DOI: https://doi.org/10.32782/2308-1988/2026-59-71
UDC 005.934:004.056

Lesia Gnylianska
PhD in Economics, Associate Professor,
National University "Lviv Polytechnic"
ORCID: https://orcid.org/0000-0003-2924-7165

Nestor Shpak
Doctor of Economics, Professors,
Professor of the Department of Management and International Entrepreneurship,
National University "Lviv Polytechnic"
ORCID: https://orcid.org/0000-0003-0620-2458

Svyatoslav Kis
Doctor of Philosophy, Senior Research Fellow,
National University "Lviv Polytechnic"
ORCID: https://orcid.org/0000-0002-2710-2520

**Гнилянська Леся Йосифівна, Шпак Нестор Омельянович,
Кісь Святослав Юліанович**
Національний університет «Львівська політехніка»

ENSURING THE CONFIDENTIALITY OF INFORMATION OF ENTERPRISES IN THE CONTEXT OF DIGITALIZATION

ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ІНФОРМАЦІЇ ПІДПРИЄМСТВ В УМОВАХ ДІДЖИТАЛІЗАЦІЇ

Summary. The article is devoted to topical issues of ensuring the confidentiality of information of enterprises in the context of digitalization. The theoretical and applied foundations of data protection in the process of digital transformation of business, which is accompanied by increased cyber threats, complication of information flows and growing security requirements, are studied. Key risks, including cybernetic, insider, technological, and organizational, are summarized. Regulatory and legal support and modern security tools, including encryption, multi-factor authentication and the Zero Trust approach, are analyzed. The expediency of the transition to adaptive models of information security management has been substantiated. A multi-level model of ensuring confidentiality is proposed, which integrates strategic and operational mechanisms and provides for continuous improvement of the protection system.

Keywords: information privacy, information security, digitalization, cyber threats, Zero Trust, cyber resilience, risk management, data protection, enterprise.

Анотація. Стаття присвячена актуальним питанням забезпечення конфіденційності інформації підприємств у контексті цифровізації та зростаючої ролі інформаційних ресурсів у формуванні конкурентних переваг бізнесу. Стаття поглиблює теоретичні та прикладні основи захисту інформації в контексті цифрової трансформації, що супроводжується активацією кіберзагроз, ускладненням інформаційних потоків, зростанням обсягів даних та підвищенням вимог до ефективності систем інформаційної безпеки. Узагальнено та систематизовано базові загрози конфіденційності інформації, серед яких виділяються кібератаки, ризики з боку інсайдерів, технологічні вразливості інформаційних систем та недоліки управління організацій. Проаналізовано інституційну та юридичну підтримку захисту інформації, а також сучасні організаційні, економічні та технологічні інструменти, зокрема шифрування даних, багатофакторна автентифікація, системи запобігання витокам інформації та концепція Zero Trust як основи для створення безпечного цифрового середовища. Підтверджено необхідність переходу від традиційних підходів до адаптивних моделей управління інформаційною безпекою, зосереджених на управлінні ризиками, гнучкості та забезпеченні кіберстійкості підприємства. Запропоновано авторами багаторівневу адаптивну модель для забезпечення конфіденційності інформації, яка інтегрує інституційно-регуляторний, стратегічний та операційний рівні управління та включає організаційні, технологічні, економічні та кадрові компоненти. Особливістю цієї моделі є використання адаптивного циклу керування на основі зворотного зв'язку, який забезпечує постійне оновлення та вдосконалення системи захисту відповідно до змін зовнішнього середовища. Набули подальшого розвитку підходи до тлумачення конфіденційності як динамічної характеристики інформаційної системи підприєм-

© Lesia Gnylianska, Nestor Shpak, Svyatoslav Kis, 2026
Стаття поширюється на умовах ліцензії відкритого доступу (CC BY 4.0)

ства та обґрунтовано визначальну роль людського фактору в забезпеченні інформаційної безпеки. Практичне значення отриманих результатів полягає в можливості використання запропонованих підходів і моделі для підвищення рівня безпеки інформаційних ресурсів підприємств в сучасній цифровій економіці.

Ключові слова: конфіденційність інформації, інформаційна безпека, діджиталізація, кіберзагрози, кіберстійкість, управління ризиками, захист даних, підприємство.

Statement of the problem. The rapid digitalization of the economy and the active introduction of information and communication technologies in the activities of enterprises lead to significant transformations of business processes and approaches to the management of information resources. At the same time, the dependence of business entities on digital data is growing, which increases vulnerability to cyber threats, information leaks, and unauthorized access. In modern conditions, the confidentiality of information becomes not only a technical, but also a strategic category that determines the level of competitiveness and economic security of the enterprise.

Despite the presence of a significant number of scientific studies in the field of information security, the existing approaches to ensuring the confidentiality of information are mostly fragmented and do not take into account the complex impact of digital transformation on all levels of enterprise management. The problem of integrating organizational, technological, economic and personnel aspects into a single system of ensuring confidentiality, capable of adapting to dynamic changes in the external environment, is of particular relevance.

In addition, there is an insufficient level of coherence between institutional and legal regulation and the practice of implementing modern information protection tools, which complicates the formation of an effective information security management system. Traditional models, focused mainly on technical means of protection, do not provide an adequate level of cyber resilience in the face of growing risks and complexity of information systems.

Thus, there is an objective need to develop comprehensive adaptive approaches to ensuring the confidentiality of information of enterprises that take into account the modern challenges of digitalization, integrate different levels of management and ensure continuous improvement of the information security system. This determines the relevance and practical significance of this study.

Analysis of recent research and publications. The problem of ensuring the confidentiality of information of enterprises in the context of digitalization is the subject of active scientific research both in domestic and foreign scientific literature. Considerable attention is paid to the implementation of information security management systems based on international standards. Thus, in the works of V. Petrashko and O. Ulichev [7], a systematic review of research on the ISO/IEC 27001 standard, which defines the requirements for the construction of an information security management system (ISMS), was carried out. The authors found that the main areas of research are the motivation for the implementation of the standard, implementation problems, application results and contextual factors of its effectiveness. The problems of ensuring the confidentiality of personal data in the digital environment are studied in the works of V. Balatska and I. Opirskyi [1], where the expediency of using blockchain technologies as a tool for increasing the level of cybersecurity and information protection is substantiated. An important direction of modern research is taking into account the human factor in the information security system. Thus, N. Kukharska and A. Lagun [5] consider human resource management as a component of information security, emphasizing the role of personnel training and the formation of a security culture in organizations. The issue of countering modern cyber threats, in particular ransomware, is studied in the works of A. Partyka, O. Harasymchuk, O. Nemkova and others [6], where the use of artificial intelligence models in information security management systems is proposed. Special attention is paid to the legal aspects of ensuring information security. In particular, O. Skochylias-Pavliv [8] examines the mechanisms of regulatory regulation of information security in Ukraine, focusing on the need to adapt them to modern digital challenges. The works of N. Yuzikova [10] consider the issues of preventing cybercrime and forming an effective information security system, taking into account international experience.

Highlighting previously unresolved parts of the overall problem. At the same time, the analysis of scientific publications shows that, despite the significant level of research on certain aspects of information security, insufficient attention has been paid to the development of complex adaptive models for ensuring the confidentiality of information of enterprises, which would integrate organizational, technological, economic and personnel components in the context of digitalization.

The article is aimed at substantiating the theoretical foundations and developing scientific and practical approaches to ensuring the confidentiality of information of enterprises in the context of digitalization, as well as the formation of the author's model of privacy management based on the integration of organizational, technological and economic mechanisms. To achieve this goal, the following tasks have been defined: to reveal the essence of information confidentiality as a component of information security of an enterprise in the context of digital transformation; analyze

modern threats to the confidentiality of information of enterprises, in particular cyber threats, insider risks and technological vulnerabilities; to investigate the institutional and legal support of information protection and its compliance with international standards; to generalize the organizational and economic mechanisms for ensuring the confidentiality of information at enterprises; to characterize modern technological tools for information protection in the context of digitalization and to substantiate the need to apply adaptive and risk-based approaches to information confidentiality management; to develop an author's multi-level model for ensuring the confidentiality of information of the enterprise and to propose an approach to assessing the effectiveness of ensuring the confidentiality of information of the enterprise.

Summary of the main research material. In the current conditions of digital transformation of the economy, ensuring the confidentiality of information of enterprises acquires a systematic and interdisciplinary character, combining technological, organizational, economic and managerial aspects. The growth of data volumes, the active use of cloud services, the automation of business processes and the development of network interactions significantly increase the level of information risks and require a revision of traditional approaches to information security management.

Effective ensuring of information confidentiality involves not only the introduction of modern technical means of protection, but also the formation of a holistic management system focused on identifying, assessing and minimizing risks. It is important to harmonize the internal policies of the enterprise with the current regulatory framework, as well as to increase the level of awareness of personnel on information security issues.

In this context, there is a need for a comprehensive study of modern approaches to ensuring the confidentiality of information of enterprises, analysis of key threats and tools for their neutralization, as well as substantiation of effective management models capable of adapting to the dynamic conditions of the digital environment. This determines the logic of further presentation of the material aimed at revealing the theoretical foundations, analyzing practical tools and developing adaptive approaches to ensuring the confidentiality of information.

Information confidentiality is a key component of the information security of the enterprise, which provides for restricting access to data only for authorized persons and preventing their unauthorized disclosure [5]. In the context of digital transformation, its importance is growing significantly, as enterprises actively use digital platforms, cloud services, and large amounts of data, which increases the risks of information leakage.

The essence of confidentiality lies not only in technical data protection, but also in the formation of a comprehensive access control system, which includes organizational regulations, technological tools (encryption, authentication) and control of personnel behavior [1]. In modern conditions, it is considered as a dynamic characteristic of the information system, which requires constant monitoring, adaptation to new threats and integration with other security elements – integrity and availability of information [7].

At the same time, ensuring the confidentiality of information in the digital environment is complicated by the constant evolution of technologies and the expansion of the range of information risks. The growth in the number of data processing and transmission channels, the use of remote services and the human factor form new vulnerabilities in security systems. In this regard, it is advisable to consider in more detail the main threats to information confidentiality in the context of digitalization (Table 1), since the digitalizationof business processes significantly expands the range of threats to the information security of enterprises.

Table 1 – The main threats to the confidentiality of information of enterprises in the context of digitalization

Threat group	Characteristics	Consequences
Cyber threats	Phishing, virus attacks, ransomware	Data loss, financial loss
Insiders	Personnel errors, information leakage	Reputational risks
Technological	Software vulnerabilities, cloud risks	Unauthorized access
Organizational	Lack of security policies	Uncontrolled access
External	Cyberattacks by competitors, hackers	Commercial losses

Source: formed by the authors according to [1; 4]

The human factor, which is the cause of a significant share of information security incidents, is especially dangerous. In addition, the spread of remote work increases the risks of data leakage through insufficiently secure communication channels.

At the same time, effective counteraction to these threats is impossible without a proper regulatory framework and coordinated institutional regulatory mechanisms. Ensuring the confidentiality of information requires a clear definition of legal norms, standards and responsibilities of business entities in the field of data processing and protection. In this context, the study of institutional and legal provision of information confidentiality is of great importance. In particular, the Law of Ukraine "On Protection of Information in Information and Communication Systems" [2], the Law of Ukraine "On Personal Data Protection" [3]. At the international level, an

important role is played by: GDPR (General Data Protection Regulation), ISO/IEC 27001[9]. In the context of Ukraine's European integration, the issue of harmonization of national legislation with European norms is relevant, which increases the requirements for information protection systems of enterprises.

At the same time, the presence of a developed regulatory framework in itself does not guarantee an adequate level of information protection without the effective implementation of the relevant provisions at the enterprise level. Practical assurance of confidentiality requires the introduction of effective management approaches, rational allocation of resources and the formation of internal mechanisms of control and responsibility. In this regard, it is advisable to consider the organizational and economic mechanism for ensuring the confidentiality of information. Effective provision of information confidentiality involves the formation of a comprehensive information security management system of the enterprise. The main elements of which are: implementation of information security policy; control of access to information; risk assessment and minimization; staff training; information security audit.

The implementation of the organizational and economic mechanism for ensuring the confidentiality of information needs to be specified in the form of practical means and managerial decisions used at the enterprise level. It is the toolkit that allows you to transform general approaches into effective protection measures, ensuring access control, minimizing risks and increasing the efficiency of information security management. In this context, it is advisable to move on to the consideration of organizational, economic, technological tools, andrelevant technologies for the protection and provision of confidential information (Tab. 2–3).

Table 2 – Organizational and economic tools for ensuring the confidentiality of the enterprise

Tool	Essence	Effect
Security Policy	Data Access Regulation	Risk reduction
Risk Management	Threat Identification	Increased security
Staff training	Building a Safety Culture	Reduction of the human factor
Audit	Verification of security systems	Vulnerability Detection

Source: formed by the authors according to [5–6]

Organizational and economic tools for ensuring the confidentiality of information cover a set of managerial and financial and economic measures aimed at forming an effective data protection system at the enterprise level. These include information security policies, regulation of access to information resources, a system for distributing responsibility, motivational mechanisms for personnel, as well as planning and optimization of information security costs. An important role is also played by risk assessment and the formation of a budget for information protection measures, which ensures the rational use of resources. At the same time, organizational and economic tools are effective only if they are supported by modern technological solutions that directly protect information flows and prevent unauthorized access. In this context, it is advisable to consider technological tools to ensure the confidentiality of information. The main tools include: data encryption; multi-factor authentication; DLP systems; IDS/IPS systems; Zero Trust Architecture; blockchain technologies.

Table 3 – Modern technologies for protecting confidential information of the enterprise

Technology	Purpose	Dignity
Encryption	Data protection	High level of security
MFA	Access control	Reduction of unauthorized entry
DLP	Leak prevention	Data Transfer Control
Zero Trust	Full access verification	Risk minimization

Source: formed by the authors under [4; 5]

The development of digital technologies and the complexity of cyber threats necessitate the rethinking of traditional approaches to information protection. Organizational, economic and technological tools are increasingly being integrated into a single information security management system focused on risk, adaptability and continuous improvement. In this context, the study of the transformation of approaches to privacy in the context of digitalization is of particular relevance. Digitalization contributes to the transition to new models of information security management: from a reactive to proactive approach; from isolated systems to integrated platforms; from static protection to adaptive risk management.

The role of: cybersecurity automation is growing; the use of artificial intelligence and the concept of cyber resilience of enterprises.

An important stage in the information security management system is the assessment of the effectiveness of ensuring the confidentiality of information, which allows you to determine the level of data protection and the effectiveness of the implemented measures. Such an assessment is based on the comprehensive use of both qualitative and quantitative methods, including information security audits, penetration testing, cybersecurity incident analysis, and a system of key performance indicators (KPIs) in the field of information security. The main

indicators of the level of confidentiality include the number and nature of security incidents, the volume or frequency of data breaches, the speed of response to threats, as well as the level of compliance of information systems with current security standards and requirements. The results of the assessment serve as a basis for improving information protection policies and mechanisms. The obtained results of the assessment of the level of information confidentiality form the basis for further improvement of the information security system of the enterprise and the transition from fragmentary measures to integral management decisions. It is on this basis that it becomes possible to substantiate integrated approaches that ensure the integration of different levels of management and information security tools.

In this regard, it is expedient to apply an adaptive multi-level model for ensuring the confidentiality of enterprise information in the context of digital transformation, which is considered as an integrated information security management system focused on the constant identification, assessment and minimization of risks in a dynamic digital environment (Fig. 1).

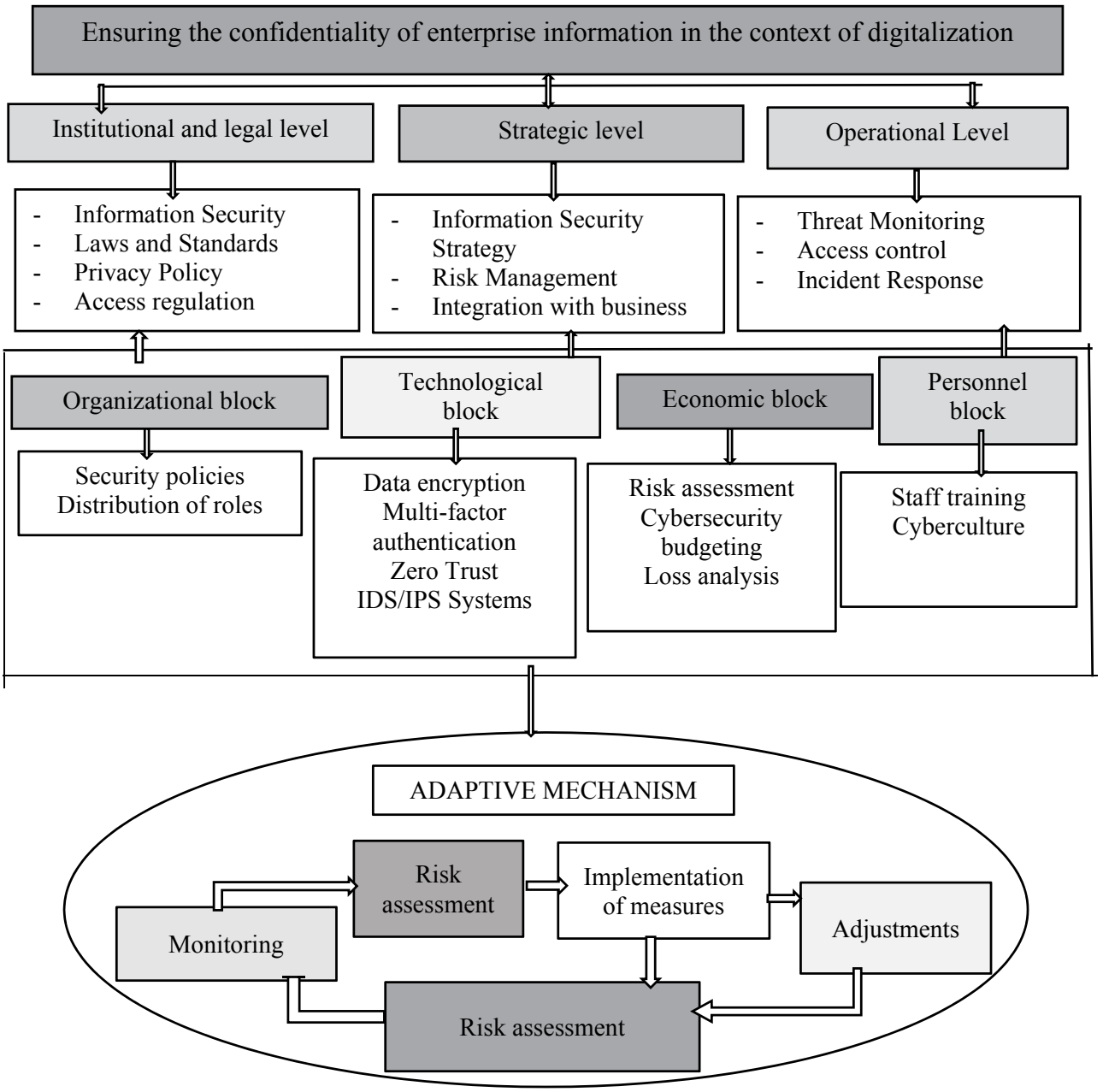

Figure 1 – Adaptive multi-level model for ensuring the confidentiality of enterprise information in the context of digital transformation

Source: generated by the authors

The proposed model for ensuring the confidentiality of enterprise information is a multi-level adaptive system that operates in a dynamic digital environment and integrates institutional, regulatory, strategic and operational components based on a risk-based approach. Its scientific novelty lies in the transition from static and fragmented protection mechanisms to a holistic dynamic privacy management system that combines technological, organizational, economic and human resources tools in a single decision-making circuit. The proposed model is based on a combination of institutional, legal, strategic and operational levels of management. Its structure includes interrelated functional blocks: organizational (access regulation, security policies, distribution of responsibility), technological (encryption, multi-factor authentication, intrusion detection systems), economic (risk assessment, budgeting of security measures) and personnel (staff training, formation of a cybersecurity culture). A feature of the model is the allocation of the personnel component as equivalent to the technological one, which allows reducing the influence of the human factor as one of the main sources of information risks. The model covers the external digital environment, which forms the spectrum of cyber threats and regulatory requirements, the institutional and regulatory level, which sets the regulatory framework, the strategic level, focused on the formation of cyber resilience and risk management policies, as well as the operational level, which is implemented through organizational, technological, economic and personnel blocks. The central element of the model is an adaptive control mechanism based on the cycle of "identification – assessment – response – learning" and ensures continuous improvement of the protection system. Additionally, a monitoring and feedback system is provided, which includes audits, KPIs, vulnerability testing and incident analysis. The result of the model implementation is to increase the level of information confidentiality, strengthen the cyber resilience of the enterprise and minimize the risks of data leakage. Among the main features of the model is its adaptability, which is realized through a continuous feedback loop (Fig. 2).

This approach ensures a timely response to changes in the external environment and an increase in the level of cyber resilience of the enterprise. Thus, the proposed model allows you to move from reactive to proactive management of information confidentiality, ensuring its protection as a dynamic resource in the context of digital transformation.

Conclusions. Summarizing the results of the study, it should be noted that ensuring the confidentiality of information of enterprises in the context of digitalization is a complex and multi-level process that requires the coordinated application of legal, organizational, economic and technological mechanisms. It has been established that the strengthening of cyber threats and the acceleration of digital transformation of the business environment necessitate the transition to adaptive, risk-oriented models of information security management focused on ensuring the cyber resilience of enterprises.

Within the framework of the study, the theoretical approach to the interpretation of information confidentiality as a dynamic characteristic of the digital system of an enterprise, which changes under the influence of external and internal factors and requires constant managerial adjustment, has been improved. An integrated model of privacy has been developed, which combines organizational, economic and technological tools based on a risk-based approach and principles of adaptive management. A system for assessing the level of confidentiality of information of an enterprise, based on a combination of quantitative and qualitative indicators, which allows to comprehensively determine the effectiveness of the information security system and timely identify critical deviations, is proposed. The expediency of using the concept of Zero Trust in combination with cyber resilience approaches as a modern basis for building an effective information security system of enterprises, which ensures minimization of the risks of unauthorized access and data leakage, has been substantiated. The scientific approach to the impact of digitalization processes on the transformation of information protection mechanisms of enterprises has been further developed, which allows us to consider information security as a continuous adaptive process integrated into the system of strategic management of the enterprise.

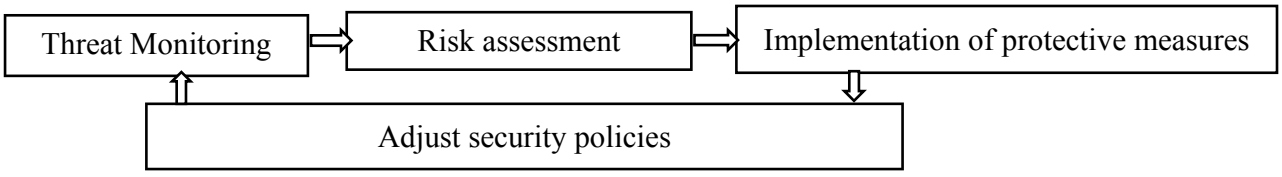

Figure 2 – Continuous feedback loop in the adaptive system for ensuring the confidentiality of information of the enterprise

Source: generated by the authors

References:

1. Balatska, V., & Opirskyi, I. (2023). Zabezpechennia konfidentsiinosti personalnykh danykh i pidtrymky kiberbezpeky za dopomohoiu blokcheinu. [Ensuring the confidentiality of personal data and maintaining cybersecurity using blockchain]. *Kiberbezpeka: Osvita, Nauka, Tekhnika,* vol. *4*(20). DOI: https://doi.org/10.28925/2663-4023.2023.20.619 (in Ukrainian)
2. Law of Ukraine. (1994, July 5). *On protection of information in information and telecommunication systems* [On Information Protection in Information and Communication Systems]. (No. 80/94-VR). *Vidomosti Verkhovnoi Rady Ukrainy, 31*, Art. 286. (in Ukrainian)
3. Law of Ukraine. (2010, June 1). *On personal data protection. [*On the protection of personal data]. (No. 2297-VI). *Vidomosti Verkhovnoi Rady Ukrainy, 34*, Art. 481. (in Ukrainian)
4. Kukharska, N., & Lahun, A. (2023). Upravlinnia liudskymy resursamy yak skladova informatsiinoi bezpeky orhanizatsii. [Human Resource Management as a Component of the Organization's Information Security*]. Kiberbezpeka: Osvita, Nauka, Tekhnika,* vol. *4*(20). DOI: https://doi.org/10.28925/2663-4023.2023.20.3544 (in Ukrainian)
5. Lande, D., Puchkov, O., Subach, I., & Rybak, O. (2023). Informatsiini tekhnolohii zabezpechennia informatsiinoi bezpeky derzhavy. [Information Technologies for Ensuring the Information Security of the State]. *Kiberbezpeka: Osvita, Nauka, Tekhnika,* vol. *4*(20). DOI: https://doi.org/10.28925/2663-4023.2023.20.142152 (in Ukrainian)
6. Partyka, A., Harasymchuk, O., Niemkova, O., Sovyn, Y., & Dudykevych, V. (2024). Rozroblennia metodu doslidzhennia kiberzlochyniv za typom virusiv-vymahachiv z vykorystanniam modelei shtuchnoho intelektu. *[*Development of a method for researching cybercrimes by type of ransomware viruses using artificial intelligence models]*, Naukovi zapysky (CSN)* vol. *6*(1). DOI: https://doi.org/10.23939/csn2024.01.015 (in Ukrainian)
7. Petrashko, V., & Ulichev, O. (2023). Doslidzhennia isnuiuchykh pidkhodiv dlia stvorennia bezpechnoi merezhi. [Exploring existing approaches to building a secure network*]. Molodyi vchenyi,* vol. *12*(124). DOI: https://doi.org/10.32839/2304-5809/2023-12-124-3 (in Ukrainian)
8. Skochylias-Pavliv, O. V. (2023). Suchasni zahrozy informatsiinii bezpetsi Ukrainy v umovakh pravovoho rezhymu voiennoho stanu. [Modern Threats to Ukraine's Information Security under the Legal Regime of Martial Law]. *Yurydychnyi naukovyi elektronnyi zhurnal,* vol. *9*, pp. 263–266. DOI: https://doi.org/10.32782/2524-0374/2023-9/65 (in Ukrainian)
9. International Organization for Standardization. (2022). *ISO/IEC 27001:2022 information security, cybersecurity and privacy protection—Information security management systems—Requirements*. ISO.
10. Yuzikova, N. (2023). Informatsiina bezpeka u systemi zakhodiv zapobihannia kryminalnym pravoporushenniam u sferi IT. [Information Security in the System of Measures to Prevent Criminal Offenses in the IT Sector]. *Analitychno-porivnialne pravoznavstvo*. DOI: https://doi.org/10.24144/2788-6018.2023.05.91 (in Ukrainian)

Список використаних джерел:

1. Балацька В., Опірський І. Забезпечення конфіденційності персональних даних і підтримки кібербезпеки за допомогою блокчейну. *Кібербезпека: освіта, наука, техніка*. 2023. № 4 (20). DOI: https://doi.org/10.28925/2663-4023.2023.20.619
2. Закон України «Про захист інформації в інформаційно-комунікаційних системах» від 05.07.1994 № 80/94-ВР. Відомості Верховної Ради України. 1994. № 31. Ст. 286.
3. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI. Відомості Верховної Ради України. 2010. № 34. Ст. 481.
4. Кухарська Н., Лагун А. Управління людськими ресурсами як складова інформаційної безпеки організації. *Кібербезпека: освіта, наука, техніка*. 2023. № 4 (20). DOI: https://doi.org/10.28925/2663-4023.2023.20.3544 (дата звернення: 05.04.2026)
5. Ланде Д., Пучков О., Субач І., Рибак О. Інформаційні технології забезпечення інформаційної безпеки держави. *Кібербезпека: освіта, наука, техніка*. 2023. № 4 (20). DOI: https://doi.org/10.28925/2663-4023.2023.20.142152
6. Партика А., Гарасимчук О., Нємкова О., Совин Я., Дудикевич В. Розроблення методу дослідження кіберзлочинів за типом вірусів-вимагачів з використанням моделей штучного інтелекту. *Наукові записки (CSN)*. 2024. Вип. 6, № 1. DOI: https://doi.org/10.23939/csn2024.01.015 (дата звернення: 05.04.2026)
7. Петрашко В., Улічев О. Дослідження існуючих підходів для створення безпечної мережі. *Молодий вчений*. 2023. № 12 (124). DOI: https://doi.org/10.32839/2304-5809/2023-12-124-3 (дата звернення: 05.04.2026)
8. Скочиляс-Павлів О.В. Сучасні загрози інформаційній безпеці України в умовах правового режиму воєнного стану. *Юридичний науковий електронний журнал.* 2023. №9. С. 263–266 DOI: https://doi.org/10.32782/2524-0374/2023-9/65
9. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva: ISO, 2022.
10. Юзікова Н. Інформаційна безпека у системі заходів запобігання кримінальним правопорушенням у сфері ІТ. *Аналітично-порівняльне правознавство*. 2023. DOI: https://doi.org/10.24144/2788-6018.2023.05.91

Дата надходження статті: 09.04.2026
Дата прийняття статті: 30.04.2026
Дата публікації статті: 15.05.2026