UDC 657:004
JEL classification: M40, M41, D24
DOI: 10.35774/visnyk2026.01.168

Risks of Accounting Digitalization by Stages of the Information Systems Life Cycle

Vasyl Muravskyi[1]

Abstract.

Introduction. *The digitalization of socio-economic processes has led to the transformation of accounting. Under the influence of digitalization trends, the methodology and organization of accounting are undergoing significant changes. The digital transformation of accounting is inevitably associated with risks and threats to enterprise operations. In order to avoid and minimize the negative consequences of accounting digitalization, it is necessary to identify and classify risks, taking into account the current level of development of information technologies and systems. Purpose of the article is to identify, classify, and systematize the risks of digitalization of accounting at various stages of implementing enterprise management information systems and to find ways to eliminate the sources of occurrence and minimize the consequences of cyber threats.. The expediency of identifying and systematizing potential risks and threats of accounting digitalization is substantiated through the manifestation of negative trends in the following areas: the functioning of accounting professionals, the organization of accounting, and the use of innovative technologies in the processing of accounting information. The necessity of classifying accounting digitalization risks according to the life-cycle stages of the development and implementation of enterprise management information systems is proven. Digitalization risks in accounting are systematized by stages, namely: the stage of studying the enterprise's economic activity, system identification, selection and planning; the stage of pre-project assessment; the stage of information system design; the stage of implementation and operation of the information system; the stage of controlling current risks through monitoring of system functioning; and the stage of assessing operating costs and performance efficiency. Consideration of the life cycles of the development and implementation of enterprise management information systems ensures the achievement of comprehensive and maximum effects from the digitalization of accounting information processing without negative consequences for the efficient functioning of the enterprise. At each stage of the development and implementation of enterprise management information systems, specific risks of accounting digitalization arise. Taking into account the negative trends of the digital transformation of accounting in the context of the life-cycle stages of information systems ensures the concentration of attention of accounting and security specialists on particular risks and threats of digitalization. The proposed classification of risks and their consideration in the organization of accounting by individual stages provides the most optimal form of digitalization of accounting processes at the enterprise.*

Keywords: *digitalization, accounting, information systems, information technologies, life-cycle stages, enterprise management.*

Received: 18 January 2026 | **Revised:** 19 January 2026 | **Accepted:** 15 February 2026 | **Published:** 28 February 2026.

Suggested Citation:

Muravskyi, V. V. (2026). Risks of accounting digitalization by stages of the information systems life cycle. *Herald of Economics*, 1, 168-178. DOI: 10.35774/visnyk2026.01.168.

[1]**Vasyl Muravskyi,** West Ukrainian National University, Ternopil, Ukraine.
ORCID ID: 0000-0002-9625-9572
E-mail: vasmur@gmail.com

Ризики цифровізації обліку за стадіями життєвого циклу інформаційних систем

Василь Муравський[1]

[1]*Західноукраїнський національний університет, м. Тернопіль, Україна*

Анотація. *Цифровізація соціально-економічних процесів призвела до трансформації бухгалтерського обліку. Під впливом цифровізаційних тенденцій змін зазнає методика та організація обліку. Цифрова трансформація обліку неодмінно пов'язана з ризиками і загрозами функціонуванню підприємств. Для уникнення та мінімізації негативних наслідків цифровізації обліку необхідна ідентифікація та класифікація ризиків з врахуванням актуального рівня розвитку інформаційних технологій та систем. Мета статті полягає в ідентифікації, класифікації та систематизації ризиків цифровізації обліку на різних етапах провадження інформаційних систем управління підприємством та пошуку шляхів ліквідації джерел виникнення та мінімізації наслідків від кіберзагроз. Обґрунтовано доцільність ідентифікації та систематизації потенційних ризиків і загроз цифровізації обліку через прояв негативних тенденцій у роботі облікових фахівців, організації бухгалтерського обліку, використанні інноваційних технологій в обробці облікової інформації. Доведено необхідність класифікації ризиків цифровізації обліку відповідно до життєвих стадій розробки та імплементації інформаційних систем управління підприємствами. Систематизовано цифровізаційні ризики в бухгалтерському обліку за такими етапами: вивчення господарської діяльності підприємства, ідентифікація системи, вибору та її планування; передпроєктне оцінювання; проєктування інформаційної системи; впровадження та експлуатація інформаційної системи; контроль поточних ризиків та моніторинг функціонування; оцінювання експлуатаційних витрат та ефективності функціонування. Врахування життєвих циклів розробки та імплементації інформаційної системи управління забезпечує отримання комплексних та максимальних ефектів від цифровізації обробки облікової інформації без негативних наслідків для ефективного функціонування підприємства. На кожному етапі розробки і впровадження інформаційних систем управління підприємством виникають специфічні ризики цифровізації обліку. Врахування негативних тенденцій цифрової трансформації обліку відповідно життєвих стадій інформаційних систем забезпечує концентрацію уваги облікових та безпекових фахівців на окремих ризиках і загрозах цифровізації. Запропонована класифікація ризиків та їх врахування у процесі організації обліку за окремими етапами забезпечує найбільш оптимальну форму цифровізації облікових процесів на підприємстві.*

Ключові слова: *цифровізація, облік, інформаційні системи, інформаційні технології, стадії життєвих циклів, управління підприємством.*

Introduction. The formation of the digital economy is accompanied by the development of highly integrated information systems. The adaptation of modern information systems to the requirements of the digital economy necessitates the transformation of economic processes at the micro level. Digitalization trends in the economy are changing the traditional foundations of accounting as the primary generator of information on socio-economic processes occurring at enterprises. Under conditions of digitalization, the methodological and organizational provisions of accounting are transformed due to the transition to a new level of integration of information systems within the enterprise information environment.

The implementation of information systems requires the search for balanced approaches to the organization of accounting and forms new requirements for the professional competencies of accounting specialists. Accounting personnel may face problems related to: working with electronic source documents under digitalization while maintaining requirements for reliability and legal validity; preventing distortion, destruction, or falsification of information in electronic data repositories; and establishing effective communication through reporting systems with internal and external stakeholders. The methods and techniques of internal and external control are also undergoing changes.

An accounting specialist becomes not only a user of a digitalized accounting system created by other professionals, but also its co-creator at all stages of formation, from assessing the specifics of the enterprise's economic activity to the stages of information system design, implementation, improvement, and operation.

A single error made in an algorithm or calculation methodology during the digitalization of accounting may be repeatedly reproduced in the future, leading to significant negative consequences in the accounting interpretation of the enterprise's financial and economic activities. Under such conditions, it is necessary to strengthen the process of controlling the risks of accounting digitalization. Accounting specialists should actively participate in the operation of the digitalized accounting system, formulate tasks and control accounting processes, identify and eliminate all possible violations in the enterprise information system that may lead to loss of control over individual business transactions with corresponding negative consequences.

Analysis of research and publications. Threats and risks of accounting digitalization have evolved simultaneously with the development of information technologies. Until recently, the implementation of information technologies stimulated the intensification of automation processes in accounting. Accordingly, most scientific studies have focused on the risks of accounting automation as a means of reducing human involvement in the processing of accounting information. In particular, issues of automated accounting have been investigated in the works of such scholars as Butynets F.F., Ivakhnenkov S.V., Davydiuk T.V., Shakhraichuk T.V. [1], Shkvir V.D., Zahorodnii A.H., Vysochan O.S. [2], Zadorozhnyi Z.-M., et al. [3], Romanenko L., Koroteieva A. [4], and William E. Perry [5].

However, the use of modern information technologies and systems is not limited solely to automation changes in accounting. The digitalization of accounting information processing enables a transition to a qualitatively new level of accounting organization. Digital transformation actualizes new risks for the accounting information system associated with the openness and publicity of information resources, conducting business via the Internet, the transition to exclusively electronic monetary transactions, deregulation of economic processes, and the intensification of cyber fraud.

A more relevant classification of accounting digitalization risks, taking into account current trends in the development of information technologies and enterprise management information systems, is presented by foreign and domestic scholars. For example, Tsal-Tsalko Yu.S. and Moroz Yu.Yu. «divide the risks caused by the implementation of digital technologies in accounting according to their sources into those arising from external threats (competitors, criminal groups, other interested parties) and internal ones (enterprise management and personnel)» [6]. Steingartner William and Galinec Darko «continued this line of research and classified threats for identifying information risks in the implementation of hybrid influence of certain countries on others» [7].

It is reasonable to agree with Denha S.M. and Veryha Yu.A. «that threats to the digitalization of accounting should primarily be divided into two categories: intentional (fraud and sabotage) and accidental (errors and disasters)» [8]. Resler M.V. «details the risks of accounting digitalization by dividing them into cybersecurity risks (hacking, data leakage, malware attacks); technology dependency risks (technical failures and software errors); skills shortage risks (lack of expertise in data analytics, cybersecurity, and digital transformation); privacy risks (potential loss of personal and financial data of employees and counterparties); and risks of excessive dependence on automation (loss of critical thinking skills and reduced capacity for analysis and strategic decision-making)» [9].

Mustafa Nasir «substantiated the intensification of variable cyber threats under conditions of pandemic expectations in the economy». The scholar explains changes in enterprise cybersecurity priorities and the increased likelihood of various cyber risks in the event of the continuation of the COVID-19 pandemic and future crisis events [10]. Asieieva Yu. «generalizes cyber risks in the context of the development of Internet dependency among different groups of information users» [11]. Sheehan Barry, Murphy Finbarr, Kia Arash, and Kiely Ronan «developed a model for assessing enterprise cybersecurity vulnerabilities based on the classification of digitalization threats and determining the probability of their activation for various European institutions» [12]. Haque Md,

ISSN 2786-4537 (print). Вісник економіки № 1, 2026 р.
ISSN 2786-4545 (online). Herald of Economics № 1, 2026

Haque Shameemul, Kumar Kailash, and Singh Narendra «systematized all risks of digitalization of information processes manifested under conditions of using Internet of Things technologies» [13].

Rozheliuk V.M. «classifies accounting digitalization risks by time (short-term, long-term, permanent), by degree of manifestation (moderate, medium, full), by nature of manifestation (latent, easily noticeable, overtly aggressive), by consequences (those that do not affect the state of affairs; those that cause difficulties and problems; those that forcibly destroy the entire system), by probability (unlikely, probable, inevitable), and by origin (external, internal)» [14].

Bardash S.V. and Hrabchuk I.L. «identify another set of risks related to the digitalization of accounting processes, focusing on the implementation of new technologies: risks of using the Internet, artificial intelligence, robotization, and automation (leakage of trade secrets, reduction of accounting staff); risks associated with the use of blockchain technology (immutability of information and inability to correct errors) and cloud and distributed computing (difficulty in controlling cloud software operation and preventing failures); as well as risks related to the stability of Internet connectivity and the availability of qualified personnel» [15].

A fairly comprehensive classification of threats to accounting digitalization at the enterprise level was proposed by Nazarova I. and Nazarov O., who systematized them into the following groups: «risks of information loss, risks of loss of access to information, risks of data falsification, risks of non-confirmation (loss) of information legitimacy, and risks of disclosure (leakage) or theft of commercial or confidential information» [16].

Despite the active implementation of information systems in the activities of Ukrainian enterprises, which forms the basis for accounting digitalization, a significant number of business entities still operate with partial automation of accounting information processing. The partial nature of accounting digitalization in the form of automation of computational processes leads to the emergence of new threats to the national economic system. For comprehensive consideration of all threats of digitalization changes, accounting should be positioned as an information system at each stage of formation and implementation of which specific threats may arise. At the same time, studies on the classification of accounting digitalization risks in terms of the life-cycle stages of development and implementation of enterprise management information systems are almost absent in the scientific discourse. The importance of classifying and generalizing risks, as well as highlighting ways to eliminate them at different stages of creating accounting information systems in order to reduce negative consequences for enterprises, determines the relevance of the research objective.

The purpose of this article is to identify, classify, and systematize the risks of digitalization of accounting at various stages of implementing enterprise management information systems and to find ways to eliminate the sources of occurrence and minimize the consequences of cyber threats.

Results. Digitalization risks are understood as the threat of losses or damages arising in the process of creating, transmitting, storing, and using information in digital form as a result of applying modern information technologies for data processing by means of computer and telecommunication equipment. Among the numerous classifications of cyber threats present in the scientific literature, it is advisable to distinguish two types of risks: those related to encroachments on information resources that arise during the implementation and operation of an enterprise information system.

The main instruments of information threats include [3]:

- manipulation of information (disinformation, distortion of information, dissemination of incomplete or false information into the information environment);

- violation of the established procedure of information exchange, unauthorized access or unjustified restriction of access to information resources, unlawful collection and use of information;

- destruction and unauthorized use of others' information resources;

- information terrorism (distribution of viruses, installation of backdoor devices, use of information interception tools, illegal use or disruption of information and telecommunication systems, imposition of false information, disclosure of compromising information, etc.).

According to their origin, information risks are divided into three categories [4]:

- risks associated with the loss (leakage, damage, destruction) of information;
- risks associated with the formation of information resources (use of incomplete or false information, lack of necessary information, disinformation), including risks of information collection, risks of aggregation and classification, risks of information processing, and risks of information presentation;
- risks associated with informational influence on enterprise activities (dissemination of false or negative information, information and psychological influence on employees and clients, information terrorism).

At the same time, threats related to the life cycle of an enterprise information system can be considered within the framework of two approaches:

- a classification approach that distinguishes between technical risks and risks associated with managing the system development process;
- an approach based on the analysis of the stages of the accounting system life cycle.

The classification according to the first approach is presented in Table 1.

Table 1

Classification of risks associated with the life cycles of an enterprise management information system

Groups	Types of risks
Technical	Number of external systems with which the information system must interact
	Character of the system functioning (local, network)
	Presence of non-standard equipment
	Presence of necessary computer and telecommunications equipment
	Ability to install software on any platform
	Degree of novelty of equipment and software
	Degree of compatibility of software from different manufacturers
	Quality of personnel training (both accountants and system integrators)
	Presence of certified specialists in the region to support the system
	Dependence on the organizational structure of the enterprise
	Dependence on the size of the enterprise and the number of accounting personnel
	Presence of administrative and technical means of information protection
Management	System size, number and geography of users
	Size of budget constraints
	Dependence on the structure of business processes at the enterprise
	Size of labor costs in the development and implementation process
	Calendar terms of work performance
	Number of performers involved in system development, equipment supply
	Interest, attitude of system users, manager, chief accountant
	Availability of a well-coordinated team of users and performers
	Support for international and national accounting standards
	Dependence on the organizational structure of the enterprise
	Dependence on the size of the enterprise and the number of accounting personnel

Source: generated by the author.

Another approach to the classification of risks arising from the digitalization of accounting involves considering the life cycles of information systems, the first stage of which is the study of the economic

ISSN 2786-4537 (print). Вісник економіки № 1, 2026 р.
ISSN 2786-4545 (online). Herald of Economics № 1, 2026

activity of a business entity [17]. At the stage of studying the enterprise's economic activity, system identification, selection, and planning, the main risks include:

- the absence of an adequate assessment of the economic feasibility of the project and its technical, operational, legal, and political components;
- underestimation of expected financial costs for system development and implementation, implementation timelines, operating conditions, and the scope of system functionalities;
- incorrect selection of the option for creating an information system, including the choice between purchasing off-the-shelf software; acquiring individual system components that can be integrated in-house or by external system integrators; third-party system development; or in-house system development;
- deficiencies in evaluating key criteria for software selection, features of the software environment architecture, compatibility with various hardware and software platforms, and the ability to integrate with third-party and proprietary software;
- failure to consider, during software selection, the size of the enterprise, daily document flow, and the number of accounting staff;
- failure to take into account, in the process of software selection, the forms and principles of structuring the accounting function;
- shortcomings in assessing existing and required computer and telecommunication equipment, as well as their technical specifications and capabilities;
- an erroneous approach to creating an accounting information system with respect to its impact on the organizational structure of the enterprise and the accounting department, either by focusing on preserving the existing structure with the adaptation of information technologies or by rationalizing and fundamentally changing the management structure.

At the stage of pre-project analysis of the information system, the data model is refined, information flow diagrams are developed, and a logical sequence of information processing is established. At this stage, the risks include:

- incomplete understanding of the information needs of internal and external users;
- insufficient analysis of information sources and communication channels for information flows;
- lack of consistency in data transformation to present information in a convenient and user-ready format;
- inadequate examination of the enterprise document flow, primary and reporting document forms, and calculation methodologies;
- ineffective analysis of primary document attributes, the volume of reporting information, the existing form of accounting, the control system, and the current information coding system.

At the stage of designing the accounting information system, the risks include:

- failure to comply with technical requirements regarding low hardware dependency, data exchange with other software and devices, operation within local computer networks and, where necessary, access to global networks, the ability to ensure protection of information from internal and external unauthorized access, damage, and falsification, as well as the ability to maintain archives and restore information in the event of failures;
- inadequate fulfillment of functional requirements related to the accumulation and processing of business transactions, the ability to calculate balances at any point in time, maintenance of analytical accounting with the required level of detail, quantitative and foreign currency accounting, and the generation of customized consolidated reports;
- non-compliance with ergonomic requirements related to the development of a user-friendly interface and a clear software help system;

- lack of adaptability of the software to legislative changes and insufficient flexibility to adjust to changes in the organizational structure of the enterprise and the accounting department.

At the stage of implementation and operation of the information system, the risks include:

- errors in personnel selection and communication arrangements;
- insufficient computer training of accounting staff, absence of a system programmer or system integrator, limited opportunities for staff training, and lack of adequate methodological and instructional materials;
- low staff motivation to use information technologies, as well as indifference or incompetence of management and the chief accountant;
- errors in the installation and configuration of hardware and software, insufficient system configuration, and poor-quality formation of the information database;
- deficiencies in organizing information security, preventing unauthorized access, and non-compliance with archiving requirements.

Under conditions of developing an accounting information system, issues of control and analysis of potential automation risks are often not given sufficient attention. Therefore, when designing a control system, it is necessary to [5, p. 104]:

- identify accounting automation risks and analyze cases of potential problem occurrence;
- determine the level of impact of possible risks on the effectiveness of accounting automation;
- establish the boundaries and magnitude of acceptable risks;
- define control points of accounting automation, i.e., system locations where risks may arise;
- develop control solutions and determine control methods to minimize risks to an acceptable level;
- conduct cost analysis and determine the economic efficiency of control methods;
- implement control measures and establish a system of methods for reducing potential risks.

At the risk identification stage, an analysis group is formed to develop risk occurrence scenarios and ultimately compile a list of risks. This group should assign responsibility for addressing specific issues and identify and communicate methods for identifying potential risks.

At the stage of determining risk severity, one of two methods is applied: stratification or estimation of annual losses. Under the stratification method, the magnitude of potential risks is determined by grouping them into strata, for example, high, medium, and low risk. When applying the expected annual loss method, potential losses are determined based on prior assessment and forecasting. In this context, the historical approach, the formalized method, the subjective assessment method, and the scenario method are used.

When establishing acceptable risk thresholds, it is necessary to determine the level of risk that users can tolerate, for which losses will be minimal and the consequences can be promptly and fully eliminated. At the stage of identifying control points, control tools in the automated system are placed where the risk of losses may arise. At the same time, control areas are defined, i.e., the domains and information processing functions that are most effective for risk reduction (Fig. 1).

In the process of developing control solutions, methods of manual and automated control are determined. Manual control involves monitoring the preparation of data entered into the digital information system and verifying the correctness of information processing at specific operational stages. Automated control is associated with the direct input of accounting data into the system. Control methods may be preventive, aimed at preventing undesirable events; detective, identifying the occurrence of an undesirable situation; corrective, eliminating the consequences of problems; discretionary, the application of which is optional; and non-discretionary (mandatory), the application of which is not subject to user choice.

ISSN 2786-4537 (print). Вісник економіки № 1, 2026 р.
ISSN 2786-4545 (online). Herald of Economics № 1, 2026

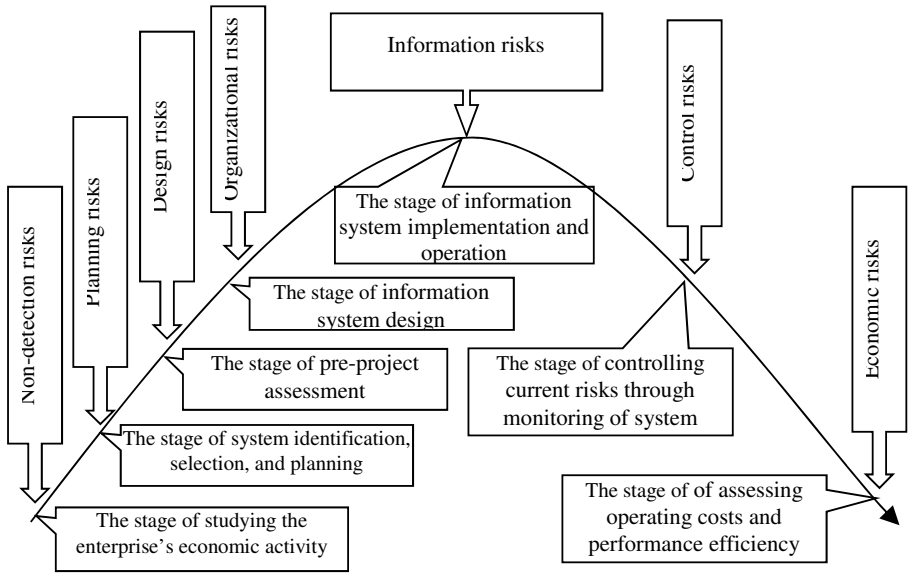

Fig. 1. Risks of accounting digitalization by stages of the information systems life cycle.
Source: generated by the author.

The objective of cost analysis and assessment of the economic efficiency of control methods is to determine the economic feasibility of implementing control measures and to make decisions by comparing the costs of introducing additional controls with potential losses from risks. Without conducting a cost–benefit analysis of control measures, it is impossible to assess whether control is excessive or insufficient.

The final stage of designing the control system is the implementation of controls that are economically justified and ensure risk reduction to an acceptable level. The process of control implementation consists of several stages: building the control system, testing (verification of compliance with specified requirements), documentation (development of instructions necessary for understanding control tasks and subsequent operation), staff training in control functions with clearly defined procedures, and the actual implementation, whereby control becomes a standardized procedure.

Conclusions. The digitalization of accounting involves identifying and assessing potential risks associated with the creation of fundamentally new conditions for the functioning of accounting personnel, changes in the organizational structure of the enterprise, the implementation of information technologies and systems, and the establishment of new communication channels for the transmission of accounting information that are open to the external environment and entrusted to the enterprise management information system. It is necessary to distinguish between information risks related to the creation, transmission, storage, and use of accounting information by means of computer and telecommunication technologies, and risks that arise at the stages of design, analysis, implementation, and operation of the accounting information system. Accounting digitalization risks should be systematized according to the stages of the life cycle of enterprise management information systems, namely: the stage of studying the enterprise's economic activity, system identification, selection, and planning; the stage of pre-project assessment; the stage of information system design; the stage of information system implementation and operation; the stage of controlling

current risks through monitoring of system functioning; and the stage of assessing operating costs and performance efficiency.

Consideration of the life cycles of the development and implementation of an enterprise information system ensures the achievement of comprehensive and maximum effects from the digitalization of accounting information processing. In order to minimize negative economic outcomes associated with financial and time losses required to correct digitalization risks, their detailed classification, taking into account the life-cycle stages of implementing an enterprise management information system, is of particular importance. At each stage of accounting digitalization, threats may change, which necessitates their timely identification. Proper and comprehensive control over accounting digitalization risks will facilitate the identification of effective approaches to monitoring the manifestation of potential risks in order to avoid them or minimize their consequences.

References

1. Information systems and technologies in accounting (2007) / F. F. Butynets [et al.]; ed. F. F. Butynets. – 3rd ed., revised and supplemented. Zhytomyr: PP "RUTA", 468 p. URL: https://repository.kpi.kharkov.ua/items/b895dd75-47bb-43cd-b4b3-d3a8d0f84f77 [in Ukrainian].
2. Shkvir, V. D., Zahorodnii, A. H., Vysochan, O. S. (2007). Information systems and technologies in accounting. 3rd ed., revised and expanded. Kyiv: Znannia, 439 p. URL: http://ктеп.kiev.ua/wp-content/uploads/2019/12/shkvir_v_d_ta_in_informatsiyni_sistemi_i_tekhnologiyi_v_obli.pdf. [in Ukrainian].
3. Zadorozhnyi, Z.-M., Muravskyi, V., Shevchuk, O., Muravskyi, V. (2020). the Accounting System As the Basis for Organising Enterprise Cybersecurity. *Financial and Credit Activity Problems of Theory and Practice,* 3 (34), 149-157. URL: https://doi.org/10.18371/fcaptp.v3i34.215462. [in English].
4. Romanenko, L., Koroteieva, A. (2003). Risks in economic activity. Finance of Ukraine, 5, P. 121–127. URL: https://scholar.google.com/scholar?hl=uk&as_sdt=0,5&cluster=7122348208935055289. [in Ukrainian].
5. Perry, W. E. (1986). The Accountants' Guide to Computer Systems. John Wiley & Sons, 199 p. URL: https://books.google.com.ua/books/about/The_Accountants_Guide_to_Computer_System.html?id=ip-7AAAAIAAJ&redir_esc=y [in English].
6. Tsal-Tsalko, Yu. S., Moroz, Yu. Yu. (2017). Enterprise accounting policy and its cybersecurity. *Accounting, Analysis and Control under Modern Concepts of Managing Economic Potential and Market Value of the Enterprise*, Vol. I, Part I, P. 8–11. URL: http://ir.polissiauniver.edu.ua/handle/123456789/7427 [in Ukrainian].
7. Steingartner, W., Galinec, D. (2021). Cyber threats and cyber deception in hybrid warfare. *Acta Polytechnica Hungarica*, 18, P. 25–45. URL: https://doi.org/10.12700/APH.18.3.2021.3.2. [in English].
8. Denha, S. M., Veryha, Yu. O. (2004). Information protection in computer accounting information systems. *Accounting and Auditing*, 5, P. 59–65. URL: http://dspace.puet.edu.ua/bitstream/123456789/938/1/Захист%20інф%20в%20КСБО.doc. [in Ukrainian].
9. Resler, M. (2024). Impact of the digital economy on the accounting and analytical system. Acta Academiae Beregsasiensis. Economics, 5, P. 441–450. URL: https://doi.org/10.58423/2786-6742/2024-5-441-450. [in Ukrainian].
10. Mustafa, N. (2020). Cyber risk and Covid-19: managing cyber risks arising from the pandemic. Brighttalk Webinar Series. URL: https://doi.org/10.13140/RG.2.2.12218.82886. [in English].
11. Asieieva, Yu. (2020). Problem questions of cyber-addictions classification. *Psychology and Personality*, 2, P. 23–40. URL: https://doi.org/10.33989/2226-4078.2020.2.211910. [in English].

12. Sheehan, B., Murphy, F., Kia, A., Kiely, R. (2021). A quantitative bow-tie cyber risk classification and assessment framework. *Journal of Risk Research*, P. 1–20. URL: https://doi.org/10.1080/13669877.2021.1900337. [in English].
13. Haque, Md., Haque, S., Kumar, K., Singh, N. (2021). A comprehensive study of cyber security attacks, classification, and countermeasures in the Internet of Things, P. 63–90. URL: https://doi.org/10.4018/978-1-7998-4201-9.ch004. [in English].
14. Rozheliuk, V. M. (2013). Measures to ensure protection of accounting information. *Accounting, Analysis and Audit: Problems of Theory, Methodology and Organization*, 2 (12), P. 335–340. URL: https://api.dspace.wunu.edu.ua/api/core/bitstreams/1a5bdc63-cdfb-4239-8fdc-4e8ccefe4c05/content [in Ukrainian].
15. Bardash, S. V., Hrabchuk, I. L. (2021). Digital technologies in accounting: main opportunities and risks. Efficient Economy, 9. URL: https://doi.org/10.32702/2307-2105-2021.9.18. [in Ukrainian].
16. Nazarova, I., Nazarov, O. (2025). Risk assessment and systems for protecting accounting information under IT application conditions. *Bulletin of Economics*, 1, P. 244–255. URL: https://doi.org/10.35774/visnyk2025.01.244. [in Ukrainian].
17. Muravskyi, V. (2023). Accounting and cybersecurity. Ternopil: West Ukrainian National University, 200 p. URL: https://dspace.wunu.edu.ua/items/60ef2fe2-6624-4bea-81b5-9979bebce568 [in Ukrainian].

Література

1. Інформаційні системи і технології в обліку : підручник / Ф. Ф. Бутинець [та ін.] ; ред. Ф. Ф. Бутинець. 3-е вид., перероб. і доп. Житомир : ПП "РУТА", 2007. 468 с. URL: https://repository.kpi.kharkov.ua/items/b895dd75-47bb-43cd-b4b3-d3a8d0f84f77.
2. Шквір В. Д., Загородній А. Г., Височан О. С. Інформаційні системи і технології в обліку : навч. посіб. 3-тє вид., переробл. і доповн. К. : Знання, 2007. 439 с. URL: http://ктеп.kiev.ua/wp-content/uploads/2019/12/shkvir_v_d_ta_in_informatsiyni_sistemi_i_tekhnologiyi_v_obli.pdf.
3. Zadorozhnyi Z., Muravskyi V., Shevchuk O., Muravskyi V. the Accounting System As the Basis for Organising Enterprise Cybersecurity. Financial and Credit Activity Problems of Theory and Practice. 2020. № 3 (34). P. 149-157. URL: https://doi.org/10.18371/fcaptp.v3i34.215462.
4. Романенко Л., Коротеєва А. Ризики у діяльності. Фінанси України. 2003. № 5. С. 121–127. URL: https://scholar.google.com/scholar?hl=uk&as_sdt=0,5&cluster=7122348208935055289.
5. Perry W. E. The Accountants' Guide to Computer Systems. John Wiley & Sons, 1986. 199 p. URL: https://books.google.com.ua/books/about/The_Accountants_Guide_to_Computer_System.html?id=ip-7AAAAIAAJ&redir_esc=y.
6. Цал-Цалко Ю. С., Мороз Ю. Ю. Облікова політика підприємства та її кібербезпека. *Облік, аналіз і контроль в умовах сучасних концепцій управління економічним потенціалом і ринковою вартістю підприємства.* Т. І, ч. І. Житомир : ПП «Рута», 2017. С. 8–11. URL: http://ir.polissiauniver.edu.ua/handle/123456789/7427.
7. Steingartner W., Galinec D. Cyber Threats and Cyber Deception in Hybrid Warfare. Acta Polytechnica Hungarica. 2021. Т. 18. С. 25–45. URL: https://doi.org/10.12700/APH.18.3.2021.3.2.
8. Деньга С. М., Верига Ю. О. Захист інформації в комп'ютерних інформаційних системах бухгалтерського обліку. *Бухгалтерський облік і аудит.* 2004. № 5. С. 59–65. URL: http://dspace.puet.edu.ua/bitstream/123456789/938/1/Захист%20інф%20в%20КСБО.doc.
9. Реслер М. Вплив цифрової економіки на обліково-аналітичну систему. *Acta Academiae Beregsasiensis. Economics.* 2024. № 5. С. 441–450. URL: https://doi.org/10.58423/2786-6742/2024-5-441-450.

10. Mustafa N. Cyber Risk and Covid-19: Managing Cyber Risks Arising from the Pandemic. Brighttalk Webinar Series. 2020. URL: https://doi.org/10.13140/RG.2.2.12218.82886.
11. Asieieva Yu. Problem questions of cyber-addictions classification. Psychology and Personality. 2020. № 2. С. 23–40. URL: https://doi.org/10.33989/2226-4078.2020.2.211910.
12. Sheehan B., Murphy F., Kia A., Kiely R. A quantitative bow-tie cyber risk classification and assessment framework. Journal of Risk Research. 2021. С. 1–20. URL: https://doi.org/10.1080/13669877.2021.1900337.
13. Haque Md., Haque S., Kumar K., Singh N. A Comprehensive Study of Cyber Security Attacks, Classification, and Countermeasures in the Internet of Things. 2021. С. 63–90. URL: https://doi.org/10.4018/978-1-7998-4201-9.ch004.
14. Рожелюк В. М. Заходи забезпечення захисту облікової інформації. *Бухгалтерський облік, аналіз та аудит: проблеми теорії, методології, організації* : зб. наук. праць. 2013. № 2 (12). С. 335–340. URL: https://api.dspace.wunu.edu.ua/api/core/bitstreams/1a5bdc63-cdfb-4239-8fdc-4e8ccefe4c05/content.
15. Бардаш С. В., Грабчук І. Л. Цифрові технології в сфері бухгалтерського обліку: основні можливості та ризики. Ефективна економіка. 2021. № 9. URL: https://doi.org/10.32702/2307-2105-2021.9.18.
16. Назарова І., Назаров О. Оцінка ризиків і системи захисту облікової інформації в умовах застосування ІТ. *Вісник економіки*. 2025. Вип. 1. С. 244–255. URL: https://doi.org/10.35774/visnyk2025.01.244.
17. Муравський В. Облік та кібербезпека : моногр. Тернопіль : ЗУНУ, 2023. 200 с. URL: https://dspace.wunu.edu.ua/items/60ef2fe2-6624-4bea-81b5-9979bebce568.