УДК: 004.056.552
JEL Classification: C88, D83

Хаджинова О. В.[1], Хаджинова М. С.[2]

INFORMATION SECURITY AUDIT

O.Khadzhynova, M. Khadzhynova Information security audit.

The article defines that information security auditing aims to identify and assess potential issues and vulnerabilities in the operation of an enterprise's information systems. The essence and scope of different types of information security audits for enterprises are explored. A sequence for conducting an information security audit is proposed, highlighting its stages, each aimed at ensuring the protection of the enterprise's information system from unauthorized access while maintaining business continuity.

Key words: *information security; information technology; enterprises; information and telecommunication system; audit.*

Хаджинова О.В. Хаджинова М. С. Аудит інформаційної безпеки

У статті визначено, що аудит інформаційної безпеки спрямований на виявлення та оцінку потенційних проблем і вразливостей у роботі інформаційних систем підприємства. Досліджено сутність та масштаби різних видів аудиту інформаційної безпеки підприємств. Запропоновано послідовність проведення аудиту інформаційної безпеки з виділенням його етапів, кожен з яких спрямований на забезпечення захисту інформаційної системи підприємства від несанкціонованого доступу при збереженні безперервності бізнесу.

Ключові слова: інформаційна безпека; інформаційні технології; підприємства; інформаційно-телекомунікаційна система; аудит.

Problem Statement. The outbreak of the new coronavirus infection COVID-19 has had a serious impact on the political, socio-economic, and public life of the entire world. Today, business management must develop and adopt management decisions that will not only address the crisis phenomena caused by the pandemic but also quickly adapt to irreversible fundamental changes. The creation of new business opportunities, ensuring sustainable development of enterprises, and

[1] https://orcid.org/0000-0002-7750-9791
Хаджинова Олена Вікторівна, в.о. ректора ДВНЗ «Приазовський державний технічний університет», професор, доктор економічних наук, Дніпро khadzhynova_o_v@pstu.edu
Olena Khadzhynova, Acting Rector of SHEI «Pryazovskyi State Technical University», Professor, Doctor of Economic Sciences, Dnipro

[2] *https://orcid.org/0000-0001-8126-788X*
Хаджинова Марія Сергіївна*, магістр менеджменту, Харківський національний економічний університет імені Симона Кузнеця khadzhynova.mariia@gmail.com*
Mariia Khadzhynova, *master of Management degree applicant, Simon Kuznets Kharkiv National University of Economics*

strengthening competitiveness can be achieved through the implementation of the latest developments in information technology. Systematic scientific research has shown that the use of information technologies has led to the integration of economic processes into the digital space and requires changes in traditional approaches, principles, and management methods, which necessitate the construction of new models of enterprise management systems.

The transformation of economic processes has become one of the main vectors of socio-economic activity, leading to the development of online business, the influx of investments, the execution of transactions via e-commerce, improved efficiency in the allocation of financial resources, flexibility in banking operations, and increased productivity in many developed countries.

However, there is also a negative side to the digital transformation of economic processes. An imperfect legislative framework, the use of outdated IT infrastructure with unlicensed software, leads to an increase in unauthorized access, falsification of commercial secrets, fraudulent actions with business emails, and the cessation of business activities due to unexpected failures in information systems. The aforementioned negative consequences point to the growing problems of managing information security in enterprises under modern conditions.

Therefore, there is a need to assess the current level of information security, predict the risks and threats of hacker attacks and cyberterrorism aimed at stealing the enterprise's digital assets, falsification, blocking or copying confidential information, financial fraud, data destruction, manipulation of business processes, concealment of traces, and the system malfunctioning. Potential events that could harm information systems can be mitigated through regular auditing of the information security of the IT infrastructure and the enterprise's information system as a whole. These measures will help reduce or eliminate risks and threats associated with the leakage of commercial secrets, equipment being infected with malware, as well as correct the information security management system.

Analysis of Research and Publications. In modern scientific literature, information security auditing is presented as a key component of protecting an enterprise's information system. The theoretical and practical significance of information security auditing has been reflected in the research of Roj Ja. V., Mazur N. P., Skladannyj P. M. [1], Judin O. K., Zjubina R. V., Matvijchuk-Judina O. V. [2], Kryvoruchko O. V., Desjatko A. M., Sunichuk O. M. [3], and others.

However, the digital transformation of economic processes, the accelerated development of scientific and technological progress, and the increasing threats of the disclosure of confidential information and commercial secrets of enterprises require further study of information security auditing and the protection of the enterprise's information assets.

The aim of the article is to propose a step-by-step process for information security auditing that will reliably ensure the protection of the enterprise's information system from unauthorized access.

Main material. Today, information technologies play a significant role in ensuring the effective execution of business processes for business entities. The widespread use of information technologies in the operations of enterprises necessitates addressing issues related to data protection. The primary goal of any information security system is to create the necessary conditions for the enterprise's operation, prevent security threats, protect the legitimate interests of the enterprise from unlawful intrusions, and prevent the theft of financial assets, disclosure, loss, leakage, distortion, and destruction of confidential information. To assess the status of the enterprise's information infrastructure and develop methods to achieve the alignment of the infrastructure with business needs, as well as to achieve information security in the modern world, information security auditing serves as a key tool.

Information security auditing is a crucial component for the proper functioning of the entire information system of the enterprise. It is aimed at an objective, independent, and comprehensive assessment of the effectiveness, efficiency, and adequacy of the management system and information security measures of the enterprise. The audit helps to identify weak points, vulnerabilities, shortcomings, and potential problems in the functioning and implementation of the information security management system. Additionally, based on the results of the audit, proposals are developed for the modernization and standardization of the IT infrastructure with the aim of ensuring the enterprise's information security. These measures contribute to the creation of a culture of continuous improvement for the business entity.

The main goals of conducting an information security audit for an enterprise are to evaluate the correctness of the information security tasks in relation to business objectives, including legal obligations; analyze the implementation of information security tasks and controls; and analyze the performance of information security tasks by the organization's employees.

Thus, an information security audit is a comprehensive study and evaluation of the enterprise's information security management system. It allows for assessing the effectiveness, efficiency, and adequacy of the management system, the compliance of information systems with international standards for the collection, storage, and destruction of confidential information, as well as the security status of the entire IT infrastructure of the enterprise, including equipment, data centers, software, networks, and services.

A comprehensive information security audit combines several types of information security auditing checks for the enterprise (see Figure 1).

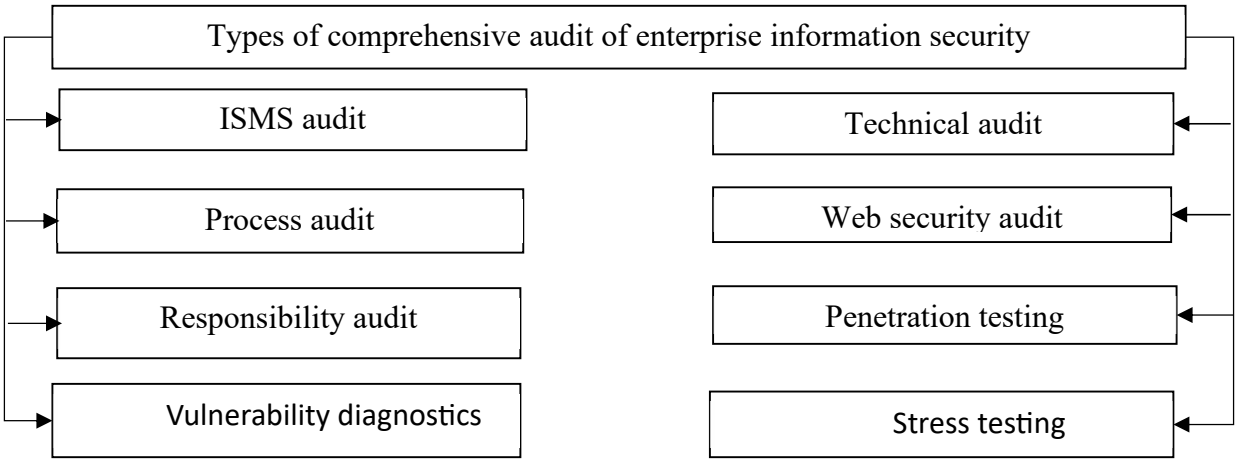

Fig. 1. Types of enterprise information security audits

The audit of the Information Security Management System (ISMS) assesses the compliance of the implemented information security measures and the introduced management system with the ISO/IEC 27001:2014 standard, "Information Technology. Security Techniques. Information Security Management Systems. Requirements" [4].

The ISMS audit allows for the formulation of recommendations regarding information security management. It enables the verification and modernization of the software involved in the comprehensive process of managing information security, and the systematic evaluation of IT architecture risks considering the impact of threats and vulnerabilities to the enterprise.

During the technical audit, the configurations of the information system or its components are checked according to the existing recommendations from manufacturers or internationally recognized organizations such as NIST, CIS, NSA, etc. This type of audit must be combined with a process audit, particularly if

deficiencies are found in domain controllers or vulnerability management processes that are not functioning effectively.

Within the "process audit," the settings of the processes used by the enterprise to ensure information security are verified. These may include processes related to access control, configuration management, vulnerability management, and other IT operations.

Web security audits prevent falsification, destruction, leakage of information, and threats typically caused by web applications. This type of information security audit provides comprehensive solutions for identifying various vulnerabilities in web applications, preventing unauthorized access to software over the internet, and more.

The audit of information security compliance with international ISO standards is considered a high-level audit. It includes best practices in the field of information security. The relevant audit requirements are reflected in international ISO/IEC standards: ISO/IEC 17799 "Information Technology. Information Security Management" [5], ISO/IEC 27001:2015 "Information Technology. Security Techniques. Information Security Management Systems. Requirements" [6], state standards DSTU 3396.1-96 "Information Protection. Technical Protection of Information. Procedures for Conducting Work," as well as in the Ukrainian legislative framework for information protection [7]. This type of audit checks the degree of compliance of the enterprise's information system with ISO 27000 standards and the internal information security requirements of the enterprise.

Thus, compliance auditing is a systematic process of reviewing documentation that shows how accurately an enterprise adheres to laws, regulations, and international ISO standards in the field of information security.

The next type of information security audit is called penetration testing. It allows for testing vulnerable areas of the information system by simulating a breach and attempting to penetrate the database server, authentication server, application server, and other systems, trying to bypass or disable security features.

Another type of information security audit is vulnerability diagnostics. It involves diagnosing the operating system, network, web applications, and middleware for vulnerabilities. By performing this diagnostic, the security status of web applications, the network, and the server is assessed, and risks of unauthorized access to the enterprise’s websites and applications are mitigated, thus preventing information leakage by identifying security issues.

Stress testing is yet another type of information security audit for enterprises. It helps businesses quickly diagnose their information system's ability to defend against hacker attacks and unauthorized access through online tests, which businesses encounter while operating in the internet space.

Thus, the aforementioned types of information security audits contribute to comprehensive protection of information systems, web applications, and software. They test vulnerable areas of the information system by simulating breaches of the database server, authentication server, and application server.

Information security audits are conducted in accordance with procedures defined in ISO/IEC 27007 to ISO/IEC 27009 standards. Figure 2 shows the various stages of the information security management system audit.

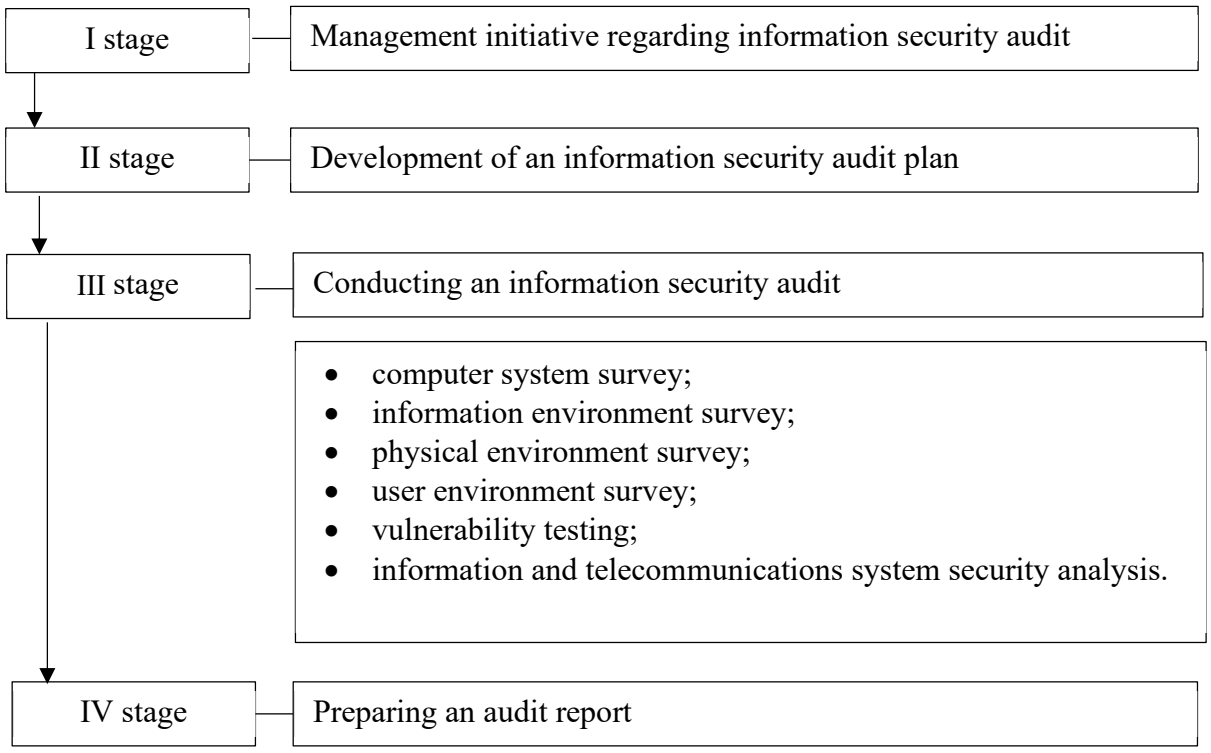

Fig. 2. Stages of an enterprise information security audit

In the first stage, the initiation of the information security audit is carried out by the top management of the enterprise. The head of the security service appoints the information security auditor, clearly defines their rights and responsibilities, and establishes the tasks and objectives of the audit. The auditor is fully responsible for the quality and effectiveness of the audit. They must possess sufficient knowledge and skills in the field of information security to identify and minimize risks and threats related to the audit program. The auditor is required to be able to define the

scope and objectives, select and use appropriate tools, and choose suitable auditing methods.

In the second stage, the audit plan is developed, ensuring the effective and efficient information security audit for the enterprise. It is impossible to cover all areas of the enterprise's information security within a single audit. Therefore, the audit should be planned for a specific period, typically around three years. The mid-term plan is a document that describes elements such as: the goals and scope of the audit, the information security audit policy, the approximate period of implementation, and the frequency of checks over a specified period. The mid-term audit plan for information security must be approved by the board of directors.

In recent years, there has been an intensive development of information technologies, computer hardware, telecommunications systems, and software for local and global networks, which requires the constant updating of enterprise management information systems. Continuous updates and changes must be controlled and able to ensure the preservation of the enterprise's information security. Therefore, it is necessary to conduct a systematic audit at a certain frequency within the current year.

The annual plan is an information security audit document that is developed based on the mid-term plan at the beginning of the financial year. It outlines the goals, priorities of the audit, the number and timing of the implementation of innovative information systems.

When determining and selecting the goals and topics for the audit, it is important to consider the components of information systems, networks, and digital assets that have the highest importance, urgency, and degree of vulnerability, as well as susceptibility to risks and threats from hacker attacks. The necessity of implementing new information systems must be documented. The annual plan must also be approved by the board of directors.

The information security auditor formulates a specific audit plan based on the annual plan. The implementation plan may describe the classification level and the average classification of information security audit elements. Additionally, applicable international ISO standards in the field of information security management systems may be outlined.

The head of the security service accepts the audit plan, which is then approved by the board of directors. After the audit plan is approved, the head of the security service informs the audited department about the schedule, appoints the responsible

person, requests materials from the previous audit, and makes adjustments to ensure effective auditing.

The third stage of the enterprise's information security audit is the most complex process. To carry out this audit effectively and efficiently, it is necessary to use the primary auditing methods: interviews, reviews, surveys, and inspections. These methods must be documented and can be used not only within the enterprise but also for remote audits of the enterprise's information security.

At the information security audit stage, a comprehensive examination of the information and telecommunications system is conducted, including: examination of the computing system, examination of the information and physical environment, examination of user environments, vulnerability testing.

During the examination of the enterprise's computing system, the following aspects are described:

- The availability of documentation for the information and telecommunications system and its components (passport of the information and telecommunications system).

- The overall structural diagram of the information and telecommunications system and its components (list and composition of equipment, technical and software tools, their connections, configuration features, architecture, and topology, software and hardware protection tools, and their mutual placement).

- Types and characteristics of communication channels.

- Features of the interaction between the components of the information and telecommunications system.

- Possible limitations on the use of assets.

Additionally, during the examination of the computing system, components that serve as information protection tools or contain protection mechanisms must be identified. Specifically, the potential capabilities of these tools and mechanisms, their properties, and characteristics, including those set by default, should be described.

During the examination of the enterprise's information environment, the following aspects are described:

- Characteristics of the processed information.

- Types of information circulating in the information and telecommunications system and the requirements for its protection.

- Types of objects where information is stored.

- Features of information processing technology.
- Information flow diagrams.
- Access modes to information.
- Information carriers and the procedures for handling them.

During the examination of the physical environment of the information and telecommunications system, the following characteristics are examined:

- The territorial placement of the components of the information and telecommunications system (master plan, situational plan).
- The presence of a guarded area and access control procedures on the premises.
- The presence of designated rooms where components are located.
- The presence of security and fire alarms, video surveillance systems, and access control systems in the premises.
- The access mode to components of the physical environment of the information and telecommunications system.
- The impact of environmental factors on information security.
- The presence of communication elements, life support systems, and communications systems in premises that have access beyond the controlled area.
- Conditions for storing magnetic, optical-magnetic, paper, and other information carriers.
- The availability of design and operational documentation for the physical environment components.

During the user environment examination, the following aspects are described:

- The presence of regulatory documents governing the activities of enterprise personnel regarding the security of information in the information and telecommunications system.
- The presence of an information security department (unit), its functions, and responsibilities.
- The functional and quantitative composition of users of the enterprise's information and telecommunications system, their functional duties, and level of qualification.
- Categories of users based on their authority levels.
- The authority of users regarding the organization of access to information processed in the information and telecommunications system.

- The authority of users to manage assets or protection mechanisms in the information and telecommunications system.

During vulnerability testing, all components of the information and telecommunications system are scanned, and penetration tests are conducted if necessary.

In the security analysis phase, the results of the examination are analyzed and systematized, identifying vulnerabilities and assessing the level of protection of the enterprise's information and telecommunications system.

Based on the results of the security analysis, a report is prepared, and recommendations are made to neutralize the identified vulnerabilities. For this purpose, a protocol for threats and vulnerabilities in the enterprise's information security is maintained during the audit. Additionally, the information obtained about the audit process is confidential and must not be disclosed to anyone except the enterprise's management.

Based on the audit protocol, an audit report is prepared, which indicates the effective functioning level of the working cycle, the degree of vulnerability of information assets, networks, and the information system as a whole to cyberattacks aimed at intellectual property theft, and reflects the information protection measures against hacker attacks. Furthermore, the auditor provides recommendations for the modernization and development of the enterprise's information system, as well as suggestions for improving its functionality.

Based on the results of the audit, the management initiates actions to modernize the enterprise's information security management system.

Conclusions and Prospects for Further Research. Thus, an audit of the enterprise's information and telecommunications system provides company management with an objective assessment of its current state, processes, and events related to its operation. It helps determine the compliance of the information system with the enterprise's management requirements for supporting business processes. During the audit process, the enterprise receives formalized descriptions of the existing information architecture, as well as the connection between the software-hardware architecture of the information system and the operations of the corresponding technological and functional departments.

The information security audit is aimed at an independent, comprehensive evaluation of the effectiveness, efficiency, and adequacy of the information security management system. The audit focuses on creating centralized access control

systems, protecting the enterprise's management system, ensuring business continuity, and establishing functions to combat hacker attacks, illegal income, and fraud.

Conducting a qualified information security audit and implementing the set of measures for protecting information resources based on the recommendations developed as a result of the audit provides confidence in the security of the information and telecommunications system for a certain period. Since high technologies are evolving dynamically, and with them, the means of committing IT crimes are also improving, the information security audit of the enterprise should be carried out periodically and at an increasingly technologically advanced level. Only with this approach will the audit yield positive results and contribute to the improvement of the enterprise's information security.

References:

1. *Roj Ja. V., Audyt informacijnoji bezpeky - osnova efektyvnogho zakhystu pidpryjemstva / Ja. V. Roj, N. P. Mazur, P. M. Skladannyj // Kiberbezpeka: osvita, nauka, tekhnika. – 2018. – № 1. – S. 86-93. – Access mode: http://nbuv.gov.ua/UJRN/cest_2018_1_11*
2. *Judin O. K. Suchasni praktyky vprovadzhennja systemy audytu informacijnoji bezpeky na ob'jektakh krytychnoji infrastruktury / O. K. Judin, R. V. Zjubina, O. V. Matvijchuk-Judina // Naukojemni tekhnologhiji. – 2019. – # 1. – S. 36-43. – Access mode: http://nbuv.gov.ua/UJRN/Nt_2019_1_7*
3. *Kryvoruchko O. V. Modeljuvannja informacijnoji systemy provedennja nezalezhnogho audytu informacijnoji bezpeky / O. V. Kryvoruchko, A. M. Desjatko, O. M. Sunichuk // Upravlinnja rozvytkom skladnykh system. – 2020. – Vyp. 43. – S. 67-75. – Access mode: http://nbuv.gov.ua/UJRN/Urss_2020_43_12*
4. *DSTU ISO/IEC 27001:2014 Informacijni tekhnologhiji. Metody bezpeky. Systemy menedzhmentu informacijnoju bezpekoju. Vymoghy (ISO/IEC 27001:2013;ISO/IEC 27001:2013/Cor 1:2014;IDT)*
5. *DSTU ISO / IEC: 17799 «Informacijni tekhnologhiji. Upravlinnja informacijnoju bezpekoju».*
6. *DSTU ISO/IEC 27001:2015 Informacijni tekhnologhiji. Metody zakhystu. Systemy upravlinnja informacijnoju bezpekoju. Vymoghy (ISO/IEC 27001:2013; Cor 1:2014, IDT)*
7. *DSTU 3396.1-96 Zakhyst informaciji. Tekhnichnyj zakhyst informaciji. Porjadok provedennja robit.*