УДК 657.6:004.056
JEL Classification M41, M42, G32, L86
DOI https://doi.org/10.33146/2518-1181-2026-2(112)-44-52

The Impact of Cyber Risks on the Functioning of the Accounting System and Their Management

Tetyana Demchenko[1]

Abstract. *The rapid digitalization of accounting and the growing reliance of accounting systems on information and communication technologies increase their vulnerability to cyberattacks, data leakage, unauthorized access, and the compromise of the integrity of financial information. Therefore, the development of effective approaches to identifying, assessing, and managing cyber risks is particularly relevant to ensure the continuity of the accounting system, the reliability of reporting, and the protection of accounting data. The article aims to reveal the impact of cyber threats on the enterprise's accounting system and to substantiate approaches to managing cyber risks in the context of the digitalization of management. This study is based on accounting information systems and a risk-based approach to managing cyber risks. From this point of view, accounting systems are integrated information environments where the processing of financial data depends on cybersecurity mechanisms and IT management. The study also applies the concept of cyber risk management, which integrates cybersecurity into corporate governance and internal control systems. Accordingly, cyber risks are interpreted not only as technical threats but also as structural factors that affect the reliability of financial reporting and decision-making processes. The article offers an overview of modern cyber risks, analyzing the trends of their evolution and spread. The results of the study show that effective cyber risk management requires an integrated approach that combines technical means of information protection, organizational measures, and improvements to the internal control system. Therefore, enterprises should integrate cybersecurity principles into the accounting system to ensure the integrity and reliability of financial information. The results of the study serve as a basis for improving risk management approaches to enhance information security for enterprises.*

Keywords: *cyber risks, accounting, risk management, digitalization, cybersecurity, information security, financial reporting, internal control, accounting information systems.*

Received: 18 April 2026 | **Revised:** 13 May 2026 | **Accepted:** 19 May 2026 | **Published:** 30 May 2026

Suggested Citation
Demchenko, T. (2026). The Impact of Cyber Risks on the Functioning of the Accounting System and Their Management. *Oblik i finansi*, *2*(112), 44-52. https://doi.org/10.33146/2518-1181-2026-2(112)-44-52

[1] **Tetyana Demchenko**, Uman National University, Ukraine.
ORCID 0000-0002-7471-540X
E-mail: demchenko.tanya7@gmail.com

Вплив кіберризиків на функціонування системи бухгалтерського обліку та управління ними

Тетяна Демченко[1]
[1] *Уманський національний університет, Україна*

Анотація. *Стрімка цифровізація бухгалтерського обліку та зростання залежності облікових систем від інформаційно-комунікаційних технологій підвищують їхню вразливість до кібератак, витоку даних, несанкціонованого доступу та порушення цілісності фінансової інформації. Відтак особливої актуальності має набуває розроблення ефективних підходів до ідентифікації, оцінювання та управління кіберризиками задля забезпечення безперервності функціонування системи бухгалтерського обліку, достовірності звітності та захисту облікових даних. Метою статті є розкриття впливу кіберзагроз на систему бухгалтерського обліку підприємства та обґрунтування підходів до управління кіберризиками в контексті цифровізації управління. Теоретична основа цього дослідження базується на інформаційних системах бухгалтерського обліку та ризик-орієнтованому підході до управління кіберризиками. З цієї точки зору, системи бухгалтерського обліку розглядаються як інтегровані інформаційні середовища, де обробка фінансових даних залежить від механізмів кібербезпеки та управління ІТ. У дослідженні також застосовується концепція управління кіберризиками, яка інтегрує кібербезпеку в системи корпоративного управління та внутрішнього контролю. Відповідно, кіберризики інтерпретуються не лише як технічні загрози, але й як структурні фактори, що впливають на надійність фінансової звітності та процеси прийняття рішень. Стаття пропонує огляд сучасних кіберризиків, аналізуючи тенденції їх еволюції та поширення. Результати дослідження доводять, що ефективне управління кіберризиками потребує комплексного підходу, який поєднує технічні засоби захисту інформації, організаційні заходи та вдосконалення системи внутрішнього контролю. Отже, принципи кібербезпеки повинні бути інтегровані в систему бухгалтерського обліку, що є важливою умовою забезпечення достовірності фінансової інформації. Результати дослідження можуть бути використані для вдосконалення підходів до управління ризиками та підвищення рівня інформаційної безпеки підприємств.*

Ключові слова: *кіберризики, бухгалтерський облік, управління ризиками, цифровізація, кібербезпека, інформаційна безпека, фінансова звітність, внутрішній контроль, облікові інформаційні системи.*

INTRODUCTION

The digital transformation of business processes increases enterprises' dependence on information systems that process accounting and financial data. Under these conditions, traditional approaches to accounting organization no longer ensure an adequate level of information protection and require consideration of new types of risk. The integration of cyber risks into enterprise management systems and internal control frameworks is becoming increasingly relevant. An insufficient level of cybersecurity may not only lead to data loss but also distort financial reporting and violate accounting procedures. Thus, the study of the impact of cyber threats on accounting systems represents an important research task.

LITERATURE REVIEW

Nowadays, researchers place significant emphasis on cyber risks within accounting systems and enterprise accounting information systems. In particular, they regard cyber risks as an integral component of modern Accounting Information Systems (AIS), forming an interdisciplinary research domain at the intersection of accounting, information technologies, and cybersecurity. Thus, current studies increasingly shift from fragmented descriptions of cyber threats toward the development of integrated cyber risk management models to ensure the reliability of financial reporting and the effectiveness of internal control systems.

In particular, Cram et al. (2023) propose a conceptual model of cyber risk governance in AIS, where cybersecurity is embedded within corporate governance and internal control systems. They state that the effective functioning of accounting systems requires multi-layered data protection, access control mechanisms, and continuous monitoring of cyber threats, which collectively form the foundation of modern risk governance in accounting information systems.

A similar approach is developed by Chowdhury et al. (2022), who propose a risk-based framework for integrating cybersecurity into AIS. The researchers argue that cyber risk management should be embedded within financial accounting processes and internal control systems, thereby mitigating the impact of cyberattacks on the accuracy, completeness, and reliability of financial reporting.

Monteiro and Cepêda (2021) examine the transformation of accounting information systems in the digital era. They found that adopting cloud technologies, big data analytics, and automated information processing systems enhances accounting efficiency; however, it simultaneously widens the scope of cyber threats and increases the need for cyber resilience in accounting systems.

By paying special attention to the impact of artificial intelligence on accounting systems, Zhang et al. (2023) analyze the ethical and organizational implications of AI implementation in managerial accounting, emphasizing

that automation of financial processes improves efficiency but also introduces new risks to the integrity, transparency, and controllability of financial data. This study highlights the growing role of cybersecurity as a core structural component of digital accounting environments.

Empirical studies and analytical reports confirm the increasing scale and complexity of cyber threats. The Radware (2025) report documents a significant rise in DDoS attacks, indicating intensified cyber risk exposure in the global digital environment. Similarly, Cognyte (2025) reports an increase in stolen credentials and the expanding use of artificial intelligence in cybercrime, further elevating the risk of unauthorized access to corporate information systems.

Ukrainian scholarly research complements these international approaches. Vavilenkova (2024) examines risks associated with cloud technologies in accounting systems, identifying data leakage and dependence on external infrastructure as key vulnerabilities. Muravskyi et al. (2021) classify cyber risks in accounting, emphasizing their impact on the reliability of financial reporting and the effectiveness of internal control systems.

Struk (2026) provides a comprehensive assessment of the cybersecurity of accounting information in the context of innovative enterprise development, demonstrating the direct impact of cyber incidents on the quality of financial information, the continuity of accounting processes, and the stability of internal control systems. She emphasizes the need to integrate cybersecurity as a systemic component of accounting rather than merely an external technical tool.

According to the State Service of Special Communications and Information Protection of Ukraine, more than 60% of cyber incidents originate from phishing attacks, highlighting the critical role of the human factor within the structure of cyber risks. Taking these trends into account, Prokofieva and Bespalova (2024) substantiate the need to develop comprehensive cyber risk management strategies in the context of digital economic transformation.

Finally, Sigaiev and Volovyk (2017) analyze the mechanisms of botnet formation as tools for large-scale cyberattacks, posing a serious threat to the stability of enterprise information systems.

Thus, the literature review demonstrates a clear shift from descriptive studies of cyber threats toward the conceptualization of cyber resilience in accounting systems and financial reporting processes, in which cyber risks are recognized as a key determinant of reporting reliability and internal control effectiveness.

RESEARCH OBJECTIVE

This article aims to investigate the impact of cyber threats on the enterprise accounting system and to determine approaches to cyber risk management in the context of the digitalization of the economy.

RESEARCH METHODOLOGY

The theoretical framework of this study is grounded in Accounting Information Systems (AIS) and a risk-based approach to cyber risk management. Within this perspective, accounting systems are considered integrated information environments where financial data processing depends on cybersecurity and IT governance mechanisms. The study also adopts the concept of cyber risk governance, which integrates cybersecurity into corporate management and internal control systems (Cram et al., 2023). Accordingly, cyber risks are understood not only as technical threats but also as structural factors that affect the reliability of financial reporting and decision-making processes. Therefore, cyber risk management is viewed as a multi-layered framework combining technical, organizational, and governance-level controls. The conceptual model links AIS principles with cyber risk governance to explain the relationship between cyber threats, accounting information integrity, and internal control effectiveness.

The information base of the study comprises:

– peer-reviewed scientific publications by domestic and international scholars on cyber risks, accounting, and information systems;

– analytical reports of international cybersecurity organizations and companies (Radware, Cognyte, NCC Group);

– regulatory and methodological materials of the State Service of Special Communications and Information Protection of Ukraine;

– open-source datasets and publicly available reports on cyber incidents and cyber threats.

These sources represent the contemporary stage of digital economic transformation and reflect current global and regional trends in cyber risk evolution.

The author applies the following research methods:

Analysis and synthesis – to systematize theoretical approaches to cyber risk interpretation and to assess their impact on accounting systems.

System approach – to consider accounting as an integral component of enterprise information infrastructure operating under conditions of digital transformation and technological interdependence.

Comparative analysis – to classify major types of cyber threats and evaluate their implications for accounting processes and financial reporting.

Abstraction and generalization – to derive generalized conclusions regarding the impact of cyber risks on enterprise financial and economic functioning.

Content analysis – to examine scientific publications and analytical reports to identify dominant cyber threats and contemporary risk management approaches.

Visualization of research results was achieved through figures and tables.

RESULTS

In the current economic and social conditions of business functioning, digitalization is transforming the classical model of risks. Alongside traditional risks (credit, currency, interest rate, inflation, and liquidity risks), new types of risks are emerging, including cyber risk, algorithmic risk, data loss risk, IT failure risk, digital fraud risk, and dependence on cloud services. Thus, risks can be characterized as becoming faster, more global, harder to predict, and increasingly intangible.

The impact of these risks on the enterprise accounting system becomes particularly significant, as the accounting system serves as a key source for the formation, storage, and processing of financial information. In a digital environment, accounting is evolving into an information-analytical system that depends on the quality of IT infrastructure and software, as well as the level of cybersecurity protection.

Figure 1 presents the main types of cyber risks in the enterprise accounting system.

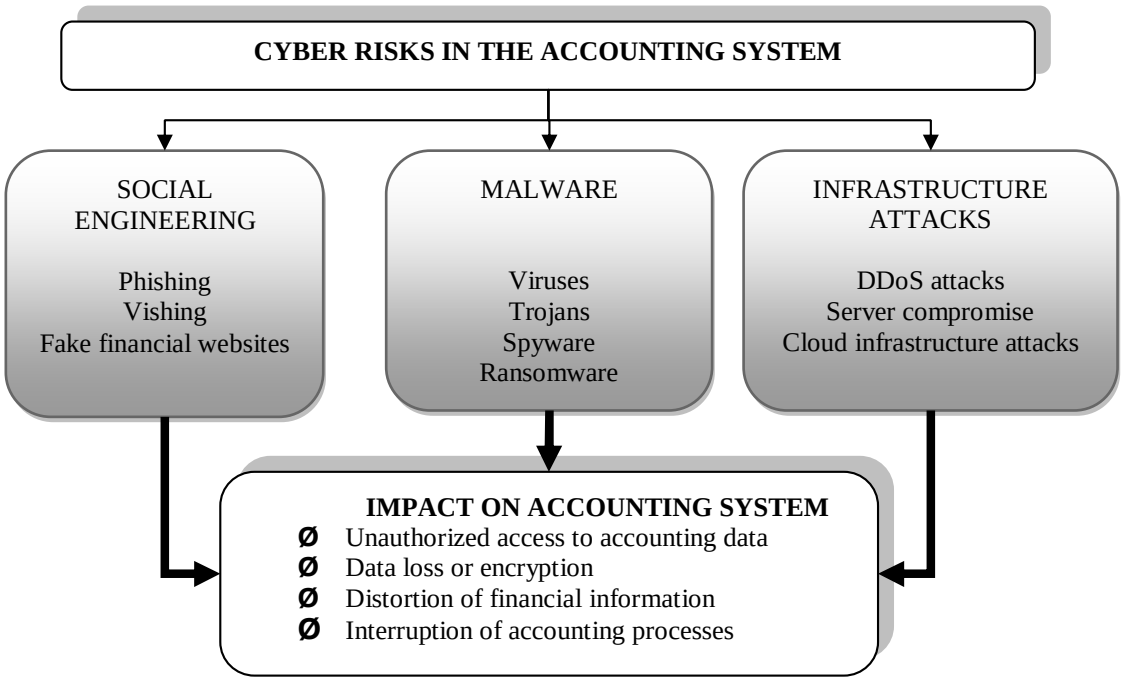

Figure 1. Classification of Cyber Risks in the Accounting System

Source: compiled by the author.

Cyber risks directly affect the reliability and completeness of accounting information, which may lead to the distortion of financial statements, loss of primary accounting documents, disruption of the continuity of the accounting process, and a decrease in trust in an enterprise's financial data. Figure 2 presents the model of the impact of cyber risks on the enterprise accounting system.

Accounting functions not only as a system for recording business transactions but also as an object of cybersecurity, requiring the implementation of cyber risk management procedures, internal control mechanisms, and information security measures.

Since cyber risk is defined as the probability of financial losses resulting from the disruption of information systems, unauthorized access, or data destruction, the following classification of cyber threats can be distinguished:

1. Social engineering, which is based on psychological manipulation of individuals aimed at inducing them to disclose confidential information (such as passwords or card numbers) or to perform harmful actions (such as money transfers or installation of malicious software). Instead of breaking technical systems, attackers "break" the human factor by exploiting emotions, trust, or fear. The main types of social engineering include:

- Phishing, which involves the mass distribution of fraudulent emails or messages that imitate official requests from banks, social networks, or service providers (e.g., "update your password," "your account has been blocked") (NCC Group, 2024). The aim is to persuade the user to follow a malicious link or open an infected file;
- Vishing, which refers to telephone fraud where attackers impersonate bank employees, police officers, or support agents in order to obtain card details (CVV codes, passwords) or to induce money transfers;
- Fake financial websites, where fraudulent web resources visually replicate well-known banks, payment systems, ticket booking platforms, or classified services. Users themselves enter their login credentials or card data, which attackers then steal.

Protection against these threats requires not sharing personal data, carefully verifying website URLs, and critically assessing urgent or pressure-based requests.

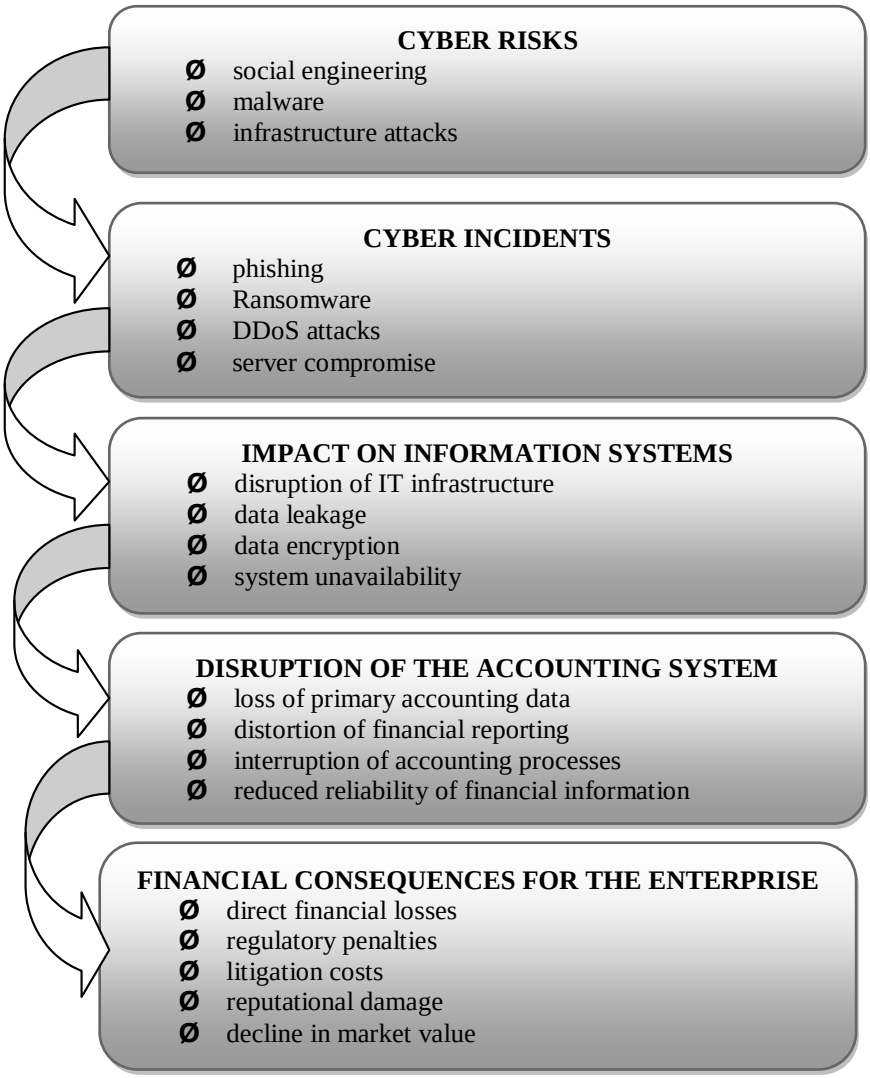

Figure 2. The Impact of Cyber Risks on the Enterprise Accounting System
Source: compiled by the author.

2. Malware (malicious software) refers to the use of programs designed to steal data, damage systems, or gain unauthorized access to devices:

- Viruses, which are capable of self-replication and infecting files;
- Trojans (Trojan horses), which disguise themselves as legitimate software, thereby tricking users into installing them manually;
- Spyware, whose purpose is the covert collection of information about an organization's activities (such as browsing history, entered passwords, and personal data) and its transmission to attackers. Typical signs include slower computer performance, the appearance of unwanted advertisements, and changes in browser settings. Examples include keyloggers (which record keystrokes) and other Trojan-based spyware tools;
- Ransomware (encryption malware) is primarily motivated by financial gain through extortion. Once installed on a device, it encrypts documents, photos, and databases, making them inaccessible. A message is then displayed demanding payment (usually in cryptocurrency) for the decryption key. However, even after payment, there is no guarantee that the data will be restored.

Protection against these threats requires using antivirus software, keeping software up to date, avoiding opening suspicious email attachments, and maintaining regular backups of important data.

3. Infrastructure attacks are cyberattacks aimed at disrupting the operation of fundamental components of IT networks (servers, network equipment, and cloud services), thereby making online resources unavailable to users. Their primary objective is to exhaust system resources (memory, processor capacity, bandwidth), compromise systems for data theft, or paralyze business processes. The main types include:

- DDoS (Distributed Denial of Service) attacks (Cognyte, 2025) involve the massive overloading of a server or website with fake traffic generated by thousands of infected devices (botnets) (Sigaiev & Volovyk, 2017). As a result, the website becomes extremely slow or completely unavailable to legitimate users. Such attacks may be volumetric (flooding network bandwidth), protocol-based (exhausting system resources), or application-layer attacks targeting web servers;

- Server compromise, which refers to unauthorized access to server control through software vulnerabilities, weak passwords, or malware (Prokofieva & Bespalova, 2024). In such cases, attackers may steal confidential data (e.g., customer databases), delete information, install ransomware, or use the compromised server to distribute spam;

Cloud infrastructure attacks that target cloud service providers (such as AWS, Azure, and Google Cloud) or misconfigured cloud storage systems (Radware, 2025). These attacks may result in data leakage from open cloud storage containers (e.g., S3 buckets), theft of cloud resources for cryptocurrency mining, or complete disruption of cloud-based applications.

In 2024, a significant increase in global cyber threat activity was observed, with the number of cyber incidents continuing to rise (Figure 3).

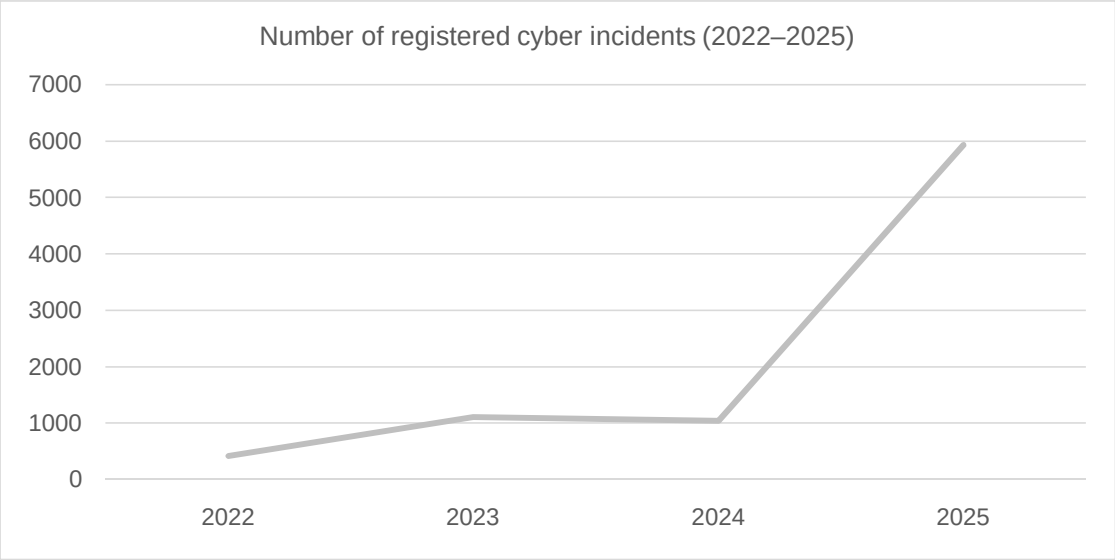

Figure 3. Trend of registered cyber incidents in Ukraine (2022–2025)

Source: Compiled by the author based on official CERT-UA data (2022–2025).

According to international analytical reports, the number of ransomware-related attacks exceeded 5,200 in 2024, a record level in recent years (Radware, 2025).

An approximately 28% increase in the volume of stolen credentials was also recorded compared to the previous period, significantly increasing the risk of unauthorized access to enterprise information systems (Chowdhury et al., 2022). In addition, a sharp rise in DDoS attacks was observed, with their scale in 2024 increasing several times compared to the previous year (Cognyte, 2025).

In 2025, cyber incidents in Ukraine were predominantly characterized by malware-based attacks and social engineering techniques. The structure of incidents reflects the multi-stage nature of cyber threats, where malware distribution and infection processes play a central role. The largest share of incidents was associated with malware distribution (34.7%), indicating the systematic and large-scale deployment of malicious software targeting information systems (CERT-UA, 2025). Phishing remained the second most prevalent method (29.2%), confirming the continued high dependence of cyber threats on the human factor (CERT-UA, 2025).

A considerable proportion of incidents was also linked to malware infections (16.7%), reflecting the execution phase of multi-stage attack vectors aimed at gaining unauthorized access to information systems (CERT-UA, 2025). Account compromise cases accounted for 7.2%, representing a less frequent but highly critical type of incident often used as an entry point for further malicious activities (CERT-UA, 2025). Other types of cyber incidents constituted 12.3%, demonstrating the diversity and continuous evolution of cyber threat vectors (CERT-UA, 2025).

Overall, the findings reported by CERT-UA (2025) indicate a shift toward large-scale automated attacks and social engineering techniques, highlighting the growing importance of human-centric vulnerabilities in cybersecurity systems. Figure 4 presents the distribution of cyber incidents by type in 2025.

The results confirm that malware-related attacks and phishing dominate the cyber threat landscape in 2025, highlighting the growing role of automated attacks and human-factor vulnerabilities.

Overall, global trends indicate an increasing complexity of cyber threat structures, their growing automation, and rising financial losses for businesses (Table 1).

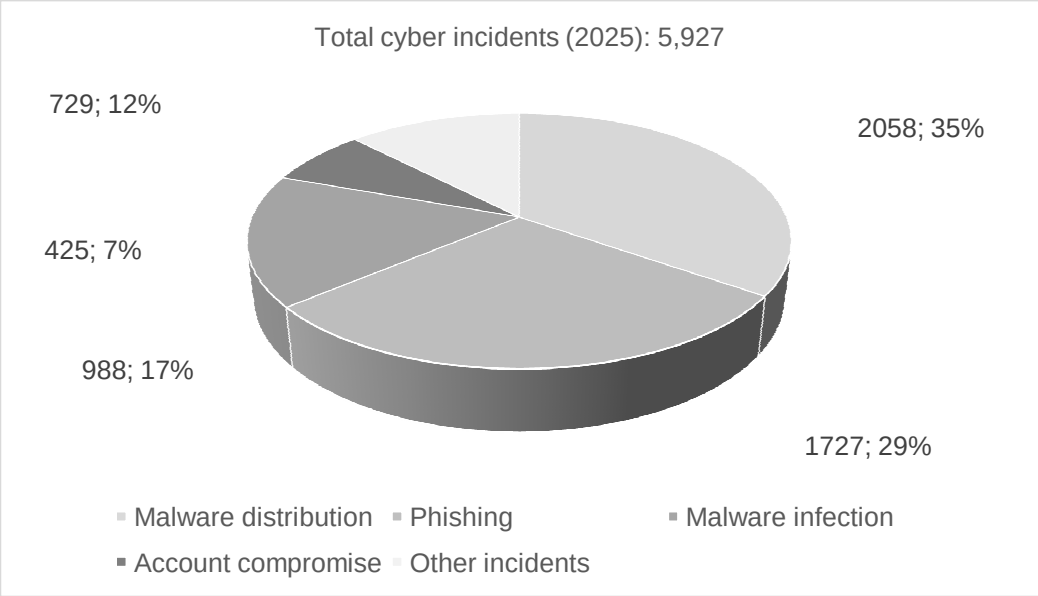

Figure 4. Structure of cyber incidents in Ukraine by type (2025)

Source: Compiled by the author based on official CERT-UA data (2025).

Table 1. Classification of Cyber Risks and Their Impact on the Enterprise Accounting System

Cyber Risk Category	Types of Cyber Threats	Impact mechanism	Impact on Accounting System
Social engineering	Phishing, vishing, fake financial websites	Psychological manipulation of users aimed at obtaining confidential information (logins, passwords, banking credentials)	Unauthorized access to accounting systems, distortion of financial data, fraudulent transactions
Malware (malicious software)	Viruses, Trojans, spyware, ransomware	System infection, data theft or encryption, covert monitoring of user activity	Loss of primary accounting documents, system locking, disruption of accounting continuity, financial losses
Infrastructure attacks	DDoS attacks, server compromise, cloud infrastructure attacks	Overloading or compromising IT infrastructure, disruption of system availability	Unavailability of accounting systems, interruption of accounting processes, risk of data loss or leakage

Source: compiled by the author based on (Chowdhury et al., 2022; Cram et al., 2023; Verkhovna Rada of Ukraine, 2023; Radware, 2025).

The updated classification provides a more comprehensive view of cyber risks by integrating their mechanisms of impact and appropriate control measures within enterprise accounting systems.

Protection against such threats typically includes using specialized DDoS protection services (e.g., Cloudflare, AWS Shield), regularly updating software, implementing multi-factor authentication (MFA), and configuring firewalls. A firewall (network firewall or inter-network screen) is a software- or hardware-based security barrier that monitors and filters incoming and outgoing internet traffic according to predefined security rules. It acts as a protective shield, preventing unauthorized access, cyberattacks, viruses, and malicious content by separating trusted and untrusted networks.

Thus, the financial consequences of cyber incidents for businesses may include direct financial losses, regulatory fines, legal costs, client compensation, a decline in market value, and reputational damage. Accordingly, cybersecurity emerges as a key component of an enterprise's financial security.

CONCLUSIONS

The study has shown that the digitalization of economic processes significantly transforms the nature of risks, giving rise to a new class of threats –cyber risks – which are systemic in nature and directly affect the functioning of enterprises. Cyber risk is the probability of financial losses from disruptions to information systems, unauthorized access to data, or data destruction, thereby increasing the vulnerability of modern accounting and information systems.

The synthesis of theoretical approaches enabled the systematization of the main groups of cyber threats, including social engineering, malicious software, and infrastructure attacks. Each of these groups has specific mechanisms of impact; however, all of them lead to the violation of the integrity, reliability, and availability of accounting information.

Thus, accounting in a digital environment is evolving into a critical enterprise information system, directly affected by cyber threats. The occurrence of cyber incidents may result in data loss or distortion, disruption of accounting continuity, reduced quality of financial reporting, and complications in internal control procedures.

Effective cyber risk management should be based on a comprehensive approach that combines technical security measures, organizational safeguards, and improvements to internal control systems. Therefore, the integration of cybersecurity principles into the accounting system is essential for ensuring the reliability of financial information and the stability of enterprise functioning in the context of the digital economy.

Declaration of Conflicting Interests

The author declarese no potential conflicts of interest with respect to the research, authorship and/or publication of this article.

4 References

Chowdhury, M., Rahman, M., & Islam, S. (2022). Cybersecurity integration framework for accounting information systems: A risk-based approach. *Journal of Cybersecurity and Digital Accounting, 6*(2), 127–139. https://doi.org/10.54660/IJMOR.2022.1.1.127-139

Cognyte. (2025). 2025 Threat Landscape Report: Global trends in cyberattacks, ransomware and stolen credentials. Retrieved from: https://www.businesswire.com/news/home/20250410430200/en/Cognyte-2025-Threat-Landscape-Report-Reveals-Global-Trends-in-Cyberattacks-Ransomware-and-Stolen-Credentials

Cram, W. A., Wang, J., & Yuan, X. (2023). Cybersecurity in accounting information systems: A framework for risk governance. *International Journal of Accounting Information Systems, 48*, 100598. https://doi.org/10.2308/JETA-2020-081

Monteiro, J., & Cepêda, C. (2021). Accounting information systems: Scientific production and trends in research. *Systems, 9*(3), 67. https://doi.org/10.3390/systems9030067

Muravskyi, V., Pochynok, V., & Farion, V. (2021). Classification of cyber risks in accounting. *Visnyk Ekonomiky*, 2, 129–144. https://doi.org/10.35774/visnyk2021.02.129

NCC Group. (2024). Annual Cyber Threat Monitor Report 2024. Retrieved from: https://www.nccgroup.com/newsroom/ncc-group-releases-annual-cyber-threat-monitor-report-2024/

Prokofieva, O. V., & Bespalova, Yu. Yu. (2024). Cyber risks and their management in the context of globalization and digital transformation. *Efektyvna Ekonomika*, 5. http://doi.org/10.32702/2307-2105.2024.5.87

Radware. (2025). Cyber threat report: Web DDoS attacks surge 550% in 2024. Retrieved from: https://www.nasdaq.com/press-release/radwares-cyber-threat-report-web-ddos-attacks-surge-550-2024-2025-02-26

Sigaiev, A., & Volovyk, A. (2017). Botnets: methods of detection and counteraction. *Legal, Regulatory and Metrological Support of Information Protection System in Ukraine*, 1(33). Retrieved from: http://pnzzi.kpi.ua/article/view/169410

State Service of Special Communications and Information Protection of Ukraine. (n. d.). 60% of cyberattacks start with phishing: time to increase vigilance. Retrieved from: https://cip.gov.ua/ua/faqs/60-kiberatak-pochinayetsya-z-fishingu-chas-pidvishiti-pilnist

State Service of Special Communications and Information Protection of Ukraine. (2025). CERT-UA in 2025 processed almost 6,000 cyber incidents: number of hostile attacks increased by 37%. Retrieved from: https://cip.gov.ua/ua/news/cert-ua-u-2025-roci-opracyuvala-maizhe-6000-kiberincidentiv-kilkist-vorozhikh-atak-zrosla-na-37

State Service of Special Communications and Information Protection of Ukraine. (2024). The vulnerability detection and cyber incident response system of the Data Protection Center helped identify and process 1,042 cyber incidents in 2024. Retrieved from: https://www.cip.gov.ua/ua/news/sistema-viyavlennya-vrazlivostei-i-reaguvannya-na-kiberincidenti-ta-kiberataki-dckz-dopomogla-viyaviti-ta-opracyuvati-1042-kiberincidenti-u-2024-roci

State Service of Special Communications and Information Protection of Ukraine. (2023). In 2023, the number of registered cyber incidents increased by 62.5%: report of the Operational Center for Cyber Incident Response. Retrieved from: https://cip.gov.ua/ua/news/2023-roku-kilkist-zareyestrovanikh-kiberincidentiv-zrosla-na-62-5-zvit-operativnogo-centru-reaguvannya-na-kiberincidenti-dckz

State Service of Special Communications and Information Protection of Ukraine. (2022). Statistical report on the results of the Vulnerability Detection and Cyber Incident Response System in 2022. Retrieved from: https://scpc.gov.ua/uk/articles/233

State Service of Special Communications and Information Protection of Ukraine. (n. d.). List of cyber incident categories. Retrieved from: https://www.cip.gov.ua/ua/news/perelik-kategorii-kiberincidentiv

Struk, N. (2026). Assessment of cybersecurity of accounting information in the innovative activities of agricultural enterprises. *Oblik i finansi, 1*(111), 57–70. https://doi.org/10.33146/2518-1181-2026-1(111)-57-70

Vavilenkova, A. (2024). Threats of using cloud services in cybersecurity. *Cybersecurity: Education, Science, Technique*, 2(26), 409–416. https://doi.org/10.28925/2663-4023.2024.26.704

Verkhovna Rada of Ukraine. (2023). Term “DDoS attack”. Legislation of Ukraine. Retrieved from: https://zakon.rada.gov.ua/laws/term/61603

Zhang, C., Zhu, W., Dai, J., Wu, Y., & Chen, X. (2023). Ethical impact of artificial intelligence in managerial accounting. *International Journal of Accounting Information Systems*, 49, 100619. https://doi.org/10.1016/j.accinf.2023.100619