’s information security status and its compliance with the requirements, procedures and methodologies defined in the contract between the institution's management and the auditor, based on the requirements of national standards and the recommendations of international information security standards.

The auditor conducting IISA is a natural or legal entity being independent in its activities and having no conflict of interest with the institution to be audited, as well as having confirmed the qualification for conducting IISA, in accordance with the procedure for attestation (recertification) of information security auditors.

The conduct of the IISA is based on the following guidelines:

- auditors' independence – auditors are independent in their activities and have no conflict of interest. Independence is the basis of impartiality in conducting the IISA and objectivity in forming the IISA conclusions;
- completeness of information security audit – the scope of IISA is to be sufficient to develop objective conclusions on the information security status of the institution and its compliance with the established requirements of national standards and recommendations of international information security standards, considering the specifics of the institution's activity;
- conclusion uniqueness – IISA conclusions must unequivocally qualify the risk degrees;
- ethical behavior – the auditor's ethical behavior is based on responsibility, incorruptibility, impartiality.

Confidentiality – the auditor is responsible for the disclosure of information obtained during the IISA.

The main objectives of the institution's IISA on the information security effectiveness are:

- assessment of the cybersecurity current level of processed and transferred information in the institution under the organizational and technical information security measures defined by the head of the institution;
- statistical data analysis on cyber incidents and cyberattacks;
- analysis of sufficiency and relevance of compensatory measures that are used to block (neutralize) threats and reduce risks;
- identifying possible risks associated with the possibility of external and internal threats to information security;
- detecting of vulnerabilities with the possibility of fixing them in the future;
- assessment of the competence and awareness of the personnel impacting the IS;
- reporting on the results of the IISA.

The IISA organization is the responsibility of institution's head and can be carried out both on a regular and non-regular basis:

- to determine the quantitative auditors' composition for the particular IISA, it is necessary to include consideration of:
- the auditor's overall competence necessary to accomplish IISA objectives;
- the IISA selected methods;
- the auditor's ability to interact effectively with institution staff.

The institution head engages an auditor, audit team, information security audit unit (hereinafter referred to as the information security auditor) to conduct the IISA, formed on the basis of the above. The head of the institution may not engage the same information security auditor twice in a row to conduct an IISA. A contract is signed between the head of the institution and the information security auditor to conduct the IISA and an agreement on non-disclosure of confidential information.

The information security auditor conducts the IISA in accordance with the "Independent Information Security Audit Plan" for the institution (hereinafter referred to as the Independent Audit Plan), which consists of three sections specifying the activities for each component of the IISA: expert, active external and active internal. The Plan shall be approved by the institution's head where the IISA is conducted.

The main result of the institution's IISA is the report on IISA results (hereinafter – the Independent Audit Report), which must contain complete, accurate, clearly stated and intelligible IISA results, as well as:

- IISA dates and locations;
- personal details of the information security auditor;
- information about the head of the institution, employees of the critical infrastructures, participated in the IISA;
- the purpose, tasks and type of the IISA;
- listing of national and/or international information security standards, on the basis of which an independent audit has been conducted, and a justification for the applicability of the list of requirements from information security standards to the scope of the institution's activities;
- information about the applied procedures and methods of conducting an independent audit;
- description and classification of vulnerabilities detected by penetration tests, the degree of their criticality and methods of fixing;
- IISA results according to the main tasks;
- recommendations to bring and improve cybersecurity to certain requirements.

The components of the institution's IISA are:

- expert independent information security audit (hereinafter referred to as the EIISA);
- active external independent information security audit (hereinafter referred to as the AEIISA);
- active internal independent information security audit of (hereinafter referred to as AIIISA).

EIISA (expert) is conducted directly at the object of the audit by interviewing personnel involved in information security, and checking for compliance with organizational and technical measures to ensure cyber security of the institution.

The main stages of EIISA at the institution are:

- a prior review of the documents required to conduct the EIISA at the institution;
- preparing the section in the Independent Audit Plan regarding the EIISA;
- collecting EIISA data at the institution;
- collecting data analysis and preparing materials on the results of the EIISA at the institution.

TERMS AND PROCEDURES FOR CONDUCTING THE EIISA AT THE INSTITUTION

The first stage of the EIISA is to agree on:

- the purposes, scopes, and methods of conducting the EIISA;
- gaining access to the documents needed to the EIISA planning;
- the procedure on gaining limited access information established by the head of the institution;
- determination of the accompanying person from the institution.

At the second stage, the information security auditor prepares a section in the EIISA Independent Audit Plan, based on the analysis of the documents received and the results of the previous IISA (if available), in the drafting of which the information security auditor determines:

- regulatory requirements (policies, standards, guidelines and procedures) by which the protection of processed and transferred information in the institution is built;
- the tasks, objects and timing of the EIISA;
- introduction to the organizational structure of users and supporting units;
- detailed review over information about the structure of the institution's computer system in purpose to find out how security mechanisms are allocated to the structural elements and levels of operation of the institution's computer system;
- resources needed for the EIISA.

In the EIISA third stage to obtain insights, the information security auditor:

- interviews and monitors the actions of the staff of the institution to meet the requirements, namely, to verify: the formation of a general information security policy; access control of users and administrators; identification and authentication of users and administrators; registration of events components and periodic auditing; ensuring the network security of components and information resources; ensuring the availability and resilience of components and information resources; determining the conditions of use of removable (external) devices; defining the conditions of using software and hardware; identifying the conditions of placement of components;
- reviews and analyzes parameters of the institution's computer system directly during meetings with responsible staff members;
- uses prior audit reports and analyzes system logs, software and firmware event logs;
- analyzes organizational and technical (maintenance) documents;
- analyzes the configuration of the institution's computer system components;
- analyzes organizing information processing in the institution's computer system.

During the fourth and final stage of the EIISA, in accordance with the established deadlines, the information security auditor analyzes the data collected, on the basis of which prepares the results section of the institution's EIISA, as part of the Independent Audit Report.

The AEIISA (active external) is conducted outside the institution by external penetration testing to assess the computer system's ability to protect its networks, programs, endpoints, and users from external threats. AEIISA modulates the actions of an intruder who penetrates the institution's computer system from the Internet.

The main stages of conducting AEIISA in the institution are:

- prior analysis of the documents (installations, instructions, etc.) required to conduct the AEIISA at the institution;
- preparing a section in the Independent Audit Plan related to the AEIISA;
- conducting both manual external penetration testing and using software or hard-ware vulnerability searching and analysis tools;
- data collected analysis and preparation of materials on AEIISA results at the institution.

A. Conditions and procedures for the AEIISA at the institution

During the first phase of the institution's AEIISA, the necessary data for the AEIISA are collected and analyzed.

During the second stage, the information security auditor compiles a section in the Independent Audit Plan relating to AEIISA, based on the data analysis obtained and the results of previous IISA (if available), wherein the information security auditor takes into account all aspects of the audit:

- listing of the institution's facilities (IP addresses);

- the software and hardware tools involved in AEIISA;
- listing of the penetration testing programs and techniques to be conducted, agreed upon with the head of the institution.

During the third AEIISA stage external penetration testing is carried out, both manually and with the help of software or hardware performing diagnostics and monitoring of the computer system, allowing to scan networks, computers and programs to identify possible problems in the system security to assess and eliminate vulnerabilities. Data collection is performed.

On the final fourth the AEIISA stage, in accordance with the established audit timeframe, the information security auditor analyzes the obtained data, on the basis whereof prepares the section of the results of the institution's AEIISA, as a constituent of the Independent Audit Report.

AIIISA is conducted directly at the institution with internal penetration testing of all components of the computer system (subsystems, subnetworks) to assess the computer system's ability to protect its networks, programs, endpoints and users from internal threats. AIIISA modulates an insider behavior (an intruder somehow gaining access to the institution's internal local network and trying to affect the processing, storage, input/output of information).

The main AIIISA stages conducting in the institution are:

- a prior analysis of the documents required for the IISA at the institution;
- preparing a section in the Independent Audit Plan related to AIIISA;
- conducting both manual internal penetration testing and using software or hardware vulnerability search and analysis tools;
- analyzing the collected data and preparing materials on the results of the AIIISA at the institution.

B. Conditions and procedures for the AIIISA at the institution

At the first AIIISA stage, the issues are agreed upon:

- purposes, scope, and methods of the AIIISA conducting;
- gaining access to the documents needed to the AIIISA planning;
- the procedure for obtaining limited access information as established by the head of the institution.

At the second stage, the information security auditor, based on the obtained information, analysis of received documentation and the results of previous IISA (if available), prepares a section in the Independent Audit Plan relating to the institution's AIIISA, in the drafting thereof, which determines the following:

- tasks, objects and timing of the AIIISA;
- examining the function and principles of the institution's computer system to determine the existing risks and security requirements for the system;
- determines the necessary resources for AIIISA, as well as software and hardware;
- listing of penetration testing programs and techniques to be conducted, agreed upon with the head of the institution.

The third AIIISA stage involves internal penetration testing, both manual and with the help of software or hardware, diagnoses and monitors the institution's computer system, allowing to scan networks, computers and programs to identify possible problems in the system. Security, to assess and eliminate vulnerabilities. Data collection is performed.

In the final fourth AIIISA stage in accordance with the established deadlines, the information security auditor analyzes the collected data, on the basis thereof prepares the section of the results of the AIIISA of the institution, as part of the Independent Audit Report.

It is recommended to conduct IISA by a combination of stages of its components: expert, active external and active internal. In order to prevent leakage of confidential data throughout the totality, it is necessary to involve at least three information security auditors in IISA with the rights of each to conduct one IISA component: EIISA, AEIISA or AIIISA – in this case for each focus area with the proper titles, separate Independent Audit Plans and separate Independent Audit Reports are prepared.

With the purpose of approach systematizing to the analysis of the state of cybersecurity in the institution, which would be based on real indicators obtained during the IISA, the authors proposed a mathematical model for assessing the effectiveness of information security.

Methodology is a set of techniques and processes for the expedient conduct of any activity. It is a kind of tactical plan determining the technique and sequence of solving a specific scientific or practical problem.

Efficiency is the balance between the results achieved and the resources used.

For each institution, the effectiveness of information security is calculated by implementing the following steps:

Step 1

Penetration Testing (*Pts*), simulating the actions of an intruder according to the set objectives and definitely by an experienced specialist, is almost always effective. It is exactly what makes it possible to identify real information security problems in an institution and draw the attention of management to them. After all, the demonstration of successful access to well-protected information or presentation of full control over the personal computers of responsible personnel can be the most convincing evidence of the existing cybersecurity quality.

Using specialized software tools (vulnerability scanners), perform penetration testing of each technical means j of the institution one by one. A positive result of the test, denoted as *Ptsv* (+), is the resistance of technical means *j* to the influence of *v*. The methodology implies a sequential testing of all the means of the institution *J*.

On the basis of the results obtained it is necessary to calculate *Ptsj* – information security effectiveness of each technical means *j* of the institution by formula (1), as the ratio of all positive check results *Ptsv (+)*, revealed when testing each means by checks *v* with the weighting coefficient of each test K_{Wtsv} to the total number of checks *V* with weighting coefficient, which provides the current database of test checks from mitre.org (Common Vulnerabilities System and Exposures – database of IS vulnerabilities, Common Weakness Enumeration – software weak spots and vulnerabilities system of categories) or another specific cyberthreat base.

This article considers the possibility of using for each penetration test a weighting coefficient of K_{Wtsv}, that will take into account the maximum possible amount of damage caused in the case of an IS threat, which allows to expose this test. However, the criteria for assigning each penetration test an appropriate weighting coefficient depending on its importance for the IS requires separate research and proceedings, which is not the purpose of this article:

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

where *Ptsv* (+) – a positive result of the test (safety is ensured), *Ptsv* – total number of tests (Penetration test), K_{Wtsv} – the weighting coefficient of each test, $v = 1, \dots, V$ – the number of vulnerabilities for each tested item, $j = 1, \dots, J$ – the number of the institution's items being audited.

Step 2

Calculate P_1 – total efficiency of information security of all technical means of the institution on the basis of the weighting coefficient of each item K_{Wzj} by the formula (2).

Similarly to step 1, this article considers the possibility of using for each technical item a weighting coefficient K_{Wzj}, which will consider the maximum possible amount of damage caused in case of realization of an IS threat due to vulnerability exposed by penetration testing. However, the criteria for assigning each technical item a weighting coefficient K_{Wzj} depending on its importance for the IS requires separate research and proceedings, which are not the purpose of this article.

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

where *Ptsj* – the result of effectiveness of information security of each item by penetration testing, $j = 1, \dots, J$ – the number of the institution's items being audited.

Consequently, P_1 is an indicator allowing to estimate the level of the computer system protection by the results of Penetration Testing according to the linear scale of information security threat assessment (see Table 1).

Table 1. Total efficiency of information security of all technical means of the institution on the basis of the weighting coefficient of each item

P_1	**Cybersecurity level (assessment)**	**The cybersecurity level of the computer system to prevent the implementation of threats to IS**
$0{,}9 < P_1 \leq 1$	high	High level, the threat almost never will be realized
$0{,}75 < P_1 \leq 0{,}9$	average	Average level, the threat probability is quite low
$0{,}5 < P_1 \leq 0{,}75$	low	Low level, average threat probability of realization
$0{,}25 < P_1 \leq 0{,}5$	very low	Very low level, the threat is likely to be realized
$0 \leq P_1 \leq 0{,}25$	unsatisfactory	Unsatisfactory level, the threat will almost always be realized

Step 3

Provide an expert assessment of the effectiveness of each organizational measure $P_{EF\text{-}OZg}$ and an expert assessment of the $K_{W\text{-}OZg}$ weighting coefficient of each organizational measure *g*.

Expert assessment is a determination procedure of quantitative or qualitative characteristics of a process or event, carried out by experts on the basis of professional knowledge and experience and provided in the form of a conclusion, a descriptive interpretation, ranking and rating.

A complicated issue is the question of determining the expert effectiveness assessment of each organizational measure $P_{EF\text{-}OZg}$ and the expert assessment of the weighting coefficient $K_{W\text{-}OZg}$ of each organizational measure g. Because this article task is to determine a systematic approach to the analysis of the cybersecurity status in the institution based on the real indicators obtained during an IS audit. The specified will allow a comparative information security analysis of the institution at certain intervals or different institutions, in an effort to identify directions for improving the approaches to information protection.

Similar to step 1 in this article, it is considered the possibility of using for each organizational measure an expert effectiveness assessment of its $P_{EF\text{-}OZg}$, as well as a weighting coefficient $K_{W\text{-}OZg}$ of each organizational measure *g*, which will also consider the maximum possible damage caused in case of the implementation of an IS threat, due to the vulnerability made possible by the imperfection of a particular organizational measure. The mentioned values depend on the importance of appropriate IS measures and require a special study and research.

Step 4

Calculate P_2 – the information security effectiveness of organizational measures of the institution by formula (3), using $P_{EF\text{-}OZg}$ and $K_{W\text{-}OZg}$.

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

where $g = 1, ..., G$ – auditable organizational measure, G – the auditable organizational measures total number.

Consequently, P_2 is an indicator provides an assessment of the level of protection of processed information and circulated in the institution under the organizational information security measures determined by the head of the institution. For evaluating the significance of the selected assessment criterion P2 using a linear scale for assessing information security threats (see Table 2).

Table 2. The information security effectiveness of organizational measures of the institution

P_2	**Cybersecurity level (assessment)**	**The level of cybersecurity achieved by organizational institution measures used to ensure IS**
$0,9 < P_2 \leq 1$	high	High level, the emergence of IS threats are hardly possible
$0,75 < P_2 \leq 0,9$	average	Average level, probability of IS threats is quite low
$0,5 < P_2 \leq 0,75$	low	Low level, probability of information security threats
$0,25 < P_2 \leq 0,5$	very low	Very low level, the IS threats occurrence are the most probable
$0 \leq P_2 \leq 0,25$	unsatisfactory	Unsatisfactory level, IS threats are constant (constantly present)

Step 5

The institution's management determines the organizational and technical measures to ensure information security in the institution – these are norms and rules that must be obeyed by all staff members. There are many IS threats which are impossible or extremely difficult to protect against by technical means alone. First of all, the issue is about internal threats created by the institution's staff. After all, about 80% of the damage is due to incidents caused by them. In dealing with such threats, organizational measures come to the fore. Organizational IS support should be based on an interrelated structure combined by general principles of documents – from purely conceptual to quite specific, focused on a particular technology or area of activity (IS concepts, IS policies, instructions and IS regulations).

In order to conduct a level probability assessment of the internal threats by company personnel, testing, training and certification of staff should be carried out.

Calculate the efficiency of awareness of each specialist – O_{OSm} of the institution by the formula (4):

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

where T_m – the score obtained in testing the employee m of the institution from 0 to $B_{\max}$, N_m – the score obtained as a result of training of the employee m of the institution from 0 to $B_{\max}$, A_m – the score obtained as a result of certification of the employee m of the institution from 0 to $B_{\max}$, $B_{\max}$ – the maximum score specified in the assessment scale, $m = 1, ..., M$ – the employee number of the inspected institution, M – total employee number of the institution.

Step 6

Calculate the employee knowledge efficiency of the institution P_3 by the formula (5):

$$P_3 = \frac{\sum_{m=1}^{M} O_{OSm}}{M \cdot B_{\max}}, \qquad (5)$$

where O_{OSm} – each specialist's knowledge effectiveness, $B_{\max}$ – the maximum score provided by the assessment scale, $m = 1, ..., M$ – number of employees of the audited institution, M – total employee number of the institution.

P_3 is an indicator allowing to get an assessment of the information security level due to the employees' knowledge of certain organizational measures to ensure information security in the institution. To determine the significance of the selected P_3 assessment criterion, apply the Harrington verbal-numerical scale (see Table 3).

Table 3. The employee knowledge efficiency of the institution

P_3	**Cybersecurity level** **(assessment)**	**The IS level that is reached by the knowledge of employees of the specific organizational measures to ensure IS**
$0{,}8 \le P_3 \le 1$	very high	Very high efficiency level, the system operates in the specified mode, the emergence of information security threats is practically impossible
$0{,}63 \le P_3 < 0{,}8$	High	High level, the system operates in the specified mode, the probability of information security threats is quite low
$0{,}37 \le P_3 < 0{,}63$	average	Average level, the stable operation of the system is disrupted, the probability of information security
$0{,}2 \le P_3 < 0{,}37$	very low	Very low level, stable operation of the system on the verge of failure, the emergence of information security threats is most probable
$P_3 < 0{,}2$	unsatisfactory	Unsatisfactory level, there is no stable operation of the system, information security threats are constant (constantly present)

Step 7

Calculate P_T – the general information security efficiency of the institution by the formula (6):

$$P_T = \frac{P_1 + P_2 + P_3}{3}. \qquad (6)$$

Consequently, P_T is an indicator provides an assessment of the information security effectiveness level of the institution. To determine the significance of the selected assessment criterion P_T, apply a linear information security threat assessment scale (see Table 4).

Table 4. The general information security efficiency of the institution

P_T	Cybersecurity level (assessment)	The IS level of processed and transferred information in the institution
$0{,}9 < P_T \leq 1$	high	High information security level, computer system vulnerabilities are virtually absent, the emergence of IS threats is hardly possible.
$0{,}75 < P_T \leq 0{,}9$	average	Average information security level, the existing vulnerabilities of the computer system may lead to minor breaches of IS, the probability of information security threats is quite low.
$0{,}5 < P_T \leq 0{,}75$	low	Low information security level, the existing vulnerabilities of the computer system are not able to provide sufficient protection of information, the probability of information security threats.
$0{,}25 < P_T \leq 0{,}5$	very low	Very low information security level, the existing vulnerabilities of the computer system are not providing information protection, the emergence of information security threats is the most probable (constantly present).
$0 \leq P_T \leq 0{,}25$	unsatisfactory	Unsatisfactory information security level, information protection is not ensured, information security threats are constant (constantly present).

Proceeding from the mathematical model in the IISA, the overall information security effectiveness of the institution P_T is a criterion for conducting an assessment of the information security level and depends on the values it adopts.

CONCLUSIONS

Thus, the IISA is mandatory for all institutions. The clear implementation of the specified stages of the IISA will determine the cybersecurity effectiveness of the institution.

The IISA – is one of the most effective tools for obtaining an independent and objective assessment of the current level of institutions' protection from information security threats. In addition, the results of the IISA provide the basis for the formation of a strategy for the development of the cyber security system of institutions.

It is worth noting that IISA is appropriate to implement on a regular basis. In this case, the IISA will increase the information security level of the institution.

In addition, the result of the IISA is to obtain a real indicator of the overall information security effectiveness of the institution. This indicator is useful for a comparative analysis of the factors through which the institution will achieve the best results in ensuring information security, as well as to identify trends in improving the efficiency of productive resources, etc.

The peculiarity of the proposed system of information security assessment indicators of the institution is such that it covers economic indicators, technical and software parameters of the information security system and assesses the organizational measures and staff knowledge of the institution information security policy. Also, such information security indicators assessment system can be applied in any institution, regardless of its size, field and direction of activity, making it universal. At the meantime, it is worth noting this article reveals the main stages of the IISA methodology in the institution on the information security effectiveness, and some of the indicators, offered coefficients require additional study and research, which is a promising direction to further research.

REFERENCES

[1] Artemchuk, M.; Bezpartochnyi, M.; & Vysotska, V. Ensuring information security with firewalls at the Internet border. Actual Problems of Cybersecurity. Kyiv: State University of Telecommunications, 2020, 17–20.

[2] Korpan, Y. Information security threat classification in computer systems during remote data processing. In Information Protection Methods in Computer Systems and Networks. Data Registration, Storage, and Processing, 2015, 17(2), 39–46.

[3] Resolution of the Cabinet of Ministers of Ukraine from June 19, 2019, № 518 "On Approval of the General Cybersecurity Requirements for Critical Infrastructures", 2019. Retrieved from https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text

[4] Roy, Y.; Vysotska, V.; & Bezpartochnyi, M. Information Security Audit – The Basis of Effective Company Protection. Cybersecurity: Education, Science, Technology, 2018, 1(1), 86–93. https://doi.org/10.28925/2663-4023.2018.1.8693

[5] Resolution of the Executive Board of the National Bank of Ukraine. "On Approval of the Regulation on Control over Compliance by Banks with the Applicable Legal Requirements on Information Security, Cybersecurity, and Electronic Trust Services," 2021. Retrieved from 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. Retrieved from http://www.drs.gov.ua/wp-content/uploads/2021/07/dokument-6273_0_19-21.pdf

[7] Kononova, V.; Skochylias-Pavliv, O.; & Opirskyy, I. Evaluation of information resources protection. Lviv Polytechnic National University Institutional Repository, 2021, pp. 99–105. Retrieved from http://ena.lp.edu.ua

[8] Molodetskaya-Grynchuck, K. Method for assessing signs of threats to state information security in social Internet services. Automation of Technological and Business Processes, 2017, 9(2). Retrieved from http://atbp.onaft.edu.ua/

[9] Shtonda, R. Tasks and Stages of Independent Information Security Audit of Military Units (Institutions) on the Cybersecurity Effectiveness. Scientific and Practical Conference. Development and Application Prospects of Modern Systems and Means of Communication in the Interests of Troops Management, 2018, 22–23.

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

[11] West-Brown, M.; Stikvoort, D.; Kossakowski, K.-P.; Killcrece, G.; Ruefle, R.; & Zajicek, M. Handbook for Computer Security Incident Response Teams (CSIRTs). Handbook, CMU/SEI-2003-HB-002, 2003/ Retrieved from https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf

[12]Cyberspace Operations. Joint Publication, 2023, 3-12. Retrieved from https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-12/3-12-AFDP-CYBERSPACE-OPS.pdf

[13]NIST Special Publication 800-61. Revision 2. Computer Security Incident Handling Guide, 2020. Retrieved from https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

[14]Donegan, K. Computer Security Incident Response Teams, 2023. Retrieved from https://whatis.techtarget.com/definition/Computer-Security-Incident-Response-Team-CSIRT

[15]Nistir, A. Integrating Cybersecurity and Enterprise Risk Management (ERM), 2020. Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8286.pdf

[16]Managing Information Security Risk: Organization, Mission, and Information System, 2011. Retrieved from https://www.nist.gov/publications/managing-information-security-risk-organization-mission-and-information-system-view

[17] Practice Guide Draft. Privileged Account Management for the Financial Services Sector, 2020. Retrieved from https://www.nccoe.nist.gov/financial-services/privileged-account-management

[18]Rehman, S.; Allgaier, C.; & Gruhn, V. Security Requirements Engineering: A Framework for Cyber-Physical Systems. In 2018 International Conference on Frontiers of Information Technology (FIT), 2018, 315–320. https://doi.org/10.1109/FIT.2018.00062

[19]Security and Privacy Controls for Federal Information Systems and Organizations, 2021. Retrieved from https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf

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